NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF ARTS AND SOCIAL SCIENCES

COURSE CODE: CSS 441

COURSE TITLE: Technical/Electronics Aspects of Security

Course Guide

CSS 441

Technical/Electronics Aspects of Security

Course Developers/Writer s	Dr. R.A Okunola (U.I) Dr. A.T Adegoke (NOUN)
Course Editor	Dr. Wole Atere (OSU)
Course Coordinator	Dr. A.T Adegoke (NOUN)
Programme Leader	Dr Olu Akeusola(NOUN)

INTRODUCTION

CSS 441: Technical/Electronics Aspects of Security is a 3-credit unit course. It is a compulsory course for both undergraduate and postgraduate students in the field of Criminology and Security Studies of the University. The course is also recommended to any other student(s) particularly those in the school of Arts and Social Sciences, who may have interest in the study and survey of security theory and practice. The course can also be taken as elective or required course by other Students whose main field(s) of discipline is not Criminology and Security Studies. However the course shall consist of 20 units, which include: introduction to e-security, electronic risks; e-security in emerging markets, Technological Innovation-costs implication on security; hand and powered tools in security; the Security and electronic banking;; electronic data Interchange (EDI) messaging security; closed circuit television and the role of security Operatives in Surveillance and Information Security in Nigeria, Africa, other developing nations and countries in the Americas and Europe. The knowledge industry and information technology are given special attention with the aim of stimulating effective knowledge of the overall security situations and agenda in the world so that students can identify, analyse, and proffer solutions to various aspect of conventional, modern and traditional mode of security

The course has no compulsory prerequisite for it to be registered for. The course guide informs us on what this course is all about, what students should appreciate in each unit, what text materials we shall be using and how we can make best use of these materials. This course guide also emphasises on the need for students to take tutored marked assignments so seriously. However, necessary information on tutored marked assignments shall be made known to students in a separate file, which will be sent to each of them at appropriate time. This course is also supported with periodic tutorial classes.

What You Will Learn In This Course

CSS 441 **Technical/Electronics Aspects of Security** as a course in the field of Criminology and Security Studies at the National Open University of Nigeria focuses on a wide range of issues that bother on ways to effect basic security measures and policies as well as identification of basic technicalities involve in electronic security vis-à-vis other mode of threats that can jeopardise the safety of any people, community or nation. In this course we will carefully analyse and assess various security measures, usages, advantages and disadvantages. Where possible, their management and operation, to assist the students not only to identify these security technicalities but also to develop a diagnostic framework through which they can proffer solutions towards effective security control and management. In this course, the student or reader will also be exposed to various measures that can safeguard the protection of life and property against incidents of crime and other security related issues.

Nevertheless, the essence of these control and management measures is at least to provide the students with various ways through which he/she can minimise losses from any incident of disaster, if it can not be prevented from occurring. Knowing the impact that active involvement of civilians in security management in an IT world can have in complementing and increasing the capacity of the security personnel to carry out their duties effectively, the course explores the strategic importance of civil

security and how it can contribute to effective security management and threat mitigation. The issue of intelligence is very germane in security studies. Due to this reason, it is not surprising to see a great number of countries expending huge resources in human and financial terms to fortify their environment against or in readiness for any imagined or perceived threats and abnormal technological or electronic warfare; and owing to the fact that security discourse can not be complete without looking at issues of science and technology, the course covers a wide range of issues regarding technicalities and electronic security.

Course Aims

The overall aim of CSS 441: Technical/Electronics Aspects of Security as a course is to introduce you to the basic definitions of concepts relating to technical and electronic aspects of security. It is also aimed at exposing student or reader to knowing most of the existing aspects of electronic security, which may be categorised. In furtherance of its overall aim, the study will also help us to explore some other issues like information on banking and election, warning signs in security management, and software application in security. it also presents the conceptual meaning, case studies and the impact assessment of these issues to illuminate on how they constitute threat to human existence.

Undoubtedly, the way the course draws its references from countries of the West in the analysis of various disasters makes it astounding and thought provoking to providing a pathway for African Students and Scholars in the field of Criminology and Security Studies to help deliberate analytical consciousness on the aspects of general practice of security which are vulnerable to human livelihood with hope of energising them towards developing viable frameworks through which security problems ravaging Nigeria and Africa as a whole can be addressed. As you may be aware disaster issues are always to be considered important and should be given attention. The course is also aimed at understanding:

- the term e-security and enabling technology
- Security Survey of Electronic Crime
- The growing integration of technologies among the Internet, wireless, Internet provider (IP), telephone, and satellite. Security implication.
- Roles of the Private and Public Sectors in E-Security.
- Duties as Chief Information Security Officer (CISO)
- Hand and Power tools in security
- Electronic security, as organization issue
- Electronic Data interchange (EDI)? Discuss any security issue in EDI
- Hardware-based security system
- Current Encryption Technology in security management
- Hackers are able to decrypt all traffic from the browser to secure servers, obtaining information on credit card numbers or other private information.
- Concept of trust and security in e-voting.
- DRE System
- Security surveillance
- Security intelligence
- Basic Engineering concepts in E-Voting Systems
- Online Voting System security requirements.
- Security as an Externality

- The economics of information security
- Concepts of Offence and Defence in Information Warfare
- Features of information technology markets
- Legislation, security and privacy.

Course Objectives

With utmost desire to achieve the aims set out above, the course has some set of objectives as demonstrated in all the units of the course. Each unit has its own objectives. Objectives are always included at the beginning of every unit to assist the student in appreciation of what he or she will come across in the study of each unit to facilitate his or her better understanding of the course CSS. 441: **Technical/Electronics Aspects of Security**. Students are therefore advised to read these objectives before studying the entire unit(s). Thus, it is helpful to do so. You should always look at the unit objectives after completing a unit. In this way, you can be sure that you have done what was required of you by the unit. Stated below are the wider objectives of this course as a whole. By meeting these objectives, you should have achieved the aims of the course as a whole.

At the end of the course, you should be able to:

- Explain the meaning of E-Security
- The impact of Electronic Risks
- Probe into the role E-security in Emerging Markets
- Develop a Risk Management Framework
- Highlight possible policy response to e-security with emphasis on some four Pillars in security.
- Differentiating between hand and powered tools in security
- Explain various ways of securing electronic through the use of computer based software programmes.
- Explain electronic security in the agitation electronic voting
- Probing into Electronic Banking and Security Solutions
- The role of CCTV System in Surveillance and security
- examine basic engineering terminologies in e-security
- Lastly to explain the economics and hard nature of information security

Working through this course

In completing this course, student is required to study the whole units, and try to read all (or substantial number of) the recommended textbooks, journals and other reading materials including electronic resources. Each unit contains self assessment exercise(s) and student is required to submit his or her assignment for the purpose of assignment. At the end of the course, student(s) shall be examined. The time of the final examination and venue shall be communicated to all the registered students in due course by relevant school authorities-study centre management. Below are the components of the course and what you are required to do

Course Materials

Major component of the course include:

1. Course Guide
2. Study Units
3. Textbooks
4. Assignments Files
5. Presentations Schedule

It is incumbent upon every student to get his or her own copy of the course material. You are also advised to contact your tutorial facilitator. If you have any difficulty in getting any of the text materials recommended for your further reading.

Study Units

In this course there are twenty units, divided into four modules, (five in each module). Below are the units:

Module 1
Unit 1. Introduction to E-Security
Unit 2. Electronic Risks
Unit 3. E-security in Emerging Markets
Unit 4. Risk Management Framework
Unit 5.Tradeoffs: Security, Quality of Service, Privacy, Technological Innovation, and Costs

Module 2
Unit 1. Policy Response: Overview of the Four Pillars
Unit 2. Security of Payment Systems
Unit 3. Hand and powered tools in security
Unit 4. Electronic Document Security
Unit 5. Electronic Security: Protecting Your Resources

Module 3
Unit 1. Electronic Voting System
Unit 2. Security Analysis of Remote E-Voting
Unit 3. The Security of Electronic Banking
Unit 4. Security Solutions To Electronic Banking
Unit 5. Electronic Data Interchange (EDI) Messaging Security

Module 4
Unit 1. Converting an Analog CCTV System to IP-Surveillance
Unit 2. Closed Circuit Television and the Role of Security Operatives in Surveillance and Intelligence Gathering
Unit 3. Requirements Engineering for E-Voting Systems
Unit 4. The Economics of Information Security
Unit 5. Hard Nature of Information Security

Text books, Journals and References

Course Material

The following Text books, Journals are course material recommended to each student taking the course.

Required Readings:

Mussington, David, Peter Wilson, and Roger C. Molander. 1998. ñExploring Money Laundering Vulnerabilities Through Emerging Cyberspace Technologies: A aribbean Based Exercise.ò Rand and Critical Technologies Institute (CTI).

Tzekov, Lubomir. 2002. ñE-security Risk Mitigation in Financial Transactions.ò Presentation at the World Bank Global Dialogue on E-security, September 25. http://www1.worldbank.org/finance/html/ dl11bkgd.html. retrieved 18/06/05

Kahn, Alfred E. 1970. *The Economics of Regulation: Principles and Institutions*. John Wiley & Sons, Inc. Kahn, David. 1996. *The CODE-BREAKERS*. Scribner.

Shu-Pui, Li. 2002. E-Security: Risk Mitigation in Financial Transactions. Presentation at the World Bank Global Dialogue on E-security, September25. http://www1.worldbank.org/finance/html/ dl11bkgd.html. retrieved 26/03/10

Tzekov, Lubomir. 2002. ñE-security Risk Mitigation in Financial Transactions.ò Presentation at the World Bank Global Dialogue on E-security, September 25. http://www1.worldbank.org/finance/html/ dl11bkgd.html. retrieved 17/02/09

The United States Financial Intelligence Unitôs (FINCEN) Report, 2003. Suspicious Activity Reports (SARs) for Computer Intrusions: September 15, 2002 to September 15, 2003

Furst, Karen, William W. Lang, and Daniel E. Nolle. 1998. ñTechnological Innovation in Banking and Payments: Industry Trends and Implications for Banks.ò *Quarterly Journal* 17 (3): 23-31.

La Repubblica. 2003. ñMajor Italian Banking and Credit Card Hacking Organization Smashed by Police.ò SNP Security News Portal, January 29, 2003.
E-security 2002. www.worldbank.org/finance. retrieved 09/03/08 The Council of Europe, Convention on Cybercrime, ñhttp://conventions.coe.intò

Bannan, Karen. 2001. ñSafe Passage.ò *PC Magazine*, August. Basel Committee on Banking Supervision. 2001. *Risk Management Principles for E-Banking*, May.

Gilbride, Edward. 2001. ñEmerging Bank Technology and the Implications for E-Crime.ò Presentation, September 3.

John L. Henshaw and Elaine L. Chao 2002. Hand and Power Tools. U.S. epartment of Labor, Occupational Safety and Health Administration. OSHA 3080.

Brown, B. (1995): *CCTV in Town Centres: Three Case Studies*, Crime Prevention and Detection Series, no.73. London: HMSO.

Clarke, R.V.G and Felson, M. (1993): *Routine Activity and Rational Choice*. New York :Transaction Publications.

Evett, C. and Wood, J. (2004): Designing a Control Room, *CCTV Image*, Spring, pp 24-25.
Farrall, S., Bannister, J., Ditton, J. and Gilchrist, E. (2000): óSocial Psychology and the Fear of Crime: Re-examining a Speculative Modelô, *British Journal of Criminology*, 40, 399-413.

Laycock, G. and Tilley, N. (1995): *Policing and Neighbourhood Watch: Strategic issues*, Crime Detection and Prevention Series, 60. London: HMSO.

Schryen, G. (2004). ñSecurity Aspects of Internet Votingò, Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS 37), January

Mercuri, R., Neumann, P.G (2003) "Verification for Electronic Balloting Systems" Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 31-42. Kluwer, Boston.

Ted Humphreys, 2006: Electronic Data Interchange (EDI) Messaging Security. Journal of Information Security. Pp.423-438.

Pratchett, L. (2002) "The implementation of electronic voting in the UK" LGA Publications, the Local Government Association.

Jefferson D., A.D. Rubin, B. Simons, and D. Wagner. Analyzing internet voting security. Communications of the ACM, 47(10):59ï 64, 2004.

Tavani H.T. Defining the boundaries of computer crime: piracy, breakins, and sabotage in cyberspace. ACM SIGCAS Computers and Society, 30(3):3ï 9, 2000.

Pfleeger, Charles P. 1997. Government. Emerging electronic methods for making retail payments. June 1996. Security in Computing. Prentice Hall,

Tim Wilmshurst, ñAn Introduction to the design of small-scale embedded systemsò, ISBN: 0-333-92994.

W Curtis, H Krasner, N Iscoe, 1988. A Field Study of the Software Design Process for Large Systems", in *Communications of the ACM* v 31 no 11 (Nov 88) pp 1268-1287

K. Campbell, L. A. Gordon, M. P. Loeb and L. Zhou. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. In J. Comput. Secur. 11, 431 (2003).

Schryen, G. (2004). ñSecurity Aspects of Internet Votingò, Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS 37), January

I. Bray, An Introduction to Requirement Engineering. Harlow Essex: Addison Wesley, 2002.

F. Breyfogle, Implementing Six Sigma: Smarter Solutions Using Statistical Methods, Wiley, 1999.

A. D. Rubin, ñSecurity Considerations for Remote Electronic Voting,ò CACM, vol. 45, pp. 39-44, Dec. 2002.

Buckwalter A. 1984. Surveillance and Undercover Investigation Butter Writh, Criminal Investigation

Anderson, W.B 1987. Notable Crime Investigation, Spring Field, III Thomas.

Schultz D.O. 1978. Criminal Investigation Techniques Houston, Gulf Publishing,
Norris, C., and G. Armstrong (1997) óCategories of control: the social construction of suspicion and intervention in CCTV systems.ô A draft manuscript of *The Rise of the Mass Surveillance Society*, Oxford: Berg.

R. S. Pressman, Software Engineering: A Practitionerôs Approach. New York NY: Addison Wesley, 2005.

K. Daimi, and C. Wilson, ñElectronic Voting System Security requirements Engineering,ò in Proc. The International Conference on Software Engineering Research and Practice 2005, Las Vegas, USA, pp. 230-235.

Assignment File
In this file you will find the necessary details of the assignments you must submit to your tutor for assessment. The marks you get from these assignments will form part of your final assessment in this course,

Assessment
There are two aspects to the assessment of the course. First are the tutor-marked assignment; second there is the written examination. In tackling the assignments, you are expected to apply information and knowledge acquired during this course. The assignments must be submitted to your tutor for assessment in accordance with the deadlines stated in the Assignment file. The work you submit to your tutor for assessment will count for 30% of your total course work. At the end of the course, you will need to sit for a final three-hour examination. This will also count for 70% of your total course mark.

Tutor- Marked Assignment
There are twenty tutor-marked assignments in this course. You need to submit four assignments out of which the best three will be used for your assessment. These three assignments shall make 30% of your total course work. Assignment question for the units in this course are contained in the assignment file. You should be able to complete your assignments from the information and materials contained in your set textbooks, reading and study units. However, you are advised to use other references to broaden your view point and provide a deeper understanding of the subject. When you have completed each assignment, send it together with TMA (Tutored-Marked Assignment) file to your tutor. Make sure that each assignment gets to your tutor on or before the deadline. And in case of being unable to complete your work on time,

contact your tutor or better still your study centre manager (overseer) before the submission deadline of assignments elapses to discuss the possibility of an extension.

Final examination and grading

The final examination of CSS 441 shall be of three hours duration and have a value of 70% of the total course grade. The examination shall consist of questions which reflect the type of self-testing. Practice exercises and tutor-marked problems you have come across. All areas of the course will be assessed. You are advised to revise the entire course after studying the last unit before you sit for the examination. You will find it useful to review your tutored-marked assignments and the comments of your tutor on them before the final examination.

Course Marking Scheme.

This table shows how the actual course marking is broken down.

Assessment	Marks
Assignment 1-4	Four assignments are to be submitted, out of which the three best shall be considered at 10% each, making 30% of the overall scores
Final Examination	70% of overall course marks
Total	100% of course marks.

Table 1: Course Marking Scheme

Course Overview

The table brings together the entire units contained in this course, the number of weeks you should take to complete them, and the assignments that follow them.

Unit	Title	Week's Activity	Assessment (end of unit)
	Course Guide	1	
1.	Introduction to E-Security	1	Assignment 1
2.	Electronic Risks	2	Assignment 2
3.	E-security in Emerging Markets	2	Assignment 3
4.	Risk Management Framework	3	Assignment 4
5.	Tradeoffs: Security, Quality of Service, Privacy, Technological Innovation, and Costs	4	Assignment 5
6.	Policy Response: Overview of the Four Pillars	5	Assignment 6
7.	Security of Payment Systems	6	Assignment 7
8.	Hand and powered tools in security	6	Assignment 8
9.	Electronic Document Security	7	Assignment 9
10.	Electronic Security: Protecting Your Resources	7	Assignment 10
11.	Electronic Voting System	8	Assignment 11
12.	Security Analysis of Remote E-Voting	9	Assignment 12
13.	The Security of Electronic Banking	10	Assignment 13
14.	Security Solutions To Electronic Banking	11	Assignment 14

15.	Electronic Data Interchange (EDI) Messaging Security	11	Assignment 15
16.	Converting an Analog CCTV System to IP-Surveillance	12	Assignment 16
17.	Closed Circuit Television and the Role of Security Operatives in Surveillance and Intelligence Gathering	13	Assignment 17
18.	Requirements Engineering for E-Voting Systems	14	Assignment 18
19.	The Economics of Information Security	15	Assignment 19
20.	Hard Nature of Information Security	16	Assignment 20
21.	Revision	17	
22.	Examination	18	

Table 2: Course Overview

Presentation Schedule

The presentation Schedule included in your course materials gives you the important dates for the completion of tutor-marked assignments and attending tutorials. Remember you are required to submit all your assignments by the due date. You should guard against falling behind in your work.

How To Get The Best From This Course

In distance learning the study units replace the university lecturer. This is one of the great advantages of distance learning; you can read and work through specially designed study materials at your own pace, and at a time and place that suit you best. Think of it as reading the lecture instead of listening to a lecturer. In this same way that a lecturer might set you some reading to do, the study units tell you when to read your set of books or other materials. Just as a lecturer might give you an in-class exercise, your study units provide exercises for you to do at appropriate points. Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit and the course as a whole. Next is a set of learning objectives. These objectives shall let you know what you should be able to do by the time you have completed the unit. You should use these objectives to guide your study. When you have finished the units, you must go back and check whether you have accepted the objectives. If you have a habit of doing this you will significantly improve your chances of passing the course. The main body of the unit guides you through the required reading from other sources.

Reading Section

Remember that your tutorôs job is to assist you. Whenever you need help, do not hesitate to call and ask your tutor to provide it.

1. Read this Course Guide thoroughly.

2. Organised a Study Schedule. Refer to the óCourse Overviewô for more details. Note the time you are expected to spend on each unit and how the assignments

related to the units. Whatever method you chose to use, you should decide on and write in your own dates for working on each unit.

3. Once you have created your own study schedule, do everything you can to stick to it. The major reason why students fail is that they get behind with their course work. If you get into difficulties with your schedule, please let your tutor know it is too late for help.

4. Turn to unit 1 and read the introduction and the objectives for the unit.

5. Assemble the study materials. Information about what you need for a unit is given in the óOverviewô at the beginning of each unit. You will almost always need both the study unit you are working on and one of your set books on your desk at the same time.

6. Work through the unit. The content of the unit itself has been arranged to provide a sequence for you to follow. As you work through the unit s you will be instructed to read sections from your set books or other materials. Use the unit to guide your reading.

7. Review the objectives for each study unit to confirm that you have achieved them. if you feel unsure about any of the objectives, review the study materials or consult your tutor.

8. When you are confident that you have achieved a unitôs objectives, you can then start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep yourself on schedule.

9. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned pay particular attention to your tutorôs comments, both on the tutor-Marked Assignment from and also on what is written on the assignment. Consult your tutor as soon as possible if you have any questions or problems.

10. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in this Course-Guide).

Facilitators/Tutors and Tutorials

There are between eight (8) and twelve (12) hours of tutorials provided in support of this course. The dates, time and venue of these tutorials shall be communicated to you. The name and phone number of your tutor will be made available to you immediately you are allocated a tutorial group. Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must mail your tutor marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible. Do not hesitate to contact your tutor by phone, e-mail, or discussion board if you need help. You will definitely benefit a lot by doing that. Contact your tutor if:

- You do not understand any part of the study units or the assigned readings;
- You have difficulty with the self-tests or exercises; and ;
- You have a question or problem with an assignment, with your tutorôs comment on an assignment or with the grading of an assignment.

You should make an effort to attend the tutorials. Thus, it is the only opportunity you have to enjoy face contact with your tutor and to ask questions which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefits from the course tutorials, prepare a question list before attending them. You will learn a lot from participating in discussion actively.

Summary

- CSS: 441 aims to expose you to issues, ideas and methodologies, framework in engaging some common tecknicalities in electronic security as well as various technological advancement in the an increasing Information Technological world where the world wide web and cyber space control commerce and vitually every part of human life. As you complete this course, you should be able to answer and discuss reasonably the following:
  - Understanding the term e-security
  - Security Survey of Electronic Crime
  - The growing integration of technologies among the Internet, wireless, Internet provider (IP), telephone, and satellite. Security implication.
  - Roles of the Private and Public Sectors in E-Security.
  - Duties as Chief Information Security Officer (CISO)
  - Hand and Power tools in security
  - Electronic security, as organization issue
  - Electronic Data interchange (EDI)? Discuss any security issue in EDI
  - Hardware-based security system
  - Current Encryption Technology in security management
  - Hackers are able to decrypt all traffic from the browser to secure servers, obtaining information on credit card numbers or other private information.
  - Concept of trust and security in e-voting.
  - DRE System
  - Security surveillance
  - Security intelligence
  - Basic Engineering concepts in E-Voting Systems
  - Online Voting System security requirements.
  - Security as an Externality
  - The economics of information security
  - Concepts of Offence and Defence in Information Warfare
  - Features of information technology markets
  - Legislation, security and privacy.

Finally, you are advised to read the course material appreciably well in order to prepare fully and not to be caught pants down by the final examination questions. So, we sincerely wish you success in your academic career as you will find this course (CSS 441) very interesting. You should always avoid examination malpractices!

CSS 441

Technical/Electronics Aspects of Security

Course Developers/Writer s — Dr. R.A Okunola (U.I)
Dr. A.T Adegoke (NOUN)

Course Editor — Dr. Wole Atere (OSU)

Course Coordinator — Dr. A.T Adegoke (NOUN)

Programme Leader — Dr Olu Akeusola(NOUN)

Module 1

Unit 1. Introduction to E-Security
Unit 2. Electronic Risks
Unit 3. E-security in Emerging Markets
Unit 4. Risk Management Framework
Unit 5.Tradeoffs: Security, Quality of Service, Privacy, Technological Innovation, and Costs

UNIT 1

Introduction to E-Security

Contents

1.0 INTRODUCTION

Every day, governments, business, and consumers choose to use new technologies to build a global electronic economy. It is becoming apparent that the impacts of the use of these technologies on sustainable development deserve increased attention. This includes defining personal privacy and determining how to best protect it; deciding what levels of trust and confidence in service providers should be expected; determining how to measure these attributes; and deciding what protections should be provided by security measures. This section identifies and discusses four key pillars that are necessary to foster a secure electronic environment and the safety and soundness of financial systems worldwide. Hence, it is intended for those formulating policies in the area of electronic security and those working with financial service providers (such as executives and management). The detailed annexes of this reading material are relevant for Chief Information and Security Officers and others who are responsible for securing network systems. First, the material defines electronic finance (e-finance) and electronic security (e-security) and explains why these areas require attention. Next, it presents a picture of the emerging global security industry. Then, it develops a risk management framework to assist policymakers and practitioners in understanding the tradeoffs and risks inherent in using an open network infrastructure. It also provides examples of tradeoffs that may arise with respect to technological innovations, privacy, quality of service, and security in the design of an e-security policy framework. Finally, it outlines issues in four critical and interrelated areas that require attention in the building of an adequate e-security infrastructure. These are: (i) the legal, regulatory, and enforcement framework; (ii) external monitoring of e-security practices; (iii) public-private sector cooperation; and (iv) the business case for practicing layered e-security that will improve internal monitoring.

2.0 Objectives

At the end of this unit, students should be able to:

a. Define and explain the term e-security and other related concepts

b. Identify various public policy framework to improve electronic safety

3.0 Main body

3.1 What is Electronic Security?

Speaking broadly, electronic security (e-security) is any tool, technique, or process used to protect a systemôs information assets. E-security enhances or adds value to an unprotected network, and is composed of soft and hard infrastructures. The soft infrastructure components are the policies, processes, protocols, and guidelines that protect the system and the data from compromise. The hard infrastructure consists of hardware and software needed to protect the system and data from threats to security from inside or outside the organization. As a business principle, the appropriate degree of e-security used for any activity should be proportional to the activityôs underlying value. E-security is a risk-management and risk-mitigation tool. Todayôs growing worldwide e-security industry provides a wide variety of targeted security services ranging from active content filtering, firewalls, intrusion detection, penetration testing, cryptographic tools to authentication mechanisms. Given that the Internet and other open network technologies basically are broadcasting mediums transmitting across an unprotected network, it is critical that security be added to assure that the information is sent only to the intended recipients, rather than accessible to the world at large. E-Security is an increasingly important issue as technology plays an ever greater role in the delivery of financial services and promotion of e-commerceð and it would be worthwhile for policymakers to appreciate the urgency with which this issue should be addressed. By 2005, it is estimated that the share of banking done online will be close to 50 percent in industrial countries and will rise from one to almost ten percent in emerging markets (Claessens, Glaessner, Klingebiel, 2002). In both developed and emerging markets, the key sectors of the payment systems are migrating to an Internet based platform. There can be little doubt that in emerging markets it is even more critical that efforts be undertaken to ensure the trust and confidence of e-market participants. The safety and soundness of their electronic transactions is an essential infrastructure needed to support sustainable development and to realize the benefits of the new economy. Moreover, this is an issue with truly global implicationsð already thieves are taking advantage of weak regulatory environments to base their operations in one country, but attack institutions in others. As financial markets become increasingly integrated, the systemic risks of such attacks increase, and it will be emerging markets, with the least financial and institutional depth, that prove to be most vulnerable.

3.2 The Problems of Economic Incentives Posed by Electronic Security

In addition to providing e-security, a small number of vendors supply a multitude of interlinking services to e-finance providers (for example, financial service companies)

in many countries. The cross-linking ownership raises many complex questions, such as the need to review the adequacy of competition policy, as well as the potential for, and ramifications of, multiple conflicts of interest. More important may be issues of the impact of ownership concentration on systemic risk, and the lack of incentives to report security breaches accurately. Convergence of the telecommunications industry and the financial services sector through the Internet heightens the importance of, and the necessity for, sound public policy and informed regulation to ensure that government, business, and people continue to have access to secure financial services. Beyond the issues raised by cross-linked ownership of the e-security and telecommunications industries, there are even more basic issues to address in designing an e-security public policy framework.

First, telecommunications, energy, and financial services are crucial components of the critical infrastructures in every country. Disrupting these infrastructures for even a short period of time can cause significant economic and other damage to a country. Each of these infrastructures relies heavily on electronics. Given the risks that electronic vulnerabilities pose to a countryôs critical infrastructures, e-security is an essential risk management tool, important in promoting and protecting the public interest and welfare. There is a fundamental public interest case for a government to regulate its financial services. The case has grown even stronger with these technologies so as to ensure that the financial system and its related components use the necessary level of e-security and access remains stable.

Second, a market failure is occurring because inadequate incentives exist within the workplaceð as well as the regulatory and enforcement arenasð to require the timely and accurate reporting of e-security breaches. Clearly, regulators have a role to play in overcoming this dilemma. By requiring timely and accurate reporting with sufficiently strong penalties for failing to report, management and/or employees are given an incentive structure that encourages the reporting of breach incidents to appropriate authorities.

Third, the reach of the Internet and open network technologies implies that access to financial services is global and its availability is no longer constrained by borders. The feared domino effect and contagion experienced so often in the financial services industries in the 1980s and 1990s serve to remind us of the dangers of an over-reliance on any given aspect of finance and the ensuing disproportionate concentration of risk. Hence mitigating e-security risks requires unprecedented efforts to promote collective action within countries (for example, interagency and public-private sector cooperation) as well as between countries by market participants, regulators and law enforcement.

Fourth, formulating e-security policy must balance a number of complex competing concerns; in the end, e-security cannot be seen as an end in itself, but rather as only one aspect of risk management. Given the interconnected nature of the global payments system it is a crucial fundamental component of global risk mitigation. The domino effect of a single e-bank failure could have significant ramifications. Tradeoffs exist between the costs of providing financial services, the size of a bankôs transactions, and the sophistication of the e-security arrangements that may be required to mitigate the risks. In addition, it is necessary to carefully weigh essential tradeoffs between the paradox of using security to protect privacy versus a barrier to

access. These tradeoffs cannot be decided in isolation. The public and private sectors must work through these issues on a collaborative basis.

In the light of these four complex public policy issues any approach to designing a public policy framework to improve electronic safety and soundness will need to rest on four fundamental pillars.

- Pillar 1: Strengthening the overall legal, regulatory, and enforcement framework within and across countries.

- Pillar 2: Improving external monitoring of e-security risks at a variety of levels that include: improvements in technology supervision (on and off-site); better monitoring by private insurance companies; and improving the education about these risks at the level of final users in companies and among consumers.

- Pillar 3: Establishing public/private partnerships within and across countries in two critical areas: improving the basic database for e-security incident information worldwide; and improving and gradually harmonizing the certification processes and standards in e-security in a careful manner that allows for rapid dynamic technological change inherent in this area.

- Pillar 4: Strengthening internal monitoring, by clearly identifying business objectives that link the costs of not securing a business to the potential and actual savings from e-security. Improve incentives for financial service providers and vendors to adopt e-security as a required element in any online business process and use,

* these four pillars will be extensively discussed in unit 2.

Self Assessment Exercise

Discuss the effect of modern day technologies on security

4.0 Conclusion

The importance of e-security cannot be overemphasised in reducing the rate of crime in upcoming economies with high failure rates. Though electronic security (e-security) as defined; is composed of soft and hard infrastructures involving tools, techniques, or processes used to protect a systemôs information assets. It is germane to state that E-security is an offshoot of the knowledge industry therefore it is envisaged that it will enhance or add value (s) to an unprotected network of people, nations, and services if properly utilised.

5.0 Summary

In this unit, our focus has centred on describing and explaining the meaning of e-security, risk management tools in developing economies and telecommunications industries in the designing of an e-security public policy framework.. The writer wishes to inform that there are other definitions and related issues on electronic security and technicalities involved. Other issues not discussed here can easily be found on the internet and other scholarly materials recommended. In case students

have any question regarding any aspect of this study for assistance please contact your tutorial facilitator.

6.0 Tutor Marked Assignment

(1) What do you understand by the term e-security?
(2) Discuss some policy framework to improve electronic safety?

7.0 References/ Further Reading

(1) Arkin, Ofir. (2002). ñWhy E.T. Canôt Phone Home? Security Risk Factors with IP Telephony-based Networks.ò Sys-Security Group, November. http://www.syssecurity.com/archive/papers/Security_Risk_Factors_with_IP_Telephony_based_Networks.pdf

(2) Claessens, Stijn, Thomas Glaessner, and Daniela Klingebiel. (2002). *Electronic Finance: A New Approach to Financial Sector Development.* World Bank Discussion Paper No. 431. Washington, D.C.

(3) European Central Bank. (2003). *Electronic Money System Security Objectives. according to the Common Criteria Methodology.* May.

(4) Furst, Karen, William W. Lang, and Daniel E. Nolle. (1998). ñTechnological Innovation in Banking and Payments: Industry Trends and Implications for Banks.ò *Quarterly Journal* 17 (3): 23-31.

(5) Glaessner, T. C., K Ellermann T. Mcnevin, V. (2004) Electronic Safety and Soundness: *Securing Finance in a New Age. A* World Bank Working Paper No. 26.

(6) Kellermann, Tom. (2002). *Mobile Risk Management: E-Finance in the Wireless Environment.* World Bank, Washington D.C. http://wbln1023.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/Mobile_Risk_Management/$FILE/Mobile_Risk_Management.pdf.

(7) *La Repubblica*. (2003). ñMajor Italian Banking and Credit Card Hacking Organization Smashed by Police.ò SNP Security News Portal, January 29.

Unit 2.
Electronic risk

CONTENTS

1.0 Introduction

Electronic Risks

The access and availability that the Internet and new communications technologies provide are two way streetsð interconnectedness allows us to reap mutual benefits, but also forces us to bear common risks to critical infrastructures. Reliance on computers for back-end operations, and integration with the Internet and other open network technologies as the front-end interface, allows anyone to enter a system and disrupt, disable or corrupt business, government, education, hospitals, financial services and any other sectors that rely on computers as their business engine. Privacy, security, safety and soundness are all at risk, as economic pressures to increase speed and reduce costs force business to use new technologies to integrate functions and services in order to compete.

These same technologies also facilitate more efficient and quicker ways to commit old crimes such as fraud and theft. Remote access, high-quality graphics and printing, and new multipurpose tools and platforms provide greater means to commit such crimes as theft and impersonation online (Jupiter Communications 2001). Disturbingly, as the technology becomes more complex, a perpetrator needs fewer skills to commit these crimes. While the art of online penetrations (that is, hacking), was once a highly sophisticated skill, now underground hacker websites provide multifaceted tools necessary to break into financial platforms. Perhaps the most frightening risk associated with the convergence of technology and crime is the speed and magnitude with which the crimes can be undertaken. For example, in the past it would have taken months or perhaps even years for highly organized criminals to steal 50,000 credit card numbers. Today, one criminal using tools that are freely available on the Web can hack into a database and steal that number of identities in seconds.

2.0 Objectives

At the end of this unit, you should be able to:

a. Understand and explain the term electronic risk.

b. Explain the need to study its implication in a globalising world.

c. Identify various risks associated with electronic transactions

3.0 Main body

3.1 Security Survey of Electronic Crime

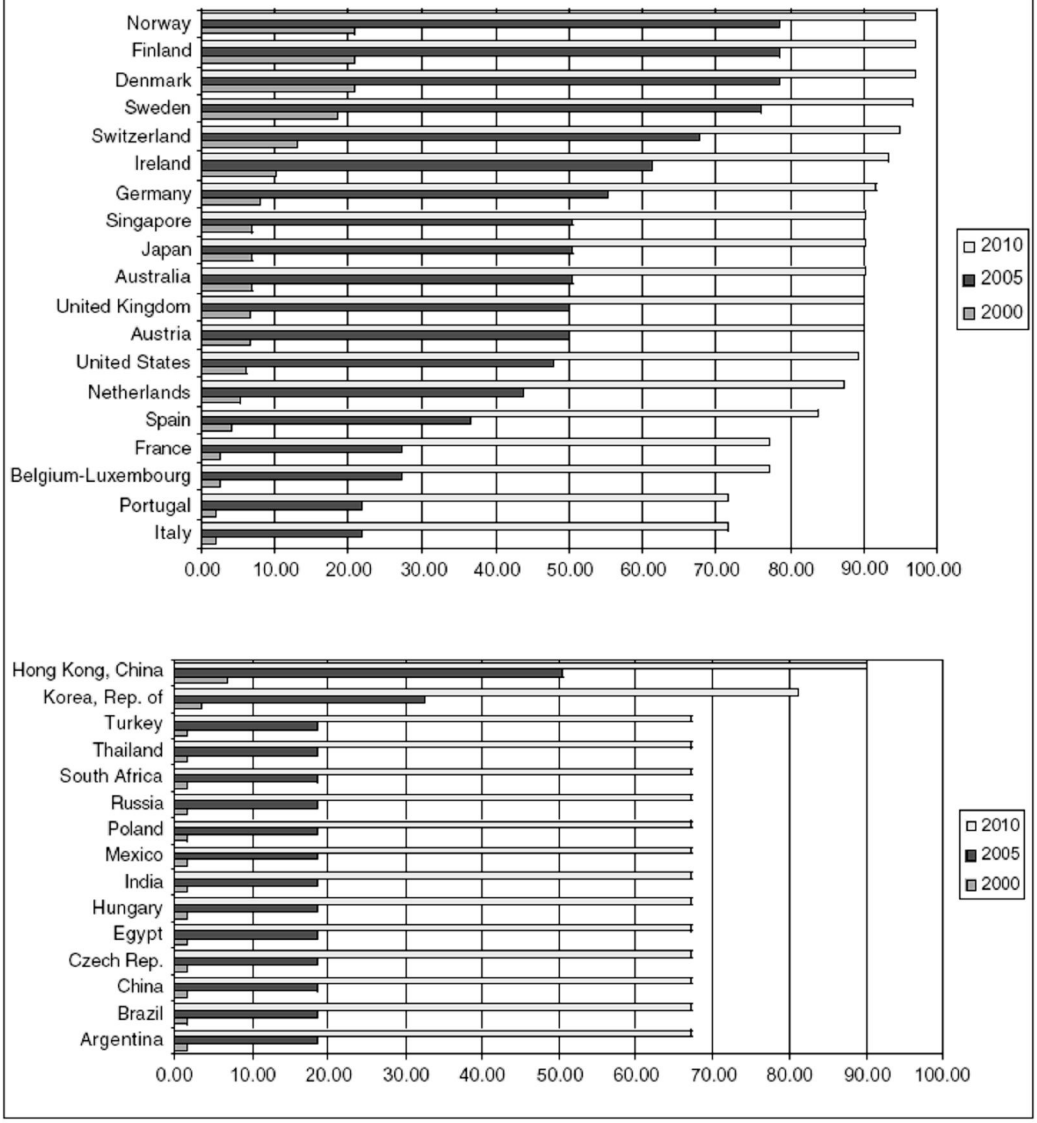
Upward trends in cyber crime statistics reveal that criminals are in fact taking advantage of both the speed and capabilities which new technologies offer (see Annex A for a detailed listing of major e-security incidents made public). Attacks on servers doubled in 2001 from 2000. The 2002 CSI/FBI Computer Crime Survey (for additional information visit: www.gocsi.com) reported that 90 percent of organizations in the United States (including large companies, medical institutions, and government agencies) detected security breaches. Moreover, serious security breaches such as theft of proprietary information, financial fraud, denial of service attacks, and network compromises were reported by 70 percent of organizations in 2001. Eighty-four percent of the surveyed organizations cited the Internet connection as the critical point of attack (FBI and CSI 2003). The CERT chart below illustrates an upwards trend in reported cyber crime incidents. In addition to Internet service interruption, cyber crime incidents can also put significant financial losses at stake. The 2003 CSI/FBI Computer Crime and Security Survey indicates that total annual losses reported by 251 organizations amounted to nearly $202 million. The Internet Data Corporation recently reported that more than 57 percent of all hack attacks last year were targeted towards the financial sector (www.idc.com; and www.cert.org)). A Bank for International Settlements 2002 report on loss events surveyed 89 international banks and determined that those 89 banks sustained 47,000 loss events in 2002 (www.bis.org.). Sixty percent of those loss events occurred in retail banking and over 42 percent of losses were attributed to external fraud. In short, without strong security controls, banks risk the possibility of financial loss, legal liability, and harm to their reputation (United States Financial Intelligence; 2002). Several pervasive venues for electronic attacks in the area of e-financial services have been publicly documented, but continue to be problematic. The most frequent problems in this arena are:

(i) insider abuse,
(ii) identity theft,
(iii) fraud, and
(iv) breaking and entering, often conducted by hackers.

Though these areas must be addressed and risks mitigated, there continues to be a relative lack of accurate information about intrusions and associated losses. This deficiency in reporting intrusion to regulators and law enforcement agents is the fundamental reason why issues related to e-security are not recognized as an immediate priority. In the United States, a 2001 CSI/FBI Computer Crime Survey identified the following five major reasons organizations did not report electronic intrusions to law enforcement agents:

- Negative publicity;
- Negative information competitors would use to their advantageð for example, to steal customers;
- Lack of awareness that they could report events;
- Decision that a civil remedy seemed best;
- Fear among IT personnel of reporting incident because of job security.

FIGURE 1.1: E-FINANCE PENETRATION: 2000 AND PROJECTED RATES FOR 2005 AND 2010



Note: The figures show projections based on takeoff years with better connectivity. The projections assume that all emerging markets have the same connectivity rating as in today's lowest-ranked industrial country, 6 (or better if their current rating is already higher); thus, the projections lead to the same minimum level of penetration in each emerging market.

Source: Claessens, Glaessner, and Klingebiel 2002.

FIGURE I.2: NUMBER OF INCIDENTS REPORTED BY CERT, WORLDWIDE

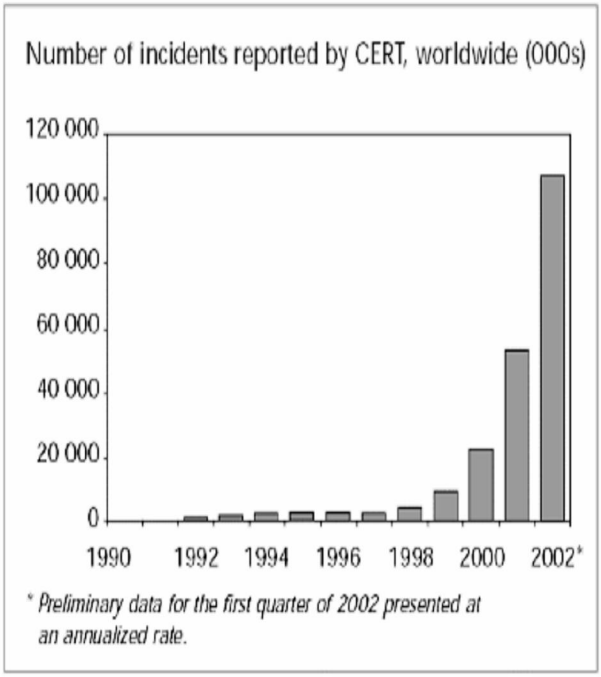


TABLE 1.1: GLOBAL CONNECTIVITY TRENDS

Country	Number of mobile phone subscribers (Millions)	Percentage of population who are mobile or cellular subscribers	Percentage of population who are Internet users
Developed Countries[a]	**45.0**	**64**	**39**
Australia	11.2	58	34
Finland	4.0	78	43
France	35.9	61	26
United States	127.0	44	50
United Kingdom	47.0	78	40
Developing Countries[a]	**21.6**	**15**	**7**
Brazil	28.7	17	5
Bulgaria	1.6	19	8
Cambodia	.2	2	<1
China	144.8	11	3
Egypt	2.8	4	1
Guatemala	1.1	10	2
India	5.7	1	1
Indonesia	5.3	2	2
Mexico	20.1	20	3
Philippines	10.6	14	3
Republic of Korea	29.0	61	51
South Africa	9.2	21	7

a. These are averages for developed and developing countries respectively.
Source: International Telecommunications Union, *World Telecommunications Indicators Database 2001.*

3.2 Decomposing the Risks Associated with Electronic Transactions

Many governments acknowledge the large inherent difficulty in estimating the full magnitude of the money laundering (ML) problem. For example, former IMF Director Michel Camdessus estimated the global volume of ML at between two to five percent of global GDP, a range encompassing $600 billion to $1.8 trillion. One example of how this phenomenon is growing via the Internet are the operations of E gold. This site provides users with an electronic currency, issued by E-gold Ltd., a Nevis corporation, 100 percent backed at all times by gold bullion in allocated storage. E-gold was created in response to a need for a global currency on the World Wide Web. E-gold operates in units of account by weight of metal, not US dollars or any other national currency unit. Weight units have a precise, invariable, internationally recognized definition. Additionally, precious metals, gold in particular, enjoy a long history of monetary use around the world. Thus, E-gold is being used for international transactions. Here a ñnon-financial institution is becoming a de facto money remitter or intermediary. No real records are stored, few diligence standards are followed, no specific reports on suspicious activity are filed, etc. E-gold sells the ability for people to exchange money, thus circumventing the financial institutions and their corresponding oversight/regulatory mechanisms. Intangible services like consulting are common facades for the disbursement of funds between organized criminal syndicates. These entities usually establish themselves in jurisdictions where

secrecy laws prevent adequate disclosure. For example, E-Gold utilizes the Internet and nations like Luxemburg and other neutral regimes to base their servers. It is important to state here that public awareness is the critical first step. However, there are inherent reasons why it will be difficult to address these issues without some public sector role. Technological advances have created a much more complex interrelationship between e-security and risks of different types. Attempts to systematically see how electronic transactions impact the old risk paradigm highlights some new sources of risk, although the basic categories of risk are not new, and financial service providers have always viewed them with concern. Some of these risks are listed and explained below:

Systemic Risk. One of the most important links between e-finance, e-security, and risk is the systemic impact that the associated risks can have on the related payment systems through interaction with compromised networks. Appropriate security should be proportional to the value of underlying transactions. For this reason, in the case of large-value clearinghouses, extensive e-security is or should be in place. Any intrusion or interruption in a payment systemôs electronic messaging could easily create significant system-wide exposure. Recent trends whereby major large-value payments networks are increasingly moving to voice over Internet protocol suggests that increasing care will be needed in the security of such systems as Society for Worldwide Interbank Financial Telecommunication (SWIFT) because it has moved from a closed legacy mainframe to an Internet technology backbone. Another source of systemic risk that could become more importantð especially in emerging marketsð relates to the concentration or single point of failure associated with hosting services that are often provided by only one company to all the major banks. Hence a compromising of this third party provider can cause extensive problems for the banks.

Operational Risk. Inadequate e-security can result in interruptions of service andð in some cases, depending on the nature and adequacy of backup systemsð even the loss of critical information. As part of managing operational risk, financial services providers worldwide need to pay greater attention to the way they secure their IT systems. The risks involved in e-security often relate to extortion and reputation risk, which usually are not specifically taken into account in the allocations set aside to cover operational risk.

Risk of Identity Theft, Fraud, and Extortion. Penetration by hackers often leads to extortion demands. In addition, identity theft is a growing concern for e-finance service providers. Its growth has been rapid, but as in the case of hacking, it is not reported in a timely manner or accurately; thus, its growth may be considerably understated. This problem is not unique to financial servicesð it also affects the integrity and reliability of the credit information gathered and assessed by credit bureaus, downstream to credit decisions.

Risk of money laundering. Financial Action Task Force (FATF) principle XIII stipulates that knowledge of oneôs customers is critical in deterring money laundering, but unfortunately the very nature of the Internet and with the proliferation of e-finance, ñknow thy customerò has become extremely difficult in cyber space. The existence of special financial service providers like ñE-goldò coupled with the anonymity provided by the Internet hamper efforts to curtail money laundering.

Beyond the risks of identity theft or extortion, the use of the Internet and a large variety of casino websites along with other forms of quasi payment arrangements over the Internet can be shown to facilitate what amounts to the electronic laundering of money (Mussington, et al. 1998).

Risk of Credit Quality Deterioration for the Financial Services Provider. Although not often acknowledged, a substantial denial of service or long-term intrusion that results in fraud, impersonation, or corruption of data can effectively cripple a bankôs operations for a period of time. If that time is sufficient, it can irreparably damage the bankôs reputation and possibly compromise its credit standing. Because market participantsô confidence is critical, such an event could have a pernicious impact in a relatively short time.

Risks in Failure Resolution. A final form of risk associated with the delivery of e-financial services and security relates to the risks introduced when a brick-and-clicks or wholly Internet based bank fails. Here the process of closure itself is difficult to define and even more difficult to implement if the entity has its servers in offshore centres. Closure in this case would require extensive cross-border coordination among authorities in what could be numerous disparate jurisdictions. Cooperation, and thus closure, may not be feasible with the speed that can be applied in the case of a non-Internet-based bank. At the point of intervention, if the records and other essential information about digital assets are not preserved under well-defined guidelines, and if they are not secured or cannot be retrieved from servers, then, at the very least, claimantsô rights may be compromised.

Self Assessment Exercise;

1. List and explain some of the factors in decomposing the risk in electronic transactions.

2. What are the major reasons hindering crime reporting to law enforcement?

4.0 Conclusion

No doubt the alarming rate at which electronic crimes are being perpetuated has put in place a lot of measures in combating the menace. Some of such measures include first and foremost knowing the various risks involved in electronic transactions, which to a large extent brings about proper check against intruders of secured personal codes.

5.0 Summary

In this unit, our focus has centred on describing and explaining statistical trends in electronic risks individuals and nations are exposed to. Also noted is the notion that some of these risks are not perpetuated by complete strangers but also with the connivance of insiders in the industries.

6.0 Tutor Marked Assignment

ñGlobal electronic risk is on the increaseò. Explain with the use of current global statistics and tables.

7.0 References/ Further Reading

(1) Bank of International Settlements, www.bis.org. retrieved 01/02/10

(2) Kellermann, Tom and Yumi Nishiyama. (2003). *Blended Electronic Security Threats: Code Red, Klez, Slammer, and Bugbear.* World Bank, Washington, D.C.

(3) *La Repubblica*. (2003). ñMajor Italian Banking and Credit Card Hacking Organization Smashed by Police.ò SNP Security News Portal, January 29, 2003. www.idc.com..2002. Worse Year for hacking in the United States. Retrieved 17/01/08

(4) Mussington, David, Peter Wilson, and Roger C. Molander. (1998). ñExploring Money Laundering Vulnerabilities Through Emerging Cyberspace Technologies: A Caribbean Based Exercise.ò Rand and Critical Technologies Institute (CTI).

(5) Noguchi, Yuki. (2003). ñSatellite Phone Firms Win Ruling.ò *The Washington Post*, January 31.

(6) Office of the Comptroller of the Currency (of the U.S. Treasury). (2001). ñBank Provided Account Aggregation Services.ò OCC Bulletin 2001-12, February 28.

(7) Society for Worldwide Interbank Financial Telecommunication (SWIFT). For additional information, please see: http://www.swift.com/.

(8) The United States Financial Intelligence Unitôs (FINCEN) Report, (2003). Suspicious Activity Reports (SARs) for Computer Intrusions: September 15, 2002 to September 15.

(9) UNIT 3

E-security in Emerging Markets

Contents

Contents

1.0 INTRODUCTION

Increased worldwide connectivity to an open, networked infrastructure and the subsequent shift to online transactions creates new vulnerabilities and risks worldwide. Electronic risk is present not only in developed economies it is also becoming prevalent in emerging markets. E-security issues are of particular importance in emerging markets where technological capabilities offer potential leapfrogging opportunities, but where concurrently, a lack of a technical workforce, education, and legal and regulatory infrastructure can thwart the safety and soundness of the IT environment. Because the sustainability of the digital infrastructure is determined by its level of security, including both the physical security of the Internet, and the enabling environment consisting of sufficient legal and regulatory frameworks, addressing security needs upon an infrastructureôs development is of critical importance.

2.0 Objectives

The objectives of this unit are for students and readers to know:

a. Existing barriers in emerging economies as they affect security matters.

b. The ways and manner these barriers can be curbed or managed.

c. Some attributes of some selected countries.

3.0 Main body

3.1 Barriers to Implementing E-Security in Emerging Markets

Through a number of case studies, the World Bank has identified several areas that can affect the extent to which emerging countries will effectively implement e-security measures. These are:

- Rapid technological growth without proper regard to security.

- The lack of education on electronic risks to regulators and supervisors.
- The lack of institutional infrastructure, including legal, regulatory and law enforcement.
- The lack of social capital and technological ñbrain drain.ò
- A high level of industry concentration in the telecommunications industry.

First, many developing countries are quick to embrace technologies, such as wireless, for the potential benefits they offer. These technologies are often adopted without proper consideration to, or understanding of, the inherent risks (Kellermann 2002). Countries adopt inherently risky technologies, relying on single silver bullet solutions such as Public Key Infrastructure (PKI) to mitigate all risks rather than adopting a multi-layered approach that secures each component of the technologies in play. Furthermore, due to limited access to information technology, a number of developing countries provide online services to deliver personal information and services through public kiosks, Internet cafes, or other public spaces where multiple persons use the same computer. Consumers use these computers without realizing that they are potentially bargaining away their privacy and as the confidentiality and integrity of their information for convenient access, speed, and reduced cost.

Second, a major problem is the lack of awareness of the dangers inherent in the digital environment. Many developing countries lack the educational materials to properly train citizens on risks and mitigation techniques. As a result, users do not take steps to mitigate threats in the online environment so that commerce can occur with minimal risk. Simultaneously, a lack of awareness proves to be a key limitation for e-finance; customers do not trust online transactions, which thus inhibit e-commercial activity. Without proper education, system administrators in emerging countries can face a critical handicap in their ongoing security efforts. This serves to weaken their technological infrastructures, making them vulnerable to cyber attacks, and ultimately affecting their chances of succeeding in the global marketplace.

Third, many developing countries lack the institutional structure to implement, monitor and enforce proper e-security measures. Laws, including cyber crime and e-commerce, must be restructured to create better incentives for proper e-security. Furthermore, even if the regulation does exist, a deficiency in the enforcement capabilities for these laws can greatly hinder their effectiveness.

Fourth, many countries do not have a real e-security industry, which in part reflects the concentration in many emerging markets in the information and communication technology industry, especially in the telecommunications sector. Here, the hosting, service provision, and ownership of physical communications lines are often in the hands of one or a few entities. This concentration of risk results in an unacceptable level of systemic risk. In such a case, one cyber attack can ripple across a number of industries if there is only one critical point of failure (for example, all the banks and other companies use the same hosting services provided by a dominant telecom/cellular provider). Conflicts of interest also occur that hinder incentives for such a conglomerate telecom and e-security provider to provide adequate e-security in the services rendered.

Finally, deficiencies in the institutional structure for security include a basic lack of human capital in these technical areas of technology risk management. Many

emerging countries in particular lack the human capital necessary to assess e-security vulnerabilities, to make recommendations to remediate, and to enforce compliance with cyber laws. Many well trained technical persons in emerging markets in such areas are lured to higher paying jobs in foreign countries. As a result, limited research and development occurs in e-security for many emerging countries. The growing worldwide problems associated with e-security have impacted many emerging markets. Below are just a few selected examples.

3.2 Some Selected Cases

In **Brazil**, where the information and telecommunication infrastructure is highly developed, and more widely accessible than in many other developing markets, electronic transactions have rapidly gained popularity. The Brazilian Payment System (SPB) launched in 2002 operates over an Internet technology backbone and e-banking is offered over wireless devices. The Brazilian government is a major promoter of online technologies, as evident in the number of online services offered on the government portal, Redegoverno (http://www.redegoverno.gov.br).As an example of its widespread diffusion, an article from 2001 notes that 90 percent of all submitted income tax declarations were done online (International Trade Administration 2001). Brazilôs increase in legitimate online activities came with its respective illegitimate, or malicious, activities. Cyber crime in Brazil leapt from 5,997 incidents in 1999 to 25,092 incidents a mere two years later, in 2002. Recognizing the need for security, Brazil created the NBSO (the Brazilian Computer Emergency Response Team) in 1997 to raise public awareness and share information on cyber threats.

In **South Africa**, widespread technological diffusion is reflected in their high penetration rates, which are among the top in Africa. But, high connectivity rates and the diffusion of online capabilities creates a prime target for hackers. Recently, a hacker infiltrated ABSA Bank, one of South Africaôs largest banks. Over 500,000 Rand was stolen from customer accounts. The country recently adopted regulatory initiatives, including the recent Electronic Communication and Transaction (ECT) Law. This law stipulates punishments for many forms of cyber crimes, including hacking. Additionally, many in the private sector are using Public Key Infrastructure (PKI) in an effort to assuage their growing numbers of security intrusions, electronic thefts, and denial of service attacks. However, similar to Brazil, which also set forth government-sanctioned provisions for a national PKI system, an over-reliance upon PKI can prove problematic if other critical layers of security are neglected.

The geographical landscape of the **Philippines** with its many islands and rugged terrain makes this country an ideal place for cellular infrastructure growth. Difficult and costly to build a physical telecommunications network, the rapid and inexpensive cellular infrastructure creates leapfrogging opportunities to bring telecommunications and financial services to remote regions. However, increased connectivity does not come without risks. This country produced the creator of one of the most notorious worms and expensive viruses, the Love Bug, otherwise known as the I Love You virus. Ramifications of this virus were felt worldwide, and at a cost to the global community of several billion dollars. The types of vulnerabilities that can be introduced as Philippine citizens increasingly use cell phones as devices to not only obtain account information at banks but also confirm trades or purchases of government securities as now being planned will also present challenges.

Self Assessment Exercise

What are the implications of widespread inexpensive cellular infrastructures?

4.0 Conclusion

Having explained some of the issues inherent in this unit can be said here that E-security issues are of particular importance in both developed and emerging markets where technological capabilities offer potential leapfrogging opportunities. However, in situations characteristically attached to developing economies with strong and fast receptivity to technological changes, coupled with concurrent lack of technical workforce, education, adequate legal and regulatory infrastructure can thwart the safety and soundness of the IT environment exposing people to security risks.

5.0 Summary

In most emerging economies the information and telecommunication infrastructure is increasingly being developed and becoming more sophisticated as well as widely accessible than in others where electronic transactions have rapidly gained popularity. In Brazil, for example, accessibility is quite higher than others in her category such as the Philippines. Nevertheless the geographical landscape; the many islands and rugged terrain make this country an ideal place for cellular infrastructure growth and other technologies which present security challenges. It is in these regards that the World Bank has identified several areas that can affect the extent to which emerging countries will effectively implement e-security measures.

6.0 Tutor Marked Assignment

Explain with relevant examples the key issues thwarting the safety and soundness of the IT environment.

7.0 References/ Further Reading

(1) National Institute of Standards and Technology (NIST). (2003). ñStandards for Security Categorization of Federal Information and Information Systems.ò Draft, May.

(2) Pelton, Joseph. (1993). ñFive Ways Nicholas Negroponte is Wrong About the Future of Telecommunications.ò *Telecommunications* 11(4).

(3) Shapiro, Carl, and Hal Varian. (1999). *Information Rules: A Strategic Guide to the Network Economy*. Boston, Mass.: Harvard Business School Press.

(4) Shu-Pui, Li. (2002). E-Security: Risk Mitigation in Financial Transactions. Presentation at the World Bank Global Dialogue on E-security, September25. http://www1.worldbank.org/finance/html/ dl11bkgd.html. retrieved 26/03/10

(5) Tzekov, Lubomir. (2002). ñE-security Risk Mitigation in Financial Transactions.ò Presentation at the World Bank Global Dialogue on E-security, September 25. http://www1.worldbank.org/finance/html/ dl11bkgd.html. retrieved 17/02/09

(6) Weinberg, John. (1997). ñThe Organization of Private Payment Networks.ò *Economic Quarterly Volume* 83(2). Federal Reserve Ban of Richmond, Richmond, Va.

UNIT 4
Risk Management Framework
Contents

1.0 Introduction

This unit highlights some of the key risks that the increasing use of technologies to exchange digital information pose to consumers, businesses, and the public interest. Technology may change the way services are delivered, but it has not changed the underlying basic principles of good business. Securing the open network is first and foremost a business issue, and is based upon basic principles of sound business such as responsibility, accountability, trust and duty. Technology is only a part of the business solution. However, what is in the best interests of businesses is not always in the best interests of consumers or the public good. In this section we identify the fundamental source of ñpublic interestò and the case for regulation in this area. For several critical reasons, e-security warrants certain forms of public intervention.

2.0 Objectives

This unit attempts to explain
1. Public interest in assuring e-security
2. Why the right form of regulation is needed

3.0 Main body

3.1 The Public Interest and E-Security

Financial services, particularly banking and the payment systems are integral parts of every countryôs critical economic infrastructure. Compromising the payment system by illegal access and hacking can have broad implications for a countryôs entire economy. Given the level of integration between countries, it can evoke a detrimental impact on other economies as well, as could similar impacts in other critical infrastructure areas, from transportation to energy, to telecommunications. Moreover, a problem in one area of critical infrastructure may compromise other critical infrastructures. For example an intrusion or breach in the case of a telecommunications company if the entity provides data storage or hosting services can have an impact on the banking system and risks of related intrusions. Hence, the public interest and welfare are potentially at risk when government, business, commerce, and consumers fail to meet certain minimum e-security standards. Recognizing the importance of the role of the public sector in maintaining and defending a countryôs critical infrastructure emphasizes the need for unprecedented

cooperation between countries as set out by the Group of 8 (see sec the G-8 Principles for Protecting Critical Information Infrastructure below).

Second, the role of government and law enforcement agencies in e-security can be justified on familiar classic market-failure grounds. Specifically, the existing base of information that supports projections about the extent of the e-security problem is substantially flawed. This is because financial services providers, hosting companies, and other enabling companies have inadequate incentives to report intrusion or penetration information accurately. Their legitimate concerns about the disclosure of such information and its potential damage to both their reputation and public confidence in their business logically create these incentives. In this case, insurance markets cannot price the insurance risk in an actuarially fair manner. Financial services providers react to incentives, and the pressure from stock analysts to cut costs and the related move to outsource key technology support functions has naturally led to much greater emphasis on connectivity and service reliability as opposed to e-security. More generally a fundamental asymmetric information problem exists in the area of technology services, whereby the sheer speed of advances and the complexity of some types of technologies have resulted in a situation where buyers of technology are often at an informational disadvantage vis-à-vis many types of vendors. This general problem also characterizes the entire area of e-security where evaluating the products being sold by e-security vendors and their proficiency is highly complex if not impossible and many forms of entities providing ñcertificationò services are not really legally liable. Hence, as in most industries characterized by such informational problems there is a case for well designed regulation in the IT area and in the area of e-security specifically.

Third, information technology is subject to large increasing returns to scale on both the demand side and the supply side (Shapiro and Varian 1999). Market outcomes in such industries (including financial services, which are heavily dependent on IT) will tend to be somewhat concentrated and often will require industry standardization and coordination. In emerging markets that are not large, these effects are often magnified. For example, it is often the case that the same entity that provides telecommunications services also provides the only available hosting services to major banks. In addition, in many of these markets, the telecommunications provider is also an ISP and a provider of such services as digital data storage, and even e-security.

Finally in many emerging markets the telecommunications provider may itself be government owned. Important public policy issues result from this industrial organization. The concentration of hosting services provided to banks can actually increase operational and related systemic risks related to cyber attacks, as there is inherently no built in redundancy and a problem that occurs in a hosting company serving multiple banks can create problems simultaneously in all banks. This may create a critical single point of failure. Concentration in the provision of these many types of services can also result in competition problemsð and more insidiously, conflicts of interestð that can prevent adoption of implementation of proper e-security.

Fourth, the reach of the Internet and technologies imply that financial services are increasingly becoming more borderless and global. Hence mitigating e-security risks

requires unprecedented efforts to promote collective action within countries (interagency and public-private sector cooperation) as well as between countries by market participants, regulators and law enforcement agencies. Usually such collective action problems cannot be solved via simple cooperation among private parties so again the role of authorities in countries throughout the world and private market participants needs to be considered. Increasing efforts are being made to address these collective action problems. Compounding these problems is that collective action is needed even if one can solve the problem of market failure and create better incentives for timely and accurate reporting of e-security incidents. The integrated nature of these problems requires the private and public sectors (such as the law, regulatory and supervisory agencies within and across countries) to develop unprecedented approaches to cooperation. At its broadest level the problem of electronic safety and soundness is a risk management problem that is part of business process and needs to become much more a part of doing proper day-to-day commerce and risk management. Hence it is important to understand in some detail how to decompose the risks associated with electronic transactions in designing public policy.

These different arguments for a public interest role are not unrelated. They suggest that the way forward must take in to account the fact that e-security is a form of public good, reflecting the impact that it can have on key infrastructure and on other economic agents. A breach of e-security can compromise the identities of many un-knowing consumers of financial services. Paradoxically, financial service providers, ISPs, hosting companies, and other related companies do not operate under sufficient incentives to ensure that they secure their systemsð rather, the emphasis is on providing fast and uninterrupted service. Even the contractual relationships between the many entities involved in the provision of the technology backbone have differing levels of actual liability and typical service level agreements do not address e-security breaches so incentives to secure computers or servers is often left to the ultimate user.

3.2 The Electronic Security Industry and G-8 Principles for Protecting Critical Information Infrastructure

Todayôs e-security industry boasts an ever-growing array of companies. The types and numbers of choices can be confusing for the expert and overwhelming to the novice. These companies are involved in every facet of securing the networks used by financial services providers. They range from those that provide active content filtering and monitoring services to those that undertake intrusion detection tests, create firewalls, undertake penetration testing, develop encryption software and services, and offer authentication services. In scope, the e-security industry increasingly is becoming a worldwide presence as it grows parallel with the expanding connectivity to the Internet. The growing integration of technologies among the Internet, wireless, Internet provider (IP), telephone, and satellite will also present new challenges for e-security and the structure of the financial services industry and e-finance. Because E-security companies are becoming increasingly global in nature, it is important when designing public policy to understand the links between such companies and the electronic finance industry. There is a high degree of cross-ownership and market concentration between and across various aspects of e-finance and e-security. One vendor may provide multiple services to several interlinked customers. For instance, a vendor may provide security to the financial services providerôs online platform. This same vendor also may provide security

services directly to the bank for its offline computer systems. In addition, it may supply security services to the hosting company. Telecommunications companies in many emerging markets provide hostingð or what many refer to as ñe-enabling servicesòð to the banking community. By establishing a convenient online platform that customers can access through a variety of electronic devices, these hosting companies (ISPs) have become targets of organized crime.

In many emerging markets, the telecommunications company may have an interest inð or own outrightð the ISP provider and the hosting company and may provide various forms of financial services as well. Moreover, many telecommunication companies also have multiple interests in many different forms of technology providers, from fixed-line telephony to wireless to satellites. This monopolistic industry structure should raise concernð it signifies the need to discuss and debate difficult public policy issues now, such as competition policy, and how these issues might be addressed in designing new legal and regulatory elements of the present frameworks (Claessens, Glaessner, and Klingebiel 2002).

Along with a complex concentrated and cross-linked structure, convergence in technologies will present special challenges in the design of public policies relating to e-security. Specifically, increasing points of vulnerability will merge, and any well-designed e-security system must address them. These new points of vulnerability might include the potential interfaces between customer access devices, such as a PC with modems, land-line phones that can be linked with any Internet platform through voice recognition, wireless phones, or personal digital assistants (PDAs) with an online platform. The point at which the message leaps from one channel to another is the point at which it is most vulnerable. Hence, financial services providers will need to address a much wider array of risks and expend effort to define liability, and public policymakers will need to examine the impacts of potential weaknesses, given what is already a complex e-finance industrial structure.

G-8 Principles for Protecting Critical Information Infrastructure

Information infrastructures form an essential part of critical infrastructures. In order to effectively protect critical infrastructures from damage and to secure them against attack, the G8 has developed 11 specific principles. They are:

I. Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.

II. Countries should raise awareness to facilitate stakeholdersô understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.

III. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.

IV. Countries should promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.

V. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

VI. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.

VII. Countries should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.

VIII. Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

IX. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.

X. Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

XI. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

Self Assessment exercise
List and explain the eleven G-8 Principles for Protecting Critical Information Infrastructure.

4.0 Conclusion

No doubt, information technology is subject to large increasing returns to scale on both the demand side and the supply side in any nationôs economy. Market outcomes in such industries involved in financial services, which are heavily dependent on IT will tend to be somewhat concentrated and often will require industry standardization and coordination. These G-8 Principles for Protecting Critical Information Infrastructure highlights eleven specific principles which serve as a guide to effectively protect critical information infrastructures globally.

5.0 Summary

This unit examines and highlights some basic issues in the Electronic Security Industry and G-8 eleven specific principles for Protecting Critical Information Infrastructure as well as some of the key risks that the increasing use of technologies to exchange digital information pose to consumers, businesses, and the public interest. Technology may change the way services are delivered, but it has not changed the underlying basic principles of good business. Securing the open network is first and foremost a business issue, and is based upon basic principles of sound business such

as responsibility, accountability, trust and duty. This, the G-8 seeks to ensure with its guideline as discussed in the main body.

6.0 Tutor Marked Assignment

Discuss the challenges in the growing integration of technologies among the Internet, wireless, Internet provider (IP), telephone, and satellite.

7.0 References/ Further Reading

(1) Claessens, Stijn, Thomas Glaessner, and Daniela Klingebiel. (2002). *Electronic Finance: A New Approach to Financial Sector Development.* World Bank Discussion Paper No. 431. Washington, D.C.

(2) Group of 8 Press Release, (2003). G-8 Principles for Protecting Critical Information Infrastructure

(3) http://wbln1023.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/Mobile_Risk_Management/$FILE/Mobile_Risk_Management.pdf. Retrieved 01/03/10

(4) Kahn, Alfred E. (1970). *The Economics of Regulation: Principles and Institutions*. John Wiley & Sons, Inc. Kahn, David. 1996. *The CODE-BREAKERS*. Scribner.

(5) Kahn, Alfred E. (1998). *The Economics of Regulation: Principles and Institutions*. Cambridge, Mass.: MIT Press.

(6) Kellermann, Tom. (2002). *Mobile Risk Management: E-Finance in the Wireless Environment.* World Bank, Washington D.C.

(7) Kellermann, Tom. (2002). *Electronic Security: Risk Mitigation in Satellite-Based Networks*. World Bank, Washington D.C.

(8) Kellermann, Tom and Yumi Nishiyama. (2003). *Blended Electronic Security Threats: Code Red, Klez, Slammer, and Bugbear.* World Bank, Washington, D.C.

(9) OECD *Guidelines (*2002). *the Security of Information Systems and Networks: Towards a Culture of Security*

(10) Shapiro, Carl, and Hal Varian. (1999). *Information Rules: A Strategic Guide to the Network Economy*. Boston, Mass.: Harvard Business School Press.

(11) Shu-Pui, Li. (2002). E-Security: Risk Mitigation in Financial Transactions. Presentation at the World Bank Global Dialogue on E-security, September 25. http://www1.worldbank.org/finance/html/dl11bkgd.html

UNIT 5
Tradeoffs: Security, Quality of Service, Privacy, Technological Innovation, and Costs

Contents

1.0 Introduction
Designing public policy, creating legislation, and promoting regulation in this highly complex area requires balancing a number of essential tradeoffs. This even applies in designing standards and guidelines that might be used by a self-regulatory agency or by an official agency.

2.0 Objectives
Therefore this unit seeks to investigate the various essentials in security, from costs, quality of services, technology innovation and privacy. It is expected that readers should get themselves acquainted with these essentials.

3.0 Main body
3.1 Electronic Security: Some Essentials

a. Security and Costs. Security should always be proportional to the real value of the underlying transaction. Given this proviso, it appears that when the transaction value is small, no clear economic or risk-management case can be made for employing the most sophisticated e-security regimes when a less expensive form of security will yield the same return. For example, a financial services provider would not want to use an expensive and cumbersome authentication process, such as PKI, for small-value transactions when tokens or other simpler forms of authentication will mitigate the risk of theft, and so on, to an acceptable level.

b. Security and Quality of Service. Similarly, tradeoffs exist between the convenience or quality of service, as computed in terms of speed and the extent and degree to which security is used. The more complex the security process used, such as PKI (public key infrastructure), the longer the transaction takes to be completed. Advances in these technologies are lessening this tradeoffs. Over time, effective authentication or encryption systems will be available that do not slow the speed of transactions and do not disparage the quality of service. Moreover, one can argue that confidence in the security of services is an essential aspect of quality in providing financial services.

c. Security and Technological Innovation. For e-security systems to be effective, it is important to ensure that private parties agree to certain standards and guidelines. But the proliferation of technologies that can be used to transmit information and their rapid rate of integration inherently creates a reluctance to adopt standards or guidelines. Technological innovation can be stifled and customer service can suffer if security standards are not sufficiently flexible and technology-neutral. As will be noted in later sections, even the definition of an electronic signature needs to be very carefully designed so as not to preempt the use of a number of alternative technologies. In other words, the concept of technology neutrality is an important one to adopt when formulating legislation and regulation.

d. Security and Privacy. Ironically, the need for more effective e-security may sometimes conflict with and negatively affect the userôs privacy. Inadvertently, it may also affect the privacy of third parties who are identified in affected information. This tension is natural, and it is not new. On the one hand, certain types of e-security services may be consistent with protecting privacy (e.g., programs such as cyber patrol). On the other hand, security may be needed to track and verify the userôs movements. In other cases, however, the person undertaking the transaction may want to remain anonymous as part of a trading strategy. Developing the proper balance between security and privacy is a delicate matter. It often is decided within a cultural paradigm. Sometimes this means that something considered private in one culture may not be deemed so in another. Moreover, the laws (for example, bank secrecy provisions) often compromise the ability of the authorities to investigate properly and take enforcement actions in complex electronic crime cases.

3.2 The Roles of the Private and Public Sectors in E-Security

Any policy framework needs to try and delineate the roles of the public and private sector with some clarity. Technology and its rapid pace of change along with the informational and incentive problems outlined make it essential that both the private sector and the public sector play a role in improving e-security. The challenge is how to ensure that awareness of the issue and better transparency can become the norm as part of ordinary business process. The roles of the public and private sector must be designed to reinforce each other to the greatest extent possible. However, the design of such policies should put a premium on simplicity and assure that enforcement is a reality. Many of the approaches to be undertaken will need to be strongly conditioned by the underlying industrial organization of the telecommunications and financial services industries along with the e-security industry in specific emerging markets.

a. Roles of the Private Sector

The private sector can play several important roles. First, and most importantly as part of ordinary business practice, private companies should secure their electronic operations to avoid reputational and other actual losses. Hence, this source of operational risk needs to be much better assessed and dealt with in day to day operations. Internal monitoring is the first line of defence. However, despite the need for the private sector to take on this pro-active role, there are a variety of reasons why private companies often are pressured to under-invest in overall electronic safety and soundness. As noted above there is a classic market failure whereby there is a natural lack of incentives for ñtruthful disclosureò of e-security problems precisely due to possible reputation damage. Hence, a key aspect of the role of the public sector and other private market participants is to create more awareness of the risks being borne

by the entire financial services industry due to lack of accurate information and cooperation. Internal monitoring and layered e-security should be a critical aspect of business practice, and e-security, but governments may need to provide incentives to ensure that such practices are rigorous enough.

Second, the private sector should seek means to cooperate with academic institutions and governments to greatly improve the education of the general population in this essential area of critical infrastructure. As noted, the Internet can be viewed as a very large, semi self governing entity. Better governance overall of its common technology platform must become a much higher priority for the private sector, not only the government. To date systematic cooperation in educational efforts aimed at education of users as well as providers of financial or other services have been less than satisfactory even in some of the most advanced developed countries in the world.

Third, the private sector will need to make unprecedented efforts to cooperate with law enforcement agencies and with supervisory authorities within and across borders due to the very global nature of the Internet technology backbone. Here, law enforcement entities need to work with the private sector to develop ways of reporting and sharing information that guarantees that confidential information about a specific e-security breach will not be disclosed if it is shared with authorities. Establishing an infrastructure that can actually engender such incentives to report to authorities and even to properly report within specific financial services providers to the Chief Information Security Officer (CISO) is highly complex, but needs to be addressed.

Fourth, the private sector in many countries will need to couple improving awareness with a concerted approach to create governance and management structures inside financial service providers and banks that can greatly improve active internal monitoring of e-security and risks. Here although external supervisors can act to raise the standards, the need to establish much sounder policies, practices, and procedures is essential. In many emerging markets, financial service and non-financial entities do not even have a CISO; nor is an understanding of technology related risk management expertise a criterion for choosing Directors for appointment to Boards. Beyond actions at the level of individual financial service providers, private associations (including the bankers and securities markets associations or even self regulatory associations) have a key role to play in maintaining the reputation and trust that consumers have in their members. Hence, ways to self-monitor where banks are proactive in monitoring each other and setting certain minimum standards for management of such risks via such associations needs to be explored.

b. Roles of the Public Sector

Mitigating the risks of electronic transactions, as argued in the first section of this unit, is an area of significant public interest. In designing policy there is a need for carefully structured interventions by the public sector, especially in emerging markets. The classic literature on competition and market failure suggests a number of roles that the public sector needs to play. As in the case of the private sector above, these key roles are neither well-established nor is an accountability framework in place for the agencies involved (for example, supervisory and enforcement) in most emerging markets. Some of these roles are:

1. Regulation

Given the public interest in this area and the importance of market structure combined with the rapid deployment of sophisticated technologies in many emerging markets and the increasing use of technology in delivery of financial services, several areas of public sector legal and regulatory practice are especially important to define.

- *Defining Liability of Parties and Standards of Governance:* Incentive problems often arise in the area of e-security, because governance and more broadly liability of multiple parties is ill-defined. In the case of e-security these problems arise at the level of the Board, the management, among the administrative and technology staff and vis-à-vis a whole host of different types of third party providers of enabling technologies. These third party providers run the gamut from hosting services or ISPs to e-security vendors. The legal and regulatory frameworks of most countries do not assign sufficient liability via representation and warranties in the case of these parties. In addition, corporate governance reform does not really address the need for companies to actually create a CISO or preferred arrangements with regard to the liability of the Board, the management, and the individuals or officers charged with undertaking the e-security function. As in most areas of corporate governance the issues to be addressed are complex and subtle because the degree of liability is not independent of the capacity to properly define the precise electronic related risks to which the provider of a service is liable. In addition assignment of liability between the provider of a service versus the financial institution purchasing the service is often complex. For example, many ISPs would argue that they are simply a pipe and should bear no liability for an e-security breach to a user of their service.

- *Defining legal concepts that are simple and are enforceable within and across countries:* The governments of different countries need to pay special and increasing attention to how to define simple and enforceable legal concepts that will reduce incentives for e-security breaches. They must also assure enough harmonization to reduce the scope for new forms of regulatory arbitrage where hacking syndicates locate in countries with weak legal and enforcement frameworks.

- *Defining Standards and Certification Processes:* Standards in an area like e-security cannot be static. It is apparent that the public and private sectors in many countries will need to work together to assure that standards are not in effect a means for entrenched providers of services to retain excessive market power. In many emerging markets certification is effectively used in this manner, and often self-regulatory associations have no effective legal liability, so that in the end the effectiveness of such entities to police providers of e-security services, certify such providers, or assure proper entry or security standards is suspect. More broadly the way in which certification processes are established in this area, as well as the setting of standards in many emerging markets is in need of review. Here the promulgation of certain international standards (such as the ISO standards) will require much more effort and cooperation. The role of private companies that can act as monitoring agents of those offering services electronically is important to foster in many emerging markets, supervision and enforcement as well as human capital that may be weak or underdeveloped. In this context the use of regulation in order to create incentives for financial service providers to have to insure against certain forms of e-security risks at the margin as part of an overall policy of prudence can be beneficial.

2. *Monitoring* Beyond the role of the public sector in establishing the overall legal/regulatory and incentive framework in this highly complex area there is another role that the public sector plays via either direct or indirect monitoring of the e-security practices of financial service providers. This monitoring role is nothing new. Three key mechanisms are especially relevant: supervision as a means of prevention; supervision of third-party monitoring agents such as insurance companies, and supervision and monitoring of those entities claiming to provide various forms of certification services or developing ñstandardsò for e-security such as certification authorities; self regulatory associations, etc.

- *Supervision of Electronic Financial Service Providers:* This important function is now becoming more complex in the age of rapid advances in technology so that both examination and enforcement actions are becoming more complex. Regulatory supervision must work with the financial service industry and the e-security industry to develop new methods of examining, new concepts of monitoring, and new means of intervention. For example, it is now possible to remotely monitor banks on a continuous, automated basis. This enables supervisors to track risk, exposure, etc. on a real time basis.

- *Supervision of Private Monitoring Agents:* Insurance companies writing cover need to be carefully supervised so that they properly insist on better overall e-security. In addition the establishment of higher standards of security and due care by credit rating agencies and the insistence on better security processes by all companies and financial service providers in this key area (source) of operational risk are important. Securities regulators and insurance supervisors need to more carefully supervise private monitoring agents and insist on certain minimum standards in assessing their actions to monitor the e-security practices and operational risk of financial service providers.

- *Supervision of Certification Agents and the Technology Providers:* Just as formal supervision entities have a role to play so too do other regulatory agencies such as the competition commission or trade commission, or the regulatory entity dealing with the telecommunications sector. In many emerging markets there are no real processes in place to supervise entities that certify providers of e-security services and in many emerging economies this e-security industry does not exist except for services provided by the local telecommunications provider.

3. Promoting Awareness and Education

Other essential roles for the public sector in this area are to promote awareness and to provide ongoing training and education. The importance of awareness and education among making persons in companies and consumers of electronically provided services cannot be underestimated in importance. Global efforts to introduce the responsible adoption of technology will require unprecedented networking and coordination between Universities, governments and the corporate sector worldwide.

Self Assessment Exercise

Explain the key essentials in e-security

4.0 Conclusion

The role of both the public and private sectors cannot be undermined in enhancing effective e-security operations. To a very large extent apart from the technological innovation, enlightenment campaigns need to be well spread so that the general public will optimally benefit from todayôs world of electronic security compliance; checks and balances.

5.0 Summary

This unit explains some key essentials about e-security, such as cost; quality of service, technological innovation and Privacy. It goes further to emphasise the role of the public and private sectors in e-security.

6.0 Tutor Marked Assignment

Succinctly highlight the roles of the Private and Public Sectors in E-Security.

7.0 References/ Further Reading

(1) Mussington, David, Peter Wilson, and Roger C. Molander. (1998). ñExploring Money Laundering Vulnerabilities Through Emerging Cyberspace Technologies: A aribbean Based Exercise.ò Rand and Critical Technologies Institute (CTI).

(2) Organization for Economic Cooperation and Development (OECD). (2002). *OECD Guidelines for the Security of Information Systems and Networks*.

(3) Schneier, Bruce. (2000). *Secrets & Lies—Digital Security in a Networked World*. John Wiley & Sons.

(4) Tzekov, Lubomir. (2002). ñE-security Risk Mitigation in Financial Transactions.ò Presentation at the World Bank Global Dialogue on E-security, September 25. http://www1.worldbank.org/finance/html/ dl11bkgd.html. retrieved 18/06/05

(5) Vijayan, Jaikumar. (2002). ñVOIP: Donôt overlook security.ò *Computerworld*, October 7.

(6) Woochan Kim. ñE-security in Financial Transaction: Case of Korea.ò Presentation at the World Bank Global Dialogue on E-security. September 25. http://www1.worldbank.org/finance/html/dl11bkgd.html. retrieved 19/01/09

Module 2
Unit 1. Policy Response: Overview of the Four Pillars
Unit 2. Security of Payment Systems
Unit 3. Hand and powered tools in security
Unit 4. Electronic Document Security
Unit 5. Electronic Security: Protecting Your Resources

UNIT 1
Policy Response: Overview of the Four Pillars

Content

UNIT 1
Policy Response: Overview of the Four Pillars

8.0 Introduction

In the light of these complex public policy issues, any approach to designing a public policy framework that improve electronic safety and soundness will need to rest on four fundamental pillars. This reading materials is built on the concept that trust and confidence of market participants are fundamental component of a robust economy. It is important to recognize that to be most effective, reforms in all four pillars are needed in most emerging markets and the design of these reforms must reinforce each other. The balance between the public and private sectors and their roles is especially important in the first three pillars, and there is a real need for authorities to adopt simple and clear principles and legal reforms. Knowledge of the technology is essential in properly designing reforms in each area. At the same time, in many emerging markets, work in designing reform must be multi-disciplinary and must include at a minimum the legal profession, finance and risk professionals, economists, actuaries, and persons with the requisite understanding of technology.

9.0 Objectives

This section seeks to broadly examine the four pillars involved in the building of policy framework and practice of electronic security

10.0 Main body

3.1 Four Pillars: An Overview of the Four Pillars

Pillar 1: Legal, Regulatory, Enforcement Framework and Overall Framework: Countries adopting electronic banking or electronic delivery of other financial services (e.g., distribution and trading of securities) should incorporate e-security concerns into their laws, policies and practices. The framework must require business to be responsible for security, to use of security to protect back-end and front-end

electronic operations, and to provide for appropriate punishment to combat cyber crime and cyber terrorism.

At a minimum, an e-finance legal framework should consist of the following:

a. *Electronic Transactions Law:* This should define what is meant by an electronic signature, record, or transaction, and recognize the legal validity of each of these.

b. *Payment Systems Security Law.* These statutes should identify, license, and regulate any payment system entities that directly affect the system. They should provide that all such entities must operate in a secure manner, and require timely and accurate reporting on all electronic-related money losses or suspected losses and intrusions. Finally, they should require that the financial institution and related providers have sufficient risk protection.

c. *Privacy Law*. Privacy law should encompass data collection and use, consumer protection and business requirements, and notices about an entityôs policy on information use. At a minimum, the privacy law should embrace the fair information practice principles of notice, choice, access, and minimum information necessary to complete the transaction.

d. *Cyber Crime Law.* These laws should address abuses of a computer or network that result in loss or destruction to the computer or network, as well as associated losses. They should also provide the tools and resources needed to investigate, prosecute, and punish perpetrators of cyber crimes and, where needed, address the subject of adequate record retention to allow for electronic forensics and investigation.

e. *Anti-Money Laundering Laws*. These statutes should define money laundering and require international cooperation in the investigation, prosecution, and punishment of such crimes pursuant to the guidance provided by the Financial Action Task Force (FATF).

f. *Enforcement*. Perhaps as important as the legal framework will be the need to enforce the provisions of e-security laws within and across national boundaries. The fact that so many different types of computer or system related intrusions actually originate through activities conducted in countries with weak legal and enforcement regimes for e-security, makes it essential that a broad international approach that relies on more homogeneous laws and enforcement actions across countries be put in place.

Pillar 2: Improving the Monitoring of E-security Practices

Designing incentives to improve the e-security practice of financial service providers is not independent of the various institutional arrangements and development of financial markets in countries or offshore. However, in many emerging markets at least three parties have a role to play in monitoring and creating incentives for better e-security. These parties are: regulators and supervisors; insurance companies through the policies they write and the related monitoring they provide; and the public at large, particularly those who work in companies or financial service providers and

final consumers of financial services. Any framework must support actions in each of these areas.

1. Supervision and Prevention Challenges and Monitoring by the Regulatory Authorities

Beyond the monitoring of the payments system and the related supervision of money transmitters is the need to revisit the regulation, supervision, and prevention approaches to financial services providers that engage in electronic banking or provision of other financial services.

a. *Capital Requirements.* The new Basel guidelines for capital, especially those dealing with operational risk, do not address the problem of measuring either the risk to reputation or the strategic risk associated with e-security breaches. A more productive approach might be to use the examination process to identify and remedy e-security breaches in coordination with better incentives for reporting such incidents. In addition, authorities could encourage or even require financial services providers to insure against some aspects of e-risks (for example, denial of service, identity theft) that are not taken into account within the existing capital adequacy framework.

b. *Downstream Liability.* The interlinked nature of financial services providers, money transmitters, and ISPs implies that the traditional regulatory structure must change or expand beyond its present configuration. The legal or regulatory framework should create incentives for ISPs, hosting companies, application service providers, and software, hardware, and e-security providers to be accountable to the financial services industry.

c. *Supervision and Examination Processes*. Further areas for the Basel Committee on Banking Supervisionôs Electronic Banking Group to evaluate include: the means used to examine the IT systems of banks or other financial services providers in order to modernize the examination approach; the institutionôs current documented security program; the current approaches to modelling operational risk in the light of the growing importance of cyber-risks, and the procedures used to identify and assess entities that provide a data processing or money transmitter service to the institution.

d. *Coordination of agencies within and across borders.* One important issue facing most countries is the need to improve the sharing of information across and among their regulatory and law enforcement agencies. Many countries have a number of entities for gathering critical information, but often it is not shared within a country or across nations (sometimes for legal reasons). Improvement in this area will require joint enforcement actions and much greater cross-border cooperation.

2. The Role of Private Insurance as a Complementary Monitoring System

The global insurance industry can increasingly act as an important force for change in e-security requirements. First, it can strive to improve the minimum standards for e-security in the financial services industry. Second, insurance companies can require that financial services entities use vendors that meet certified, industry-accepted standards to provide e-security services as a way of mitigating their risks of underwriting coverage. Third, insurance companies can encourage regulators to require that financial services entities both provide information and improve the quality of data and information on incidents so they can better actuarially measure e-

risks and return on investment. Finally, the industry should promote solutions that require e-security vendors and other e-enabling companies (hosting, etc.) to engage in risk sharing and in carrying appropriate liability.

3. Education and Prevention of E-Security Incidents

In many countries, more than half of all e-security intrusions are still carried out by insiders. An uneducated or undereducated workforce is inherently more vulnerable to this type of incident or attack. Educational initiatives will have to be targeted to financial services providers (both systems administrators and management), to various agencies involved in law enforcement and supervision, and to actual online users of financial services. Initiatives in this area must not only be undertaken with countries but worldwide. This is likely to be one of the most important initiatives that multilateral and bilateral lenders can support over the next decade to support the timely and proper development of proper e-security infrastructure in emerging markets. Due to the dynamic nature of both technology and the cyber-threat, recurrent security training is essential for all IT personnel and management. Education regarding the institutionôs policies and proper procedure in protecting open architecture systems will ensure that each participant is an important actor in the provision of security. Use of innovative techniques for training including distance learning and use of other technology in educational initiatives will also make this effort more economical (www.worldbank.org/finance).

Pillar 3: Public-Private Sector Cooperation and the Need for Collective Action
Two highly important areas that must be a focal point of public policy in the area of e-security relate to the accuracy of the basic information about such incidents and standards and certification processes in a number of dimensions. These critical areas are not only impacted by the legal regime in place and the degree of monitoring and reporting, but also by the nature of institutional arrangements in place to encourage collective action within and across countries.

a. Accuracy of Information and Public-Private Sector Cooperation

The lack of accurate information on e-security incidents is the result of the lack of incentives to capture the data, measure it, and inform users. E-security would improve worldwide through the creation of a set of national and cross-border incentive arrangements to encourage financial services providers to share accurate information on actual denial-of-service intrusions, thefts, hacks, and so on. Greater public-private sector cooperation is needed in this area. Critical to any global solution will be for a universally trusted third party to administer a global base of information relating to e-security incidents. In this area, the role of multilateral agencies to facilitate cooperation deserves examination as well as the potential for use of self-regulatory organizations with very wide global ownership under a wholly separate technical management (such as Carnegie Mellon CERT) that might act to assure the absolute privacy and non-identification of parties contributing the information. Such arrangements and relevant non-disclosure provisions and potential liability for any third party that would store such information could be highly complex to organize but does merit investigation as well.

b. Certification, Standards, and the Roles of the Public and Private Sectors

Both public and private entities must work cooperatively to develop standards and to harmonize certification and licensing schemes in order to mitigate risk even if such standards are essentially sufficiently dynamic to allow for rapid technological advances. Two categories that require particular attention in terms of certification deal with e-security service providers themselves and the transaction elements in e-finance. A necessary first step in securing e-finance is to require licensing by financial regulators of vendors that directly affect the payment system, such as money transmitters or ISPs. A further step could be to require the financial services and e-security industry to jointly certify vendors that provide e-security services. Incentives to undertake this responsibility carefully will not be unrelated to the underlying legal framework and relative liability borne by these parties (for example, financial service providers and third party vendors). Obtaining collective action across members of diverse industries will require a definite joint public private partnership in support of the public interest role of the electronic safety and soundness of financial services. A second area to address is certification of such transaction elements as electronic signatures. The value certification brings to a transaction in part depends on who or what provides the certification and on the elements that are being certified. Certification structures located in different jurisdictions must consistently provide the same attributes to the transaction and that a certifierôs scope of authority and liability must remain consistent across jurisdictional borders.

Pillar 4: Business Process and Incentives for Layered Electronic Security
Security is a business issue, not a technical issue. Risk of being hacked deals with probabilities not possibilities. Understanding the business is critical when attempting to be proactive in cyberspace. One of the most important efforts needed to improve e-security is to clearly link business objectives to processes that link the costs of not securing a business to the potential and actual savings from layering security in a world where open architecture systems prevail. Three general axioms to remember in building a security program include:

a. Attacks and losses are inevitable.
b. Security buys time.
c. The network is only as secure as its weakest link.

Twelve core layers of proper e-security are fundamental in maintaining the integrity of data or digital assets and mitigating the risks associated with open architecture environments.

Twelve layers of electronic security
These twelve layers of e-security are recommended as a required component of best business practice, and should the remit of a Chief Information Security Officer (CISO) with designated roles and responsibilities:

1. Risk management frameworks that are broader based than those often associated with operational risk and business continuity;
2. Cybernetic intelligence to provide antecedent analysis of threats and vulnerabilities;
3. Carefully designed access controls and authentication on a multilevel basis that relies on more than one authentication technology;
4. Firewalls that allow for the implementing of boundaries between networks;
5. Active content filtering at the application level;

6. Implementation of adequate intrusion detection systems;
7. Use of virus scanner to limit the entry of malicious codes and worms;
8. Use of strong encryption so that messaging can proceed with integrity;
9. Vulnerability and penetration testing to see where key points of vulnerability exist, with required remediation and reporting;
10. Implementation of proper systems administration,
11. Adoption of policy management software to ensure control of bank policies regarding such issues as employee computer usage; and
12. Development of an explicit business continuity or incident response plan to assure a rapid recovery after any significant computer security incident.

Self assessment exercise

Explain the importance of the four pillar framework to electronic security

11.0 Conclusion

In all the four pillars of e-security framework, the role of education and educated populace go a long way in ameliorating the problems inherent in electronic transaction. So also the roles of a good Chief Information Security Officer (CISO) is dependent on Information Technology (IT)

12.0 Summary

A broader look at the four pillars electronic framework was done with emphasis placed on the role Chief Information Security Officer (CISO) need to play in any security outfit. The importance of incorporating e-security concerns into their laws, policies and practices was explained in pillar one while the monitoring of e-security practices and practitioners was discussed in Pillar two, Pillar three sees the need for effective collaboration between the public and private in security; Pillar four emphasise the need for security to be viewed as a business strategy rather than as a technical issue.

13.0 Tutor Marked Assignment

1. Examine the role of education/educated populace in electronic security
2. What are your expected duties as Chief Information Security Officer (CISO) in a company?

14.0 References/ Further Reading

(1) Allen, Julia. (2001). *CERT Guide to System and Network Security Practices.* Indianapolis, Ind.: Addison-Wesley.

(2) American Bar Association. (2003). International Corporate Privacy Handbook. August.

(3) Bannan, Karen. (2001). ñSafe Passage.ò *PC Magazine*, August. Basel Committee on Banking Supervision. 2001. *Risk Management Principles for E-Banking*, May.

(4) Bannan, Karen (2001). *Basel Committee on Banking Supervision Consultative Document: The New Basel Accord*. January.

(5) E-security (2002). www.worldbank.org/finance. retrieved 09/03/08 The Council of Europe, Convention on Cybercrime, ñhttp://conventions.coe.intò

UNIT 2

Security of Payment Systems

Content

1.0 Introduction

Though most countries have laws in place to regulate different components of the payments system, no country has yet addressed payments systems issues comprehensively. Payment systems legislation should identify, license, and regulate any directly related payment system entities, such as money transmitters and ISPs. It should require such elements to operate in a safe and sound manner so as to protect the integrity and reliability of the system. It should require the timely and accurate reporting of all security incidents, including all electronically related money losses. Finally, it should require all payment system entities to adhere to a documented security program and should encourage some form of shared risk protection. In particular, money transmitters and ISPs that provide services to the financial sector should be required by regulation or legislation to provide liability for their services. Sharing risk is a proven model in the financial services arena, and there is as yet no evidence that this would increase the basic service cost. In fact, only when service entities are required to report losses or suspected losses can sufficient information be garnered to improve pricing for e-security performance bonds and e-commerce liability insurance. As a result of the lack of a comprehensive law regulating payment systems coupled with the lack of standardization in regulation and oversight, many money transmitters insert significant risk into the payments system. Typically, they are undercapitalized, use little or no risk-management analysis, and are extremely susceptible to bankruptcy and failure. With the escalation of Internet related commercial activities and the requisite need to provide ubiquitous payment system conduits, money transmitters are increasing the disintermediation of the traditional payments systems and have a higher profile in the eyes of law enforcement.

2.0 Objectives

This unit seeks to examine The potential risks associated with e-transactions.

3.0 Main body

Security of Payment Systems and Privacy law

Clearly, privacy is an area of the law that is undergoing considerable scrutiny throughout the world. It is an issue of fundamental importance, reflecting the very substance of our cultural identities, values, and mores, and it must be handled with the utmost care. Poorly considered decisions made in this arena may haunt us for years to

come. On the issue of privacy protection, some countries have chosen to legislate on a functional or piecemeal basis, while others have taken a more encompassing, process-oriented approach. Two approaches are also being used on the issue of consent. The first is to assume consent unless the party affirmatively chooses not to have the information sold or used for other purposes. The second is to assume that the party has not consented to any use of the information unless the party gives that consent. The United States follows the first approach in financial activity and the second in medical information. The European Union (EU) exemplifies the second in each area and continues to be the leader in providing privacy protection to its citizens with its 1990 EU Directive on Data Collection. No matter which approach is used, at a minimum, privacy laws should embrace the Fair Information Practice Principles set out in the European Union Directive on Data Protection and adopted by the Federal Trade Commission. These principles consist of notice, choice, access, and consent. They should address privacy rights concerning any data collected, stored, or used by an entity for different purposes, in particular those uses that could affect a personôs basic human rights, such as criminal, financial, business, or medical uses. In practice, privacy laws would require entities to do the following: advise persons about how data will be used; collect only the minimum data needed to complete the transaction or record at issue; use the data only for those purposes that it advised the person it would be used for; and permit persons to view any information collected and dispute the validity of any such information with timely corrections. Finally, the law should impose restrictions on any entity collecting, holding, or disclosing information in a form that would allow identification of the person it relates to, however that may be defined.

Cyber Crime

Significant debate is transpiring in legal communities worldwide over the impact of cyber crime on fundamental concepts of law, such as jurisdiction, and in particular on how the electronic culture is changing traditional legal paradigms. Financial cyber crime is a top priority in this dialogue because, more often than not, it requires intense international cooperation among what can be an overwhelming number of law enforcement agencies and regulators from different countries. Because no country is immune, every country should benefit from pooling resources to address this problem. But, more than any other aspect of computer law, financial cyber crime tests the continuing validity of the industrial regulatory and law enforcement model. For example, as a result of their lack of cyber crime legislation the Ukraine and Belarus have become major staging grounds for organized hacker syndicates. Because of the underlying complexity of such cases and the overlapping jurisdictions of authority within a country, one of the first things the laws should address is who or what has authority and responsibility for these cases. A significant cost avoidance could result from such reform, and money saved could be invested in training resource experts and the tools needed to investigate, prosecute, and punish cyber crime perpetrators. Substantively, the laws should address abuses of a computer or network that result in loss or destruction to the computer, the network, or people, and should include provisions for restitution for associated losses.

A December 2000 McConnell International survey provides a snapshot of the state of computer crime legislation worldwide. It examined the legal frameworks of 52 countries to determine each oneôs ability to prosecute perpetrators of ten types of computer crime. The survey showed that a patchwork of outdated and inconsistent

laws effectively function as a shield from prosecution for cyber criminals who attack electronic systems and information. In April 2002, an unauthorized user accessed over 260,000 California state personnel files. It took the state six weeks to discover that the system had been hacked. In response, that same year California enacted Senate Bill 1386. This law, effective July 1, 2003 mandates every state agency and every person or business that conducts business in California, that owns or licenses computerized data that includes personal information as defined in the Act, to provide notice in specified ways to any resident of California that the security of the data had been breached and that the entityôs personal information was or is reasonably believed to have been taken by the unauthorized user. California is the first state to require mandatory reporting of security breaches. It acknowledges the exponential growth of identity theft and the need for reforms to address the market failure. Although the Act is a giant step forward for consumers, it contains certain exemptions from the notice requirement. Nevertheless, other states now are responding to Californiaôs lead and are introducing mandatory reporting legislation.

For countries looking to develop cyber crime legislation, the Council of Europe provides some guidance. In 2001, it developed the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, and violations of network security. The treaty also provides for a series of powers and procedures, such as the search of computer networks and interception. The convergence of the telecommunications, computer, and financial services industries is changing the fundamentals of the industrial organization of the financial services sector. It also is redefining traditional boundaries and jurisdictional limits of responsibility because of shifting legal, regulatory, and financial concepts. Money transmitters and Internet service providers (ISPs) have become a critical sector of this new economic structure, and can have a direct impact on the security of a financial service provider, and potentially on the wider financial sector and economy as a whole. However, as a result of the lack of standardization in regulation and oversight, many money transmitters and ISPs insert significant risk into the payments system. Yet they are not required to post bond for their services and they carry no liability. In fact, legislation in some countries holds that ISPs are not liable for transmission failures or losses. Also, because money transmitters and ISPs are not subject to reporting requirements, little information is available on the extent of the vulnerabilityð though frequent losses are known about informally.

The ability to define a function or service is a crucial first step in determining whether it should be regulated or not, and who or what should regulate it. Money transmitters may perform a variety of services, including money order issuance, wire transfers, currency exchanges, check-cashing, and check-presentment. More recently, money transmitters have been providing electronic check-presentment services and point-of sale money payment order information to the accepting bank. Money transmitters operate outside the depository institution but often are associated in some way with one or more depository institutions in a downstream relationship. An ISP is often referred to in the law as a ñcommon carrierò. This is the same term that is used to define the basic utility service provided by telephone companies. The term implies that the provider holds itself out to the public as willing and able to move information from one point to another. Whether or not an entity is an ISP is difficult to determine under existing laws. ISPs are not regulated in most countries. Because the primary

focus of legislative initiatives targeting money transmitters has been to deter money laundering, most of the activity affecting this industry is derived from antiï money laundering sources. Developing appropriate regulatory schemes includes developing an approach to mitigate or manage risk.

Here, the concern is that money transmitters and ISPs are not legally liable for the services they provide. With the escalation of Internet-related commercial activities and the requisite need to provide ubiquitous payment system conduits, money transmitters are increasing the disintermediation of the traditional payments systems and have a higher profile in the eyes of law enforcement. The open, universal access architecture of the Internet places greater emphasis on identifying and analyzing systemic risks and vulnerabilities, eliminating risks where feasible, and continually monitoring both risks and security. Few emerging markets appear to have dealt with these issues explicitly thus far. This poses the question of how to do more with less and yet still increase security and privacy. The first recommendation is to enact legislation regulating all money transmitters and ISPs that provide service to the financial services sector, requiring them to be secure. The Uniform Money Services Business Act would be a good basis for regulating these providers. Another approach would be to build in a service-level agreement with appropriate refund mechanisms, liability, and warranties to the terms and conditions. Another avenue of defence is self-regulation through the automated clearinghouse process or, more broadly, via specific arrangements outlining security standards in the case of wholesale or retail payment networks. Building clearinghouse rules requiring all entities to use vendors that provide an appropriate level of security and to post sufficient money or bond to cover losses would create an incentive for the parties to establish a proper e-security standard. Insurance coverage is yet another means of protection. Financial services entities should use insurance to protect themselves from gap loss, whereby e-risk is realized even after insurance companies have required a financial services provider to meet specific security standards.

Self Assessment Exercise
Discuss the term privacy protection and its implication

4.0 Conclusion

No matter which approach is used, at a minimum, privacy laws should embrace the Fair Information Practice Principles set out in the European Union Directive on Data Protection. . The treaty also provides for a series of powers and procedures, such as the search of computer networks and interception. The convergence of the telecommunications, computer, and financial services industries is changing the fundamentals of the industrial organization of the financial services sector. It also is redefining traditional boundaries and jurisdictional limits of responsibility because of shifting legal, regulatory, and financial concepts.

5.0 Summary

Though most countries have laws in place to regulate different components of the payments system, no country has yet addressed payments systems issues comprehensively. Based on this fact some recommendations were made, that the Payment systems legislation should identify, license, and regulate any directly related payment system entities, such as money transmitters and ISPs. It should require such elements to operate in a safe and sound manner so as to protect the integrity and

reliability of the system. It should require the timely and accurate reporting of all security incidents, including all electronically related money losses. Finally, it should require all payment system entities to adhere to a documented security program and should encourage some form of shared risk protection.

6.0 Tutor Marked Assignment

Explain the importance of legislation in the improvement of security and privacy.

7.0 References/ Further Reading

(1) Bajkowski, Julian. (2003) ñAustralian Amex site made óunusableô by Slammer worm.ò *Computerworld*, February 3,

(2) Claessens, Stijn, and Marion Jansen, eds. (2000). *The Internationalization of Financial Services.* Boston, Mass.: Kluwer Academic Press for the World Bank and the World Trade Organization.

(3) Computer Security Institute. (2003). *CSI/FBI Computer Crime Report*. CSI, San Francisco.

(4) Federal Bureau of Investigations and Computer Security Institute. (2003). ñ2003 CSI/FBI Computer Crime and Security Survey.ò Eight Annual Report, by Computer Security Institute.

(5) Furst, Karen, William W. Lang, and Daniel E. Nolle. (1998). ñTechnological Innovation in Banking and Payments: Industry Trends and Implications for Banks.ò *Quarterly Journal* 17 (3): 23-31.

(6) Glaessner, Thomas, and Tom Kellerman, and Valerie McNevin. (2002). ñElectronic Security: Risk Mitigation in Financial Transactions.ò Processed.

(7) Gilbride, Edward. (2001). ñEmerging Bank Technology and the Implications for E-Crime.ò Presentation, September 3.

(8) Group of 8. (2003). ñPrinciples for Protecting Critical Information Infrastructure.ò May.

UNIT 3
Hand tools and powered tools

Content

1.0 Introduction

The unit identifies various types of hand and power tools and their potential hazards with regards to electrical connections. It also highlights ways to prevent worker injury through proper use of the tools and through the use of appropriate personal protective equipment.

2.0 Objectives

To understand the security and hazards hand and powered tools can create in the work environment.

3.0 Main body

3.1 Tools and Hazards

Tools are such a common part of our lives that it is difficult to remember that they may pose hazards. Tragically, a serious incident can occur before steps are taken to identify and avoid or eliminate tool-related hazards. Employees who use hand and power tools and are exposed to the hazards of falling, flying, abrasive, and splashing objects, or to harmful dusts, fumes, mists, vapours, or gases must be provided with the appropriate personal protective equipment. All electrical connections for these tools must be suitable for the type of tool and the working conditions (wet, dusty, flammable vapours). When a temporary power source is used for construction a ground-fault circuit interrupter should be used. Employees should be trained in the proper use of all tools. Workers should be able to recognize the hazards associated with the different types of tools and the safety precautions necessary.

Five basic safety rules can help prevent hazards associated with the use of hand and power tools:
ÅKeep all tools in good condition with regular maintenance.
ÅUse the right tool for the job.
ÅExamine each tool for damage before use and do not use damaged tools.
ÅOperate tools according to the manufacturersô instructions.
ÅProvide and use properly the right personal protective equipment.

3.2. Tools and Hazards

This section identifies various types of hand and power tools and their potential hazards. They also identify ways to prevent worker injury through proper use of the

tools and through the use of appropriate personal protective equipment. Hand tools are tools that are powered manually. Hand tools include anything from axes to wrenches. The greatest hazards posed by hand tools result from misuse and improper maintenance. Some examples include the following:

- If a chisel is used as a screwdriver, the tip of the chisel may break and fly off, hitting the user or other employees.
- If a wooden handle on a tool, such as a hammer or an axe, is loose, splintered, or cracked, the head of the tool may fly off and strike the user or other employees.
- If the jaws of a wrench are sprung, the wrench might slip.
- If impact tools such as chisels, wedges, or drift pins have mushroomed heads, the heads might shatter on impact, sending sharp fragments flying toward the user or other employees.

The employer is responsible for the safe condition of tools and equipment used by employees. Employers shall not issue or permit the use of unsafe hand tools. Employees should be trained in the proper use and handling of tools and equipment. Employees, when using saw blades, knives, or other tools, should direct the tools away from aisle areas and away from other employees working in close proximity. Knives and scissors must be sharp; dull tools can cause more hazards than sharp ones. Cracked saw blades must be removed from service. Wrenches must not be used when jaws are sprung to the point that slippage occurs. Impact tools such as drift pins, wedges, and chisels must be kept free of mushroomed heads. The wooden handles of tools must not be splintered. Iron or steel hand tools may produce sparks that can be an ignition source around flammable substances. Where this hazard exists, spark-resistant tools made of non-ferrous materials should be used where flammable gases, highly volatile liquids, and other explosive substances are stored or used.

Appropriate personal protective equipment such as safety goggles and gloves must be worn to protect against hazards that may be encountered while using hand tools. Workplace floors shall be kept as clean and dry as possible to prevent accidental slips with or around dangerous hand tools. Power tools must be fitted with guards and safety switches; they are extremely hazardous when used improperly. The types of power tools are determined by their power source: electric, pneumatic, liquid fuel, hydraulic, and powder-actuated. To prevent hazards associated with the use of power tools, workers should observe the following general precautions:

- Never carry a tool by the cord or hose.
- Never yank the cord or the hose to disconnect it from the receptacle.
- Keep cords and hoses away from heat, oil, and sharp edges.
- Disconnect tools when not using them, before servicing and cleaning them, and when changing accessories such as blades, bits, and cutters.
- Keep all people not involved with the work at a safe distance from the work area.
- Secure work with clamps or a vice, freeing both hands to operate the tool.
- Avoid accidental starting. Do not hold fingers on the switch button while carrying a plugged-in tool.
- Maintain tools with care; keep them sharp and clean for best performance.
- Follow instructions in the userôs manual for lubricating and changing accessories.
- Be sure to keep good footing and maintain good balance when operating power tools.

- Wear proper apparel for the task. Loose clothing, ties, or jewellery can become caught in moving parts.
- Remove all damaged portable electric tools from use and tag them: ñDo Not Use.ò

Guards

The exposed moving parts of power tools need to be safeguarded. Belts, gears, shafts, pulleys, sprockets, spindles, drums, flywheels, chains, or other reciprocating, rotating, or moving parts of equipment must be guarded. Machine guards, as appropriate, must be provided to protect the operator and others from the following:

- Point of operation.
- In-running nip points.
- Rotating parts.

Flying chips and sparks. Safety guards must never be removed when a tool is being used. Portable circular saws having a blade greater than 2 inches (5.08 centimeters) in diameter must be equipped at all times with guards. An upper guard must cover the entire blade of the saw. A retractable lower guard must cover the teeth of the saw, except where it makes contact with the work material. The lower guard must automatically return to the covering position when the tool is withdrawn from the work material.

Operating Controls and Switches

The following hand-held power tools must be equipped with a constant-pressure switch or control that shuts off the power when pressure is released: drills; tapers; fastener drivers; horizontal, vertical, and angle grinders with wheels more than 2 inches (5.08 centimetres) in diameter; disc sanders with discs greater than 2 inches (5.08 centimetres); belt sanders; reciprocating saws; sabre saws, scroll saws, and jigsaws with blade shanks greater than 1/4-inch (0.63 centimetres) wide; and other similar tools. These tools also may be equipped with a ñlock-onò control, if it allows the worker to also shut off the control in a single motion using the same finger or fingers. The following hand-held power tools must be equipped with either a positive ñon-offò control switch, a constant pressure switch, or a ñlock-onò control: disc sanders with discs 2 inches (5.08 centimetres) or less in diameter; grinders with wheels 2 inches (5.08 centimetres) or less in diameter; platen sanders, routers, planers, laminate trimmers, nibblers, shears, and scroll saws; and jigsaws, sabre and scroll saws with blade shanks a nominal 1/4-inch (6.35 millimetres) or less in diameter. It is recommended that the constant- pressure control switch be regarded as the preferred device. Other hand-held power tools such as circular saws having a blade diameter greater than 2 inches (5.08 centimetres), chain saws, and percussion tools with no means of holding accessories securely must be equipped with a constant-pressure switch.

Electric Tools

Employees using electric tools must be aware of several dangers. Among the most serious hazards are electrical burns and shocks. Electrical shocks, which can lead to injuries such as heart failure and burns, are among the major hazards associated with electric powered tools. Under certain conditions, even a small amount of electric current can result in fibrillation of the heart and death. An electric shock also can cause the user to fall off a ladder or other elevated work surface and be injured due to

the fall. To protect the user from shock and burns, electric tools must have a three-wire cord with a ground and be plugged into a grounded receptacle, be double insulated, or be powered by a low voltage isolation transformer. Three-wire cords contain two current carrying conductors and a grounding conductor. Any time an adapter is used to accommodate a two-hole receptacle, the adapter wire must be attached to a known ground. The third prong must never be removed from the plug.

Double-insulated tools are available that provide protection against electrical shock without third-wire grounding. On double insulated tools, an internal layer of protective insulation completely isolates the external housing of the tool.

The following general practices should be followed when using electric tools:
ÅOperate electric tools within their design limitations.
ÅUse gloves and appropriate safety footwear when using electric tools.
ÅStore electric tools in a dry place when not in use.

ÅDo not use electric tools in damp or wet locations unless they are approved for that purpose.
ÅKeep work areas well lighted when operating electric tools.
Å Ensure that cords from electric tools do not present a tripping hazard. In the construction industry, employees who use electric tools must be protected by ground-fault circuit interrupters or an assured equipment-grounding conductor program.

Portable Abrasive Wheel Tools
Portable abrasive grinding, cutting, polishing, and wire buffing wheels create special safety problems because they may throw off flying fragments. Abrasive wheel tools must be equipped with guards that:
(1) cover the spindle end, nut, and flange projections;
(2) maintain proper alignment with the wheel; and
(3) do not exceed the strength of the fastenings.

Before an abrasive wheel is mounted, it must be inspected closely for damage and should be sound- or ring-tested to ensure that it is free from cracks or defects. To test, wheels should be tapped gently with a light, non-metallic instrument. If the wheels sound cracked or dead, they must not be used because they could fly apart in operation. A stable and undamaged wheel, when tapped, will give a clear metallic tone or ñring.ò To prevent an abrasive wheel from cracking, it must fit freely on the spindle. The spindle nut must be tightened enough to hold the wheel in place without distorting the flange. Always follow the manufacturerôs recommendations. Take care to ensure that the spindle speed of the machine will not exceed the maximum operating speed marked on the wheel. An abrasive wheel may disintegrate or explode during start-up. Allow the tool to come up to operating speed prior to grinding or cutting. The employee should never stand in the plane of rotation of the wheel as it accelerates to full operating speed. Portable grinding tools need to be equipped with safety guards to protect workers not only from the moving wheel surface, but also from flying fragments in case of wheel breakage.

When using a powered grinder:
ÅAlways use eye or face protection.
ÅTurn off the power when not in use.

ÅNever clamp a hand-held grinder in a vise.

Pneumatic Tools

Pneumatic tools are powered by compressed air and include chippers, drills, hammers, and sanders. There are several dangers associated with the use of pneumatic tools. First and foremost is the danger of getting hit by one of the toolôs attachments or by some kind of fastener the worker is using with the tool. Pneumatic tools must be checked to see that the tools are fastened securely to the air hose to prevent them from becoming disconnected. A short wire or positive locking device attaching the air hose to the tool must also be used and will serve as an added safeguard. If an air hose is more than 1/2-inch (12.7 millimetres) in diameter, a safety excess flow valve must be installed at the source of the air supply to reduce pressure in case of hose failure. In general, the same precautions should be taken with an air hose that are recommended for electric cords, because the hose is subject to the same kind of damage or accidental striking, and because it also presents tripping hazards. When using pneumatic tools, a safety clip or retainer must be installed to prevent attachments such as chisels on a chipping hammer from being ejected during tool operation. Pneumatic tools that shoot nails, rivets, staples, or similar fasteners and operate at pressures more than 100 pounds per square inch (6,890 kPa), must be equipped with a special device to keep fasteners from being ejected, unless the muzzle is pressed against the work surface. Airless spray guns that atomize paints and fluids at pressures of 1,000 pounds or more per square inch (6,890 kPa) must be equipped with automatic or visible manual safety devices that will prevent pulling the trigger until the safety device is manually released. Eye protection is required, and head and face protection is recommended for employees working with pneumatic tools. Screens must also be set up to protect nearby workers from being struck by flying fragments around chippers, riveting guns, staplers, or air drills. Compressed air guns should never be pointed toward anyone. Workers should never ñdead-endò them against themselves or anyone else. A chip guard must be used when compressed air is used for cleaning. Use of heavy jackhammers can cause fatigue and strains. Heavy rubber grips reduce these effects by providing a secure handhold. Workers operating a jackhammer must wear safety glasses and safety shoes that protect them against injury if the jackhammer slips or falls. A face shield also should be used. Noise is another hazard associated with pneumatic tools. Working with noisy tools such as jackhammers requires proper, effective use of appropriate hearing protection.

Liquid Fuel Tools

Fuel-powered tools are usually operated with gasoline. The most serious hazard associated with the use of fuel-powered tools comes from fuel vapours that can burn or explode and also give off dangerous exhaust fumes. The worker must be careful to handle, transport, and store gas or fuel only in approved flammable liquid containers, according to proper procedures for flammable liquids. Before refilling a fuel-powered tool tank, the user must shut down the engine and allow it to cool to prevent accidental ignition of hazardous vapours. When a fuel-powered tool is used inside a closed area, effective ventilation and/or proper respirators such as atmosphere-supplying respirators must be utilized to avoid breathing carbon monoxide. Fire extinguishers must also be available in the area.

Powder-Actuated Tools

Powder-actuated tools operate like a loaded gun and must be treated with extreme caution. In fact, they are so dangerous that they must be operated only by specially trained employees. When using powder-actuated tools, an employee must wear suitable ear, eye, and face protection. The user must select a powder levelð high or low velocityð that is appropriate for the powder-actuated tool and necessary to do the work without excessive force. The muzzle end of the tool must have a protective shield or guard centred perpendicular to and concentric with the barrel to confine any fragments or particles that are projected when the tool is fired. A tool containing a high-velocity load must be designed not to fire unless it has this kind of safety device. To prevent the tool from firing accidentally, two separate motions are required for firing. The first motion is to bring the tool into the firing position, and the second motion is to pull the trigger. The tool must not be able to operate until it is pressed against the work surface with a force of at least 5 pounds (2.2 kg) greater than the total weight of the tool. If a powder-actuated tool misfires, the user must hold the tool in the operating position for at least 30 seconds before trying to fire it again. If it still will not fire, the user must hold the tool in the operating position for another 30 seconds and then carefully remove the load in accordance with the manufacturerôs instructions. This procedure will make the faulty cartridge less likely to explode. The bad cartridge should then be put in water immediately after removal. If the tool develops a defect during use, it should be *tagged* and must be *taken out of service immediately* until it is properly repaired. Safety precautions that must be followed when using powder actuated tools include the following:

- Do not use a tool in an explosive or flammable atmosphere.
- Inspect the tool before using it to determine that it is clean, that all moving parts operate freely, and that the barrel is free from obstructions and has the proper shield, guard, and attachments recommended by the manufacturer.
- Do not load the tool unless it is to be used immediately.
- Do not leave a loaded tool unattended, especially where it would be available to unauthorized persons.
- Keep hands clear of the barrel end.
- Never point the tool at anyone.

When using powder-actuated tools to apply fasteners, several additional procedures must be followed:

- Do not fire fasteners into material that would allow the fasteners to pass through to the other side.
- Do not drive fasteners into very hard or brittle material that might chip or splatter or make the fasteners ricochet.
- Always use an alignment guide when shooting fasteners into existing holes.
- When using a high-velocity tool, do not drive fasteners more than 3 inches (7.62 centimetres) from an unsupported edge or corner of material such as brick or concrete.
- When using a high velocity tool, do not place fasteners in steel any closer than 1/2-inch (1.27 centimetres) from an unsupported corner edge unless a special guard, fixture, or jig is used.

Hydraulic Power Tools

The fluid used in hydraulic power tools must be an approved fire resistant fluid and must retain its operating characteristics at the most extreme temperatures to which it

will be exposed. The exception to fire-resistant fluid involves all hydraulic fluids used for the insulated sections of derrick trucks, aerial lifts, and hydraulic tools that are used on or around energized lines. This hydraulic fluid shall be of the insulating type. The manufacturerôs recommended safe operating pressure for hoses, valves, pipes, filters, and other fittings must not be exceeded.

All jacksð including lever and ratchet jacks, screw jacks, and hydraulic jacksð must have a stop indicator, and the stop limit must not be exceeded. Also, the manufacturerôs load limit must be permanently marked in a prominent place on the jack, and the load limit must not be exceeded. A jack should never be used to support a lifted load. Once the load has been lifted, it must immediately be blocked up. Put a block under the base of the jack when the foundation is not firm, and place a block between the jack cap and load if the cap might slip.

To set up a jack, make certain of the following:
ÅThe base of the jack rests on a firm, level surface;
ÅThe jack is correctly centred;
ÅThe jack head bears against a level surface; and
ÅThe lift force is applied evenly.

Proper maintenance of jacks is essential for safety. All jacks must be lubricated regularly. In addition, each jack must be inspected according to the following schedule:
(1) For jacks used continuously or intermittently at one siteð inspected at least once every 6 months,
(2) For jacks sent out of the shop for special workð inspected when sent out and inspected when returned, and
(3) For jacks subjected to abnormal loads or shockð inspected before use and immediately thereafter.

Self Assessment Exercise

What do you understand by the term hand tools? What Are the Dangers of Powered Tools?

4.0 Conclusion

There are various tools in the work environment which are capable of posing personal as well as industrial security treats if they are not properly used. Some of these tools have been broadly categorised based on the technological know-how and in terms of shapes and sizes into two: hand and powered tools. It is hereby important to say that so long as they are properly used, maintained or repaired as at when due they pose little or no security threat.

5.0 Summary

This unit identifies various types of hand and powered tools and their potential hazards; ways to prevent worker injury through proper use of the tools and through the use of appropriate personal protective equipment. Powder-actuated tools was said to operate like a loaded gun and must be treated with extreme caution. For hydraulic power tools, the fluid must be an approved fire resistant fluid and must retain its operating characteristics at the most extreme temperatures to which it will be exposed.

Fuel-powered tools are usually operated with gasoline. The most serious hazard associated with the use of fuel-powered tools comes from fuel vapours that can burn or explode and also give off dangerous exhaust fumes**.** Pneumatic tools are powered by compressed tools such as chippers, drills, hammers, and sanders. Of all mentioned it is obvious that irrespective of the size and make-up caution is expected to be taken whenever they are being used.

6.0 Tutor Marked Assignment

1. Define Power tools and explain with adequate examples.
2. Power tools must be fitted with guards and safety switches; they are Power tools and could be extremely hazardous discuss.

7.0 References/ Further Reading

(1) Armstrong, G. and Giulianotti, R. (1998): From Another Angle: Police Surveillance and Football Supporters, in C.Norris, J. Moran, and G. Armstrong (eds.):*Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate.

(2) Brand, S. and Price, R. (2000): *The Economic and Social Costs of Crime*. Home Off ice Research Study No 217. London: Home Office.

(3) Brown, B. (1995): *CCTV in Town Centres: Three Case Studies*, Crime Prevention and Detection Series, no.73. London: HMSO.

(4) Clarke, R.V.G and Felson, M. (1993): *Routine Activity and Rational Choice*. New York :Transaction Publications

(5) Evett, C. and Wood, J. (2004): Designing a Control Room, *CCTV Image*, Spring, pp 24-25.

(6) Farrall, S., Bannister, J., Ditton, J. and Gilchrist, E. (2000): ÓSocial Psychology and the Fear of Crime: Re-examining a Speculative ModelÔ, *British Journal of Criminology*, 40, 399-413.

(7) John L. Henshaw and Elaine L. Chao 2002. Hand and Power Tools. U.S. department of Labor, Occupational Safety and Health Administration. OSHA 3080.

(8) Laycock, G. and Tilley, N. (1995): *Policing and Neighbourhood Watch: Strategic issues*, Crime Detection and Prevention Series, 60. London: HMSO.

(9) **UNIT 4**

Electronic Document Security

Content

1.0 Introduction

As organizations move more business processes online, protecting the confidentiality and privacy of the information used during these processes is essential. Because many automated processes rely on electronic documents that contain mission-critical, personal, and sensitive information, organizations must make significant investments to properly protect these documents.

2.0 Objectives

This unit is intended to provide the reader with a brief overview of relevant document security issues and technologies, as well as to introduce the Adobe suite of document security solutions. The unit also summarizes Adobe implementations for document control and digital signatures.

3.0 Main body

3.1: Security of Electronic Document

There are three main reasons that organizations need to address the security of electronically shared documents:

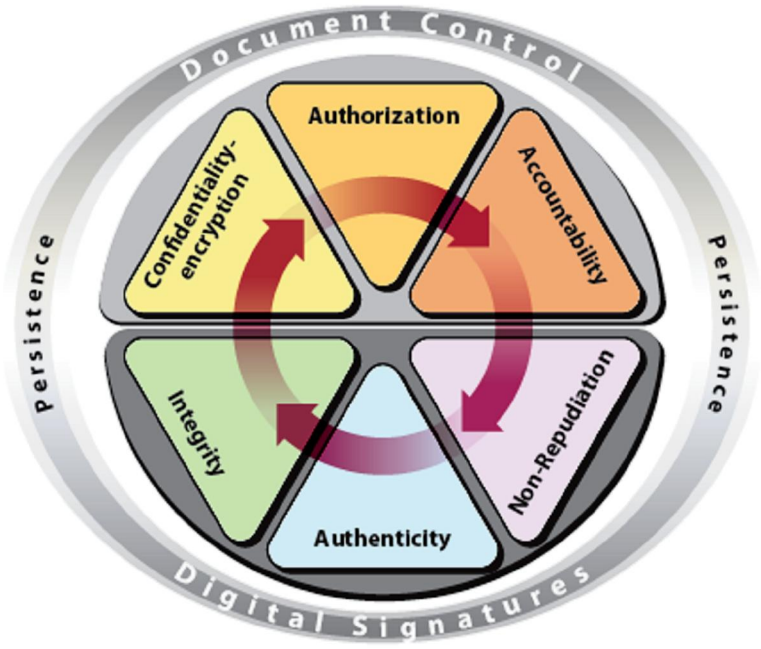
1. Regulatory requirementsð Many companies are directly or indirectly affected by government mandates and regulations for providing consumer privacy.

2. Return on investment (ROI)ð Organizations can achieve significant ROI by migrating to electronic business processes. Automated workflows allow prospects, customers, partners, and suppliers to participate, enabling organizations to reap significant cost savings while improving customer satisfaction and loyalty. However, many workflows cannot be automated until adequate protections are put in place on the electronically shared information. For instance, how can you be sure that the bank statement you received is truly from your bank (authenticity), that it has not been altered in transit (integrity), and that it has not been viewed by someone other than the intended recipient (confidentiality)?

3. Information securityð Thefts of proprietary information are increasing, which can jeopardize revenue, competitive advantage, and customer relationships; generate negative publicity; and result in significant penalties and fines for failure to comply with privacy laws. Many information security solutions attempt to protect electronic documents only at their storage location or during transmission. For example,

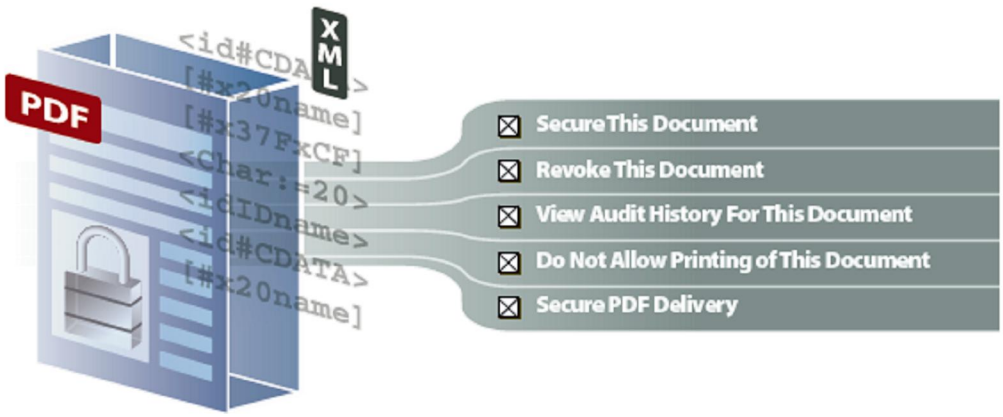
organizations rely on document management systems and virtual private networks (VPNs) to protect documents. With this approach document security remains a problem because these solutions secure only the communication line or storage site; they do not provide protection for the actual content of an electronic document throughout its lifecycle. When the document reaches the recipient, the protection is lost, and the document can be intentionally or unintentionally forwarded to and viewed by unauthorized recipients. Consequently, many organizations are forced to engage in an inconsistent combination of online and paper processes in which sensitive documents must still be printed and physically delivered to achieve adequate security. As a result, the potential benefits of online processing cannot be fully realized.

A significantly more effective solution for protecting an electronic document is to assign security parameters that are an integral part of the document itself. The following criteria define persistent document security:
Confidentialityð Who should have access to the document?
Authorizationð What permissions does the user have for working with the document?
Accountabilityð What has the recipient done with the document?
Integrityð How do you know if the document has been altered?
Authenticityð How do you know where the document came from?
Non-repudiationð Can the signatory deny signing the document?



Six key criteria for providing persistent document security

The following sections survey the major technologies used to provide document control and digital signatures and identify the technologies. For instance Adobe has implemented some document security solutions as shown below. It gives various options on how documents can be secured by organisations and computer owners.



Document control provides confidentiality, authorization, and accountability. The illustration above shows some of the document control options available with Adobe LiveCycleÊ Policy Server and Adobe® Acrobat® software.

3.2 Document control

1. Confidentiality—encryption

Encryption is the process of transforming information *(plaintext)* into an incomprehensible form *(ciphertext)*. Encryption is an effective technique for managing document access.
Decryption is the reverse process that transforms ciphertext back to the original plaintext.

Cryptography refers to the two processes of encryption and decryption and its implementation is referred to as a *cryptosystem*. Popular encryption systems use the concept of keys. An encryption key is data that combines with an encryption algorithm to create ciphertext from plaintext and recover plaintext from ciphertext. Today, security experts widely agree on ñKerckhoffôsò principle as the basis of an effective cryptosystem. Kerckhoffôs principle states that the key is the only portion of a cryptosystem that must remain secret for the entire system to be secure. If the strength of the cryptosystem relies on the fact that an attacker does not know how the algorithm works, then it is just a matter of time before it can be reverse-engineered and broken. Two main types of encryption keys include symmetric and asymmetric.

a. Symmetric keys
Symmetric key cryptography uses the same key for both encryption and decryption and is very fast and difficult to break with large keys. However, because both parties need the same key for effective communication to occur, key distribution becomes an issue. Today, common symmetric key encryption algorithms are AES, DES, 3DES, and RC4. Adobe products leverage AES (128- and 256-bit) and RC4 (128-bit), as they have evolved into very strong standards.
b. Asymmetric keys
Asymmetric key cryptography, also called *public key cryptography*, uses key pairs for encryption and decryption. For instance, if the first key encrypts the content, then the second key of the pair decrypts the content. Similarly, if the second key is used to encrypt the information, then the first key must be used to decrypt the content.

Typically, one key in the pair is labelled as the public key and the other as the private key. An individual keeps the private key secret, while the public key is freely distributed to others who wish to communicate with the individual. When someone wishes to send the individual a confidential message, he or she can encrypt it with the freely available public key and send the ciphertext to the individual. Because the individual is the only one who has the private key, he or she is the only one who can decrypt the content. Asymmetric keys help solve the key distribution problem, but the algorithms tend to be slower for equivalent strengths. Some common asymmetric algorithms are RSA, DSA, and El Gamal. Adobe leverages RSA (512-, 1024-, and 2048-bit) as it has evolved into a global standard.

- **Hybrid Encryption**

Security systems tend to use a hybrid solution to increase the security and speed of encrypting documents. One approach is to use asymmetric keys to protect the symmetric keys, and then use the symmetric keys for encrypting the information. This technique helps to solve both the key distribution challenge of symmetric key cryptography while solving the performance problem of asymmetric key cryptography. Adobe Acrobat software leverages hybrid approaches so single documents can be protected for multiple recipients, each possessing unique key pairs. The file size is not significantly increased during this method because the entire document does not need to be encrypted for each person. Instead, the document is encrypted with a single symmetric key and that symmetric key is encrypted for each recipient with their respective public key.

2. Authorization

In addition to managing who can open a document, organizations gain additional protection through authorization. Authorization specifies what a user can do with a document and is achieved via permissions and dynamic document control.

• **Permissions** govern a userôs actions while working with a protected document. Permissions can specify whether or not a recipient who has access to the document is allowed to print or copy content, fill in fields, add comments or annotate the document, insert or remove pages, forward the document, access the document offline, digitally sign the document, and so forth.

• **Dynamic document control** maintains access rights and permissions assigned to an electronic document once it has been published and distributed. A documentôs author can make changes to a released document without having to manually redistribute it since the changes are automatically pushed to all existing versions of the document no matter where they reside. Using dynamic document control, organizations can manage and monitor electronic document use inside and outside the firewall, online and offline, and across multiple documents.

Dynamic document control includes the following capabilities:

Å**Document expiration and revocation**ð Post-publication document control can be maintained through the application of expiration dates and the ability to revoke access to a document. For example, an author can send a document that will expire in two weeks so that recipients will not be able to access it once the expiration date has passed. Or, access to a document can be automatically revoked if an authorized recipient leaves the project or changes departments.

Å**Offline access management**ð Organizations can manage how long an authorized recipient can access a document offline. Once the specified length of time has passed, the recipient can no longer view the document and must go back online to gain further access. Any access or permission changes that the author has made to the distributed document will be applied when the recipient goes back online.
Å**Persistent version control**ð Content and document management systems provide an effective mechanism for version control as long as a document stays within the confines of the system. Persistent version control expands on these capabilities by maintaining version control outside the system and offline. It allows document authors to make changes to a documentôs usage policies and prevent the obsolete version from being accessed while providing end users with the location of the updated version, no matter where the document resides.

3. Accountability
Document auditing allows organizations to maintain accountability with regard to the use of protected documents, because they can know precisely:
ÅHow a recipient has used a document
ÅHow often each type of usage occurred
ÅWhen that usage occurred
Accountability is achieved when an author can track each recipientôs use of a document for each permission assigned (such as allowing a user to fill in fields on a form, print, forward, save a copy, and so forth.) Auditing should include automatic notifications about the use of protected documents. For example, a customer service representative sends a customer a time-critical electronic statement that requires an action on the customerôs part, such as a reply or digital signature. Once the customer receives the electronic document, the representative is automatically notified when the customer opens it. If the customer fails to open the document, the representative is notified after 24 hours. Alternatively, a customer relationship management (CRM) system can leverage failure notification to initiate an escalation or specific follow-up task by the customer service representative.

Digital signatures
When enterprises distribute documents electronically, it is often important that recipients can verify:
ÅThat the content has not been altered *(integrity)*
ÅThat the document is coming from the actual person who sent it *(authenticity)*
ÅThat an individual who has signed the document cannot deny the signature *(non-repudiation)*
Digital signatures address these security requirements by providing greater assurances of document integrity, authenticity, and non-repudiation.

4. Integrity
Digital signatures enable recipients to verify the integrity of an electronic document that is used in one-way or round-trip workflows. For example, when a digital signature is applied to a quarterly financial statement, recipients have more assurance that the financial information has not been altered since it was sent. Methods for maintaining integrity include:
Å**Parity bits or cyclical redundancy checking (CRC) functions**ð CRC functions work well for unintentional modifications, such as wire interference, but they can be circumvented by a clever attacker.

Å**One-way hash**ð A one-way hash creates a fixed-length value, called the hash value or message digest for a message of any length. A hash is like a unique fingerprint. With a hash attached to the original message, a recipient can determine if the message was altered by re-computing the hash and comparing his or her answer to the attached hash. Common hashing algorithms are MD5, SHA-1, and SHA-256. Adobe has adopted the SHA-1 and SHA-256 algorithms because of their wide acceptance as a security standard.

Å **Message Authentication Codes (MAC)**ð A MAC prevents an attacker from obtaining the original message, modifying it, and attaching a new hash. In this case, a symmetric key is connected to the MAC and then hashed (HMAC). Without the key, an attacker cannot forge a new message. Adobe uses HMACs where appropriate.

5. Authenticity

Digital signatures provide document authenticity by verifying a signerôs digital identity. For example, a digitally signed quarterly financial statement allows recipients to verify the identity of the sender and assures them that the financial information has not been altered since it was sent. Digital signatures are created using asymmetric key cryptography. For document encryption, a documentôs author encrypts a document using a public key. Because the recipient is the only person with the private key, he or she is the only one who can decrypt the message. Digital signatures reverse the use of public and private keys for document authenticity. The author encrypts the hash of the message with a private key. Only the public key can correctly decrypt the hash and use it to see if it matches a new hash of the document. Because recipients of the document have the authorôs public key, they gain greater assurances that the individual who signed the document was the person who encrypted the original hash.

The process that constitutes a digital signature is as follows:

ÅA hash is created of the original document.

ÅThe digital signature is created, which encrypts the hash with a private key.

ÅThe signature is included with the document.

Adobe Acrobat supports multiple digital signatures placed anywhere in the document for proper presentation. In fact, Adobe Acrobat tracks all previously ñsignedò versions within the document for easy verification of changes made during the documentôs lifecycle. Furthermore, Adobe offers a certified signature, which is the first signature on the document. With a certified signature, the author can specify what changes are allowed for integrity purposes. Adobe Acrobat will then detect and prevent those modifications.

6. Non-repudiation

Non-repudiation is a document security service that prevents the signor of the document from denying that they signed the document. Support for this service is often driven by authentication and time-stamping capabilities such as PKI.

- **Public key infrastructure (PKI)**

Public key infrastructure (PKI) mainly provides a digital certificate that enables a documentôs recipient to know whether or not a specific public key really belongs to a specific individual. Digital certificates bind a person (or entity) to a public key. Certificate authorities (CA) issue these certificates and recipients must trust the CA who issued the certificate. X.509 is the widely accepted certificate standard that

Adobe uses. If a certificate expires or a private key is compromised, the CA will revoke the certificate and record the revocation. As part of the process of authenticating a digital certificate, recipients can check the certificateôs status. Certificate validity can be checked using the following standard methods:
ÅCertificate revocation list (CRL)
ÅOnline Certificate Status Protocol (OCSP)
Adobe uses both CRL and OCSP.

The following additional mechanisms can make up a PKI:
Å**Public-Key Cryptography Standards (PKCS)**ð A set of standard protocols for PKI used by multiple vendors. The standards include RSA encryption, password-based encryption, extended certificate syntax, and cryptographic message syntax for secure multipurpose Internet mail extensions (S/MIME).
• **Registration authority**ð Used to run background checks on individuals who wish to obtain a certificate.
Å**Certificate repository**ð Repositories that house digital certificates.
Å**Key update, backup, recovery, and history**—Mechanisms for key maintenance and archiving.
Å **Cross-certification**ð In the absence of a single global PKI, which is highly unlikely, this mechanism allows users from one PKI to validate certificates from users in another trusted PKI.
Å**Time stamping**ð A critical component of non-repudiation that offers a time stamp from a trusted third party.

Self Assessment Exercise
What are the main reasons for securing electronically shared documents?

4.0 Conclusion
The use of sensitive and mission-critical information in electronic processes is essential for thousands of businesses and government agencies. Adobe security solutions leverage standards-based techniques for document control and digital signatures to provide effective solutions that enhance the privacy and confidentiality of electronic documents and forms. With a comprehensive set of desktop- and server-based solutions, Adobe offers convenient, easy-to-use document security capabilities that encourage users to keep information private and help organizations meet the strictest regulations for sharing information electronically. Adobe security solutions enable organizations to replace paper-based business processes with electronic processes to reap the benefits of improved operational efficiency, reduced costs, and increased customer and constituent satisfaction.

5.0 Summary
This unit examines information security solutions and how best electronic documents can be secured at their storage location or during transmission. However, these solutions do not provide protection for the entire lifecycle of an electronic document. When the document reaches the recipient, the protection is lost, and the document can be intentionally or unintentionally forwarded to and viewed by unauthorized recipients. A significantly more effective solution is to protect a document by assigning security parameters that travel with it. Six criteria must be met in order to provide more effective protection for an electronic document throughout its lifecycle:

1. Confidentiality; 2 Authorization; 3 Accountability; 4 Integrity; 5 Authenticity; 6 Non-repudiation

The two major security techniques used to establish these six document security criteria are document control and digital signatures. The Adobe suite of security solutions delivers document control and digital signature services that simplify the process of protecting sensitive electronic documents and forms. Organizations can easily integrate Adobe document security solutions into current business processes and enterprise infrastructure to support a wide range of simple and complex processes. Adobe solutions dynamically protect electronic documents inside and outside the network, online and offline to provide persistent, end-to-end protection throughout an electronic documentôs lifecycle.

6.0 Tutor Marked Assignment

List and explain six criteria that must be met in order to provide more effective protection for an electronic document.

7.0 References/ Further Reading

(1) Mercuri, R. (2000) "Voting Automation (Early and Often?), Inside Risks" Communications of the ACM, vol.43, n.11.

(2) Mercuri, R., Neumann, P.G (2003) "Verification for Electronic Balloting Systems" Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 31-42. Kluwer, Boston.

(3) Rubin, A. (2001) "Security Consideration for remote electronic voting over the Internet" AT&T labs ï Florham Park, NJ, http://avirubin.com/evoting. security.html.

(4) Schryen, G. (2004). ñSecurity Aspects of Internet Votingò, Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS 37), January

(5) *www.adobe.com/security 200* A primer on electronic document security technical White Paper *retrieved 17/09/08*

(6) **UNIT 5**

Electronic Security: Protecting Your Resources

Content

Content

1.0 Introduction

Everyone has heard stories of computer security problems within various organizations, with consequences ranging from loss of corporate secrets to significant financial loss. Unfortunately, many organizations still feel that running anti-virus software and implementing password-controlled network security secures their electronic resources from malicious attackers. The reality of modern Information Technology is that achieving impenetrable electronic security is virtually impossible. No one can afford to regard electronic threat as a simple problem with a simple solution.

2.0 Objectives

This unit describes some of the threats your organization faces when it provides Internet access to its members. It includes information on the types of threats, and how WebSpy software can be used to protect your organization.

3.0 Main body

Organizations may believe they are too small, and do not have any thing of interest or of value to an attacker. The fact is that all organizations have something of interest, such as hard disk space, bandwidth and processing power. The increased use of IP address scanning tools, denial of service tools and IIS worms implies that electronic security is an issue every organization should be concerned with. There are three main areas of electronic threat:

1. **Unauthorized External Access** Any organization connected to the Internet is subject to this threat. Implementing network security measures help to reduce this threat, however determined individuals can usually find a way to get through these security measures. Financial details, intellectual property, trade secrets, and confidential information are the main targets of this type of threat.

2. **Unauthorized Internal Activities** Trusted users of a network may either maliciously or unintentionally disclose valuable or confidential information to a third party. This security threat can often go unnoticed as the user is operating within their assigned level of security.

3. **Malware** Software designed to infiltrate or damage a computer system, such as viruses, worms, trojans, spyware, backdoors, rootkits and some hardware, can infect

your organization when connected to an external network such as the Internet. The risk is intensified through irresponsible or unaware staff. The possible consequences of these threats include:

- Diminished competitiveness due to the loss of crucial corporate information
- Financial loss due to the theft of proprietary information and through fraudulent activity
- Loss of time and resources when dealing with security breaches
- Lost productivity and wasted investment
- Legal proceedings resulting from the exposure of confidential information
- Negative publicity

These consequences can have severe impacts. All organizations must ensure their electronic resources are secure.

A Growing Concern

Organizations around the world are recognizing their vulnerability. The 2007 Computer Security Institute Survey highlighted the growing problem:

1. 46% of respondents detected computer security breaches within the past 12 months, with 26% having more than 10 incidents occur
2. The average annual loss reported was over $350,000

This survey also identified the two largest threats as internal:

1. 59% detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems)
2. 52% detected computer viruses

Other areas of concern include:

1. 18% of respondents reported a ótargeted attackô ï a malware attack aimed exclusively at their organization
2. Financial fraud was the source of greatest financial loss with an overall cost of over $20,000,000
3. 29% of organizations reported computer intrusions to law enforcement agencies

Electronic Security Approaches

There are two main approaches to security: *active* or *passive*. An *active* approach to security covers all actions designed to prevent a breach of your system's security model. A *passive* approach refers to the actions taken to monitor the security of your system based on that security model. All users should employ both active and passive approaches to security. Each of these approaches strengthens the other. Using monitoring products such as those developed by WebSpy Ltd. may provide you with information from server logs about a particular user abusing the organizations electronic resources (passive approach to security). This information may lead you to install an application that prevents or discourages them using the network in this way (active approach to security).

How do you determine your risk?
Every organization has different needs and priorities. So how do organizations determine the level of security they need? Organizations can employ a number of approaches to assess the level of security they need.

- **Quantitative risk assessment**

Many techniques have been developed attempting to qualitatively assess the risk of electronic threat, such as multiplying a risk threat frequency by a loss amount and comparing the result with the value of the protected asset. The main problem with this method is that the figures used in calculations are often highly subjective and inaccurate. Monitoring products such as those developed by WebSpy Ltd. help organizations assess how their systems are being used, in order to increase the accuracy of data used in risk assessment calculations.

- **Best practices** Commonly accepted baselines for security protection are often employed by organizations to avoid the uncertainty of conducting a formal risk analysis. This approach offers better protection from liability lawsuits, however unique security threats may be overlooked unless the organization conducts a comprehensive analysis of their situation. The International Standards Organization (ISO) has developed security standards (namely the ISO17799 standard) that organizations can adopt to secure their systems from malicious attack. Another organization that develops common guidelines on all areas of security is GASSP (Generally Accepted System Security Principles).

- **Scenario analysis approaches** The scenario analysis approach involves the creation of various scenarios in which computer security can be compromised. An appropriate mitigation procedure is then developed in attempt to prevent the security threat from occurring. The main disadvantage with this approach is the vast number of scenarios that exist. It is virtually impossible to attend to them all, therefore only threats that pose a significant risk to the organization are addressed.

- **Cost-benefits analysis** Cost benefit analysis attempts to base the choice of security safeguards on the cost of the protected asset. For some organizations, the loss of information may not have a large financial cost. The benefits of implementing an expensive system security solution will not justify the cost in such situations.

- **Insuring all risks** For organizations that cannot afford to design an electronic security solution, simply insuring all assets against risk may be a more viable solution. When this approach is taken, electronic security procedures often need to be assessed by an insurance company.

A combination of any of the above methods is often the best approach as it results in a more comprehensive analysis, and the implementation of a more effective security solution.

The WebSpy Approach
When determining your security requirements, no approach will be successful unless you have a clear understanding of how your electronic resources are used. Monitoring your Internet and network usage over a period of time provides you with information

required to make important decisions regarding your organizations electronic security. In an environment of evolving threats, it is important for an organization to have the ability to identify and adapt to new threats quickly. The capture and analysis of electronic resource usage at any point in time enables organizations to quickly respond to new threats. This flexibility is not available when using a purely predictive approach. Monitoring does not prevent the users of a network from accessing certain content. This means that the benefits of online research tools are not affected. In addition, monitoring also helps prevent one of the three main electronic threats: unauthorized internal activities. When an organizationôs members know they are being monitored, they are less likely to use electronic resources in a way that is against the organizations acceptable use policy.

Self Assessment Exercise
Electronic security is an issue in every organization. Discuss

4.0 Conclusion

With a comprehensive use and best practices of IT solutions, the security of electronic documents to a high level is assured. Some of the viruses such as, worms, trojans, spyware, backdoors, rootkits and some adware, if carefully understood can be well handled if organisations or individuals have adequate knowledge about risk management and approaches to assess the level of security they need. Knowledge is vital in any aspect of electronic security.

5.0 Summary

This unit examines major areas of electronic threat such as Unauthorised External and Internal Access; Infiltrated cum Damaging designers software. It highlights some modern concepts and approaches in protecting organisations resources in an Information Technological World. The use of anti-virus soft ware and the implementation of password-controlled network security were discussed and how they operate to secure electronic resources from malicious attackers. It concluded that achieving a hundred percent security is virtually impossible.

6.0 Tutor Marked Assignment

What are the approaches to assess the level of security needed by any organisation?

7.0 References/ Further Reading

(1) Approaches to choosing the strength of your security measures http://www.linuxsecurity.com/feature_stories/feature_story-98.html Retrieved 27/04/05

(2) Big-picture approaches to security - Network World Fusion http://www.nwfusion.com/newsletters/wireless/2002/01162807.html

(3) Generally Accepted System Security Principles (GASSP) http://web.mit.edu/security/www/gassp1.html. Retrieved 22/11/07

(4) International Standards Organization http://www.iso.org Computer Security Institute http://www.gocsi.com/ retrieved 16/01/02

(5) ISO17799 News - Issue 2 http://www.iso17799-web.com. Retrieved 12/09/09

(6) ISS' Top Ten Vulnerabilities https://gtoc.iss.net/topten.php. Retrieved 31/09/07

(7) WebSpy Ltd. website http://www.webspy.com. Retrieved 10/09/09

Module 3

Unit 1. Electronic Voting System
Unit 2. Security Analysis of Remote E-Voting
Unit 3. The Security of Electronic Banking
Unit 4. Security Solutions To Electronic Banking
Unit 5. Electronic Data Interchange (EDI) Messaging Security

UNIT 1

Electronic Voting System

Content

1.0 Introduction

Elections allow the populace to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviours and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. Unsurprisingly, history is littered with examples of elections being manipulated in order to influence their outcome. The design of a ñgoodò voting system, whether electronic or using traditional paper ballots or mechanical devices must satisfy a number of sometimes competing criteria. The *anonymity* of a voterôs ballot must be preserved, both to guarantee the voterôs safety when voting against a malevolent candidate, and to guarantee that voters have no evidence that proves which candidates received their votes. The existence of such evidence would allow votes to be purchased by a candidate. The voting system must also be *tamper-resistant* to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders. These are security issues which must be tackled and put in place in order to encourage and build voters confidence in electioneering. Another factor, as shown by the so-called ñbutterfly ballotsò in the Florida 2000 presidential election, is the importance of *human factors*. A voting system must be comprehensible to and usable by the *entire* voting population, regardless of age, infirmity, or disability. Providing accessibility to such a diverse population is an important engineering problem and one where, if other security is done well, electronic voting could be a great improvement over current paper systems. Flaws in any of these aspects of a voting system, however, can lead to indecisive or incorrect election results.

2.0 Objectives

This unit seeks to bring to the fore the importance of electronic system of voting in this century. Secondly it examines the relationship between e-voting and free election in advanced and developing nations.

3.0 Main body

3.1 Electronic Voting Systems.

E-Voting is a type of voting that includes the use of a computer rather than the traditional use of ballot at polling centres or by postal mail. It encompasses various types of voting: kiosks, the Internet, telephones, punch cards, and mark sense or optical scan ballots. All these types of E-Voting system have shown an accurate and speedy performance. Despite the advantages of E-voting, the range of its use worldwide is still, however, limited as it has a downside on many levels such as: legislative, social, political and technological levels (Watt, 2002). Management of risks: confirms the fact that the system is being tampered with. The implementation of the E-voting system raises several issues related directly to elections such as legal, social, technical, political, administrative and financial issues. However, Benefiting from the positive aspects of E-Voting requests the implementation of security measures in order to repair the lack of transparency and to regain the trust of electorates and liable Authorities (Watt, 2002; Xenakis and Macintosh, 2004). Due to some unforeseen cases, several elements should be held into account during the processing of the E-voting system:

A. Functionality: the voting process should be functional and simple since voters have little knowledge of the E-voting process. The E-voting system provides a unique interface that prohibits any attempt to tamper with the system itself.

B. Confidentiality: the voterôs ballot should be accurately and confidentially registered (Bederson et al., 2003). The confidentiality feature protects votersô choices in a way that it will be impossible to join a voting and a voter well to prove the voter's ballot.

C. Security: ballots should not be intercepted nor tempered with. The results should not be known until the official opening of the electronic urn. Only eligible voters whose names appear on the Voters List are entitled to vote and according to the law the voter has the right to vote one time. The system would consider invalid any ballot cast before the opening or after the closing of poll. In the past few years, especially after the year 2000, the advantages and the security risk of E-Voting have been at the core of several debates. A large number of publications detailed security risks and integrity related to E-Voting (Boutin, 2004).

Meanwhile, E-Voting remains unpopular and limited to few countries. The United States of America is considered the leading country in implementing E-Voting system (Paielli and Ossipoff, 1988). However, some E-Voting systems are complex leading to a lengthy voting process (Buck, 2004). In Europe, E-Voting was introduced to Belgiumôs elections November 24th 1991. Amongst provinces in Belgium, two were chosen to try the E-voting system. In 1999, the system was extended to 44% of the population. However, authorities still aim to achieve 100% coverage by 2006

elections (De Vuyst and Fairchild, 2005). Geneva had been using E-Voting ever since 2000 through the internet. However, E-Voting did not replace two other types of voting already in use there: postal and conventional voting. As for UKôs case, several pilot projects have been conducted in order to modernize the voting process. On May 2nd 2000, 16 UK Local Authorities carried out E-Voting and counting pilot schemes. 76 resorted to conventional paper ballots, 6 resorted to touch-screen voting kiosks, 5 resorted to internet, 3 resorted to the phone (touch tone) and 2 resorted to SMS text message. It has to be said that during UK Local elections on May 1st 2003, 20 E-Voting pilot projects got the approval. 8 Local Councils piloted E-counting of paper ballots while other Councils gave voters the chance to vote electronically through various channels: 8 offered Kiosk voting at polling centres or in public spaces, 14 offered Internet voting, 12 offered phone voting, 4 offered SMS voting, while 3 offered interactive digital television voting (Xenakis and Macintosh, 2005).

There have been several studies on using computer technologies to improve elections. These studies caution against the risks of moving too quickly to adopt electronic voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. As a result of the Florida 2000 presidential election, the inadequacies of widely-used punch card voting systems have become well understood by the general population. Despite the opposition of computer scientists, this has led to increasingly widespread adoption of ñdirect recording electronicò (DRE) voting systems. DRE systems, generally speaking, completely eliminate paper ballots from the voting process. As with traditional elections, voters go to their home precinct and prove that they are allowed to vote there, perhaps by presenting an ID card, although some states allow voters to cast votes without any identification at all. After this, the voter is typically given a PIN, a smartcard, or some other token that allows them to approach a voting terminal, enter the token, and then vote for their candidates of choice. When the voterôs selection is complete, DRE systems will typically present a summary of the voterôs selections, giving them a final chance to make changes. Subsequent to this, the ballot is ñcastò and the voter is free to leave.

The most fundamental problem with such a voting system is that the entire election hinges on the correctness, robustness, and security of the software within the voting terminal. Should that code have security relevant flaws, they might be exploitable either by unscrupulous voters or by malicious insiders. Such insiders include election officials, the developers of the voting system, and the developers of the embedded operating system on which the voting system runs. If any party introduces flaws into the voting system software or takes advantage of pre-existing flaws, then the results of the election cannot be assured to accurately reflect the votes legally cast by the voters. Although there has been cryptographic research on electronic voting, and there are new approaches, currently the most viable solution for securing electronic voting machines is to introduce a ñvoter-verifiable audit trailò. A DRE system with a printer attachment, or even a traditional optical scan system (e.g., one where a voter fills in a printed bubble next to their chosen candidates), will satisfy this requirement by having a piece of paper for voters to read and verify that their intent is correctly reflected. This paper is stored in ballot boxes and is considered to be the primary record of a voterôs intent. If, for some reasons, the printed paper has some kind of error, it is considered to be a ñspoiled ballotò and can be mechanically destroyed, giving the voter the chance to vote again. As a result, the correctness of any voting

software no longer matters; either a voting terminal prints correct ballots or it is taken out of service. If there is any discrepancy in the vote tally, the paper ballots will be available to be recounted, either mechanically or by hand. (A verifiable audit trail does not, by itself, address voter privacy concerns, ballot stuffing, or numerous other attacks on elections.)

3.2 Securing Electronic Votes: Free and Fair Elections

Security is a key factor in any election process. Every voter expects the vote he casts to be confidentially and correctly saved and counted. In order to maintain security, the main interface in the E-Voting system is designed in a full-screen view and cannot be closed or minimized. Voters are given a touch-screen with no keyboard. Each voting machine in every polling centre operates separately during the voting process. As for ballots, they are saved in a local database. As soon as poll closes, the Deputy Returning Officer in every polling centre counts ballots and reports results to the main server using a special interface and expect confirmation. Encrypted data is transmitted through a secure 128 bits modem-to-modem connection using the Communication Security Protocol (SSL 128). This Protocol allows a safe communication (modem-to-modem) between the authenticated client and the server. A hard copy of results from the polling centre is later delivered to Election Authority that gathers them through the main system in order to quickly deliver final results. For this, many government entities have adopted paperless ñCERTIFIEDò DRE systems without appearing to have critically questioned the security claims made by the systemsô vendors. Until recently, such systems have been dubiously ñcertifiedò for use without any public release of the analyses behind these certifications, much less any release of the source code that might allow independent third parties to perform their own analyses. Some vendors have claimed ñsecurity through obscurityò as a defence, despite the security communityôs universally held belief in the inadequacy of obscurity to provide meaningful protection.

One of the characteristics of advanced countries is the relatively high level of administrative competence, and that is probably the reason that social scientists, who study comparative democracies, have given so little attention to the conduct of elections. Most of the services that advanced countries provide their citizens are more complex than registering voters or conducting elections. Indeed, in most industrialised and few developing countries, people learn the results of elections from television projections not from votersô counts. Few citizens in advance countries even know the rules and procedures for counting, announcing and certifying the results because they take it for granted that it will be honest and impartial. In developing countries, the problem of conducting free and fair elections is compounded by the intensity of politicisation at an early stage in the democratisation process. The politicisation is different from what occurs in advanced democracies. Until two decades ago., the vast majority of the worlds rulers came to power by force of arms. The stakes involved in seizing power or losing it were so high that ambitious men did not hesitate to use whatever force they could muster. Elections are a more civilised way to choose leaders, but in a country with small but divided elite, the losers of an election may find themselves without alternative means of employment. The technical elements of conducting an election are also of a magnitude of difficulty as to overwhelm most poor countries. Contemplate the range of activities that need to be undertaken in a short time and often in a very tense politicised environment.

In Nigeria, State and national elections in 1999 and 2003 were marred by violence and widespread fraud. The results of the general elections held in 2003 in particular were deemed by domestic and international observers to be illegitimate in many areas. Nigeriaôs failures to hold genuinely democratic elections that afford citizens an opportunity to elect the candidates of their choice lies at the heart of many of the countryôs most pressing human rights problems. In this pre-election period, the Nigerian press has already recorded more than 50 incidents of election-related violence since November 2006, in which more than 50 people reportedly have lost their lives. The political system has often rewarded corrupt and abusive individuals with public office. This appears to encourage many politicians to view unlawful behaviour as a necessary component of electoral success. Many politicians hire political thugs to intimidate their opponents and their supporters, and generally enjoy impunity for such actions despite provisions in Nigeriaôs Electoral Law that specifically criminalize them. Free and fair elections in Nigeria depend upon an independent electoral commission. So far, in 2007, the independence of Nigeriaôs Independent National Electoral Commission is in doubt with serious questions and court challenges surrounding the governmentôs attempt to use INEC to disqualify several key opposition candidates, including the then vice-president (Alhaji Abubakar Atiku).

Human Rights Watch calls upon candidates to:
1. Commit to ensuring that the conduct of their own electoral campaigns is free from violence, intimidation, and other abuses;
2. Propose reforms that Nigeriaôs next government should undertake to make the political system more open, accountable, and respectful of human rights; one of such is the agitation for electronic voting.
3. Propose measures for the government to improve the enforcement of existing laws meant to hold to account individuals who attempt to manipulate the electoral process through violence and fraud, including provisions of the electoral law that criminalize conspiracy, bribery, and the use of thugs to intimidate voters; and
4. Explain what measures they would take to insulate Nigeriaôs Independent National Electoral Commission from political pressure.

Self Assessment Exercise
What is DRE System? Explain the relevance of the DRE system to political security and stability of developing nations?

4.0 Conclusion
Given the wide but thin character of contemporary democratic experiment using the e-voting system, perhaps the best way to prevent back-sliding or democratic experiment failure is by strengthening the institutions that ensure that the allocation of power reflects popular preferences. The boundary lies with policing in all democracies, but particularly in those that are still navigating difficult transitions.

5.0 Summary
The E-Voting system as described in this unit might be proposed as a voting system to be applied during elections. The system works virtually through interactive, efficient and easy-to-use graphical interface. An effective electronic voting system will certainly satisfy the above listed conditions: functionality, confidentiality and security

6.0 Tutor Marked Assignment

What is electronic voting? Discuss the factors hindering the implementation of e-voting in developing countries.

7.0 References/ Further Reading

(1) Bederson, B. Hersson, P. Neimi, R. Traugott, M. Conrad, F. (2003) "An Assessment of voting technology and ballot design" http://www.cs.umd.edu/~bederson/voting/nsf-project.shtml.

(2) Boutin, P. (2004) "Is E-Voting Safe?" PC World magazine, 6:1-6.

(3) Buck, F. (2004) "Looking past voting machines to voter interface" Facsnet Editor, http://www.facsnet.org/tools/law_gov/ elections.php3.

(4) California Internet Voting Task Force. *A Report on the Feasibility of Internet Voting*, Jan. (2000). http://www.ss.ca.gov/executive/ivote/.

(5) Chaum, D.. (2004). Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1):38ï 47.

(6) Dill, D. L., R. Mercuri, P. G. Neumann, and D. S. Wallach. (2003). *Frequently Asked Questions about DRE Voting Systems*, Feb.. http://www.verifiedvoting.org/drefaq.asp.

(7) Gritzalis, D. (2003). *Secure Electronic Voting*. Springer-Verlag, Berlin Germany.

(8) Mercuri, R. (2000). *Electronic Vote Tabulation Checks and Balances*. PhD thesis, University of Pennsylvania, Philadelphia, PA, Oct. 2000.

(9) Mercuri, R., Neumann, P.G (2003) "Verification for Electronic Balloting Systems" Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 31-42. Kluwer, Boston.

(10) National Science Foundation. *Report on the National Workshop on Internet Voting: (*2001). *Issues and Research Agenda*, Mar.. http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.

(11) NBS. Data encryption standard, January (1977). Federal Information Processing Standards Publication 46.

(12) Nechvatal, J. E; Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback. (2000). *Report on the Development of the Advanced Encryption Standard (AES)*, Oct.

(13) Paielli, R. Ossipoff, M. (1998) "General election in Santa Clara County, California in November. Available online" http://www.electionmethods.org.

(14) Pratchett, L. (2002) "The implementation of electronic voting in the UK" LGA Publications, the Local Government Association.

(15) RABA Innovative Solution Cell. (2004). *Trusted Agent Report: Diebold AccuVote-TS Voting System*, Jan. 2004. http://www.raba.com/press/TA_Report_AccuVote.pdf.

(16) Rubin. D. (2002). Security considerations for remote electronic voting. *Communications of the ACM*, 45(12):39ï 44, Dec. http://avirubin.com/e-voting.security.html.

(17) Watt, B. (2002) "Implementing Electronic Voting" A report addressing the legal issues by the implementation of electronic *Voting: What Is; What Could Be*, July (2001). http://www.vote.caltech.edu/Reports/.

(18) Xenakis, A. and Macintosh. A., (2004) "Procedural security in electronic voting" Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS 37), January 2004.

Unit 2
Security Analysis of Remote E-Voting

Content

1.0 Introduction

The Internet has transformed the way we live, interact, and carry out transactions. Traditionally, physical contact among parties in a business transaction was used to enhance trust. But in e-enabled service, trust is built based on algorithms that define authenticity of parties and maintain their confidentiality preferences as in the natural world. The advent of online shops like EBay, Google, and Yahoo, online educational programs, telemedicine among others have gone a long way in enforcing the belief that most human transactions can be carried out safely at the click of a button. Although the pioneers of online services have experienced problems as regards security, privacy, anonymity, and usability, the large amounts of transactions that are being carried online (worth about 100 billion dollars annually for e-commerce only) is a good indicator of how important the Internet is to the modern societies. To continue harnessing the possibilities that the Internet can offer to human societies, researchers have proposed a number of ways to implement online remote voting over the Internet so as to enhance democracy. It is through democracy that liberty and freedoms are entrenched in the human societies which are vital components of economic prosperity.

2.0 Objectives

In this unit, we analyze security considerations for a remote Internet voting system based on the system architecture of remote Internet voting. We examine whether it is feasible to successfully carry out remote electronic voting over the existing Internet infrastructure that conforms to the requirements of a public election process of integrity, anonymity, confidentiality, and intractability.

3.0 Main body

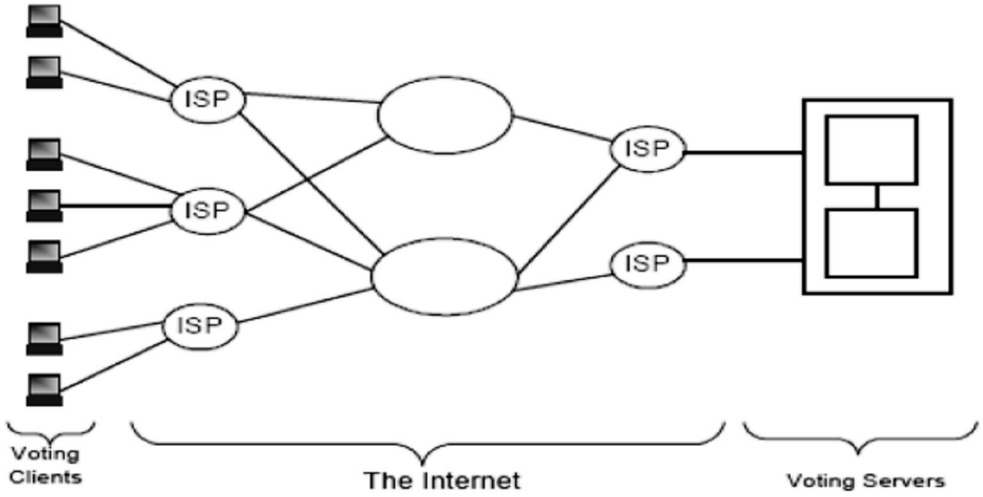
In this unit we use the phrase ñInternet votingò to refer to electronic voting (e-voting) over the Internet. Unlike traditional voting systems in which voter choices and intentions are represented in form of a paper ballot or other means like a punch card, Internet voting uses electronic ballots that are used to transmit votersô choices to electoral officials over the Internet. Internet voting can be categorized into three forms that are described below:

ÅPoll-site Internet voting; in this system, voters cast their ballots from a number of designated polling stations. The controlled physical environment at the polling site offers more possibilities of managing some security risks. Poll-site Internet voting offers more convenience and efficiency than traditional voting systems.

ÅKiosk Internet voting; is similar to poll-site, but voting machines are placed away from traditional voting locations and could be set up in convenient places like schools, libraries, and malls. Like poll-site voting, kiosk voting would make it possible to manage some security risks by controlling the physical environment.

ÅRemote Internet voting; this scheme allows voters to cast ballots from practically any where in the world as long as they have access to the Internet link. While this offers tremendous convenience, it also introduces several potential security risks because the physical voting environment is not controlled. Issues of intimidation, voter impersonation among others do arise. Figure 1 presents a generic remote Internet Voting architectural diagram.

Fig. 1: Internet Voting Architecture



3.1. Remote e-Voting System

Just like any other system, the remote e-voting system is made up of a number of components and has stringent requirements to meet. In the subsections below, we present the requirements and the building blocks of an e-voting system.

A. Requirements

Like the traditional voting system it ensures that only registered voters participate in the voting process, and that a voter can only cast one ballot, and that the vote is cast in privacy without unlawful influences and that the voting process is transparent to all interested parities. Remote e-voting systems are also expected to provide a platform of conducting a fair and transparent election.

1) Ease of use

For e-voting systems to gain acceptance, the systems should be user friendly, i.e., requiring less time to learn and operate. Users naturally desire a new system to be more user-friendly than the one being replaced. A system that is functionally sound

but with poor usability can be a cause of errors (on the voterôs side) during electoral process. Often times, system developers focus more on system functionalities and the expense of usability. This for an e-voting system could lead to low voter turnout and voters feel their time is precious to waste in learning a system that does not directly add value to their lives.

2) Authentication
Authentication is very important to maintaining overall security of the system. Strong authentication mechanisms have to be implemented to grant access to authorized users and to keep out intruders in order to maintain system accountability. Additionally, mutual authentication has to be provided to protect voters from providing their security credentials to rouge servers. Most of the cases in which phishing scams are successful occur because mutual authentication is not provided because users are not enabled to authenticate servers that they are connecting to.

3) Integrity
The integrity of votes cast and the entire voting system hardware and software should be maintained. The counting process of votes should produce reproducibly correct results. Integrity is an important requirement that requires servers and client computers being free of trapdoors and any other forms of internal threats that could cast doubt on the safety of the voting system.

4) Voter anonymity
Voters should be able to cast their votes without being traceable as is the case in traditional manual election process. The voting system should not link a cast vote to a voter. Failure of the voting system to provide anonymity would mean that interested parties could trace and know that someone did or did not vote for a given individual or policy. Such act would endanger the voters and compromise the fairness of the election results.

5) System accountability
The voting system should be transparent enough to allow accountability by interested parties in case of disputes. Accountability is important for defusing disputes regarding voter complains which could involve wrongly registered votes or incorrect tallying. An audit trail that does not link a voter to a cast vote is desirable in case one wishes to know if their vote was counted.

6) Confidentiality of the vote
The system should maintain the confidentiality of the votes during and after the voting process. This is very important to allay any fear of votes tampering.

B. System components
1) Voters
These are persons registered with the system, with the rights to participate in the election. They are a critical component of the remote e-voting system as most of the feasible security breach can occur at this level. Of course, these voters are expected to be humans who are registered and authorized to participate in the electoral process.

2) System administrators

These are persons with the authority to operate the voting system. System administrators undertake tasks of installation, upgrade and application of security patches and have privileges to access both physically and logically all components of the voting systems except client computers.

3) Client computers
These are end user terminals that are remotely connected to the voting servers over the Internet from which voters cast their votes. They run generic softwares and are highly vulnerable to logical attacks.

4) Network infrastructure
This is mainly comprised of communications media that connect the internet service providers (ISP) to the client computer, ISP gateways, interconnecting servers, layer three switches among others. The communications media consist of fiber networks, Ethernet cables, telephone lines, and wireless medium.

5) Voting server(s)
Voting servers are part of the Trusted Computing Base (TCB) of the voting system. A trusted computing base is that part of the system that is responsible for enforcing security policies they are strategically located in the system for faster access at low risk of compromise. Normally they are physically located in a secure environment at the election organizersô premises.

6) Voting protocol
The voting protocol is another key element in the system. The protocol governs the logic that handles security of the ballots, registration of users, authentication of participating parties, verification of votes cast and vote counting. We can as well say that the voting protocol is the heart of the voting system, without which all the designs are fruitless. The remote e-voting system requires a voting protocol that can guarantee confidentiality, integrity, and authenticity of the votes.

7) Voting System Software
This is a crucial component of the voting system that has the actual implementation of the voting protocol and services that are needed in the voting process. Apart from software that exists in the network devices like routers and switches, other software components on both the client and server side have to be customarily developed for the voting process. Usually, a large component of the voting system is executed from the server side and a thin client made available via network connections to clients. A secure communication between the client and server software is always expected to be provided to keep out adversaries.

3.2 Threat Analysis
In the following sections we present threats to the remote e-voting system. The threat can be categorized into: technical and social depending on the schemes of attacks and target components.

A. Trapdoors
This is a technical threat-software developers and system administrators usually create - accounts that are usually not known to normal system operators (trapdoors). These accounts are used for trouble shooting purpose and at times for achieving personal

goals. However, skilled hackers also obtain these accounts and even create other trapdoors which are more difficult to close or detect for their future use. Trapdoors can exist in any software that runs on a computing device. The software can be a web browser, web server, application server, word processor, a favorite screensaver among others.

B. Virus attacks Protection against virus attacks is not a trivial issue in a large election in which voters use their home computers to cast their votes. It is very hard to ensure that users do not have viruses on their computers that could do something unexpected in the polling day. Most of the attacks on computer vulnerabilities are very stealth and sophisticated for an average computer user to predict or detect. The most notable user exploits are those that attack email clients like Microsoft Outlook and Outlook Express. Some of these viruses donôt require the user to open an attachment or an email in order to infect his/her computer. In Outlook Express, a virus can activate even if the e-mail is only viewed through the Preview Panel. Attacks during a major election are expected to be more subtle than the more famous script kiddiesô attacks. Probably people who write script-kiddies maybe the ones involved for malicious intent. A nation wide election in any country is most likely to attract the attention of state enemies who may be willing to invest enough resources to employ highly skilled crackers to sabotage the voting process. This is a technical threat as well.

C. Phishing scams
Through social engineering and intimidation, eligible voters can be led into giving away their security credentials to criminals who might want to influence the outcome of the voting process. Some phishing scams deploy rogue websites that appear like genuine ones and are used by attackers to get credentials illegally from voters. This threat can be classified as either technical or social depending on the mechanism of attack used. When software is used to confuse the user into thinking that the presented interface is genuine, then a technical phishing scam is said to be used. On other hand, voters can be conned by individuals into giving away their voting credentials; in which case a social phishing scam is said to be used.

D. Compromise of voterôs privacy
System designs that keep audit trails of the voting process (that can later be used to link voters to their votes) are a source of compromise to voterôs privacy. If this is done, voters who are sensitive to their privacy can choose to abstain from the voting process for fear of their safety, hence influencing the electoral system.

E. Subverting System Accountability and Integrity
Though subverting system accountability is non-trivial for a well designed remote e-voting system, it still remains a threat especially from internal organizational administrators who may take advantage of their system privileges and tamper with audit trails of the system. An attack on system accountability could be launched from the client software, where by a supposedly cast vote is either dropped or registered with changed voter intention and then tallied on the server side in accordance to the desires of the intruder. Additionally, the tallying process on the server side of the voting system can also be tampered with to favour given subject or candidate.

F. Compromise of client computers
Current research has revealed that there are wider spread and reported vulnerabilities in Windows systems compared to other operating systems like UNIX, Linux, and MacOS. Almost all internet applications on Windows Operating System (OS) have at one time contained security vulnerability. The continued discovery of buffer overflows in several windows systems including most internet applications is quite a big problem. This causes a big threat to remote voting over the internet, since above 90% of internet users are running windows operating systems.

Most of these flaws are known to cracker communities and can be easily exploited in a public election to interfere with the voting process in various ways (DDOS being the most likely). Since most people use windows systems with popular applications like e-mail clients, chat tools, office suites, document views like Adobe and others, a group of people from these companies can easily install a backdoor or a Trojan-horse inform of an update which can go quite unnoticed to many people as illustrated by Ken Thompson. The effect of such subversion could render client computers unusable for a while during an election day, or redirecting them to dummy web server.

3.3 Analysis of Proposed Mitigation Schemes
In an effort to mitigate the above mentioned threats, researchers have proposed a number of mitigation controls and in the following paragraphs we summarize some.

A. Solution to mitigate authenticity
Researchers have suggested that physical and logical access to the voting systems should be based on credential and rights granted either on role based or need to know policy. Voters and administrators must gain access with nontrivial authentication mechanisms that may require use of smartcards for stronger security. However, some authentications schemes which offer a strong authentication require either a user to memorize complex credentials or they are technically expensive in monetary and privacy terms. This is because users may be required to buy end user authentication devices like cryptographic calculators and biometric readers; additionally, transfer of biometric data over public networks raises privacy concerns on the side of users.

B. Virus attacks
Research indicates that sensitizing users into knowing the dangers of keeping update versions of software and being careful on the type of software they install on their computers can tremendously reduce the risks. Though most antivirus software is commercial, there are also non commercial versions of software that voters could use before a voting process to ensure that their computers are free of viruses. However, these problems cannot be easily solved for all client computers participating in an election where people are voting from their homes.

C. Solution to Phishing Scams
Social phishing scams can be prevented by educating people with detailed information of various means through which they (voters) can be exploited. However, this requires that the educators themselves keep updated with current methods of exploitation. Otherwise, the taught methods of attack and defense for the voters could be out dated and could still leave the voters vulnerable to social phishing scams. More importantly, technical phishing scams are more dangerous than social ones, since their effect can be easily wide spread in an election process. However, the solution equally

solves the problem on a wide scale. Strong authentication is required in the voting system by means of mutual authentication. Mutual authentication schemes require the clients to be authenticated to the server software, and the server software also authenticated to the client. In that way, voters are protected from technical phishing scams.

D. Solution to integrity threats
System changes must be prohibited throughout the active stages of the election process. Voting systems need to be verified by independent non partisan bodies that will look at the source code and verify that it does exactly what it was designed to do. The use of cryptography exchange of messages can guarantee integrity of information exchange. The requirements of vote secrecy and voter anonymity has not been a problem in itself, but achieving both of them (secrecy and voter anonymity) at the same time has been a problem to vote accountability and dispute resolution after voting process.

E. Subverting system accountability (voting server)
Although in some literature, researchers have advocated for use of encryption and checksums on audit trails to help in detecting changes to file system audit trails, additional use of audited open systems code on the server environment can also minimize the risks of running source code with undesirable side effects.

F. Network infrastructure
Through redundancy, use of cryptograph, and the concept of honey spots, attacks on network infrastructure can be minimized. However, we note that it is fairly difficult to prevent some attacks along the communication channels like Denial of service (DDOS).

G. Legal Protection
Attacks on mission critical systems in countries like the USA, UK and Brazil are being handled as criminal cases for which culprits have to be prosecuted. The act of hackers/crackers gaining unauthorized access to computer system can be compared to someone breaking into a house as a means of checking whether it is secure. Microsoft is also putting a lead in this pursuit with over 100 law suits outside the USA and it serves to protect electronic systems in the same way the law protects houses from bugler attacks. Without legal prosecution, then many attacks on systems will continue to be tried out and eventually some will succeed. This behaviour has to be controlled legally, so that security checks can only be done by legally accepted organizations such as certified security organizations, but not any underground team of hackers who might have malicious and personal goals. Of course some sophisticated attacks can go unnoticed and other non-traceable attackers could launch successful attacks without being punished for their wrong doings. This is why security of a system cannot be left to legal protection and prosecution alone. System stake owners need to do all they can to keep the voting system technically sound.

H. Open Source Systems in Electronic voting
In literature, a concept of using open source systems for e-voting has been proposed. The debate rages on whether it is a good idea to have open source systems powering electronic voting over the Internet or not? The question of whether open source systems can be trusted more than closed source systems still stands? Ken Thompson

in his paper entitled ñReflections on Trusting Trustò indicates you cannot trust a code that you did not totally create yourself. The paper by Ken presents an ingenious piece of code which can be used to create another program from itself in a way that is not easy to detect by non sharp-eyed programmer. Software written in a similar comportment can be used to introduce trap and back doors in an application.

The question of trust cannot certainly be left unanswered for an important democratic exercise like voting. People need be assured that there are no uncertainties regarding security for the systems that has been deployed. Experience from exposed vulnerabilities in closed source system has shown that closed systems cannot be thought of as being more secure than open systems. The most common example is of windows operating systems, where much vulnerability have been uncovered by independent security experts working without access to the source code. This is not to suggest that open source systems are bullet proof, it rather shows that vulnerabilities can be uncovered or even easily exploited in closed systems. Bruce Schneider, author of Practical Cryptography and one of the foremost experts on cryptography explains in his article on voting systems, that security is almost always in the details of the rest of the system; where by a secure system is only as strong as its weakest link. The biggest weakness of these companies (that keep closed source) is the need to keep the source code secure in order to keep the system secure. The analysis provides an example of how vulnerabilities can be discovered in source code by someone who is not the author of that source code. In the analysis done in February 2004, on AccuVote- TS electronic voting system, lots of problems, including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes were identified. It was also discovered in the analysis done on AccuVote-TS voting system that without any insider privileges, voters could cast an unlimited number of votes without being detected by any mechanism within the voting terminal software. In the AccuVote-TS systems, smartcards were not performing any cryptographic operations, giving way for forged smartcards to authenticate themselves. The system was found to be so insecure that even ballot definitions could be changed and even voting results modified by persons with forged credentials. It is noted that most developers may know what is required to be done, but because of project time demands and sometimes because they do not have many people watching what type of code they are writing, many of them end up coding in undesirable styles leaving behind undocumented features. Open source developers are always aware that many people will be reviewing their code so developers do their best to have the best output.

5. Analysis Summary

Our study of remote e-voting has revealed quite a number of important critical issues that are summarized in this section. A trusted computing base (TCB) is a primary requirement for secure electronic voting over the Internet but building one is one fundamental challenge researchers are still facing. Internet voting system cannot guarantee security to users voting from their computers operating in an insecure environment. The presence of viruses, untrusted user computer applications from various vendors and phishing scams, renders client computers vulnerable to thousands of attacks. More expensive measures can be taken by providing voters with cryptographic calculators and smart cards to provide an improved security to the client side of the TCB. However, problems concerning more subtle attacks like Distributed Denial of service (DOS) attacks do not have a solid solution yet. Also,

fundamental and original design flaws in Internet protocols can create an open door for quite a large number of security exploits. DNS spoofing is a security threat that involves voters being redirected to a different server from a genuine one. This attack can have several impacts on the results of an election. Voters could be made to think that they are voting for the correct person among the candidates, yet they are voting for a dummy candidate. DNS spoofing that targets demographics that are known to vote for a particular party or candidate can negatively impact on the results of their total votes. Buffer overflows can be exploited in poorly designed systems to alter the trend of the election. The ability for DDOS attack to be launched for a particular domain name can end the whole story of a voting process in quite a short time. Apparently the current implementation of raw sockets in windows XP has simple opened gates of possibilities for DDOS attacks. The experiences in 2003 of SCO going offline due to DDOS showed the world that more very sophisticated attacks that are not easy to filter can actually bring down a targeted network.

Trust is still a very big problem in electronic voting software. Apart from trusting electronic voting software, the compilers that were used for these programs/systems also need to be trusted. Presence of a Trojan-horse in widely deployed systems can alter results of an election in favour of some candidates. Open source systems and public scrutiny of source code will help in buying votersô trust in electronic systems. Using of security independent bodies like universities and accredited security organizations to perform source code analysis for vulnerabilities will enhance the quality of source code for mission critical systems. Most of the vulnerabilities in software also arise from poor programming principles which are rather difficult to completely eliminate for programming languages like C and C++. Using a type safe language like Java helps in avoiding buffer overflows that are common in C and C++ programming languages. As indicated in the software evaluation report by Kohno et al. (2004); the choice of a programming language can either lead to an increase or decrease of vulnerabilities in a system. It is easier to unknowingly introduce a bug in a C or C++ program that could be easily exploited with a buffer overflow as compare to Java or a safe dialect of C like Cyclone. Possibilities of coercing voters into choosing different candidates, most especially on Election Day is a big problem to remote e-voting. Additional issues of votersô coercion, vote selling, vote solicitations have put remote e-voting into question, since these problems do not have solid solutions. As much as security and technological details of Internet voting systems can be perfected to an appreciable degree, there is no clear solution as far as we know regarding vote selling if people are allowed to vote from home, or even coercion of a voter into choosing a candidate against oneôs choice. In order to ensure voter trust and legitimacy of election results, all levels of Internet voting process must be observable. Because fair elections and elections perceived to be fair, are important targets in any voting system. The use of open source systems can help in buying trust of citizens; since code reviewed publicly will most likely not have unfair operations.

Self Assessment Exercise
Explain the concept of trust and security in e-voting.

4.0 Conclusion
This unit has revealed that, public analysis of systems improves security and increases public confidence in the voting process. If the software is public, no one can insinuate that the voting system has unfairness built into the code. Proliferation of similarly

programmed electronic voting systems can escalate further large scale manipulation of votes. It is very hard to guarantee security of a remote e-voting system, in an environment that cannot be explicitly controlled by the voting regulatory body. All technologies are useful only if they are used in the right way. In the AccuVote-TS voting system provides a clue of how a poor usage of cryptography rendered a supposedly secure system to be flawed. Open source systems and peer reviews can help solve the problem. Independent bodies study and evaluate systems for errors, security and design flaws. The technological advancements of e-commerce services that were never expected to be an on-line success, is a good indicator that in future we may have trusted remote voting systems. Using experimental prototypes in small election cycles will help in preparing e-voting for large scale public elections. The challenges that face Internet voting systems are not quite severe to prevent them from being used. Just like any other systems - even manual ones - that may have weakness and problems that need to be solved, Internet voting provides lots of more flexibility as compare to traditional methods of voting. The infrastructure is also relatively cheaper to maintain, considering that it is built upon existing systems that are used in everyday life of voters. A desirable voting system should be accessible to all potential voters. In some societies like in the developing countries, not all voters have access to a computer and Internet. In fact a good number of them do not have knowledge of computer usage and the Internet. In such cases, the Internet can be used as an option to improve voterôs turnout. However, if the election is only facilitated by Internet voting, then the technology would end up becoming a barrier to voter participation.

5.0 Summary

The voters can cast their ballots using client computers that are connected to the Internet through Internet Service Providers (ISP) that link the client computers to voting servers. This unit focuses on the challenges of implementing a viable remote e-voting system. We discussed the different threats this system faces to deliver a credible election result and the current approaches to mitigate these threats. We presented the limitations to the proposed mitigation and propose improvements on these schemes. Discussed also, was the cost benefit analysis of e-election and conclusion with future research directions in e-voting systems.

6.0 Tutor Marked Assignment

The remote e-voting system is made up of a number of components and has stringent requirements to meet. Discuss

7.0 References/ Further Reading

(1) Caida. Code red. http://www.caida.org/analysis/security/code-red/. Accessed on August 10th, 2006 Caida. Denial of Service Attack on SCO. http://www.caida.org/analysis/security/sco-dos/.

(2) Hollinger, R.C. and Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. Criminology, 26(1):101ï 126.

(3) Jefferson D., A.D. Rubin, B. Simons, and D. Wagner. (2004). Analyzing internet voting security. Communications of the ACM, 47(10):59ï 64.

(4) Jefferson, D., Rubin, A.D., Simons, B. and Wagner, D. A (2006). Security Analysis of the Secure Electronic Registration and Voting Experiment

(SERVE), New York Times (http://www. servesecurityreport. Org, accessed on December 19th.

(5) Jim T., G. Morrisett, D. Grossman, M. Hicks, J. Cheney, and Y. Wang. (2002). Cyclone: A safe dialect of C. USENIX Annual Technical Conference, pages 275ï 288.

(6) Kohno T., A. Stubblefield, AD Rubin, DS Wallach, and UC San Diego. (2004). Analysis of an electronic voting system. Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pages 27ï 40.

(7) Marc Friedenberg, Ben Heller, Ward McCracken, and Tim Schultz. (2007). ñEvoting System Requirements: An Analysis at the legal, Ethical, Security, and Usability levelsò www.marcfriedenberg.com/wp-content/evoting.pdf Accessed on Feb 16th,

(8) National Science Foundation, (2006). USA. Internet Voting is no òMagic Ballot,ò Distinguished Committee Reports. http://www.nsf.gov/od/lpa/news/press/01/pr0118.htm, 2001. accessed on August 12th.

(9) Neumann P.G. (1993). Security criteria for electronic voting. 16th National Computer Security Conference.

(10) Puigserver, MM, Gomila, JLF, and Rotger, LH. (2004). A Voting System with Trusted Verifiable Services. Lecture Notes in Computer Science, pages 924ï 937.

(11) Rubin A. (2002).Security Considerations for Remote Electronic Voting over the Internet. Comm. Of ACM, 45:12.

(12) Sun, H.M , (2000) An efficient remote use authentication scheme using smart cards,, IEEE Transactions on Consumer Electronic Vol 46/4, pg 858ð 961.

(13) Tavani H.T. (2000). Defining the boundaries of computer crime: piracy, breakings, and sabotage in cyberspace. ACM SIGCAS Computers and Society, 30(3):3ï 9.

UNIT 3

THE SECURITY OF ELECTRONIC BANKING

Content

1.0 Introduction

The Internet has played a key role in changing how we interact with other people and how we do business today. As a result of the Internet, electronic commerce has emerged, allowing businesses to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers effectively is the banking industry. The electronic banking system addresses several emerging trends: customersô demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are the concerns of security and privacy of information.

2.0 Objectives

This section discusses the motivations and ventures in Electronic Banking. Second, it addresses the disastrous ventures in Electronic Banking with an example. It looks into the concerns about Electronic Banking from various perspectives as well as germane security issues and attacks.

3.0 Main body

3.1 The Security of Electronic Banking

In todayôs highly technological world, the machine that destroys paper money and converts it into electronic money is far from reality. But the part on the person interacting with his or her banking account late at night is becoming more of a reality. The information superhighway has found its way into many homes, schools, businesses, and institutions. Many people are cruising the Internet each day to obtain information on the weather, latest sport scores, local news, and many other exciting information. These people also buy and sell goods on this new media. Consequently, many businesses are reaching out to customers worldwide using the Internet as its communication channel. This new electronic media of interaction has grown to be known as the electronic commerce. ñElectronic Commerce integrates communications, data management, and security services, to allow business applications within different organizations to automatically interchange information.ò

Consequently, electronic commerce is comprised of interconnected communications networks; advanced computer hardware and software tools and services; established business transaction, data exchange, and interoperability standards; accepted security and privacy provisions; and suitable managerial and cultural practices. This infrastructure will facilitate diverse and distributed companies nationwide to rapidly, flexibly, and securely exchange information to drive their business processes. The banking industries is one such business that is using this new communication media to offer its customer value added service and convenience. This system of interaction between the consumers and the banking industries is call the electronic banking system. ñElectronic banking is the use of a computer to retrieve and process banking data (statements, transaction details, etc.), and to initiate transactions directly with a bank or other financial services provider remotely via a telecommunications networkò (www.electrobank.com/ebaeb.htm). Electronic banking is a new industry which allows people to interact with their bank accounts via the Internet from virtually anywhere in the world. The electronic banking system addresses several emerging trends: customer demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. This system allows consumers to access their bank accounts, review most recent transactions, request a current statement, transfer funds, view current bank rates and product information and reorder checks. The electronic banking system can be seen as an ñextension of existing banks.ò Banks cater for a very large population of Internet users. Heidi Goff, Senior Vice President for Global Point of Interaction of Mastercard, estimated that there will be more than 200 million users by the year 2010. Many other estimates conclude similar results, which lead to the indication that the Internet will play a major role in everyoneôs life and promote the electronic banking industry.

3.2 Motivations of Electronic Banking

The Internet is growing at an exponential rate. According to a survey, the Internet has doubled its size from 6.6 million hosts in the mid 1995 to 12.8 million hosts in mid 1996. As a consequence of the popularity of the Internet, hundreds of thousands of Internet users are trying electronic banking. As the Internet continues to expand, the convenience associated with electronic banking will attract more customers. One expectation of electronic banking is that it will replace the need for writing cheques. In todayôs market, ñAccording to preliminary data from the latest Federal Reserve survey of patterns of consumer spending, almost four-fifths of consumer expenditures are handled by checks, directly or indirectly. This means that electronic banking has a very large potential for use since many people expect that electronic checks will substitute paper checks. Moreover, for consumers, electronic money (electronic cash and electronic checks) means greater efficiency than using coins, paper bills, and traditional banks. The electronic banking system brings the convenience of 24-hour, seven days a week, banking by offering home PCs tied directly to a bankôs computers. In addition, electronic money also offers greater security than a paper-and-coin system. Users are able to make a backup copy of their funds and if the electronic money is stolen, the users can invalidate the serial number just as they now stop payment on a paper check.

a. Ventures in Electronic Banking

i. Domestic

In order for this industry to expand further, secure transactions with the trust of the consumers are necessary. Many banks are advertising secure on-line service, allowing their customers a wide range of activities that they can do. Security First Network Bank is the first federally approved on-line bank that is certified by the Office of Thrift Supervision, the federal regulatory body for the saving bank industry. With the support of the federal agencies, Security First Network Bank can give their customers more than just their assurance, but the assurance of the government, which gives consumers a large incentive to try electronic banking. For a truly convenient system, banks need to connect to customers as well as to other financial institutions. Creating a common link between multiple banks so that banks can better and more safely communicate amongst themselves is becoming more of a reality. Fifteen of North Americaôs leading banks and IBM are working together to form an integrated network called Integrion Financial Network. The banks will be able to offer their customers access to their services through the public Internet and parallel private network access, with security and privacy.

ii. International

In Europe, the Inter-bank Standards Association Belgium has established the Belgiumôs electronic banking system to connect Belgiumôs three largest banks together to develop uniform standards for electronic payments in Belgium. This system, developed by Utimaco uses electronic signatures according to the RSA method to guarantee accountability and security against the forging of electronic transaction. Internationally, GENDEX Bank International is trying to connect the banking systems of various nations, states, independent principalities, and sovereign individuals to form an international banking system. This integration of electronic banking communities will promote the standardization of the industry. However, the primary concern today is the security issue which is also affecting most developing nations adopting similar patterns.

iii. Disastrous Ventures in Electronic Banking

In August of 1995, Citibank had problems with outsiders breaking into their system. A $10 million computer fraud against Citibank was the first successful penetration by a hacker into the system which transferred trillions of dollars a day around the world. Of the $10 million dollars illegally transferred, $400,000 were not found. Many banking experts predicted that these break-ins were bound to occur with banking business being done electronically at a time when more sophisticated personal computers are available. Since this break-in, Citibank has required its customers to use an electronic device that creates a new password for every transfer.

b. Important Concerns About Electronic Banking

Since Electronic Banking is a new technology that has many capabilities and also many potential problems, users are hesitant to use the system. The use of Electronic Banking has brought many concerns from different perspectives: government, businesses, banks, individuals and technology.

1. Government: From the government point of view, the Electronic Banking system poses a threat to the Antitrust laws. Electronic Banking also arouse concerns about the reserve requirements of banks, deposit insurance and the consumer protection laws

associated with electronic transfer of money. The US government is concerned with the use of high quality of encryption algorithms because encryption algorithms are a controlled military technology.

2. Businesses: Businesses also raise concerns about this new media of interaction. Since most large transfer of money are done by businesses, these businesses are concerned about the security of their money. At the same time, these businesses also consider the potential savings in time and financial charges (making cash deposits and withdrawals which some banks charge money for these processes) associated with this system. Another businesses concern is connected to the customer. Businesses ponder the thought that there are enough potential customers who would not make a purchase because the business did not offer a particular payment system (e.g. electronic cash and electronic check). This would result in a loss of sales. On the other side of the coin, if this system becomes wide spread, this would allow more buying power to the consumer which puts pressure on businesses to allow consumers to use electronic transfer of money.

3. Banks: Banks are pressured from other financial institutions to provide a wide range of financial services to their customers. Banks also profit from handling financial transactions, both by charging fees to one or more participants in a transaction and by investing the funds they hold between the time of deposit and the time of withdrawal, also known as the ñspreadò. With more financial transactions being processed by their central computer systems, banks are also concern about the security of their system.

4. Individuals: Individuals are mainly concerned with the security of the system, in particular with the unwarranted access to their accounts. In addition, individuals are also concerned with the secrecy of their personal information. 82% of American poled expressed concern over privacy of computerized data. As more and more people are exposed to the information superhighway, privacy of information and the security that goes hand in hand with this information is crucial to the growth of electronic transactions. Some privacy technologies related to the electronic banking industry are electronic cash and electronic checks which will be discussed in the software solution section. In order to provide effective and secure banking transactions, there are four technology issues needed to be resolved. The key areas are:

a. Security
Security of the transactions is the primary concern of the Internet-based industries. The lack of security may result in serious damages such as the example of Citibank illustrated in the earlier section. The security issue will be further discussed in the next section along with the possible attacks due to the insufficient protections. The examples of potential hazards of the electronic banking system are during on-line transactions, transferring funds, and minting electric currency, etc.

b. **Anonymity (Privacy)**
Generally speaking, the privacy issue is a subset of the security issue and thus will be discussed in the Privacy Technology section later. By strengthening the privacy technology, this will ensure the secrecy of senderôs personal information and further enhance the security of the transactions. The examples of the private information

relating to the banking industry are: the amount of the transaction, the date and time of the transaction, and the name of the merchant where the transaction is taking place.

c. Authentication

Encryption may help make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction. There are two possible ways to verify the integrity of the message. One form of verification is the secure Hash algorithm which is ña check that protects data against most modification.ò The sender transmits the Hash algorithm generated data. The recipient performs the same calculation and compares the two to make sure everything arrived correctly. If the two results are different, a change has occurred in the message. The other form of verification is through a third party called Certification Authority (CA) with the trust of both the sender and the receiver to verify that the electronic currency or the digital signature that they received is real.

d. Divisibility

Electronic money may be divisible into different units of currency, similar to real money. For example, electronic money needs to account for pennies and nickels.

Security Issue

Quoting the CEO of DigiCash, Dr. David Chaum, ñSecurity is simply the protection of interests. People want to protect their own money, and banks their own exposure. The role of government is to maintain the integrity of and confidence in the whole system. With electronic cash, just as with paper cash today, it will be the responsibility of government to protect against systemic risk. This is a serious role that cannot be left to the micro-economic interests of commercial organizations.ò The security of information may be one of the biggest concerns to the Internet users. For electronic banking users who most likely connect to the Internet via dial-up modem, is faced with a smaller risk of someone breaking into their computers. Only organizations such as banks with dedicated Internet connections face the risk of someone from the Internet gaining unauthorized access to their computer or network. However, the electronic banking system users still face the security risks with unauthorized access into their banking accounts. Moreover, the electronic banking system users are also concerned about non-repudiability which requires a reliable identification of both the sender and the receiver of on-line transactions. Non-secure electronic transaction can be altered to change the apparent sender. Therefore, it is extremely important to build in non-repudiability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates.

Attacks

The Citibank $10 million break-in is one example of how the system is vulnerable to hackers. Hackers have many different ways that they can try to break into the system. The problem of the systems today are inherent within the setup of the communications and also within the computers itself. The current focus of security is on session-layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over untrusted channels, and a trusted code at both endpoints. It is really important to have a secure protocol because the *trusted channels* really donôt exist in most of the environment. For example, downloading a game off the Internet would be dangerous because Trojan

horses and viruses could patch the client software after it is on the local disk, especially on systems like windows 95 which does not provide access control for files. This leads to the use of software-based protections and hardware-based protections. Many systems today use some form of software-based protection. Software-based protections are easily obtained at lower costs than hardware-based protections. Consequently, software-based protection is more widely used. But, software-based protection has many potential hazards. For software-based systems, there are four ways to penetrate the system. First of all, attacking the encryption algorithms is one possible approach. This form of attack would require much time and effort to be invested to break in. A more direct approach would be using brute force by actually trying out all possible combinations to find the password. A third possible form of attack is to the bankôs server which is highly unlikely because these systems are very sophisticated. This leaves the fourth possible method, which also happens to be the most likely attack, which is to attack the clientôs personal computers. This can be done by a number of ways, such as planting viruses (e.g. Trojan Horse) as mentioned above. But, unlike the traditional viruses, the new viruses will aim to have no visible effects on the system, thus making them more difficult to detect and easy to spread unintentionally. Many problems concerning the security of transactions are the result of unprotected information being sent between clients and servers. In systems such as NFS, AFS, and Windows NT, there is no authentication of file contents when sent between the client and server. In these systems, file contents read from the servers are not authenticated in any secure fashion. Consequently, the client does not have any mechanism to determine if the bytes are indeed being sent by the server and not from a hackerôs program. Given this information, one possible scenario of attack is presented as follows:

> The attacker is assumed to have network access to any machine on any Ethernet sub-net between the file/server and the clients under attack. In under a day, a software package could be designed to exploit the lack of authentication in the NFS security product to patch the object code of any executable on-the-wire as it travels between the NFS server and the client machine. When the client retrieves data from the NFS server, it sends a short request message detailing which block from the file it is interested in. The attack software is located on an Ethernet segment between the client and the NFS server, so it is able to sense this traffic. The attack software waits for any request for a particular block of a particular executable such as the block containing the session key generation code in the Netscape executable. The software then is able to forge a reply from the NFS server and transmit it to the client. If the forged packet reaches the client before the real reply, it is accepted and the real reply is discarded as a duplicate. The forged reply generally reaches the client before the real reply. Given this ability, hackers could locate the code that select the session key within Netscape. Then they can patch only bytes into the code which causes the selection of a predictable session key every time the browser engages in the SSL (Secure Socket Layer) protocol. With this, hackers are able to decrypt all traffic from the browser to secure servers, obtaining information on credit card numbers

or other private information. Credit card numbers are especially easy to recognized since they are grouped in 16 digits that have a distinct mathematical relationship.

Self Assessment Exercise

Examine some of the discussed concerns In electronic banking

4.0 Conclusion

The Internet has grown exponentially, with more than 100 million users worldwide currently. The Internet enhances the interaction between two businesses as well as between individuals and businesses. As a result of the growth of the Internet, electronic commerce has emerged and offered tremendous market potential for todayôs businesses. One industry that benefits from this new communication channel is the banking industry. Electronic banking is offering its customers with a wide range of services: Customers are able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time restrictions. Electronic Banking is offered by many banking institutions due to pressures from competitions. To add further convenience to the customers, many banking institutions are working together to form an integrated system. On the other hand, this has not been readily accepted by its users due to the concerns raised by various groups, especially in the areas of security and privacy. Moreover, there are many potential problems associated with this young industry due to imperfection of the security methods.

5.0 Summary

The Internet has played a key role in changing how we interact with other people and how we do business today. As a result of the Internet, electronic commerce has emerged, allowing businesses to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The electronic banking system addresses several emerging trends: customersô demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are the concerns of security and privacy of information. The current focus of security of information transfer is on the session layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over un-trusted channels and a trusted code at both endpoints.

6.0 Tutor Marked Assignment

Explain how hackers are able to decrypt all traffic from the browser to secure servers, obtaining information on credit card numbers or other private information.

7.0 References/ Further Reading

(1) Chaum, David.(1997). Scientific Banking in American. August. Pp.137-42.

(2) Internet Security. Http://cfn.cs.dal.ca/Education/CGA/netsec.html retrieved 17/04/07.

(3) Introduction to PGP. Http://sun1.bham.ac.uk/N.M.Queen/pgp/pgp.html retrieved 10/08/09.

(4) Off the Charts The Internet 1996. Http://www.iw.com/1996/12/charts.html. PC Banking Services Spread, but Success is Still Uncertain. http://conceptone.com:80/netnews/nn942.htm

(5) Pfleeger, Charles P. (1997). Government. Emerging electronic methods for making retail payments. June 1996. Security in Computing. Prentice Hall.

(6) Security Comes First With Online Banking at Security First Network Bank. http://www.hp.com/ibpprogs/gsy/advantage/june96/custspot.html.. Retrieved 04/04/10

(7) UNIT 4

Security Solutions to Electronic Banking

Content

1.0 Introduction

In software-based security systems, the coding and decoding of information is done using specialized security software. Due to the easy portability and ease of distribution through networks, software-based systems are more abundant in the market. Encryption is the main method used in these software-based security systems. Encryption is a process that modifies information in a way that makes it unreadable until the exact same process is reversed. In general, there are two types of encryption. The first one is the conventional encryption schemes, one key is used by two parties to both encrypt and decrypt the information. Once the secret key is entered, the information looks like a meaningless jumble of random characters. The file can only be viewed once it has been decrypted using the exact same key. The second type of encryption is known as public key encryption. In this method, there are two different keys held by the user: a public key and a private key. These two keys are not interchangeable but they are complementary to each other, meaning that they exist in pairs. Therefore, the public keys can be made public knowledge, and posted in a database somewhere. Anyone who wants to send a message to a person can encrypt the message with the recipient public key and this message can only be decrypted with the complementary private key. Thus, nobody but the intended receiver can decrypt the message. The private key remains on oneôs personal computer and cannot be transferred via the Internet. This key is encrypted to protect it from hackers breaking into the personal computer.

2.0. Objectives

This unit examines some solutions on how best to tackle the numerous problems hindering electronic banking system worldwide.

3.0. Main Body

3.1 Security Solution: Current Encryption Technology

There are four examples of current encryption technology presented below: Digital Signature, Secure Electronic Transaction, Pretty Good Privacy, and Kerberos.

1. Digital Signature

Digital Signature was first proposed in 1976 by Whitfield Duffie, at Stanford University. A digital signature transforms the message that is signed so that anyone

who reads it can know who sent it. The use of digital signatures employs a secret key (private key) used to sign messages and a public key to verify them. The message encrypted by the private key can only be verified by the public key. It would be impossible for any one but the sender to have created the signature, since he or she is the only person with the access to the private key necessary to create the signature. In addition, it is possible to apply a digital signature to a message without encrypting it. This is usually done when the information in the message is not critical. In addition, this allows people to know who compose the message. Because the signature contains information so called ñone-way hashò, it is impossible to forge a signature by copying the signature block to another message. Therefore, it is guaranteed that the signature is original. One example of the use of digital signature in the electronic banking industry is by First Digital Bank in America. The First Digital Bank offers electronic bank notes: messages signed using a particular private key to provide unforgettable credentials and other services such as an electronic replacement for cash. ñAll messages bearing one key might be worth a dollar, all those bearing a different key five dollars, and so on for whatever denominations were needed. These electronic bank notes could be authenticated using the corresponding public key which the bank has made a matter of record. First Digital Bank would also make public a key to authenticate electronic documents sent from the bank to its customers.ò (Chaum 1992)

2. Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) software system is the global standard for secure card payments on the Internet, which is defined by various international companies such as Visa MasterCard, IBM, Microsoft, Netscape Communications Corp., GTE, SAIC, Terisa Systems and Verisign. SET promises to secure bank-card transactions online. Lockhart, CEO of MasterCard said, ñ We are glad to work with Visa and all of the technology partners to craft SET. This action means that consumers will be able to use their bank cards to conduct transactions in cyberspace as securely and easily as they use cards in retail stores todayò (Http://www.cnnfn.com/news/9602/01/visa.mastercard/index.html). SET adopts RSA public key encryption to ensure message confidentiality. **RSA is** An encryption mechanism by RSA Data Security that uses both a private and a public key. RSA is also used for authentication. Moreover, this system uses a unique public/private key pair to create the digital signature. The main concerns for the transaction include not only to ensure the privacy of data in transit, but also to prove the authenticity which both the sender and the receiver are the ones they claim to be.

Digital signature is used to achieve the authenticity. A digital signature is produced by first running the message through a hashing algorithm to come up with the message digest. Next, by encrypting the message digest with senderôs private key, this would uniquely identify the sender of the message. When receiving the message, the receiver decrypts the encrypted message with senderôs public key. This ensures that the message was actually from the appropriate person. Besides uniquely identifying the sender, the digital signature also ensures that the original message was not tampered with in transit. The receiver can use the original hashing algorithm to create a new message digest after decrypting the message and compare the new message digest to the original digest. If they match each other, it can be sure that the message has not been altered in transit. Although the public key encryption and the digital signature ensures the confidentiality and the authenticity of the message, a potential danger exists in that the information the sender provides may not be real. For example, the

sender may encrypt a bank card number which belongs to someone else by using his/her own private key. To ensure the true authentication, there is a need for a process of certification. A third party who is trusted by both the sender and the receiver will issue the key pair to the user who provides sufficient proof that he is who he claims to be. One assumption lies in the receiverôs trust that the CAôs own key pairs, which are used in the certification process, have not been compromised. ñAssuming SET will impact the deployment of RSA encryption for home banking and bill payment services online, one might wonder whether the banking industry should just adopt SET for other non-credit card transactions, as well. A senior banking executive at a major US bank contends that SET has the capability to allow payments that are not card-based. The processes in SET are not specific to card transactions. They are generic: authentication, certification, encryption and so on.ò (Http://www.rsa.com/set/bankset.htm)

3. Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP), created by Philip Zimmermann, is a ñhybrid cryptosystem that combines a public key (asymmetric) algorithm, with a conventional private key (symmetric) algorithm to give encryption combining the speed of conventional cryptography with the considerable advantages of public key cryptographyò (http://rschp2.anu.edu.au:8080/howpgp.html). The advantage of PGP is that it does not require a trusted channel of transmitting the encryption key to the intended recipient of your message. Furthermore, it has the ability to sign the messages by encrypting them with senderôs private key which can not be replaced by any other key. Once the receiver received the message, he/she can then decrypt the message with the senderôs public key which can not be forged and represents the true identity of the sender.

4. Kerberos

Kerberos is named after the three-headed watchdog of Greek mythology and it is one of the best known private-key encryption technologies. Kerberos creates an encrypted data packet, called a ticket, which securely identifies the user. To make a transaction, one generates the ticket during a series of coded messages by making exchanges with a Kerberos server, which sits between the two computer systems. The two systems share a private key with the Kerberos server to protect information from hackers and to assure that the data has not been altered during the transmission. One example of this encryption is NetCheque which is developed by the Information Sciences Institute of the University of Southern California. NetCheque uses Kerberos to authenticate signatures on electronic checks that Internet users have registered with an accounting server.

- Hardware-Based Systems

Hardware-based systems offer a more secure way to protect information, but, it is less portable and more expensive than software-based systems. The hardware-based security system creates a secure, closed channel where the confidential identification data is absolutely safe from unauthorized users. There are two hardware-based systems discussed in this section: Smartcard system and MeCHIP.

1. Smartcard System

Smartcard System is a mechanical device which has information encoded on a small chip on the card and identification is accomplished by algorithms based on

asymmetric sequences. Each chip on the Smartcard is unique and is registered to one particular user, which makes it impossible for a virus to penetrate the chip and access the confidential data. However, practical limitations in the Smartcard system prevent it from broad acceptance for major applications such as home banking or on-line distribution. One draw-back for the Smartcard is that it can not handle large amounts of information which need to be decoded. Furthermore, the Smartcard only protects the userôs private identification and it does not secure the transfer of information. For example, when the information is keyed into the banking software, a virus could attack the information, altering its destination or content. The Smartcard would then receive this altered information and send it, which would create a disaster for the user. Nevertheless, the Smartcard is one hardware-based system that offers confidential identification.

2. MeCHIP

MeCHIP which developed by ESD is connected directly to the PCôs keyboard using a patented connection. All information which needs to be secured is sent directly to the MeCHIP, circumventing the clientôs vulnerable PC microprocessor. Then the information is signed and transmitted to the bank in secure coded form. A closed, secure channel from the client to the bank is assumed in this case. All information which is transmitted and received is logged and verified to ensure that it has not been tampered with. If there are any deviations, the session is immediately terminated. This hardware-based solution offers the necessary security at the personal computer to transfer confidential information.

3.2 Privacy Technology

Privacy technology can be used to assure that consumers, merchants, and the transactions themselves remain confidential. For instance, companies sending important, secret information about their marketing strategy to one of its partners would like to keep that information private and out of the hands of its competitors. This technology will keep all information secure and can be applied to electronic cash, also known as ñe-cashò. The privacy technology provides a fully digital bearer instrument that assigns a special code to money, just like a bank note. The security of e-cash is superior to paper cash because even if it is stolen, it can not be used. However, e-cash has its share of disadvantages because it lacks the privacy of use. ñThis system is secure, but it has no privacy. If the bank keeps track of note numbers, it can link each shopôs deposit to the corresponding withdrawal and so determine precisely where and when Alice spends her money.ò (Chaum, 1992) This would make it possible to create spending profiles on consumers and threaten their privacy. Furthermore, records based on digital signatures are more vulnerable to abuse than conventional files. Not only are they self-authenticating, but they also permit a person who has a particular kind of information to prove its existence without either giving the information away or revealing its source. ñFor example, someone might be able to prove incontrovertibly that Bob had telephoned Alice on 12 separate occasions without having to reveal the time and place of any of the calls.ò (Chaum, 1992). One solution to this lack of privacy is the implementation of ñblind signaturesò. How it works is that before sending the bank note number to the bank for signing, the user multiplies the note number by a random factor. Consequently, the bank knows nothing about what it is signing except that the note has a specific digital signature belonging to a personôs account. After receiving the blinded note signed by the bank the user can divide out the random factor and use it by transferring it to a merchantôs

account as a payment for merchandise. The blinded note numbers are untraceable because the shop and the bank cannot determine who spent which notes. This is because the bank has no way of linking the note numbers that the merchant deposited with the purchaserôs withdrawals. Whereas the security of digital signatures is dependent on the difficulty of particular computations, the anonymity of blinded notes is limited only by the unpredictability of the userôs random numbers. The blinded electronic bank notes protect an individualôs privacy, but because each note is simply a number, it can be copied easily. To prevent double spending, each note must be checked on-line against a central list when it is spent which makes this verification procedure unacceptable for many applications, especially for minor purchases. Thus, this technology currently, is only applicable for large sums of money.

Self Assessment Exercise

Discuss the merit and demerit of Hardware-based security system of protecting information.

4.0 Conclusion

In order to reduce the potential vulnerabilities regarding security, many institutions and organisations have developed various solutions in both software-based and hardware-based systems. Generally speaking, software-based solutions are more common because they are easier to distribute and are less expensive. In order for electronic banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous. The future of electronic banking will be a system where users are able to interact with their banks ñworry-freeò and banks are operated under one common standard.

5.0 Summary

The solution addresses the use of secure protocols because trusted channels donôt really exist in most of the environment, especially since we are dealing with linking to the average consumers. The solutions to the security issues require the use of software-based systems or hardware based systems or a hybrid of the two. These software-based solutions involve the use of encryption algorithms, private and public keys, and digital signatures to form software packets known as Secure Electronic Transaction used by Mastercard and Pretty Good Privacy. Hardware-based solutions such as the Smartcard and the MeChip provide better protection for the confidentiality of personal information. Software-based solutions have the advantage over hardware-based solutions in that they are easy to distribute and are generally less expensive.

6.0 Tutor Marked Assignment

Succinctly discuss the four Current Encryption Technology in security management.

7.0 References/ Further Reading

(1) Encryption Crash. Http://www.iw.com/1997/01/news.html#crash

(2) Encryption Issues.
Http://www.muc.edu:80/cwis/person/student/lockett/encryption.html

(3) How PGP works. Http://rschp2.anu.edu.au:8080/howpgp.html

(4) Internet Security. Http://cfn.cs.dal.ca/Education/CGA/netsec.html

(5) Introduction to PGP. Http://sun1.bham.ac.uk/N.M.Queen/pgp/pgp.html

(6) Off the Charts The Internet. Http://www.iw.com/1996/12/charts.html

(7) PC Banking Services Spread, but Success is Still Uncertain. http://conceptone.com:80/netnews/nn942.htm

(8) Security Comes First With Online Banking at Security First Network Bank. http://www.hp.com/ibpprogs/gsy/advantage/june96/custspot.html.

(9) SET Specification. Http://www.visa.com/cgi-bin/vee/sf/set/intro.html.

(10) Solving the Puzzel of Secure Electronic Commerce. Http://www.rsa.com/set/bankset.htm.

(11) The comp.security.pgp FAQ. Http://www.gpg.net/gppnet/pgp-faq/faq-01.html#1.3

(12) The MeCHIP. Http://www.esd.de/eng/chip/index3.htm.

(13) Visa, Mastercard to Set Standard for Electronic Commerce. http://www.cnnfn.com/news/9602/01/visa.mastercard/index.html.

UNIT 5

Electronic Data Interchange (EDI) Messaging Security

Content

1.0 Introduction

The modern economy and the future wealth and prosperity of industry and commerce rely increasingly on the exchange of data and information, in electronic form, between business partners. The speed and reliability of the information exchanged coupled with the spread in the distributed use and applications of IT are increasingly affecting the competitiveness of businesses and international trade. Electronic information exchanged in this way is growing in volume because of the increasing number of business partners that may be involved (suppliers, customers, manufacturers, bankers, carriers, and so on) and the numerous documents that need to be exchanged. The performance of the system handling these documents can significantly affect the economy and future prosperity of a business. The ability to process and exchange trade data as quickly as possible allows stocks to be reduced at a profitable rate, helps cut financial costs, and gives firms such as this an additional competitive edge by improving the service offered to their customers. In addition to the speed, the flexibility in responding to customersô changing needs and desires adds value to the service being offered and creates better commercial relationships. In response to the need for effective and efficient solutions to handle this way of doing business, Electronic Data Interchange (EDI) offers substantial advantages and opportunities. The EDI approach has been identified as the most important user base of open networks and likely to create one of the most fundamental changes in the way that future business is carried out. EDI is being used in a growing number of market sectors, in a wide range of user applications. The use of EDI trading systems is underpinned in many respects by the need for security, and it is the use of commercially reasonable security features for EDI that will bring about its long-term success.

2.0 Objectives

This unit looks at a particularly important aspect of EDI ð the security of EDI messages. In particular, it focuses on the secure communications of EDI messages using **X.400, X.435,** and **X.500** standards,. To start with, some introductory material is presented that views security in the context of Open-EDI.

3.0 Main body

3.1 Security and the Open-EDI requirements

There have been many attempts over the years to understand the security requirements for EDI. One of the most important efforts is described in the European report ñSecurity in Open Networksò [SOGI89]. This report, commonly referred to as the SOGITS Report, confirmed the business need for EDI security. It identified EDI as the most important and demanding use of open networks, and, through an extensive survey covering 59 organizations in 12 countries in Europe, it reinforced the need for a range of solutions addressing several key areas of technical work. The SOGITS Report [SOGI89] considered the needs of users and suppliers of EDI-based systems across a wide range of applications, including corporate trading systems, financial systems, import/export systems, cargo handling systems, computer-aided acquisition and logistics (CALS), CAD/CAM (computer-aided design/computer-aided manufacturing), procurement and stores, and so on. IT and communications systems that are associated with the use of EDI will have a wide range of security requirements commensurate with the nature and value of the business using the system. These requirements can range from very broad, in the case of a sensitive commercial business exchange (where the integrity, confidentiality, and availability of the EDI information being exchanged are critical to the business mission), to a more basic form of requirement, which might be the data integrity of a regular shipment order. Users of EDI trading systems include government departments (for example, Custom and Excise), manufacturing industries (including the car industry, aerospace industry, chemical industry, and electronics industry), finance, and insurance. In most areas of application, the three major risks to EDI messages are:

ÅLoss of integrity (that is, alteration, modification, or destruction), for example, important for payment services; sensitive information (including medical records and personnel records); critical processes; commercial designs, specifications, and manufacturing processes (for example, in the case of CAD/CAM);

ÅLoss of confidentiality (that is, copied, seen, or heard by unauthorized persons), for example, important for sensitive information (including medical records and personnel records) and for intellectual property, commercial designs, specifications, and manufacturing processes (for example, in CAD/CAM); and

ÅNonavailability (that is, not accessible when needed), for example, important for ñjust-in-timeò situations and for 24-hour trading, production automation, critical processes, and so on.

There are many customer benefits and demands for EDI. As a result, there is a growing demand for a set of commercially reasonable security solutions. Priority must be given to a standardized approach to EDI security if the long-term benefits of EDI to the business environment are to be achieved. The current trend to obtaining the more substantive business opportunities through the use of EDI will be through a standardized approach leading to a secure Open-EDI environment.

The Essence of EDI Messaging Security

One must assume that EDI may be used across a wide-ranging messaging continuum covering different types of network services and various value-added application

platforms. This range of communications provision will reflect a need for different levels and types of security to protect these EDI messages. The EDI components chain and the emerging EDI enabling technologies to support the proprietary/direct-link type of offering to the Open-EDI approach based on international standards.
EDI security appears at several interrelated stages of system technology:
Åthe user/application interface,
ÅEDI applications and value-added services,
Åthe processing (both batch and interactive) and storage of EDI messages, and
Åthe communication of these messages in an open systems environment.

The basic security objectives that may need to be met at each stage are those of authentication and integrity, non-repudiation, access control, availability, audit, and accountability. These objectives must be satisfied by both logical and legal controls and procedures, which are supported by a range of technologies, tools, and standards. Current assertions about the security of EDI messages being handled at and between these various stages are often based on a level of ñtrustò in the increasingly complex systems that handle such messages, and the rules of engagement agreed to between messaging partners. It is therefore imperative that both the logical and legal aspects of EDI security are dealt with hand in hand. These two aspects of EDI security need to work with each other to provide the right levels of overall trust and protection to EDI messages and interchanges. The rest of this unit looks at secure messaging for EDI.

Secure Messaging Standards
The standards industry has tackled many aspects of EDI security. In particular, the most important work in this area concerns EDI messaging based on the use of International Message Handling Standards [CCIT88a], [CCIT90]. The scope of this work covers secure message transfer, which provides the benefits of secure messaging to a wide range of distributed applications such as EDI. Protection in an EDI messaging environment is essentially concerned with the non-repudiable submission, delivery, and receipt of messages in a way that preserves the integrity, confidentiality, and availability of the messages being communicated. The current messaging standards provide the means of applying security mechanisms to meet different types of security objectives and levels of security. A brief introduction to the most important standards in this area follows.

X.400 message handling systems (1988)
CCITT, in its 1988 version of the X.400 recommendations for message handling (and the corresponding ISO 10021 equivalent standard), has made major extensions to the Message Transfer System (MTS) to provide for secure messaging [CCIT88a]. The 1988 X.400 standard allows the provision of different types and levels of security service independent of the type of message being transferred. Applying security mechanisms to the MTS ensures that the benefits of secure messaging are obtained independent of the content type of the message. For some content types, additional security mechanisms may be defined in the content-type protocol. The security specified in this standard thus provides for secure message transfer services and distributed inter-working in support of applications such as electronic mail and EDI. The security model used to specify the security features of the 1988 standard is based on a threat assessment of an assumed messaging environment. This assessment considers the main threats to be associated with the unauthorized access to the messaging system, threats to the message itself, and intra-message threats. Table 1

shows an example threat/security service scenario that might be covered by this model. This table of threats and services is an indicative example rather than a definitive list. The designer of a secure messaging system would need to determine which threats are actually present and applicable to the messaging environment under consideration and which of these can be countered by the X.400 security services available. In essence, the designer will need to develop a technical security policy for the messaging environment.

Table 1. Threats and services.

Threat	Examples	Security Services
Masquerade	Impersonation, false claims/acknowledgments	Authentication
Unauthorized message modification	Modify, delete, destroy messages	Integrity
Repudiation	Denial of origin, submission, or delivery of a message	Nonrepudiation
Leakage of information	Unauthorized release of message contents	Confidentiality

The security services defined in X.400 provide the link between the security requirements and objectives as described in a security policy, and the security mechanisms (for example, digital signatures) and management controls (for example, for the management of public keys) to satisfy these requirements. The 1988 X.400 recommendations specify the following security services:
Å Authentication. Message origin authentication, peer entity authentication, probe/report origin authentication, proof of submission, and proof of delivery.
ÅIntegrity. Connection, content, and message sequence integrity.
ÅNonrepudiation. Nonrepudiation of delivery, of origin, and of submission.
ÅConfidentiality. Connection, content, and message flow confidentiality.
ÅSecurity content.
ÅMessage security labelling.

Each of these security services can be implemented by one or more types of security mechanism, to satisfy the requirements of many different messaging applications needing different levels of security. In implementing these security measures and controls, the level of assurance at which these must be applied and maintained will be considered. In the case concerning the use of cryptographic mechanisms, it might be a question of the strength of mechanism and the mode of operation being used.

X.435 EDI messaging (1992)
Since the introduction of the 1988 X.400 standard, CCITT has been working on a series of recommendations, referred to as the X.435 series for secure EDI messaging. X.435 will use the X.400 security mechanisms in addition to some EDI-specific security measures not defined in the X.400 standard. This standard will thus provide a security messaging capability for EDI applications, supporting the use of a range of EDI message formats currently being standardized, such as EDI for Administration,

Commerce, and Trade (EDIFACT), American National Standards Institute ANSI/X12, and United Nations Trade Document 1 (UN/TD 1). The basic security features being progressed by the X.435 EDI messaging standards work, in addition to the 1988 X.400 security features, include the following:
Å*EDI Messaging (EDIM) responsibility authentication.* Proof of transfer, retrieval, and EDI notification.
Å*Nonrepudiation of EDIM responsibility.* EDI notification, retrieval, transfer, and content. In addition, work has started on:
Åmessage store extensions (including control of delivery, user security management, and audit),
Åmessage transfer audit, and
Åother enhanced security management controls.

The practical realization of this might typically be a standard EDI software package containing EDI application software, various format options (for example, EDIFACT), and an EDI user agent. The standard package could be modified to incorporate the necessary security controls to provide the capability of implementing a number of proof services, and possibly other services. In addition, security could be offered at the message transfer level via the message transfer agents to provide a secure transfer medium.

X.500 directory systems (1988)
CCITT and ISO/IEC incorporated into their 1988 X.500 series of directory system standards [CCIT88c] an ñAuthentication Frameworkò (X.509) that defines mechanisms and protocols for entity authentication. These mechanisms are based on the use of public key technology, digital signatures, and the introduction of various public key elements such as certificates and tokens. Other publications [ANSI92a, b] are applicable to the financial sector. The X.509 standard also introduces the concept of a Certification Authority (CA) through which users are identified, registered, and then issued their public key certificate(s). The use and application of the X.509 certificates and the concept of Certification Authorities (CAs) are a natural complement to the distributed nature of the X.500 directory system approach and to the provision of publicly available information services. It can be shown that this natural duality also holds between the X.509 technology and the provision of a number of EDI security features. The X.509 standard when implemented will constitute a secure naming and routing process in a multi-domain messaging environment. In addition, a number of the security services specified in X.400 can be implemented using the X.509 technology (certificate, token, and digital signature). These security services include user identification, content integrity, and various non-repudiation/proof services, for example, proof of delivery. X.509 technology can provide a distributed use of authentication, thus allowing secure distributed processing of EDI transactions and greater security of trading partner connectivity. Although the X.509 technology is not the only solution to the provision and implementation of X.400 and consequently EDI security, it is certainly one of the most effective and the most practical. The distributed nature of messaging and in particular EDI messaging makes the X.509 technology a natural partner for secure trading across distributed environments. The X.509 technology is able to play a major part in the realization of a number of these services, in particular, the provision of non-repudiation services, the responsibility authentication options, and the various authentication and integrity services. However, other methods for providing these

services are also available; these include the use of symmetric encipherment techniques, message authentication codes (MACs), and manipulation
detection codes (MDCs).

Non-Repudiation, Responsibility, and Proof
One of the important features of EDI messaging is that of non-repudiation, which provides some level of proof or evidence that an EDI message has been sent or has been delivered. For example, non-repudiation of delivery provides the originator of the message with proof that a message has been delivered, and this proof should hold up against any attempt by the recipient(s) to deny receiving the message or its content. Both the X.400 and X.435 standards allow for a number of different elements of service to be available in order to provide a wide range of non-repudiation services.

Current standards [CCIT88a] introduce the concept of a ñresponsibility transfer boundaryò and provide specification for the provision of several ñresponsibilityò security services. The basic idea behind this concept is to transfer responsibility of certain aspects of a message, as it passes from one component of the EDI messaging systems to another component. For example, after transferring an EDI message through the network of message transfer agents into the EDI message store (EDI-MS), the end system EDI user agent will at some point in time retrieve this message from the EDI-MS. By providing a proof of retrieval message, responsibility for that message now rests with the EDI user agent [SC2792].

Self Assessment Exercise
What do you understand by Secure Messaging Standards?

4.0 Conclusion
There is no doubt that the growing trend toward open systems will see an ever-increasing requirement to achieve the right levels of business confidence and assurance in these systems [SOGI89, HUMP90a, BLAT90]. EDI is the growing business technology of the 1990s. It is a key change dynamic to business development. It is the baseline for improving business performance and efficiency, building new markets, and expanding old ones ð and it allows the introduction of new business opportunities. It is a technology that has support from government, industry, finance, and commerce. The SOGITS Report [SOGI89] confirmed the business need for EDI security. It identified EDI as the most important and demanding use of open networks and through an extensive survey reinforced the need for a standards program addressing several key areas of technical work. This unit identifies not only the need for technical and quality standards for EDI security but also the need for urgent consideration to be given to the legal aspects of these electronic solutions. It emphasizes the need for work on practical standards for EDI security, third-party services (directories, notaries, and so on), messaging gateways for multi-domain communications, techniques for non-repudiation, audit, and authentication.

5.0 Summary
This unit has mainly concentrated on X.400, X.435, and X.500 standards, and their use in EDI messaging. The X.400 technology provides a basis upon which secure trading systems can be developed which would satisfy a high percentage of the market requirements, in particular, for international trade and wide-area regional

trade. It is probably one of the most significant steps in achieving a secure Open-EDI environment. However, this is just part of the solution, albeit a very important part. There are still issues to be dealt with in providing secure distributed systems technology in such a way that all barriers (for example, technical, administrative, and international) are removed to allow the introduction of a fully integrated Open-EDI environment. This standards-driven technology cuts across many multi-disciplined areas: from work on CAEs (common application environments), open systems management, and distributed applications to work on techniques, services, and protocol building. It is a standard technology that is targeted toward the future integration of the current set of services and applications, together with the introduction of additional ones to meet the future needs of a wide range of distributed business environments. Also this section considers some of the aspects of international security standards as they apply to the provision of secure EDI messaging. In particular, the use of the 1988 X.400 message handling system standards has been the basis for this overview. The X.400 1988 standard, together with the X.500 directory systems standard and the X.435 EDI messaging standard, form an internationally agreed upon basis of future secure EDI technology and secure EDI messaging environments.

6.0 Tutor Marked Assignment

What is Electronic Data interchange (EDI)? Discuss any security issue in EDI

7.0 References/ Further Reading

(1) Frank Vahid and Tony Givargis, (2002) ñEmbedded System: Design A unified Hardware/Software Introductionò, John Wiley & Sons, Inc.

(2) Jean-Michel, Oz Livea, Jacques Rouillard, (2007). ñHardware/Software Co-Design & Co-Phillip A.Laplante, ñReal-Time Systems Design and Analysisò, Second Edition, ISBN: 81- 203-1684-3.

(3) Ted Humphreys, (2006). Electronic Data Interchange (EDI) Messaging Security. Journal of Information Security. Pp.423-438.

(4) Tim W. (2000), ñAn Introduction to the design of small-scale embedded systemsò, ISBN: 0-333-92994-Verificationò, ISBN: 0-7923-9689-8.

(5) Wayne W. (2004) ñComputers as Components: Principles of Embedded Computing System Designò, ISBN: 9971-51-405-2.

Module 4

Unit 1. Converting an Analog CCTV System to IP-Surveillance
Unit 2. Closed Circuit Television and the Role of Security Operatives in Surveillance and Intelligence Gathering
Unit 3. Requirements Engineering for E-Voting Systems
Unit 4. The Economics of Information Security
Unit 5. Hard Nature of Information Security

UNIT 1

Converting An Analog CCTV System to IP-Surveillance

Content

1.0 Introduction

Digital video recording has been around for a while nowð there are hundreds of DVRs in the market today. It used to be that only large installations or Fortune 1000 companies could afford digital. But according to a recent report from industry analysts Frost and Sullivan, demand for digital systems surpassed that for analog systems sometime in 2002. Digital technology has shown its superiority, but in the last two years it has become a commodity. What is the next step, beyond the DVR, for end users to make their security systems digital? IP-Surveillance solutions have emerged as an attractive alternative to the DVR as it provides a bridge to enter the digital world with the ultimate solution of a high-performance, low-cost digital video surveillance and monitoring.

2.0 Objectives

In this unit, we will provide a guide for the end user who is interested in making the transition from a current analog system to a digital one. We will demonstrate how this move can be undertaken in a progressive, step-by-step manner and review the many benefits that come from implementing digital technology. Finally, we will examine three specific applications of digital IP-Surveillance technology. Now is the right time to take the step towards digital surveillance and monitoringð let us see how.

3.0 Main body

3.1 Benefits of going digital

For the past 20 years, monitoring and surveillance applications have been served by analog technology. CCTV has traditionally been recorded to VCRs (video cassette recorders), and because of its perceived ease of use and manageable price point, analog was probably the right choice at the time of purchase. However, the rise of digital has laid bare analogôs many shortcomings. Analog CCTV systems are generally maintenance intensive, offer no remote accessibility, and are notoriously difficult to integrate with other systems. Despite these obvious deficiencies, the end user who has invested in cameras, cables, and more, and is satisfied with the current quality is right to ask, ñWhy buy new equipment?ò

Implementing a digital system does not require throwing away those trusted (and already paid-for) cameras. With IP-Surveillance, you can still use all the cameras, lenses, and cables in place through this step-by-step migration to digital technology. And if this is not enough reason to seriously consider an upgrade, examine the TLV, or time-lapse video, recording component. These systems are highly labour intensive because of the need to change tapes and perform system maintenance. Tape wear and tear is an ever-present problem. Furthermore, the actual quality of the images recorded is often unsatisfactory, particularly if used for official investigations. With the introduction of digital video recorder (DVR) technology, the storage media are no longer dependent on operator interventionôs or tape quality. And with IP-Surveillance technology, the video server and network server represent the next level of improvement by connecting existing cameras to the network with a video server and then storing the images on the network server.

Digital's many benefits. With the spread of digital recording technology, its many advantages have become apparent: ease of use, advanced search capabilities, simultaneous record and playback, no image degradation, improved compression and storage, integration potential, and so on. But with digital technology as its core, IP-Surveillance provides all these advantages and many more:

Remote accessibility. The main benefit from connecting those analog cameras to a network is that the user can now see surveillance images from any computer on the

networkð without the need and expense of additional hardware or software. If you have a port to Internet, you can securely connect from anywhere in the world to view a chosen facility or even a single camera from your surveillance system. By using a Virtual Private Network (VPN) or the company intranet, you can manage password-protected access to images from the surveillance system. Similar to secure payment over the Internet, a userôs images and information are kept secure and viewed only by approved personnel.

Unlimited, secure storage. Store as many hours of images as you wantð provided you have hard disk capacity. And store and view images off-site in any location in cases where monitoring and storage are mission critical or need back up.

Flexible, pro-active image distribution. Take snapshots of an intruder or incident and send by e-mail to police or appropriate authorities. Also, police or other password-approved parties can log on to cameras and view activities around a userôs facilities.

Automatic alerts. The video server can automatically send an e-mail with an alarm image to selected e-mail addresses, so the right people have the information they need to take timely action.

Total cost of ownership and performance. At the beginning of this section, we listed the many advantages of digital technology, but it bears repeating that with no further need of time-lapse video equipment, no more tapes and no more tape changing

and cataloging are required. Maintenance costs go way down. And while system performance and results markedly increase, total cost of ownership over time will continue to decrease. IP-Surveillance provides all the superior functionality of digital technology, plus the tremendous benefits of increased accessibility, storage and distribution of images, and a superior cost-benefit picture. At this point, analog owners are convinced it is time to make the switch, but what factors bear consideration?

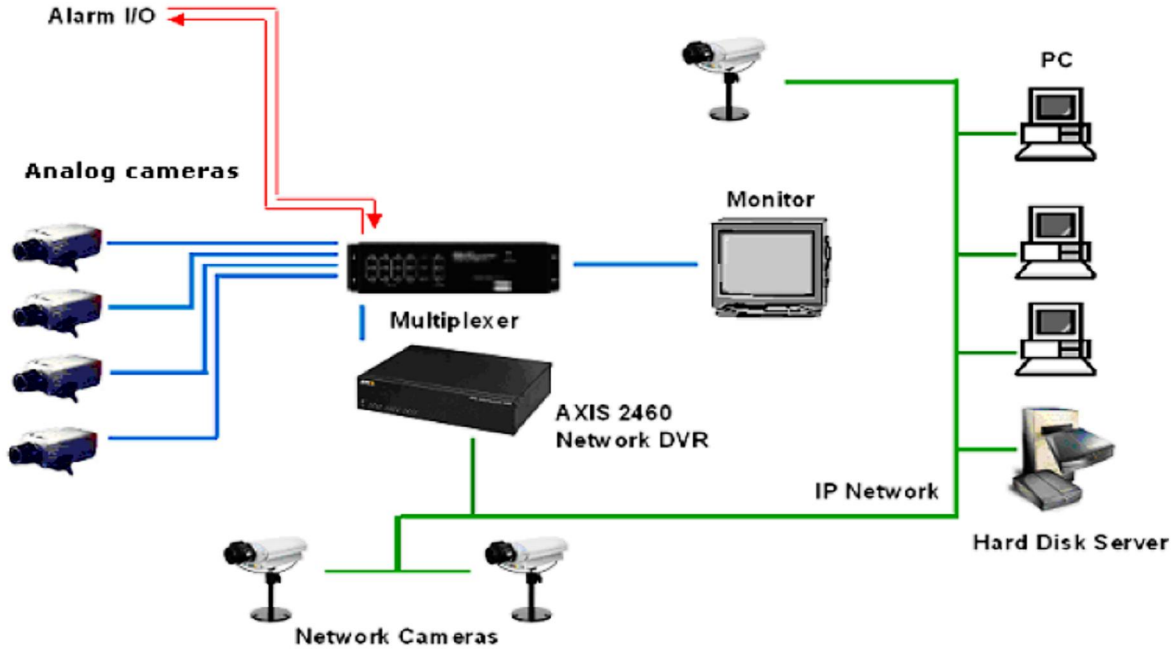


Figure 1: Analog and digital systems working in parallel

3.2 Factors to consider: The move to digital

At this point, we have seen that the transition from an existing analog system to a high-functioning digital IP-Surveillance system can be done step by step and in a cost-effective manner, but there are still a number of factors to consider. What about network bandwidth, bandwidth connections (network, xDSL, ISDN, cellular phone etc.), hard disk storage requirements and software?

1 Network Bandwidth

If you are using a local network, cameras can be patched through a special dedicated router for the camera, thus eliminating most concerns about bandwidth. However, if images are sent by PSTN, bandwidth considerations do come into play. To get a performance of 30 frames per second, you need a minimum bandwidth of 120 kB/s.

2 Hard disk space

Hard disk storage requirements are dependent on the frame rate of the video you want to store. If you want to store all video at 30 frames per second (30 fps) as opposed to 1 fps, then that requires 30 times the amount of storage. Each application has different recording and storage needs. In terms of video fps, and hard disk storage requirements will differ accordingly.

3 Software application

A wide variety of software applications can be used. What software to use is governed by the end-user application and their specific needs. An example of application software is Milestone's Xprotect Business product, an advanced and highly scalable video surveillance software with built motion detection, intelligent PTZ patrolling features, high capacity recording and remote access via the Web. Another is a management software from SeeTec, a software for remote camera configuration and management, direct or automatic control of cameras and accessory equipment, image representation, display and message forwarding. A third is the Softsite32 from JDS Digital Security Systems. Softsite32 is a stand-alone application that enables viewing, recording and management of video streams and snapshots. It is highly scalable and robust, with quick installation and setup. JDS has a growing worldwide install base, public and private implementations, as well as custom solutions

Analog CCTV to IP-Surveillance: Case studies
Current analog CCTV systems, like the one shown below, now have few advantages beyond familiarity and cost. Analog CCTV relies on time-lapse technology. Storage is limited to low-tech tapes, which make maintenance high and search capabilities low. Analog has low integration potential and provides no opportunity for remote access. It is an old and familiar system, and its time for retirement is now.

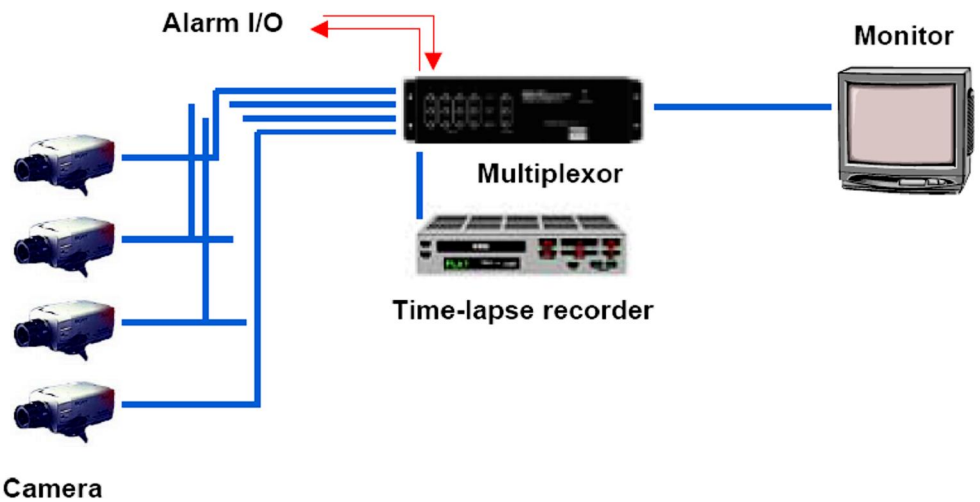


Figure 2: Analog CCTV Systems

a. The Digital Revolution Upgrade: Video Server Technology

In the configuration below, the video server provides the connection between the analog cameras and the network. With the simple addition of this technology, a whole new list of features and functions becomes available:

ÅRemote access of images utilizing the computer networkð eliminating the need for dedicated security monitors in a central office

ÅPassword-protected access anywhere there is an Internet connection

ÅConnect to a remote control station to view what is going on and control cameras and other aspects of the surveillance system

ÅEase of integration with other systems and applications

ÅLower TCO (total cost of ownership) by leveraging existing network infrastructure and legacy equipment

ÅCreates a future-proof system, so no more complete system overhauls

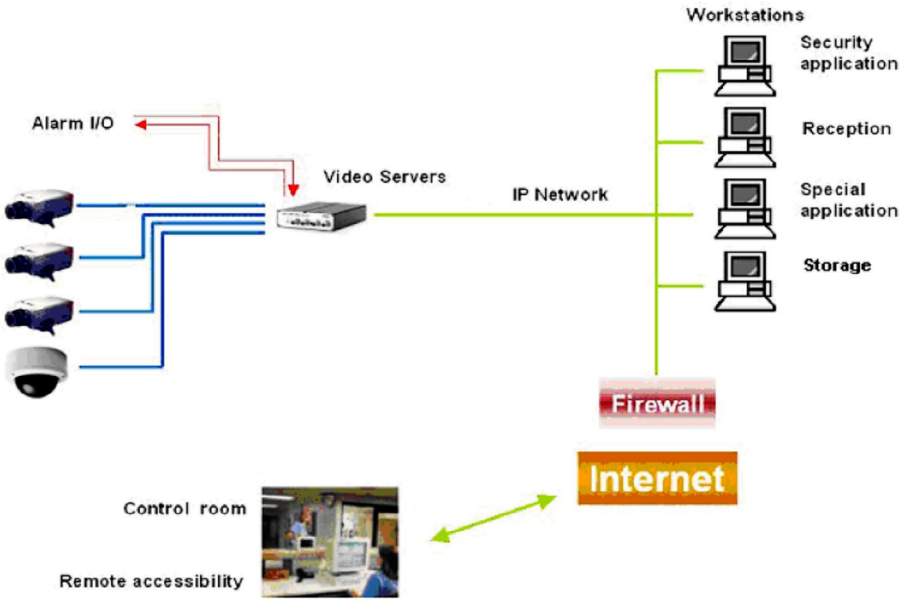


Figure 3: *Upgrade: The ongoing digital revolution*

Expand the Benefits Over Time: The Network Camera

But we donôt need to stop with the first-level upgrade described above. The digital revolutionôs video server and camera technology enables us to expand the system and its advantages. With a digital system, you can connect as many cameras as you want. You can attach each new camera directly to the network. This provides a new set of added benefits:

- Viewing access can be restricted to only authorized persons, or live video can be posted on a companyôs Web site for the entire world to see.
- If the building is equipped with an IP network, then the necessary infrastructure already exists to add network cameras without high installation costs.
- Network cameras perform many of the same functions as a standard analog CCTV camera, but with greater functionality and at a substantial cost saving.
- Network cameras plug directly to the existing network, yielding substantial savings because the coaxial cabling required for analog cameras is not needed.
- When computers are already in place, no additional equipment is needed to view the video output from a network camera.
- Output can be viewed in its simplest form in a Web browser at the computer monitor, and in more complex security solutions, with the aid of dedicated software.

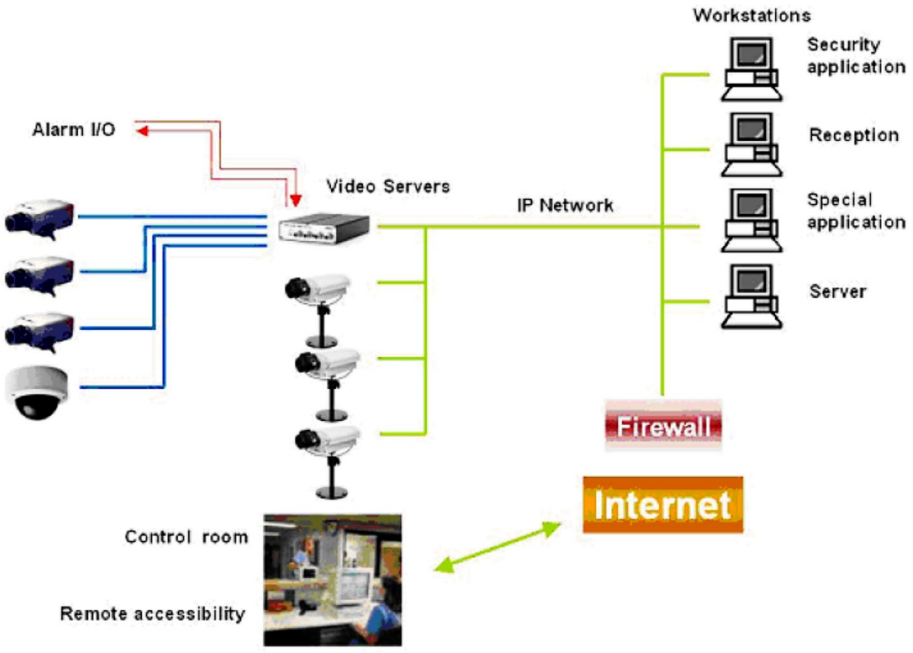


Figure 4: *The ongoing digital revolution*

Self Assessment Exercise
What are the limitations in Analog security surveillance?

4.0 Conclusion

The digital solution is easier and cheaper than you think. Even with the enormous growth of CCTV and the recent acceleration in migration to digital video technology, significant hurdles remain for a majority of users in making the switch from analog to digital video recording. Many end users are still not aware that there is a step-by-step path available to transform existing analog security systems to digital technology. In terms of education, most end users still need a deeper understanding of the benefits and possibilities of digital and network-based surveillance systems. It is also important to know that in the transition from analog to digital surveillance systems, no system is too small or too tightly tied to analog technology, to benefit from digital technology. Even a single analog camera connected to a video server will provide the user with the full range of advantages that come from digital, networked surveillance.

Consider the ease and cost-effectiveness of a progressive, step-by-step move to digital with IP-Surveillance. Now is the right time to take the digital step.

5.0 Summary

The past 20 years, revealed that monitoring and surveillance applications have been served by analog technology and the traditional recoding of VCRs into CCTV has come to bear in recent times. Digital technology has shown it is superiority over analog, nevertheless its importance cannot be undermined depending on the level of development of a nation. This unit highlights the major benefits of a digital technology in security such as remote accessibility; unlimited, secure storage; Flexible, pro-active image distribution and Automatic alerts. These benefits also serve as advantages of the analog system.

6.0 Tutor Marked Assignment

List and explain some of the strengths in digital security technology

7.0 References/ Further Reading

(1) Axis White Paper, 2002 Converting an Analog CCTV System to IP-Surveillance Axis Communications www.axis.com.

(2) McCahill, M. (2002) *The Surveillance Web: The Rise of Visual Surveillance in an English City*.Cullhompton: Willan Press.

(3) Monmonier, M. (2002) *Spying with Maps: Surveillance, Technologies and the Future of Privacy*. Chicago: The University of Chicago Press.

(4) Nieto, M. (1997) ôPublic video surveillance: is it an effective crime prevention tool?ô California Research Bureau. http://www.library.ca.gov/CRB/97/05/

(5) Norris, C. and G. Armstrong (1999) *The Maximum Surveillance Society: The Rise of CCTV.* Oxford: Berg.

(6) Norris, C. and G. Armstrong (1998) óCCTV and the rise of the surveillance society.ô In P. Carlen, and R. Morgan (eds.) *Crime Unlimited*. London: McMillan Press.

(7) Norris, C., and G. Armstrong (1997) óCategories of control: the social construction of suspicion and intervention in CCTV systems.ô A draft manuscript of *The Rise of the Mass Surveillance Society*, Oxford: Berg.

(8) Webster, W. C. R. (1998) óSurveying the scene: geographic and spatial aspects of the closed circuit television surveillance revolution in the UK.ô Paper presented to the European Group of Public Administration Annual Conference, 12th meeting of the Permanent Study Group on Informatization in Public Administration, Glasgow Caledonian University, 30 August - 2 September.

UNIT 2

Closed Circuit Television and the Role of Security Operatives in Surveillance and Intelligence Gathering

Content

1.0 Introduction

The sum total of the health of a nation is indexed by its security rating. This is because the wheel of Nation building in economy, politics, and social development is propelled or hampered by its relative level of security or insecurity. No wonder, countries that have advanced are those with stable security compared to war ï ravaged countries that are characterized by under-development, hunger, diseases and poverty. Therefore, security is a key to nation building.

2.0 Objectives

This unit seeks to identify and define the context of key words:

i. Security operatives
ii. Surveillance
iii. Intelligence gathering
iv. Closed circuit television - CCTV and
v. the role of the Nigeria Security and Civil Defence Corp in the application of electronic gadgets.

3.0 Main body

3.1 Security Operatives:

These are the personnel charged with the responsibility of providing security services or details in their respective field of special assignment. The government security agencies are the Military, and various paramilitary organizations. These include the Army, Navy, Air force; the Police, Nigeria Security and Civil Defence Corps (NSCDC), Prison Service, Immigration etc. There are also private security service providers etc.

Surveillance

Surveillance is the covert observation of places, persons and vehicles for the purpose of obtaining information concerning the identities or activities of subjects. The surveillant is the person who maintains the surveillance or performs the observation. The subject is the person or place being watched.

Surveillance may be divided into three kinds:
i. Surveillance of places
ii. Tailing or shadowing
iii. Roping or undercover investigation

Intelligence Gathering

Before we start to exchange ideas, let me briefly tell you a story, there once lived a man. He is so lazy to the point that his neighbours are contemplating ejecting him from the area. He used to sit in front of his mud house watching his neighbours planting maize and all he ever thought of is how he will steal from it. One day, barely few minutes when he sat outside his house, he noticed that the maize planted a few days ago have started germinating. He observed this over some days and he was quite amazed to see the relative changes going on over time. The man in question later propounded the theory of Dy/Dx, which means the smallest change that can take place with an outstanding effect and with minimum negative effect. The man is called Calculi and his theory is Calculus. It is this theory that all Engineering Mathematics depends on till date. So coming to scientific definition or explanation of intelligence, it is the capacity, ability, tendency(ies) to meet novel situation. The ability to perform tests or tasks involves the grasping of relationships or ideas. It is not a prediction of future performance since quite a number of factors can alter it. Therefore, intelligence is the summation or assembly of data, information arising from surveillance activities. The data so gathered are processed or analyzed such that those of security interests in the case in question are assembled for operational use by way of arrest, tackling, foiling, investigation, interrogation or prosecution. Intelligence reports usually serve as leads or guides to implementing a security action plan.

Closed Circuit Television, CCTV

The television camera and receiver have been added to the resources of the security investigators. By means of a closed circuit television system, the activities of the subject can be observed from a distance. A number of private companies have installed these circuits to watch the activities and general behaviour of their employees. In one factory, four concealed cameras were installed to virtually monitor the production line. A receiving set, connected to the cameras by a coaxial cable was installed in the office of the plant manager. The employee of any section of the production line could then be observed by the manager surreptitiously and leisurely. CCTV appliances are used in supermarkets to monitor the activities of workers and customers in the hall. It has equally found its use in modern Banking Security Watch, and in Private Premises Surveillance. The footage of any armed robbery invasion in a bank can be replayed to analyze the involvement of each person present at the scene of the robbery.

Instrumentation *is taken to mean more than criminalistics*; it includes also all the technical methods by which the fugitive is traced and examined, and the general way investigation is advanced. Thus, the print systems, modus operandis, the lie detector, communication systems surveillance equipment, such as telephone lens and detective dyes, searching apparatus such as x-ray unit and metal detector, and other investigative tools are contained within the scope of the term. There has been a tendency in recent years to place too great a relative value on the contribution of instrumentation to the detection of crime. The inexperienced are especially prone to place their faith in technical to the neglect of the more basic and generally more

effective procedures of information and interrogation. Greater publicity is given the instruments and techniques of criminalistics because they are frequently quite picturesque and attract the attention of the newspapers, features writers and dramatists. A small articulate group of persons, such as the medical examiners by making known their work in correct fashion, will at the same time convey a highly favourable impression of their contribution to the investigative work whereas the bulk, 95% of the work, might have been carried out by precinct detectives in a homicide investigation. However, the limitation of technical method is minimized in CCTV application due to its life-like video picturesque, it also compensates for complexities arising in criminal situations where no physical evidence can be found. Crimes like larceny and robbery, for example are usually committed without leaving physical evidence in the form of traces.

Using CCTV For Surveillance And Information Gathering

In using CCTV for surveillance, balance must be established between invasions of privacy/fear of authoritarian control of the population and increase safety of public properties and reduction in crime and antisocial behaviour may be on the increase.

Limitation of CCTV

Like any other instrument of operations, there are limitations. Major limitations of conventional CCTV systems are the impracticality of deploying sufficient number of people to be in front of television screens observing largely uneventful video. As long as this is the case, CCTV will tend to remain a reactive tool. The inability of being truly pro-active, producing timely alarms and eventually being able to prevent incidents is what ultimately limits these systems.

Installation and Cost

The installation of CCTV cameras especially in urban environments is now increasing in Nigeria but are in commonplace and well-known area in developed countries. UK lead the world with an estimated 4 million public cameras installed in a country of less than 60 million. So if we are to go with that simple arithmetic, we will need about 11 million cameras in Nigeria. What about the cost, management, maintenance etc?

We must all agree on this fact that human intelligence is the real intelligence. The performance of technical/scientific devices will only function and be reliable to the extent to which they are used, programmed or monitored, downloaded or analyzed. This is possible only through human intelligence. There is need for individual human intelligence ï as in dutifulness, diligence and integrity as well as corporate human intelligence. The corporate intelligence calls for the need for symbiotic working relationship in intelligence gathering through information passage and management, surveillance and logistics support, and a combined will to ensure a secured society. Grass root network need to be mobilized and sensitized against insurgence of crime. For example Petroleum Pipeline vandalizing, and PHCN facilities sabotage. All stakeholders, such as the community, the private sectors, and of course the security operatives need to marshal their various arsenals into an impenetrable security fortress.

The community and their leaders should give support by way of information, as a lead to crime prevention, foiling or apprehension. The private Sector participation ï Banks, Industries and Gas and Oil operators should support the security operators with funds, and logistics for proper security coverage. The security operatives on their part should

sink there differences, and work collaboratively for effective crime control and prevention.
With these in place, security intelligence as a tool becomes an intelligent device to achieve a secured society.

3.2 The Nigeria Security and Civil Defence Corps NSCDC: Relevance and Application

The Nigeria Security and Civil Defence Corps by the National Assembly Act No 2 of 2003 and its amended version of 2007, is mandated to give security reports, gathered from surveillance, to the government. According to section 3 subsection U of the NSCDC Act 2007, the Corps shall provide intelligence information to the Ministry of Interior on any matter relating to:
i. Crime control generally
ii. Riot, disorders, revolts, strike or religious unrest.
iii. Subversive activity by members of the Public aimed at frustrating any government programme or policy.
iv. Industrial action and strike aimed at paralyzing government activities.
v. Any other matter as may be directed by the Minister and
iv. Have power to arrange and mediate in the settlement of disputes among willing members of the Public.

The Civil Defence Corps officers are trained to adapt to military resilience as well as civilian sensibility. officers are resident among the people, spread over the nooks and crannies of the society. This naturally provides network coverage for intelligence sniffing and gathering.

Technical Involvement

The very nature of public or private investigation work requires intense concentration on the art of surveillance. As a result of extended study, exceptional ingenuity and impressive expense authorization, private agencies have developed a number of excellent instrumental techniques for surveillance. A few examples are:

Automobile surveillance: This is the method of tailing a vehicle by attaching to the under structure of the vehicle a miniature transmitter with a mercury battery, as the power supply. The investigatorôs car equipped with a receiver and a direction finding antenna can then follow at a distance which precludes detection.

Wiretaps and bugs: A wire tap is an electronic device that picks up both ends of a telephone conversation. A bug detects voices in a defined space. The telephone can be tapped at a number of places along the line, either in building, along the street lines, even at the telephone exchange. The tapped line is monitored by earphones or run into a recorder.
The more common forms of tapping are the following:
ÅDirect tap
ÅInduction coil
ÅBugs
ÅBody worn transmitter
ÅRecorder
ÅTelevision

Self Assessment Exercise
What do you understand by the term security intelligence?

4.0 Conclusion
The role of the NSCDC as mentioned above clearly shows that in modern day security operation and management, electronic aspects of security through the use of CCTV and other surveillance devices can not be overlooked. This has been demonstrated as necessary hence the practical knowledge of these equipments are made mandatory for every security personnel be it military or Para-military.

5.0 Summary
The importance of security was discussed in relation to security operatives, surveillance, Intelligence gathering, closed circuit television - CCTV and the role of the Nigeria Security and Civil Defence Corp in the application of electronic gadgets. Brief emphasis was laid on technical Involvement in security; Automobile surveillance and Wiretaps in securing telephone conversation that detects voices in a defined space.

6.0 Tutor Marked Assignment
What are the roles of the Nigerian Security and Civil Service corps in electronic security application?

7.0 References/ Further Reading
(1) Abolurin, J. A. (2007). The Nigeria Security and Civil Defence Corps and the Challenges of Humanitarian Assistance in Nigeria and Beyond. Ibadan. The Centre for peace and Conflict Studies, university of Ibadan.

(2) Adebayo Akinade, (2004). Managerial and Operational Skills For Modern Security Practice.

(3) Anderson, W.B (1987). Notable Crime Investigation, Spring Field, III Thomas.

(4) Buckwalter A. (1984). Surveillance and Undercover Investigation Butter Writh, Criminal Investigation.

(5) NSCDC in The Last 3 Years! What Legacy? (2008). *The Defender*. 2008. A Quarterly News Magazine Publication of NSCDC

(6) Rapp. B. (1985). Shadowing and Surveillance: A complete Guide Book, Port Townsend, Wash Loompanies.

(7) Schultz D.O. 1978. Criminal Investigation Techniques Houston, Gulf Publishing,

Unit 3
Requirements Engineering for E-Voting Systems

Content

1.0 Introduction

There has been a great debate on the advantages and problems of various electronic voting schemes. Questions like ñHow will the internet alter democratic institutions?ò ñHow will people get information about elections? and ñHow would people vote in general elections?,ò have encapsulated the attention of many minds. The prospect of being able to vote ñin your pajamas,ò as it is being described, captured the imagination of political leaders, technology innovators, and voters around the world. The aim of electronic voting schemes is to provide a set of protocols that allow voters to cast ballots while a group of authorities collect votes and output the final tally. Problems with voting machines extend from the quality of the locks, to the need for a printed audit trail, to the hacking of the communication links. Although voting makes many people to believe that voting is the perfect application for technology, but in reality applying it is hard. For a voting system to be ideal, four attributes must be satisfied: anonymity, scalability, speed, and accuracy. These attributes will be covered by both the functional and non-functional requirements.

2.0 Objectives

In this unit, both functional and non-functional requirements for Online Voting Systems are presented. They will describe how an online voting system ought to behave. For a system that can have a great impact on democracy and the way people will vote, engineering the requirements is crucial as no one will trust a system that is constructed based on wrong or imprecise requirements. As the design and implementation of Online Voting Systems has requirements engineering as its foundation, we need requirements that have zero tolerance with respect to deviating from actual need. This unit also emphasizes the need for voting system security requirements. Example of use cases will be provided.

3.0 Main Body

1 Functional and Non-Functional Requirements

Requirements are defined during the early stages of system development as a specification of what should be implemented. They describe how the system should behave or system attributes. In other words, they represent what the system should do from the stakeholdersô point of view, and they should meet their needs. There are a number of ways to define requirements engineering. Requirements engineering is the first major activity following the completion of a statement of need. It is defined in terms of its major activities: understanding problems, solution determination, and specification of a solution that is testable, understandable, maintainable, and that

satisfies project quality rules. A number of researchers relate requirement engineering to some goals. Requirements Engineering (RE) is concerned with the identification of goals to be achieved by the envisioned system, the refinement of such goals and operationalization into specifications and constraints, and the assignment of responsibilities for the resulting requirements to agents such as humans, devices, and software. According to Nuseibeh and Easterbrook (2000), Requirements Engineering is the branch of software engineering concerned with the real world goals for, functions of, and constraints on software systems. It is also concerned with the relationship of these factors to precise specifications of software behaviour, and to their evolution over time and across software families. Goal-oriented Requirements Engineering is concerned with the use of goals for eliciting, elaborating, structuring, specifying, analyzing, negotiating, documenting, and modifying requirements. One of the main objectives of Requirements Engineering (RE) is to improve systems modelling and analysis capabilities so that organizations can better understand critical system aspects before they actually build the system. The functional requirements along with quality attributes and other non-functional requirements will constitute the Software Requirements Specification. Functional requirements are the capabilities of the system and domain specific. However, non-functional requirements are constraints on the functional requirements or quality requirements. There are a number of techniques to modelling, representing, and checking requirements. Some of these approaches are; Case-Driven, Viewpoint-Based, Behavioural Pattern Analysis (BPA), Software Architecture Orientation, and Formal Methods approaches.

2 User Groups

The key to successfully using the online voting system is the ability to use the system and access the information available to help. The help facility should be fully functional and able to instruct users through every step while allowing others more versatility in using the web environment. This is achieved by skipping all help functions and proceeding directly to the voting process. Accordingly, users are divided into the following six groups:

1. *Knowledgeable Group*: We believe the more educated the person is, the less likely the help function will be needed and the probability of successfully completing the voting is high.

2. *Frequent Group*: These are users that surf the web frequently for various purposes. In general they perform routine tasks. Most of them have memorized the steps needed to get to the site they need. However, it does not necessarily mean they can use the online voting system without any problem.

3. *Inexperienced Group*: This group of users includes those who use the web very rarely or not at all. They will, most likely, need more assistance and, therefore, need more time in carrying out the voting process. This group of users will have a high number of elderly.

4. *Government Group*: This group will be mainly using the administration functions needed for counting and maintaining the voting data. The group will also be involved with setting up and completing the ballots for regular users.

5. *Technical Group*: This group will be in charge of troubleshooting and maintaining the software, hardware and the network. They will not have access to actual voting data.

6. *Computer and Network Security Group*: As security is essential for such a system, this group will ensure that security is met at the software, hardware, network and physical levels.

3 Problems-Solution Characteristics

There are a number of problems that the online voting solution should address. Among these are::

- Voter secrecy: No one should know what the voter voted
- Voter authentication: Voters should be who they claim they are
- Verifiability of votes: Internal tracking of votes, to ensure every ballot is registered to the voter who submitted it.
- Accuracy of voter turnout. Each voter is tracked to completion, so voter data is available at any time.
- Safe transfer of votes from userôs computer to the server
- Safety of caste votes: Proper security process and user registration can guarantee ballot assurance.
- Uniqueness of casting ï A person can cast only one vote
- Permitting the voter to vote for as many candidates for an office as the voter is lawfully entitled to vote for without exceeding the limit
- Empty ballot box at the start of voting
- Voter should be able to verify the vote before it is cast
- Provision for editing the vote any number of times
- User manuals should be provided for voters several days before election
- Trial version should be released several days before the election
- All server operations, whether operating system function, software functionality or OSI (Open System Interconnection) model functionality, must be protected

The above mentioned problems will give rise to the question of economic benefits of the online voting system (solution). Once the product is released, it should have the following benefits:

(1) If the online voting system is successful, people need not go to the polling booths to cast their votes. They can vote from their home and hence a lot of time will be saved
(2) The existing paper ballot system will be discarded and hence a lot of materials can be saved
(3) Counting the ballots will be executed more accurately, quickly, and consistently
(4) As the existing paper ballot system will be discarded, many resources deployed by the Government will be freed for other purposes
(5) Reports can quickly be generated and hence a lot of manual labour will be saved
The output of a voting system is characterized as good if it is capable of verifying the votes, providing accuracy of the voter turnout to the number of people voted, avoiding coercion, and counting all votes.

4. FUNCTIONAL REQUIREMENTS

Enhancement to the online voting system will primarily provide a more precise vote management tool that will establish accountability and improve data accuracy, and thus allowing voters to feel a greater level of confidence in the reported data. The majority of the precinct managers, who will benefit from these enhancements, currently use their professional judgment and expertise to anticipate the voterôs needs when making decisions. They also rely on outside vendor data and poorly captured metrics from the current state of traditional voting system. Appropriate behaviour constitutes the functionality of a system and there is often a tight correspondence between particular requirements and particular functions of the solution system.

The following represents a partial lit of functional requirements for the Online Voting System:

- The system must provide voters with accurate data
- Metric reports of current/live votes must be provided
- The system should make use of tools available for users on the internet
- It must adhere to government requirements
- Ease of GUI use that can be accessed via web browser must be established
- The system must follow technical development standards supported on known operating systems such as Windows, Linux, and UNIX, in addition to future operating systems versions
- The system must grant technician/customer general communications and training documents
- The system must supply a prototype or process to approve site customization
- Backup data restore capabilities should be granted
- The system must send a notification to administrator if an onsite workstation is classified as inoperative or unusable
- The system should send a notification to administrator of updates from verification popup windows
- The system must supply standard reports for decision making
- Audit trails of who made changes to the database must be maintained
- The system should allow voting administrators to make updates to the voter information database
- The system must verify on a daily basis responsible users ID and location
- The system must provide standard error checking
- The system must provide data integrity checks to ensure data remains consistent and updated

5. MAJOR CONSTRIANTS

When dealing with requirements engineering for any systems, there are some constraints that must be considered. The major constraints for the Online Voting System are:

1. Voting is carried out from many consoles on the internet.
2. All voting is done in one day.
3. Many interfaces exist including Windows Explorer, Netscape, and Mozilla browsers.
4. The operating system in use are, but not limited to, Windows, Linux, and UNIX.

5. Many different levels of expertise in the system use will be prevalent.
6. Each state can administer the system differently depending on state laws.
7. Each state can have unique election and proposals, needing many different administrative interfaces.

6. NONFUNCTIONAL REQUIREMENTS

Nonfunctional requirements are requirements that are not specifically concerned with the functionality of a system. They normally place restrictions on the product being developed and the development process. Nonfunctional requirements may be regarded as parameters of functionality in that they determine how quickly, how accurately, how reliably, how securely, etc., functions must operate. Some of the Online Voting Systemôs nonfunctional requirements are as follows:

- Response and net processing time must be acceptable by user and by application.
- Defects in the local voting database file must be less than a very small positive value, according to the six sigma representation.
- Defects contained in the collection server must be less than a very small positive value, according to the six sigma representation.
- Defects in the master/server database must be less than a very small positive value, according to the six sigma representation.
- Number of collection failures per voting process must be at six sigma, or better.
- When checking the database for errors, a 100% scan of the data is required, rather than selecting a sample set.
- The system must be working at 100% peak efficiency during the voting process.
- Transfer of existing and future data to a Voting Management Data Centre must be granted.
- The system should be allowed to add more voters, to allow a greater connectivity rate.
- A process must be devised to support normal precinct business hours.
- Due to the shortness of the voting timeframe, the system should support response time for addressing severe issues in less than 5 minutes.
- The system should provide documentation to inform users of system functionality and any change to the system.
- The system should provide friendly graphical Interface to ensure ease of use when end users utilize system functionality.

7. SECURITY REQUIREMENTS

Electronic voting systems represent a great security challenge. Any successful attack would be highly visible, and thus, motivating much of the related hacking activity to date. Traditionally, security is incorporated in a software system after all the functional requirements have been addressed. Due to its criticality, security should be integrated in the software life cycle. Voting software security can be achieved if security is merged into voting software functional requirements during the early stages of software requirements engineering. Although, security requirements are non-functional requirements, we deliberately avoided including them within the non-functional requirements due to the crucial role they play in the success of the online

voting system. Below is a partial list of the Online Voting System security requirements.

- The voting system should include controls to prevent deliberate or accidental attempts to replace code such as unbounded arrays and strings
- The system should have zero-tolerance with regard to compromise
- Election process should not be subject to any manipulation including even a single vote manipulation
- The system should provide accurate time and date settings
- The system should not allow improper actions by voters and electoral officials
- The system should not allow Local Election Officials (LEOs) to download votes to infer how voters in their precinct have voted
- The system should provide means for protecting and securing recounts of ballots cast in elections
- The system should not allow voter submissions to be observed or recorded in any way that is traceable to the individual voter
- The system should ensure that election results would be verifiable to independent observers. This implies that published election results correspond to the ballots cast by legitimate voters
- The system should not allow tampering with audit logs

8. DEVELOPING USE-CASES

A use-case tells a stylized story about how an end-user interacts with the system under a specific set of circumstances. The story may be narrative text, an outline of tasks or interactions, a template-based description, or a diagrammatic representation. Regardless of its form, a use-case depicts the system from the end-userôs point of view. Examples of use cases for the Online Voting System are given below.

USE CASE 1: **Voting**

Actor: Any person that is allowed to vote

Goal: To cast their votes in a safe and secure manner.

Preconditions: The process is password protected.

The voter must know her/his PIN, without which they cannot vote.

Scenario:

1. The voter enters the website address in his browser.
2. The voter selects the state to which he/she belongs.
3. The user is allowed to have a look at the tutorial section which is optional.
4. The voter enters the Name, SSN, State ID, Date of Birth, and Gender.
5. If the input of the voter matches the records, he/she is allowed to login.
6. The voter is allowed to choose one of two options: Party Selection or Individual Selection.
7. The voter casts her/his vote to the favourite choice under a selection.
8. The voter navigates to all the pages and votes to his/her choice under each category.
9. The voter checks the final screen of the vote.
10. The voter is allowed to edit his/her vote any number of times.
11. If she/he is satisfied with the final vote screen, he/she casts the vote.
12. If the vote reaches the server, a message is displayed to the voter that his vote has reached the ballot.

13. The voter logs out.

Exceptions:
1. The voter may enter the wrong details.
2. The voter might try to select options more than the allowable ones.
3. The voterôs connection with the server may terminate before the vote reaches the server.
4. The voterôs connection with the server may terminate in the course of the session.
5. After the vote is cast, the voter may try to navigate back to cast another vote.

Event:
If the voter is not identified in three attempts, the process stops and the voter needs to contact the election conducting authority to restart the process.

Frequency:
Used as many number of times as there are voters.
Secondary Actors: Election conducting staff who are contacted by voters in case of difficulties.

USE CASE 2: **Configuration**
Actor: Configurator **(**usually an authorized person of the election commission).
Goal: To configure the voting system by entering the offices for which voting is to be done and configuring the candidates for the offices.
Preconditions: There are no preconditions while installing.

Scenario:
1. The actor clicks the button ñConfigure.ò
2. The actor clicks either ñSingle Configurationò or ñMultiple Configurationò button based on whether the election is held for a single province or a multiple province.
3. If the ñMultiple Configurationò button is pressed, the actor is prompted to enter the common offices and the offices that are specific to that province.
4. The actor enters the criteria based on which provinces are distinguished.
5. The actor is allowed to add a new office or edit an existing office by pressing ñAdd New Officeò or ñEdit Existingò button respectively.
6. The name of the office and the number of candidates for that office are entered.
7. The actor clicks the next button which allows him/her to enter the name of the candidates and the party to which they belong.

Exceptions: There are no exceptions.
Frequency: Usually once.
Secondary Actors: Software staff.

Self Assessment Exercise
List and explain some Online Voting System security requirements.

4.0 Conclusion
Voting might look like a suitable or perfect choice for computer applications, but in reality implementing it is harder than it first appears. Many comments have been made by computer professionals and voting officials on electronic voting systems

advantages and disadvantages with a special emphasis on their security. We have attempted to tackle the problem of representing stakeholdersô needs for an online voting system. Essential functional requirements, that lay the basis for the system design phase, have been stated. These were supported by nonfunctional requirements including security requirements. The Requirements Engineering for E-Voting should be flaw-free. It is our belief that flaws in an online voting system will result in failure of the voting system which will jeopardize democracy and disappoint voters.

5.0 Summary

Manual voting systems have been deployed for many years with enormous success. If those systems were to be replaced with Electronic Voting Systems, we have to be absolutely sure that they will perform at least as efficient as the traditional voting systems. Failures or flaws in Online Voting Systems will jeopardize Democracy in the country implementing them. The main focus of requirements engineering is on defining and describing what a software system should do to satisfy the informal requirements provided by a statement of need. In this unit, we have defined and describe what the Online Voting System should do to ensure a robust, accurate, secure and quality-based design and implementation.

6.0 Tutor Marked Assignment

Define and describe what the Online Voting System should do to ensure a robust, accurate, secure and quality-based design and implementation.

.

7.0 References/ Further Reading

(1) Baudron, O., Fouque P., Pointchevel, D., Stern, J. and Poupard, G. (2001). ñPractical Multi-Candidate Election System,ò In Proc. The Twentieth Annual ACM Symposium on Principles of Distributed Computing, Rhode Island, USA, pp. 274 - 283.

(2) Bray, I. (2002). An Introduction to Requirement Engineering. Harlow Essex: Addison Wesley,

(3) Breyfogle, F. (1999). Implementing Six Sigma: Smarter Solutions Using Statistical Methods, Wiley.

(4) Daimi, K. and Wilson, C. (2005), ñElectronic Voting System Security requirements Engineering,ò in Proc. The International Conference on Software Engineering Research and Practice Las Vegas, USA, pp. 230-235.

(5) El-Ansary, A. (2002). ñBehavioural Pattern Analysis: Towards a New Representation of Systems Requirements Based on Actions and Events,ò In Proc: SAC, pp.984-991.

(6) Gilliam, D. P., Wolfe, T. L. Sherif, J. S. and Bishop, M. (2003). ñSoftware Security Checklist for the Software Life Cycle,ò in Proc. WETICEô03, pp. 243-248.

(7) Hausmann, J. H., Heckel, R. and Taentzer,, G. (2002). ñDetection of Conflicting Functional Requirements in a Use Case-Driven Approach,ò In Proc: ICSEô02, pp. 105-115.

(8) Nuseibeh, B. and Easterbrook, S. (2000), ñRequirements Engineering: A Roadmap,ò In Proc. The International Conference on Future of Software Engineering. Pp. 35-46.

(9) Peters, J. and Pedrycz, W. (2000). Software Engineering ï An Engineering Approach. New York, NY: Wiley.

(10) Pressman, R. S. (2005). Software Engineering: A Practitionerôs Approach. New York NY: Addison Wesley.

(11) Raksin, J. (2004). ñThe GIGO Principle and Voting Machine,ò ACM QUEUE, Vol. 2, No. 2, pp. 10-11, April.

(12) Rubin, A. D. (2002). ñSecurity Considerations for Remote Electronic Voting,ò CACM, Vol. 45, Pp. 39-44.

(13) Schneier, B. (2004). ñVoting Security and Technology,ò IEEE Security & Privacy, Vol. 2, No. 1, pp 10-10, Jan.

(14) Van Der Poll, J. and Kotzé, P. (2003). ñCombining UCMs and Formal Methods for Representing and Checking the Validity of Scenarios as User Requirements,ò In Proc: SAICSIT, pp. 59-68.

UNIT 4

The Economics of Information Security

Content

1.0 Introduction

Over the past 10 years, people have realized that security failure is caused at least as often by bad incentives as by bad design. Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail. The growing use of security mechanisms to enable one system user to exert power over another user, rather than simply to exclude people who should not be users at all, introduces many strategic and policy issues. The tools and concepts of game theory and microeconomic theory are becoming just as important as the mathematics of cryptography to the security engineer. The difficulty in measuring information security risks presents another challenge: These risks cannot be managed better until they can be measured better. Insecure software dominates the market for the simple reason that most users cannot distinguish it from secure software; thus, developers are not compensated for costly efforts to strengthen their code. However, markets for vulnerabilities can be used to quantify software security, thereby rewarding good programming practices and punishing bad ones. Insuring against attacks could also provide metrics by building a pool of data for valuing risks. However, local and global correlations exhibited by different attack types largely determine what sort of insurance markets are feasible. Information security mechanisms or failures can create, destroy, or distort other markets; digital rights management (DRM) in online music and commodity software markets provides a topical example. Economic factors also explain many challenges to personal privacy. Discriminatory pricing which is economically efficient but socially controversial is simultaneously made more attractive to merchants and easier to implement because of technological advances. We conclude by discussing a fledgling research effort: examining the security impact of network structure on interactions, reliability, and robustness.

2.0 Objectives

Our goal in this unit is to present several promising applications of economic theories and ideas to practical information security problems. Considered are the misaligned incentives in the design and deployment of computer systems. Next, is to examine the impact of externalities on information security knowing the fact that network insecurity is somewhat like air pollution or traffic congestion, in that people who

connect insecure machines to the Internet do not bear the full consequences of their actions.

3.0 Main body

3.1 Misaligned Incentives

One of the observations that drove initial interest in information security economics came from banking. In the United States, banks are generally liable for the costs of card fraud; when a customer disputes a transaction, the bank either must show that the customer is trying to cheat or must offer a refund. In the United Kingdom, the banks had a much easier ride: They generally got away with claiming that their automated teller machine (ATM) system was ósecure,ô so a customer who complained must be mistaken or lying. óLucky bankers,ô one might think; yet UK banks spent more on security and suffered more fraud. How could this be? It appears to have been what economists call a moral hazard effect. Legal theorists have long known that liability should be assigned to the party that can best manage the risk. Yet everywhere we look, we see online risks allocated poorly, resulting in privacy failures and protracted regulatory tussles. For instance, medical records systems are bought by hospital directors and insurance companies, whose interests in account management, cost control, and research are not well aligned with the patientsô interests in privacy. Incentives can also influence attack and defence strategies. In economic theory, a hidden action problem arises when two parties wish to transact but one party can take unobservable actions that affect the outcome. The classic example comes from insurance, where the insured party may behave recklessly (increasing the likelihood of a claim) because the insurance company cannot observe his or her behaviour. We can use such economic concepts to classify computer security problems. Routers can quietly drop selected packets or falsify responses to routing requests; nodes can redirect network traffic to eavesdrop on conversations; and players in file-sharing systems can hide whether they have chosen to share with others, so some may ófree-rideô rather than help to sustain the system. In such hidden-action attacks, some nodes can hide malicious or antisocial behaviour from others. Once the problem is seen in this light, designers can structure interactions to minimize the capacity for hidden action or to make it easy to enforce suitable contracts.

First, a system structured as an association of clubs reduces the potential for hidden action; club members are more likely to be able to assess correctly which members are contributing. Second, clubs might have quite divergent interests. Although peer-to-peer systems are now thought of as mechanisms for sharing music, early systems were designed for censorship resistance. A system might serve a number of quite different groups maybe Chinese dissidents, critics of Scientology, or aficionados of sadomasochistic imagery that is legal in California but banned in Tennessee. Early peer-to-peer systems required such users to serve each otherôs files, so that they ended up protecting each otherôs free speech. One question to consider is whether such groups might not fight harder to defend their own colleagues, rather than people involved in struggles in which they had no interest and where they might even be disposed to side with the censor. Danezis and Anderson introduced the Red-Blue model to analyze this phenomenon. Each node has a preference among resource types for instance, left-leaning versus right leaning political manuscripts whereas a censor who attacks the network will try to impose a particular preference, thereby meeting the approval of some nodes but not others. The model proceeds as a multi-round game

in which nodes set defence budgets that affect the probability that they will defeat or be overwhelmed by the censor. Under reasonable assumptions, the authors show that diversity (where each node stores its preferred resource mix) performs better under attack than does solidarity (where each node stores the same resource mix, which is not usually its preference). Diversity makes nodes willing to allocate higher defence budgets; the greater the diversity, the more quickly solidarity will crumble in the face of attack.

3.2 Security as an Externality

Information industries are characterized by many different types of externalities, where individualsô actions have side effects on others. The software industry tends toward dominant firms, thanks in large part to the benefits of interoperability. Economists call this a network externality: A larger network, or a community of software users, is more valuable to each of its members. Selecting an operating system depends not only on its features and performance but also on the number of other people who have already made the same choice; for example, more third-party software is available for more popular platforms. This not only helps to explain the rise and dominance of operating systems, from System/360 through Windows to Symbian, and of music platforms such as iTunes; it also helps to explain the typical pattern of security flaws. Put simply, while a platform vendor is building market dominance, it must appeal to vendors of complementary products as well as to its direct customers; not only does this divert energy that might be spent on securing the platform, but security could get in the way by making life harder for the complementers. So platform vendors commonly ignore security in the beginning, as they are building their market position; later, once they have captured a lucrative market, they add excessive security in order to lock their customers in tightly. Further externalities can be found when we analyze security investment, as protection often depends on the efforts of many principals. Budgets generally depend on the manner in which individualsô investments translate to outcomes, but the impact of security investment often depends not only on the investorôs own decisions but also on the decisions of others. Consider a medieval city. If the main threat is a siege, and each family is responsible for maintaining and guarding one stretch of the wall, then the cityôs security will depend on the efforts of the laziest and most cowardly family. If, however, disputes are settled by single combat between champions, then its security depends on the strength and courage of its most valiant knight. But if wars are a matter of attrition, then it is the sum of all the citizensô efforts that matters.

System reliability is no different; it can depend on the sum of individual efforts, the minimum effort anyone makes, or the maximum effort anyone makes. Program correctness can depend on minimum effort (the most careless programmer introducing a vulnerability), whereas software validation and vulnerability testing might depend on the sum of everyoneôs efforts. There can also be cases where security depends on the best effort the actions taken by an individual champion. A simple model by Varian (2004) provides interesting results when players choose their effort levels independently. Each playerôs cost is the effort expended in defence, whereas the expected benefit to players is the probability that the system avoids failure. When this probability is a function of the sum of individual efforts, system reliability depends on the agent with the highest benefit-cost ratio, and all other agentsô free-ride.

In the minimum-effort case, the agent with the lowest benefit-cost ratio dominates. As more agents are added, systems become increasingly reliable in the total-effort case but increasingly unreliable in the weakest-link case. What are the implications? One is that software companies should hire more software testers and fewer (but more competent) programmers. Work such as this has inspired other researchers to consider interdependent risk. A recent influential model by Kunreuther and Heal (2003) notes that security investments can be strategic complements: An individual taking protective measures creates positive externalities for others that in turn may discourage their own investment. This result has implications far beyond information security. The decision by one apartment owner to install a sprinkler system that minimizes the risk of fire damage will affect the decisions of his neighbours; airlines may decide not to screen luggage transferred from other carriers that are believed to be careful with security; and people thinking of vaccinating their children against a contagious disease may choose to free-ride off the herd immunity instead. In each case, several widely varying equilibrium outcomes are possible, from complete adoption to total refusal, depending on the levels of coordination between principals.

Katz and Shapiro (1985); famously analyzed how network externalities influence the adoption of technology: they lead to the classical S-shaped adoption curve, in which slow early adoption gives way to rapid deployment once the number of users reaches some critical mass. Network effects can also influence the initial deployment of security technology. The benefit that a protection technology provides may depend on the number of users that adopt it. The cost may be greater than the benefit until a minimum number of players adopt; if everyone waits for others to go first, the technology never gets deployed. Ozment and Schechter in 2006 analyzed different approaches for overcoming such bootstrapping problems. This challenge is particularly topical. A number of core Internet protocols, such as DNS and routing, are considered insecure. More secure protocols exist (e.g., DNSSEC, SBGP); the challenge is to get them adopted. Two security protocols that have already been widely deployed, SSH and IPsec, both overcame the bootstrapping problem by providing adopting firms with internal benefits. Thus, adoption could be done one firm at a time, rather than needing most organizations to move at once. The deployment of fax machines also occurred through this mechanism: Companies initially bought fax machines to connect their own offices.

3.3 Economics of Vulnerabilities

There has been a vigorous debate between software vendors and security researchers over whether actively seeking and disclosing vulnerabilities is socially desirable. Rescorla (2004), has argued that for software with many latent vulnerabilities (e.g., Windows), removing one bug makes little difference to the likelihood of an attacker finding another one later. Because exploits are often based on vulnerabilities inferred from patches or security advisories, he argued against disclosure and frequent patching unless the same vulnerabilities are likely to be rediscovered later. Ozment found that for FreeBSD, a popular UNIX operating system that forms the core of Apple OS X, vulnerabilities are indeed likely to be rediscovered. Ozment and Schechter (2006) also found that the rate at which unique vulnerabilities were disclosed for the core and unchanged FreeBSD operating system has decreased over a 6-year period. These findings suggest that vulnerability disclosure can improve system security over the long term. Vulnerability disclosure also helps to give vendors an incentive to fix bugs in subsequent product releases. Arora et al. (2004) have

shown through quantitative analysis that public disclosure made vendors respond with fixes more quickly; the number of attacks increased, but the number of reported vulnerabilities declined over time. This discussion raises a more fundamental question: Why do so many vulnerabilities exist in the first place? Surely, if companies want secure products, then secure software will dominate the marketplace. But experience tells us that this is not the case; most commercial software contains design and implementation flaws that could have easily been prevented. Although vendors are capable of creating more secure software, the economics of the software industry provide them with little incentive to do so. In many markets, the attitude of óship it Tuesday and get it right by version 3ô is perfectly rational behaviour. Consumers generally reward vendors for adding features, for being first to market, or for being dominant in an existing market and especially so in platform markets with network externalities. These motivations clash with the task of writing more secure software, which requires time-consuming testing and a focus on simplicity.

Another aspect of vendorsô lack of motivation is that the software market is a ómarket for lemonsô. In a Nobel prizewinning work, economist George Akerlof (1970) employed the used car market as a metaphor for a market with asymmetric information. He imagined a town in which 50 good used cars (worth $2000 each) are for sale, along with 50 ólemonsô (worth $1000 each). The sellers know the difference but the buyers do not. What will be the market-clearing price? One might initially think $1500, but at that price no one with a good car will offer it for sale, so the market price will quickly end up near $1000. Because buyers are unwilling to pay a premium for quality they cannot measure, only low-quality used cars are available for sale. The software market suffers from the same information asymmetry. Vendors may make claims about the security of their products, but buyers have no reason to trust them. In many cases, even the vendor does not know how secure its software is. So buyers have no reason to pay more for protection, and vendors are disinclined to invest in it. How can this be tackled? There are two developing approaches to obtaining accurate measures of software security: vulnerability markets and insurance. Vulnerability markets help buyers and sellers to establish the actual cost of finding vulnerability in software, which is a reasonable proxy for software security. Originally, some standards specified a minimum cost of various kinds of technical compromise; one example is banking standards for point-of-sale terminals. Then Schechter (2004); proposed open markets for reports of previously undiscovered vulnerabilities. Two firms, iDefense and Tipping Point, are now openly buying vulnerabilities, so a market actually exists (unfortunately, the prices are not published). Their business model is to provide vulnerability data simultaneously to their customers and to the vendor of the affected product, so that their customers can update their firewalls before anyone else. However, the incentives in this model are suboptimal: Bug-market organizations might increase the value of their product by leaking vulnerability information to harm non-subscribers.

Several variations on vulnerability markets have been proposed. Bhme (2006) has argued that software derivatives are a better tool than markets for the measurement of software security. Here, security professionals can reach a price consensus on the level of security for a product. Contracts for software could be issued in pairs; the first pays a fixed value if no vulnerability is found in a program by a specific date, and the second pays another value if vulnerabilities are found. If these contracts can be traded, then their price will reflect the consensus on the program. Software vendors, software

company investors, and insurance companies could use such derivatives to hedge risks. A third possibility, offered by Ozment (2004), is to design a vulnerability market as an auction. One criticism of all market-based approaches is that they might increase the number of identified vulnerabilities by compensating people who would otherwise not search for flaws. Thus, some care must be exercised in designing them. An alternative approach is to rely on insurers. The argument is that underwriters assign premiums based on a firmôs information technology (IT) infrastructure and the processes by which it is managed. Their assessment may result in advice on best practice and, over the long run; they amass a pool of data by which they can value risks more accurately. Right now, however, the cyber-insurance market is both underdeveloped and underused.

Why could this be? One reason, according to Bhme and Kataria (2006), is the problem of interdependent risk, which takes at least two forms. A firmôs IT infrastructure is connected to other entities, so its efforts may be undermined by failures elsewhere. Cyber-attacks also often exploit vulnerability in a system used by many firms. This interdependence makes certain cyber risks un-attractive to insurers particularly those where the risk is globally rather than locally correlated, such as worm and virus attacks, and systemic risks such as Y2K. Many writers have called for software risks to be transferred to the vendors; but if this were the law, it is unlikely that Microsoft would be able to buy insurance. So far, vendors have succeeded in dumping most software risks, but this outcome is also far from being socially optimal. Even at the level of customer firms, correlated risk makes firms under-invest in both security technology and cyber-insurance. Insurance companies must charge higher premiums, so cyber-insurance markets lack the volume and liquidity to become efficient. Insurance is not the only market affected by information security. Some very high-profile debates have centred on DRM; record companies have pushed for years for DRM to be incorporated into computers and consumer electronics, whereas digital-rights activists have opposed them. What light can security economics shed on this debate?

Varian presented a surprising result in January 2005: that stronger DRM would help system vendors more than it would help the music industry, because the computer industry is more concentrated (with only three serious suppliers of DRM platforms: Microsoft, Sony, and the dominant firm, Apple). The content industry scoffed, but by the end of 2005 music publishers were protesting that Apple was getting an unreasonably large share of the cash from online music sales. As power in the supply chain moved from the music majors to the platform vendors, so power in the music industry appears to be shifting from the majors to the independents, just as airline deregulation has favoured aircraft makers and low-cost airlines. This is a striking demonstration of the predictive power of economic analysis. There are other interesting market failures. Recently, for example, a number of organizations have set up certification services to vouch for the quality of software products or Web sites. The aim has been twofold: to overcome public wariness about electronic commerce, and by self-regulation to forestall more expensive regulation by the government But certification markets can easily be ruined by a race to the bottom; dubious companies are more likely to buy certificates than reputable ones, and even ordinary companies may shop around for the easiest deal. Edelman (2005) has shown that such óadverse selectionô is really happening: Whereas some 3% of Web sites are malicious, some 8% of Web sites with certification from one large vendor are malicious. He also

discovered inconsistencies between ordinary Web search results and those from paid advertising: Where as 2.73% of companies ranked at the top in a Web search were bad, 4.44% of companies who had bought ads from the search engine were bad. His conclusion: ódonôt click on ads.ô

3.4 Economics of Privacy

The persistent erosion of personal privacy with advances in technology has frustrated policy people and practitioners alike. Privacy-enhancing technologies have been offered for sale, yet most have failed in the marketplace. Again, economics explains this better than technical factors do. Odlyzko (2003) has argued that privacy erosion is a consequence of the desire to charge different prices for similar services. Technology is increasing both the incentives and the opportunities for discriminatory pricing. Companies can mine online purchases and interactions for data revealing individualsô willingness to pay. The results are the complex and ever-changing prices charged for such commodities as airline seats, software, and telecommunications services. Such differential pricing is economically efficient but is increasingly resented. Acquisti and Varian (2005) analyzed the market conditions under which first-degree price discrimination can actually be profitable: It may thrive in industries with wide variation in consumer valuation for services, where personalized services can be supplied with low marginal costs, and where repeated purchases are likely. So much for the factors, that make privacy intrusions more likely. What factors make them less so? Campbell et al. found that the stock price of companies reporting a security breach is more likely to fall if the breach leaked confidential information. Acquisti et al (2006) conducted a similar analysis for privacy breaches. Their initial results are less conclusive but still point to a negative impact on stock price, followed by an eventual recovery. Incentives also affect the detailed design of privacy technology. Anonymity systems depend heavily on network externalities: Additional users provide cover traffic necessary to hide usersô activities from an observer. This fact has been recognized by some developers of anonymity systems (Dingledine and Matthewson, 2006). As a result, some successful applications anonymize Web traffic, emphasize usability to increase adoption rates.

3.5 Network Topology and Information Security

The topology of complex networks is an emerging tool for analyzing information security. Computer networks from the Internet to decentralized peer-to-peer networks are complex but emerge from ad hoc interactions of many entities using simple ground rules. This emergent complexity, coupled with heterogeneity, is similar to social networks and even to the metabolic pathways in living organisms. Recently a discipline of network analysis has emerged at the boundary between sociology and condensed-matter physics. It takes ideas from other disciplines, such as graph theory, and in turn provides tools for modelling and investigating such networks for a recent survey). The interaction of network science with information security provides an interesting bridge to evolutionary game theory, a branch of economics that has been very influential in the study of human and animal behaviour. Network topology can strongly influence conflict dynamics. Often an attacker tries to disconnect a network or increase its diameter by destroying nodes or edges while the defender counters with various resilience mechanisms. Examples include a music industry body attempting to close down a peer-to-peer file-sharing network, a police force trying to decapitate a terrorist organization, and a totalitarian government conducting surveillance on political activists. Police forces have been curious for some years about whether network science might be of practical use in covert conflicts, either to insurgency or

to counterinsurgency forces. Different topologies have different robustness properties with respect to various attacks. Albert et al. showed that certain real-world networks with scale-free degree distributions are more robust to random attacks than to targeted attacks. This is because scale-free networks, like many real-world networks, get much of their connectivity from a minority of nodes that have a high vertex order. This resilience makes them highly robust against random upsets, but if the ókingpinô nodes are removed, connectivity collapses.

The static case of this model is exemplified by a police force that becomes aware of a criminal or terrorist network and sets out to disrupt it by finding and arresting its key people. Nagaraja and Anderson recently extended the model to the dynamic case, in which the attacker can remove a certain number of nodes at each round and the defenders then recruit other nodes to replace them. Using multi-round simulations to study how attack and defence interact, they found that formation of localized clique structures at key network points worked reasonably well, whereas defences based on rings did not work well at all. This helps to explain why peer-to-peer systems with ring architectures turned out to be rather fragile and also why revolutionaries have tended to organize themselves in cells.

Self Assessment Exercise
Discuss the economics of information security

4.0 Conclusion

Over the past few years, a research program on the economics of security has built many cross-disciplinary links and has produced many useful (and indeed delightful) insights from unexpected places. Many perverse aspects of information security that had long been known to practitioners but were dismissed as ógood weatherô have turned out to be quite explicable in terms of the incentives facing individuals and organizations, and in terms of different kinds of market failure. As for the future, the work of the hundred or so researchers active in this field has started to spill over and the effect is enormous.

5.0 Summary

The economics of information security has recently become a thriving and fast moving discipline. As distributed systems are assembled from machines belonging to principals with divergent interests, we find that incentives are becoming as important as technical design in achieving dependability. The new field provides valuable insights not just into ósecurityô topics (such as bugs, spam, phishing, and law enforcement strategy) but into more general areas such as the design of peer-to-peer systems, the optimal balance of effort by programmers and testers, why privacy gets eroded, and the politics of digital rights management.

6.0 Tutor Marked Assignment

Define and explain the term Security as an Externality.

7.0 References/ Further Reading

(1) Acquisti A. and Varian. H. (2005). Conditioning prices on purchase history. In Marketing Science Vol. 2. 43-67.

(2) Akerlof., G. A. (1970).The market for ólemonsô: quality uncertainty and the market mechanism. In Quarterly Journal of Economics 84, 488.

(3) Campbell, K. L., Gordon, A., Loeb, M. P. and Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. In Journal of Computer. Security. 11, 431-439. http://www.dtc.umn.edu/weis2004.econinfosec.org/docs/46.pdf. Retrieved 14.02/10.

(4) Kannan, K. and Telang. R. (2004), Economic analysis of market for software vulnerabilities. In Third Workshop on the Economics of Information Security http://www.dtc.umn.edu/weis2004/kannan-telang.pdf. Retrieved 14/02/10.

(5) Katz M. L., and Shapiro. C. (1985). Network externalities, competition, and compatibility. In The American Economic Review 75, 424

(6) Kunreuther, H. and Heal, G. (2003). Interdependent security. In Journal of Risk and Uncertainty 26, 231

(7) Odlyzko. A. (2003). Privacy, economics and price discrimination on the internet. In Fifth Intôl. Conference on Electronic Commerce (ACM Press, New York, NY, USA,

(8) Ogut, H., Menon, N. and Raghunathan, S. (2005). Cyber insurance and IT security investment: impact of interdependent risk. In Fourth Workshop on the Economics of Information Security http://www.infosecon.net/workshop/pdf/56.pdf.

(9) Ohme R. B¨ and Kataria. G. (2006). Models and measures for correlation in cyber-insurance. In Fifth Workshop on the Economics of Information Security on the Economics of Information Security http://www.dtc.umn.edu/weis2004/ozment.pdf. Retrieved 14/02/10.

(10) Ohme, R. B (2006). A comparison of market approaches to software vulnerability disclosure. In ETRICS. Springer Verlag, Pp. 298-311. LNCS 2995.

(11) Ozment A. and Schechter. S. E. (2006). Bootstrapping the adoption of internet security protocols. In Fifth Workshop on the Economics of Information Security http://weis2006.econinfosec.org/docs/46.pdf. Retrieved 14.02/10.

(12) Ozment, A. (2004). Bug auctions; vulnerability markets reconsidered. In Third Workshop Pp. 355-366.

(13) Rescorla. E. (2004), Is finding security holes a good idea? In Third Workshop on the Economics of Information Security http://www.dtc.umn.edu/weis2004/rescorla.pdf. Retrieved 14.02/10.

(14) Schechter. S. E. (2004). Computer security strength and risk: a quantitative approach, Ph.D. thesis, Harvard University.

(15) Varian. H. (2004). System reliability and free riding. In Economics of Information Security, L. J. Camp, S. Lewis, eds. (Kluwer Academic Publishers, vol. 12 of Advances in Information Security, pp. 1-15. http://weis2006.econinfosec.org/docs/16.pdf. Retrieved 14/02/10.

UNIT 5
Hard Nature of Information Security

Content

1.0 Introduction

In a survey of fraud against auto-teller machines, it was found that patterns of fraud depended on who was liable for them. In the USA, if a customer disputed a transaction, the onus was on the bank to prove that the customer was mistaken or lying; this gave US banks a motive to protect their systems properly. But in Britain, Norway and the Netherlands, the burden of proof lay on the customer: the bank was right un- less the customer could prove it wrong. Since this was almost impossible, the banks in these countries became careless. Eventually, epidemics of fraud demolished their complacency. US banks, meanwhile, suffered much less fraud; although they actually spent less money on security than their European counter-parts, they spent it more effectively (Anderson, 1994). There are many other examples. Medical payment systems that are made for insurers rather then by hospitals fail to protect patient privacy whenever this conflicts with the insurer's wish to collect information about its clients. Digital signature laws transfer the risk of forged signatures from the bank that relies on the signature (and that built the system) to the person alleged to have made the signature. Common Criteria evaluations are not made by the relying party, as Orange Book evaluations were, but by a commercial facility paid by the vendor. In general, where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected.

A different kind of incentive failure surfaced in early 2000, with distributed denial of service attacks against a number of high-profile web sites. These exploit a number of subverted machines to launch a large coordinated packet flood at a target. Since many of them flood the victim at the same time, the traffic is more than the target can cope with, and because it comes from many different sources, it can be very difficult to stop. Varian (2000) pointed out that this was also a case of incentive failure. While individual computer users might be happy to spend $100 on anti-virus software to protect themselves against attack, they are unlikely to spend even $1 on software to prevent their machines being used to attack Amazon or Microsoft. This is an example of what economists refer to as the `Tragedy of the Commons'. If a hundred peasants graze their sheep on the village common, then whenever another sheep is added its owner gets almost the full benefit - while the other ninety-nine suffer only a small decline in the quality of the grazing. So they aren't motivated to object, but rather to add another sheep of their own and get as much of the grazing as they can. The result is a dustbowl; and the solution is regulatory rather than technical. A typical tenth-

century Saxon village had community mechanisms to deal with this problem; the world of computer security still doesn't. Varian's proposal is that the costs of distributed denial-of-service attacks should fall on the operators of the networks from which the flooding traffic originates; they can then exert pressure on their users to install suitable defensive software, or, for that matter, supply it themselves as part of the subscription package. These observations prompted us to look for other ways in which economics and computer security interact.

2.0 Objectives

Information insecurity is at least as much due to perverse incentives. Thus this study seeks to explain many of the problems facing electronic security more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons.

3.0 Main body

1 Network Externalities

Economists have devoted much effort to the study of networks such as those operated by phone companies, airlines and credit card companies. The more people use a typical network, the more valuable it becomes. The more people use the phone system -or the Internet - more people there are to talk to and so the more useful it is to each user. This is sometimes referred to as *Metcalfe's law*, and is not limited to communication systems. The more merchants take credit cards, the more useful they are to customers, and so the more customers will buy them; and the more customers have them, the more merchants will want to accept them. So while that net- works can grow very slowly at first - credit cards took almost two decades to take off - once positive feed-back gets established, they can grow very rapidly. The telegraph, the telephone, the fax machine and most recently the Internet have all followed this model. As well as these physical networks, the same principles apply to virtual networks, such as the community of users of mass-market software architecture. When software developers started to believe that the PC would outsell the Mac, they started developing their products for the PC first, and for the Mac only later (if at all). This effect was reinforced by the fact that the PC was easier for developers to work with. The growing volume of software available for the PC but not the Mac made customers more likely to buy a PC than a Mac, and the resulting positive feedback squeezed the Mac out of most markets.

A similar effect made Microsoft Word the dominant word processor. For our present purposes, here are three particularly important features of information technology markets.

- First, the value of a product to a user depends on how many other users adopt it.

- Second, technology often has high fixed costs and low marginal costs. The first copy of a chip or software package may cost millions, but subsequent copies may cost very little to manufacture. This is not unique to information markets; it's also seen in business sectors such as airlines and hotels. In all such sectors, pure price competition tends to drive revenues steadily down towards he marginal cost of production (which in the case of information is zero). So businesses need ways of selling on value rather than on cost.

- Third, there are often large costs to users from switching technologies, which leads to lock-in. Such markets may remain very profitable, even here (incompatible) competitors are very cheap to produce. In fact, one of the main results of network economic theory is that the net presented value of the customer base should equal the total costs of their switching their business to a competitor.

All three of these effects tend to lead to "winners take all" market structures with dominant firms. So it is extremely important to get into markets quickly. Once in, a vendor will try to appeal to complementary suppliers, as with the software vendors whose bandwagon effect carried Microsoft to victory over others. In fact, successful networks tend to appeal to complementary suppliers even more than to users: the potential creators of \killer apps" need to be courted. Once the customers have a substantial investment in complementary assets, they will be locked in. These network effects have significant consequences for the security engineer, and consequences that are often misunderstood or misattributed. Consultants often explain that the reason a design broke for which they were responsible was that the circumstances were impossible. It is important to realize that this is not just management stupidity.

Another common complaint is that software platforms are shipped with little or no security support, as with Windows 95/98; and even where access control mechanisms are supplied, as with Windows NT, they are easy for application developers to bypass. In fact, the access controls in Windows NT are often irrelevant, as most applications either run with administrator privilege (or, equivalently, require dangerously powerful operating system services to be enabled). This is also explained simply from the viewpoint of network economics: mandatory security would subtract value, as it would make life more difficult for the application developers. Indeed, it has been observed that much of the lack of user-friendliness of both Microsoft software and the Internet is due to the fact that both Microsoft and the Internet achieved success by appealing to developers. The support costs that Microsoft dumps on users - and in fact even the cost of the time wasted waiting for PCs to boot up and shut down - greatly exceed its turnover. Network owners and builders will also appeal to the developers of the next generation of applications by arranging for the bulk of the support costs to fall on users rather than developers, even if this makes effective security administration impractical. One reason for the current appeal of public key cryptography may be that it can simplify development - even at the cost of placing an unreasonable administrative burden on users who are neither able nor willing to undertake it. The technical way to try to fix this problem is to make security administration more `user-friendly' or `plug-and-play'; many attempts in this direction have met with mixed success. The more subtle approach is to try to construct an authentication system whose operators benefit from network effects; this is what Microsoft Passport does, and we'll discuss it further below. In passing, it is worth mentioning that (thanks to distributed denial of service attacks) the economic aspects of security failure are starting to get noticed by government. A recent EU proposal recommends action by governments in response to market imperfections, where market prices do not accurately reflect the costs and benefits of improved network security (European Union; 2001).

2. Competitive Applications and Corporate Warfare

Network economics has many other effects on security engineering. Rather than using a standard, well analyzed and tested architecture, companies often go for a proprietary obscure one to increase customer lock-in and increase the investment that competitors have to make to create compatible products. Where possible, they will use patented algorithms (even if these are not much good) as a means of imposing licensing conditions on manufacturers. For example, the DVD Content Scrambling System was used as a means of insisting that manufacturers of compatible equipment signed up to a whole list of copyright protection measures. This may have come under severe pressure, as it could prevent the Linux operating system from running on next-generation PCs; but efforts to foist non-open standards continue in many applications from SDMI and CPRM to completely proprietary systems such as games consoles. A very common objective is differentiated pricing. This is usually critical to firms that price a product or service not to its cost but to its value to the customer.

Another business strategy is to manipulate switching costs. Incumbents try to increase the cost of switching, whether by indirect methods such as con- trolling marketing channels and building industries of complementary suppliers, or, increasingly, by direct methods such as making systems compatible and hard to reverse engineer. Meanwhile competitors try o do the reverse: they look for ways to reuse the base of complementary products and services, and to reverse engineer whatever protection the incumbent builds in. This extends to the control of complementary vendors, sometimes using technical mechanisms. Sometime, security mechanisms have both product differentiation and higher switching costs as goals. An example which may become politicized is `accessory control'. According to one company that sells authentication chips into the automative market, some printer companies have begun to embed cryptographic authentication protocols in laser printers to ensure that genuine toner cartridges are used. If a competitor's cartridge is loaded instead, the printer will quietly downgrade from 1200 dpi to 300 dpi. In mobile hones, much of the profit is made on batteries, and authentication can be used to spot competitors' products so they can be drained more quickly. Another example comes from Microsoft Passport. This is a system whose ostensible purpose is single signon: a Passport user doesn't have to think up sep- rate passwords for each participating web site, with the attendant hassle and risk. Instead, sites that use Passport share a central authentication server run by Microsoft to which users log on. They use web redirection to connect their Passport-carrying visitors to this server; authentication requests and responses are passed back and forth by the user's browser in encrypted cookies. So far, so good. but the real functions of Passport are somewhat more subtle.

First, by patching itself into all the web transactions of participating sites, Microsoft can collect a huge amount of data about online shopping habits and enable participants to swap it. If every site can exchange data with every other site, then the value of the network to each participating web site rows with the number of sites, and there is a strong network externality. So one such network may come o dominate, and Microsoft hopes to own it.

Second, the authentication protocols used between the merchant servers and the Passport server are proprietary variants of Kerberos, so the web server must use Microsoft software rather than Apache or Netscape (this as supposedly been `mixed' with the latest release, but participating sites still cannot use their own authentication server, and so remain in various ways at Microsoft's mercy). So Passport is not so

much a security product, as a lay for control of both the web server and purchasing information markets. It comes bundled with services such as Hotmail, is already used by 40 million people, and does 400 authentications per second on average. its known flaws include that Microsoft keeps all the users' credit card details, creating a huge target; various possible middleperson attacks; and that you can be impersonated by someone who steals your cookie le. (Passport has a `logout' facility that's supposed to delete the cookies for a particular merchant, so you can use a shared PC with less risk, but this feature didn't work properly for Netscape users when it was first deployed. The constant struggles to entrench or undermine monopolies and to segment and control markets determine many of the environmental conditions that make the security engineer's work harder. They make it likely that, over time, government interference in information security standards will be motivated by broader competition issues, as well as by narrow issues of the effectiveness of infosec product markets (and law enforcement access to data). So much for commercial information security. But what about the government sector? As information attack and defence become ever more important tools of national policy, what broader effects might they have?

3. Information Warfare - Offence and Defence

One of the most important aspects of a new technology package is whether it favours offence or defence in warfare. The balance has repeatedly swung back and forth, with the machine gun giving an advantage to the defence in World War 1, and the tank handing it back to the offence by World War 2. The difficulties of developing secure systems using a penetrate-and-patch methodology have been known to the security community since at least the Anderson report in the early 1970s; however, a new insight on this can be gained by using an essentially economic argument, that enables us to deal with vulnerabilities in a quantitative way. So information warfare looks rather like air war-fare looked in the 1920s and 1930s. Attack is simply easier than defence. Defending a modern information system could also be likened to defending a large, thinly-populated territory like the nineteenth century Wild West: the men in black hats can strike anywhere, while the men in white hats have to defend everywhere. Another possible relevant analogy is the use of piracy on the high seas as an instrument of state policy by many European powers in the sixteenth and seventeenth centuries. Until the great powers agreed to deny pirates safe haven, piracy was just too easy. The technical bias in favour of attack is made even worse by asymmetric information. Suppose that you head up a U.S. agency with an economic intelligence mission, and a computer scientist working for you has just discovered a beautiful new exploit on Windows 2000. If you report this to Microsoft, you will protect 250 million Americans; if you keep quiet, you will be able to conduct operations against 400 million Europeans and 100 million Japanese. What's more, you will get credit for operations you conduct successfully against foreigners, while the odds are that any operations that they conduct successfully against U.S. targets will remain unknown to your superiors. This further emphasizes the motive for attack rather than defence. Finally - and this appears to be less widely realized - the balance in favour of attack rather than defence is still more pronounced in smaller countries. They have proportionally fewer citizens to defend, and more foreigners to attack. In other words, the increasing politicization of in- formation attack and defence may even be a destabilizing factor in international affairs.

4. Distinguishing Good from Bad

Since Auguste Kerckhos wrote his two seminal papers on security engineering in 1883 (http://www.fabien-petitcolas.net/kerckhoffs/), people have discussed the dangers of `security-by-obscurity', that is, relying on the attacker's being ignorant of the de- sign of a system. Economics can give us a fresh insight into this. We have already seen that obscure designs are often used deliberately as a means of entrenching monopolies; but why is it that, even in relatively competitive security product markets, the bad products tend to drive out the good? The theory of asymmetric information gives us an explanation of one of the mechanisms. Consider a used car market, on which there are 100 good cars (the `plums'), worth $3000 each, and 100 rather trouble- some ones (the `lemons'), each of which is worth only $1000. The vendors know which is which, but the buyers don't. So what will be the equilibrium price of used cars? If customers start off believing that the probability they will get a plum is equal to the probability they will get a lemon, then the market price will start o_ at $2000. However, at that price only lemons will be offered for sale, and once the buyers observe this, the price will drop rapidly to $1000 with no plums being sold at all. In other words, when buyers don't have as much information about the quality of the products as sellers do, there will be severe downward pressure on both price and quality. Infosec people frequently complain about this in many markets for the products and components we use. The problem of bad products driving out good ones can be made even worse when the people evaluating them aren't the people who suffer when they fail. Much has been written on the ways in which corporate performance can be adversely affected when executives have incentives at odds with the welfare of their employer. For example, managers often buy products and services which they know to be suboptimal or even defective, but which are from big name suppliers. This is known to minimize the likelihood of getting red when things go wrong. Corporate lawyers don't condemn this as fraud, but praise it as `due diligence'. Over the last decade of the twentieth century, many businesses have sought to fix this problem by extending stock options to ever more employees.

However, these incentives don't appear to be enough to ensure prudent practice by security managers. (This might be an interesting topic for a PhD; does it comes down to the fact that security managers also have less information about threats, and so cannot make rational decisions about protection versus insurance, or is it simply due to adverse selection among security managers?) This problem has long been perceived, even if not in precisely these terms, and the usual solution to be proposed is an evaluation system. This can be a private arrangement, such as the equipment tests carried out by insurance industry laboratories for their member companies, or it can be public sector, as with the Orange Book and the Common Criteria. For all its faults, the Orange Book had the virtue that evaluations were carried out by the party who relied on them - the government. The European equivalent, ITSEC, introduced a pernicious innovation- that the evaluation was not paid for by the government but by the vendor seeking an evaluation on its product. This got carried over into the Common Criteria. This change in the rules provided the critical perverse incentive. It motivated the vendor to shop around for the evaluation contractor who would give his product the easiest ride, whether by asking fewer questions, charging less money, taking the least time, or all of the above. To be fair, the potential for this was realized, and schemes were set up whereby contractors could obtain approval as a CLEF (commercial licensed evaluation facility). The threat that a CLEF might have its license withdrawn was supposed to offset the commercial pressures to cut corners.

The failure modes appear to involve fairly straightforward pandering to customers' wishes, even (indeed especially) where these were in conflict with the interests of the users for whom the evaluation was supposedly being prepared. The lack of sanctions for misbehaviour -such as a process whereby evaluation teams can lose their accreditation when they lose their sparkle, or get caught in gross incompetence or dishonesty, is probably a contributory factor. But there is at least one more significant perverse incentive. From the user's point of view, an evaluation may actually subtract from the value of a product. For example, if you use an unevaluated product to generate digital signatures, and a forged signature turns up which someone tries to use against you, you might reasonably expect to challenge the evidence by persuading a court to order the release of full documentation to your expert witnesses. A Common Criteria certificate might make a court much less ready to order disclosure, and thus could severely prejudice your rights. A cynic might suggest that this is precisely why it's the vendors of products which are designed to transfer liability (such as digital signature smartcards), to satisfy due diligence requirements (such as firewalls) or to impress naive users (such as PC access control products), who are most enthusiastic about the Common Criteria. So an economist is unlikely to place blind faith in a Common Criteria evaluation. Fortunately, the perverse incentives discussed above should limit the uptake of the Criteria to sectors where an official certification, however irrelevant, erroneous or misleading, offers competitive advantage.

Self Assessment Exercise

Discuss the three particularly important features of information technology markets.

4.0 Conclusion

Much has been written on the failure of information security mechanisms to protect end users from privacy violations and fraud. This misses the point. The real driving forces behind security system design usually have nothing to do with such altruistic goals. They are much more likely to be the desire to grab a monopoly, to charge different prices to different users for essentially the same service, and to dump risk. Often this is perfectly rational. In an ideal world, the removal of perverse economic incentives to create insecure systems would depoliticize most issues. Security engineering would then be a matter of rational risk management rather than risk dumping. But as information security is about power and money - about raising barriers to trade, segmenting markets and differentiating products - the evaluator should not restrict herself to technical tools like cryptanalysis and information flow, but also apply economic tools such as the analysis of asymmetric information and moral hazard. As fast as one perverse incentive can be removed by regulators, businesses (and governments) are likely to create two more. In other words, the management of information security is a much deeper and more political problem than is usually realized; solutions are likely to be subtle and partial, while many simplistic technical approaches are bound to fail. The time has come for engineers, economists, lawyers and policymakers to try to forge common approaches.

5.0 Summary

Information security comes down to technical measures. Given better access control policy models, formal proofs of cryptographic protocols, approved firewalls, better ways of detecting intrusions and malicious code, and better tools for system evaluation and assurance, the problems can be solved. Information insecurity is at least as much due to perverse incentives. Many of the problems were explained more

clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons.

6.0 Tutor Marked Assignment

Explain the concepts of Offence and Defence in Information Warfare

7.0 References/ Further Reading

(1) Akerlof, G.A. (1970). The Market for 'Lemons': Quality Uncertainty and Market Mechanism," Quarterly Journal of Economics v 84 (August) pp 488-500.

(2) Anderson, J. (1973).`Computer Security Technology Planning Study', ESD-TR-73-51, US Air Force Electronic Systems Division (1973) http://csrc.nist.gov/publications/ history/index.html.

(3) Anderson, R.J (1994). Why Cryptosystems Fail" in *Communications of the ACM* vol 37 no 11 (November) Pp 32-40.

(4) Bloom, J.A., Cox, I.J., Kalker, T., Linnartz, JPMG ML Miller, Traw, CBS (1999). Copy Protection for DVD Video", in *Proceedings of the IEEE* v 87 no 7 (July) Pp 1267-1276.

(5) CERT, Results of the Distributed-Systems Intruder Tools Workshop, Software Engineering Institute, Carnegie Mellon University, http://www.cert.org/reports/dsit_ workshop-final.html, December 7, 1999.

(6) Curtis, W., Krasner, H., and Iscoe, N. (1988). A Field Study of the Software Design Process for Large Systems", in *Communications of the ACM* v 31 no 11 (Nov 88) pp 1268-1287.

(7) European Union, (2001). *`Network and Information Security: Proposal for a European Policy Approach'*, COM(2001)298 final, 6/6/2001.

(8) Kerckhos, A. (2000). La CryptographieMilitaire", in *Journal des Sciences Militaires*, 9 Jan 1883, pp 5-38; http://www.fabien-petitcolas.net/ kerckhoffs/

(9) Varian, H. (2000). Managing Online Security Risks", Economic Science Column, The New York Times, June 1, 2000, http: //www.nytimes.com/library/financial/ columns/060100econ-scene.html