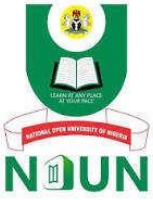
COURSE GUIDE

CYB 214
VOIP AND MULTIMEDIA SECURITY

Course Team Olanloye Odunayo PhD (Course Writer)- NOUN
Dr. Alamu Femi Oladele (Content Editor)- NOUN



NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
University Village
Plot 91, Cadastral Zone
Nnamdi Azikiwe Expressway
Jabi, Abuja

Lagos Office
14/16 Ahmadu Bello Way
Victoria Island, Lagos

E-mail : centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Printed 2024

ISBN: 978-978-786-274-2

CONTENT **PAGE**

INTRODUCTION

Welcome **to CYB 214: VoIP and Multimedia Security.** CYB 214 is a two-credit unit course that has a minimum duration of one semester. It is a compulsory course for undergraduate students that are enrolled in BSc Cybersecurity at the National Open University of Nigeria. The course guides you through the techniques and methodologies for an effective malware analysis by means of static, dynamic and behavioral approaches.

COURSE COMPETENCIES

- Understanding the basic concepts and types of multimedia.
- Understand the various applications of multimedia across different sectors.
- Learning about multimedia systems and technologies, including hardware and software.
- Acquiring skills to address technical, ethical, and legal challenges in multimedia.
- Understanding multimedia security, including encryption and digital rights management.
- Unfold the ability to analyze and apply multimedia security techniques.
- Familiarity with VoIP technology and its integration with multimedia.
- Understanding the evolution and security issues related to VoIP.

COURSE OBJECTIVES

The primary objectives of the course are to:

- Provide a detailed understanding of multimedia and its various components.
- Explore the applications and benefits of multimedia in different fields.
- Introduce students to multimedia systems and technologies.
- Discuss the challenges associated with multimedia, including technical, ethical, and legal issues.

- Provide a comprehensive overview of multimedia security techniques.
- Introduce VoIP technology, its applications, and security concerns.
- Equip students with the skills to apply security measures to multimedia and VoIP systems.

WORKING THROUGH THIS COURSE

In order to finish the course in a good manner, go through the study units, attend to the audios and videos, complete all assessments, click the links and read the content, be active in the relevant discussion threads, view the recommended texts and other resources provided, make your portfolios, and do the online facilitation.

Every study unit contains an introduction, intended learning outcomes, the main body, conclusion, summary of the unit and references or further readings. The introduction will highlight what is expected of you in the study unit. Read and take note of the intended learning outcomes (ILOs). The intended learning outcomes tell you what you should be able to do at the completion of each study unit. Thus, you can assess your learning at the completion of every unit to confirm that the intended learning outcomes have been met. To that end, to achieve the intended learning outcomes, the knowledge necessary is provided in the form of texts, video and links embedded into modules and units. Jumps forth the links as may be instructed but in situations you are reading the text off line you will have to cut and paste the link address in a browser. The audios as well as the videos may be downloaded for offline viewing. There's also the option of printing or downloading the texts and storing them in your PC or external hard disk. The conclusion tells you what is the main knowledge you will take home from the unit. Unit summaries are provided in downloadable audios as well as videos.

Assessments, as revealed by their definition, can be divided into two major types, namely formative assessments and summative assessments. Formative assessments will allow you to gauge your progress towards the attainment of the learning objectives. This is in the form of in-text questions, discussion boards and self-assessment exercises.

Summative assessment system will be used by the university in assessing your performance in academic work. This will include Continuous Assessment Component (CAC) and final examinations administered as Computer Based Test (CBT). During the semester, a minimum of three continuous assessments will be conducted and one final examination will be provided at the end of the semester. Computer

base tests and final examination are the only assessment components that you cannot avoid.

The study is organized into 12 study units which are arranged into four modules. The presentation of the modules and units is as follows:

STUDY UNITS

MODULE 1 INTRODUCTION TO MULTIMEDIA AND SECURITY

Unit 1 Introduction to Multimedia
Unit 2 Multimedia Security
Unit 3 Multimedia Encryption Techniques

MODULE 2 MULTIMEDIA AND VOIP TECHNOLOGY

Unit 1 Multimedia Traffic Security
Unit 2 Techniques for Streaming Data Traffic
Unit 3 Overview of VoIP Technology

MODULE 3 HISTORY AND VOIP SECURITY

Unit 1 Evolution of VoIP
Unit 2 Fundamental Elements for VoIP Deployment
Unit 3 Security Issues of VoIP

MODULE 4 APPLICATION OF VOIP

Unit 1 VoIP Protocol Vulnerabilities
Unit 2 Other VoIP Security Issues and Vulnerabilities
Unit 3 Security Policy for VoIP Applications

REFERENCES AND FURTHER READINGS

Aloraini, S. (2005). The impact of multimedia on teaching and learning in higher education: A review of the literature. International Journal of Humanities Social Sciences and Education, 3(7), 55-75.

Englander, I., & Wong, W. (2021). The architecture of computer hardware, systems software, and networking: An information technology approach. John Wiley & Sons.

Kumar, A., Singh, S., & Gupta, R. (2020). Multimedia security and privacy protection in the Internet of Things. International Journal of Multimedia Information Security, 10(2), 1-12.

Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7th ed.). Pearson.

Li, Z. N., Drew, M. S., Liu, J., Li, Z. N., Drew, M. S., & Liu, J. (2021). Introduction to multimedia. Fundamentals of Multimedia, 3-26.

Rosenberg, J., & Schulzrinne, H. (2002). An overview of the Session Initiation Protocol (SIP). IEEE Communications Magazine, 40(3), 30-37.

Yang, W., Wang, S., HuHu, J., & Karie, N. M. (2022). Multimedia security and privacy protection in the internet of things: research developments and challenges. International Journal of Multimedia Intelligence and Security, 4(1), 20-46.

Ze-Nian Li & Mark S. Drew. (2004). Fundamentals of Multimedia. Prentice Hall.

PRESENTATION SCHEDULE

The timeline of the presentation shows the critical dates for the completion of the computer-based test, forum discussions, and facilitation attendance. Take note that you will have to hand in all your assignments on time. Take precautions so that there are no delays and no plagiarized work. Plagiarism is a vice that is punishable by law and even more so in academic circles.

ASSESSMENT

In this course, two types of assessments will be scored. The Continuous assessments and the final examination. The continuous assessment shall be in three folds. There will be two computer-based assessments. The regular computer assessment will be done as scheduled in the academic calendar of the university. Strict adherence is required on the timimg. The Computer Based Assessments shall carry a weighting of 10% for each component, while scores for participation in discussion forums and portfolios shall ice capped at 10% provided one has 75% attendance. Therefore, the maximum score for continuous assessment shall be 30% which will contribute to the overall course grade.

The final examination for CYB 214 will not exceed two hours and will account for 70% of the overall course grade. The examination will require the students to answer 70 multiple-choice questions that reflect cognitive reasoning.

Note: You will attain a 10% mark, if you participate in course forum discussions and in your portfolios by at least 75% participation; otherwise, you will forfeit the 10% from your overall mark. You will be required to upload your portfolio using google Doc. What are you

expected to do in your portfolio? Your portfolio should be note or jottings you made on each study unit and activities after completed the study. This will include the time you spent on each unit or activity.

TUTOR-MARKED ASSIGNMENT

During this course, you are expected to cover twelve (12) units, and Tutor Marked Assignments are found at the end of each unit. Each assignment is worth 10% of your overall grade, and the highest three assignments submitted will account for 30% of your overall grade. Lastly, after the course is finished, there will be a final examination, which will weigh 70% of the total grade.

You can also use extra material not provided by the course in order to accomplish your Tutor-marked Assignments. Be careful to send your assignments to your tutor on or before the stated deadline. If for any reason you are unable to submit your assignment on time, speak to your tutor prior to the deadline in order to request more time. Be aware that no extensions will be granted after the submission deadline except in very rare cases.

FINAL EXAMINATION AND GRADING

The final examination for CYB 214 will last for 4 hours and have a value 70% of the total course grade. The examination will consist of questions which reflect the self-assessment exercise and tutor-marked assignments that you have previously encountered. Furthermore, all areas of the course will be examined. It would be better to use the time between finishing the last unit and sitting for the examination, to revise the entire course. You might find it useful to review your TMAs and comment on them before the examination. The final examination covers information from all parts of the course.

COURSE MARKING SCHEME

The following table includes the course marking scheme

Table 1 Course Marking Scheme

ASSESSMENT	MARKS
Assignments 1 – 12	12 Assignments: 30% of the best 3. Total = 10% X 3 = 30
Final Examination	70% of the overall course marks
Total	100% of Course Marks

COURSE OVERVIEW

This table, table 2 presents the units, the number of weeks required to complete each unit as well as the necessary assignments.

Table 2: Course Organizer

Unit	Title of Work	Weeks Activity	Assessment (End of Unit)
Course Guide		Week	
Module 1		**INTRODUCTION TO MULTIMEDIA AND SECURITY**	
Unit 1	Introduction to Multimedia	Week 1	Assignment 1
Unit 2	Multimedia Security	Week 2	Assignment 2
Unit 3	Multimedia Encryption Techniques	Week 3	Assignment 3
Module 2		**MULTIMEDIA AND VOIP TECHNOLOGY**	
Unit 1	Multimedia Traffic Security	Week 4	Assignment 4
Unit 2	Techniques for Streaming Data Traffic	Week 5	Assignment 5
Unit 3	Overview of VoIP Technology	Week 6	Assignment 6
Module 3		**HISTORY AND VOIP SECURITY**	
Unit 1	Evolution of VoIP	Week 7	Assignment 7
Unit 2	Fundamental Elements for VoIP Deployment	Week 8	Assignment 8
Unit 3	Security Issues of VoIP	Week 9	Assignment 9
Module 4		**APPLICATION OF VOIP**	
Unit 1	VoIP Protocol Vulnerabilities	Week 10	Assignment 10
Unit 2	Other VoIP Security Issues and Vulnerabilities	Week 11	Assignment 11
Unit 3	Security Policy for VoIP Applications	Week 12	Assignment 12

HOW TO GET THE MOST FROM THE COURSE

It is necessary that you possess a personal laptop and internet connection in order to gain maximum benefits from this course. This will enable

you to learn from anywhere in the globe. Approach the course by means of Intended Learning Outcomes (ILOs) during your self-study. At the end of every unit, use the ILOs to assess yourself and determine whether you have attained what you were supposed to attain.

Take your time and work through each unit making your notes. Attend the online real time facilitation as programmed. Where you skipped the programmed online real time facilitation, watch the recorded facilitation session at your own convenient time. Video recording will be done for each online real time facilitation session and uploaded on the platform.

Apart from facilitating in real time, also see the video and audio recorded summary in each unit. Video / audio summaries are aimed at highlighting the salient part in every unit. You can access the audio and video links within the text as well as on the course page.

Work through all self-assessment exercises. Finally, obey the rules in the class.

FACILITATION

You will receive online facilitation. The facilitation is learner centred. The mode of facilitation shall be asynchronous and synchronous. For the asynchronous facilitation, your facilitator will:

- Present the theme for the week;
- Direct and summarise forum discussions;
- Coordinate activities in the platform;
- Score and grade activities when need be;
- Upload scores into the university recommended platform;
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures; and podcast

For the synchronous:

- There will be eight hours of online real time contact in the course. This will be through video conferencing in the Learning Management System. The eight hours shall be of one-hour contact for eight times.
- At the end of each one-hour video conferencing, the video will be uploaded for view at your pace.
- The facilitator will concentrate on main themes that are must know in the course.
- The facilitator is to present the online real time video facilitation time table at the beginning of the course.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

Do not hesitate to contact your facilitator. Contact your facilitator if you:

- do not understand any part of the study units or the assignment.
- have difficulty with the self-assessment exercises
- have a question or problem with an assignment or with your tutor's comments on an assignment.

Also, use the contact provided for technical support.

Read through all the feedback and annotations provided by your teacher, particularly on your coursework, engage in the various discussion forums offered. This gives you a chance to interact with other people in the program. Ample time will be allocated for any issues which may have arisen during the course. It is advised that participants come prepared with a set of questions that the course facilitator will consider and address to the participants as well. Doing the discussion is most nourishing and one gains a lot of knowledge that way.

Lastly, fill in the survey questionnaire. This will provide the institution feedback on your difficulties and ways of addressing such difficulties in regard to assertions on the course materials and the lessons learnt.

COURSE INFORMATION

Course Code:	CYB 214
Course Title:	VoIP and Multimedia Security
Credit Unit:	2
Course Status:	Compulsory
Course Blub:	The course provides a comprehensive overview of multimedia, its integration into various sectors, and the security challenges and solutions associated with it.
Semester:	Second
Course	Duration: 12 Weeks

Required Hours for Study: 65

ICE BREAKER

Welcome to CYB 214: VoIP and Multimedia Security, a two-unit course that explores into the exciting world of modern communication technologies and the security challenges that accompany them. In this course, we will explore the fundamentals of Voice over IP (VoIP) technology and multimedia, examining how these systems work, their

applications, and, most importantly, how to secure them in a digital world where threats are ever-evolving.

The integration of voice, video, and data over internet protocols has revolutionized industries, but it also opens up new vulnerabilities. Throughout this course, you will gain practical insights into VoIP protocols, multimedia encryption, and security techniques that are critical in today's interconnected environment. Our goal is to equip you with the knowledge and skills to protect communication systems from potential breaches and ensure the integrity and confidentiality of multimedia data.

Before we begin, allow me to introduce myself. My name is Olanloye Odunayo, and I will be guiding you through this course. With a background in Machine Learning, cybersecurity, network security, and multimedia technology, I have had the privilege of working with numerous technologies in this field, and I am excited to share my experience with you. I believe in a hands-on, interactive approach to learning, so expect a mix of theory, real-world examples, and practical exercises.

Now, I would like to get to know you better! Please introduce yourself by uploading your profile picture, sharing your workplace or study area, and providing a brief introduction including your GSM number and any expectations you have for this course. Feel free to tell us about your background and what you hope to achieve by the end of this course.

I look forward to an engaging and productive learning journey with all of you! Let's fasten our seat belts and dive into the world of VoIP and Multimedia Security!

MAIN COURSE

CONTENTS

MODULE 1: INTRODUCTION TO MULTIMEDIA AND SECURITY

Introduction

Multimedia has revolutionised the way we communicate, learn, and engage with information. Its components, applications, and challenges are crucial to understanding its impact on various sectors. By addressing the challenges and leveraging the benefits of multimedia, we can create more engaging, interactive, and dynamic experiences that enhance user engagement and retention.

Unit 1: Introduction to Multimedia
Unit 2: Multimedia Security
Unit 3: Multimedia Encryption Techniques

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

UNIT 1 INTRODUCTION TO MULTIMEDIA

Unit Structure

1.0 Introduction

Multimedia refers to the integration of multiple forms of media, where "media" encompasses various methods of communicating information. These includes text, audio, images, video, and animation. Media can be

understood as any medium through which information or content is transmitted or presented. In the context of multimedia, these different types of media are combined to create dynamic, engaging, and often interactive experiences, enhancing how information is conveyed and perceived. This integration allows for richer communication across sectors like education, entertainment, and business. It enhances the way information is presented and perceived by allowing for interactive and dynamic content. Multimedia is widely used across various sectors, impacting education, entertainment, business, and more. Multimedia is a dynamic and rapidly evolving field that impacts various aspects of our lives. Its integration across different sectors continues to enhance the way we communicate, learn, and entertain ourselves. As technology advances, the possibilities for multimedia are boundless, promising more interactive and immersive experiences in the future.

2.0 Intended Learning Outcomes (ILOs)

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

- discuss the various concepts of multimedia
- discuss various types of multimedia
- state the multimedia systems and technologies
- explain the applications area of multimedia

3.0 Main Content

3.1 Definition and Concepts

Multimedia is defined as the combination of different content forms such as text, audio, images, animations, or video. It can be recorded and played, displayed, interacted with, or accessed by information content processing devices, such as computerized and electronic devices.
Multimedia, defined as the combination of text, audio, images, video, and animation, enhances the way information is presented and perceived, making it more interactive and dynamic.

3.2 Types of Multimedia

Multimedia is a combination of various media platforms that include different contents, such as words or text, audio, music, images, infographics, videos, and animations. The key components of multimedia include:

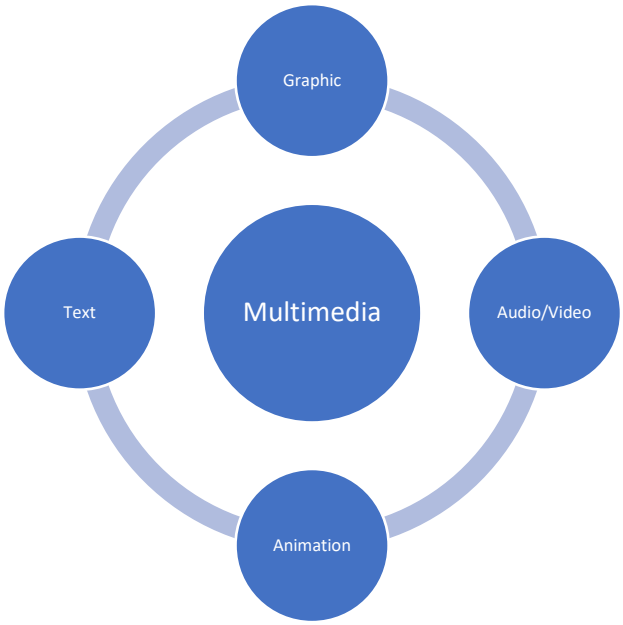


Fig. 1.1 Types of Multimedia

Text: The most basic and widely used form of multimedia. It includes anything that can be read or written, from simple text files to complex documents and web pages.

Audio: This encompasses any sound element, including speech, music, and sound effects. Audio can enhance user experience and provide additional context or atmosphere to multimedia content.

Images: Static visual representations, including photographs, drawings, and illustrations. They convey information quickly and effectively.

Video: Video is a powerful multimedia component that combines moving images with audio to create a compelling narrative. It is widely employed for storytelling, demonstrations, and presentations.

Animations: Animations introduce a sense of motion to multimedia content, utilizing moving images or illustrations to enhance engagement. They can explain intricate concepts, add a playful or dynamic element to presentations, or guide the viewer's attention.

Interactive Elements: Interactive elements, such as buttons, links, and forms, enable users to interact with multimedia content, making it more engaging and dynamic.

Multimedia Systems and Technologies

Multimedia systems are platforms that enable the creation, storage, processing, and delivery of multimedia content, which includes text, images, audio, video, and interactive elements. These systems are

designed to handle a wide variety of media formats and provide users with the tools necessary to combine and manipulate different types of content. To fully understand multimedia systems, it is essential to explore both the hardware and software components that make these systems possible.

Hardware

Multimedia hardware includes devices like computers, smartphones, tablets, cameras, microphones, and speakers. These devices are essential for capturing, creating, and displaying multimedia content.

The hardware used in multimedia systems plays a crucial role in capturing, storing, and displaying multimedia content. Some key components include:

Computers and Mobile Devices: These serve as the primary platforms for creating and viewing multimedia content. Computers with high processing power, ample memory, and advanced graphics capabilities are essential for tasks such as video editing, 3D animation, and high-resolution image processing.

Cameras and Scanners: Used to capture visual content, including images and video. Digital cameras, webcams, and 3D scanners are examples of hardware used to input visual data into a multimedia system.

Microphones and Audio Input Devices: These capture sound, such as voice or music, and convert it into digital formats for use in multimedia projects.

Storage Devices: Multimedia files, especially high-resolution video and audio files, require significant storage space. Hard drives, solid-state drives (SSD), and cloud storage solutions offer scalable options for storing large multimedia projects.

Monitors and Display Screens: High-definition (HD) and Ultra-HD displays are essential for viewing multimedia content in its full detail. These screens are crucial for video editing, graphic design, and 3D modeling.

Graphics Cards (GPUs): Modern multimedia systems rely on powerful GPUs to process and render high-quality video, images, and animations. GPUs offload complex visual processing tasks from the CPU, enabling smoother playback and faster rendering times.

Software

Multimedia software includes applications for creating, editing, and viewing multimedia content. Examples include Adobe Photoshop for image editing, Adobe Premiere for video editing, and various audio editing tools like Audacity.

Content Creation Software

Image Editing Software (e.g., Adobe Photoshop, GIMP): Used for creating and manipulating images, graphics, and illustrations. These programs allow users to edit images, create infographics, and design visuals for multimedia projects.
Audio Editing Software (e.g., Audacity, Adobe Audition): These tools are used to record, edit, and mix audio. They allow for the manipulation of sound effects, voiceovers, music tracks, and other audio elements in multimedia content.

Video Editing Software (e.g., Adobe Premiere Pro, Final Cut Pro): These applications are essential for editing and producing video content. They offer tools for cutting, splicing, and adding effects to video, making them integral to multimedia production.

3D Animation and Modeling Software (e.g., Blender, Autodesk Maya): Used to create 3D animations, visual effects, and interactive content. These programs are widely used in gaming, film, and architectural visualization.

Content Playback Software

Media Players (e.g., VLC, Windows Media Player): These applications are used to play multimedia files, including video, audio, and images, on various devices. Media players support a wide range of file formats and codecs to ensure smooth playback.

Browsers (e.g., Google Chrome, Mozilla Firefox): Modern web browsers are equipped with the ability to stream and display multimedia content, such as videos, audio, and interactive web applications. With HTML5 and WebGL support, browsers have become vital for delivering multimedia content online.

Multimedia Development Software

Authoring Tools (e.g., Adobe Flash, Articulate Storyline): These are used to create interactive multimedia applications, such as educational modules, presentations, and simulations. They allow for the integration of different media types into cohesive, interactive experiences.

Game Development Engines (e.g., Unity, Unreal Engine): These platforms enable developers to create immersive, interactive multimedia experiences, especially in the field of gaming and virtual environments. They combine elements of 3D modeling, animation, sound, and physics engines.

Compression and Encoding Software

Multimedia compression tools (e.g., HandBrake, Adobe Media Encoder): These are crucial for reducing the file size of multimedia content while maintaining quality. Compression is particularly important for streaming, as it optimizes multimedia for web use without compromising performance.

Codecs (e.g., H.264, MP3): Codecs are used to encode and decode digital media, ensuring that multimedia files are efficiently compressed and compatible with various devices and software applications.

Emerging Trends in Multimedia Systems

Artificial Intelligence (AI) in Multimedia: AI is increasingly being used to automate content creation, enhance media quality, and personalize multimedia experiences based on user preferences.

5G and Edge Computing: These technologies are revolutionizing the speed and quality of multimedia streaming, especially for high-definition content and interactive media.

Cloud-based Multimedia Systems: Cloud technologies allow for scalable, flexible multimedia production and distribution, making it easier to collaborate, store, and stream media.

3.3 Applications of Multimedia

1. Education: Multimedia enhances learning experiences by making educational content more engaging and interactive. It includes e-learning platforms, educational videos, and interactive simulations.
2. Entertainment: This sector benefits significantly from multimedia. It includes movies, video games, music, and virtual reality experiences.
3. Business: Multimedia is used in advertising, marketing, training, and presentations. It helps businesses communicate their message effectively and engage with customers.
4. Medicine: In the medical field, multimedia is used for training, simulations, patient education, and telemedicine.
5. Commerce: Multimedia is used in e-commerce to provide interactive product demonstrations, product reviews, and customer testimonials.
6. Social Work: Multimedia is used in social work to create interactive and engaging content for social media platforms, enhancing communication and outreach efforts.
7. Journalism: Multimedia is used in journalism to create interactive and engaging news stories, enhancing the user experience and increasing reader engagement.
8. Engineering: Multimedia is used in engineering to create interactive and engaging simulations, enhancing the learning experience and increasing user engagement.

3.4 Multimedia Development Process

Planning: Define objectives, target audience, and content requirements.
Design: Create a blueprint for the multimedia project, including storyboards and mockups.
Development: Produce the multimedia content using appropriate tools and technologies.
Testing: Ensure the content works as intended and meets quality standards.
Deployment: Publish the multimedia content and make it accessible to the target audience.

3.5 Challenges in Multimedia

Technical Challenges: Issues like compatibility, bandwidth, and storage can affect the creation and distribution of multimedia content.
Ethical and Legal Issues: Copyright infringement, privacy concerns, and the ethical use of multimedia need to be addressed.

1. **Distributed Networks/Application Distribution**: Distributed networks and application distribution pose significant challenges, as data is spread across multiple computers, making security and data management complex.
2. **Sequencing within the Media**: Sequencing within the media is a significant challenge, as multimedia content requires precise synchronization to ensure a seamless user experience.
3. **Capacity of Data Storage and Management**: The capacity of data storage and management is a significant challenge, as multimedia content requires large storage capacities and efficient data management systems.

3.6 Future Trends in Multimedia

Augmented Reality (AR) and Virtual Reality (VR): These technologies are set to revolutionize the way we interact with multimedia, offering immersive experiences.
Artificial Intelligence (AI): AI can enhance multimedia creation and consumption by providing smart editing tools, personalized content, and improved user experiences.
5G Technology: Faster internet speeds will enable higher-quality multimedia streaming and more interactive applications.

 Discussion

After reading unit 1 from module 1 of this course material, can you categorize various applications of multimedia? Enumerate the various types of multimedia and their challenges.

 4.0 Self-Assessment Exercise(s)

Question 1: Discuss the concept of Multimedia
Answer:
Multimedia integrates multiple forms of media, such as text, audio, images, video, and animation, creating dynamic and interactive content. It is widely used in various sectors, enhancing how information is presented and perceived.

Question 2: State and discuss the challenges in multimedia
Answer:
Challenges in multimedia include technical issues like bandwidth and storage, ethical concerns such as copyright and privacy, and issues related to synchronization (sequencing within media). The capacity to store and manage large multimedia data efficiently is another significant challenge.

Question 3: Enumerate the development process of multimedia
Answer:
Planning: Defining objectives and content requirements.
Design: Creating blueprints, storyboards, and mockups.
Development: Producing content using appropriate tools.
Testing: Ensuring functionality and quality.
Deployment: Publishing the content for the target audience.

Question 4: State and discuss five (5) application areas of multimedia
Answer:
Education: Enhances learning experiences through interactive simulations.
Entertainment: Used in movies, video games, and music.
Business: Employed in marketing, training, and presentations.
Medicine: Applied in training simulations and telemedicine.
Journalism: For creating interactive news stories.

Question 5: Discuss the future trends in multimedia
Answer:

Future trends include Augmented Reality (AR), Virtual Reality (VR), Artificial Intelligence (AI) for content creation, and 5G technology for faster and higher-quality multimedia streaming.

5.0 Conclusion

You have learnt from this unit that Multimedia has become an integral part of our digital landscape, revolutionizing how we communicate, learn, and engage with information. Multimedia is a combination of various media platforms that include different contents, such as words or text, audio, music, images, infographics, videos, and animations.

6.0 Summary

At the end of this unit, you have learnt the definition of a multimedia, the various application of multimedia, the types of multimedia and the development process of multimedia. In the next unit, you will be introduced to the multimedia security.

7.0 References/Further Readings

Aloraini, S. (2005). The impact of multimedia on teaching and learning in higher education: A review of the literature. International Journal of Humanities Social Sciences and Education, 3(7), 55-75.

Englander, I., & Wong, W. (2021). The architecture of computer hardware, systems software, and networking: An information technology approach. John Wiley & Sons.

Kumar, A., Singh, S., & Gupta, R. (2020). Multimedia security and privacy protection in the Internet of Things. International Journal of Multimedia Information Security, 10(2), 1-12.

Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7th ed.). Pearson.

Li, Z. N., Drew, M. S., Liu, J., Li, Z. N., Drew, M. S., & Liu, J. (2021). Introduction to multimedia. Fundamentals of Multimedia, 3-26.

UNIT 2: MULTIMEDIA SECURITY

Unit Structure

1.0 Introduction

Multimedia security is achieved by one or more techniques which are used to safeguard the multimedia material. These are largely oriented around cryptography and they either provide security to communication or protect from content theft (DRM, Watermarking) or do both. Communication security with respect to digital images and textual digital media can be achieved by utilizing normal symmetric key encryption. Such media can be treated as a binary sequence and the entire payload can be protected using a cryptosystem such as Advanced Encryption Standard (AES) or Data Encryption Standard (DES). In a typical situation, when the multimedia data is not dynamic (not a live stream), we can take it to be simple binary information and apply the normal encryption methods.

As we know that data includes all information in any ledger, book which may be pertinent, state, or nation etc In simple words data means how every information is being captured on pages of any document or book. So, to put simply “data encryption” means “encoding information so that it cannot be read by anybody else”. It is the process of making any readable data mix up with some characters and making it to someone who cannot understand the meaning unless it is made back again to

readable form using a specific key. In other words, encryption is meant to enhance the confidentiality, integrity and security of important data dispersion such that access to the original data is provided only to certain persons or systems.

Security is gaining immense popularity in the present scenario of advanced technology and internet. There are many applications of security, for example, it is used in secure communication like emails, messaging, and so on, data storage, financial transactions, and so ever. Broadly, encryption can be classified into two categories:

Symmetric Encryption: Envelopes are shared between sender and receiver for encryption as well as decryption. Examples: AES, DES.

Asymmetric Encryption: It makes use of two keys, a public key which is used to encrypt the data and a private key which is used to decrypt the data. Examples: RSA, ECC.

Encryption is regarded as one of the main components when designing advanced systems for securing data or communication over networks. Its often considered the simplest form of executing encryption where entire multimedia stream is encrypted using normal.

Nonetheless, this is not so easy to achieve because of the numerous limitations for example the near real-time speed of the content. Video and audio multimedia content communication encryption is not just the use of already known encryption schemes such as DES or AES to the content's binary code. It requires a thoughtful design where the appropriate encryption solution is selected and applied for the audio and video content. Nowadays the interest is primarily concerned with improvement of cryptosystems already used for the purpose of protecting real-time audio and video. This also aims at utilizing the specific properties of a number of standard audio and video formats in order to achieve the requisite speed for real time streaming. This is called partial encryption.

For the majority of textual data, still images, and mediocre quality audio or video, it is possible to implement SRTP (Secure Real-time Transport Protocol) for enhanced security of data during transmission. In laymen terms, SRTP is a classic protocol for streaming multimedia that relies on AES, an advanced strong encryption technique, to scrap encrypt all the content within the stream.

It is not easy to decide on an appropriate degree of security. There is a need to find the midpoint between the value of the information and the expenditure required to keep it secure. If the information is of less value,

then less cumbersome and less complex encryption can be adopted. On the contrary, when handling sensitive materials such as state or military operations, the best cipher technique must be employed.

Again, in applications such as pay-per-view where there are significant data transfers but such are not critical, basic encryption may suffice. In contrast, in the case of video calls (especially in business or high government meetings), much more powerful encryption is required. They say this is due to the fact that one will be expected to use broadband and at the same time provide video security of that level without any break in transmission.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Recognise the different encryption techniques for video encryption
- Undersand video Scrabling
- Describe the selective Video Encryption
- Understand the video encryption algorithm
- Describe the partial encryption algorithms by Cheng and Li, 2000

3.0 Main Content

3.1 Video Encryption Techniques

In this part, we delve into several research exploration avenues taken in the field of video communication encryption. Earlier, it was mentioned that there exists a simple and straightforward approach to encrypt multimedia content. The entire multimedia content is encrypted with a single symmetric key cryptosystem. Again, even the recent high speeds of symmetrical schemes like DES or AES do not come cheap in terms of computational expense for many real-time audio visual data.

3.1.1 Video Scrambling

Scrambling is regarded as one of the quickest ways of impairing the video signal, while at the same time, it is considered a very insecure way of doing so. On the whole, scrambling was simply an industrial need imposed on cable operators by the immediate realities which made it possible to employ a faster means of preventing free viewing of paid cable channels from sheer inconvenience of doing anything to the video signal in a cable system.

While the term scrambling does not have a clear cut meaning, it implies the most primitive types of encryption practices, such as simple substitution or simple transposition ciphers, which in current times have the lowest order level of security. Initial implementations of signal scrambling involved either an analog device that would temporally permute the original signal or distort it in a frequency domain using filter banks or frequency converters. However, these schemes rely heavily on very low level of security making them very easy to use crack resourced with modern computers. If the original video or audio signal can be obtained by the attacker, it is not of concern, apart from the temporary delays created by these particular methods.

Most of the time still this is a solution that enables cable operators across the globe to function quite well as because the majority of people do not want to know or do not have the technical capabilities to break the coded video signal, but modified cable boxes that can be used to decode any scrambled contents are not that difficult to build. Nevertheless, scrambling is out of the question for processors and systems that provide a more serious level of infosec than the physically enforced one.

3.1.2 Selective Video Encryption

To achieve the real-time requirement for playing back audio and video multimedia, it is often proposed selective encryption techniques. The principal concept of selective encryption is to encrypt only a portion of the compressed bit stream. A common approach in selective encryption is to merge compression and encryption like shown in figure 2.1.

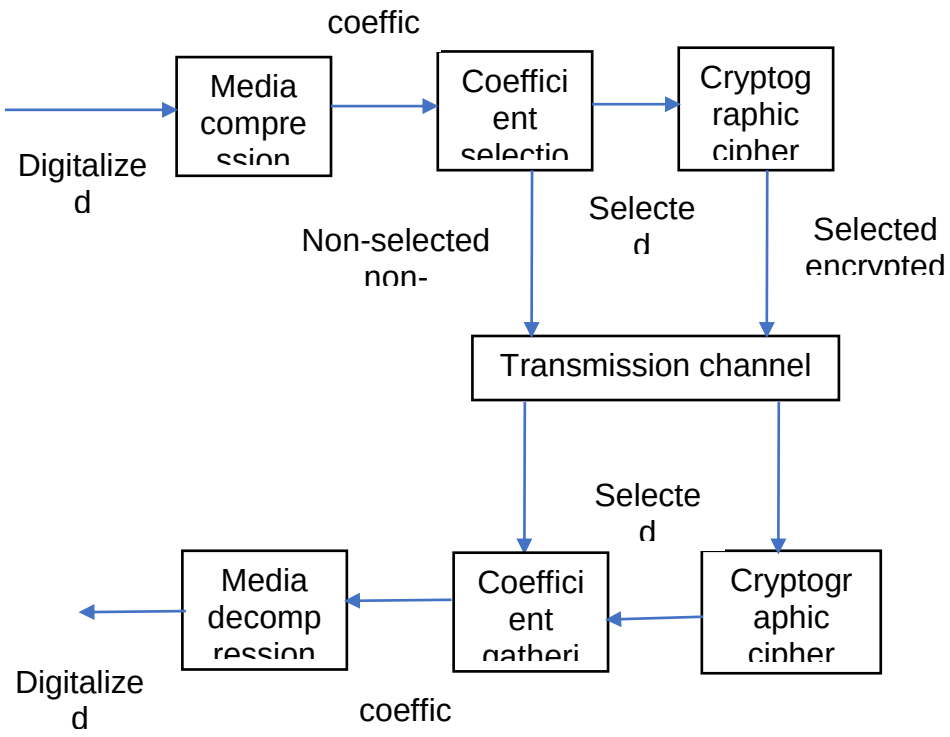


Figure 2.1 A common selective encryption scheme

As an illustration, it is possible to take the most significant coefficients from the last stages or even the intermediate stages of a compression operation and encode these coefficients only. Other coefficients are left unprotected. Less important coefficients may, however, be lightly encrypted in some schemes. By, "light," we mean that there is enciphering, which is fast but not too secure for use in a general sense (that is speed and security cannot be kept at the same level). Hence, we classify this method as variable encryption, whereby, various encryption techniques of different security levels are utilized. Limited encryption is a form of variable encryption, which can be included in its extension.

SECMPEG (Secure MPEG) is a technology proposed in 1995 by Meyer and Gadegast. Meyer and Gadegast suggested an encryption technique called Secure MPEG (SECMPEG) for MPEG-1 video standard in 1995. The SECMPEG provides four levels of security. At first level, the SECMPEG encrypts the sequence header to the slice header (SH-SH) and in SH, MBs motion vectors and DCT blocks are carried out without encryption. At the second level, parts of I-blocks that are the most important are encrypted as well (e.g. the upper left corner of the I-block region). At the third level, frame-based encryptor encrypts all I-frames and then I-frames only clauses. In the last level, which corresponds to the fourth level of the pyramid, SECMPEG performs enciphering/encoding of an entire MPEG-1 sequence (this method is called naive). Encrypting in their work was done using DES symmetric

key cryptosystem and this was a logical choice because it has been invented for almost three decades since 1976 and NIST had adopted it as their official symmetric algorithm and even the US government was using it. Where confidentiality was needed, it is understandable that because it's a symmetric key cryptosystem, only the covered content could be encrypted. In this paper, Meyer and Gadegast also proposed a solution to protect the integrity of the data. Therefore, a low-level means of integrity was implemented - Cyclic Redundancy Check (CRC). This was left for more study because those were full-fledged mechanisms which included public key crypto systems and the use of cryptographically secure hash functions like MD4, MD5 or SHA.

The selective encryption in SECMPEG (levels 1, 2, and 3) has certain limitations. It has been demonstrated that while an independent P-frame or B-frame is devoid of content without its I-frame counterpart, a P-frame or B-frame cannot be underestimated in the presence of its corresponding base I-frame. Agi and Gong's experiments showed that even when I-frames are encrypted, some I-blocks remain visible in other frames. A few trade-off enhancements were then proposed by the same authors, such as increasing the I-frame rate or securing all P- and B-frames, along with I-framing. These improvements lessen velocity and further impair the compression ratio. Since SECMPEG effects modifications to the MPEG-1 structure, a special encoder and decoder is required to operate SECMPEG streams.

Yet, the SECMPEG paper and its implementation by Meyer and Gadegast was among the first significant studies involving selective encryption of content-rich multimedia streams. These authors were perhaps the first ones who saw the potential of encrypting only parts of the bit stream in video coding. His tests showed that the visual interference was considerable only while encrypting the DC coefficients and the first three to eight AC coefficients of the 8 8 JPEG blocks of MPEG-1 I-frames in the bit stream.

In the year 1995, Maples and Spanos developed security mechanisms called Aegis, which is one more research contribution on selective encryption of video streams using MPEG. Aegis is 'MPEG video framework which includes security features' and was developed originally for MPEG-1 and MPEG-2 video standards. In an MPEG video stream, it selectively encrypts I-frames of all MPEG groups of pictures while leaving B and P Frames unencrypted. Furthermore, Aegis also encrypts the MPEG video sequence header where all the parameters used to initialize the decoder, which consists of dimensions of the picture, the frame rate, the bit rate, buffer sizes etc, are held. To conclude, this approach also ciphers the last 32 bits of stream known as the ISO end code. As a result, it further masks the MPEG signature of

the bit stream. Aegis which was a cryptographic engine utilized by Maples and Spanos was based on the DES standard. More or less, Aegis resembles the level 3 of SECMPEG as conceived by Meyer and Gadegast, and the vulnerabilities of SECMPEG are also present in Aegis.

As pointed out earlier, Agi and Gong challenged the postulation by Aegis and SECMPEG who suggested the encryption of only the I-frames due to concerns that their studies revealed some qualities of the scene were present in the P and B frame information whenever these were decoded. For instance, they claimed, a talking head was ascertainably in the video. In addition, Alattar and Al-Regib also made similar remarks concerning the safety of SECMPEG. The quality of this type of safety is worth noticing, since in many applications falling under it, the safety features are not high up the list of the priorities (for instance, the sleight of hand entertainment, encoded pay television), but such quality degradation would be acceptable for more serious applications, such as secured military or corporate video conferences. Aegis is equally regarded as one of the earliest works in the field of selective video encryption. The results of selective encryption experiments reported by Maples and Spanos validated the incredible speed improvement over the straightforward method.

Tang's Zigzag Permutation Algorithm, initiated in 1996. While Tang's approach to zigzag permutation is quite revolutionary in that it tries to concentrate on the compression of each frame within the MPEG video with the interspersed encryption. The JPEG and I frame of the MPEG video compress with a zigzag pattern of 8X8 blocks. A set of 64 entries that are ready to undergo the entropy encoding takes the form of a zigzag pattern. The CyberTerror's premise revolves around a very simple concept: an array of 8X8 blocks is transformed into a 1X64 vector via random mapping of the positions – i.e. blocks. The process is made up of three stages:
Stage 1: A collection of 64 such lists is constructed
Stage 2: A slitting operation of the block with dimensions 8 by 8 is performed as follows: We represent the DC value with an 8 bit binary number whose bits are b7b6b5b4b3b2b1b0. The number is then divided into two equal parts, the first half being b7b6b5b4 and the second being b3b2b1b0. Hence we have b7b6b5b4 put into the DC coefficient b3b2b1b0 being put into the A C 63 coefficient the last AC coefficient which is the least significant one in the block so as to not cause any visible drop in quality.
Stage 3: The split block is randomly permuted.

The algorithm of video encryption developed by Qiao and Nahrstedt in 1997. V. E. A. that is Video Encryption Algorithm by Qiao and

Nahrstedt is developed in a manner that can make the most out of the statistical characteristics of MPEG format videos. The algorithm consists of the following four (4) phases:
Step 1: Let the 2n-byte sequence, denoted by $a_1 a_2 \ldots a_{2n}$, represent the chunk of an I-frame
Step 2: Create two lists, one with odd indexed bytes $a_1 a_3 \ldots a_{2n-1}$, and the other with even indexed bytes $a_2 a_4 \ldots a_{2n}$, a2a4. . .a2n
Step 3: Xor the two lists into an n-byte sequence denoted by $c_1, c_2 \ldots c_n$
Step 4: Apply the chosen symmetric cryptosystem E (e.g., DES or AES) with the secret key $KeyE$ on either the odd list or even list and, thus, create the ciphertext sequence $c_1 c_2 \ldots c_n \; E_{key} \; E(a_1 a_3 \ldots a_{2n-1}) or \; c_1 c_2 \ldots c_n E_{key} \; E(a_2 a_4 \ldots a_{2n})$, respectively.

Evidently, the reverse process of transmittal end, consists of two simple operations on the ciphertext output half. First operation involves using the S-Box encryption mechanism E with the appropriate key over the output half to get sequence number one, and then performing an exclusive OR operation between this output and the input half of the ciphertext number one to get the sequence number two.

3.2 Image Encryption Techniques

In the case of still images, the security is most of the time obtained by the simplistic approach of encrypting the whole image. Nevertheless, naive techniques for enciphering and deciphering still images apply in certain scenarios and impose a severe limitation in communication and processing. For example, small mobile devices have limited bandwidth and processing power that calls for a different approach. Apart from this, the different techniques that are developed to transcode images are also used for selective video encryption.
In this part, we present some enhanced image encryption techniques that have been recently suggested where image compressing full image in able to process is rather time wasting. This is selectively encrypting the image. A closely related notion was already examined in the previous segment.

3.2.1 Partial Encryption Algorithms by Cheng and Li, 2000

Cheng and Li presented partial encryption techniques which are applicable for images encoded using two distinct categories of compression techniques: quadtree based compression technique and zerotree wavelet compression technique. The encryption/decryption function is not defined; nevertheless, the user in general may choose the standard cryptosystems like the International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), etc.

The image compression technique bases the idea on the generation of a quadtree and description of all the blocks in the tree with appropriate parameters. To the sake of argument, it is postulated that only one parameter that explains a block in the tree, average intensity is taken into account. Block intensity does not carry any significant information regarding the original image, however quadtree decomposition provides ways in drawing the silhouettes of objects in the original picture. Accordingly, the quadtree encryption technique designed by Cheng and Li does not encrypt the intensities measured in the blocks which are the leaf nodes of the quadtree but rather encrypts the quadtree structure alone. The quadtree partial encryption can be applied to lossless image compression and lossy image compression. Other factor to be considered is the leaf node ordering for the transmission. Figure 2.2 describes the various leaf ordering that will be considered. Each of the trees illustrated in Figure 3.9 has four branches connected to the other, in the following order: NE, SW, SE, and NW quadrants; where the black leaf node is assigned the numerical value of 0, while the white leaf node is assigned the numerical value of 1. There is a weakness to some type of attacks in the case when BOI has been used, in which ordering of leaf nodes is done based on the order of leaves encoding the quad tree, in that the nodes of the tree have been placed in a preceding order. Let's illustrate the tree in figure 2.2 according to the restrictions of the leaf ordering category I, this would produce a sequence of 0010011011110010. As a consequence the authors recommend employing Leaf Ordering II, where leaves are encoded by the traversing the tree oppositely of the breadth first. This helps in enhancing the level of security. If the tree from figure 2.2 was subjected to order II leaf ordering, a binary sequence of 1111000001100101 would be attained.

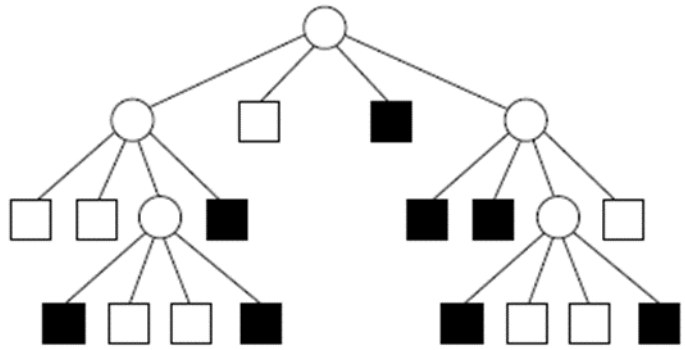


Figure 2.2 An example of a quadtree for a black-and-white (binary) image.

The zerotree wavelet-based compression algorithm is designed to send over the zerotree structure and the significant coefficients. An illustration of such compression algorithm is the SPIHT compression algorithm, where the significance of the coefficient trees is transmitted. In the SPIHT algorithm the zerotree is not encoded but rather inferred based on the significance of the coefficient sets. Furthermore, the

structure of the tree carries a considerable weight in the processing of the SPIHT algorithm. In a typical SPIHT encoded image, there are three classification of data types, the sign bits, the refinement bits and the significance bits (comprising the pixel significances and that of the sets). Just a minutia of incorrect data at the beginning of the coded block encoded by significance bits is enough to trigger trouble in the decoding stage. Generally, this issue arises in the category of significance bits because their inaccuracy leads to a wrong understanding of the significance of the following bits, which is not the case for the sign or refinement bits. Therefore, spontaneous significance information is re-coded for protection along with the primary threshold parameter n that indicates which coefficients are significant only. Moreover, the wavelet transformation structure generates a number of coefficient bands which are termed pyramid decomposition, with the figures inscribed in the bands known as pyramids levels. The authors only consider enciphering the significance information contained within the top two levels, as all other pixels and sets are present due to the composition of sets from the top two levels. Lower levels can't give any information about the first two levels' significant bits merely by inspecting their contents.

3.3 Audio and Speech Encryption Techniques

Confidentiality is paramount in the communications of many audio sequences, invariably resulting in audio compressions. At times, applying the most basic techniques could be sufficient, but in most cases, this proves to be quite costly (for example in small mobile gadgets). When it comes to information security, audio data that probably occupies the prime position is the speech data. Unlike music file and other recreational audio segments, quite a number of applications demand that level of security concerning speech. Thus this section deals with the issue of protection of speech including but not limited to MP3s as well as other audio sequences that have undergone compression.

3.3.1 Encryption of Compressed Speech

Speech scrambling with the help of technology has been in existence for many years. To demonstrate, similar to an analog video signal, initial solutions were dependent on specifically trained hardware systems which would rearrange portions or segments of speech in time, or distort the signal in the frequency domain by simply using inverters and banks of filters. These systems are extremely insecure from the computing power's perspective of today. Research today focuses on guaranteeing safety to the speech recorded in a digital state, through the use of partial or selective encryption.

Selective Encryption Algorithm for G.723.1 Speech Codec by Wu and Kuo, 2000. Among numerous digital speech codecs that exist today, the G.723.1 compression standard which is an International Telecommunication Union (ITU) recommended standard is probably the most widely used. It is also very effective as it has a very low compression ratio. This makes it ideal for transmitting voice over packet switching networks. It is also included in the ITU H.324 standard which enables and regulates the use of videoconferencing/telephony through the ordinary public switched telephone network.

Compression is implemented using analysis synthesis model. The compression encoder works with all components of the decoder which is used to generate a speech segment with respect to certain input parameters. Then the encoder manipulates the parameters until an acceptable range of distortion between the source speech and the repro generated speech is achieved. The G.723.1 modal coefficients contented along with the specific decoder used – the line spectrum pair (LSP), pitch and excitation decoders. Further, the above-mentioned codec operates in two modes of 6.3 Kbps and 5.3 Kbps.

Perception-Based Partial Encryption Algorithm by Servetti and De Martin, 2002. In the year 2002, a team of researchers by the names of Servetti and De Martin experienced a breakthrough in the usability of speech encryption techniques, where they were able to come up with a perception based scheme for partial encryption of the telephone bandwidth speech. The algorithm was implemented for the ITU-T G.729 codec for a rate of 8Kbps. In the publication of Servetti and De Martin, two methods of encrypting partially the telephonic speech were offered. The purpose of the method was low security but high bit rate (similar to the degradation schemes for videos and images). Here the aim was just to impair the speech sufficiently to preclude instant listening-in. More extensive analysis of the encrypted speech, however, could be done and would reveal the modified speech. In the second algorithm, an additional security layer is provided by encrypting a larger amount of the bit stream. Servetti and De Martin maintain that while approximately half the bit stream is encrypted, the security offered by the method is on par with that of naive enciphering.

3.3.2 Encryption of Compressed Audio

MP3 Player Most of the time, various applications exist, where the general audio data has to be secured, and the costlier elementary approach would probably be impractical. This created some research activities, focused on attempting to create solutions for selective encryption of compressed audio streams.

Copyright Protection for Music Content by Thorwirth, Horvatic, Wei and Zhao 2000, 1999. For standards compliant to perceptual audio-coding (PAC) based compressions such as MPEG-I Layer-3 (MP3), Thorwirth et al. recommended a selectable encryption system. In their suggestion, the authors focused on considering the issue of encrypting audio files encoded in the MP3 format. MP3, also known as MPEG-I layer three audio coding technology, was invented during the late years of the 1980s in Fraunhofer Institute. This codec was able to reach spectacular compression rates of 1:10- 1:12 without sacrificing the audio quality of a Compact Disc. It is a Perpetual Audio Coder (PAC) which employs advanced concepts of masking to eliminate the redundancy in raw audio digital signal. According to perceptual models, all the elements of the raw audio signal which cannot be perceived by the ear are considered as redundancy. This is the compression built-into the format called mp3 audio standard.

The usable frequency range is further divided into blocks which are referred to as audio quality layers. The lowest audio quality layer is between 20Hz and 4kHz while the highest audio quality layer which is for a compact disk quality range is between 20Hz and 22kHz. To achieve enforced audio quality control by the use of encryption, the researchers suggest that the lossy encoded audio quality layers be encrypted. The said algorithm does this by prescribing the frequency spectrum limits such that these limits help in defining the audio quality layers. The above said layer is then divided into fixed-sized blocks and a block cipher is applied to those blocks. After the encryption stage, the encrypted information can be inserted back into the MP3 bit stream rather easily, thus allowing the format to be intact. The MP3 sequences encoded in this manner are still playable by any legitimate.

Discussion

After reading this unit, think about how you could develop a novel algorithm for video encryption. Create a group with minimum of three members and provide a response based on your knowledge and experience of video, audio and speech encryption.

4.0 Self-Assessment Exercise(s)

Question 1
Describe the stages of selective video encryption
Answer

Selective video encryption encrypts only part of a video stream, focusing on essential coefficients in the compression process. It aims to balance speed and security by lightly encrypting less significant coefficients while protecting more important parts.

Question 2
Discuss the Audio and Speech Encryption Techniques:
Answer
These techniques include encryption of compressed speech and audio, utilizing methods like scrambling and partial encryption. For speech, codecs like G.723.1 and G.729 are used, with selective encryption applied to minimize computational overhead.

Question 3
Describe Partial Encryption Algorithms by Cheng and Li 2000:
Answer
These algorithms encrypt only certain parts of an image (e.g., the quadtree structure in a compressed image) to reduce computational load while maintaining security.

5.0 Conclusion

You have learnt from this unit that a multimedia security in general is provided by a method or a set of methods used to protect multimedia content. These methods are heavily based on cryptography and they enable either communication security or security against piracy. It is also oriented toward exploiting the format-specific properties of many standard video and audio formats in order to achieve the desired speed and enable real-time streaming. This is referred to as selective encryption.

6.0 Summary

At the end of this unit, you have learnt the different types of Video Encryption Techniques and the selective video encryption. The image encryption techniques; the partial encryption algorithms by cheng and Li, 2000. In the next unit, you will be introduced to multimedia encryption techniques.

7.0 References/Further Readings

Kumar, et al. (2020). Multimedia security and privacy protection in the Internet of Things. International Journal of Multimedia Information Security, 10(2), 1-12.

Milovanovic, M., Obradovic, J., & Milajic, A. (2013). Application of interactive multimedia tools in teaching mathematics--examples of lessons from geometry. Turkish Online Journal of Educational Technology-TOJET, 12(1), 19-31.

Pavithra, A., Aathilingam, M., & Prakash, S. M. (2018). Multimedia and its applications. International journal for research & development in technology, 10(5), 271-276.

Unit 3: Multimedia Encryption Techniques

Unit Structure

1.0 Introduction

Statement of problem in contemporary society reveals that as the digitalization of the business world continues evolving, and technical innovations are on an upward trend. Practically every sector of the economy throughout the globe can serve as a potential industry to distribute in-house digital multimedia content over the web. Nonetheless, the increase in the number of digital documents, the availability of multimedia processing applications and the global reach of the Internet pupils has presented the right environment for copyright piracy and reckless spread of multimedia content. Multimedia Content Security in Multimedia Networking is one of the foremost issues and challenges these days. To address those issues, two types of multimedia security systems are being designed: 1. Systems of multimedia encryption technology providing digital content distribution security over diverse distribution systems in a fuzzy end to end manner 2. Use of multimedia watermarking technology which helps to protect the copyright, trace ownership, and authenticate the content.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Discuss the various multimedia information security
- Understand the two types of cryptosystem
- Understand the several basic types of cryptanalytic attack

3.0 Main Content

3.1 Overview of Modern Cryptography

With regard to security of multimedia information, cryptography has three main objectives:
(1) confidentiality,
(2) data integrity and
(3) authentication.

Confidentiality means that the information is only accessible to the people that have permission. An undesired communicating party known as adversary should not reach the communication material. This maintenance of data integrity means that the data has not been interfered with in any unauthorized way. Finally, methods of authentication fall into two categories: entity authentication and message authentication. Message authentication guarantees that a particular person is sending the message. Such authentication also takes into account the securing of the data from modification in transit since altered data cannot belong to the particular sender. Entity authentication guarantees to the recipient of the message the identity of the sender and the fact that this person was actively involved.

Cohesive techniques – modern cryptography offers answers to these three ends. Broadly, there are two classes of cryptosystem:
(1) deterministic cryptosystem (private) key systems and
(2) public key cryptosystems.

1.2 Symmetric Key Cryptosystems

All of the classical cryptosystems, which are defined as any cryptosystems invented prior to the 1970s, fall under the category of symmetric key cryptography. In fact, the majority of practical encryption techniques employed these days are also symmetric. Some of the highly rated modern symmetric techniques include AES, DES, IDEAS and so on. One of the aspects that all symmetric key cryptography systems share is that: they all use a covert key that is only known between the parties involved in the communication. This key is employed for both encrypting the message and decrypting, thus the term “key” in the phrase symmetric encryption. This mode of cryptography provides confidentiality only and does not address the other aspects of the cryptographic goals.

Another point - the flaw of symmetric key encryption is mostly scaling. When using symmetric key based cryptography, it is very unlikely that a

big communication network can be maintained. For example, suppose we have 'n' nodes in a communication network. If one of the nodes needs to exchange confidential information to all of the other nodes, then that one node will need to posses n-1 shared keys. When n happens to be a big number like say 1000, it suddenly becomes very cumbersome. Quite the contrary, in comparison with private key systems, they are less comfortable than public key systems since symmetric key systems for equivalent security do not require large key sizes. As a result, it speeds up the processes and cuts down the space of resources needed.

1.3 Pubic Key Cryptosystems

In a public key cryptographic system, there are two keys, the first key is the public key which is available for everyone while the other is the private key that the owner, keeps to himself. The system is said to be 'asymmetric' because different keys are taken advantage of in the processes of encryption and decryption- the public key and the private key. In cases where a public key is used to encrypt any data, the exact private key is the only means of decrypting that data, and that relationship remains true for any private key. At present, virtually all crystal systems based on public keys are used for solving problems that are computationally difficult.

Public key cryptosystems by their design do not require any mutual secret among the communicating participants. This conundrum eliminates the need for the previously explained architecture for the immense confidential communication network. Also, public key systems of signing documents encouraged inventions that were meant to satisfy every purpose of cryptography. Building upon public key cryptography and the associated authentication services, complemented by secure hash functions, there exist even technologies that support the functionalities of digital signatures, authentication and data integrity.

The increase in the speed of processors, coupled with the modern cryptographic advancements, became the reason why the key sizes in public key encryption increased tremendously. This proved to be an adversary in comparison to symmetric key systems: Public key encryption is much more time-consuming and has high memory and processing power requirements. For instance, the security level of a 128 bit key for DES algorithm is equal to that of a 1024 bit key for RSA algorithm.

In addressing these issues, various strategies have been proposed by the scholars. To address the key size limitation on the use of public key cryptography in devices with limited computing capabilities like smart

cards or handheld wireless devices, Neil Koblitz came up with the idea of employing an exotic group in the public-key algebraic structure, the elliptic curve group. CertiCom has implemented almost all existing literature on elliptic curve cryptography that allows smaller keys when applying public key cryptosystems based on the DLP. The elliptic-curve algebra in group theory is very complex and so the cryptanalysis connected to it is very advanced thus making the key requirements smaller. Using more advanced magical abilities was provided also by public key cryptographic systems which earlier carried out a more complicated computational task, lattice reduction for instance. One of such is the rather recent NTRU cryptosystem, which uses a structure of a ring of truncated polynomials and which, unlike other asymmetric systems, is based on much more complicated lattice problems. To date, however, not enough studies have been conducted with regard to the security of NTRU. The most typical implementation approach is the use of hybrid cryptography, that is to say the combination of symmetric and asymmetric key encryption. Such combination is useful in resolving the hindrances posed by the sole use of symmetric key encryption whereby the actual message is encoded using a fast symmetric key technique and only the key used in the symmetric encoding is secured using an asymmetric technique such as RSA. In this way, the entire objectives of cryptography can fabric be realized who would use different Nunsons in with higher efficiency.

1.4 Cryptanalysis

Cryptanalysis is the process of compromise which includes understanding the information in a message that has been transformed through encryption without having access to the corresponding key. Depending on how much information is available, and how much the system can be controlled by the opponent (the cryptanalyst), there exist several fundamental forms of cryptanalytic attack which include:

1. Ciphertext-only attack: the adversary can access encrypted messages only (one or more). The most important goal of a proposed cryptosystem is to be able to counter this attack.
2. Brute force attack: This is a category of a ciphertext - only attack. It relies on eliminating every potential key until the correct one is found, and for cryptographic systems well conceited, this should be practically impossible. As at now, a 128-bit key is regarded as untouchable under the modern brute force method.
3. Known-plaintext attack: In such an attack, the adversary knows some portion of the plaintext that is associated with the given ciphertext. This can help in figuring out the key or part of the key.
4. Given a plaintext, an attacker can choose it and put it in the “black box” that contains the algorithm for encryption and the key for encryption. The black box will give back the corresponding cipher text

and with the given amount of plaintext-ciphertext pairs, the attacker is able to retrieve the underlying key. Or part of it, at least.
5. Chosen-ciphertext attack: In this case, an adversary is allowed to insert the selected ciphertext into the 'black box' containing the decryption algorithm along with the appropriate key. The 'black box' gives the relevant decrypted text, after which the adversary seeks to recover the dkey or some portion of it by studying the collected cipher – text/plain text pairs.

4.0 Self-Assessment Exercise(s)

Question 1:
Discuss the several basic types of cryptanalytic attack:
Answer:
Ciphertext-only attack: The adversary only has access to encrypted messages.
Brute force attack: Exhaustive key search is used.
Known-plaintext attack: The adversary knows some plaintext and ciphertext pairs.
Chosen-plaintext and chosen-ciphertext attacks: The adversary can choose plaintext or ciphertext to learn the key.

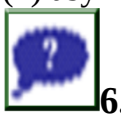
Question 2:
Discuss the two types of Modern cryptosystem:
Answer:
Symmetric key cryptosystems: The same key is used for encryption and decryption.
Asymmetric key cryptosystems: Public and private keys are used for encryption and decryption, respectively.

Question 3:
Explain the two major multimedia security technologies to mitigate the technical challenges of multimedia:
Answer:
Encryption: Ensures confidentiality during multimedia transmission.
Watermarking: Protects multimedia content by embedding a digital watermark for tracking and ownership verification.

5.0 Conclusion

You have learnt from this unit the encryption technique developed to deal with multimedia security. Modern cryptographic techniques provide solutions for these three objectives. In general, there are two

types of cryptosystem: (1) symmetric (private) key cryptosystems and (2) asymmetric (public) key cryptosystems.



6.0 Summary

At the end of this unit, you have learnt about the different types of cryptanalytic attack. In the next unit, you wil be learning about Multimedia Traffic Security.

7.0 References/Further Readings

Lu, C.-S., and Liao, M.H.-Y. (2000). Structural digital signature for image authentication: An incidental distortion resistant scheme. Proceedings of Multimedia and Security Workshop at the ACM International Conference on Multimedia, pp. 115-118.

Lu, C.-S., and Liao, M.H.-Y. (2003). Structural digital signature for image
authentication: An incidental distortion resistant scheme. IEEE Transactions on Multimedia, 5(2), 161-173.

Michael H, Andrew C, Jamie L & Aaron W. (2014). The Art of Memory Forensic: Detecting Malware and Threats in Windows, Linux and Mac memory. (1st edition). Wiley press.

MODULE 2: MULTIMEDIA AND VOIP TECHNOLOGY

Module Introduction

In the contemporary era, multimedia traffic has emerged as a pillar of communication and relation, coupled with the boom in the Internet of things, wireless sensor networks, and wearables. The growing dependence on multimedia data transfer has also given rise to its fair share of security challenges. This section seeks to offer insight into the paradigm of multimedia traffic security, the importance of safeguarding multimedia information and strategies to achieve the security of all multimedia traffic.

Unit 1: Multimedia Traffic Security
Unit 2: Techniques for Streaming Data Traffic
Unit 3: Overview of VoIP Technology

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

UNIT 1: MULTIMEDIA TRAFFIC SECURITY

Unit Structure

1.0 Introduction
2.0 Intended Learning Outcomes (ILOs)
3.0 Main Content
    3.1 Multimedia Traffic and Its Significance
    3.2 Security Threats to Multimedia Traffic
3.3 Security Measures for Multimedia Traffic
4.0 Self-Assessment Exercise(s)
5.0 Conclusion
6.0 Summary
7.0 References/Further Readings

1.0 Introduction

In connection with the evolution of the mode of communication where different components of a message are interdependent on each other like pictures, sounds, and even videos, the need to secure multimedia traffic

has emerged as an important issue of concern in today's world of computer security. Multimedia traffic is the term that refers to the movement of distinct types of data (graphics, sound, videos, and interactive materials) over various medium; the internet, or even private means of communication. This type of traffic is usual in activities such as video calls, online gaming, downloading and watching movies, and social networking, hence it is an enormous fraction of the digital activities that take place every day.

Nevertheless, multimedia traffic involves particular issues related to censorship due to a number of reasons such as the amount of particles used, need for real time delivery, and the various types of data employed. The magnitude of these files, the real-time cadence of streamplay, and the user experience expected all raise the bar concerning security for multimedia data like motion pictures, and soundtracks, etc., above forged press. Weaknesses in multimedia traffic can have dire implications such as alterations of information, breach of data, and interference with service – all of which may result in a risk to the confidentiality, integrity, and availability of information.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Identify multimedia several security threat
- Identify several measures to multimedia traffic security

3.0 Main Content

1.1 Multimedia Traffic and Its Significance

Multimedia traffic concerns the transfer of multimedia content such as graphics, sound and video across computer networks. The importance of multimedia traffic emanates from its extensive range of use in diverse sectors such as entertainment, education, and communication. Wherein, as a growing trend, multimedia data faces the biggest threat to security from its sheer volume and diversity. Therefore, the safety of multimedia traffic is paramount in averting unauthorised usage, alteration or rip-off of confidential data.

Multimedia traffic is also defined by the dimensions of volume, velocity and variety. One of the reasons for the huge amount of multimedia traffic is the increased deployment of multimedia applications like

teleconferencing, online interactions like gaming and social networking. The high velocity in transmission of multimedia traffic comes about as a result of the requirement for immediate or real time processing and streaming of the multimedia materials. There will be images, videos, sound files and so on which are the components of multimedia and all these together create a problem in terms of security.

Multimedia traffic is all about the communication of multimedia information like photographs, videos, audio and interactive activities over computer networks. With the increased use of the internet, network bandwidth is filled mostly by data which can be classified as multimedia content. Sites offering video on demand to social networking, e-learning, video conferencing and even online gaming, all involve multimedia in one way or the other. Because so much content is created, disseminated and consumed in this way, appropriately handling and controlling media traffic and meeting the expectations of end users becomes crucial in performance and security of the system.

Key Characteristics of Multimedia Traffic

Multimedia traffic exhibits distinct characteristics that differentiate it from traditional data traffic, making its management more complex. These include:

High Volume
Multimedia files, especially videos, can be large, contributing to a massive volume of traffic. Streaming services like YouTube, Netflix, and live gaming can generate billions of gigabytes of data daily.
High Bandwidth Requirements
Due to its large size and complexity, multimedia content requires higher bandwidth to ensure smooth and uninterrupted transmission. Bandwidth is essential for real-time streaming, such as video conferencing, where any delays can lead to buffering or low-quality playback.
Real-time Transmission
Unlike text-based data, multimedia often requires real-time processing and delivery. For instance, live video streams and video conferencing depend on the ability to transmit and receive data without delays or interruptions.
Variety of Formats
Multimedia traffic includes diverse file types (images, audio, video, animations, etc.), each with its own requirements in terms of encoding, compression, and transmission protocols.

Why Multimedia Traffic Security is Important

The increasing dependence on multimedia applications in various sectors, including entertainment, education, healthcare, and business, makes the security of multimedia traffic critical. For instance, an organization might use video conferencing for confidential meetings, which must be secured to prevent eavesdropping or data breaches. Similarly, streaming services need to protect copyrighted content from unauthorized access or piracy.

Hackers can exploit weaknesses in the transmission of multimedia data to:

Eavesdrop on communications (such as VoIP calls or video conferences), Tamper with multimedia streams, altering videos, images, or audio files, launch denial-of-service (DoS) attacks that disrupt services like video streaming or conferencing.

Significance of Multimedia Traffic

Multimedia traffic is crucial for various sectors, from entertainment to education and business. Its significance can be understood through the following points:

Global Communication
Multimedia has revolutionized communication. Voice over IP (VoIP), video calls, and conferencing tools (e.g., Zoom, Skype) allow real-time communication across the globe, removing geographical barriers and enhancing collaboration in personal and professional environments.

Entertainment
Platforms such as Netflix, YouTube, and online gaming services rely on the efficient transmission of multimedia traffic to provide users with high-quality streaming experiences. Entertainment is one of the most significant drivers of multimedia traffic today.

Education
E-learning platforms and digital education systems make extensive use of multimedia. From video lectures to interactive tutorials and virtual classrooms, multimedia traffic supports modern educational models that enhance learning experiences globally.

Business and Enterprise Applications
Many businesses depend on multimedia traffic for webinars, video conferencing, virtual meetings, and real-time collaboration. Companies also use multimedia in marketing, product demonstrations, and online training.

Social Media and Content Sharing
Social platforms like Instagram, TikTok, and Facebook are powered by multimedia traffic, enabling users to upload, share, and view videos, images, and audio. Multimedia content is central to user engagement on social media.

Healthcare (Telemedicine)
Telemedicine and remote healthcare consultations rely on multimedia traffic for transmitting medical imaging, conducting video consultations, and sharing health records securely between patients and healthcare providers.

Real-time Systems
Multimedia traffic is critical for real-time systems such as surveillance, live broadcasts, online gaming, and IoT applications, where timely delivery of audio, video, and data is essential for functionality.

Key Components of Multimedia Traffic Security

To ensure the protection of multimedia traffic, several security measures need to be implemented:

Encryption: Encryption transforms multimedia data into a secure format that can only be accessed by authorized users. Protocols such as Secure Real-Time Transport Protocol (SRTP) are used to encrypt real-time multimedia traffic like video calls and live streaming.

Access Control: Proper authentication and authorization mechanisms ensure that only authorized individuals can access or manipulate multimedia content, safeguarding it from unauthorized users.

Digital Watermarking: Embedding invisible marks into multimedia files can help track and identify unauthorized distribution, particularly important for protecting intellectual property.

Intrusion Detection Systems (IDS): These systems monitor network traffic for unusual patterns and alert administrators to potential security breaches, such as attempts to intercept or disrupt multimedia streams.

Firewalls and Secure Gateways: These technologies help filter and block malicious traffic, ensuring that multimedia streams are transmitted securely and without disruption.

Challenges in Managing Multimedia Traffic

Managing multimedia traffic comes with a set of challenges, primarily due to its complexity and the demands of real-time delivery. These challenges include:

Quality of Service (QoS)

Ensuring high-quality service is crucial for multimedia applications. Delays, packet loss, and jitter can negatively impact user experience, especially for real-time applications like video conferencing or live streaming.

Bandwidth Constraints

Multimedia traffic consumes large amounts of bandwidth. Networks must be equipped to handle peak traffic without slowing down or compromising the quality of service.

Security Concerns

Multimedia traffic is vulnerable to security threats such as data interception, unauthorized access, and manipulation. Protecting multimedia data through encryption and secure protocols is vital.

Latency and Delay

In multimedia traffic, particularly in real-time applications, even slight delays can lead to poor user experiences. Network optimization is crucial to minimize latency.

3.2 Security Threats to Multimedia Traffic

Multimedia traffic faces several security threats, including:

1. **Data Tampering**: Unauthorized modification of multimedia data can lead to loss of integrity and authenticity.
2. **Data Theft**: Theft of multimedia data can result in unauthorized access and misuse.
3. **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks**: These attacks can disrupt multimedia data transmission, causing service disruptions and financial losses.
4. **Social Engineering**: Unaware employees can be targeted by social engineering attacks, compromising network security.

3.3 Security Measures for Multimedia Traffic

To ensure the security of multimedia traffic, several measures can be implemented:

1. **Encryption:** Encrypting multimedia data using algorithms like AES and RSA can prevent unauthorized access.
2. **Digital Watermarking:** Embedding digital watermarks in multimedia data can help track and identify unauthorized use.

3. **Firewalls and Intrusion Detection Systems:** Implementing firewalls and intrusion detection systems can prevent unauthorized access and detect potential threats.
4. **Access Control:** Implementing access control measures, such as authentication and authorization, can restrict unauthorized access to multimedia data.
5. **Regular Updates and Maintenance:** Regularly updating software and hardware, as well as performing routine maintenance tasks, can help prevent security vulnerabilities.

Multimedia traffic security is a critical concern in today's digital landscape. The increasing reliance on multimedia data transmission has led to a surge in security threats, making it essential to implement robust security measures to protect multimedia traffic. By understanding the significance of multimedia traffic and the security threats it faces, organisations can take proactive steps to ensure the integrity and confidentiality of their multimedia data.

 **Discussion**

After reading this unit, explain multimedia traffic security. Start your response by clearly stating various mode to traffic security.

 **4.0 Self-Assessment Exercise(s)**

Question 1: What is multimedia traffic, and why is it significant in today's digital landscape?

Answer
Multimedia traffic refers to the transmission of multimedia content, such as images, audio, video, and interactive data, over computer networks. It is significant because it supports critical services like video streaming, online communication (VoIP, video conferencing), e-learning, real-time gaming, and social media. As multimedia content consumes more bandwidth and requires real-time transmission, managing its security and performance is essential for ensuring a seamless user experience and protecting sensitive information from unauthorized access.

Question 2: List and explain three key characteristics of multimedia traffic.

Answer

High Volume: Multimedia content, especially videos, consumes significant amounts of data, leading to high traffic volumes on networks.

Real-time Processing: Multimedia traffic often requires real-time transmission, particularly for live video streaming, video conferencing, and gaming, where delays or interruptions can degrade the user experience.

High Bandwidth Demand: Due to the large file sizes of multimedia content, networks must provide sufficient bandwidth to support smooth and uninterrupted transmission, especially for high-definition video and interactive content.

Question 3: What are the common security threats associated with multimedia traffic?

Answer
Common security threats to multimedia traffic include:

Data Tampering: Unauthorized modification of multimedia content, which can compromise its integrity.

Eavesdropping: Intercepting multimedia communications, leading to potential breaches of privacy.

Denial of Service (DoS) Attacks: Disrupting multimedia services by overwhelming the network with excessive traffic, leading to service downtime.

Data Theft: Unauthorized access to sensitive multimedia data, such as videos or images containing personal or confidential information.

Question 4: Describe two common techniques used to secure multimedia traffic.

Answer

Encryption: Encryption algorithms, such as AES (Advanced Encryption Standard), are used to protect multimedia data from unauthorized access by converting it into a coded format that can only be decrypted by authorized users.

Digital Watermarking: This technique embeds invisible marks or metadata into multimedia content, allowing content owners to track and identify unauthorized usage or distribution, thus safeguarding intellectual property.

Question 5: What challenges are faced when managing multimedia traffic security, and how can they be addressed?

Answer
Challenges in managing multimedia traffic security include:

Bandwidth Constraints: The high bandwidth requirements of multimedia content can overwhelm networks, leading to performance issues. This can be addressed by using content delivery networks (CDNs) and optimizing data compression techniques.

Real-time Security: Real-time multimedia services such as video conferencing demand low latency and high security. This challenge can be addressed by implementing Secure Real-time Transport Protocol (SRTP) to encrypt and protect real-time multimedia traffic without causing significant delays.

Quality of Service (QoS): Ensuring the smooth delivery of multimedia while maintaining security is difficult. Using QoS mechanisms can help prioritize multimedia traffic to reduce delays and packet loss.

5.0 Conclusion

Multimedia traffic security is a critical concern in today's digital landscape. The increasing reliance on multimedia data transmission has led to a surge in security threats, making it essential to implement robust security measures to protect multimedia traffic. By understanding the significance of multimedia traffic and the security threats it faces, organizations can take proactive steps to ensure the integrity and confidentiality of their multimedia data.

6.0 Summary

At the end of this unit, you have learnt the measures to put in place for multimedia traffic security. In the next unit, you learn about techniques for Streaming Data Traffic.

7.0 References/Further Readings

Lata, N., & Kumar, R. (2022). Communication technologies, smart home solution and security trends in Internet of Things. Journal of Algebraic Statistics, 13(1), 42-61.

Liu, Y., & Ko, Y. C. (2021). Image processing method based on chaotic encryption and wavelet transform for planar design. Advances in Mathematical Physics, 2021(1), 7511245.

Pommer, A., Uhl, A., Okša, G., Trobec, R., Vajtersic, M., & Wyrzykowski, R. (2000, September). Multimedia soft encryption using NSMRA wavelet packet methods: Parallel attacks. In Proc. Int. Workshop on Parallel Numerics (ParNum'2000) (pp. 179-190).

Singh, I., & Lee, S. W. (2022). Self-adaptive and secure mechanism for IoT based multimedia services: a survey. Multimedia Tools and Applications, 81(19), 26685-26720.

UNIT 2: TECHNIQUES FOR STREAMING DATA TRAFFIC

Unit Structure

1.0 Introduction

Streaming data traffic has become a crucial component of modern data management, enabling organizations to harness real-time insights and drive business decisions. This report aims to provide a comprehensive overview of general knowledge and techniques for streaming data traffic, covering key concepts, best practices, and challenges.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Identify Characteristic of streaming data traffic
- Understand the concepts and techniques of data traffic
- Understand the pracitice for streaming Data traffic
- Identify the key components of a data streaming

3.0 Main Content

3.1 Understanding Streaming Data Traffic

Streaming data traffic refers to the continuous flow of data from various sources, such as sensors, IoT devices, social media, and applications,

into a data processing system. This data is typically processed in real-time to extract valuable insights, detect patterns, and make predictions. The key characteristics of streaming data traffic include:

1. High Volume and Velocity: Streaming data traffic involves processing large volumes of data at high speeds, often exceeding millions of events per second.
2. Variety and Veracity: Streaming data traffic encompasses diverse data types, including structured and unstructured data, and requires robust mechanisms to ensure data quality and integrity.
3. Real-Time Processing: Streaming data traffic demands real-time processing to enable timely decision-making and minimize latency.

3.2 Key Concepts and Techniques

1. Streaming Data Processing: Streaming data processing involves processing data as it is generated, often using distributed systems and scalable architectures.
2. Streaming Data Integration: Streaming data integration involves integrating data from multiple sources, transforming it into a unified format, and processing it in real-time.
3. Streaming Data Analytics: Streaming data analytics involves analyzing data in real-time to extract insights, detect patterns, and make predictions.
4. Streaming Data Storage: Streaming data storage involves storing data in a way that allows for efficient retrieval and processing, often using distributed storage systems.

3.3 Checking for Obfuscation

1. Take a Streaming-First Approach: Design data integration and processing pipelines with a streaming-first approach to ensure real-time data processing.
2. Use Streaming SQL: Utilize Streaming SQL to analyze data in real-time, enabling fast and efficient querying of large volumes of data.
3. Optimize Data Flows: Optimize data flows by minimizing disk I/O, using in-memory processing, and leveraging parallel processing to ensure high performance.
4. Monitor and Manage: Continuously monitor and manage streaming data traffic to ensure data quality, integrity, and performance.

3.4 Challenges and Solutions

1. Data Quality and Integrity: Ensure data quality and integrity by implementing robust data validation, cleansing, and transformation mechanisms.
2. Scalability and Performance: Scale streaming data processing systems to handle high volumes of data while maintaining performance and low latency.
3. Data Integration and Processing: Integrate and process data from diverse sources, transforming it into a unified format for real-time analysis.
4. Real-Time Analytics and Decision-Making: Enable real-time analytics and decision-making by leveraging streaming data processing and analytics tools.

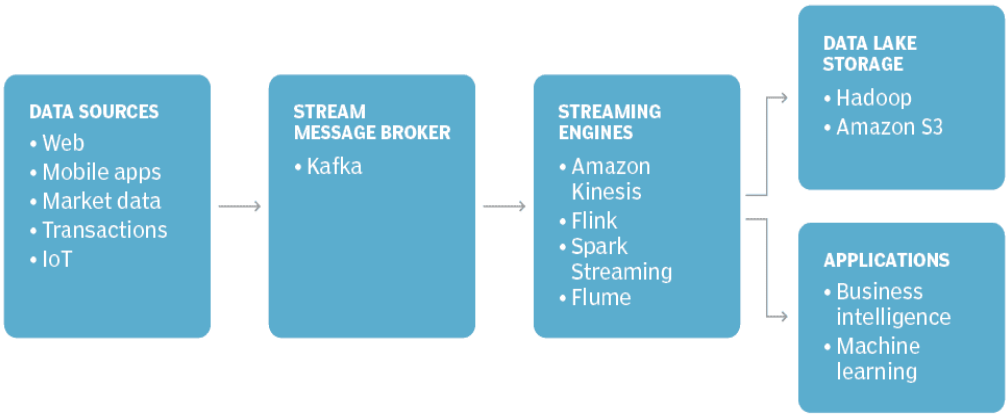
3.5 Key Components of Data Streaming System

1. **Message Broker**: This component takes data from various sources and standardizes it into a common message format. It then sends the data to other components for further processing. Examples include Apache Kafka and Gazette
2. **Stream Processor**: These tools receive the output messages from the message broker and make the required changes or adaptations. Such changes or adaptations can take the form of filtering, aggregating, joining, or enhancing the information so as to make it more applicable to the subsequent systems. Some frequently used processing tools are Apache Spark Streaming, Apache Flink, and Storm.
3. **Data Storage**: Due to the enormous amount of streaming data produced, it must be stored in a manner which allows the data to be accessed rapidly and efficiently by downstream applications. There are different types of data storage systems that can be adopted in data streaming architectures which include in-memory databases, distributed file systems, and NoSQL databases. These continuous data are mostly stored in data lakes like Azure Data Lake Store or Google Cloud Storage, thanks to their versatility and ability to deal with large variabilities of data, and many volumes of it.
4. **Analysis, Reporting, & Visualization Tools**: These instruments serve the purpose of evaluating the information that is being consumed and obtaining useful information from it. This means employing models of machine learning to recognize a pattern in the data, or the lack of it, as well as performing statistical operations in order to find features in the data, such as trends or relationships. The information obtained from the conducting of the analysis as a result is easy to read and contains all essential

materials due to use of reporting tools. Perspectives are provided by visualizing the data by making composed images incorporating numbers, drawings or maps containing the observations or information derived from the data. Grafana, Tableau, and Power BI are some of the most commonly preferred tools for the purpose of performing real time analytical operations on streaming data.

5. **Adapters**: Transducers modify the incoming data to a format understandable by the engine for stream data processing and subsequently transmits the data to the engine for stream processing. Following the data processing engine is a device known as output adapter which changes the modified data to a required format before releasing the data out.
6. **Stream Data Processing Engine**: This component processes input data in accordance with a pre-registered query or filter and then sends the data to the output adapter
7. **Query Groups**: Query groups represent the analysis scenarios that the stream data processing engine adheres to when determining how to process input data. A query group consists of an input stream queue (input stream), query, output stream queue (output stream). The query defines how input data is to be processed
8. **Aggregators**: Aggregators collect event streams and batch files and pass them onto brokers
9. **Brokers**: Brokers make data available for consumption or ingestion by a streaming data engine that blends streams together
10. **Streaming Data Storage**: Advancements in cloud storage technology, data warehouses, and data lakes have made storing streaming event data economical. Many businesses can easily retain detailed records on all their operations, capable of pulling historic records, and are able to do so without having to own the infrastructure themselves.

These components work together to enable organizations to analyze and act on a data stream in real time, rather than waiting for batch processing.



Stream Processing Architecture

Streaming data traffic has become a critical component of modern data management, enabling organizations to harness real-time insights and drive business decisions. By understanding key concepts, techniques, and best practices, organizations can effectively manage and process streaming data traffic to achieve competitive advantages.

3.6 Benefits of Data Streaming in the Telecommunications Sector

1. **Fraud Detection**: Understanding of call and data usage trends to identify and mitigate risks of fraud, thereby maintaining the safety and fairness of the system
2. **Performance Analysis**: Determining where the network bottlenecks exist and increasing the capacity to meet that demand to achieve proper service quality with minimum downtimes.
3. **Service Personalization**: Adjusting the telecommunications services to suit each customer according to their recent usage patterns, thus boosting customer satisfaction and retention.
4. **Network Monitoring**: Identifying and fixing network problems in an anticipatory manner, minimizing interruption of service and enhancing the level of service for customers.

The advantages empower telecom organizations to utilize real-time information for operational improvements, enhanced experiences of consumers, and advantages in competition.

Discussion

Practical Question: You are part of a team tasked with designing an online video streaming platform similar to Netflix or YouTube. The platform will serve millions of users globally, delivering high-quality video content in real-time. Given the diverse user base, the platform must support both high-definition (HD) and standard-definition (SD) streaming while ensuring minimal buffering, low latency, and high

reliability. Additionally, the platform needs to optimize network resources, prevent congestion, and ensure content security.

Discussion Question

How would you design the data streaming architecture to balance quality, bandwidth, and latency?

Consider aspects like data compression, real-time traffic management, buffering strategies, and security protocols. How would you handle streaming for users with limited bandwidth without sacrificing too much quality?

What specific techniques and technologies would you implement to ensure a smooth user experience in various network conditions?

Discuss the role of Content Delivery Networks (CDNs), adaptive bitrate streaming, and protocols like RTP or HTTP Live Streaming (HLS). How would you prioritize streaming traffic to minimize interruptions and ensure a high quality of service (QoS)?

How would you ensure the security of multimedia content during streaming?

Explore methods such as encryption, digital rights management (DRM), and watermarking. How would you protect the platform from security threats like piracy or data interception?

Engagement Prompt: You and your classmates are encouraged to collaborate and come up with a streaming strategy that addresses both technical challenges and user experience. Consider real-world streaming platforms as examples and share your thoughts on how they successfully manage these challenges. What can be improved or optimized in those systems? Feel free to present any innovative ideas or approaches!

4.0 Self-Assessment Exercise(s)

Question 1

Highlight the challenges and solutions of data streaming:

Answer

Challenges: Ensuring data quality, scalability, real-time processing, and integration.

Solutions: Implement robust validation mechanisms, scale architectures, and optimize data flow through in-memory and parallel processing.

Question 2

Identify the practices for streaming data traffic:

Answer

Use a streaming-first approach.
Utilize streaming SQL for real-time analysis.
Optimize data flows and monitor systems continuously.

Question 3

List and discuss the key concepts and techniques for data streaming:

Answer

Streaming data processing: Processing data in real-time.
Streaming data integration: Combining data from multiple sources.
Streaming data analytics: Analyzing real-time data for insights.
Streaming data storage: Efficient storage systems for quick data retrieval.

5.0 Conclusion

You have learnt from this unit techniques for streaming data traffic and understand the streaming data traffic with their various concepts and techniques. Various benefits of data streaming were discussed and these benefits enable telecommunications companies to harness the power of real-time data to improve their operations, enhance customer experiences, and stay ahead of the competition.

6.0 Summary

As you have learnt, data streaming as a tool for fraud detection, performance analysis and network analysis in the telecoms sector. These benefits enable telecommunications companies to harness the power of real-time data to improve their operations, enhance customer experiences, and stay ahead of the competition.

7.0 References/Further Readings

Kumar, et al. (2020). Multimedia security and privacy protection in the Internet of Liu, W. (2021). Research on the application of multimedia elements in visual communication art under the internet background. Mobile Information Systems.

Queiroz, W., Capretz, M. A., & Dantas, M. (2019). An approach for SDN traffic monitoring based on big data techniques. Journal of Network and Computer Applications, 131, 28-39.

Sait, A. R. W., Uthayakumar, J., Shankar, K., & Kumar, K. S. (2019). Introduction to multimedia tools and applications. Handbook of multimedia information security: Techniques and applications, 3-14.

Shahraki, A., Abbasi, M., Taherkordi, A., & Jurcut, A. D. (2022). A comparative study on online machine learning techniques for network traffic streams analysis. Computer Networks, 207, 108836.

Things. International Journal of Multimedia Information Security, 10(2), 1-12.

UNIT 3: OVERVIEW OF VOIP TECHNOLOGY

Unit Structure

1.0 Introduction

In recent times, global communication can be said to have improved due to global movements of people and advancements in communication. The use of wireless technologies has removed the hassle of having to deal with cabled connections. The existence of cell phones means that one's mobility from place to place does not limit one's accessibility to other people. In spite of the fact that the invention of communication has always aimed at enabling faster horizontal and vertical communication amongst people, the aspects of communication and networking have refocused over time to include enhancement of quality, reliability efficiency, flexibility, security and many others.

Nonetheless, investment is required to even set up the necessary infrastructure for the architectural model development. This made it so that, except for government officials and civil service agencies, communication networks were available only to the rich in the early days. Over time, the evolution of mainstream trunked systems that

enabled ordinary telephones and the introduction of digital technologies for coaxial cables, the new generations of mobile phones enabled the communication to the general public, Distribution of communication. Afterward, the networking also has had a steady pollution due to increasing usage of the Internet and the World Wide Web, which enabled data to be transferred from one area to another. Later, in order to facilitate communication at less cost and also to integrate voice services with data services, facilities came up known as Voice over Internet Protocol or VOIP.

Much effort has been invested in carrying out feasible strategies for deploying and maintaining VoIP in real-life networks, which has and continues to lead to the gradual increase of VoIP subscribers. The success of designers in this field has spurred research on the possible incorporation of VoIP into Public Switched Telephone Networks (PSTN) and cellular networks through the design of interfaces and gateways. Two main approaches can be pointed out in regard to the market strategies aimed at making VoIP commercially viable to consumers. The first policy is the one most of the service providers of VoIP tend to use in relation to service which is mainly the deployment of VoIP with an array of VoIP servers, VoIP enabled phones, private branch eXchange (PBXs), gateways, etc. Apart from this, some providers go ahead and develop both hardware and software modules to assist people in the understanding and practical utilization of VoIP systems as well as in the further developments of the technology within this field. This second strategy is applied by many application developers who want to utilize VoIP technologies within their applications in order to reach more users, for example, in case of social games and social networks.

As it is with every advancement in technology, the challenges of scalability have impeded the development of VoIP and the problems are made worse with the demanding Quality of Service (QoS) standards. This book explains the issues concerning VoIP and provides solutions on the improvement of real time VoIP calls in suboptimal networks. Voice over IP (VoIP) came into being with the convergence of internet and telecommunications with the aim of cutting down the costs of communication whilst integrating data with voice services.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit you will be able to:

- Identify what is voice over IP (VoIP)
- Discuss the three fundamental classes of VoIP

- Understand the communication aspects for different applications

3.0 Main Content

3.1 What is Voice over IP (VoIP)?

VoIP, or Voice over Internet Protocol, is the routing of voice transmissions over the Internet or through any other Internet Protocol (IP) network. Rather than the old-fashioned lines for transmitting voice signals alone through circuit-switched systems, voice is carried instead over a common unreserved packet-switched network. For communication of voice information, it is broken up into smaller packets as is also done in the transmission of data. Packets are pieces of information that have been divided into manageable routing size. Subsequently, the division of information into packets has to be followed by the sending of packets and their reassembly in a structured way. The Real-time transport protocol (RTP) is a common protocol for delivering audio and video over the internet, including a standardized packet format. Also, the voice also needs to be made compressive in such a way that it takes up less space and captures only a specific range of frequencies. This too can be done through the use of relevant techniques.

There are various standards for implementing VoIP services, and the guidelines include session initiation protocol (SIP) and H.323. Those protocols enable users to perform multimedia communication (voice, with video or simply data) over the IP networks. Nonetheless, they are different in a significant manner. For instance, H.3260 has much of its content from the older systems and is therefore an umbrella standard made up of many standards. In contrast, SIP is more advanced than H.3260 in that it does not fill itself with information elements from the past and it is a provided ASCII protocol.

The aims behind the implementation of VoIP technology are as follows: (a) To reduce network maintenance and operations costs by a substantial margin and (b) To introduce new services at the earliest possible time.
Indigenous technologies like multimedia messaging service (MMS), video conferencing, voicemail and other types of Voice Over Internet Protocol (VoIP) services are increasingly accepted into the economies. This is demonstrated in figure 5.1. The mobile applications are divided into three categories: calling, messaging and mailing, depending on the type of communication. Thirdly, the services are classified according to the features of different senses – text, image, voice or video – that they provide. In figure 5.1, there is an increase in the end to end delay allowances of the services as one moves from down to top (from the

mailing to the calling in this case) and the end user value also increases with it. On the contrary, the capacity requirements also increase as one

	PBX-like VoIP	PSTN-like VoIP	IM-like VoIP

moves from left to right (i.e. from text to video).

1. VoIP services can be provided over the internet in many ways with the network and the servers being managed by different players. Pricing schemes, addressing models, interconnection to Public Switched Telephone Networks (PSTN) and mobile networks, and regulation also show variation. The classification introduced considers that such phenomena as VoIP can be classified according to the basic services that they could be analogized with. These include:

1. VoIP as we have it in PBX,
2. VoIP which fits into conventional telephony systems, and
3. VoIP as in Instant Messaging.

In most cases, this type of VoIP service is found in large corporations where effective communications at cheap rates are possible. Neither is It household service as in IP telephony replacing the geography-based PSTN telephone system in small enterprises. Simple VoIP, on the other hand, is directed more on the World Wide Web users.

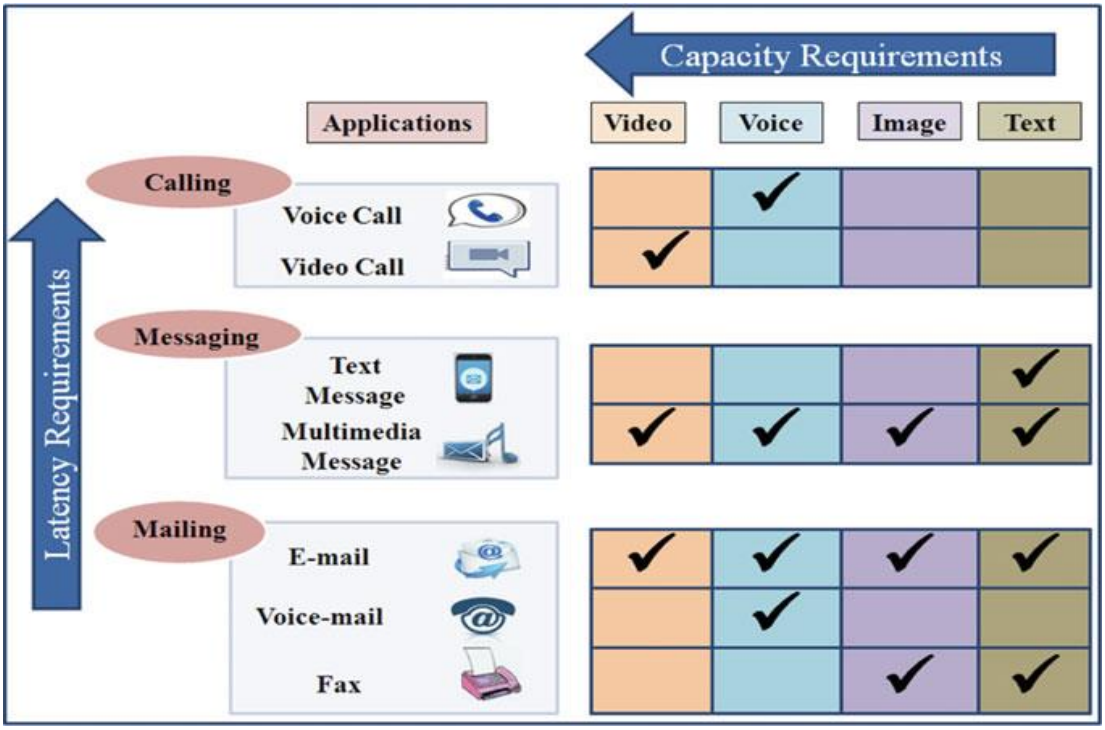


Figure 5.1 Communication aspects for different applications

Their characteristics are summarized in Table 5.1.

Table 5.1. VoIP Classes

Domain	Fixed, wireless	Fixed, wireless	Fixed, wireless, mobile
Target users	Large enterprises	Consumers, small business	Consumers
Managed by	Corporation (IP PBX)/local service provider (IP Centrex)	Broadband ISP/local service provider	Global service provider
Typical pricing scheme	Free calls inside the LAN PSTN-like pricing on outgoing calls	Free/low-cost calls to other VoIP users, PSTN-like pricing on outgoing calls	Free calls to other VoIP users, PSTN-like pricing on outgoing calls
QoS control	High	Medium/low	Low
Examples	Cisco Call Manager	Vonage, Net2phone (U.S), Ipon, Sonera	MSN Messenger, Yahoo! Messenger, Skype.

Among the main objectives of the application of VoIP technology is (a) significant reduction of costs for the maintenance and operations of existing networks and (b) deployment of new services within a short period of time. In this connection, It is worth noting that implementation of VoIP could take place through various networks such as wireless local Area networks (WLAN), WiMax, mobile systems including cellular networks, and cognitive radio networks. Each one of these networks has its own standards and regulations, which bring different issues that need to be solved in order to implement VoIP.

3.2 Reasons for Implementing VoIP

VoIP technologies presented as one where a service provider can avoid the deployment of expensive voice transport networks and instead offer voice services over the internet using data transport networks because there was no cost of transport of packets over IP networks. Over time, it started finding uses in people's homes and also office networks. The reasons for the popularity and success of VoIP can be summarized in the following factors.

A. The simple provision of this system on the other hand – Several functions which in the past necessitated multiple geographical locations have been made possible with the VoIP system largely thanks to the innovative capabilities of the VoIP call controllers eliminating administrative hitches and speeding postal policy deployment.

B. Reduced Complexity of Transport Networks—After certain adjustment, standard IP networks can as well serve the transmission of VoIP packets, thus eliminating the need of prior encumbering

investments in dedicated voice leased lines before the commencement of business.
C. Cost reduction—There is a massive decline in operational and maintenance cost. This is largely advantageous to businesses whose operations involve making a lot of phone calls every day, or those who make expensive overseas calls.
D. Enhanced services—VoIP system can also facilitate and provide additional services to customers like MMS, PTT and many others.
E. Anytime, anywhere communication— With IM-based VoIP, the customers having access to the Internet and registered account can communicate at any time and place as there are no inconveniences like the ones presented by infrastructure-based means of communication.
F. Easy upgradation—Owing to the easy operational characteristics of VoIP systems; it is easy to modernize the services offered under the technology.

Nonetheless, since VoIP transmits speech in an IP network which is a normal “best-effort” packet delivery, a certain level of QoS is expected. Voice warranty must be ensured aggressively as it is real time and very sensitive to loss. Additionally, there is potential for risk since voice packets can be intercepted and personal affiliations can be infiltrated.

A VoIP service would allow a provider to offer voice transmission over the Internet thanks to the 'free' transport of data packets over the IP networks. However, as VoIP operates over IP which is the “best-effort” protocol, it requires certain QoS guarantees.

4.0 Self-Assessment Exercise(s)

Question 1
What is Voice over IP (VoIP)?
Answer
VoIP is the transmission of voice communications over IP networks. It breaks voice data into packets and reassembles them using protocols like RTP for efficient real-time communication.
Question 2
Discuss the three fundamental classes of VoIP
Answer

- **PBX-like VoIP**: Used in enterprises for internal communication.
- **PSTN-like VoIP**: Replaces traditional phone services in homes and small businesses.
- **IM-like VoIP**: Targets internet users for casual communication via platforms like Skype or WhatsApp.

5.0 Conclusion

You have learnt from this unit the three fundamentally different classes of VoIP. The characteristic of each were summarized in a tabular form. VoIP is a technology that enables routing of voice communications through Internet or any other Internet protocol (IP)-based networks.

6.0 Summary

A number of protocols are applied in the provision of VoIP services and the more prominent of them all is SIP and H.323. These protocols aim at enabling users to communicate in various formats (audio, video and data depending on what is appropriate) over the IP networks. However, they are very different in terms of internal architecture. For example, H.323 is fond of upward compatibility as it contains many elements of traditional communication system and is a family of protocols. On the contrary, SIP is not a content addressing system as it contains minimal to zero communication elements of the traditional systems and is a text based protocol.

7.0 References/Further Readings

Alsharida, R., Hammood, M., Ahmed, M. A., Thamer, B., & Shakir, M. (2021). RC4D: A New Development of RC4 Encryption Algorithm. In Selected Papers from the 12th International Networking Conference: INC 2020 12 (pp. 19-30). Springer International Publishing.

Amalou, W., & Mehdi, M. (2022). An approach to mitigate DDoS attacks on SIP based VoIP. Engineering Proceedings, 14(1), 6.

Chen, L., Xia, C., Lei, S., & Wang, T. (2021). Detection, traceability, and propagation of mobile malware threats. IEEE Access, 9, 14576-14598.

Nazih, W., Elkilani, W. S., Dhahri, H., & Abdelkader, T. (2020). Survey of countering DoS/DDoS attacks on SIP based VoIP networks. Electronics, 9(11), 1827.

Signes-Pont, M. T., Cortés-Castillo, A., Mora-Mora, H., & Szymanski, J. (2018). Modelling the malware propagation in mobile computer devices. Computers & Security, 79, 80-93.

Suthar, D., & Rughani, P. H. (2020, December). A comprehensive study of VoIP security. In 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 812-817). IEEE.

MODULE 3: HISTORY AND VOIP SECURITY

Module Introduction

The Voice over Internet Protocol (VoIP), as an advanced technology, has captured a lot of attention in the recent past. IP telephony systems or other types of VoIP applications make it possible to transmit voice over packet based data networks, either private or public. The process of VoIP simply involves the sending of voice data in packets over a certain network, then decoding and assembling the data at the other end. As a result, concern for safety is the chief obstacle that has made most companies shy away from adopting VoIP technology for their operations. Making IP telephony secure is a complex undertaking due to the breadth of areas covered, ranging from cryptography to control access implementation. In a straight forward manner, the known progress – called engineering of a security policy – begins with risk analysis and culminates with model for the security policy containing numerous security assertions ready for embedding into the security framework.

In this subsection, we first analyze some of the theoretical aspects of security in VoIP, the threats and vulnerabilities associated with VoIP protocols and technologies. We then discuss how a VoIP security policy can be viewed in terms of communication and application security properties: confidentiality, integrity and availability of the VoIP applications. And lastly but not the least, a security policy framework is suggested that is viewed through the practice of network security to assist in developing a security framework for mobile VoIP applications in the near future.
This module is classified into the following three (3) units:

Unit 1: Evolution of VoIP
Unit 2: Fundamental Elements for VoIP Deployment
Unit 3: Security Issues of VoIP

In every unit, I will look into the specific theme in detail, and I will underline individual evaluation activities towards the end of the unit. And lastly, I underline Readings for Further Studies at the end of every unit.

UNIT 1: EVOLUTION OF VOIP

Unit Structure

1.0 Introduction

VoIP as a concept would not be possible without two basic technologies – the telephone and the Internet. Telephony began in 1844, thanks to Samuel Morse who invented the telegraph enabling the transmission of short electric pulses over long distances… longer than any person, or even horse can travel. This led to the development of the first telephone by Graham Bell on the 10th day of march 1876. Come 1906, the 1st vacuum tube was conceptualized by Lee De Forest, an American inventor who advanced electronics making it possible to amplify both sound and picture, including telegraph and telephone signals. The 1920s witnessed the first successful use of voice communication systems that employed amplitude modulation. In the years that followed, the public sphere expanded considerably due to the advent of numerous radio station broadcasts which made possible the concepts of real time communication through information dissemination. Certainly however, there still existed some form of wires because the radio was not dependable due to other factors.

2.0 Intended Learning Outcomes (ILOs)

BY the end of this unit, you will understand how VoIP works and the technology behind it evolution.

3.0 Main Content

3.1 Telephone Technology

While other forms of communications were replaced by the telephone technology, in the modern world, the telegram remained used as a medium of data transmission through telegraphy. Advancements in radio technology came at around the 1930s where the invention of frequency modulation (FM) was advanced offering clearer audio and less prone to disturbances than the older AM broadcast system. The post-World War II period was an era of great advancement where the transistor (December 1947) and computing devices were invented. These machines made it easy for individuals to collect and share gigantic volumes of information at a very high rate. The epoch of space exploration and aviation technology began on the fourth of October 1957 when the Soviet Union successfully launched its first satellite Sputnik. Satellite communication enabled provision of adequate and efficient long distances communications by either supplementing or replacing wires. Anytime, anywhere communication became a necessity for many. Nevertheless, it took nearly twenty-six years after the launch of Sputnik before the rest of the world was able to utilize cell phones to make voice communications in real time.

Long before cell phones were invented, in order to have a conversation with someone, a person would dial an operator and provide them with the name or a number of the person they wanted to connect with. After which, the operator would use a patch cord to hook up the two people's telephones through their respective wall jacks. Between exchanges, a series of wires joined called trunks, operated as the early versions of networks. These networks were not standalone but interconnected in layers until they could join nations around the globe. This marked the onset of the Public Switched Telephone Network, or PSTN, which is, in essence, a fully interconnected network of individual voice telephone networks, operating with the primary focus on voice traffic. It is a circuit-switched system meaning that for the time a call lasts, a special line is set for the three participants in the telephone conversation. The PSTN was originally purely analog, however the majority of this network is digital with the help of additional algorithms ensuring the successful completion of voice calls.

The undying quest for more and more interconnectivity, as evidenced by the growth of networking, translated to the growth of the Internet in 1968 through ARPANET, as also followed the conception of hypertext transfer protocol and hypertext markup language. This is the point when the World Wide Web came to life, which further popularized the use of

the Internet. The transmission control protocol/ Internet protocol (TCP/IP) Doctor Vint Cerf invented in 1971 identified what package data could be send over the Internet and provided guidelines on how those packages would find their way to the end users. Considering the increasing rise of the Internet and relaxation of the policies that governed the telecommunication sector then, enabling technologies in the form of constructing voice applications on data networks became the order of the day. This is best shown in Figure 6.1. In the long run, this raised the development of VoIP which enabled the carrying of voice on any IP packet transmitting networks including the Internet.

As a result of the explosive development of the World Wide Web and liberalization of the telecommunications sector, the tendency of infrastructure convergence where voice applications are built over data networks gave rise to VoIP.

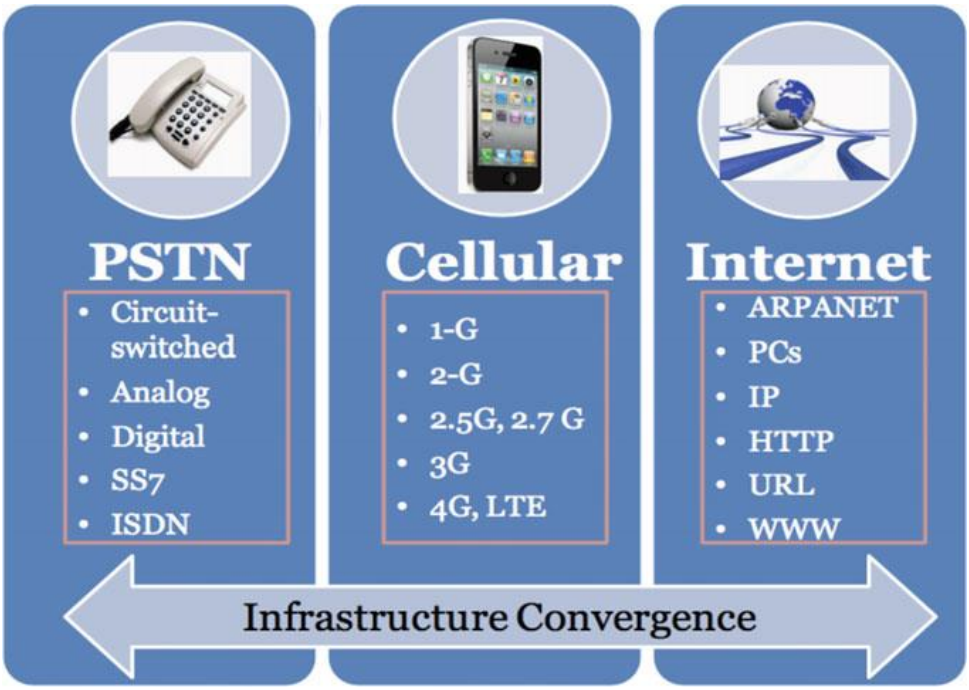


Figure 6.1 Evolution of VoIP technology

3.2 Working Technology of VoIP

VoIP communication means a telephone network that can be connected to the Internet. The fundamental procedure involves capturing the voice signal in its analog form and transmitting it over the Internet in packets containing IP addresses. At least one audio input device such as a microphone should be present on the transmitting end. The sound from the microphone is digitized by an analog to digital converter (A/D) that samples the audio at an ultra-high speed (that is, a minimum of 8000 times on a per second basis). Then, the information in a digitized form is further compressed into miniature samples, which are then combined

into large quantities and put into a data packet, which is ready for the IP network, this operation is called packetization. In most cases, within a single IP packet, there can be inserted audio of 10 milliseconds or more, with 20 and 30 ms common. This audio can be compressed in many different ways, the process of which is referred to as a "compressor/ de-compressor", or simply Codec. There are many different types of Codecs, with several for use with Movies and recordings with sound. In the case of VoIP, Codecs are geared toward helping compress voice, in which case the bandwidth used is much lower when compared to uncompressed audio stream aiding in the quality of VoIP Calls. Most of the Codecs are prescribed by the standards of the International Telecommunication Union, the Telecommunication sector (ITU-T). Each of them has varying characteristics super imposed on the amount of bandwidth they need and the quality of the speech signal produced encoded.

Once the binary information is transformed into a code and grouped into packets on the transmitting site, packets carrying voice information can be also sent over the network. Fig. 6.2 illustrates the pathway from one endpoint to the other for VoIP purposes (the converse path exists for such connections as well).

Voice packets share the network with packets of different applications and travel over common channels to reach their destination. At the other end, they are stripped off their packaging and processed. Digital information is then transformed back to audible sounds and output through a device, often in the form of a loudspeaker. All this flow of information is represented in the Figure 6.3.

The fundamental principle of working with VoIP is to convert the voice from its natural analog form and transport it in the form of IP packets to any IP based medium including the Internet.

There is also a likelihood that certain IP packets may get lost in transit due to the nature of the network. Considering that real time communication is very informative and sensitive to any losses of information, some appropriate measures should be taken to enhance the delivery and reduce packet losses such as through resource reservations among other ways. Such codecs can mask the missing packets by interpolation of sound that is pleasant to the ear. This is known as packet loss concealment (PLC). Another technique is known as redundancy in which a packet or group of packets is transmitted several times with the intention of overcoming the problem of packet loss. Techniques to recover from errors such as forward error correction (FEC) take into account prior packets and include some of this information in later packets. Afterward, the lost packet is filled in with the information bits

from neighboring packets using the appropriate FEC scheme that is complimented by mathematical equations. A packet that is considered to be 'lost in transmission' might actually have reached the desired destination, although after a considerable delay. It is not unusual for such applications to receive packets in an out-of-order fashion on a packet enabled network. This is time sensitive in case of a VoIP system as delay in the played out of a voice packet means that the information is stale and hence not worth playing out. Such old packets are in fact lost during transmission owing to the processing by PLC algorithms and are thus regarded as lost in the system.

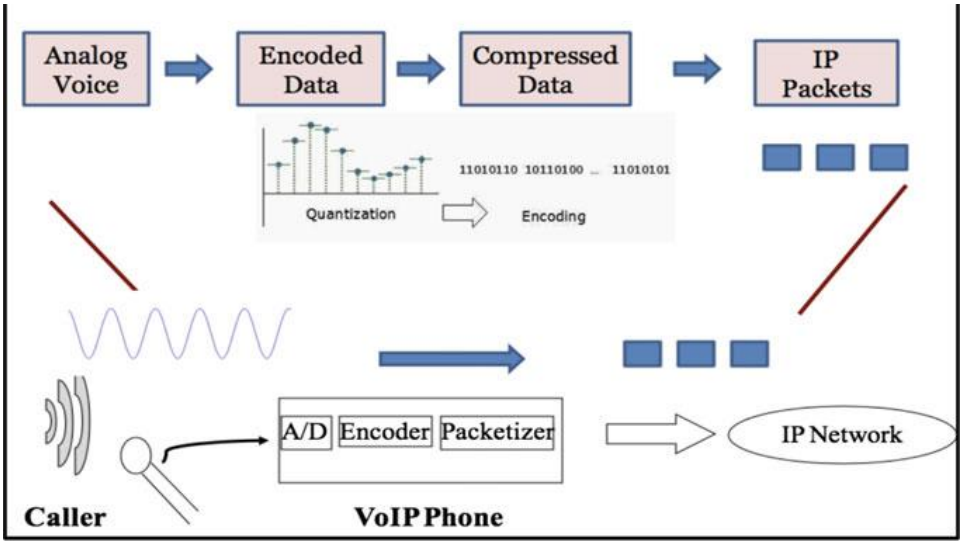


Figure 6.2 working mechanism behind VoIP communication

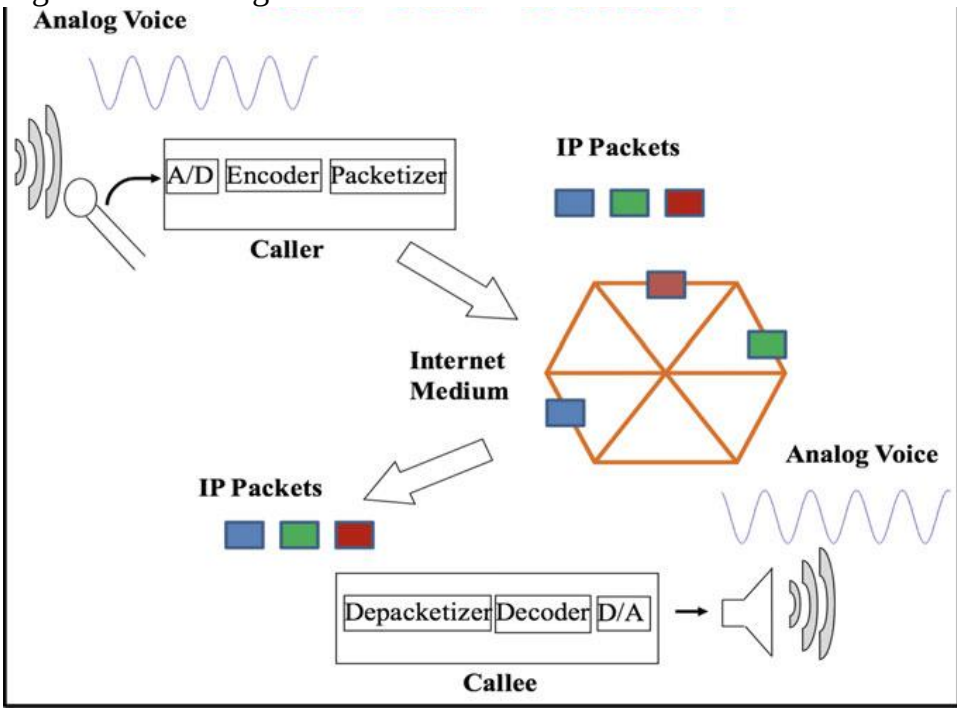


Figure 6.3 Complete VoIP communication between the sender and the receiver

The data present in IP packets can also serve as a basis for the ascertainment of packet delay and loss. During the conversation process, such delays may over the course of performance increase or decrease thus leading to a delay component that is deemed variable commonly known as jitter. In as much as delay must be kept below a certain threshold level, it is jitter that translates into choppy voice or forced silences and therefore must be kept to a bare minimum. This is the reason why A VoIP Applications use Jitter buffer algorithms. Packs are 'held' in a queue prior to play out and this holding period is adjusted over time either to cut down on the number of play out packets that arrive too late or the ear to mouth delay, or both.

Since any real-time communication is prone to loss of information, it is necessary to take actions in order to reduce the end to end delay as well as the packet loss by utilization of resources reservation and other measures.

VoIP phones naturally contain longer pauses when the operator is not speaking. This allows codecs to implement "silence suppression" and avoids transmitting audio during the silences, therefore reducing the amount of bandwidth used. To prevent dropouts from being experienced by the users on either end of the call, 'comfort noise' is generated. Also, when VoIP is integrated to the PSTN, it has to contend with line and acoustic echoing. Echo cancellers may be designed to work on line echo, acoustic echo or both. The performance of the cancellation directly correlates with the design of the algorithm in place.

Codecs take advantage of the silence periods by restricting the transmission of data during the quiet space between two speech utterances, and particularly using "silence suppression" methods which effectively conserve the network bandwidth.

Underneath we can see figure 6.4 which shows how VoIP packets are produced post compression, echo cancellation and silent suppression. The input to the system is time division multiplexed PCM bit stream and the output is VoIP packets. One more issue which accompanies the successful implementation of the VoIP application is the installation of the user interface with video and audio capturing devices and the provision of high-level data transfer between them. A signaling protocol for call initiation, management, and termination must also be put in place. GAPS/ASCII protocols must be adhered to which allow the computers to meet and agree on what information will be exchanged before packets are allowed to flow. Standard protocol describing the contents of the media packets (i.e. packet payload format) should also be established. Voice over Internet Protocol also expands beyond computers to cover mobile internet protocol-based phones, analog

terminal adapters and gateways. Each such design implies different communication and networking peculiarities that need to be focused upon.

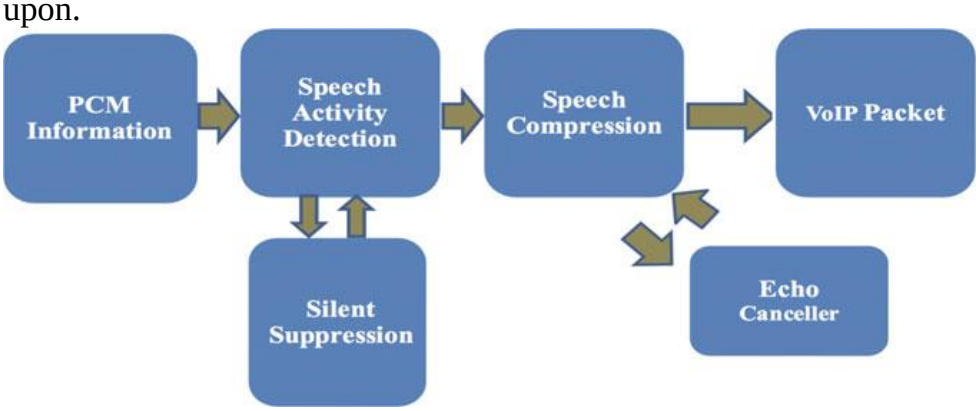


Figure 6.4 VoIP packet

It is crucial to note that many other issues besides simply transmitting and receiving audio or video packets cannot be overlooked simplicity call signaling protocols. e.g. SIP, H.323.

In Figure 6.5, the various components that make up a VoIP-based telecommunications system are shown. The figure represents the use of VoIP technology in various communication networks that utilize IP and PSTN connections.

4.0 Self-Assessment Exercise(s)

Question 1

Explain the key developments in the evolution of VoIP.

Answer

Transition from traditional telephony to packet-based networks.

Integration of VoIP with data services and advancements in compression algorithms.

Widespread adoption in enterprises, replacing PBX systems.

Question 2

Discuss the impact of VoIP on telecommunication.

Answer

VoIP reduced communication costs and allowed businesses and consumers to integrate voice and data services. It also brought scalability issues and introduced new quality of service (QoS) challenges.

5.0 Conclusion

In this unit on the Evolution of VoIP, we explored the transformation of traditional telephone technology into the modern, internet-based communication system known as Voice over IP (VoIP). VoIP has revolutionized how we communicate by enabling voice calls to be transmitted over internet protocols, rather than relying on traditional telephone networks. This shift not only reduced communication costs but also allowed for the integration of voice, video, and data services into a single platform.

We examined the structure of VoIP packets and how they differ from traditional telephony, highlighting how voice data is broken into small packets, transmitted over networks, and reassembled at the destination. You also learned how VoIP uses protocols like SIP (Session Initiation Protocol) and RTP (Real-Time Transport Protocol) to manage call setup, data transmission, and termination.

The evolution of VoIP reflects the broader trend towards digitization in communication, offering greater flexibility, scalability, and cost-efficiency. As VoIP continues to evolve, its applications in personal communication, businesses, and global collaboration will only expand, paving the way for even more advanced innovations in communication technologies. Understanding how VoIP works and its role in modern telephony is essential for anyone working with or managing digital communication systems.

6.0 Summary

We covered the structure of VoIP packets, learning how voice data is broken down, transmitted over networks, and reassembled in real-time. Key protocols such as SIP and RTP were discussed, highlighting their role in managing VoIP calls and ensuring efficient data transmission. This section emphasized how VoIP has transformed communication systems and continues to shape the future of telephony, offering significant benefits for businesses and personal communication alike.

7.0 References/Further Readings

Abualhaj, M. M., Abu-Shareha, A. A., Al-Khatib, S. N., Al-Zyoud, M., Al Saaidah, A., Hiari, M. O., & Alsharaiah, M. A. (2023). Improving VoIP Bandwidth Utilization Using the PldE Technique. Transport and Telecommunication Journal, 24(3), 288-296.

Abualhaj, M. M., Shambour, Q. Y., Hussein, A. H., & Kharma, Q. M. (2021). Down to Zero Size of VoIP Packet Payload. Computers, Materials & Continua, 68(1).

Adjardjah, W., Kumassah, F., Abdallah, D. M., & Addor, J. A. (2023). Performance Evaluation of VoIP Analysis and Simulation. Journal of Engineering Research and Reports, 25(7), 176-191.

Kharma, Q. M., Hussein, A. H., Taweel, F. M., Abualhaj, M. M., & Shambour, Q. Y. (2022). Investigation of Techniques for VoIP Frame Aggregation Over A-MPDU 802.11 n. Intelligent Automation & Soft Computing, 31(2).

Kolhar, M. (2021). Zeroize: A new method to improve the utilization of 5G networks when running VoIP over IPv6. Applied System Innovation, 4(4), 72.

UNIT 2: FUNDAMENTAL ELEMENTS FOR VOIP DEPLOYMENT

Unit Structure

1.0 Introduction

Voice over IP (VoIP) is a terninal improvement in operating communication services as it reduces the costs incurred in communication and integrates data services with voice communications. Held to the positive evolution of telephone and the World Wide Web, VoIP could also be used primarily to (a) cut down the costs of the network maintenance and operations tremendously and (b) provide services in the market within a short period of time. The process consists of digitally processing the wave signal of a voice and encoding it into packets for the purpose of transmission using the internet protocol.

Deployment has definitely become simple with VoIP, other than utilizing existing standard IP networks to transport its packets, there is high cut in costs, enhancements are simple and many more.

VoIP technology can be adopted by corporates, hospitals, hotels, banking sector, law firms and construction companies among other industries..

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will learn the fundamental elements of a VoIP network. The role of VoIP in multiconferencing system and various application of VoIP.

3.0 Main Content

3.1 Fundamental Elements of VoIP

The key components that are necessary to enable VoIP to work over a public network are discussed below in a list format.

1. Computer enabled with IP—End users involved in VoIP communication must possess devices that can be Networked to the Internet and supports VoIP routing. Such a workstation can be a soft phone embedded on a computer linked to an Internet Protocol (IP) network. Hard-wired IP-enabled landline phones or even glossy smart phones could also be incorporated in the use of VoIP technology.
2. VoIP server—The VoIP server is the core component that is utilized in commencing, maintaining and finally directing the calling communication to the other end. This is in reference to telecommunications, the one who is dialing is called as a caller and the one who picks up the phone on the other side is referred to as a caller. In addition to the all this, the VoIP server must support the relevant call signalling protocol such as SIP or H 323, as well as the routing of the IP packets to intended destinations. Call admission control is one of the prime roles played by the server. This is also possible for use with QoS control of resources management schemes.
3. Gateway voice-over-internet protocol VoIP has a fundamental drawback of lack of interoperability between different platforms in a network. This can necessitate the inclusion of a gateway in such networks. Gateways enable these networks to work in harmony and help VoIP users to reach users on the public switched telephone network PSTN. Furthermore, a firewall can also be integrated into the gateway in order to allow only certain, properly filtered packets through, ensuring a safe connection.

4. Gatekeeper - A gatekeeper is a network element that controls access to the resources of a network. It mainly deals with admission control, calls addressing, registration, dial plans, and usage of end-points, as well as managing the servers. The company providing VoIP services can upload not only call's logs but also users' billing information in a gatekeeper. If necessary, such functions can be implemented in the

server, but for most cases Aunt Sally's locks are built independently of the server for easy use of the core server functions.

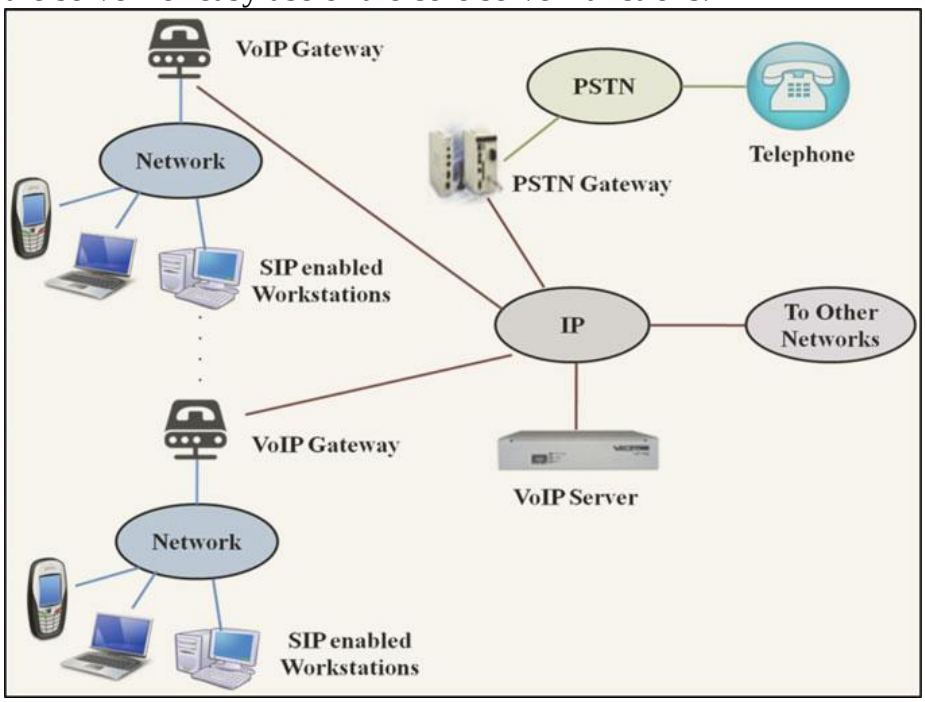


Figure 6.5. Fundamental elements of a VoIP Network

3.2 VoIP Applications

In addition to its primary function of internet telephony using a broadband connection, VoIP technology can also be employed to create many additional features. Such developments are of great necessity nowadays since most of the telecommunications service providers are looking to offer value-added services to gain and keep more subscribers. The convergence, or rather "infrastructure convergence", of VoIP with data networks allows the customer to solve many problems in an inexpensive and conveniently easy fashion. Furthermore, with the advent of SIP and other similarly straightforward protocols, software systems developed to work over a purely circuit-switched network can be readily adjusted to enjoy the benefits of all-IP transmissions. Perhaps the most known element in mobile communications is the short message service or SMS which facilitates sending and receiving short text messages through communicating fixed or mobile telephone lines. Another enhancement on this service is known as Multimedia messaging service or simply MMS which allows not only sending and receiving text messages but also sending and receiving pictures, sounds and even videos. Nonetheless, it has been noticed that traditional texting based on GSM networks has quite a number of limitations. The most obvious limitation is the cut-off on the number of messages that an individual GSM device is able to send. This is even more complicated where the messaging system uses media rich MMS, which deter superior bandwidths. While extra devices can however augur well with sending

larger bulk messages, there are situations where the device connection does not work especially during heavy usage periods such as those of New Year's celebrations and other similar holidays. In addition to other limitations, only a single static originator's address is permitted for sending out messages.

The deployment of messaging over IP networks on the existing VoIP infrastructure is the primary solution to all these subjects. To begin with, all IP enabled devices are able to send the messages. Thus, users can send messages even during an emergency without having a telephone or a GSM connection. Further, weak signal strength will not hinder the delivery of IP messages. To finish with, different IP senders may also use the same device for sending IP messages using their own registered accounts. There are studies that show that more than US$ 10 billion worth of losses were reported by the mobile industry as a result of customers movement away from traditional text messaging towards the cheaper alternative an IP messaging service.

Multiconferencing solutions also embraced VoIP technology so that all professionals within the business as well as in the service sector can reach to each other 'on the go'. In addition to the economization possibilities brought about by the use of VoIP for conference calls, users can enjoy its extra features such as accessing voicemail via the web, emailing voice messages and sending documents during the call. A schematic representation of the VoIP-oriented multiconferencing system is presented in Figure 6.6. The VoIP conference server collects relevant information about each participant and enables only those who are registered and verified to join the conference. Call information together with required metrics is also collected for billing reasons.

Moreover, there has been an overwhelming increase in the popularity of social networking sites and applications with several platforms such as Facebook, LinkedIn, Gtalk, and other verticals which enable people to communicate and share ideas across the continents. These portals allow registered users to create an account and search for other users with similar interests and communicate via text, audio, or video calls. The fact that most of these service providers do not require any charges from the users makes it a necessity of using VoIP system to put the needed facilities in place.

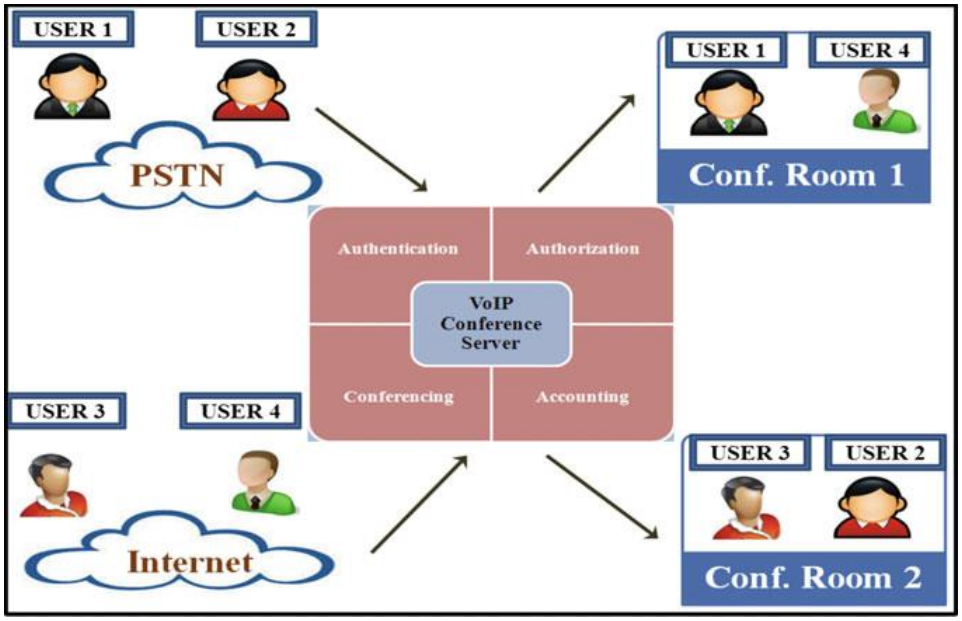


Figure 6.6 Role of VoIP in Multiconferencing system

The benefits of VoIP for online gaming do not end here. Some games nowadays come with realistic models and believable backgrounds, as well as the potential of the World Wide Web that enables millions of other gamers from every corner of the world to be accessed effortlessly by the players. Internet connection has been made possible by VoIP, which despite some drawbacks has enhanced the overall experience of such games by enabling gamers to interact and play. The most important one is the fact that gaming software and VOIP applications can be used simultaneously making it possible to enjoy the experience within the shortest time possible without the need of changing to different windows to talk to teammates. Besides, it allows for game play invitation to be done in the middle of the game, which increases the thrill of these types of games, thus enhancing the acceptance of the gaming software.

As of today, military institutions are gradually upgrading their old TDM telecommunications systems into ones that are more advanced and run on VoIP technology. In addition to the fundamental benefits of VoIP communication that is All-IP, VoIP is more robust than TDM especially over management which is easier than that of the older TDM system. Security and survivability are understandable military mandates; hence they are basic requirements of any VoIP applications. Hence why in development of military VoIP in networks standard protocols modified versions are applied.

One such example is MLPP a standard defined by ITU which is actively employed by the US Department of Defense and implements multilevel precedence and preemption priority call treatment services.

VoIP also seems to be penetrating every sector that offers IP related services and will claim considerable proportion of the traffic generated on the internet.

The different domains that could embrace the usage of VoIP technology are numerous and can be pictured in Figure. 6.7.

3.3 VoIP: Present and Future

The year 1995 saw the earliest reported instance of Voice over Internet Protocol (VoIP) technology and since then the software programming that supports it has improved markedly. The relevant protocols have been revised to address issues of networking quality and inter-operability of devices. Step by step, though, VoIP has been finding its way into the developing networks of wireless communications as discussed in the next section.

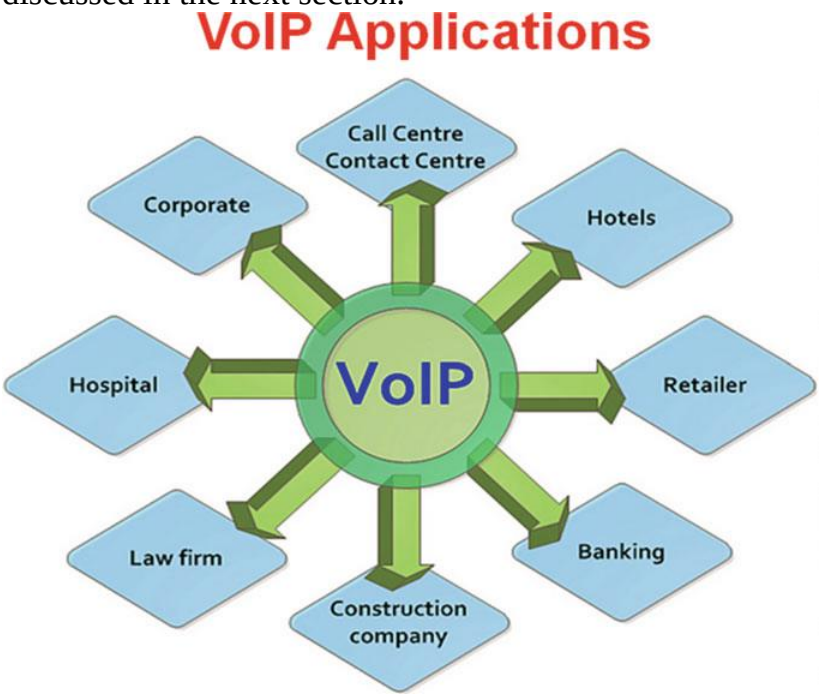


Figure 6.7 Application areas for VoIP

3.4 VoIP over WLAN

Wireless Local Area Networks (WLANs) are gaining ground in almost all sectors of the economy. It is viewed as the primary infrastructure for office and campus networks. National or worldwide standards for WLANs (IEEE 802.11 a/b/g/n) and wireless voice clients appear to be the two main reasons why WLANs have become one of the most implemented types of networks. The launch of dual-connectivity smartphones has enabled the growth of the WLANs subscribers' population. Hence, VoIP over WLAN (which is simply VoWLAN) is very promising.

VoWLAN has several design issues. The issues of real-time constraints have to be solved in line with the existing standards of WLAN.

Considering that WLAN operates under a randomly accessed protocol allowing clients to move around freely, and that it operates in an unreserved ISM frequency band, a number of implications for the design of VoIP systems are to be critically considered and meticulously justified, including the following.

• Keeping the Quality of Service (QoS) requirements for wireless "over the air" links through appropriate resources reservations and policies for QoS.
• ensuring that network design allows for interaction of VoIP server with the WLAN access points and other devices and layout of local area networks for optimal reach
• devising measures that can be employed in securing the network by requiring users to authenticate and the data bits to be encoded
• attaching VoIP application Software with the Wireless LAN and make sure it works with the VoIP's Client operating system.
The full process of installing VoIP over WLAN is done in various stages as shown in Figure 6.8.

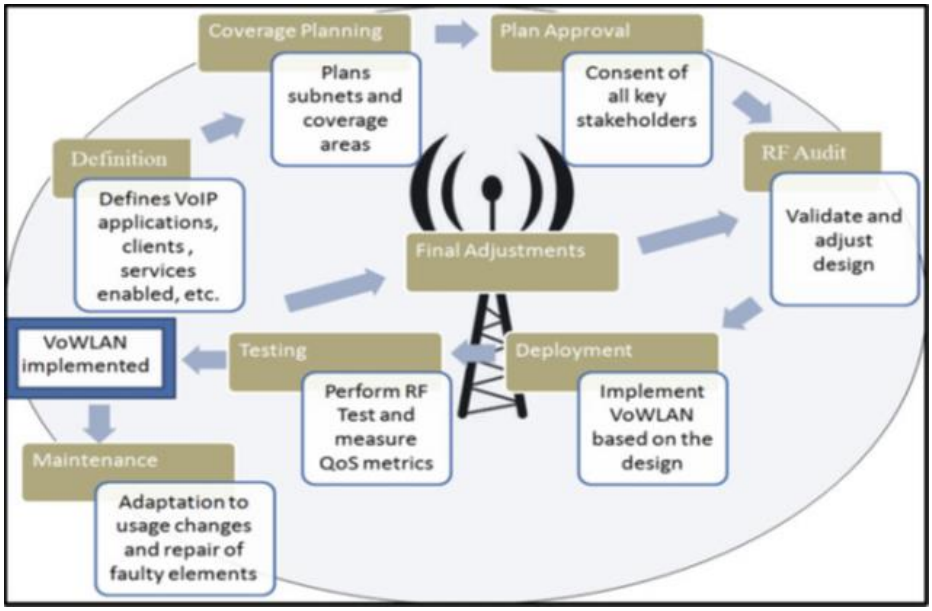


Figure 6.8 Steps for deploying VoIP over WLAN
Since WLAN relies on a random access protocol which permits free user movement and operates within the uncontrolled ISM band, it has several ramifications in the design of VoIP services that must be analyzed and addressed as part of planning.

3.5 VoIP over WiMAX

WiMAX denotes the approved wireless telecommunications standards whose various architectures and systems are all based on the IEEE 802.16 standards established by the WiMAX Forum. Such a network, based on WiMAX technology, provides a data rate approaching 30-40

megabits per second for both fixed and portable access applications. Mobile WIMAX integrates the mobile and fixed broadband networks allowing for multiple services over a single wide area broadband radio access network and dynamic network topology. WiMAX, being a more high-throughput, high coverage and data-rate technology than Wi-Fi, forms a good host for Voice over Internet Protocol (VoIP) and multimedia communication. The WiMAX 802.16e (mobile WiMAX) standard on the other hand supports five classes of Quality of Service (QoS) in the air interface (the interface that connects the access point and the mobile subscriber) that facilitate different kinds of traffic within the network. Unsolicited grant service (UGS) is meant for constant bit rate (CBR) services and can be applied in situations such as VoIP without the need for silent suppression. Real time polling service (rtPS) allows for the commencement of audio and video stream delivery. Extended rtPS is where UGS and rtPS functionalities are fused and VoIP is provided with the Ae2 silent suppression.
VoIP service can only be availed by the customers when the voice-enabled WiMAX network is designed strategically. The competitive strategy has to be customer driven which takes into consideration the pricing elements of the VoIP services offered. The design plan for VoIP in WiMAX is demonstrated in Table 6.1.

Nevertheless, there are various design challenges that need to be resolved before VoIP can be availed to WiMAX subscribers. So far, only a few laptops and computers have WiMAX reception cards, while even fewer mobile phones are WiMAX enabled. To get around this, the market has WiMAX modems today that can be connected to computers and phones. However, they are cumbersome due to the energy need which works against mobility. For a smart WiMAX connection, such management should also assist in the aspect of hardware and software facilities in order to incorporate VoIP applications successfully and retain the complete VoIP QoS. Consequently, many VoIP calls in a WiMAX network are a dilemma because of the nature of VoIP with its small size and use of short bursts of data that is sent out at intervals due to the “persistent scheduling” approach that has been adopted by WiMAX in provision of VoIP services.

In addition to voice over IP technology, WiMAX also found immense application in multimedia communication by serving as a better platform than Wi-Fi in terms of high data rate, coverage and throughput. Still, many design issues must be tackled before VoIP can be actually used by WiMAX subscribers.

Table 6.1 Design strategy for VoIP in WiMAX

	Residential	**Small/medium business**	**Mobile customer**
Service as per user requirements	Maintain moderate voice quality and enable basic features	Maintain high voice quality and enable basic features	Maintain basic voice quality and enable high features
Pricing	Low	High	Competitive
Strategy planning	Cost-effective solution for voice and data	Offer better product for maximum user satisfaction	Overcome the difficulties of mobility and offer basic service

3.6 Voice over LTE

All mobile phone companies faced an increase in investment and considerable market growth with the advent of various value-added services that have stimulated demand for more data to be transmitted at very high speeds and at minimal delays. That is why the cellular technology was evolving incessantly as it passed through the traditional 1G to 3G networks. Advances in wireless communication technology have resulted into the development of all-IP oriented Long-Term Evolution (LTE) networks also known as fourth generation (4G) networks. LTE, on the other hand, has a fully IP network architecture supported by evolved UMTS terrestrial radio access network (eUTRAN) and evolved packet core (EPC) which offers better bandwidth efficiency and enhances quality of service compared to 3G where voice calls and short messages service (SMS) are switched through circuits and data is packet switched.

There have been various voice over LTE transfer paradigms proposed as CSFB or circuit switched fall back, SV-LTE or simultaneous Voice over LTE, and VoLGA which is Voice over LTE via GAN. Nevertheless, the most optimal implementation is one based on IMS or IP multimedia system VoLTE which is used to deliver voice traffic over LTE network using IP and is the voice standard for LTE defined by the 3GPP. Lets us start with IMS voip, which is offered as a service according to the 3GPP standard implementation of SIP or session initiation protocol and addresses retaining data rates of LTE. It moreover addresses the long thin tower in a network of towers connection that causes the unnecessary long delay in setting up of voice calls as well as promotes use of all IP networks thus reducing operating costs and enabling HD voice and it also paves the way for new services that are IP based.

The optimal solution appears to be CS-based VoLTE, which incorporates the application of the IMS, Voice over LTE as defined by 3GPP and which embodies the provision of VoIP as well as SMS services to the users with LTE content.

4.0 Self-Assessment Exercise(s)

Question 1
List and describe the fundamental elements needed for VoIP deployment
Answer
IP network infrastructure: Routers, switches, and gateways.
VoIP protocols: SIP, H.323 for managing communication.
End devices: IP phones, softphones, and supporting hardware.

Question 2
Explain the role of VoIP gateways and PBX systems in deployment
Answer
VoIP gateways bridge traditional PSTN networks with IP-based VoIP systems, while PBX systems manage internal calls within an enterprise or network.

5.0 Conclusion

In this lesson, you studied that some of the advantages of VoIP are easy and quick deployment, ability to use existing standard Internet Protocol networks to transmit its data packets, significant cost benefits, simple enhancements and many more. There are several sectors that can make use of VoIP technology and they include: corporates, hospitals, hotels, banking sector, law firms, construction industry, etc.

6.0 Summary

Voice over IP (VoIP) is an effective breakthrough designed to bring down costs on communication and integrate voice along with data services. Thanks to the inventions of the telephone and the Internet, it was possible to realize VoIP as (a) a reduction in the costs related to the maintenance and operations of networks, and (b) a quicker deployment of new services. The technology encompasses the process of converting the sound waves into numerical values and transmitting these values in the form of Internet Protocol (IP) packets through the internet.

7.0 References/Further Readings

Chen, L. C., Shih, I. C., & Liu, J. S. (2020). Identifying the main paths of knowledge diffusion in the voice over internet protocol. Journal of Internet Technology, 21(1), 85-98.

Ivanova, M. (2022). Scientometric Analysis “Voice Over IP”. In Developments in Information & Knowledge Management for Business Applications: Volume 5 (pp. 649-670). Cham: Springer International Publishing.

Jaish, A. A., & Al-Shammari, B. K. (2023). Quality of experience for voice over internet protocol (voip). Wasit Journal of Engineering Sciences, 11(3), 96-105.

Marcel, M. L. C. (2020). Integration of a Voice Over Internet Protocol (VoIP) Solution with Internet Protocol Version 6 (IPv6) in an Internet Protocol Version 4 (IPv4) Data Network to Increase Employee Productivity.

Ylli, E., Tafa, I., & Cejku, F. (2021). EXPLOITING VOIP SECURITY ISSUES IN A CLASSIC SCENARIO. International Journal of Research In Commerce and Management Studies (ISSN: 2582-2292), 3(1), 20-36.

UNIT 3: SECURITY ISSUES OF VOIP

Unit Structure

1.0 Introduction

This section starts by discussing the aspects contributing to the acceptance of the Voice over Internet Protocol (VoIP) services and the entire range of challenges placing the security of VoIP at risk, the challenges emanating from the nature of operation of helpful protocols and the networks they operate in. Security risks are outlined and presented drawing from the CIA model which stands for confidentiality, integrity and availability. When looking at each one of these risks on its own, it is possible to apply countermeasures that are once in existence for different but related threats to resolve the risk. Nevertheless, the various aspect of VoIP protocols and the insertiveness of the VoIP architecture imply that the problem of securing VoIP should be treated in a "from one end to the other" way. Most probably, every country and province of the world has its own legal restrictions governing the internet, majority of times the travel gateway that facilitates VoIP communication is indeed the world wide web. Firewall settings, system updates, and similar factors outlined before would not be physically within the reach of the manager. We give a conceptual system to provide security policy service for VoIP in a mobile environment. This generic model would enable the automation of finding and managing security policy and security state of VoIP resources along a call path, thus making it possible for a VoIP user over a WAN to ensure and maintain security.

2.0 Intended Learning Outcomes (ILOs)

BY the end of this unit, you will understand the rationale for the use of VoIP, the protocol components of VoIP and the Traditional telephone network and a VoIP network.

3.0 Main Content

3.1 Rationale for the Use of VoIP

At present, the Internet is the principal channel through which companies transact business. It is evident that the advent of the Internet has compelled most of the companies to adapt in their strategies and systems by embracing various forms of Internet technology that are in place in order to compete in the market. VoIP technology is becoming widely used and recognized in the field. A few VoIP software services became available that provided the same features (for instance: caller id, call waiting, etc.) as conventional Private Branch eXchange (PBX) systems.
A number of companies are migrating to VoIP technology, because this allows them to keep using the existing local networks for transporting voice and regular data traffic. This innovative technology allows a huge cut in expenses by lowering down operations like the maintenance of the system, long distance calls, and other expenditures related to a conventional telephony system.

3.2 Protocol Components of VoIP

Typically, VoIP technology adopts a range of related protocols for its operations, which typically include signaling protocols such as the session initiation protocol (SIP), and data control and transfer protocols such as the Transmission Control Protocol (TCP), the Real Time Transport Protocol (RTP), the User Datagram Protocol (UDP) and the Internet Protocol (IP). VoIP services like internet protocol IP telephony systems work by converting voice into data packets and transmitting it through private or public IP networks, only to reassemble and decode it at the receiving end. Nevertheless, concern for security remains the major hindrance that bars a majority of companies from embracing the use of VoIP technologies. Security is viewed as a basic and necessary requirement for the application of VoIP systems.

3.3 Intruders in a Traditional Telephone Network and a VoIP Network

Usually, intruders are defined as those who illegally access a PBX or voicemail systems and use such systems to make free telephone calls by hacking into computers. Some researches even suggest that some of the reasons which prompt such unwanted intrusion include revenge, sabatooge, blackmail or pure greed. Regarding VoIP applications, one can also imagine a scenario where the intruder can snoop on the outgoing and inbound telephone numbers, access someone's voicemail or eavesdrop on conversations using IP networks. One such incident of VoIP application hack was experienced by an organization known as Sunbelt Software, based in the US. An outsider managed to penetrate their company's VoIP application via the remote access capabilities of the system. As a result, the organization was presented with an exorbitant bill with numerous international calls on it.

3.4 Attacks on Circuit-Switched and IP-Based Networks

In addition to voice eavesdropping, impersonated calls, fraudulent usage, annoying telemarketing calls, and denial-of-service attacks, there are several other threats to circuit switch telephone networks. Most of these risks are still present in packet-sliced networks, particularly in VoIP networks. Since VoIP operates on standard IP networks, VoIP services are subject to IP protocol-associated security threats both established and emerging. This increases the scope of security issues quite significantly when comparing it with a conventional public switched telephone network (PSTN). Further, the proprietary protocols that several VoIP providers Ares is based on, have exposed VoIP users to malware, bugs, abnormal port activities, and so on.

A Network-based VoIP system is more prone to various network attacks: hostile software (worms, viruses, and trojans), DDoS, and other forms of Denial of Service attack, pharming and crowds. These acts of aggression also cripple the systems under attack by wasting resources, interfering with honest networks users, leaking sensitive data or changing codes and information. The damages or effects of such caused diseases, however, are not limited to only those systems which are under attack. It also affects other systems, which are healthy and even those systems which are not at risk at all. The internet has created a body which supports arms of virus infections across each continent with the intention of infecting countless hosts, thereby leading to the clogging of the entire network. It talks about the security troubles of VoIP systems and presents a few recommendations for the users of this form of telephony.

3.5 VoIP Security Requires an End-to-End Security Model

As far as voice communication services are concerned, there are various forms of aggressions aimed at them and it can be such things as, inter alia, wiretapping, call masquerading, account abuse, spam, and denial of services (`doC). A good number of these threats are still present in case of packet-switching networks within which VoIP networks operate.
As it utilizes regular IP networks for its services, VoIP applications inherit range of security concerns that are both existent and nonexistent with the IP protocol. This results in a significantly bigger security problem domain as compared to the case of standard public switched telephone networks. In addition, closed, or proprietary protocols associated with many VoIP service providers have exposed the VoIP users to virus attacks, security flaws, unsolicited port activities and many others.

At the same time, VoIP is more susceptible to different hazards such as the use of viruses and malwares such as worms, trojans and viruses, dos and ddos attacks, flash mobbing, and internet pharming attacks. Such attacks however do not only affect systems that have been compromised, but include also un compromised systems and even those that are not exposed to the threat. In effect, the entire ‘clouds’ of systems that use the Internet are awfully infected by germs that are codes for who knows what, but which tend to spread fast looking for hosts to infect so as to cause some level of blockage to the networks. Also, it considers the security problems related to the implementation of VoIP, and its intended use, and proposes a set of recommendations for the users of such a telephony technology.

4.0 Self-Assessment Exercise(s)

Question 1
List and explain the primary security concerns in VoIP
Answer
Eavesdropping: Unauthorized interception of voice packets.
Denial-of-Service (DoS) attacks: Disrupt VoIP services by overwhelming the network.
Caller ID spoofing: Falsifying the caller’s identity.

Question 2
Discuss how to mitigate VoIP security risks
Answer
Use encryption protocols like SRTP for voice data.

Implement firewalls and intrusion detection systems.

Utilize secure authentication and access control mechanisms.

5.0 Conclusion

We present a VoIP security policy service framework intended for mobile VoIP systems. Such a model would facilitate the automatic retrieval and the subsequent reasoning over security policy needs and security requirements of VoIP applications and links over the call path, thereby allowing for defences to be validated and enforced in the case of a WAN traversed by a VoIP caller.

6.0 Summary

In this unit, we analyze a security policy understanding communication as well as application security properties – confidentiality, integrity and availability in order to develop a security framework for VoIP applications. Lastly, we present a security policy framework that addresses the network security issues for developing a security framework for mobile VoIP applications in the coming years.

7.0 References/Further Readings

Biondi, P., Bognanni, S., & Bella, G. (2020, April). Voip can still be exploited-badly. In 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC) (pp. 237-243). IEEE.

Chen, L. C., Shih, I. C., & Liu, J. S. (2020). Identifying the main paths of knowledge diffusion in the voice over internet protocol. Journal of Internet Technology, 21(1), 85-98.

Ivanova, M. (2022). Scientometric Analysis “Voice Over IP”. In Developments in Information & Knowledge Management for Business Applications: Volume 5 (pp. 649-670). Cham: Springer International Publishing.

Jaish, A. A., & Al-Shammari, B. K. (2023). Quality of experience for voice over internet protocol (voip). Wasit Journal of Engineering Sciences, 11(3), 96-105.

Marcel, M. L. C. (2020). Integration of a Voice Over Internet Protocol (VoIP) Solution with Internet Protocol Version 6 (IPv6) in an Internet Protocol Version 4 (IPv4) Data Network to Increase Employee Productivity.

Ylli, E., Tafa, I., & Cejku, F. (2021). EXPLOITING VOIP SECURITY ISSUES IN A CLASSIC SCENARIO. International Journal of

Research In Commerce and Management Studies (ISSN: 2582-2292), 3(1), 20-36.

MODULE 4: APPLICATION OF VOIP

MODULE INTRODUCTION

This module will cover Session initiation protocol SIP – a real-time signaling protocol for IP voice systems which was developed by the Internet Engineering Task Force for a purpose of enabling bi-directional communication session's initiation by means of exchange of messages between two or more nodes. SIP is responsible for basic call control tasks, such as setting up and taking down communication sessions i.e. call initiation, dial tone and termination signaling. These comprise too the signaling employed in other features like call id, call transfer, and call holding features. It serves purposes of the Signaling Systems 7 (SS7) standard used in circuit switch telephone services and the H.323 standard used in packet switch networks. It is referred to an application level protocol, which means that, it can be used on top of other protocols. It can be sent using either UDP, TCP or SCTP. Transmission of SIP over UDP enhances the speed and efficiency of SIP.

This module is classified into the following two (3) units:

Unit 1: VoIP Protocol Vulnerabilities
Unit 2: Other VoIP Security Issues and Vulnerabilities
Unit 3: Security Policy for VoIP Application

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

UNIT 1: VOIP PROTOCOL VULNERABILITIES

Unit Structure

1.0 Introduction
2.0 Intended Learning Outcomes (ILOs)
3.0 Main Content
    3.1 Security Issues of SIP
    3.2 Security Issues of H.323
4.0 Self-Assessment Exercise(s)
5.0 Conclusion
6.0 Summary
7.0 References/Further Readings

1.0 Introduction

The session initiation protocol involves a few basic request messages that include INVITE, ACK, OPTIONS, CANCEL, BYE, and REGISTER. In cases where a user agent client desires to set up a session, he or she shall send an INVITE message. This message shall elicit a response containing OK and the additional ACK message.

When two parties want to end the call, one of them will send a BYE message. In turn the CANCEL message cancels the pending invite. To inquire or amend non-essential characteristics of the session such as cryptographic protection, OPTIONS is employed. Protocols used in VoIP system are many and hence much of the vulnerabilities come from these protocols. SIP has text encoding making it simple to study or break using common studies like Perl or lex and yacc. The basic definition of SIP traffic is unencrypted text. Because of this, the voice traffic can be easily packet sniffed (especially for capturing caller IDs or passwords), and it is also possible to fabricate packets for the purpose of controlling the device and its state and call. For instance, this kind of adjustment can easily lead to a situation where a call may be redirected, terminated before it is supposed to, or toll fraud executed with little effort.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will understand the Security issues of SIP and the Security Issues of H.323.

3.0 Main Content

3.1 Security Issues of SIP

The Internet Engineering Task Force (IETF) developed Session Initiation Protocol (SIP) as a real time signaling protocol for voice over IP (VoIP). It is used for initiation of a communication session during which two or more nodes communicate by way of message exchange. Typical call control functions are also handled by SIP including session initiation and termination or call setup, initial ringing and call end signaling only. SIP takes care of other signaling as well which is required in such features as caller ID, call transfer, and call waiting. In that, it is similar to the Signalling System No. 7 (SS7) in circuit switched environments and H.323 in VoIP. It is an application transport

protocol which means it can run on top of other protocols. User Datagram Protocol (UDP), Transmission Control Protocol (TCP) and Stream control transmission protocol (SCTP) can transport it. Transporting SIP via UDP enhances speed and reduces delays, therefore enhancing efficiency.

The transmission control protocol is utilized in instances where, for the purpose of security, secure socket layer/transport layer security (SSL/TLS) is necessary. As compared to other protocols, the stream control transmission protocol (SCTP) has an additional advantage which extends its applicability to resist Denial of Service (DoS) attacks by using a four-way handshake process in its operations. SCTP is also enhanced by the use of other security services by the deployment of "TLS over SCTP" or "SCTP over IPSec" mechanisms."

The session initiation protocol has several components that include user agent, redirect server, registrar server, location server and proxy server. UA software provides both client-side and server-side components. At the client end, outbound calls are placed, while at the server end, incoming calls are answered. Proxy server does some processing or translation, after which traffic forwarding is performed. Handling of request authentication is performed by registrar server while redirect server takes care resolving of information for UA clients. UA clients request UA servers in order to start a call. The user contacts a registrar server and informs her about her location in order for people to reach her.

As has been illustrated, it is evident that conventional telephone systems (PBXs) have been replaced by IP voice gateways which are typically based on either Microsoft or Linux operating systems. VoIP servers and call detail record servers are highly targeted by malicious programs and hackers.

Session initiation protocol makes use of a few request messages including "INVITE", "ACK", "OPTIONS", "CANCEL", "BYE", and "REGISTER". A UA client wishing to initiate a session sends an "INVITE" message. This is followed by a response of "OK" and an "ACK" message.
To disconnect a session, a "BYE" message is sent. In case of pending invite "CANCEL" cancels it. To query or change optional parameters of the session such as encryption, "OPTIONS" is used. The specialized protocols for VoIP systems, in this respect, engender many vulnerabilities. SIP is encodes via a standard text format, enabling it to be disassembled or parsed using widely available 'Perl', 'lex' and 'yacc' tools. Under most conditions, SIP signaling does not carry any encryption. Thus encoded couth traffic can easily be session bored such

as in case of looking for the caller or password, and also permits packet forge attacks on the device and the call state. For instance this kind of attack may then be employed to cause unintended calling session drop, redirection of an incoming call, or more simply abuse of the phone system for toll fraud. Unencrypted VoIP calls are also quite easy to eavesdrop on. Numerous hackers can easily get free available software from the Internet and easily intercept the calls they want to. Protection of things like caller id and account details would mean that SIP traffic would have to be encrypted. It is true that some attempts have been made for the purpose of developing encrypted signaling but up to this point, a solution that can be utilized on a large scale has not been encountered.

Attacks that exploit weaknesses in VoIP signaling protocols such as SIP are known to exist. One such attack is termed the "BYE" attack. The purpose of such an attack is to terminate an ongoing communication session between two parties, whenever the offensive party wishes to do so, hence arguably coupling it to DoS attacks. Imagine there are three SIP UAs; Alice, Bob and the assailant and Alice and Bob happen to be conversing. The assailant can send a spoofed BYE message to Alice, thus making her think that Bob has signaled his willingness to end the conversation. Accordingly, Alice ceases to send "RTP" flow while Bob continues sending RTP packets to her obliviously, since he is unaware of the events that just transpired. Certain Intrusion Detection Systems (IDSs) are capable of recognizing such attacks.

We can configure the IDS to identify the receival of RTP packets even after sending a BYE. In the former case, if Bob is the real one who sends a BYE and wishes to end the call, there should not be any "RTP" traffic from Bob going to Alice after she receives a "BYE" message. In the event of IDS, when 'RTP' flow is indicated after the receipt of a 'BYE' message, alarm gets triggered.

The SIP protocol supports not only VoIP network calls but also other applications not limited to messaging. It is also possible for a malefactor to alter the header of the instant message. This way, a message can be sent to Alice, who will think it was sent by Bob. This is what is termed fake instant messaging. There is also another class of attacks based on signaling, which is referred to as call hijacking. In this form of attack, the evil doer exploits the "REINVITE" message that is used for moving from one call leg to another. In case of call hijacking attacks, this lead to one of the UA clients getting stuck enjoying a very annoying dead call as there will be no voice packets from the other side. Such an attack can also be classified as a DoS attack. This constitutes an intentional misdirection of information. To avoid such an attack, the same misdirection can be used as in the case of the BYE attack.

3.2 Security Issues of H.323

H.323 is the standard specified by the International Telecoms Union (ITU-T) for voice and video over a reconnized packet switched network. H.323 makes use of several protocols namely H225, H245… etc, each of which has its own function in the call set up process. Usually, H.323 networks are composed of the fastlync gateway, gatekeeper, multipoint control unit, and back end service respectively. The fastlync gateway acts as an interworking media between the H.323 domain and external networks such as SIP or PSTN which are non H.323.

The gateway also accommodates bandwidth management and address resolution features. A gatekeeper is not mandatory but and it focuses on efficient utilization of the network resources. Where it exists, Gatekeeper usually also possesses a Back End Service (BES) whose function is maintenance of a given endpoint's data such as permissions, services or configuration. mcu is also an optional part of h.323 networks. The multipoint control unit also enables communication of three or more endpoints via multipoint control communication and other similar activities.

In most cases, traffic within the H.323 protocol is directed to dynamic ports which presents great difficulties to non-specific firewalls that systems which do not deal with VoIP. Hence, there arises the need for a voice over IP enabled extra security application. Network address translation (NAT) presents another significant challenge in H.323 based networks. As both external IP address and port number cannot be linked to H.323 header and message contents IP address and port numbers used by other devices, a sending devices internal network. Therefore correct address and port number have to be provided to the endpoints for call connection to take place. In comparison to H.323 SIP is less rigid, uncomplicated and cheap in its realization. Moreover, SIP is more advantageous in the case of sophisticated end-user equipment and provision of value-added services.

H.235 proposes different profiles of security. The range of possibilities presented by H.235 allows for different ways to protect communication. In this chapter we explain one of them — H.235v2.
H.235v2 uses Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). To maintain compatibility between products, it provides a number of security profiles that are stated in the annexes to H.235v2. In order to provide authentication and integrity of messages, H.235v2 employs the use of shared secrets. It also supports H.245 tunneling and secure fast connect as well.

4.0 Self-Assessment Exercise(s)

Question 1
Discuss the vulnerabilities of VoIP protocols (e.g., SIP, H.323)
Answer
SIP and H.323 are vulnerable to eavesdropping, DoS attacks, and spoofing. Their reliance on IP networks makes them susceptible to the same security risks as any other internet-based service.
Question 2
Explain how VoIP protocol vulnerabilities can be mitigated:
Answer
Encrypt communication using TLS for SIP or IPsec for general VoIP traffic.
Implement robust authentication mechanisms.
Regularly update software to patch known vulnerabilities.

5.0 Conclusion

The transmission control protocol is only used where secure socket layer/transport layer security (SSL/TLS) security is required. Stream control transmission protocol (SCTP) is more resistant to DoS attacks due to its four-way handshake method. SCTP can employ extra protection mechanisms by utilizing “TLS over SCTP” or “SCTP using IPSec.”

6.0 Summary

Traffic associated with the H.323 protocol is nearly always sent over a set of dynamic ports which poses a significant challenge to other firewalls which are not VoIP-enabled and hence not programmed to understand H.323 traffic. Therefore, a VoIP-enabled firewall becomes a necessity. Yet another complicating factor where H.323 networks are concerned is NAT; in H.323 addresses and messages, the external IP and port do not correspond to both the actual, and internally used IP and port values.

7.0 References/Further Readings

Subraveti, H. H. S. N., Knoop, V. L., & van Arem, B. (2020). Improving traffic flow efficiency at motorway lane drops by influencing lateral flows. Transportation Research Record, 2674(11), 367-378.

Sharathkumar, S., & Sreenath, N. (2023). Distributed Clustering based Denial of Service Attack Prevention Mechanism using a Fault Tolerant Self Configured Controller in a Software Defined Network.

Tas, I. M., & Baktir, S. (2023). A novel approach for efficient mitigation against the SIP-based DRDoS attack. Applied Sciences, 13(3), 1864.

Kafke, J., & Viana, T. (2022). Call Me Maybe: Using Dynamic Protocol Switching to Mitigate Denial-of-Service Attacks on VoIP Systems. Network, 2(4), 545-567.

Gaylah, K. D., & Vaghela, R. S. (2022, November). Mitigation and prevention methods for distributed denial-of-service attacks on network servers. In International Conference on Advancements in Smart Computing and Information Security (pp. 70-82). Cham: Springer Nature Switzerland.

UNIT 2: OTHER VOIP SECURITY ISSUES AND VULNERABILITIES

Unit Structure

1.0 Introduction

The security risks posed towards VoIP could also impact convergence. VoIP is subjected to the same category of threats that are posed to data networks. This comprises some of the famous attacks like DoS attacks, authentication as well as others. Since voice communication is essential for business, it is expected that in the event of failure of the data network, at least the voice network will still operate.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will understand various VoIP security issues and vulnerabilities.

3.0 Main Content

3.1 Convergence Issues

Among the plentiful benefits of VoIP solution, one of the key ones is the convergence of voice and data networks in that it is cheaper and simpler to manage voice when it is transported as data over a data network system. However, this convergence is turning out to be another challenge in safeguarding the VoIP system. The security threats that are directed to VoIP systems may have effects on convergence as well. As with its data transport functions, the communication of audio can be compromised through a host of attacks used against voip networks. In business, voice communication is very important and therefore it is preferred that where the normal data network fails, the voice network is able to operate independently. However, if both voice and data networks happen to be on the same core network, then in the event of any risk both systems will be put down at the same time. The best alternative could be preserving the voice over its own network. It is important to mention though, that this approach about preserving voice within its own network is valid or applies to only to the businesses that do not mind the consequences of the shutdown of both the voice and the data networks. For such organizations, where such degree of risk is tolerable, current levels of convergence are appropriate.

However, there may be other businesses whose survival highly depends on voice; for them, the isolating process is the only solution. They may still be willing to have some features of convergence such as triggering of customer data displays by entering a caller ID. This calls for the establishment of another architecture that will integrate the different systems for such information to be available. By the separation of data and voice, when a virus hits the data network it can never affect VoIP system. To help achieve this ie security within voice systems, most VoIP deployments have data and voice set up in separate VLANs. A virtual LAN is a way to create a common telephone network within an organization using the local area network but ensuring that the normal data networking activities of the organization are separated from the telephone activities.

3.2 Man-in-the-Middle Attacks

The term man-in-the-middle attacks denotes a class of intrusion techniques where an outsider can intercept and alter communications between two parties without arousing any suspicion or detection from either of the parties. The typical man-in-the-middle attack that has been widely experienced involves the address resolution protocol (ARP)

which interferences with VoIP application traffic directing it to an intruder's system. At this point, the espionage or attacking computer system is even able to take over all sessions of the targeted communications through a VoIP, which can be further manipulated, eliminated or even stored for future use.

For instance, other speech, noise or even latency can be injected into a conversation by an intruder; a scenario which can involve tonal or silent voids as well. Broadly, there are three types of deception in the conversations that are man-in-the-middle protected- VoIP communications: (1) eavesdropping: unauthorized interception and decoding of voice data packets, RTP media stream or signaling messages; (2) packet spoofing: call interception through mimicking voice packets or broadcasting information; and (3) replay: retransmitting legitimate sessions in a way that makes the affected VoIP applications work with the old data again. In order to address any of the abovementioned issues, It means VoIP applications can choose to implement the public key infrastructure (PKI) as a data security measure, designed to allow a user's data to be transmitted securely over the internet while ensuring that the user is who he/she claims to be with regards to the publics or single's keys. It is common that without proper encryption, any SIP session packetized voice data packet can merely be sniffed by anyone over peer-to-peer IP networks that are liable to security concerns regarding confidentiality and also the integrity of the data.

So to say, man-in-the-middle attacks present risks to confidentiality and integrity since this particular attack puts into risk the voice packets from the lawful users and also alters the other participant's conversation.
Nevertheless, while there are protective measures such as improving the level of encryption to reduce the risk of eavesdropping as well as replay attacks, VoIP systems remain vulnerable to eavesdropping. As stated before, ensuring that the data network and voice network are separated using VLANs is the first step in securing the VoIP system, but sadly, attackers are getting wiser and always think of better ways of penetrating the system.

3.3 Denial of Service, Distributed DoS

Denial of service attacks, in all its reiterations, implicates blocking access to a network service by attacking its servers, proxies, or voice-gateway with overwhelming influence of malicious traffic. A DoS is an incident in which a user cannot access a resource or service that would normally be available to him or her. Moreover, the same way that a regular PBX system can be attacked using maximum aggressiveness and causing DoS attacks (for instance, sending unauthorized call control

packets), a VoIP app's networks and protocols are also vulnerable. For instance, in IP voice communication systems, voice mail services or SMS services could be subjected to similar attacks of message inundation. By and large, the Denial of Service attacks can be broadly categorized into three major types:

1. Buffer overflow or Mcast — In this attack, the intruders typically attempt to overload the targeted VoIP applications by sending extremely large Internet control message protocol (ICMP) messages or by sending data above what the port is capable of handling. To combat this issue, VoIP applications can implement a security feature which allows. This feature can shut down non-essential ports; operate packet rejection before the peer table; disable bouncing and abuse of ICMP; and reasonably d regulate the packet sizes to be received within tolerable limits that avoids causing the stack from overflowing.

2. SYN—A SYN flood is an attack in which the assailant attempts to use up all available TCP ports in the target's machine by constantly opening TCP connections which are not completed hence the ports are retained until such time a timeout occurs. To solve this device context, VoIP applications could implement the following security measures: a shutdown unsolicited ports; b cshorten the timeouts in the TCP stack; and c wheeze more memory to connection buffers.

3. Smurf—A target device is sent an IP ping request by the attackers. The ping packet then gets broadcasted to many computers on the local network with the DNS server address of the target device as the return address. To tackle this situation, VoIP applications can provide a security mechanism to turn off pinging and ICMP messages. In conclusion, DoS attacks are likely to pose risks on availability since denial of service would involve making the VoIP application useless.

3.4 Botnet Threats

As already indicated, the goal of a DoS attack is to render a service unusable by its legitimate users. DDoS attacks, on the other hand, employ many systems in the network to conduct a DoS attack. To execute a 'distributed denial of service' (DDoS) attack, one usually finds 'agent' machines or already compromised computers to use in the attack. This process of reconnaissance is usually carried out as a means of scannig the wireless systems in search of anything useful. As soon as an appropriate target is managed to be identified, that target is immediately taken over. The invader afterward provides those particular computers with the so-called remote control programs "bots." After the commands meant for the zombie-infested machines have been installed on them, the machines remain idle waiting for instructions from the

controller of the bots. Thus, it is possible for the perpetrator to focus a great many attacked systems upon a particular objective. The term used to describe such a range of computer systems occupied with bots is botnet. In most cases, the attacked machines are usually available on the high-speed economical cables that are always connected to the Internet. Attackers almost always obscure their real identity. One of the most commonly used tactics is IP address spoofing where the source address in attack packets is not an attacker's real address. For example, in the Denial of Service attack, the Server targeted can be overwhelmed by asking for too much information that may cripple the system altogether. Botnets are typically orchestrated by the 'botmaster' who provides commands through an Internet Relay Chat (IRC) channel to which the infected nodes also connect. In order to capture the user, agents will surveil the IRC network, and even prevent access to certain channels where the infected machines communicate. Today, it is quite a norm to use a DDoS assault or 'flood' in attacking certain enterprises using thousands of hacked machines in addition to other attacks like spamming and phishing. VoIP systems are by nature at the risk of numerous threats particularly DDoS and DoS attacks. The Internet telephone attributes offered by companies like Vonage and Skype can facilitate the programmers' control over their infected devices.

3.5 Spam over VoIP

Another potential issue is that of spam (that is, invasive junk messages). Just like email systems, spam over Voice over Internet Protocol (VoIP) is known as Spam over Internet Telephony (SPIT). SPIT can also be treated as another type of threat posed by a lot of bots which are likely to paralyze the VoIP. And when a VoIP user receives numerous incessant daily calls from an audio spammer he is likely to stay away from VoIP services.

Spam over the Internet Telecommunications is worse than spam. Receiving our emails even with a few minutes delay is not a big issue, but with SPIT, it is very unpleasant to the end users as it targets the gateways and reduce the voicing quality. Any IP based phoneline system can be a victim of SPIT. Several companies are establishing remedies for such threats to counter the SPIT challenge. Solutions to SPIT include filtering, black/white lists, calling reputation, etc. However, these measures are becoming less useful each day as SPIT strategies are advancing.

3.6 Phone-Targeted Malcode

A virus is an unwelcome software component that precedes the user's instructions and infects the computer systems without their approval.

Interests of the VoIP technology are wide since it encompasses a lot more than voice transmission over distance. The threat of a virus infection is likely to increase as all VoIP applications are allocated with unique IP addresses similar to computers connected to the internet as more VoIP applications are developed. Thereby, applications that use a voice over internet protocol could be vulnerable to virus attacks. It is common for such a circumstance to include a scenario where a virus compromises the VoIP systems with a small self-replicating code injected through a stack overflow attack. In this case, it is important for the VoIP applications to embed a security measure that will monitor the size of the incoming data packet so that it does not exceed the limits of the already existing space in the stack. To conclude, virus attacks are potential security risks based on the need to protect confidentiality, integrity, and availability. The threat of malicious code is ever present and the need to detect and defend against such attacks is an endless challenge, many Intrusion Detection Systems (IDS) have been advocated. One such type of ID systems, uses the fact that fast spreading 'malicious codes' tend to carry out a 'large' number of similar actions within a 'short' time frame.

3.7 Rogue Sets

Rogue set attacks are when a deception is acted out to make an effort to get access to the resources of another person. The attackers execute digital impersonation by installing a new range of VoIP applications within the compromised IP networks then proceed to impersonate one of the call participants. The compromised malicious application then has unlimited access to the provision of malicious activities over the compromised IP application even to the minimal threat on the IP network. To prevent such an attack, VoIP applications may employ a network lock-down strategy against any possible exploitations.

In a lock-down mechanism, only the system administrators can install new VoIP applications onto the network with access to the administrative password and the addition of the new set generates logs to the administrator. Moreover, the VoIP application will be denied access if more than three passwords are input. Thus, the confidentiality protections against rogue sets attacks are effective, but not perfect, as intruders are able to penetrate the IP network.

3.8 Toll Fraud

The term toll fraud refers to situations where a person is able to use the facilities of equipment in making illegal calls. This is one of the common forms of telephony fraud in which an unauthorized offender is able to make expensive long distance calls using devices which they are

not approved to use. In this case, employees in the firm can take advantage of the telephony system's features such as return calls from voice mail (VM) or trunk-to-trunk transfers to make outside calls as well as call forwarding (CF) to outside numbers. In order to prevent this type of attack, it is possible to impose a control mechanism on VoIP applications across the IP network. This exigency implies that even ill-will apparatus has to be authenticated before they gain entry into the Internetwork. Every device is constrained when it comes to external calls. Furthermore, dialing restrictions are imposed on certain categories of individuals and during particular times determined by the administrator. registry of dialing rules has to be complied with for all external calls, which is done before the initiation of any external call.

3.9 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a networking protocol that allows devices to receive IP addresses automatically in any network. DHCP can also be misused technically, as it is easy for someone to impersonate a DHCP server and directly attach himself to the target device's network. Users who connect to the network may unintentionally cause service attacks, thus creating interference in the normal operation of the VoIP server by 'borrowing' all available IP addresses from the server. Also, a rogue VoIP client could spoof its DHCP responses and provide a false configuration. Such an attack can lead to Denial of Service, or facilitate the execution of a MITH, a man-in-the-house attack. In order to prevent such an attack, it is possible for a VoIP application to implement a security policy that restricts IP address allocations to the use of completely default configuration or perform effort to ensure that DHCP response does not serve any objectives of the VoIP application. In another case, we can also suggest this measure: a hundred percent secured VoIP network will have static IP addresses configured for all VoIP applications. Therefore, based on the analysis of the distribution of vulnerabilities, DHCP attacks pose a danger in terms of availability since such an attack can significantly degrade the functioning of VoIP systems.

3.10 Pharming

Pharming attacks also represent another possible DDoS threat to VoIP systems. It is difficult to pin down the origins of the term 'pharming' which is a more sophisticated term than the totally unoriginal 'phishing'. In this case, a person is lured (usually by email or IM) to fill in more personal data than he/she would wish to particularly provide via an (in most instances fake) website. With that said, farmed attacks entail the use of a systems weakness, in this case – a domain name server (dns) which allows redirecting the flow between a client and the server that

they are trying to access. To elaborate further, a simple voice over internet protocol can be misused where telephone calls are made to corporation's customers with the intention of conning them out of sensitive information disguised as a corporate representative. Further voip pharming attacks are centered on adding great volume of traffic to a certain domain for the purposes of executing a DDoS attack.

3.11 Flash Crowds

Besides traditional DoS and DDoS attacks, VoIP systems could be vulnerable to flash-crowds (i.e. sudden surge of innocuous requests directed at the same service). A number of attempts on black-out mitigation have been made. For example, some find the properties of the so called flash crowds. These properties then are used to create dynamic load balancing Web cache algorithm.

The system is based on the fact that high bandwidth applications (i.e. applications with requests per second greater than some threshold) are impacted by flash crowds to a greater extent than low bandwidth applications. The logic is that the variation in response of the high bandwidth application, and the request arrival rate are measured and these two associated with their long term average values are then compared. A flash-crowd signal is generated to a request regulator (which therefore suppresses the inflow of requests) when the response of the fast connections drops (to a certain level below the long term average) and there is a surge in the number of incoming requests (to a certain level above the long term average).

4.0 Self-Assessment Exercise(s)

Question 1
List other security issues associated with VoIP:
Answer
Voice phishing (vishing): Using VoIP to impersonate legitimate entities.
Service theft: Unauthorized use of VoIP services.
Malware attacks: Targeting VoIP systems with malicious software.

Question 2
Describe how to protect against these VoIP security issues:
Answer
Use end-to-end encryption.
Regularly monitor and audit VoIP networks.
Implement stringent user authentication and authorization protocols.

5.0 Conclusion

Applications belonging to the class of Voice over Internet Protocol can embrace Public Key Infrastructure (PKI), which is a protection system aimed at guaranteeing that all information is kept safe from prying eyes to include transmission verification and authentication of both parties in the use of Public and Private Keys.

6.0 Summary

Due to the fact that this type of attack may leak the voice data packets to third parties without permission, or alter the subject matter of conversations lowered the threats to confidentiality and integrity of information raised by Man-in-the-Middle attacks.

7.0 References/Further Readings

Lu, Y. H., Hsiao, S. H. Y., Li, C. Y., Hsieh, Y. C., Chou, P. Y., Li, Y. Y., ... & Tu, G. H. (2022). Insecurity of Operational IMS Call Systems: Vulnerabilities, Attacks, and Countermeasures. IEEE/ACM Transactions on Networking, 31(2), 800-815.

Nayak, G., Mishra, A., Samal, U., & Mishra, B. K. (2022). Depth analysis on DoS & DDoS attacks. Wireless Communication Security, 159-182.

Pereira, D., Oliveira, R., & Kim, H. S. (2021). A machine learning approach for prediction of signaling sip dialogs. IEEE Access, 9, 44094-44106.

UNIT 3: SECURITY POLICY FOR VOIP APPLICATIONS

Unit Structure

1.0 Introduction

Traditionally, it is believed that security threats come from outside the organization. Nevertheless, a controlled environment still presents security threats from its authorized members. There are also more serious threats that cause such losses as tampering with, alteration, or stealing information in the telecommunications sector, including threats from abusive or revenge-seeking insiders who make intentional mistakes or commit hostile acts.

2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will understand various VoIP security issues and vulnerabilities.

3.0 Main Content

3.1 Fundamental of Security requirement

Usually, it is believed that security threats come from external sources. Well-ordered control of the environment becomes disruptive due to unauthorized personnel. Aside from physical damage, the loss caused by intentional errors or malice of employees who harbor grievance and

revenge is significant, such as the loss of data, tampering with, and pollution of information in the telecoms sector.

An important aspect of any information management systems is the need to ensure protection of the data and resources from any unauthorized access or use (confidentiality) or any unauthorized or inappropriate change or tampering (integrity) and at the same time provide them to the authorized users. For this reason, in order to address the security threats, all security policies have to address the three basic security components also known as the CIA triad which refers to confidentiality, integrity and availability respectively.

• Confidentiality: It means that no sensitive information will be revealed. Upon intrusion of the systems, voice data packets are encrypted and hacked; therefore the confidentiality of VoIP applications is compromised.

• Integrity: This restricts the changes of information to the authorized parties only. The integrity of VoIP applications is compromised in circumstances where the contents of the conversation (voice data packets) whose use has been granted is altered, deleted, destroyed, or disclosed.

• Availability: The information and services are expected to be present for use when they are required. The availability of VoIP applications is compromised whenever there is a disruption of the system by an attacker, or the system fails due to other reasons.

3.2 Security Policy

A security policy is a compilation of principles and techniques that define, constrain or govern the provision of security services within a system or organization, for the protection of certain resources. A security assertion is always defined and understood within the boundaries of a security policy. Typically, the design of a security policy would commence with a risk analysis and conclude with a body of security claims that is ready for implementation in the security framework of the object, say, a directory service. Risk Analysis is used to define the threats existent in a business process, and creates a set of security claims with respect to how certain behavior or sensitive information will be processed and secured in a distributed processing environment. A Security Policy is typically described in an abstract manner, or it may be described in an abstract manner and may be incorporated into a security model which forms the basis for carrying out security properties verification in a systematic manner.

The associated security policy implements the Secure Real-time Transport Protocol (SRTP) which in turn uses the Advanced Encryption Standard (AES) in counter mode to achieve the approximate measures presented below: 1. encryption of the respective payloads in order to ensure confidentiality for RTP; 2. integrity for the entire RTP packets, as well as protection against replay attacks at the same time; 3. the ability to refresh session keys at regular intervals which serves to reduce the volume of plain text encrypted with a given key; 4. an open-ended system that can be enhanced with new encryption methods; 5. a method of establishing session keys that uses a pseudo-random function securely at both ends; 6. the introduction of salt keys to counter pre-computation threats; and 7. support for the RTP unicast and multicast applications security.

3.3 VoIP Networks Protection

In the past when VoIP was not available, yet there were internet consumers who were aware of the risk that came with transferring data over the internet; however, they were hoping for a private network that would carry their voice calls. With the VoIP technology introduced, and as the voice and data networks started to merge together, the voice security concerns became data security concerns. As much as VoIP technology is associated with internet protocol, that does not mean that it is impossible to secure it. In order to provide protection from threats to the VoIP services, it is necessary to correct and organize the existing strategies. Integrating voice encryption, authentication, voice firewalls, and voice-data traffic separation should enable the voice protection strategy. In this strategy, appropriate measures to mitigate loss of service due to power failure also have to be introduced. It is also necessary that the voice systems and the other parts of the VoIP architecture are protected from physical access by unauthorized persons. In order to secure the VoIP networks these general suggestions have to be applied:

1. Implementing, host-based and network-based intrusion detection systems, as well as intrusion detection and prevention systems
2. Use of specialized firewalls for Voice over IP protection,
3. Alteration of preset user credentials on the several of the VoIP system components,
4. Ensuring component coverage from the existing risks, and in addition
5. The Manufacturer’s recommendations on the protection of all systems after the deployment have been adhered to.

The core principles of VoIP were presented and we enumerated the most critical risks associated with it too. With the enhanced pace of penetration of VoIP technology in telecommunication systems, it can

only be expected that the technology will, in the near future, become one of the leading telephony technologies. The VoIP, like any other facilities based on the internet protocol, bears the risk of various disruptive threats such as viruses, Denial of Services attacks, Distributed Denial of Service attacks, pharming, and others, which all have a chilling effect on the functioning of network infrastructures. One is left in little doubt that security measures must also be emphasized in order to avert problems.

4.0 Self-Assessment Exercise(s)

Question 1
What are the key elements of a security policy for VoIP applications?
Answer
Encryption protocols: Ensure confidentiality and integrity of communication.
Authentication mechanisms: Verify users and devices.
Intrusion detection and monitoring: Identify and respond to security incidents.

Question 2
Discuss how security policies should be applied to VoIP
Answer
Security policies should cover the entire VoIP infrastructure, including devices, gateways, and network elements, ensuring that best practices are followed for encryption, access control, and monitoring.

5.0 Conclusion

In coping with social behavior on the Internet the VoIP does not escape the number of weaknesses that can be exploited by malicious code, DoS, DDoS, and pharming these, in addition to flash crowds all of which are a potential threat to the underlining network infrastructure. It is clear that there is a need for security policies to be enforced in order to prevent catastrophes from occurring.

6.0 Summary

We have distilled the primary ideas regarding VoIP and discussed some of its key vulnerabilities. As VoIP keeps making inroads into the telecommunications arena, it appears that in the foreseeable future it is very likely to be one of the main telephony technologies.

7.0 References/Further Readings

Nayak, G., Mishra, A., Samal, U., & Mishra, B. K. (2022). Depth analysis on DoS & DDoS attacks. Wireless Communication Security, 159-182.

Pereira, D., Oliveira, R., & Kim, H. S. (2021). A machine learning approach for prediction of signaling sip dialogs. IEEE Access, 9, 44094-44106.

Pereira, D., Oliveira, R., & Kim, H. S. (2021). Classification of abnormal signaling sip dialogs through deep learning. IEEE Access, 9, 165557-165567.

Sharathkumar, S., & Sreenath, N. (2023). Distributed Clustering based Denial of Service Attack Prevention Mechanism using a Fault Tolerant Self Configured Controller in a Software Defined Network.

Subraveti, H. H. S. N., Knoop, V. L., & van Arem, B. (2020). Improving traffic flow efficiency at motorway lane drops by influencing lateral flows. Transportation Research Record, 2674(11), 367-378.

Tas, I. M., & Baktir, S. (2023). A novel approach for efficient mitigation against the SIP-based DRDoS attack. Applied Sciences, 13(3), 1864.