African Virtual University

Applied Computer Science: CSI 3103

INTRODUCTION TO COMPUTER SECURITY

Richard Musabe

Foreword

The African Virtual University (AVU) is proud to participate in increasing access to education in African countries through the production of quality learning materials. We are also proud to contribute to global knowledge as our Open Educational Resources are mostly accessed from outside the African continent.

This module was developed as part of a diploma and degree program in Applied Computer Science, in collaboration with 18 African partner institutions from 16 countries. A total of 156 modules were developed or translated to ensure availability in English, French and Portuguese. These modules have also been made available as open education resources (OER) on oer.avu.org.

On behalf of the African Virtual University and our patron, our partner institutions, the African Development Bank, I invite you to use this module in your institution, for your own education, to share it as widely as possible and to participate actively in the AVU communities of practice of your interest. We are committed to be on the frontline of developing and sharing Open Educational Resources.

The African Virtual University (AVU) is a Pan African Intergovernmental Organization established by charter with the mandate of significantly increasing access to quality higher education and training through the innovative use of information communication technologies. A Charter, establishing the AVU as an Intergovernmental Organization, has been signed so far by nineteen (19) African Governments - Kenya, Senegal, Mauritania, Mali, Cote d'Ivoire, Tanzania, Mozambique, Democratic Republic of Congo, Benin, Ghana, Republic of Guinea, Burkina Faso, Niger, South Sudan, Sudan, The Gambia, Guinea-Bissau, Ethiopia and Cape Verde.

The following institutions participated in the Applied Computer Science Program: (1) Université d'Abomey Calavi in Benin; (2) Université de Ougagadougou in Burkina Faso; (3) Université Lumière de Bujumbura in Burundi; (4) Université de Douala in Cameroon; (5) Université de Nouakchott in Mauritania; (6) Université Gaston Berger in Senegal; (7) Université des Sciences, des Techniques et Technologies de Bamako in Mali (8) Ghana Institute of Management and Public Administration; (9) Kwame Nkrumah University of Science and Technology in Ghana; (10) Kenyatta University in Kenya; (11) Egerton University in Kenya; (12) Addis Ababa University in Ethiopia (13) University of Rwanda; (14) University of Dar es Salaam in Tanzania; (15) Universite Abdou Moumouni de Niamey in Niger; (16) Université Cheikh Anta Diop in Senegal; (17) Universidade Pedagógica in Mozambique; and (18) The University of the Gambia in The Gambia.

Bakary Diallo

The Rector

African Virtual University

Production Credits

Author

Richard Musabe

Peer Reviewer

Ashenafi Kassahun

AVU - Academic Coordination

Dr. Marilena Cabral

Overall Coordinator Applied Computer Science Program

Prof Tim Mwololo Waema

Module Coordinator

Robert Oboko

Instructional Designers

Elizabeth Mbasu

Benta Ochola

Diana Tuel

Media Team

Sidney McGregor

Barry Savala

Edwin Kiprono

Kelvin Muriithi

Victor Oluoch Otieno

Michal Abigael Koyier

Mercy Tabi Ojwang

Josiah Mutsogu

Kefa Murimi

Gerisson Mulongo

Copyright Notice

Supported By

AVU Multinational Project II funded by the African Development Bank.

Table of Contents

Course Overview

Welcome to Introduction to Computer Security

Introduction to computer security module provides an essential study of computer security issues and methods in networked systems. It focuses on all the processes and mechanisms by which computer based devices, information as well as services are protected from unauthorized users.

Finishing this module, students will have fundamental concepts of computer security and be able to design and develop authentication systems and security systems. Students will be able to learn different types Attacks, threats, vulnerabilities and Prevention Mechanisms in computer. They will be able to understand different types of malicious software and software security.

This module is important because students learn the methods and tools in computer security and they also learn how to secure operations in a networked environment

Prerequisites

- Introduction to operating systems
- Introductions to applied computer science
- Data communications and computer networks

Materials

The materials required to complete this course are:

Laptops, Smart Phones, Video Conferencing, face to face (Boards)

Biography

- Pfleeger, Charles P., Pfleeger, Shari L., "Security in Computing", Fourth Edition, Prentice Hall PTR, 2006.

- Malik, S., "Network Security Principles and Practices". Cisco Press. 2002.

- Mark Rhodes-Ousley, et al. "Network Security: The Complete Reference," 2003.

- Kaufman, C., et al., "Network Security: Private Communication in a Public World". 2ed., Prentice Hall, 2002.

- Gert DeLaet, Gert Schauwers, "Network Security Fundamentals", Cisco Press Fundamentals Series, 2004

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008.

- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2.

- William Stallings "Cryptography and Network Security: Principles and Practice," 4th Ed, 2011.

- William Stallings "Network Security Essentials:Applications And Standards"Fourth Edition, 2011.

Course Goals

Upon completion of this course the learner should be able to :

- Identify and discuss the concepts of computer security
- Apply the functionality of authentication and access control to the computer system
- Assume responsibility for installing, configuring, and maintaining network security
- Apply Professional, ethical , legal responsibilities of computer security engineers
- Identify social impact of computer security in day to day activities i.e. online transactions, e-commerce and e-management
- Indentify Information system threats, vulnerabilities, and risks to the computer system
- Understand the method and tools of computer security

Units

- **Unit 1: General concepts of Computer security**
- It introduces the computer security concepts including key computer security objectives, challenges of computer security, and the model of computer securit
- **Unit 2: Attacks, threats ,vulnerabilities**

This unit focuses on different threat and attack types.

- **Unit 3: software security and prevention mechanism**

This unit focuses on different malicious software and prevention mechanisms

- **Unit 4: Properties of computer security**

This unit introduces different authentication methods and some security infrastructures

Units

Unit 0: Pre-Assessment

Unit 1: Fundamentals of Artificial Intelligence

- The study of mental faculties through the use of computational models
- The study of computations that make it possible to perceive, reason, and act.
- The study of natural intelligence by the use of computer models.

Unit 2: Artificial Intelligence Programming

- Programming logic
- Designing and implementing intelligent components for interactive distributed computational media
- Developing tools for authoring the knowledge needed by such systems

Unit 3: Machine Learning and Games

- Computer Vision to perceive objects,
- Robotics to move them about.
- Machine Learning to adapt to new circumstances and to detect and extrapolate patterns.

Unit 4: Natural Language, Representation and Reasoning

- Natural Language Processing to enable it to communicate successfully in English (or some other human language).
- Knowledge Representation to store information provided before or during the interrogation.
- Automated Reasoning to use the stored information to answer questions and to draw new conclusions.

Assessment

Formative assessments, used to check learner progress, are included in each unit.

Summative assessments, such as final tests and assignments, are provided at the end of each module and cover knowledge and skills from the entire module.

Summative assessments are administered at the discretion of the institution offering the course. The suggested assessment plan is as follows:

1	[Assignments]	[30%]
2	MINI TEST (Continuous assessment Test)	[30%]
3	Final assessment: Exam	[40%]

Schedule

Unit	Activities	Estimated time
[Unit 1: General concepts of Computer Security]	Activity 1:1 Definition and Examples of Computer Security	[1 hour]
	Activity 1:2: The challenges of Computer Security	30 minutes
	Activity 1:3: A model of Computer Security	30 minutes
	Activity 1.4: Introduction to Cryptography	2 hours
[Unit 2 Attacks, Threats, Vulnerabilities]	Activity 2:1 Threats and Types of Threats	[1 hour]
	Activity 2:2: Threats and Assets	1 hour
	Activity 2:3: Vulnerabilities	1 hour
Unit3: Software Security and Prevention Mechanism	Activity 3:1:Types of Malicious Software	[30 minutes]

	Activity 3:2: System Corruption and Infrastructure Theft	1 hour
	Activity 3.2: Security Auditing and Event Monitoring in a Computer system	1 hour and 30 minutes
Unit4: Properties of Computer Security	Activity 4.1: Authentication	[1 hour]
	Activity 4.2: Access Control	1 hour
	Activity 4.3: IDS	30 minutes
	Activity 4.4: Firewalls	30 minutes
Final Exams	Final assessment	3 hours

Readings and Other Resources

The readings and other resources in this course are:

Unit 1

Required readings and other resources:

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2

Unit 2

Required readings and other resources:

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2
- William Stallings "Cryptography and Network Security: Principles and Practice," 4th Ed, 2011
- William Stallings "Network Security Essentials:Applications And Standards" Fourth Edition , 2011

Unit 3

Required readings and other resources:

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2

Unit 4

Required readings and other resources:

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- William Stallings "Cryptography and Network Security: Principles and Practice," 4th Ed, 2011
- William Stallings "Network Security Essentials:Applications And Standards" Fourth Edition , 2011

Unit 1. General concepts of Computer security

Unit Introduction

With the use of the Internet, the concept of sharing and information access has changed dramatically, more and more companies open their information system to their partners or their suppliers, thus being able to arouse others curiosity to know the information in their companies. For this reason, companies must be prepared to defend this private information invasion, therefore it must meet the company's resources to protect and dominate the access control and user rights information.

However, in order to protect a computer system, it is necessary to identify potential threats and therefore know and predict the way to make the defense of the enemy. This unit introduces the computer security concepts including key computer security objectives, challenges of computer security, and the model of computer security

Unit Objectives

Upon completion of this unit you should be able to:

- Identify the key concepts of computer security
- Apply the model of computer security
- Identify different challenges of computer security
- Apply cryptographic method called Encryption
- Apply the encryption and signing at the application level Case SSL
- Apply the encryption and signing at the network level: case IPSec

Key Terms

Confidentiality: preserving authorized restrictions on information access and disclosure

Integrity: Guarding against improper information or destruction.

Availability: Ensuring timely and reliable access to and use of information

Learning Activities

Activity 1.1 - Definition and examples of Computer security

Introduction

The term security is not new for us and even young children have heard this term in radio, television etc., applied in other areas including: military, food, public, road and others. However in computers the term security is exclusively dedicated to protecting information.

Currently the concept of Information Security is standardized by ISO / IEC 17799: 2005, influenced by the Standard English (British Standard) BS 7799. The series of ISO / IEC 27000 have been reserved for dealing with security standards of information. The ISO / IEC 27002: 2005 is still considered formally as 17799: 2005 for historical purposes. The content of the Net Workshop is protected under the Creative Commons license (CC BY-NC-ND). You can play it as long as insert credits WITH LINK to ORIGINAL CONTENT and do not make commercial use of our production.

In this activity, the concept of computer security will be used to refer to the protection of the information and also key computer security objectives will be discussed

Activity Details

Computer security can be defined as the ability to offer protection to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

This definition introduces three key security objectives which are:

- Confidentiality: preserving authorized restrictions on information access and disclosure.
- Integrity: Guarding against improper information or destruction.
- Availability: Ensuring timely and reliable access to and use of information

The losses of these key security objectives will results into the following factors:

- Loss of confidentiality : Unauthorized disclosure of information
- Loss of Integrity: Unauthorized modification or destruction of information
- Loss of Availability: Disruption of access to or use of information

These three Security objectives form what is often referred to as the CIA triad (Confidentiality, Integrity, and Availability). There are many critiques that suggest that this does not provide a complete picture of security requirements. The two most commonly cited “Extra” requirements are:

1. Authenticity: Being genuine, verified and trusted. Confidence in the validity of a transmission, a message and a message originator. Verifying that users are how they say they are and that each message came from a trusted source
2. Accountability: Actions of an entity can be traced uniquely to that entity. This Supports Fault isolation, Recovery , and Intrusion detection and prevention

Conclusion

This activity introduced key computer security objectives, where we discussed the CIA trend and the extra requirements for computer security

Assessment

1. What is computer security
2. Provide three key security objectives
3. What are the two most common cited Extra requirements of computer security?

Activity 1.2 - The Challenges of Computer Security

Introduction

In this activity, different challenges of computer security will be discussed

Activity Details

Some of the Computer security challenges are:

- Complex: Computer security may look to be easy to use because its requirements are straightforward and self-explanatory i.e. confidentiality, authentication, nonrepudiation, integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning
- Development and ownership of the security algorithms: Security mechanism may require more than one algorithm or protocol; it may also require some individuals to keep some secret information (e.g., an encryption key). This brings up a challenge of creation, distribution, and protection of that secret information. There may also be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism
- Placement of Security algorithm: If your security algorithm is successful, there is another challenge of knowing where to use it. This is necessary for both physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such

as TCP/IP(Transmission Control Protocol/Internet Protocol) should the security algorithm be placed].

- Potential Attacks: While developing a specific security mechanism or algorithm, one should always first analyze the potential attacks on those security features. However, the successful attacks are designed by analyzing the problem in a completely different way; hence take advantage of an unexpected weakness in the developed algorithm.
- Battle between the Wits: Computer security is normally a battle between the minds of the person who is trying to find security holes and the administrator who tries to close them. The main advantage of the person trying to find security holes is that he or she only needs to find a single weakness while the administrator must find and eliminate all weaknesses to achieve perfect security
- Ignorance: There is a natural trend on the part of system users and administrators to understand the need of security investment until a security failure occurs
- Lack of Time: Computer security needs constant, monitoring, and this is sometimes a big challenge for some people due to lack of time with their overloaded workload.
- Poor Planning: Computer security is most of the time incorporated into a system after the design is complete rather than being an integral part of the design process. It is sometimes also seen as an obstacle to efficient and user-friendly operation of an information system or use of information.

Conclusion

This activity highlighted different challenges that are faced when implementing computer security

Assessment

Briefly describe the challenges of computer security

Activity 1.3 - A Model for Computer Security

Introduction

In this activity, the model of computer security will be discussed, where some hardware and software components are discussed.

Activity Details

A Model for Computer Security

In the computer security model, we need to look at system resource, or asset, that users and owners wish to protect. The complete computer system resources are composed of the following:

Hardware: A computer's hardware consists of electronic devices; the parts you can see and touch. It consists of its processors, its storages, its input/output devices and its communication connections (i.e. the actual machinery: wires, transistors and circuits.). The term "device" refers to any piece of hardware used by the computer, such as a keyboard, monitor, modem, mouse, etc.

Software: Software is a general term used to describe all the various programs .It consists of organized sets of instructions for operating the computer system. Some programs exist for the computer's use, to help it manage its own tasks and devices; these operations may include identifying, accessing and processing information. Other programs exist for the user, and enable the computer to perform tasks for you, such as creating documents.

Data: Data consists of raw facts, which the computer can manipulate and process into information that is useful to people. Computerized data is digital, meaning that it has been reduced to digits, or numbers. The computer stores and reads all data as numbers. Although computers use data in digital form, they convert data into forms that people can understand, such as text, numerals, sounds, and images.

Communications facilities and networks: Local and wide area network communication links, bridges, routers, and so on.

Users: People are the computer's operators, or users. Some types of computers can operate without much intervention from people, but personal computers are designed specifically for use by people

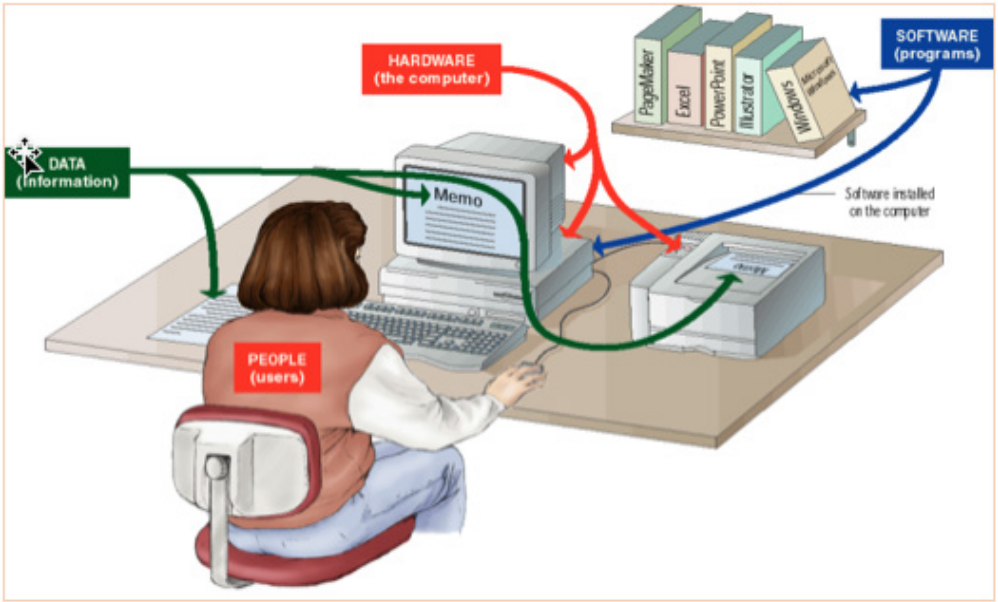

Figure 1.1: Showing a complete Computer system resources

In the terms of computer security, these computer system resources can be under different categories of vulnerabilities. The general categories of vulnerabilities of a computer system resources or network resources are:

Vulnerabilities that correspond to the CIA trend: The computer system resources can be corrupted, so that it does the wrong thing or gives wrong answers. For example, stored data values may differ from what they should be because they have been improperly modified. Computer system resources can also become leaky. For example, someone who should not have access to some or all of the information available through the network obtains such access. Finally, they can become unavailable or very slow. That is, using the system or network becomes impossible or impractical.

Threats: A threat is the main security harm to the computer security resources. They are capable of exploiting any computer security vulnerabilities. An attack is a kind of threat that if carried out successful can lead to an undesirable violation of computer security, or threat consequence. The people performing these kinds of attack are known as an attacker. The attacks can be of two types; Active attack which is an attempt to alter system resources or affect their operation and Passive attack which is an attempt to learn or make use of information from the system but does not affect system resources. These types of attacks can also be classified based on the origin of the attack i.e. Inside attack which is started by an person/item inside the security perimeter (an "insider") and Outside attack which is started by a person/item from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). These kinds of attacks can be controlled under the process known as countermeasure. It involves prevention, where a particular attack is stopped from being successfully executed. If prevention fails, then the next step is to detect the attack and then recover from the effects of the attack.

Conclusion

This activity explained the computer security model where the important computer assets and resources that need to be protected were explained.

Unit Assessment

Briefly explain the main resources that a computer security model can protect.

Activity 1:4- Introduction to cryptography

This activity introduces cryptography and it's technologies like encryption and decryption, as well as digital signatures. This will be just an introductory part as detailed cryptography will be studied in the advanced module.

Definition:

It is a collection of mathematical techniques for protecting information. The most important technique used is: encryption/decryption which is divided into Symmetric encryption (symmetric key encryption): where encrypt/decrypt a message using the same key and Asymmetric encryption (asymmetric key encryption): where one key used for encryption (public key), another key used for decryption (private key). A Key can be defined as a piece of information or sequence of bits

The Public Key Infrastructure (Encryption/Decryption)

The Public Key Infrastructure

Public Key Infrastructure (PKI) is a security architecture that has been introduced to provide an increased level of confidence for exchanging information over the Internet. It is defined in 2 ways: It defined as the method, technology and technique used to create a secure data infrastructure. It can also be defined as the use of the public and private key pair to authenticate and for proof of content.

Benefits of PKI

PKI aims to offer its users the following benefits:

- Certainty regarding the quality of information transmitted electronically
- Certainty of the source and destination of such information
- Assurance of the time and timing of such information
- Certainty of the privacy of such information
- Assurance that such information may be used as evidence in a court of law

Use of PKI

- To support secure information exchange over insecure networks. e.g. the Internet where such features cannot be provided easily
- For information exchange over private networks. e.g. an organisation's internal network
- To securely deliver cryptographic keys.
- To facilitate other cryptographically delivered security services

How Does PKI Work?

PKI uses a mathematical technique called public key cryptography. A pair of related cryptographic keys are used. It Verifies the identity of the sender (through signing)and ensures privacy (through encryption of data)

Public Key Cryptography

It U uses a pair of mathematically related cryptographic keys where one key is used to encrypt information and only the related key can decrypt that information. Knowledge of one key does not allow you to calculate the other.

Public Keys and Private Keys

The public key is made public - it is freely distributed and can be seen by all users. A corresponding (and unique) private key is kept secret and is not shared amongst users. Your private key enables you to prove that you are who you claim to be.

Public Key Encryption

When a person wants to send confidential data to a private key holder. They encrypt the data. The data is encrypted using a secret key algorithm (symmetric cryptography) which is much faster than the asymmetric cryptography. A random session key is generated using a symmetric algorithm to encrypt the data. The public key is then used to encrypt that key and both are sent securely to the recipient.

Private Key Decryption

When a private key holder receives confidential data, If the private key can decrypt the data, the user is certain that the data is meant for him/her but cannot identify the originator. The private key decrypts the session key. The decrypted session key is used to decrypt the actual data.This is more secure as the session key has to be decrypted first in order to proceed to the next process of decrypting the data

Example

When a confidential message is stored on an insecure media or if sent over an insecure communication channel, it should be protected. Let M be the set of clear messages, C all encrypted messages, K all keys. Encryption algorithm is E and the decryption algorithm is D. An encryption scheme is a tuple (M, C, K, E, D) such that for all k et elements of K there exists and such that for any clear messages; is

Note that

- if M = C, then our encryption is a permutation;
- if k = k then the encryption is symmetric;
- if is different from but one that can be derived from the other, then the larly chiff says asymmetric

Digital signature

The signature is an inscription a person because of his name (in particular, constant shape) to affirm the accuracy, sincerity of a writing or take responsibility. Indeed, sign it is part of everyday life. The gesture seems to be above the rest. However, the signature remains a self-representation that provides the eyes of others and the whole of society. In all cases, the signature is the responsibility of the signatory. This signature authenticates an artistic, literary, intellectual or contract. Without realizing it, our signing involves our responsibility in the establishment of the most common acts. The signing has two main judicial functions:

- The identification of the author and the manifestation of consent. Digital signature is the electronic counterpart to the handwritten signature, but the digital signature is linked to the signed document, it is not compared to a witness signature is verified but finally algorithmically it is universally verifiable
- A digital signature provides non-repudiation in origin. Indeed the signatory can convince a third party that is not a signatory; it cannot repudiate his signature.

A digital signature is generated by an algorithm for generating digital signatures and is verified by a digital signature verification algorithm.

There are two classes of signatures schemes:

- with appendix where the original message is to be provided to the verification algorithm
- Overlapping where the original message is retrieved from the signature.
- Let M be a finite set of messages, MS Signable a finite set of messages, S a finite set of signed messages and K a finite set of key pairs (public and secret). For any pair of public and secret key (,) There is an overlapping signature algorithm applying function and a corresponding verification algorithm : such as the signing of a message x and if then the signature is accepted or the signature is rejected.
- Signatures with appendices: each signatory has a private key to sign and a corresponding public key to verify signatures produced. Let M be a finite set of messages, S a finite set of signatures and K a finite set of key pairs (public and secret). For any pair of public and secret keys (,), There is a signature algorithm with appendix and a corresponding verification algorithm such as the signing of a message x : and

The signature and encryption are often integrated into a software protection kit (implementation of a protocol security) or hardware (VPN). These methods can also be implemented in different levels of the network model. As an example we will see the SSL protocol that is implemented at the application level and IPsec that may be installed at the entrance of a network and creating a tunnel communication between two or more sites.

The encryption and signing at the application level Case SSL

Place security at the transport layer (or to an intermediate level between the transport and applications4) for Internet communications, such was the idea of Netscape in 1995, when he proposed a security package SSL (Secure Socket Layer) in his famous browser. SSL builds a secure connection between two sockets (hence its name) with negotiating security parameters (cryptographic suite) and mutual authentication of both ends. SSL is used, for example, for electronic payments online. An encrypted session sends the credit card number. Encryption uses the RSA algorithm for authentication and a symmetric algorithm (DES, IDEA, 3DES...) to ensure the confidentiality of the transmission. Added there too is a hash function MD5 to ensure the integrity of the transmission. SSL was a huge success. Most web browsers have subsequently incorporated SSLv2 (version 2) and SSLv3 (version 3) and now TLSv1 (Transport Layer Security, version 1). Indeed, the IETF (Internet Engineering Task Force) has standardized version 3.1 and renamed TLS in RFC 2246. When a transaction is secure, browsers typically display a closed padlock in the corner of the screen. In the TCP / IP protocol stack, SSL is located between the layers and Applications TCP transport layer. SSL operates independently from the applications that use it. Its most common use is with HTTP, data transport protocol for Web pages. The user chooses his/her browser to use the conventional navigation (HTTP)

or secure browsing (HTTPS), which reads in the displayed URL. HTTPS actually means http SSL security mechanisms. Exchanges that are defined by the SSL protocol takes place in two phases, authentication server and the client. Receiving a request from a client, the server sends its certificate to the client and the list of algorithms it can use. The client checks the validity of the certificate using the public key of the certificate authority contained in the browser. If the certificate is valid, the client generates a first key it sends to the server encrypted with the public key of the server. This key is used to calculate a session key for data exchanged thereafter between the client and the server. The server may ask the client to authenticate (the client authentication is optional). The client responds by sending its certificate and session information and content of previous exchanges it signs with its private key. The server can verify that it is the customer claimed using the public key of the latter.

The encryption and signing at the network level: case IPSec

Was designed IPSec (Internet Protocol Security) to secure IPv6. The latter deployment delays imposed an IPSec adaptation to the current IPv4 protocol. Several successive RFCs describe the different elements of IPSec: RFC 2401, 2402, 2406, 2408. . We establish a tunnel between two sites, and IPSec manages all security parameters associated with the communication. Two footbridges machines located at each end of the tunnel, negotiate the terms of the exchange of information: what encryption algorithms, which methods of digital signature and key used for these mechanisms. Protection is provided to all traffics and is transparent to different applications. IPSec provides the definition of security policy with the choice of algorithms and scope. It can implement the authentication by assuming that both ends already share the secret session key generation, or by using certificates and RSA signatures. The gateway machines then process the data with the associated security policy. For example, it is possible to authenticate the IP addresses used and the data through a digital signature and encrypt the entire IP packet by encapsulating it in a new package. This has the effect of making the package unusable by an unauthorized user. Indeed, IPSec then proposes two alternative mechanisms for data exchange: ESP (Encapsulating Security Payload) and Authentication Header (AH). ESP provides integrity and confidentiality, AH provides integrity. The IP datagram flowing through the tunnel are machinery end of the tunnel gateways. IPSec encapsulates the datagram users from one site to another. This makes it impossible to know the internal IP addresses spying on Internet traffic. The value of the solution of IPSec tunnels is the fact that users do not see anything; no software is needed on their machines. However, for mobile users, consider another configuration since their traffic does not pass through the gateway machine. IPSec Transport mode known addresses this situation. Unlike the tunnel mode, it needs to install special software on each client computer to manage security settings to encrypt and calculate signatures.

These safeguards from cryptography are sometimes combined with other non-cryptographic mechanisms. In the section that follows, we will focus our attention on the safety audit

Conclusion

This activity explained the introductory part of cryptography and it's technologies which included PKI and digital signature

Unit Assessment

1. What is Cryptography?
2. What is PKI
3. How does PKI work?
4. What are the main uses of PKI?
5. Differentiate Symmetric encryption from asymmetric encryption

Unit Summary

This unit covered;

- the computer security concepts including key computer security objectives,
- challenges of computer security,
- the model of computer security where the important computer assets and resources that need to be protected were explained

The introductory part of cryptography

- Cryptographic method called Encryption
- The encryption and signing at the application level Case SSL
- The encryption and signing at the network level: case IPSec

Unit Assessment

Check your understanding!

Unit Evaluation

To verify that understands the issues discussed in this unit, answer the following questions:

Instructions

In case of doubt read the corresponding content or query again on the Internet.

Evaluation

1. What is computer security
2. 4Provide three key security objectives
3. What are the two most common cited Extra requirements of computer security?

4. Briefly explain the main resources that a computer security model can protect.
5. Briefly describe the challenges of computer security
6. Briefly explain the main resources that a computer security model can protect
7. What is Cryptography?
8. What is PKI
9. How does PKI work?
10. What are the main uses of PKI?
11. Differentiate Symmetric encryption from asymmetric encryption

ASSESSMENT STRATEGY

Assessment on this unit is made both continuous and terminal. The continuous assessment may have several components like problem solving, quizzes, assignments. The assessment strategy is aimed to test the

- Knowledge gained in key computer security concepts
- Ability to understand different challenges of computer security
- The examination is used to assess the general knowledge of computer security model

Assessment Criteria:

- For the examination setting and marking the AVU generic marking criteria will be used.
- For the assignment, criteria will be drawn up appropriate to the skills assessed , based on the AVU generic marking criteria

Grading Scheme

Activity 1.1: 6 marks

Activity 1.2: 8 Marks

Activity 1.3: 5 Marks

Activity 1.4: 10 marks

Feedback

Activity 1.1:

1. 14. What is computer security (1 mark)

   - Computer security can be defined as the ability to offer protection to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

2. 15. Provide three key security objectives (1 mark each)

   - Confidentiality: preserving authorized restrictions on information access and disclosure.
   - Integrity: Guarding against improper information or destruction.
   - Availability: Ensuring timely and reliable access to and use of information
   -

3. 16. What are the two most common cited Extra requirements of computer security? (1 mark each)

   - Authenticity: Being genuine, verified and trusted. Confidence in the validity of a transmission, a message and a message originator. Verifying that users are how they say they are and that each message came from a trusted source
   - Accountability: Actions of an entity can be traced uniquely to that entity. This Supports Fault isolation, Recovery , and Intrusion detection and prevention

Activity 1.2:

1. Briefly describe the challenges of computer security (1 mark each)

   - Complex: Computer security may look to be easy to use because its requirements are straightforward and self-explanatory i.e. confidentiality, authentication, nonrepudiation, integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning
   - Development and ownership of the security algorithms: Security mechanism may require more than one algorithm or protocol; it may also require some individuals to keep some secret information (e.g., an encryption key).
   - This brings up a challenge of creation, distribution, and protection of that secret information. There may also be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism
   - Placement of Security algorithm: If your security algorithm is successful, there is another challenge of knowing where to use it. This is necessary for both physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP(Transmission Control Protocol/Internet Protocol) should the security algorithm be placed].
   - Potential Attacks: While developing a specific security mechanism or algorithm, one should always first analyze the potential attacks on those security features.

However, the successful attacks are designed by analyzing the problem in a completely different way; hence take advantage of an unexpected weakness in the developed algorithm.

- Battle between the Wits: Computer security is normally a battle between the minds of the person who is trying to find security holes and the administrator who tries to close them. The main advantage of the person trying to find security holes is that he or she only needs to find a single weakness while the administrator must find and eliminate all weaknesses to achieve perfect security
- Ignorance: There is a natural trend on the part of system users and administrators to understand the need of security investment until a security failure occurs
- Lack of Time: Computer security needs constant, monitoring, and this is sometimes a big challenge for some people due to lack of time with their overloaded workload.
- Poor Planning: Computer security is most of the time incorporated into a system after the design is complete rather than being an integral part of the design process. It is sometimes also seen as an obstacle to efficient and user-friendly operation of an information system or use of information.

Activity 1.3:

Briefly explain the main resources that a computer security model can protect. (1 mark each)

Hardware: A computer's hardware consists of electronic devices; the parts you can see and touch. It consists of its processors, its storages, its input/output devices and its communication connections (i.e. the actual machinery: wires, transistors and circuits.). The term "device" refers to any piece of hardware used by the computer, such as a keyboard, monitor, modem, mouse, etc.

Software: Software is a general term used to describe all the various programs .It consists of organized sets of instructions for operating the computer system. Some programs exist for the computer's use, to help it manage its own tasks and devices; these operations may include identifying, accessing and processing information. Other programs exist for the user, and enable the computer to perform tasks for you, such as creating documents.

Data: Data consists of raw facts, which the computer can manipulate and process into information that is useful to people. Computerized data is digital, meaning that it has been reduced to digits, or numbers. The computer stores and reads all data as numbers. Although computers use data in digital form, they convert data into forms that people can understand, such as text, numerals, sounds, and images.

Communications facilities and networks: Local and wide area network communication links, bridges, routers, and so on.

Users: People are the computer's operators, or users. Some types of computers can operate without much intervention from people, but personal computers are designed specifically for use by people.

Activity 1.4:

1. What is Cryptography? (1 mark)

   - It is a collection of mathematical techniques for protecting information.

2. What is PKI (1 mark)

   - Public Key Infrastructure (PKI) is a security architecture that has been introduced to provide an increased level of confidence for exchanging information over the Internet.

3. How does PKI work? (2 marks)

   - PKI uses a mathematical technique called public key cryptography. A pair of related cryptographic keys are used. It Verifies the identity of the sender (through signing)and ensures privacy (through encryption of data)

4. What are the main uses of PKI? (4 marks)

   - To support secure information exchange over insecure networks. e.g. the Internet where such features cannot be provided easily

   - For information exchange over private networks. e.g. an organisation's internal network

   - To securely deliver cryptographic keys.

   - To facilitate other cryptographically delivered security services

5. Differentiate Symmetric encryption from asymmetric encryption (2 marks)

   - In Symmetric encryption (symmetric key encryption) the message is encrypt/decrypt using the same key while in Asymmetric encryption (asymmetric key encryption), one key is used for encryption (public key), another key used for decryption (private key).

Unit Readings and Other Resources

William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008

Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2

Unit 2. Attacks, threats and vulnerabilities in computer

Unit Introduction

This unit focuses on different threat and attack types. It also introduces some computer security vulnerabilities as well as different prevention mechanisms.

Unit Objectives

Upon completion of this unit you should be able to:

- Identify different threats and types of attacks
- Describe the relationship between threats and computer assets
- Identify computer security vulnerabilities
- Describe the notions of encryption and their implementations
- Identify the mechanisms of the systems and their modes of action

Key Terms

Passive Attacks: Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions

Active Attack: Active attacks involve some modification of the data stream or the creation of a false stream

Unstructured threats: Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers

Structured threats: Structured threats come from hackers who are more highly motivated and technically competent

External threats: External threats can arise from individuals or organizations working outside of a company

Internal threats: Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network

Encryption: Encryption is a cryptographic method to ensure the Confidentiality of information stored or exchanged over insecure channels

Signature: Digital signature is a security mechanism that often goes along with encryption but rather provides them authenticity

Audit: The audit is generally an activity to assess how a system (financial, insurance...) behaves or operates against the standards established in the field.

Learning Activities

Activity 2.1 - Threats and Types of attacks

Introduction

In this activity, different threats and types of attacks will be discussed. these include; unauthorized disclosure, deception, disruption, and usurpation

Activity Details

There are four kinds of threat consequences and different types of attacks that result in each consequence.

1. **Unauthorized disclosure**

This is a threat to one of the CIA trend component known as confidentiality. The following types of attacks can result in this threat consequence:

- **Exposure:** This can be intentional, where someone willingly provided sensitive information, such as credit card numbers, to unauthorized person. It can also be the result of a human, hardware, or software error, which results in an entity gaining unauthorized knowledge of sensitive data. There have been numerous instances of this, such as universities accidentally posting student confidential information on the Web.
- **Interception:** This type of attack is a common in communications systems mainly on a shared local area network (LAN), such as a wireless LAN or a broadcast Ethernet. Devices attached to the LAN can receive a copy of packets intended for another device. On the Internet, a determined hacker can gain access to e-mail traffic and other data transfers.
- All of these situations create the potential for unauthorized access to data.
- Inference: Traffic analysis is the main type of interference attack. It involves gaining information from observing the pattern of traffic on a network, such as the amount of traffic between particular communication devices on the network.
- Intrusion: This involves an attacker gaining unauthorized access to sensitive data by bypassing the system's access control protections.

2. **Deception**

This is a threat to one of the CIA trend component known as integrity. The following types of attacks can result in this threat consequence:

- **Masquerade:** Masquerade involves an attempt by an unauthorized user to gain access to a system by posing as an authorized user. This is possible if the unauthorized user gains access to another user's logon ID and password. It can also happen if malicious software, like a Trojan horse, that appears to perform a useful or desirable function but actually gains unauthorized access to system resources or tricks a user into executing other malicious acts.
- **Falsification:** This is the ability to change or replace a valid data or put false data into a file or database. For example, a student may alter his or her grades on a school database
- **Repudiation:** In this case, a user either denies sending data or a user denies receiving or possessing the data.

3. **Disruption**

This is a threat to two of the CIA trend components known as availability and Integrity. The following types of attacks can result in this threat consequence:

- **Incapacitation:** This is an attack on system availability. This can happen as a result of physical destruction of or damage to system hardware. Most notably , malicious software, like Trojan horses, viruses, or worms, could work in a way to disable a system or some of its services.
- **Corruption:** This is an attack on system integrity. Malicious software in this context could operate in such a way that system resources or services function in an unintended manner. Or a user could gain unauthorized access to a system and modify some of its functions.
- **Obstruction:** This type of attack involves obstructing the system operation in such way that you can be able to interfere with communications by disabling communication links or altering communication control information. It also involves overloading the system by placing excess burden on communication traffic or processing resources.

4. **Usurpation**

This is a threat to one of the CIA trend components known as integrity. The following types of attacks can result in this threat consequence

- **Misappropriation:** This involves theft of service. An example is a distributed denial of service attack, when malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host. In this case, the malicious software makes unauthorized use of processor and operating system resources.
- **Misuse:** Misuse can occur by means of either malicious logic or a hacker that has gained unauthorized access to a system. In either case, security functions can be disabled or thwarted.

Conclusion

This activity explained in details different threats and types of attacks on computer security.

Assessment

Briefly explain different threats and attacks on computer security

Activity 2.2 - Threats and Assets

Introduction

In this activity, the relationship between threats and computer assets will be discussed it briefly describes how computer resources are related to the concepts of the three components of the CIA trend.

Activity Details

In the previous unit, we mentioned that computer system resources can be categorized as hardware, software, data, users, communication lines and networks. In this activity, we briefly describe these categories and relate them to the concepts of the three components of the CIA trend.

- HARDWARE: The main threat to computer system hardware is the threat to one of the CIA trend component called availability. The hardware component of a computer system is the most vulnerable to attack and the least susceptible to automated controls. Threats can be of different kinds such as accidental and deliberate damage to different devices as well as their theft. The production of personal computers and workstations and the widespread use of LANs increase the potential for losses in this area. Theft of memory devices such as CD-ROMs and DVDs can lead to loss of confidentiality as that's where sensitive information is mostly kept. Physical and administrative security measures are needed to deal with these threats.
- **SOFTWARE**: Again the main threat to computer system software is an attack on CIA trend component called availability. Software, especially application software, can easily be deleted, changed or damaged which tends to make it useless. Careful software configuration management, which includes making backups of the most recent version of software, can maintain high availability.
- **DATA and USERS:** Security of the two computer system components discussed earlier (hardware and software) are a concerns of computing center professionals or individual concerns of personal computer users. The main problem is data security, which involves files and other forms of data controlled by individuals, groups, and business organizations. Security concerns with respect to data are broad, encompassing availability, secrecy, and integrity. In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or maliciously. The obvious concern with secrecy is the unauthorized reading of data files or databases, and this area has been the subject of perhaps

more research and effort than any other area of computer security. A less obvious threat to secrecy involves the analysis of data and manifests itself in the use of so-called statistical databases, which provide summary or aggregate information. Finally, data integrity is a major concern in most installations. Modifications to data files can have consequences ranging from minor to disastrous.

- **COMMUNICATION LINES AND NETWORKS:** Network security attacks can be classified as Passive Attack and Active Attack.
- **Passive Attacks**: Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are:
- **The release of message contents**: The message such as telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information and it may be easily understood, so the attacker may learn the content of this message. This is shown in Figure 2 below. We would like to prevent an opponent from learning the contents of these transmissions.

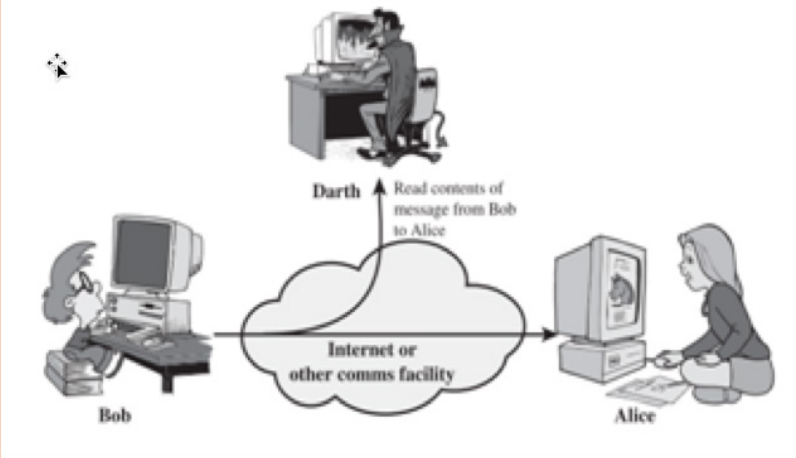

Figure 2.1: Showing the release of message contents attack

- Traffic analysis: Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent still might be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

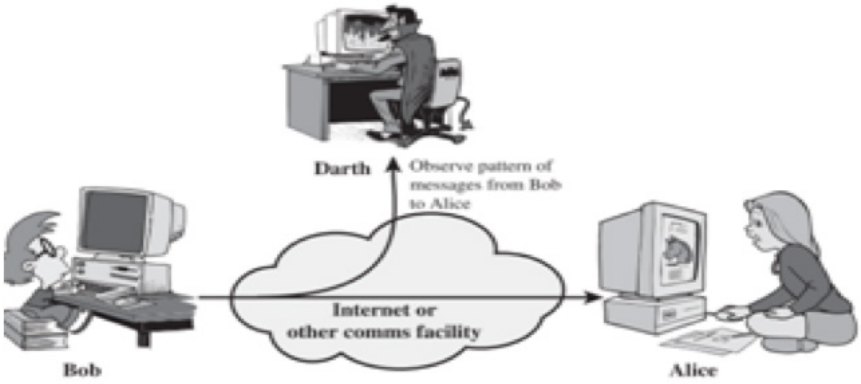

Figure 2.2 Showing Traffic analysis attack

Active Attack: Active attacks involve some modification of the data stream or the creation of a false stream. It consists four categories:

- **Masquerade:** A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.

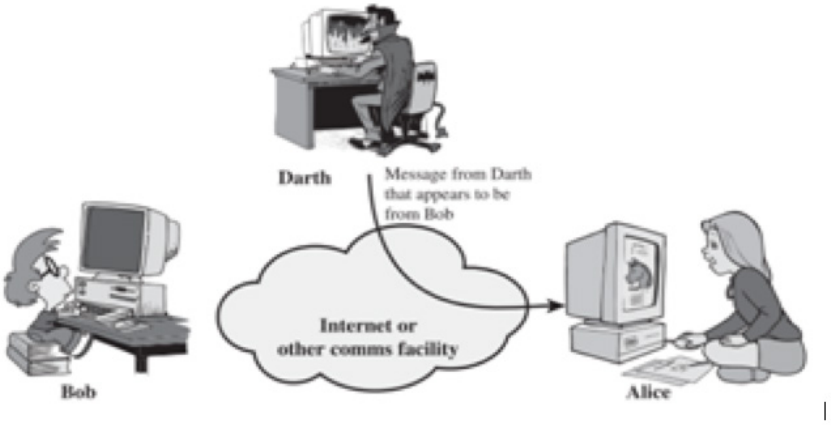

Figure 2.3: Showing Masquerade attack

- Replay: Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

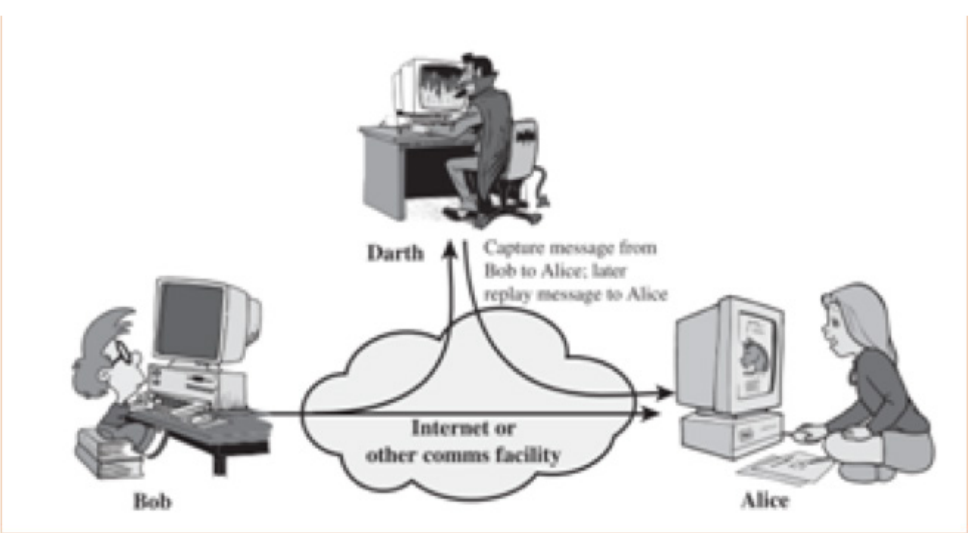

Figure 2.4: Showing Reply attack

- **Modification of messages:** Simply means that some portion of a legitimate message is altered , or that messages are delayed or reordered, to produce an unauthorized effect.

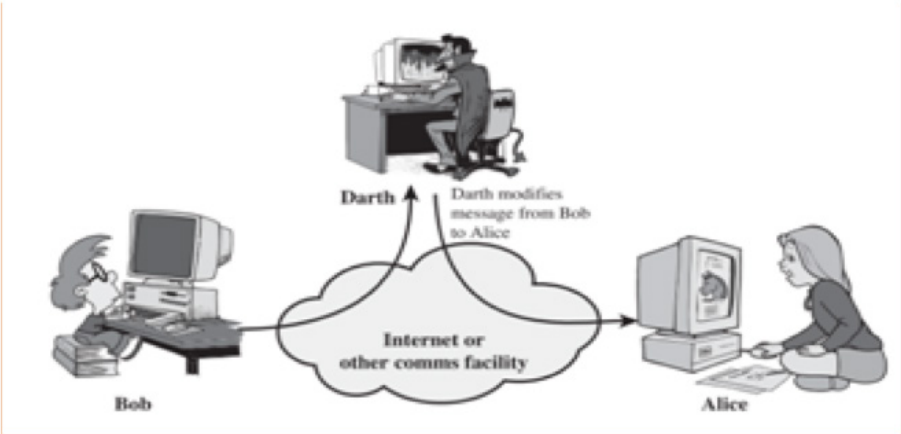

Figure 2.5:: Showing modification of messages attack

- Denial of service: Prevents or inhibits the normal use or management of communications facilities.

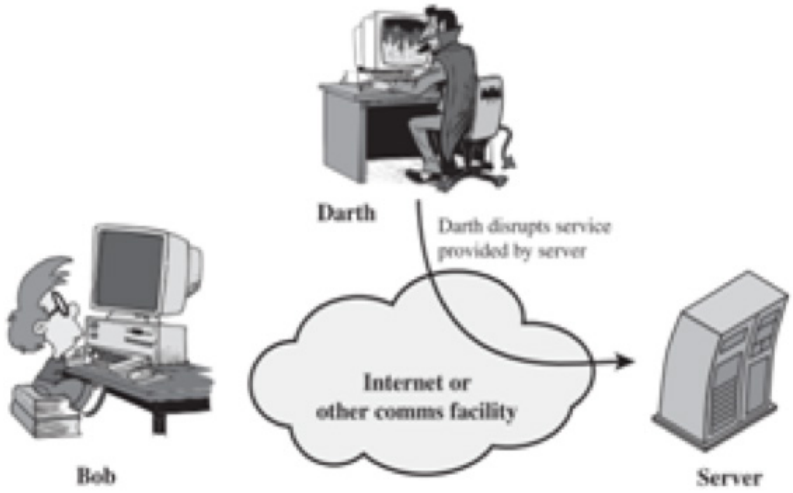

Figure 2.6: Showing Denial of service attack

Conclusion

This activity explained the relationship between threats and computer assets. It also provided a briefly description on how computer resources are related to the concepts of the three components of the CIA trend.

Assessment

1. Briefly describe two types of attacks
2. Explain how computer attacks can affect different categories of computer resources

Activity 2.3 - Vulnerabilities

Introduction

In this activity, computer security vulnerabilities will be discussed, but to be able to Cleary talk about computer security vulnerabilities, this activity also re-visits computer security threats where they are classified into different categories.

Activity Details

Computer Security Vulnerabilities:

Computer security vulnerabilities include; Technology weakness: This involves weaknesses in protocols or computer systems (e.g. operating system (OS) vulnerabilities). Configuration weakness: This also involves insecure default configuration, e.g having open ports in your network, and weak user accounts and passwords, etc. Security Policy weakness, where you allow insecure passwords and do not log any events in your system, in other words, lack of acceptable User security Policy, or education of users.

Classification of threats

There are four general categories of security threats:

Unstructured threats: Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company. For example, if an external company website is hacked, the integrity of the company is damaged. Even if the external website is separate from the internal information that sits behind a protective firewall, the public does not know that. All the public knows is that the site is not a safe environment to conduct business.

Structured threats : Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

External threats: External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.

Internal threats: Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. According to the FBI, internal access and misuse account for 60 percent to 80 percent of reported incidents.

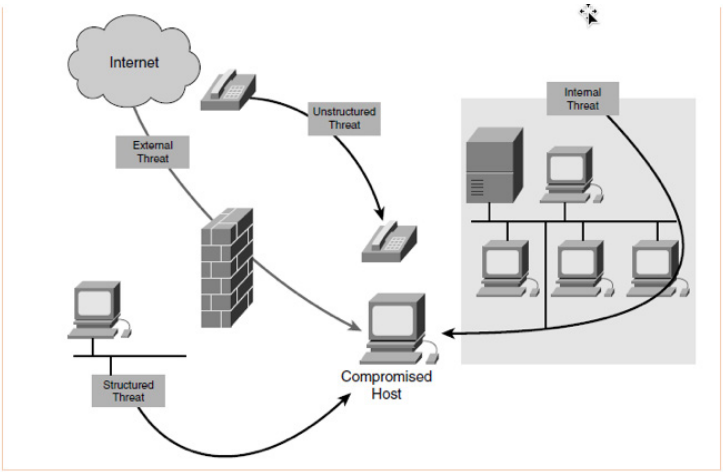

Figure 2.7 showing different Categories of Threats

Conclusion

This activity introduced different computer security vulnerabilities. This activity also re-visits computer security threats where they are classified into different categories.

Assessment

1. What are the main computer security vulnerabilities
2. Explain different classes of security threats

Unit Summary

This unit covered;

- Threats and Types of attacks
- Threats and Assets
- Vulnerabilities and Threats

Unit Assessment

Check your understanding!

ASSESSMENT STRATEGY

Assessment on this unit is made both continuous and terminal. The continuous assessment

may have several components like problem solving, quizzes, assignments. The assessment strategy is aimed to test the

- Knowledge gained in understanding different computer threats and attacks
- Ability to understand the relationship between computer threats and computer assets
- Ability to understand computer security vulnerabilities
- The examination is used to assess the general knowledge of computer security model.

Assessment Criteria:

1. Briefly explain different threats and attacks on computer security
2. Briefly describe two types of attacks
3. Explain how computer attacks can affect different categories of computer resources
4. What are the main computer security vulnerabilities
5. Explain different classes of security threats.

Grading Scheme

Refer to the course assessment Table above

Activity 2.1: 8 marks

Activity 2.2: 10 Marks

Activity 2.3: 11 Marks

Feedback

Activity 2.1:

1. Briefly explain different threats and attacks on computer security (8 marks)

- Unauthorized disclosure (2 marks)
- This is a threat to one of the CIA trend component known as confidentiality. The following types of attacks can result in this threat consequence:
- **Exposure:** This can be intentional, where someone willingly provided sensitive information, such as credit card numbers, to unauthorized person. It can also be the result of a human, hardware, or software error, which results in an entity gaining unauthorized knowledge of sensitive data. There have been numerous instances of this, such as universities accidentally posting student confidential information on the Web.
- **Interception:** This type of attack is a common in communications systems mainly on a shared local area network (LAN), such as a wireless LAN or a broadcast Ethernet. Devices attached to the LAN can receive a copy of packets intended for another device. On the Internet, a determined hacker can gain access to e-mail traffic and other data transfers. All of these situations create the potential for unauthorized access to data.

- **Inference:** Traffic analysis is the main type of interference attack. It involves gaining information from observing the pattern of traffic on a network, such as the amount of traffic between particular communication devices on the network.
- **Intrusion:** This involves an attacker gaining unauthorized access to sensitive data by bypassing the system's access control protections.
- **Deception (2 marks)**

This is a threat to one of the CIA trend component known as integrity. The following types of attacks can result in this threat consequence:

- **Masquerade:** Masquerade involves an attempt by an unauthorized user to gain access to a system by posing as an authorized user. This is possible if the unauthorized user gains access to another user's logon ID and password. It can also happen if malicious software, like a Trojan horse, that appears to perform a useful or desirable function but actually gains unauthorized access to system resources or tricks a user into executing other malicious acts.
- **Falsification**: This is the ability to change or replace a valid data or put false data into a file or database. For example, a student may alter his or her grades on a school database.
- **Repudiation:** In this case, a user either denies sending data or a user denies receiving or possessing the data.
- **Disruption (2 marks)**

This is a threat to two of the CIA trend components known as availability and Integrity.

The following types of attacks can result in this threat consequence:

- **Incapacitation:** This is an attack on system availability. This can happen as a result of physical destruction of or damage to system hardware. Most notably , malicious software, like Trojan horses, viruses, or worms, could work in a way to disable a system or some of its services.
- **Corruption:** This is an attack on system integrity. Malicious software in this context could operate in such a way that system resources or services function in an unintended manner. Or a user could gain unauthorized access to a system and modify some of its functions.
- **Obstruction:** This type of attack involves obstructing the system operation in such way that you can be able to interfere with communications by disabling communication links or altering communication control information. It also involves overloading the system by placing excess burden on communication traffic or processing resources. (
- **Usurpation (2 marks)**

This is a threat to one of the CIA trend components known as integrity. The following types of attacks can result in this threat consequence:

- **Misappropriation:** This involves theft of service. An example is a distributed denial of service attack, when malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host. In this case, the malicious software makes unauthorized use of processor and operating system resources.
- **Misuse:** Misuse can occur by means of either malicious logic or a hacker that has gained unauthorized access to a system. In either case, security functions can be disabled or thwarted.

Activity 2.2:

1. Briefly describe two types of attacks (2 marks)

- **Passive Attacks:** Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted. (1 mark)
- **Active Attack:** Active attacks involve some modification of the data stream or the creation of a false stream (1 mark)

2. Explain how computer attacks can affect different categories of computer resources (8 marks)

- **HARDWARE:** The main threat to computer system hardware is the threat to one of the CIA trend component called availability. The hardware component of a computer system is the most vulnerable to attack and the least susceptible to automated controls. Threats can be of different kinds such as accidental and deliberate damage to different devices as well as their theft. The production of personal computers and workstations and the widespread use of LANs increase the potential for losses in this area. Theft of memory devices such as CD-ROMs and DVDs can lead to loss of confidentiality as that's where sensitive information is mostly kept. Physical and administrative security measures are needed to deal with these threats. (2 marks)
- **SOFTWARE:** Again the main threat to computer system software is an attack on CIA trend component called availability. Software, especially application software, can easily be deleted, changed or damaged which tends to make it useless. Careful software configuration management, which includes making backups of the most recent version of software, can maintain high availability. (2 marks)
- **DATA and USERS:** Security of the two computer system components discussed earlier (hardware and software) are a concerns of computing center professionals or individual concerns of personal computer users. The main problem is data security, which involves files and other forms of data controlled by individuals, groups, and business organizations. Security concerns with respect to data are broad, encompassing availability, secrecy, and integrity. In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or maliciously. The obvious concern with secrecy is the unauthorized reading of data files or databases, and this area has been the subject of perhaps more research and effort than any other area of computer security. A less obvious threat to secrecy involves the analysis of data and manifests itself in the use of

so-called statistical databases, which provide summary or aggregate information. Finally, data integrity is a major concern in most installations. Modifications to data files can have consequences ranging from minor to disastrous. (2 marks)

- **COMMUNICATION LINES AND NETWORKS**: this can be attacked by either Passive Attack or Active Attack. (2 marks)

Activity 2.3

1. What are the main computer security vulnerabilities (3 marks)

Computer security vulnerabilities include;

- **Technology weakness:** This involves weaknesses in protocols or computer systems (e.g. operating system (OS) vulnerabilities).
- **Configuration weakness:** This also involves insecure default configuration, e.g having open ports in your network, and weak user accounts and passwords, etc.
- **Security Policy weakness**, where you allow insecure passwords and do not log any events in your system, in other words, lack of acceptable User security Policy, or education of users.

2. Explain different classes of security threats (8 marks)

- **Unstructured threats:** Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company. For example, if an external company website is hacked, the integrity of the company is damaged. Even if the external website is separate from the internal information that sits behind a protective firewall, the public does not know that. All the public knows is that the site is not a safe environment to conduct business.
- **Structured threats :** Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.
- **External threats:** External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.
- **Internal threats:** Internal threats occur when someone has authorized access to the network
- with either an account on a server or physical access to the network. According to the
- FBI, internal access and misuse account for 60 percent to 80 percent of reported incidents

Unit Readings and Other Resources

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2
- William Stallings "Cryptography and Network Security: Principles and Practice," 4th Ed, 2011
- William Stallings "Network Security Essentials:Applications And Standards" Fourth Edition , 2011

Unit 3. Software security and Prevention Mechanism

Unit Introduction

This unit focuses on different malicious software and their mitigation methods. Security auditing, and the event monitoring prevention mechanism will also be discussed. Security auditing is one of the prevention mechanism while monitoring is a tool still little known but essential in the implementation of a security policy.

Unit Objectives

Upon completion of this unit you should be able to:

- identify different malicious software
- Describe ways of mitigating these malwares
- Describe different security auditing mechanisms
- Identify different event monitoring prevention mechanism

Key Terms

Malicious software: Malicious software is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services

Viruses : The first category of malware propagation concerns parasitic software fragments called a virus that attach themselves to some existing executable content

A worm is a program that actively seeks out more machines to infect, and then each infected machine serves as an automated launching pad for attacks on other machine

Learning Activities

Activity 3.1 - Types of Malicious Software (Malware)

Introduction

In this activity, different types of malicious software (Malware) will be discussed. Malicious software is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services. They can also allow sensitive information to be copied or echoed to other systems.

Types of Malicious Software (Malware)

Viruses

- The first category of malware propagation concerns parasitic software fragments called a virus that attach themselves to some existing executable content. A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation. End-user workstations are the primary targets of virus infection. Viruses are very sophisticated and often appear to be harmless correspondence. They may look like a personal communication, jokes, marketing promotions, etc. Most viruses require recipients to download attachments in order to spread. Some are designed to launch automatically, with no user action required. An example of a virus is a program that is attached to command.com (the primary interpreter for Windows systems) that deletes certain files and infects any other versions of command.com that it can find

Parts of a Computer Virus:

Computer virus has three parts.

1. **Infection mechanism** : The means by which a virus spreads or propagates, enabling it to replicate. The mechanism is also referred to as the infection vector .
2. **Trigger:** The event or condition that determines when the payload is activated or delivered, sometimes known as a logic bomb.
3. **Payload:** What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.

Four Phases of a Computer Virus:

During its lifetime, a typical virus goes through the following four phases:

- Dormant phase: The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.
- Propagation phase: The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often morph to evade detection. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- Triggering phase: The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.
- Execution phase: The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Virus Attack Mitigation

These kinds of applications can be contained through the effective use of antivirus software at the user level and potentially at the network level. Antivirus software can detect most viruses and prevent them from spreading in the network. Keeping current with the latest developments in these sorts of attacks can also lead to a more effective posture against these attacks. As new virus are released, enterprises need to keep current with the latest antivirus software and application versions.

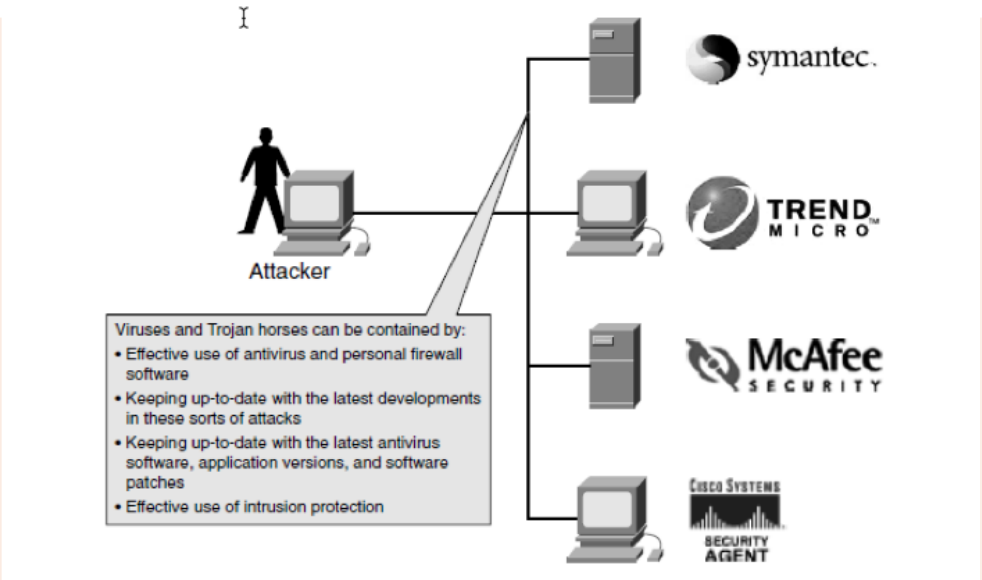

Figure 3.1 Showing Virus and Trojan horse Mitigation

Worms

A worm is a program that actively seeks out more machines to infect, and then each infected machine serves as an automated launching pad for attacks on other machines. It is An application that executes arbitrary code and installs copies of itself in the memory of the infected computer, which then infects other hosts.

The structure of a worm attack is as follows:

1. The enabling vulnerability—A worm installs itself using an exploit vector on a vulnerable system.
2. Propagation mechanism—After gaining access to devices, a worm replicates and selects new targets.
3. Payload—After the device is infected with a worm, the attacker has access to the host—often as a privileged user. Attackers could use a local exploit to escalate their privilege level to administrator.

Typically, worms are self-contained programs that attack a system and try to exploit a specific vulnerability in the target. Upon successful exploitation of the vulnerability, the worm copies its program from the attacking host to the newly exploited system to begin the cycle again. A virus normally requires a vector to carry the virus code from one system to another. The vector

can be a word processing document, an e-mail message, or an executable program. The key element that distinguishes a computer worm from a computer virus is that human interaction is required to facilitate the spread of a virus.

Worm Attack Mitigation

Worm attack mitigation, requires carefulness on the part of system and network administration staff. Coordination between system administrations, network engineering, and security operations personnel is critical in responding effectively to a worm incident.

The following are the recommended steps for worm attack mitigation:

Step 1. Containment

Step 2. Inoculation

Step 3. Quarantine

Step 4. Treatment

These are all shown in the figure below:

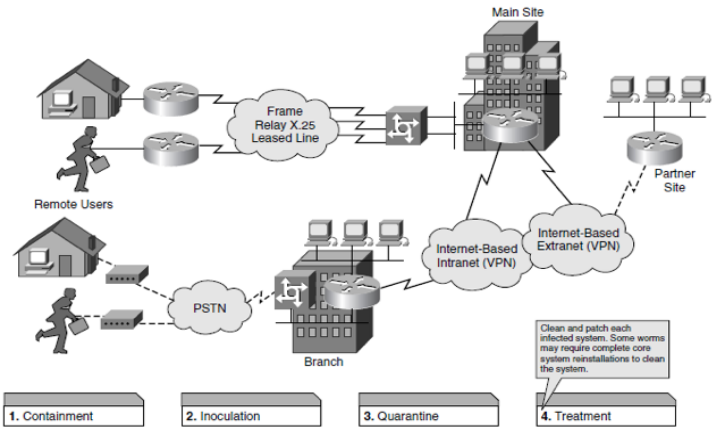

Figure 3.2 Showing Worm Attack Mitigation

E-mail spam, Trojans

The final category of malware propagation we consider involves social engineering, "tricking" users to assist in the compromise of their own systems or personal information. This can occur when a user views and responds to some SPAM e-mail, or permits the installation and execution of some Trojan horse program or scripting code.

*A **Trojan horse*** An application written to look like something else that in fact is an attack Tool. It is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. The other users receive the game and then play it, thus spreading the Trojan horse

E-mail Spam: A large proportion of all corporate email is spam. Spam costs US business billions of dollars in lost productivity and system slow-downs annually. Most spam is annoying and slows down the network. Hackers may sometimes disguise viruses, spyware, and malware as innocent-looking spam

A ***Trojan horse*** is mitigated by antivirus software at the user level and possibly the network level. There has been also the equally rapid growth of the anti-spam industry that provides products to detect and filter spam e-mails. Email security packages usually contain spam filters that: Identify non-relevant communications, Use key words and phrases, May also use format, size, or ratio of graphics to text, Spam is moved to a separate folder or deleted from email server, May also block email addresses that are known to have sent spam, preventing further disruptive emails

Conclusion

This activity explained in details different types of malicious software (Malware). This malicious software categorized based on their operations. This activity also gave different methods of mitigating these malware.

Assessment

Briefly describe different types of malicious software, you should also provide different methods of mitigating them

Activity 3.2 - SYSTEM CORRUPTION & INFORMATION THEFT

Introduction

In this activity, key loggers, phishing, spyware will be discussed

Activity Details

Computer System corruption

Once your system is effected by a malware, the next concern is what actions it will take on that system. That is, what payload does it carry? Some malware carry payloads which are not harmful. Its only purpose, either deliberate or due to accidental early release, is why it was spread. Other common malwares are harmful, they carry payloads that perform covert actions for the attacker. Some can result into data destruction on the infected system. Others can displays unwanted messages or content on the users system. More seriously, some attempts to inflict real-world damage on the system. All of these actions target the integrity of the computer systems software or hardware, or of the user's data. These changes may not occur immediately, but only when specific trigger conditions are met that satisfy their logic-bomb code

Information theft (KEYLOGGERS, PHISHING, SPYWARE)

We now consider payloads where the malware gathers data stored on the infected system for use by the attacker. A common target is the users login and password credentials to banking, gaming, and related sites, which the attacker then uses to impersonate the user to access these sites for gain. Less commonly, the payload may target documents or system configuration details for the purpose of reconnaissance or espionage. These attacks target the confidentiality of this information.

Keyloggers,

Typically, users send their login and password credentials to banking, gaming, and related sites over encrypted communication channels (e.g., HTTPS or POP3S), which protects them from capture by monitoring network packets. To bypass this, an attacker can install a keylogger , which captures keystrokes on the infected machine to allow an attacker to monitor this sensitive information. Since this would result in the attacker receiving a copy of all text entered on the compromised machine, keyloggers typical implement some form of filtering mechanism that only returns information close to desired keywords (e.g., "login" or "password" or "paypal.com"). In response to the use of keyloggers, some banking and other sites switched to using a graphical applet to enter critical information, such as passwords. Since these do not use text entered via the keyboard, traditional keyloggers do not capture this information.

Spyware:

In response graphical applet that the banks had introduced to mitigated keyloggers, attackers developed more general spyware payloads, which subvert the compromised machine to allow monitoring of a wide range of activity on the system. Spywares enables hackers to record activities and data from the infected computer. This is done via a program that dynamically gathers information and transmits it via an Internet connection. It is often bundled in with shareware and freeware programs and usually installs and runs without user knowledge

Spywares can be mitigated using firewalls and some e-mail security packages which will scan devices regularly for spyware programs and blocks known spyware programs before they can be downloaded and installed.

Phishing

Phishing is used for identity theft and fraud. Hackers pretend to send authorized emails from trustworthy institutions. Attempt to get recipients to surrender personal information such as bank account details. Most phishing attempts are aimed at individuals and some have targeted smaller businesses

Conclusion

This activity introduced key loggers, phishing, spyware, where computer system corruption was discussed as well as information theft

Assessment

1. Briefly explain how phishing techniques can be used to corrupt a computer system
2. Explain how a spyware can affect the integrity of your information

Activity 3 .3: Security auditing and event monitoring in a computer system

Introduction

In this activity, security auditing, and the event monitoring prevention mechanism will be discussed. Security auditing is one of the prevention mechanism while monitoring is a tool still little known but essential in the implementation of a security policy.

Security Auditing

The security audit is generally an activity to assess how a system behaves or operates against the standards established in the field. An audit is conducted by recognized authorities and has a certain reputation. An audit process in a company generally interviews proceeds by a group of employees or with tests on resources and respecting this well-recognized rules and standardized. Typically an security audit operation is done

- do a risk analysis
- measure the ability of a system to handle exceptions
- To monitor the implementation of the rules and procedures established within the company
- evaluating the performance of a system
- Analyze the damage caused by an attack, failure or simply a disaster.

Risk Analysis

Information systems as well as the networks are often subject to malicious attacks, configuration errors, environmental disasters or user error. Some systems may be more vulnerable than others because their configurations, nature or simply their role in the system. Nevertheless it is important to know what your information system or network is vulnerable and that means a security analysis. It must determine the risk of occurrence of such an attack and to classify these attacks more frequent and scarcer. It must also examine the vulnerability of each hardware or software component of the system taking into account its nature, its configuration and its role in the system. A safety analysis should also evaluate the measures taken to protect the computer system elements. At the end he/she must propose a risk management plan.

Evaluating the performance of a system

This activity is part of an audit to measure the ability of a company's resources and to evaluate the capacity actually used. It may then propose mechanisms to optimize the capacity to achieve the goals the company has set.

The monitoring and evaluation of the implementation of rules and procedures

In any business, there should be a manual of procedures defining the business operation. This is usually the IT department within a company that is developing a procedure manual regarding IT. And in this manual the safety aspect is not left out. During a security audit, the auditor will check if its operation the IT department following the procedures as set out in the procedures manual

Analysis of the damage

This activity is generally undertaken after the onset of an attack or disaster which losses within a company. It will assess the damage and impacts. It may also propose a recovery plan.

Evaluate a period of change or migration

When a company is in the process of migrating from one system to another, it can sponsor an audit operation that will evaluate new components operating status, see if they meet the specifications defined at the time of command. It may then propose improvements or simply to offer its total replacement. An audit process can be considered the launch of a system. It can also be performed in a given calendar. In case of attacks or failure of a system can also perform an emergency audit. To evaluate the security of a system during a security audit, we need to recognized and standardized tools. In the next section we will see both of these tools.

American Standard TCSEC

The US standard TCSEC (Trusted Computer Security Evaluation Criteria) was initiated by the DOD (Department Of Defense) of the United States. The latter set of safety rules involving a number of characteristics grouped in the Orange Book in December 1985 and in the Red Book in July 1987. These features allow determining the degree of protection of an operating system, with a total of 7 increasing levels of security the main criteria are:

- Data Privacy
- Data Integrity
- system availability

In ascending order, the next levels are defined:

- Level D: "minimal protection" for systems that could not meet higher-level class requirements.
- Level C1 / C2 "discretionary protection" where protections are left the users discretion. C2 is the maximum level for commercial organizations.
- Discretionary Access Control: defining and controlling access between users and objects to the granularity of a single user or user group.

- Accountability: identification and authentication of the user password protection and authentication data.
- Architecture Insurance: mechanisms that provide evidence that the security features are effectively and properly implemented and that the integrity of the foundation of trust is guaranteed.
- System Integrity: the elements must be provided to allow periodically validate the basis of trust.
- Tests and safety: the system security mechanisms must be tested and must operate in a manner consistent with what is stated in the documentation. Tests must be made to show that there are ways to circumvent the basis of trust.
- Documentation: user security guide, security administrator guide, test documents, specifications.
- Reuse of objects (for C2): trust-based guarantees that memory objects are cleaned before use. This means during the dynamic memory allocation, you cannot retrieve the data of the process that has just released this memory.
- Audit (C2): the system must allow the tracing of actions performed by all subjects on all objects. Its accuracy must enable tracing of all objects accessed by a user and including trace all operations of opening, reading, writing and erasing files.
- B1 / B2 / B3 "mandatory protection" and Level A "verified protection."
- These levels cover mainly military needs, or other sensitive areas such as air transport. Access to information (objects) is Not regulated by clearances subjects according the following 2 lines:
- A subject is authorized to read an object if its clearance level is higher than or equal to the classification of the object.
- A subject is allowed to write an object if its authorization level less than or equal to the classification of the object.

Products can be classified into one of these categories. However, it is important not to confuse: the classification of a product (which does not take into account its context of use) and certification (which takes into account the context of use). Note Windows NT is classified C2.

European standard ITSEC

The ITSEC (Information Technology Security Evaluation Criteria) puts together all machines / software as TOE. Security features are referred to as the security target. They include 8 topics

- Identification and Authentication
- Access control
- Accountability
- Audit
- Reusing items
- Loyalty
- Continuity of service
- Data Exchange

The first 5 topics are equivalent to those of the Orange Book of TCSEC.

The other 3 were added to overcome the shortcomings:

- Fidelity combines the functions of detection and loss prevention data alteration.

- Continuity of service combines the functions to ensure the making
- provision of timely resources.
- Data exchange defines the channel security features
- communications (encryption authentication data or all data).

Insurance levels are of 2 types:

- Assurance of compliance and accuracy (correctness) indicating whether the functionality of the security target is both properly specified and implemented.
- Insurance efficacy (effectiveness) indicating the confidence that can actually give the system during operation compared
  in compliance assurance which claims the TOE.

This dual approach leads to:

- 5 classes for general systems (F-C1, C2-F, F-B1, B2-F, F-B3)
- 5 classes for special systems (high integrity, high availability, ...)
- 8 categories correction E0 to E7

It is important to remember that a system can be classified at a level of security. But only the system administrator can certify the level of security used.

Conclusion

This activity explained the security auditing and event monitoring prevention mechanism and different approaches used to monitor different types of information

Assessment

1. Briefly explain how the security auditing prevention mechanism works
2. Briefly describe how the event monitoring prevention mechanism works

Unit Summary

This unit covered;

- different malicious software and their mitigation methods
- System corruption and Information theft
- Described different security auditing mechanisms

Unit Assessment

Check your understanding!

ASSESSMENT STRATEGY

Assessment on this unit is made both continuous and terminal. The continuous assessment may have several components like problem solving, quizzes, assignments. The assessment strategy is aimed to test the

- Ability to understand different malicious software Skills to mitigate these malwares
- Ability to describe different security auditing mechanisms
- For the assignment, criteria will be drawn up appropriate to the skills assessed , based on the AVU generic marking criteria

Assessment Criteria:

- For the examination setting and marking the AVU generic marking criteria will be used.
- For the assignment, criteria will be drawn up appropriate to the skills assessed , based

1. Briefly describe different types of malicious software, you should also provide different methods of mitigating them
2. Briefly explain how phishing techniques can be used to corrupt a computer system
3. Explain how a spyware can affect the integrity of your information
4. Briefly explain how the security auditing prevention mechanism worksBriefly describe how the event monitoring prevention mechanism works

Grading Scheme

Refer to the course assessment Table above

Activity 3.1 = 6 marks

Activity 3.2 = 6 marks

Activity 3.3 = 8 marks

Feedback

Activity 3.1:

1. Briefly describe different types of malicious software, you should also provide different methods of mitigating them (6 marks)

Viruses

- The first category of malware propagation concerns parasitic software fragments called a virus that attach themselves to some existing executable content. A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation. End-user workstations are the primary targets of virus infection. Viruses are very sophisticated and often appear to be harmless correspondence. They may look like a personal communication, jokes, marketing promotions, etc. Most viruses require recipients to download attachments in order to spread. Some are designed to launch automatically, with no user action required. An example of a virus is a program that is attached to command.com (the primary interpreter for Windows systems) that deletes certain files and infects any other versions of command.com that it can find
- Virus Attack Mitigation: These kinds of applications can be contained through the effective use of antivirus software at the user level and potentially at the network level. Antivirus software can detect most viruses and prevent them from spreading in the network. Keeping current with the latest developments in these sorts of attacks can also lead to a more effective posture against these attacks. As new virus are released, enterprises need to keep current with the latest antivirus software and application versions.

Worms

- A worm is a program that actively seeks out more machines to infect, and then each infected machine serves as an automated launching pad for attacks on other machines. It is An application that executes arbitrary code and installs copies of itself in the memory of the infected computer, which then infects other hosts.

- Worm Attack Mitigation: Worm attack mitigation, requires carefulness on the part of system and network administration staff. Coordination between system administrations, network engineering, and security operations personnel is critical in responding effectively to a worm incident.

E-mail spam, trojans

- The final category of malware propagation we consider involves social engineering, "tricking" users to assist in the compromise of their own systems or personal information. This can occur when a user views and responds to some SPAM e-mail, or permits the installation and execution of some Trojan horse program or scripting code.

A Trojan horse An application written to look like something else that in fact is an attack Tool. It is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. The other users receive the game and then play it, thus spreading the Trojan horse

E-mail Spam: A large proportion of all corporate email is spam. Spam costs US business billions of dollars in lost productivity and system slow-downs annually. Most spam is annoying and slows down the network. Hackers may sometimes disguise viruses, spyware, and malware as innocent-looking spam

E-mail spam, trojans Mitigation

A Trojan horse is mitigated by antivirus software at the user level and possibly the network level. There has been also the equally rapid growth of the anti-spam industry that provides products to detect and filter spam e-mails. Email security packages usually contain spam filters that: Identify non-relevant communications, Use key words and phrases, May also use format, size, or ratio of graphics to text, Spam is moved to a separate folder or deleted from email server, May also block email addresses that are known to have sent spam, preventing further disruptive emails

Activity 3.2:

1. Briefly explain how phishing techniques can be used to corrupt a computer system (3 marks)

   - Phishing is used for identity theft and fraud. Hackers pretend to send authorized emails from trustworthy institutions. Attempt to get recipients to surrender personal information such as bank account details. Most phishing attempts are aimed at individuals and some have targeted smaller businesses

2. Explain how a spyware can affect the integrity of your information (3 marks)

   - In response graphical applet that the banks had introduced to mitigated keyloggers, attackers developed more general spyware payloads, which subvert the compromised machine to allow monitoring of a wide range of activity on the system. Spywares enables hackers to record activities and data from the infected computer. This is done via a program that dynamically

gathers information and transmits it via an Internet connection. It is often bundled in with shareware and freeware programs and usually installs and runs without user knowledge. Spywares can be mitigated using firewalls and some e-mail security packages which will scan devices regularly for spyware programs and blocks known spyware programs before they can be downloaded and installed

Activity 3.3:

1. Briefly explain how the security auditing prevention mechanism works (4 marks)

   - The security audit is generally an activity to assess how a system behaves or operates against the standards established in the field. An audit is conducted by recognized authorities and has a certain reputation. An audit process in a company generally interviews proceeds by a group of employees or with tests on resources and respecting this well-recognized rules and standardized. Typically an security audit operation is done

   - do a risk analysis

   - measure the ability of a system to handle exceptions

   - To monitor the implementation of the rules and procedures established within the company

   - evaluating the performance of a system

   - Analyze the damage caused by an attack, failure or simply a disaster.

2. Briefly describe how the event monitoring prevention mechanism works (4 marks)

   - Monitoring is a tool still little known but essential in the implementation of a security policy. It not only helps to provide answers to the problems of availability but also when its technique is sufficiently advanced, it helps ensure the integrity of information. In addition, its low cost, ease of use and the level of information back make it a good tool in computer security. The computer monitor can be cut into three large families providing different Information levels :

   - The system monitoring: Positioned in the heart of the system, it will provide information on CPU usage, memory. . .

   - The network monitoring: This type of monitoring will be used to diagnose the availability of equipment physical connected to a network. The technologies used for this type of super vision are quite simple and the level of information returned is limited.

- Application monitoring: thanks to this monitoring, we will not have only visibility physical equipment but also the applications that are executed and the information they return.

In the latter two cases, it is obvious that the tests should be performed by equipment that are not on the machine, and the fact of making them from other sites makes sense if the server is intended for external users (eg web server connected to the Internet). Monitoring will provide in this context, a user can view the places from which it is performed

Unit Readings and Other Resources

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- Network Security 1 and 2 Companion Guide (Cisco Networking Academy) Published on Oct 5, 2006 by Cisco Press, ISBN-10: 1-58713-162-5 and ISBN-13: 978-1-58713-162-2

Unit 4. Properties of computer security

Unit Introduction

This unit introduces different authentication methods such as user authentication methods and access control. It also introduces some security infrastructures

Unit Objectives

Upon completion of this unit you should be able to:

- Apply different means of use authentication
- Describe different access control principles
- Describe the operation of access control mechanism
- Apply the safety bases and principles of operation of an intrusion detection system and firewalls

Key Terms

Authentication: User authentication is the first line of defense of a network. It aims to prevent unauthorized access to a network

Authorization: authorization focuses on determining what a user has permission to do

Nonrepudiation: This is defined as "assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data."

Firewall: A firewall is "checkpoint" central to all incoming and outgoing a system or network

IDS (Intrusion Detection System): Intrusion detection systems can detect intrusions in a computer system (an information system or network)

Learning Activities

Activity 4.1 - Authentication

Introduction

In this activity, different methods of user authentication will be discussed. Authorization and nonrepudiation will also be discussed in this activity

Activity Details

Authentication Overview

We are taking a network-based view of user authentication. User authentication is the first line of defence of a network. It aims to prevent unauthorized access to a network. It is the basis of setting access controls. It is used to provide user accountability.

Verifying User Identity

User authentication has two steps: Identification – presenting the user to the security system. Identification is the means by which a user claims to be a specific identity. Verification – providing information that binds the entity to the identity. Verification is the method used to prove that claim

Means of Authentication

There are different means of user authentication;

- Something the individual knows, E.g. password, PIN
- Something the individual possesses (tokens), E.g. cryptographic key, smartcard
- Something the individual is, E.g. fingerprint, retina
- Something the individual does, E.g. handwriting pattern, speech pattern

Password-Based authentication

Password-based authentication is the most common means of authentication. It requires no special hardware. Its typical authentication by password only, where the user supplies a username and password then the system looks up the username in the relevant database table, it checks that username, password pair exists and finally it provides system access to the user.

Attacks on Password-Based authentication

- Eavesdropping: Here the attacker can "listen" in and gain password information. Encrypting messages will prevent this
- Offline dictionary attack: A direct attack on the database storing passwords can be used to discover or change passwords. Normally strong access controls are applied to protect the databases storing password files. However, some hackers can bypass these control measures and access the password files. Prevention mechanisms include controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords should the password file be compromised.
- Specific account attack: The hacker can be determined to guess a password for a specific account until the correct password for that specific account is discovered. The best method to prevent this is by implementing the account lockout mechanism. This will disable the account after a number of failed login attempts.
- Popular password attack: The attacker will deploy different popular password to different user ID's. Normally users tend to use password which are easily

remembered, i.e., the name of your girlfriend/boyfriend, the capital city of your country, etc. So the hacker will guess these kind of passwords and apply them to different user IDs. This can be prevented by implementing policies to reduce the selection by users of common passwords and scanning the IP addresses of authentication requests and client cookies for submission patterns

- Workstation and session hijacking; the attacker can monitor when the workstation is not being used or a hacker can disconnect the session of the user and they connect themselves. The main prevention mechanism is to automatically logging the workstation out after a period of inactivity. Intrusion detection schemes can be used to detect changes in user behavior.
- Exploiting user mistakes: Some systems will provide passwords to the users. These kind of passwords are very difficult to remember, so users tend to write them somewhere. So this would make it easier for the hackers to read it. Prevention mechanisms include user training, intrusion detection, and simpler passwords combined with another authentication mechanism.
- Exploiting multiple password use: Some users use same password for different devices, so once the attacker gets to know the password, all the devices can be easily attacked. Never use the same password for different applications or devices

Password Strength

Users tend to pick weak passwords if allowed. These kinds of passwords can be easily to cracked via dictionary attack. Users should be forced to create more complex passwords. System can also supply users with a strong password however, with this method, many users will tend to write down a stronger password and this can be a greater security risk. One of the best methods of creating strong password is by using the Challenge – Response method. Here the systems are used that request specific characters in a password rather than the whole password. This is commonly used in online banking

Example Challenge-Response Method:

- The password is "MyPassword"
- The system asks for the 2nd, 3rd and 8th characters
- The user enters "y", "P" and "o"

The idea is that it would take an eavesdropper many sessions to determine the whole password

TOKEN-BASED AUTHENTICATION

Objects that a user possesses for the purpose of user authentication are called tokens. There are mainly two types of tokens that are widely used; these are cards that have the appearance and size of bank cards i.e. Memory card and smart card

Smartcards

These are tamper-resistant devices that have a small amount of memory and a small processor. They are difficult to duplicate and are easily transferable. They can use the combination of PIN/ password and have Simple computations, e.g. encryption/decryption, digital signatures.

Smartcard Examples

- Bank/ATM cards
- Credit cards
- Travel cards
- Pass cards for a workplace

Memory Cards

Memory cards have the capability to store data but cannot process it. The most common example of a memory card is the bank card which has a magnetic stripe on the back. This magnetic stripe at the back can store only a simple security code. These codes can be read and reprogrammed by an inexpensive card reader. Other kinds of memory cards include an internal electronic memory. Memory card can be used for physical access, such as a hotel room. Regarding computer user authentication, memory cards are used with some form of password or personal identification number (PIN). The best example is the automatic teller machine (ATM).

BOIMETRIC AUTHENTICATION

Biometric-based authentication is the Measurement of body's unique characteristics or behavior. These behaviors are of different types such as; Voice, Signature, Facial, Palm, Eye, Fingerprint etc. Compared to passwords and tokens, biometric authentication is both technically complex and expensive.

Physical Characteristics Used in Biometric Applications

The most common physical characteristics used in biometric based authentication are the following:

- **Facial Behaviors:** This is one of the most common means of human to human identifications. It is based on some key features such as relative location and shape of key facial characteristics, such as eyes, eyebrows, nose, lips, and chin shape.
- **Fingerprints:** . A fingerprint is the pattern of ridges and furrows on the surface of the fingertip. This approach has been around for a long time and is mostly used as means of identification for law enforcement purposes. This method is believed to be unique across the entire human population.
- **Hand geometry:** This method involves the hand geometry systems identify features of the hand, such as; shape, and lengths and widths of fingers.
- **Retinal pattern:** It is believed that the pattern formed by the veins beneath the

retinal surface is unique and therefore suitable for identification. The biometric system gets the digital image of the retinal by projecting a low-intensity beam of visual or infrared light into the eye.

- **Iris:** This is the detailed structure of the iris. It is also another unique feature that can be used for identification
- **Signature:** A signature is frequently written sequence. Every person has a different style of handwriting and this is reflected mainly in their signatures. So this method can also be used as means of identification.
- **Voice:** This is another means of identification where voice patterns are more closely tied to the physical and anatomical characteristics of the speaker.

Operation of a Biometric Authentication System

In order to be an authorized user, you must first be enrolled in the database system of authorized users. This is similar to assigning password to a specific user ID. With regards to the biometric system, the user gives the name and password or PIN to the system. At the same time, the system senses some biometric features for tis user i.e, Iris, Fingerprints, etc. All these inputs are digitized and the system extracts a set of characteristics that can be stored as a number or set of numbers representing this unique biometric characteristic; this set of numbers is referred to as the user's template. The user is now enrolled in the system, which maintains for the user a name (ID), perhaps a PIN or password, and the biometric value.

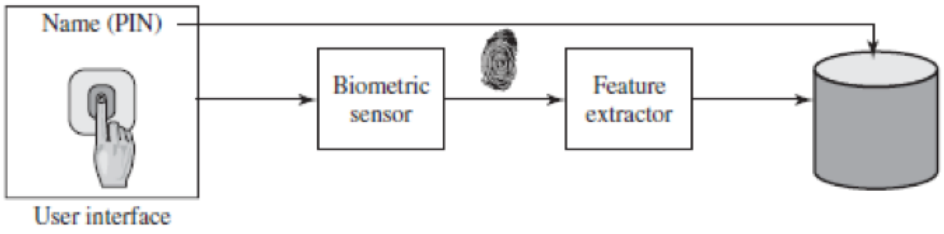

Figure 11: showing enrollement process

Depending on application, user authentication on a biometric system involves

Two methods:

- Verification: This method is similar to a user logging on to a system by using a memory card or smart card coupled with a password or PIN. For biometric verification, the user enters a PIN and also uses a biometric sensor. The system extracts the corresponding feature and compares that to the template stored for this user. If there is a match, then the system authenticates this user

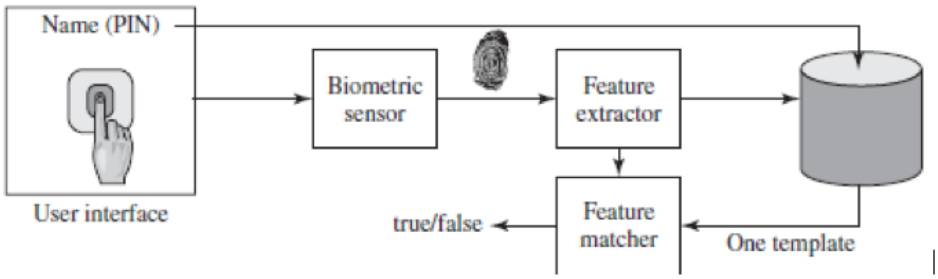

Figure 12: showing Verification process

- **Identification:** In this method, the user uses the biometric sensor with no any other additional information presented. The system then compares the presented template with the set of stored templates. If there is a match, then this user is identified. Otherwise, the user is rejected.

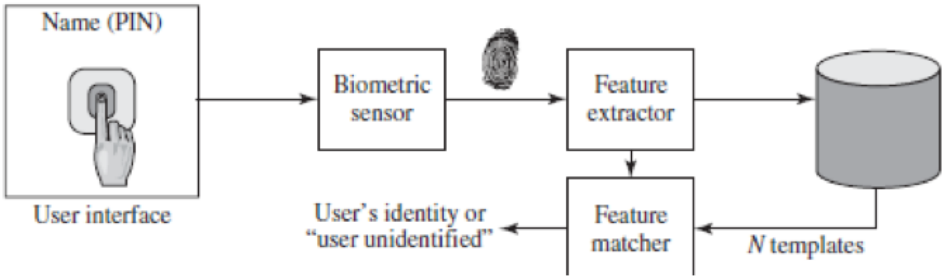

Figure 13: showing identification process

REMOTE-USER AUTHENTICATION

The form of authentication is where an individual tends to access the system which is locally present i.e. a stand-alone office PC or an ATM machine. This is one of the simplest forms of user authentication. The more complex case is when remote user authentication, happens over the Internet, a network, or a communications link. Remote user authentication raises additional security threats, such as an eavesdropper being able to capture a password, or an adversary replaying an authentication sequence that has been observed. To prevent these kinds of threats, the systems normally apply some form of challenge-response protocol

Authentication Problems

There are different user authentication problems;

- Guess or steal passwords, PIN, etc
- Forget passwords, PIN
- Steal or forge smartcards
- Lose smartcard
- False positives in biometrics
- False negatives in biometrics

- The most common method of network
- authentication uses passwords and cryptographic keys

Authorization

While authentication relates to verifying identities, authorization focuses on determining what a user has permission to do. It is defined as access privileges granted to a user, program, or process." E.g: an online banking application will authenticate a user based on his or her credentials, but it must then determine the accounts to which that user has access. Additionally, the system determines what actions the user can take regarding those accounts, such as viewing balances and making transfers

Nonrepudiation

This is defined as "assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data." E.g: Imagine a scenario wherein Alice is purchasing a car from Bob and signs a contract stating that she will pay $20,000 for the car and will take ownership of it on Thursday. If Alice later decides not to buy the car, she might claim that someone forged her signature and that she is not responsible for the contract. To refute her claim, Bob could show that a notary public verified Alice's identity and stamped the document to indicate this verification. In this case, the notary's stamp has given the contract the property of nonrepudiation. To meet this requirement, secure systems normally rely on asymmetric (or public key) cryptography. While symmetric key systems use a single key to encrypt and decrypt data, asymmetric systems use a key pair.

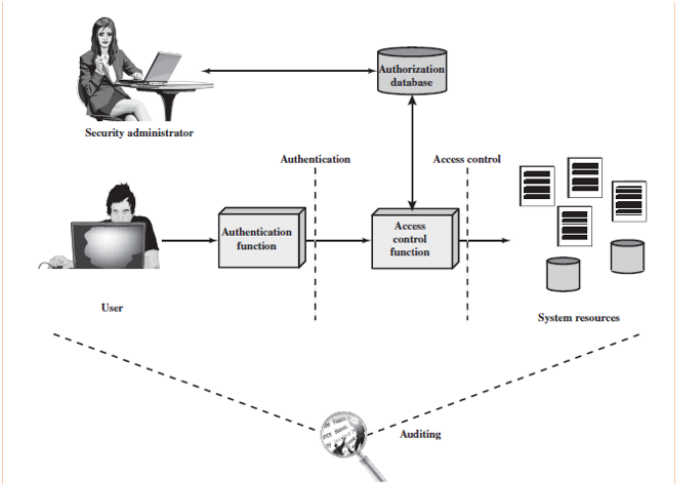

Figure 14: showing access control operation mechanism

Access Control Policies

The access control policy determines the type of access that is permitted and under which circumstances and by whom this access is permitted. This policy is sometimes embodied with in the authorization database. Access control policies can be divided into different categories;

Discretionary access control (DAC):

This category of access control policy is based on two main parts; the identity of the requesting party and the access rules (authorization) which include what the requesting party is allowed or not allowed to do. This policy was named discretionary simply because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.

Mandatory access control (MAC):

This policy is based on comparing two main items; security labels (these labels show how sensitive or critical the system resources are) and security clearance (this item shows which system entities that are qualified to access certain resources). This policy was named mandatory simply because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.

Role-based access control (RBAC):

This policy is also based on two things; the role that a user has within the system and the rules stating what accesses are allowed to users in given roles.

These three policies are not mutually exclusive and can be shown in figure below. An access control mechanism can employ two or even all three of these policies to cover different classes of system resources.

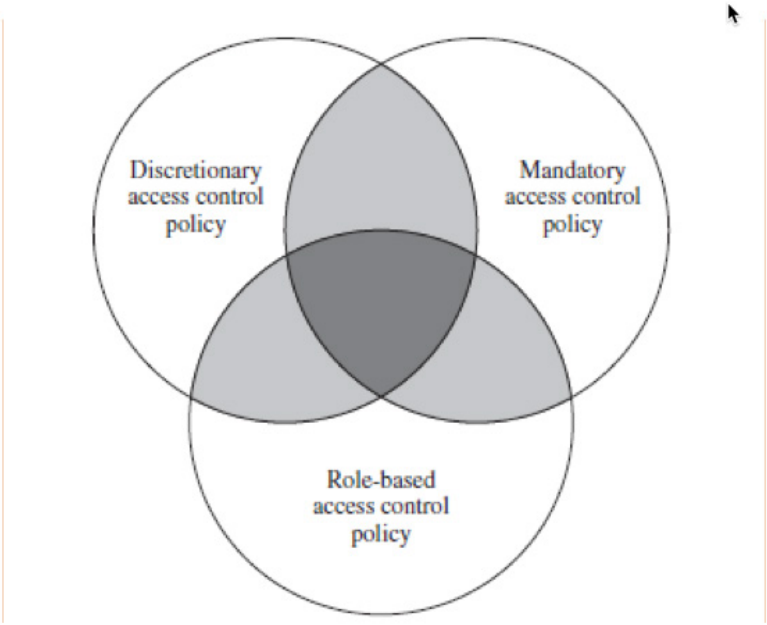

Figure 15: Showing three access control policies

Access Control Requirements

There are different concepts and features that are required for access control system

- **Reliable input:** Access control system requires inputs which are from reliable sources. For example this system assumes that a user is authentic so an authentication system is required as a front end to an access control system. Other inputs to the access control system must also be reliable. For example, some access control restrictions may depend on an address, such as a source IP address or medium access control address. The overall system must have a means of determining the validity of the source for such restrictions to operate effectively.
- **Support for fine and coarse specifications:** The access control system also requires fine grained specifications. This specification allows access to be regulated at the level of individual records in files, and individual fields within records. System administrators should also be able to choose coarse-grained specification for some classes of resource access, to reduce administrative and system processing burden
- **Least privilege:** This requirement involves the implementation of access control so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work.
- Separation of duty: This requirement involves dividing duties in a system function among different individuals. This prevents an individual from subverting the process.
- Open and closed policies: In a closed policy, only accesses that are specifically authorized are allowed. In an open policy, authorizations specify which accesses are prohibited; all other accesses are allowed.
- Policy combinations and conflict resolution: It is possible for the access control mechanism to apply multiple policies to a given class of resources. In those circumstances, one should take extreme care so that there are no conflicts such that one policy enables a particular access while another policy denies it. Or, if such a conflict exists, a procedure must be defined for conflict resolution.
- Administrative policies: Administrative policies are required to determine who can add, delete, or modify authorization rules.
- Dual control: When a task requires two or more individuals working in tandem.

Conclusion

This activity discussed different access control principles, requirements as well as access control policies

Assessment

1. Mention at least three access control requirements
2. Briefly describe three access control policies

Activity 4.3 - IDS

Introduction

In this activity, IDS will be discussed. Intrusion detection systems can detect intrusions in a computer system (an information system or network). It is important to note that absolute prevention is impossible. Nevertheless we is appropriate for the more an intrusion is detected, the less will be the damage.

The goals of an IDS are:

- The detection and the activation response mechanisms
- Recovery
- Prevention against future attacks

IDS assumes that the behavior of An attacker is different from that of a legitimate user. But in reality these behaviors can be indistinguishable. A legitimate user may have suspicious behavior or an attacker can disguise his behavior and impersonate a legitimate user.

Activity Details

Principle of operation of an IDS

Two approaches can be adopted in the implementation of an SDI. It will detect any abnormal behavior or function based on signatures. An IDS that detects abnormal behavior will monitor events and compares them to the so-called reference behavior. This is done in order to detect any deviation from normal behavior says. This normal behavior can be defined in a global manner or user. In a signature detection approach, the modes of action of known attacks are listed and detection is performed by comparisons with the signatures. Signature detection tries to characterize dangerous behavior and detect any of these behaviors when it occurs. The anomaly detection can detect unknown intrusion methods. Intrusion detection is not, however, necessarily greater than the detection signatures. The detection of anomalies conducts normal behavior by calibration, it can be ineffective if the system is calibrated so that the intruder is already there

Types of IDS

- Network based intrusion detection systems (NIDS):
- This type of IDS is positioned in strategic locations in the network. It monitors all traffic to and from network devices. In a perfect world all traffic would be monitored However, This would create a bottleneck in the network with a huge processing overhead hence It would deteriorate the network speed

Host based intrusion detection systems (HIDS):

This type if IDS operates on individual hosts or network devices. It monitors all inbound and outbound packets but only to and from the device it operates o. If suspicious activity is detected it usually alerts the user and/or network administrator of that activity

Signature-based IDS:

This types of IDS Monitors packets on the network. It Compare packets against a stored database of known malicious threats in a similar way the antivirus software operates. When a new threat appears there is a period of time before this is added to the database. Any new threat is undetected until such time as the database is updated to include this threat

Anomaly-based IDS:

This types of IDS Monitors network traffic. It Compares network traffic with a baseline. Baseline is "normal" traffic for that network:

Conclusion

This activity discussed the principle operation of IDS and the types of IDS

Assessment

1. Mention four types of IDS
2. Briefly explain the principle operation of an IDS

Activity 4.4 - Firewall

Introduction

In this activity, Firewall will be discussed. A firewall is "checkpoint" central to all incoming and outgoing a system or network. The goals of a firewall are :

- Control services: what service is accessible
- Control of behavior: comment service is it accessible
- Control User / Machine: Control access to services per user per machine
- However, a firewall does not provide protection against internal attacks. It is weaker against users who circumvent the firewall by connecting to the Internet and against the infected devices

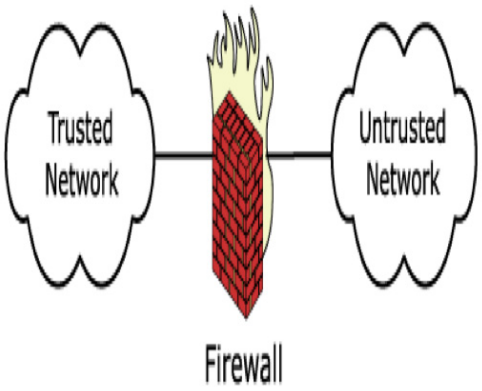

Figure 16: Showing Internet Firewall

Activity Details

How Does a Firewall Work?It Examines the traffic sent between two networks e.g. examines the traffic being sent between your network and the Internet. Data is examined to see if it appears legitimate: if so the data is allowed to pass through If not, the data is blocked. A firewall allows you to establish certain rules to determine what traffic should be allowed in or

out of your private network

Types of Firewall

1. **Software Firewall**

A software firewall protects only the computer on which they are installed. It provides excellent protection against threats (viruses, worms, etc.), it has a user-friendly interface and flexible configuration

2. **Router Firewall**

Router firewall protects your entire network or part of a network located on your router. It protects network hardware which cannot have a software firewall installed on it. It allows the creation of network-wide rules that govern all computers on the network

Firewall Operations

- Filtering principles
-

In the operation of a firewall there are two filtering principles.

- Positive filtering which passes only the traffic fulfilling criteria. Any undefined traffic will be dropped
- Negative filtering discards traffic meet certain criteria. Any undefined traffic will be accepted.
- Depending on the type of the analyzed flows can be distinguished packet filtering or application.
- Packet filtering
- A firewall can control traffic by analyzing packets entering or leaving. In this case the filter the bases may be : The filtering databases can be
- IP source or destination address
- Port numbers
- Network interface (eg, reject packet with internal IP address if coming from the wrong interface)

Such filtering has some disadvantages. Indeed it is difficult to configure a firewall while ant respects efficacy and safety. For example, some e protocol like FTP porting dynamic changes during the transfer. Configuration errors can be exploited. The fact that such a filtering There is no user identification , The firewall is no longer effective against attacks against TCP / IP protocols such as IP spoffing.

- **Filtering at the application level**

Such a firewall appears as a proxy for the users. Any connection involves two TCP connections. An internal machine to the proxy and the proxy outward. Insofar as such a filtering may proceed by a user authentication, it becomes more effective against attacks against the TCP / IP protocols. The firewall can be a network machine, separate router that provides Internet access. O n is referred to screened host firewall, firewall to wire water or bastion. This is the router that is actively making pass all the traffic from the Internet to the firewall machine. Conversely, it blocks all traffic for Internet that is issued by one of the machines other than the network firewall. The network's internal machines must know the firewall and send him all their traffic effectively for the Internet. A firewall is not a device for absolute safety. Its protection is effective if it is configured and if all communication with the outside passes through it (mobile workstations to the Internet are potential security holes). Indeed, it must be monitored very carefully the history of connections to detect intrusion attempts and change the firewall settings as new modes of attack have been reported in the issued security bulletins.

- **DMZ**

DMZ is used to make it accessible from outside a set of services: mail server, FTP server, web portal etc. The partitioning resulting from this choice implies a change in the network architecture. It should define for each area of the network, what are the allowed flow and flow allowed with the outside world.

Conclusion

This activity introduced the firewall and it's different types as well as it's operation

Assessment

1. What is a firewall?
2. List two types of a firewall
3. Briefly explain different operations of a firewall

Unit Summary

This unit covered;

- Different User authentication methods, Authorization and non repudiation
- Access control Principles
- Access control requirements
- Access control policies
- IDS
- Firewall

Unit Assessment

Check your understanding!

[ASSESSMENT STRATEGY]

Assessment on this unit is made both continuous and terminal. The continuous assessment may have several components like problem solving, quizzes, assignments. The assessment strategy is aimed to test the

- Ability to understand different means of user authentication
- Skills to control access to system and network
- Skills employ the safety bases and principles of operation of an intrusion detection system and firewalls

Assessment Criteria:

- For the examination setting and marking the AVU generic marking criteria will be used.
- For the assignment, criteria will be drawn up appropriate to the skills assessed , based on the AVU generic marking criteria

1. Briefly describe different methods of user authentication
2. Differentiate Authorization for nonrepudation
3. Explain how the Challenge-Response Method works
4. Mention at least three access control requirements
5. Briefly describe three access control policies
6. Mention four types of IDS
7. Briefly explain the principle operation of an IDS
8. What is a firewall?
9. List two types of a firewall
10. Briefly explain different operations of a firewall

Grading Scheme

Refer to the course assessment Table above

Activity 4.1 = 14 marks

Activity 4.2 = 9 marks

Activity 4.3 = 8 marks

Activity 4.4= 11 marks

Feedback

Activity 4.1:

1. Briefly describe different methods of user authentication (8 marks)

- **Password-Based authentication:** Password-based authentication is the most common means of authentication. It requires no special hardware. Its typical authentication by password only, where the user supplies a username and password then the system looks up the username in the relevant database table, it checks that username, password pair exists and finally it provides system access to the user.
- **Token-based authentication** :Objects that a user possesses for the purpose of user authentication are called tokens. There are mainly two types of tokens that are widely used; these are cards that have the appearance and size of bank cards i.e. Memory card and smart card
- **Boimetric authentication** :Biometric-based authentication is the Measurement of body's unique characteristics or behavior. These behaviors are of different types such as; Voice, Signature, Facial, Palm, Eye, Fingerprint etc. Compared to passwords and tokens, biometric authentication is both technically complex and expensive.
- **Remote-user authentication:** The form of authentication is where an individual tends to access the system which is locally present i.e. a stand-alone office PC or an ATM machine. This is one of the simplest forms of user authentication. The more complex case is when remote user authentication, happens over the Internet, a network, or a communications link. Remote user authentication raises additional security threats, such as an eavesdropper being able to capture a password, or an adversary replaying an authentication sequence that has been observed. To prevent these kinds of threats, the systems normally apply some form of challenge-response protocol

2. Differentiate Authorization for nonrepudation (4 marks)

- **Authorization** relates to verifying identities, authorization focuses on determining what a user has permission to do. It is defined as access privileges granted to a user, program, or process." E.g: an online banking application will authenticate a user based on his or her credentials, but it must then determine the accounts to which that user has access. Additionally, the system determines what actions the user can take regarding those accounts, such as viewing

balances and making transfers. While Nonrepudiation is defined as "assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data." E.g: Imagine a scenario wherein Alice is purchasing a car from Bob and signs a contract stating that she will pay $20,000 for the car and will take ownership of it on Thursday. If Alice later decides not to buy the car, she might claim that someone forged her signature and that she is not responsible for the contract. To refute her claim, Bob could show that a notary public verified Alice's identity and stamped the document to indicate this verification. In this case, the notary's stamp has given the contract the property of nonrepudiation. To meet this requirement, secure systems normally rely on asymmetric (or public key) cryptography. While symmetric key systems use a single key to encrypt and decrypt data, asymmetric systems use a key pair

3. Explain how the Challenge-Response Method works (2 marks)

In the Challenge – Response method, the systems requests specific characters in a password rather than the whole password. This is commonly used in online banking

Example Challenge-Response Method:

- The password is "MyPassword"
- The system asks for the 2nd, 3rd and 8th characters
- The user enters "y", "P" and "o"

Activity 4.2:

1. Mention at least three access control requirements (any of these) (3 marks)

- **Reliable input**: Access control system requires inputs which are from reliable sources. For example this system assumes that a user is authentic so an authentication system is required as a front end to an access control system. Other inputs to the access control system must also be reliable. For example, some access control restrictions may depend on an address, such as a source IP address or medium access control address. The overall system must have a means of determining the validity of the source for such restrictions to operate effectively.
- **Support for fine and coarse specifications:** The access control system also requires fine grained specifications. This specification allows access to be regulated at the level of individual records in files, and individual fields within records. System administrators should also be able to choose coarse-grained specification for some classes of resource access, to reduce administrative and system processing burden
- **Least privilege:** This requirement involves the implementation of access control so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work.
- **Separation of duty:** This requirement involves dividing duties in a system function among different individuals. This prevents an individual from subverting the process.

- **Open and closed policies:** In a closed policy, only accesses that are specifically authorized are allowed. In an open policy, authorizations specify which accesses are prohibited; all other accesses are allowed.
- **Policy combinations and conflict resolution**: It is possible for the access control mechanism to apply multiple policies to a given class of resources. In those circumstances, one should take extreme care so that there are no conflicts such that one policy enables a particular access while another policy denies it. Or, if such a conflict exists, a procedure must be defined for conflict resolution.
- **Administrative policies:** Administrative policies are required to determine who can add, delete, or modify authorization rules.
- **Dual control:** When a task requires two or more individuals working in tandem

2. Briefly describe three access control policies (6 marks)

Discretionary access control (DAC):

This category of access control policy is based on two main parts; the identity of the requesting party and the access rules (authorization) which include what the requesting party is allowed or not allowed to do. This policy was named discretionary simply because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.

Mandatory access control (MAC):

This policy is based on comparing two main items; security labels (these labels show how sensitive or critical the system resources are) and security clearance (this item shows which system entities that are qualified to access certain resources). This policy was named mandatory simply because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.

Role-based access control (RBAC):

This policy is also based on two things; the role that a user has within the system and the rules stating what accesses are allowed to users in given roles.

Activity 4.3:

3. Mention four types of IDS (4 marks)

- **Network based intrusion detection systems (NIDS):**

This type of IDS is positioned in strategic locations in the network. It monitors all traffic to and from network devices. In a perfect world all traffic would be monitored However, This would create a bottleneck in the network with a huge processing overhead hence It would deteriorate the network speed

Host based intrusion detection systems (HIDS):

This type if IDS operates on individual hosts or network devices. It monitors all inbound and outbound packets but only to and from the device it operates o. If suspicious activity is detected it usually alerts the user and/or network administrator of that activity

Signature-based IDS:

This types of IDS Monitors packets on the network. It Compare packets against a stored database of known malicious threats in a similar way the antivirus software operates. When a new threat appears there is a period of time before this is added to the database. Any new threat is undetected until such time as the database is updated to include this threat

Anomaly-based IDS:

This types of IDS Monitors network traffic. It Compares network traffic with a baseline. Baseline is "normal" traffic for that network:

2. Briefly explain the principle operation of an IDS (4 marks)

Two approaches can be adopted in the implementation of an SDI. It will detect any abnormal behavior or function based on signatures. An IDS that detects abnormal behavior will monitor events and compares them to the so-called reference behavior. This is done in order to detect any deviation from normal behavior says. This normal behavior can be defined in a global manner or user. In a signature detection approach, the modes of action of known attacks are listed and detection is performed by comparisons with the signatures. Signature detection tries to characterize dangerous behavior and detect any of these behaviors when it occurs. The anomaly detection can detect unknown intrusion methods. Intrusion detection is not, however, necessarily greater than the detection signatures. The detection of anomalies conducts normal behavior by calibration, it can be ineffective if the system is calibrated so that the intruder is already there

Activity 4.4:

1. What is a firewall? (1 mark)

   - A firewall is "checkpoint" central to all incoming and outgoing a system or network.

2. List two types of a firewall (2 marks)

   - Software firewall and router firewall

3. Briefly explain different operations of a firewall (8 marks)

   - Filtering principles

In the operation of a firewall there are two filtering principles.

- Positive filtering which passes only the traffic fulfilling criteria. Any undefined traffic will be dropped
- Negative filtering discards traffic meet certain criteria. Any undefined traffic will be accepted.

Depending on the type of the analyzed flows can be distinguished packet filtering or application.

- Packet filtering

A firewall can control traffic by analyzing packets entering or leaving. In this case the filter the bases may be : The filtering databases can be

- IP source or destination address
- Port numbers
- Network interface (eg, reject packet with internal IP address if coming from the wrong interface)

Such filtering has some disadvantages. Indeed it is difficult to configure a firewall while ant respects efficacy and safety. For example, some e protocol like FTP porting dynamic changes during the transfer. Configuration errors can be exploited. The fact that such a filtering There is no user identification , The firewall is no longer effective against attacks against TCP / IP protocols such as IP spooffing.

- Filtering at the application level

Such a firewall appears as a proxy for the users. Any connection involves two TCP connections. An internal machine to the proxy and the proxy outward. Insofar as such a filtering may proceed by a user authentication, it becomes more effective against attacks against the TCP / IP protocols.

Unit Readings and Other Resources

- William Stallings and Lawrie Brown ,"Computer Security Principles and Practices-second edition".2008
- William Stallings "Cryptography and Network Security: Principles and Practice," 4th Ed, 2011
- William Stallings "Network Security Essentials:Applications And Standards" Fourth Edition , 2011

Course Assessment

MINI TEST (Continuous assessment Test)/30

1. What is a passive attack?
2. Explain two types of passive attack
3. What is an active attack?
4. Explain four types of active attack
5. List 4 means of user authentication
6. Briefly explain the Attacks on Password-Based authentication
7. What are the two types of tokens that are used in Token-based authentication
8. List 5 physical characteristics used in biometric applications
9. List different problems faced in user authentication

Instructions

Attempt all questions

Grading Scheme

Mini Test /30 = 30%

Feedback

1. What is a passive attack? (1 mark)

   - Passive Attacks: Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted

2. Explain two types of passive attack (2 marks)

   - The release of message contents: The message such as telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information and it may be easily understood, so the attacker may learn the content of this message.

   - Traffic analysis: Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent still might be able to observe the pattern of

these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

3. What is an active attack? (1 mark)

- *Active Attack:* Active attacks involve some modification of the data stream or the creation of a false stream.

4. Explain four types of active attack (4 marks)

- *Masquerade:* A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.

- *Replay:* Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

- *Modification of messages:* Simply means that some portion of a legitimate message is altered , or that messages are delayed or reordered, to produce an unauthorized effect.

- *Denial of service:* Prevents or inhibits the normal use or management of communications facilities.

5. List 4 means of user authentication (4 marks)

- Something the individual knows, E.g. password, PIN

- Something the individual possesses (tokens), E.g. cryptographic key, smartcard

- Something the individual is, E.g. fingerprint, retina

- Something the individual does, E.g. handwriting pattern, speech pattern

6. Briefly explain the Attacks on Password-Based authentication (7 marks)

- *Eavesdropping:* Here the attacker can "listen" in and gain password information. Encrypting messages will prevent this

- *Offline dictionary attack:* A direct attack on the database storing passwords can be used to discover or change passwords. Normally strong access controls are applied to protect the databases storing password files. However, some hackers can bypass these control measures and access the password files. Prevention mechanisms include controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords should the password file be compromised

- *Specific account attack:* The hacker can be determined to guess a password for a specific account until the correct password for that specific account is discovered. The best method to prevent this is by implementing the account lockout mechanism. This will disable the account after a number of failed login attempts.

- *Popular password attack:* The attacker will deploy different popular password to different user ID's. Normally users tend to use password which are easily remembered, i.e., the name of your girlfriend/boyfriend, the capital city of your country, etc. So the hacker will guess these kind of passwords and apply them to different user IDs. This can be prevented by implementing policies to reduce the selection by users of common passwords and scanning the IP addresses of authentication requests and client cookies for submission patterns

- *Workstation and session hijacking*; the attacker can monitor when the workstation is not being used or a hacker can disconnect the session of the user and they connect themselves. The main prevention mechanism is to automatically logging the workstation out after a period of inactivity. Intrusion detection schemes can be used to detect changes in user behavior.

- *Exploiting user mistakes:* Some systems will provide passwords to the users. These kind of passwords are very difficult to remember, so users tend to write them somewhere. So this would make it easier for the hackers to read it. Prevention mechanisms include user training, intrusion detection, and simpler passwords combined with another authentication mechanism.

- *Exploiting multiple password use:* Some users use same password for different devices, so once the attacker gets to know the password, all the devices can be easily attacked. Never use the same password for different applications or devices

7. What are the two types of tokens that are used in Token-based authentication (2 marks)

- Memory card and smart card

8. List 5 physical characteristics used in biometric applications (5 marks)

- *Facial Behaviors:* This is one of the most common means of human to human identifications. It is based on some key features such as relative location and shape of key facial characteristics, such as eyes, eyebrows, nose, lips, and chin shape.

- *Fingerprints:* . A fingerprint is the pattern of ridges and furrows on the surface of the fingertip. This approach has been around for a long time and is mostly used as means of identification for law enforcement purposes. This method is believed to be unique across the entire human population.

- *Hand geometry:* This method involves the hand geometry systems identify features of the hand, such as; shape, and lengths and widths of fingers.

- *Retinal pattern:* It is believed that the pattern formed by the veins beneath the retinal surface is unique and therefore suitable for identification. The biometric system gets the digital image of the retinal by projecting a low-intensity beam of visual or infrared light into the eye.

- *ris:* This is the detailed structure of the iris. It is also another unique feature that can be used for identification

- *Signature:* A signature is frequently written sequence. Every person has a different style of handwriting and this is reflected mainly in their signatures. So this method can also be used as means of identification.

- *Voice:* This is another means of identification where voice patterns are more closely tied to the physical and anatomical characteristics of the speaker.

9. List different problems faced in user authentication (4 marks)

- Guess or steal passwords, PIN, etc

- Forget passwords, PIN

- Steal or forge smartcards

- Lose smartcard

- False positives in biometrics

- False negatives in biometrics

- The most common method of network

- authentication uses passwords and cryptographic keys

Final assessment: Exam/40

1. What is computer security (1 mark)
2. Provide three key security objectives (1 mark each)
3. What are the two most common cited Extra requirements of computer security? (1 mark each)
4. What is Cryptography? (1 mark)
5. What is PKI (1 mark)
6. How does PKI work? (2 marks)

7. What are the main uses of PKI? (4 marks)
8. Differentiate Symmetric encryption from asymmetric encryption (2 marks)
9. What are the main computer security vulnerabilities (3 marks)
10. Explain different classes of security threats (8 marks)
11. Briefly explain how phishing techniques can be used to corrupt a computer system (3 marks)
12. Explain how a spyware can affect the integrity of your information (3 marks)
13. Mention four types of IDS (4 marks)
14. List two types of a firewall (2 marks)
15. What is a firewall? (1 mark)

Instructions

Attempt all questions

Grading Scheme

Final assessment: Exam/40=40%

Feedback

1. What is computer security (1 mark)

   - Computer security can be defined as the ability to offer protection to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

2. Provide three key security objectives (1 mark each)

   - *Confidentiality:* preserving authorized restrictions on information access and disclosure.

   - *Integrity:* Guarding against improper information or destruction.

   - *Availability:* Ensuring timely and reliable access to and use of information

3. What are the two most common cited Extra requirements of computer security? (1 mark each)

   - *Authenticity:* Being genuine, verified and trusted. Confidence in the validity of a transmission, a message and a message originator. Verifying that users are how they say they are and that each message came from a trusted source

- *Accountability:* Actions of an entity can be traced uniquely to that entity. This Supports Fault isolation, Recovery , and Intrusion detection and prevention

4. What is Cryptography? (1 mark)

- It is a collection of mathematical techniques for protecting information.

5. What is PKI (1 mark)

- *Public Key Infrastructure* (PKI) is a security architecture that has been introduced to provide an increased level of confidence for exchanging information over the Internet.

6. How does PKI work? (2 marks)

- *PKI* uses a mathematical technique called public key cryptography. A pair of related cryptographic keys are used. It Verifies the identity of the sender (through signing)and ensures privacy (through encryption of data)

7. What are the main uses of PKI? (4 marks)

- To support secure information exchange over insecure networks. e.g. the Internet where such features cannot be provided easily

- For information exchange over private networks. e.g. an organisation's internal network

- To securely deliver cryptographic keys.

- To facilitate other cryptographically delivered security services

8. Differentiate Symmetric encryption from asymmetric encryption (2 marks)

-In *Symmetric encryption* (symmetric key encryption) the message is encrypt/ decrypt using the same key while in Asymmetric encryption (asymmetric key encryption), one key is used for encryption (public key), another key used for decryption (private key).

9. What are the main computer security vulnerabilities (3 marks)

Computer security vulnerabilities include;

- *Technology weakness:* This involves weaknesses in protocols or computer systems (e.g. operating system (OS) vulnerabilities).

- *Configuration weakness:* This also involves insecure default configuration, e.g having open ports in your network, and weak user accounts and passwords, etc.

- *Security Policy weakness*, where you allow insecure passwords and do not log any events in your system, in other words, lack of acceptable User security Policy, or education of users.

10. Explain different classes of security threats (8 marks)

-*Unstructured threats:* Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company. For example, if an external company website is hacked, the integrity of the company is damaged. Even if the external website is separate from the internal information that sits behind a protective firewall, the public does not know that. All the public knows is that the site is not a safe environment to conduct business.

- *Structured threats :* Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

- *External threats:* External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers. Internal threats: Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. According to the

FBI, internal access and misuse account for 60 percent to 80 percent of reported incidents

1. Briefly explain how phishing techniques can be used to corrupt a computer system (3 marks)

- *Phishing* is used for identity theft and fraud. Hackers pretend to send authorized emails from trustworthy institutions. Attempt to get recipients to surrender personal information such as bank account details. Most phishing attempts are aimed at individuals and some have targeted smaller businesses

2. Explain how a spyware can affect the integrity of your information (3 marks)

- In response graphical applet that the banks had introduced to mitigated keyloggers, attackers developed more general spyware payloads, which subvert the compromised machine to allow monitoring of a wide range of activity on the system. Spywares enables hackers to record activities and data from the infected computer. This is done via a program that dynamically gathers information and transmits it via an Internet connection. It is often bundled in with shareware and freeware programs and usually installs and runs without user knowledge. Spywares can be mitigated using firewalls and some e-mail security packages which will scan devices regularly for spyware programs and blocks known spyware programs before they can be downloaded and installed

3. Mention four types of IDS (4 marks)

Network based intrusion detection systems (NIDS):

- This type of IDS is positioned in strategic locations in the network. It monitors all traffic to and from network devices. In a perfect world all traffic would be monitored However, This would create a bottleneck in the network with a huge processing overhead hence It would deteriorate the network speed

Host based intrusion detection systems (HIDS):

- This type if IDS operates on individual hosts or network devices. It monitors all inbound and outbound packets but only to and from the device it operates o. If suspicious activity is detected it usually alerts the user and/or network administrator of that activity

Signature-based IDS:

- This types of IDS Monitors packets on the network. It Compare packets against a stored database of known malicious threats in a similar way the antivirus software operates. When a new threat appears there is a period of time before this is added to the database. Any new threat is undetected until such time as the database is updated to include this threat

Anomaly-based IDS:

- This types of IDS Monitors network traffic. It Compares network traffic with a baseline. Baseline is "normal" traffic for that network:

4. List two types of a firewall (2 marks)

   - Software firewall

   - router firewall

5. What is a firewall? (1 mark)

   - A *firewall* is "checkpoint" central to all incoming and outgoing a system or network.

Assignments

1. Assignment 1: Write a short report on how Security auditing prevention mechanism works
2. Assignment2: Write a short report on how event monitoring prevention mechanism works
3. Assignment:3 What are techniques used in computer system corruption and Information theft

Instructions

1. Attempt all Assignments
2. Each Assignment should be attempted separately

Grading Scheme

Assignment 1= 10%

Assignment 2= 10%

Assignment 3= 10%

Feedback

Assignment 1:

Security Auditing

The security audit is generally an activity to assess how a system behaves or operates against the standards established in the field. An audit is conducted by recognized authorities and has a certain reputation. An audit process in a company generally interviews proceeds by a group of employees or with tests on resources and respecting this well-recognized rules and standardized. Typically an security audit operation is done

- do a risk analysis
- measure the ability of a system to handle exceptions
- To monitor the implementation of the rules and procedures established within the company
- evaluating the performance of a system
- Analyze the damage caused by an attack, failure or simply a disaster.

Risk Analysis

Information systems as well as the networks are often subject to malicious attacks, configuration errors, environmental disasters or user error. Some systems may be more vulnerable than others because their configurations, nature or simply their role in the system. Nevertheless it is important to know what your information system or network is vulnerable and that means a security analysis. It must determine the risk of occurrence of such an attack and to classify these attacks more frequent and scarcer. It must also examine the vulnerability of each hardware or software component of the system taking into account its nature, its configuration and its role in the system. A safety analysis should also evaluate the measures taken to protect the computer system elements. At the end he/she must propose a risk management plan.

Evaluating the performance of a system

This activity is part of an audit to measure the ability of a company's resources and to evaluate the capacity actually used. It may then propose mechanisms to optimize the capacity to achieve the goals the company has set.

The monitoring and evaluation of the implementation of rules and procedures

In any business, there should be a manual of procedures defining the business operation. This is usually the IT department within a company that is developing a procedure manual regarding IT. And in this manual the safety aspect is not left out. During a security audit, the auditor will check if its operation the IT department following the procedures as set out in the procedures manual

Analysis of the damage

This activity is generally undertaken after the onset of an attack or disaster which losses within a company. It will assess the damage and impacts. It may also propose a recovery plan.

Evaluate a period of change or migration

When a company is in the process of migrating from one system to another, it can sponsor an audit operation that will evaluate new components operating status, see if they meet the specifications defined at the time of command. It may then propose improvements or simply to offer its total replacement. An audit process can be considered the launch of a system. It can also be performed in a given calendar. In case of attacks or failure of a system can also perform an emergency audit. To evaluate the security of a system during a security audit, we need to recognized and standardized tools. In the next section we will see both of these tools.

Assignment 2:

The event monitoring Prevention mechanism in a computer system

Introduction

Monitoring is a tool still little known but essential in the implementation of a security policy. It not only helps to provide answers to the problems of availability but also when its technique is sufficiently advanced, it helps ensure the integrity of information. In addition, its low cost, ease of use and the level of information back make it a good tool in computer security. The computer monitor can be cut into three large families providing different

Information levels :

- The system monitoring: Positioned in the heart of the system, it will provide information on CPU usage, memory. . .
- The network monitoring: This type of monitoring will be used to diagnose the availability of equipment physical connected to a network. The technologies used for this type of super vision are quite simple and the level of information returned is limited.
- Application monitoring: thanks to this monitoring, we will not have only visibility physical equipment but also the applications that are executed and the information they return.
- In the latter two cases, it is obvious that the tests should be performed by equipment that are not on the machine, and the fact of making them from other sites makes sense if the server is intended for external users (eg web server connected to the Internet). Monitoring will provide in this context, a user can view the places from which it is performed

The different approaches

In this section we will head in defining the approaches which are distinguished from each other by the type of information that can be provided by the monitoring.

- **Reliability:** This is by far the most common use of monitoring information technology. The goal here is to continuously monitor the availability of equipment and to detect the anomaly and if necessary give an alert.
- **Performance:** The performance monitoring aims to return information about the response time of a device such as the time of DNS resolution, the connection time, the first byte of the recovery time in the case of a Web page the page recovery time and all are elements of it (image, css, scripts...). Through this analysis, you will be able to diagnose
- a scalability or even over sizing of your bandwidth.
- **Content:** In this case, the information returned by the elements monitored are analyzed for example, to detect the removal of a File on a ftp server, the modification of a Web page or disappearance of a keyword.

All these approaches are complementary and can of course be found grouped together in u single analysis. The reliability analysis is implicitly present in the case of a Performance and Content analysis. To be efficient, monitoring should always be done from different control points on a distributed architecture, with techniques to analyze and continuously manage the flows. Whether with a reliability approach or Performance, monitoring is what it does best in terms of availability analysis. In effect, you can be able to continuously monitor and from as many places as you want the availability of your equipment. You get the vision from any place on the planet. It's like these people are distributed around the globe 24H / 24 and 7D 7 that will monitor your equipment and you will prevent any abnormality. If the warning system is sufficiently evolved, you may be alerted not only by mail or SMS, but also by fax or voice synthesis. Well of course, with hindsight you have access to all of the history and have a clear vision on the reliability of your IT investment. No system does is inviolable. The purpose of monitoring is to assess the risks and protect themselves accordingly with amenities such as s firewalls and other intrusion detection tools.

Assignment 1:

a. Phishing Technique:

Phishing is used for identity theft and fraud. Hackers pretend to send authorized emails from trustworthy institutions. Attempt to get recipients to surrender personal information such as bank account details. Most phishing attempts are aimed at individuals and some have targeted smaller businesses

b. Spyware Technique :

In response graphical applet that the banks had introduced to mitigated keyloggers, attackers developed more general spyware payloads, which subvert the compromised machine to allow monitoring of a wide range of activity on the system. Spywares enables hackers to record activities and data from the infected computer. This is done via a program that dynamically

gathers information and transmits it via an Internet connection. It is often bundled in with shareware and freeware programs and usually installs and runs without user knowledge. Spywares can be mitigated using firewalls and some e-mail security packages which will scan devices regularly for spyware programs and blocks known spyware programs before they can be downloaded and installed

Module Summary

Introduction to computer security module provided an essential study of computer security issues and methods in networked systems. It focused on all the processes and mechanisms by which computer based devices, information as well as services are protected from unauthorized users. It introduced the computer security concepts including key computer security objectives, challenges of computer security, and the model of computer security, different types Attacks, threats, vulnerabilities and Prevention Mechanisms in computer system was studied, security software and operations on how to secure a networked environment were introduced.

Labs:

Lab 1: Researching Network Attacks and Security

Audit Tools

Objectives

Part 1: Researching Network Attacks

- Research network attacks that have occurred.
- Select a network attack and develop a report for presentation to the class.

Part 2: Researching Security Audit Tools

- Research network security audit tools.
- Select a tool and develop a report for presentation to the class.

Background/Scenario

Network attacks have resulted in the loss of sensitive data and significant network downtime. When a network or the resources within it are inaccessible, worker productivity can suffer, and business income may be lost. Attackers have developed many tools over the years to attack and compromise the networks of organizations. These attacks take many forms, but in most cases, they seek to obtain sensitive information, destroy resources, or deny legitimate users

access to resources. To understand how to defend a network against attacks, an administrator must first identify network vulnerabilities. Specialized security audit software developed by equipment and software manufacturers can be used to help identify potential weaknesses. In addition, the same tools used by attackers can be used to test the ability of a network to mitigate an attack. After the vulnerabilities are known, steps can be taken to help mitigate the network attacks.

This lab provides a structured research project that is divided into two parts: Researching Network Attacks and Researching Security Audit Tools. You can elect to perform Part 1, Part 2, or both. Let your instructor know what you plan to do so to ensure that a variety of network attacks and vulnerability tools are reported on by the members of the class.

In Part 1, you research various network attacks that have actually occurred. You select one of these and describe how the attack was perpetrated and how extensive the network outage or damage was. You also investigate how the attack could have been mitigated or what mitigation techniques might have been implemented to prevent future attacks. You prepare a report based on a predefined form included in the lab.

In Part 2, you research network security audit tools and investigate one that can be used to identify host or network device vulnerabilities. You create a one-page summary of the tool based on a predefined form included in the lab.

You prepare a short (5–10 minute) presentation to present to the class. You may work in teams of two with one person reporting on the network attack and the other reporting on the security audit tools. All team members deliver a short overview of their findings. You can use live demonstrations or PowerPoint to summarize your findings.

Required Resources

- Computer with Internet access for research.
- Presentation computer with PowerPoint or other presentation software installed.
- Video projector and screen for demonstrations and presentations.

Part 1. Researching Network Attacks

In Part 1 of this lab, you research various network attacks that have actually occurred and select one on which to report. Fill in the form below based on your findings.

Step 1: Research various network attacks.

1. List some of the attacks you identified in your search.

Step 2: Fill in the following form for the network attack selected.

Name of attack:	
Type of attack:	
Dates of attacks:	
Computers / Organizations affected:	
How it works and what it did:	
Mitigation options:	
References and info links:	
Presentation support graphics (include PowerPoint filename or web links):	

Part 2. Researching Security Audit Tools

In Part 2 of this lab, you research network security audit tools and attacker tools and investigate one that can be used to identify host or network device vulnerabilities. Fill in the report below based on your findings.

Step 1: Research various security audit and network attack tools.

1. List some of the tools that you identified in your search

Step 2: Fill in the following form for the security audit or network attack tool selected

Name of tool:	
Developer	
Type of tool (character-based or GUI):	
Used on (network device or computer host):	
Cost:	
Description of key features and capabilities of product or tool:	
References and info links:	

Step 3: Reflection

a. What is the prevalence of network attacks and what is their impact on the operation of an

organization? What are some key steps organizations can take to help protect their networks and resources?

_____

_____

b. Have you actually worked for an organization or know of one where the network was compromised? If so, what was the impact to the organization and what did it do about it?

c. What steps can you take to protect your own PC or laptop computer?

Lab 2 Title: Security of Administrative Access using Authentication, Authorization, and Accounting (AAA)

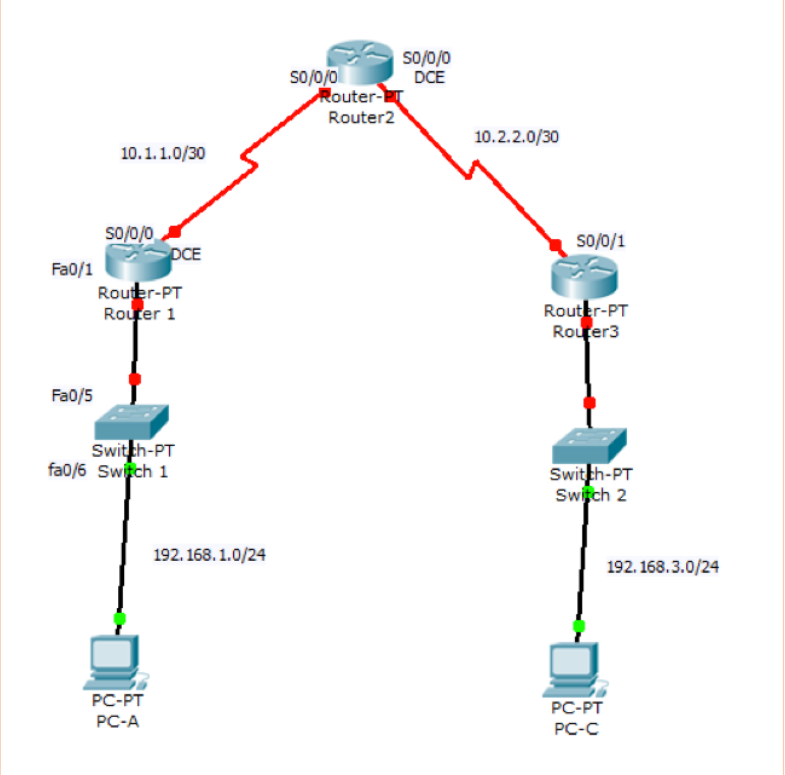

Fig:13: Lab 2Toplogy

Objectives

In the first part of this lab we will do some basic Network Device Configuration where we will :

- Configure basic settings such as host name, interface IP addresses, and access passwords.
- Configure static routing.
- In the second part of this lab, we will Configure Local Authentication where we will perfom the following actions;
- Configure a local database user and local access for the console, vty, and aux lines.
- Test the configuration.
- In the last part of this lab we will, Configure Local Authentication Using AAA where we will perform the following actions;
- Configure the local user database using Cisco IOS.
- Configure AAA local authentication using Cisco IOS.
- Configure AAA local authentication using CCP.
- Test the configuration.

Background

The most basic form of router access security is to create passwords for the console, vty, and aux lines. A user is prompted for only a password when accessing the router. Configuring a privileged EXEC mode enable secret password further improves security, but still only a basic password is required for each mode of access. In addition to basic passwords, specific usernames or accounts with varying privilege levels can be defined in the local router database that can apply to the router as a whole. When the console, vty, or aux lines are configured to refer to this local database, the user is prompted for a username and a password when using any of these lines to access the router.

Additional control over the login process can be achieved using authentication, authorization, and accounting (AAA). For basic authentication, AAA can be configured to access the local database for user logins, and fallback procedures can also be defined.

In this lab, you build a multi-router network and configure the routers and hosts. You will then use CLI commands configure routers with basic local authentication by means of AAA.

Required Resources

- 3 routers
- 2 switches
- PC-A: Windows XP, Vista or Windows 7
- PC-C: Windows XP, Vista or Windows 7
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

Activity 1: Basic Network Device Configuration

In this activity, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

All steps should be performed on routers R1 and R3. Only steps 1, 2, 3 and 6 need to be performed on R2. The procedure for R1 is shown here as an example

Step 1: Cable the network as shown in the topology. Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router. Configure host names as shown in the topology.

Configure the interface IP addresses as shown in the IP addressing table. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.

R1(config)# interface S0/0/0

R1(config-if)# clock rate 64000

To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.

R1(config)# no ip domain-lookup

Step 3: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

b. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the network topology

Step 5: Verify connectivity between devices by using ping command. If the pings are not successful, troubleshoot the basic device configurations before continuing

Step 6: Save the basic running configuration for each router.

Use the Transfer > Capture text option in HyperTerminal or some other method to capture the running

configs for each router. Save the three files so that they can be used to restore configs later in the lab.

Step 7: Configure and encrypt passwords on R1 and R3..

Here configure the same settings for R1 and R3. Let me show you configuration examples for R1

- On R1 configure a minimum password length. Use the security passwords command to set a minimum password length of 10 characters.

R1(config)# security passwords min-length 10

- On R1, Configure the enable secret password on both routers.

  R1(config)# enable secret cisco12345

- On R1, Configure the basic console, auxiliary port, and vty lines. Configure a console password and enable login for router R1. For additional security, the exec timeout command causes the line to log out after 5 minutes of inactivity. The logging synchronous command prevents console messages from interrupting command entry.

```
R1(config)# line console 0

R1(config-line)# password ciscoconpass

R1(config-line)# exec-timeout 5 0

R1(config-line)# login

R1(config-line)# logging synchronous

e. Configure a password for the aux port for router R1.

R1(config)# line aux 0

R1(config-line)# password ciscoauxpass

R1(config-line)# exec-timeout 5 0

R1(config-line)# login

f. Configure the password on the vty lines for router R1.

R1(config)# line vty 0 4

R1(config-line)# password ciscovtypass

R1(config-line)# exec-timeout 5 0

R1(config-line)# login

g. Encrypt the console, aux, and vty passwords.

R1(config)# service password-encryption
```

Step 8: Configure a login warning banner on routers R1 and R3.

- Here we configure a warning to unauthorized users using a message-of-the-day (MOTD) banner with the banner motd command so that when a user connects to the router, the MOTD banner appears before the login prompt.

R1(config)# banner motd $Unauthorized access strictly prohibited and prosecuted to the full extent of the law$

R1(config)# exit

Step 9: Save the basic configurations.

- ave the running configuration to the startup configuration from the privileged EXEC prompt.

R1# copy running-config startup-config

Activity 2: Configure Local Authentication

In this activity, you configure a local username and password and change the access for the console, aux, and vty lines to reference the router's local database for valid usernames and passwords. Perform all steps on R1 and R3. The configuration examples given are those performed on R1

Step 1: Configure the local user database.

Create a local user account with MD5 hashing to encrypt the password.

Step 2: Configure local authentication for the console line and login.

- Set the console line to use the locally defined login usernames and passwords.

R1(config)# line console 0

R1(config-line)# login local

Step 3: Set the vty lines to use the locally defined login accounts.

R1(config)# line vty 0 4

R1(config-line)# login local

- In order to add more security, set the aux port to use the locally defined login accounts.

R1(config)# line aux 0

R1(config-line)# login local

Step 4: Save the configuration on R1.

- Save the running configuration to the startup configuration from the privileged EXEC prompt.

R1# copy running-config startup-config

Step 5: Perform steps 1 through 4 on R3 and save the configuration.

Activity 3: Configure Local Authentication Using AAA on R3

In this activity, we are going to configure the Local User Database and also configure AAA Local Authentication

Step 1: Enable AAA services.

- On R3, enable services with the global configuration command aaa new-model. Because you are implementing local authentication, use local authentication as the first method, and no authentication

R3(config)# aaa new-model

Step 2: Implement AAA services for console access using the local database.

- Create the default login authentication list by issuing the aaa authentication login default method1[method2][method3] command with a method list using the local and none keywords.

R3(config)# aaa authentication login default local none

Step 3: Create a AAA authentication profile for Telnet using the local database.

- Create a unique authentication list for Telnet access to the router. This does not have the fallback of no authentication, so if there are no usernames in the local database, Telnet access is disabled. To create an authentication profile that is not the default, specify a list name of TELNET_LINES and apply it to the vty lines.

R3(config)# aaa authentication login TELNET_LINES local

R3(config)# line vty 0 4

R3(config-line)# login authentication TELNET_LINES

The African Virtual University Headquarters

Cape Office Park

Ring Road Kilimani

PO Box 25405-00603

Nairobi, Kenya

Tel: +254 20 25283333

contact@avu.org

oer@avu.org

The African Virtual University Regional Office in Dakar

Université Virtuelle Africaine

Bureau Régional de l'Afrique de l'Ouest

Sicap Liberté VI Extension

Villa No.8 VDN

B.P. 50609 Dakar, Sénégal

Tel: +221 338670324

bureauregional@avu.org