# CST901: ADVANCED COMPUTER AND NETWORK SECURITY

## AFRICA CENTRE OF EXCELLENCE ON TECHNOLOGY ENHANCED LEARNING (ACETEL)

## NATIONAL OPEN UNIVERSITY OF NIGERIA

# Course Guide for CST901

## Introduction

CST901 – Advanced Computer and Network Security is a 3-credit unit. The course is a core course in first semester. It will take you 15 weeks to complete the course. You are to spend 91 hours of study for a period of 13 weeks while the first week is for orientation and the last week is for end of semester examination. The credit earned in this course is part of the requirement for graduation.

You will receive the course material which you can read online or download and read off-line. The online course material is integrated in the Learning Management System (LMS). All activities in this course will be held in the LMS. All you need to know in this course is presented in the following sub-headings.

## Course Competencies

By the end of this course, you will gain competency in:

- Protecting Data at Rest and During Transmission
- Protecting System and Network Infrastructure
- Assessing Software Development Vulnerabilities

## Course Objectives

The course objectives are to:

- Explain the fundamentals concepts of computer security apply to different components of computing systems.
- Identify the basic cryptographic techniques using existing software in maintain information security.
- Describe how malicious attacks, threats, and protocols for security vulnerabilities impact a systems infrastructure.
- Explain and compare security mechanisms for conventional operating systems.
- Describe security requirements for database security

# Working Through this Course

The course is divided into modules and units. The modules are derived from the course competencies and objectives. The competencies will guide you on the skills you will gain at the end of this course. So, as you work through the course, reflect on the competencies to ensure mastery. The units are components of the modules. Each unit is sub-divided into introduction, intended learning outcome(s), main content, self-assessment exercise(s), conclusion, summary, and further readings. The introduction introduces you to the unit topic. The intended learning outcome(s) is the central point which help to measure your achievement or success in the course. Therefore, study the intended learning outcome(s) before going to the main content and at the end of the unit, revisit the intended learning outcome(s) to check if you have achieved the learning outcomes. Work through the unit again if you have not attained the stated learning outcomes.

The main content is the body of knowledge in the unit. Self-assessment exercises are embedded in the content which helps you to evaluate your mastery of the competencies. The conclusion gives you the takeaway while the summary is a brief of the knowledge presented in the unit. The final part is the further readings. This takes you to where you can read more on the knowledge or topic presented in the unit. The modules and units are presented as follows:

| **Module 1** | **Computer Security Technology and Principles** |
|---|---|
| Unit 1 | Security Fundamentals |
| Unit 2 | User Authentication |
| Unit 3 | Cryptographic Tools |
| Unit 4 | Access Control |
| Unit 5 | Malicious Software |
| Unit 6 | Database and Cloud Security |
| Unit 7 | Intrusion Detection |
| Unit 8 | Firewall and Intrusion Prevention Systems |

| **Module 2** | **Software Security and Trusted Systems** |
|---|---|
| Unit 1 | Software security |
| Unit 2 | Operating system security |

| **Module 3** | **Network Security** |
|---|---|
| Unit 1 | Internet security protocols and standards |
| Unit 2 | Wireless Network Security |
| Unit 3 | Cellular network security |

There are thirteen units in this course. Each unit represent a week of study.

# Presentation Schedule

The weekly activities are presented in Table 1 while the required hours of study and the activities are presented in Table 2. This will guide your study time. You may spend more time in completing each module or unit.

**Table I: Weekly Activities**

| **Week** | **Activity** |
|---|---|
| 1 | Orientation and course guide |
| 2 | Module 1 Unit 1 |
| 3 | Module 1 Unit 2 |
| 4 | Module 1 Unit 3 |
| 5 | Module 1 Unit 4 |
| 6 | Module 1 Unit 5 |
| 7 | Module 1 Unit 6 |
| 8 | Module 1 Unit 7 |
| 9 | Module 1 Unit 8 |
| 10 | Module 2 Units 1 and 2 |
| 11 | Module 3 Unit 1 |
| 12 | Module 3 Unit 2 |
| 13 | Module 3 Unit 3 |
| 14 | Revision and response to questionnaire |
| 15 | Examination |

The activities in Table I include facilitation hours (synchronous and asynchronous), assignments, mini projects, and laboratory practical. How do you know the hours to spend on each? A guide is presented in Table 2.

**Table 2: Required Minimum Hours of Study**

| **S/N** | **Activity** | **Hour per Week** | **Hour per Semester** |
|---|---|---|---|
| 1 | Synchronous Facilitation (Video Conferencing) | 2 | 26 |
| 2 | Asynchronous Facilitation (Read and respond to posts including facilitator’s comment, self-study) | 4 | 52 |
| 3 | Assignments, mini-project, laboratory practical and portfolios | 1 | 13 |
|  | Total | 7 | 91 |

# Assessment

Table 3 presents the mode you will be assessed.

**Table 3: Assessment**

| S/N | Method of Assessment | Score (%) |
|---|---|---|
| 1 | Portfolios | 10 |
| 2 | Mini Projects with presentation | 20 |
| 3 | Laboratory Practical | 20 |
| 4 | Assignments | 10 |
| 5 | Final Examination | 40 |
| Total | | 100 |

# Portfolio

A portfolio has been created for you tagged "**My Portfolio**". With the use of Microsoft Word, state the knowledge you gained in every Module and in not more than three sentences explain how you were able to apply the knowledge to solve problems or challenges in your context or how you intend to apply the knowledge. Use this Table format:

## Application of Knowledge Gained

| Module | Topic | Knowledge Gained | Application of Knowledge Gained |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

You may be required to present your portfolio to a constituted panel.

# Mini Projects with presentation

You are to work on the project according to specification. You may be required to defend your project. You will receive feedback on your project defence or after scoring. This project is different from your thesis.

# Laboratory Practical

The laboratory practical may be virtual or face-to-face or both depending on the nature of the activity. You will receive further guidance from your facilitator.

## Assignments

Take the assignment and click on the submission button to submit. The assignment will be scored, and you will receive a feedback.

## Examination

Finally, the examination will help to test the cognitive domain. The test items will be mostly application, and evaluation test items that will lead to creation of new knowledge/idea.

# How to get the Most from the Course

To get the most in this course, you:

- Need a personal laptop. The use of mobile phone only may not give you the desirable environment to work.
- Need regular and stable internet.
- Need to install the recommended software.
- Must work through the course step by step starting with the programme orientation.
- Must not plagiarise or impersonate. These are serious offences that could terminate your studentship. Plagiarism check will be used to run all your submissions.
- Must do all the assessments following given instructions.
- Must create time daily to attend to your study.

# Facilitation

There will be two forms of facilitation – synchronous and asynchronous. The synchronous will be held through video conferencing according to weekly schedule. During the synchronous facilitation:

- There will be two hours of online real time contact per week making a total of 26 hours for thirteen weeks of study time.
- At the end of each video conferencing, the video will be uploaded for view at your pace.
- You are to read the course material and do other assignments as may be given before video conferencing time.
- The facilitator will concentrate on main themes.

- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

For the asynchronous facilitation, your facilitator will:

- Present the theme for the week.
- Direct and summarise forum discussions.
- Coordinate activities in the platform.
- Score and grade activities when need be.
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures, and podcasts if need be.

Read all the comments and notes of your facilitator especially on your assignments, participate in forum discussions. This will give you opportunity to socialise with others in the course and build your skill for teamwork. You can raise any challenge encountered during your study. To gain the maximum benefit from course facilitation, prepare a list of questions before the synchronous session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help ACETEL to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

## Learner Support

You will receive the following support:

- Technical Support: There will be contact number(s), email address and chatbot on the Learning Management System where you can chat or send message to get assistance and guidance any time during the course.

- 24/7 communication: You can send personal mail to your facilitator and the centre at any time of the day. You will receive answer to you mails within 24 hours. There is also opportunity for personal or group chats at any time of the day with those that are online.

- You will receive guidance and feedback on your assessments, academic progress, and receive help to resolve challenges facing your stuides.

# Course Information

| | |
|---|---|
| Course Code: | CST 901 |
| Course Title: | Advanced Computer and Network Security |
| Credit Unit: | 3 |
| Course Status: | Compulsory |
| Course Description/Blurb: | This course is an advanced study of computer security which will cover threat and security policy models, authentication mechanisms, authorisation techniques, security models, trusted computing, network architecture security and security protocols, operating system security, database security, physical security, Internet security. |
| Academic Year: | 2020 |
| Semester: | First |
| Course Duration: | 13 weeks |
| Required Hours for Study: | 91 |

# Course Team

| | |
|---|---|
| Course Developer: | ACETEL |
| Course Writers: | Dr Shafi'i. M. Abdulhamid and Dr Morufu. Olalere, |
| Content Editor: | Dr Ismaila Idris |
| Instructional Designers: | Inegbedion, Juliet O. (PhD) and Dr.Lukuman Bello |
| Learning Technologists: | Dr Adewale Adesina and Mr Miracle David |
| Graphic Artist: | Mr Henry Udeh |
| Proofreader: | Mr Awe Olaniyan Joseph |

# Module 1: Computer Security Technology and Principles

## Module Introduction

This module is an overview of computer security technology and principles. It covers security fundamentals, user authentication, cryptographic tools, access control, malicious software, database and cloud security, intrusion detection, and firewall and intrusion prevention systems. It contains eight units as follows:

| | |
|---|---|
| Unit 1: | Security Fundamentals |
| Unit 2: | User Authentication |
| Unit 3: | Cryptographic Tools |
| Unit 4: | Access Control |
| Unit 5: | Malicious Software |
| Unit 6: | Database and Cloud Security |
| Unit 7: | Intrusion Detection |
| Unit 8: | Firewall and Intrusion Prevention Systems |

## Unit 1: Security Fundamentals

### Contents

# 1.0 Introduction

Before you can start securing your data or information, you need to have a basic understanding of the concepts of core security fundamentals. You need to understand what you are protecting, why do you need to protect and why you are protecting the protectable. Consequently, this unit is to expose you to core security principles which include confidentiality, integrity and availability. You will also learn different types of models for access control. These models include Authentication, Authorisation and Accounting. In the last past of this unit, you will learn the concept of physical security.

# 2.0 Intended Learning Outcomes (ILOs)

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

- describe the key security requirements of confidentiality, integrity, and availability.
- discuss the types of security threats and attacks to handle.

# 3.0 Main Content

## 3.1 Understanding Core Security Principles

When you are thinking of securing the network environment, the first thing to think about is the CIA triangle. The CIA here does not refer to the Central Intelligence Agency; instead, it is an acronym for the three principles of security, namely: Confidentiality, Integrity, and Availability. Let us discuss each of the three goals of network security, as indicated in figure 1.

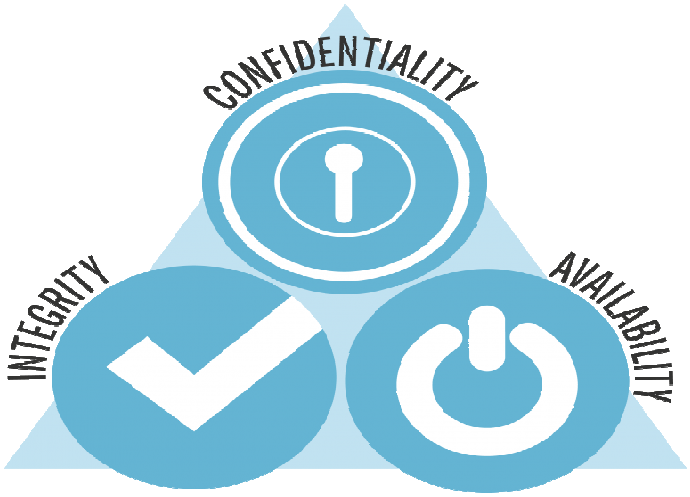


**Fig. 1.1: CIA Triangle**

### 3.1.1 Confidentiality

This part of CIA of network security principles makes sure that the data is available only to the intended and authorised users, applications, or computer systems. Confidentiality is described as the security controls required to prevent the disclosure of information to unauthorised individuals, applications or systems. In other words, confidentiality ensures protection of data. This protection applies to both transmission data and storage data. Meanwhile, different data classifications (transmission and storage data) go with different techniques of protection. For instance, the technique for protecting cryptography key is different from the technique for a protection login password. Breach in confidentiality results to data leakage and leaked data could be used to perpetrate identity theft against the owner of leaked data. The following security technologies can be implemented to achieve confidentiality in a network environment:

- Dedicated Access Control
- Strong Authentication
- Strong Encryption

### 3. 1.2 Integrity

One of the goals of information security program is to ensure that data is protected against any unauthorized or accidental changes. Unauthorised or accidental changes bring about inaccurate and inconsistency of data or information. Integrity is described as the security controls required to ensure that data or information is accurate and consistent. Integrity is to make sure that data is reliable and is not changed by unauthorized persons. In other words, integrity assures accuracy and consistency of data or information. A security program should include processes or techniques to manage intentional changes, as well as to detect changes. These processes or techniques ensure integrity. Some of the security technologies that to effectively ensure the integrity of data or information include:

- Access control
- Authentication
- Authorisation
- Accounting

### 3.1.2 Availability

Availability is the third primary security principle, and it is described as the security controls required to ensure that data or information, to a user, application, services or computer system remains accessible at all times. The main function of availability is to ensure that the data, network resources/services are continuously available to the legitimate users, applications and systems whenever they require it. In most cases, threats to availability occur in two categories. These categories include:

i. **Accidental**: Accidental threats come through natural disasters. Some of these natural disasters are storms, floods, fire, power outages, earthquakes, and so on. This category also includes outages due to equipment failure, software problems, and other unplanned systems, network, or user issues.

ii. **Deliberate:** Deliberate threat is related to outages that result from the exploitation of system vulnerability. Some examples of this type of threat include denial of service attacks or network worms that impact vulnerable systems and their availability.

## 3.2 Understand Model for Access Control

While confidentiality, integrity and availability are core network security principles or controls, there are other controls which are equally important. These controls are authentication, authorisation, and accountability (AAA). AAA is referred to as a model for access control and is also called ‘the three As’. Discussion on each of these access controls is presented in the next sub-sections.

### 3.2.1 Authentication

Authentication is the first control of the three As and the main function of this control is to verify entity access to system resources, including data and applications. Authentication is the process of identifying an individual trying to get access to a system or network resources. In most cases, Authentication is based on a username and password. In other words, authentication is used to determine and enforce the access rights of an entity.

### 3.2.2 Authorisation

An authorisation is a process of allowing or denying a user access permission to a protected system or network resource. Authentication is used to prove the identity of a user, whereas authorization gives access to an authenticated user. In other words, after a user is authenticated by means of authentication credentials (username and password), s/he can access network resources based on his or her authorisation. An authorisation is a process of giving individuals access to a system or network resource objects based on their identity.

### 3.2.3 Accounting

Accounting is the third part of the model for access control. Accounting is also referred to as Auditing. This part of control ensures that records of a user’s activity when accessing a system or network resources is kept. These records include the services accessed, the amount of time spent in the network, and the amount of data transferred during the session.

Apart from core security controls and the three as discussed in the sections above, physical security control is also essential in ensuring proper security for system or network resources. Consequently, our next section discusses physical security concept.

## 3.3 Physical Security

Network security is not only limited to the implementation of various security technologies for the protection of the entire network but also ensures that the entire network resources are physically protected. In other words, Security of computer-related assets and data involved implementation of both security technologies and physical security. However, there are many factors to consider when designing, implementing or reviewing physical security measures for the protection of assets, systems, networks, and information. These factors include but not limited to understanding site security and computer security; securing removable devices and drives; access control; mobile device security; disabling the logon locally capability, and identifying and removing key loggers and so on.

Some level of physical access control over network resource is needed for proper physical security. In an organisation, a place like a server room or Network Operating Centre (NOC) can be controlled by introducing something like badge readers and keypads to access the server room or NOC. Also, the logbook can be introduced to monitor in and out of the authorised staff that have access to the server room.

Discussion

Discuss how organisation can achieve data security or network security when techniques to address the three core security parameters are put in place.

## 4.0 Self-Assessment Exercise(s)

1. One of the following is NOT a core security perimeter.
A. Auditing
B. Availability
C. Integrity
D. Confidentiality

**Answer: A**

2. The following except one security technologies can be implemented to achieve confidentiality in a network environment.
A. Dedicated Access Control
B. Strong Authentication
C. Strong Encryption
D. Integrity check

**Answer: D**

**Assignment 1**
Using your mobile devices as case study, explain how you can achieve confidentiality and integrity of data or information in your devices.

_____________________________________________________________

_________________________________________________________________

__

**Answer**: Confidentiality and Integrity in a system can be achieved by putting in place a security technique that will prevent an unauthorised person from having access to the system. Some of the security techniques that can be used to effectively ensure the confidentiality and integrity of data or information include access control, authentication and authorisation.

## 5.0 Conclusion

In this unit, I have discussed the three-core security principle and the three model for access control. Also, the concept of physical security has been discussed. Therefore, it expected that you have a good understanding of all the areas covered in this unit.

## 6.0 Summary

In this unit, you have learnt that:

- core security principle consists of Confidentiality, integrity and availability.
- model for access control comprises of authentication, authorisation and accounting
- physical security is also important in the designing and implementation of network security.

## 7.0 References/Further Reading

Krebs, B. (15 October 2012). 'The Scrap Value of a Hacked PC, Revisited'. Retrieved from http://www.krebsonsecurity. com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Glanz, J. & Markoff, J. (15 February 2011).'Egypt Leaders Found 'Off' Switch for the Internet', *The New York Times*. Retrieved from http://www.nytimes.com/2011/02/16/technology/16internet.html

Matlack, C. (4 September 2014).'Swift Justice: One Way to Make Putin Howl', *Bloomberg Business*. Retrieved from http:/www.bloomberg.com/bw/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swiftmoney-system

# Unit 2: User Authentication

## Contents

## 1.0 Introduction

In this unit, I shall discuss the concept of user authentication and various techniques of user authentication.

## 2.0 Intended Learning Outcomes (ILOs)

By the end of this unit, you will be to:

- explain how user authentication works
- describe different techniques of authenticating a user.

## 3.0 Main Content

### 3.1 User Authentication Concept

What are the common means of authentication? The common means of authentication is password. To avoid the threat to core security principles, the user of the system or network resources need authentication. User authentication is a process of verifying what a user claim s/he is. User

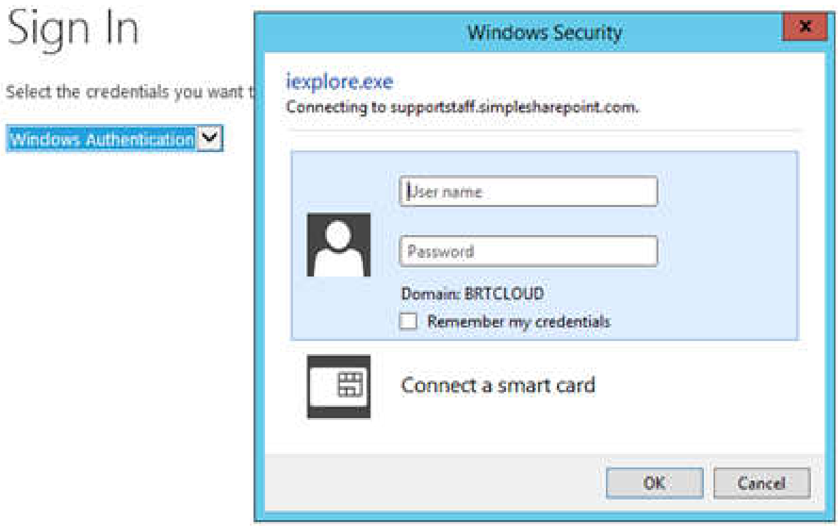
Authentication is a process of identifying a user based on authentication credentials which are usually username and password. As mentioned in Unit 1, authorisation is a process of giving permission. This implies that user authentication is not the same as user authorisation.

## 3.2 User Authentication Techniques

Apart from the most commonly used password, there are other user authentication techniques. These other techniques are based on knowledge, ownership/object and biometrics. Discussion on each of the user authentication techniques is presented in the next sub-sections.

### 3.2.1 Authentication Based on Knowledge – "What You Know"

Knowledge-based user authentication has to do with what a user knows, which is secret. Examples of knowledge-based user authentication are a Password which could be numerical, alphabetical or alphanumerical and a PIN as shown in the figure below, which is a number that is commonly used by mobile devices. Implementation of a strong password can prevent an unauthorised user or impostor from gaining access to a system or network resource as could be observed in figure 1.2.



Sign In

Select the credentials you want t

Windows Authentication

Windows Security

iexplore.exe

Connecting to supportstaff.simplesharepoint.com.

Domain: BRTCLOUD

**Fig. 1.2: Knowledge-Based Authentication**

However, this technique suffers from vulnerability to shoulder surfing and brute force attack. If an attacker can obtain the user password through any of the above attack techniques, no matter how strong the password, the attacker will gain access to the system.

### 3.2.2 Authentication Based on Ownership/Object- "What You Have"

Ownership based user authentication relies on what a system user has, which may be a token, smart card or a chip; an example can is in the figure below. This technique requires the system user to physically possess an object (such as a token or a chip) for authentication. The major problem with this kind of authentication arises when the system user loses the object to the attacker.

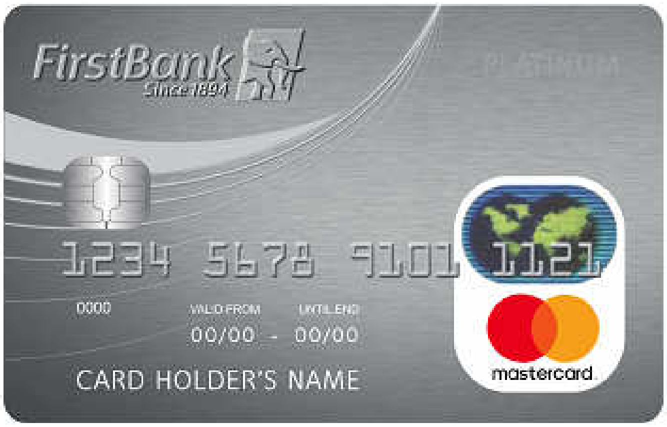


**Fig. 1.3: Smart Card of a User**

If this object is in the hands of an attacker, unauthorised access can be gained into the system, thus circumventing the authentication scheme. This implies that there is no assurance of uniquely identifying a legitimate user even with the ownership of an object. Quite a number of systems today combine this technique with the knowledge-based technique to improve the user authentication scheme.

**A real-life scenario of Authentication:**
Imagine you want to withdraw money from the closest Automated Teller Machine (ATM), two major requirements must be met, the user must have an ATM card and must know the PIN to that particular card. These two combined to form what is known as two-factor authentication; that is, what you have and what you know. The card is what you have, and the pin is what you know.

### 3.2.3 Authentication Based on Biometrics- "What You Are" and "What You Do"

Biometric user authentication relies on the physiological and behavioural characteristics of a system user. Biometric technologies are defined as automated methods of verifying or recognising the identity of a living person based on physiological and behavioural characteristics. Biometric technology is an authentication mechanism that identifies users based on a unique feature. Biometrics user authentication technique has some benefits, which makes the technique better than other user authentication techniques. These benefits are:

1. The uniqueness of identity
2. Non-transferability
3. Impossibility to forget
4. Difficulty in reproduction
5. Usability with or without specific knowledge
6. Complexity in alteration or modification.

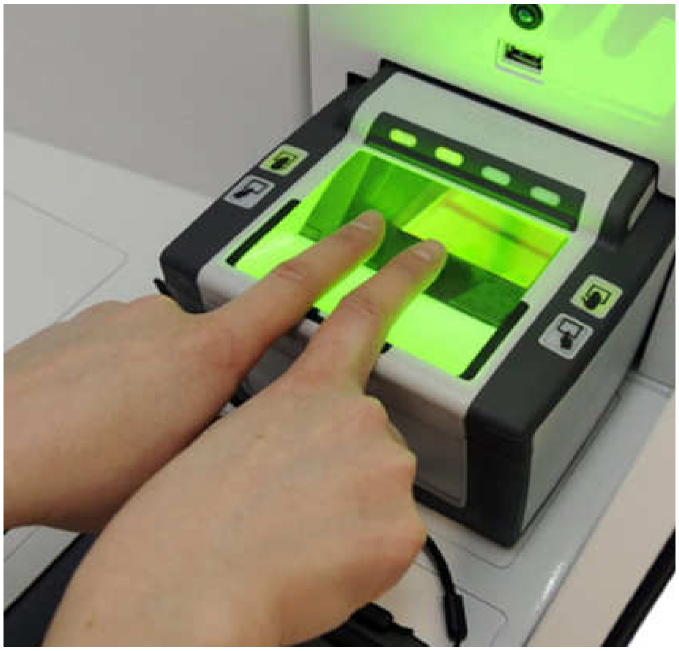


**Fig. 1.4: Fingerprint Verification System**

The uniqueness characteristic can depend on what the user is (physiological), or what the user does (behavioural). Details of this two-fold biometric authentication technique are in the following sub-sections.

### 3.2.4 Physiological Biometric- “What You Are”

A physiological biometric simply means something that system users are. This type of biometric technology performs authentication based on the physical characteristics of a system user. Examples of physical characteristics used for user authentication are fingerprints, the face, Retina pattern, and iris pattern. Physiological biometric authentication is reliable in the sense that the physical characteristics of a human being cannot be manipulated or duplicated. However, implementation of physiological biometric authentication requires additional hardware devices and software which often make the technique too expensive to implement. Also, some of the physiological authentication techniques require the collection of physiological features of a system used for training samples at different times under different conditions or moods. This creates inconvenience for the system user.

### 3.2.5 Behavioural Biometric- "What You Do"

A behavioural biometric simply means what the system user does. Behavioural biometric authentication relies on a behavioural characteristic of system users. Authentication is performed based on the pattern in which the system user does something. Examples of behavioural characteristics use for authentication are handwriting, handwriting signature, walking gait, voice, and keystroke dynamics. Behavioural characteristics are the unique characteristics of an individual that cannot be replicated. Some of these behavioural biometric authentication methods require hardware and software for their implementation while some require no hardware or software for their implementation. For instance, online (dynamic) signature verification uses a signature that is captured by pressure-sensitive Tablets that extract the dynamic properties of a signature in addition to the shape of the signature. In contrast, offline signature verification requires a scanner for scanning both the training and test samples.

Discussion

Authentication is an important access control technique which is one of the access control models discussed earlier in Unit 1. When implementing authentication technique for any system, consideration must be given to strong authentication technique. Meanwhile Authentication technique can be single-factor, two-factors or multi-factors. Single-factor authentication technique is when an individual is required to verify their identity through a single category of credential. Of course, Two-factors authentication technique requires two categories of credentials. Multi-factors authentication requires more than two categories of credentials. For strong authentication technique, multi-factors technique is considered the best. Are there challenges in implementing multi-factors authentication technique? What do you need to consider before implementation?

## 4.0 Self-Assessment Exercise(s)

1. User authentication is a process of identifying a user based on authentication credentials which is usually ____________ and ___________

   A. OTP and Token
   B. Username and Password
   C. Authentication and Credential
   D. Identifying and Verifying

**Answer: B**

2. The following are characteristics of biometric-based authentication except

A. The uniqueness of identity

B. Non-transferability

C. Complexity in alteration or modification

**D. Fingerprint and iris**

3. If you are to recommend behavioural biometric authentication technique for small-scale industry, which category of the behavioural biometric authentication technique will you recommend?

4. Give reason(s) for your response in '3'

____________________________________________________________

____________________________________________________________

**Answer**: In terms of implementation, there are two categories of behavioural biometric authentication methods require hardware and software for their implementation while some require no hardware or software for their implementation. For instance, online (dynamic) signature verification uses a signature that is captured by pressure sensitive Tablets that extract the dynamic properties of a signature in addition to the shape of the signature, while offline signature verification requires a scanner for scanning both the training and test samples.

## 5.0 Conclusion

In this Unit, I have discussed the concept of user authentication. I have also discussed different user authentication techniques. These techniques are Knowledge-based technique, ownership-based technique and biometrics-based technique. I believe that you now have a better understanding of different user authentication techniques.

## 6.0 Summary

In this unit, you have learnt that:

- User authentication is a means of securing the system or network resources.
- There are different techniques for user authentication.
- Knowledge-based, ownership-based and biometrics-based are different techniques for user authentication.

## 7.0 References/Further Reading

http://peter.havercan.net/computing/plain-persons-guide-to-secure-sockets-layer.html

Jeetendra,Pande (2017).*Introduction to Cyber Security*. Uttarakhand Open University.

Shubert, A. (2011). “Cyberwarfare: A different way to attack Iran's reactors.”*CNN.*

# Unit 3: Cryptography Tools

## Contents

## 1.0 Introduction

In this unit, I will discuss the concept of cryptography. I will also discuss the types of cryptography. The unit will round up with a discussion on various modern encryption algorithms.

## 2.0 Intended Learning Outcomes (ILOs)

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

- describe the concept of cryptography
- explain different types of cryptography
- manage the operation of selected encryption algorithms.

# 3.0 Main Content

## 3.1 Cryptography Concept

In order to provide additional security control (such as confidentiality and integrity), cryptography can be used in the design and deployment of the user authentication techniques discussed in Unit 2. Let me ask you, what is cryptography? Cryptography which is not a process of hiding the existence of message; instead, it is the science of protecting information by transforming it into a secure format. The process of transforming a message into a secure format is called encryption. Encryption can also be described as a process of converting data into a format that cannot be read by another user. Once a user has encrypted a message, that message automatically remains encrypted. To make a message or information. When a message is scrambled with an encryption algorithm, it makes it inaccessible to an unauthorised person. However, the scrambled message can be reverted reversed to make the message accessible. The process of reversing scrambled message is called Decryption. In other words, Decryption is the process of converting an encrypted message back to its original format. For a better understanding of how encryption and decryption work, I will discuss the terminologies of cryptography in the next sub-section.

## 3.2 Cryptography Terminologies

I will give an example of an encryption and decryption process to show a clear picture of cryptography terminologies. Let assume Mr A is sending a message to Mr B and Mr A does not want Mr C to have access to the message. Mr A needs to convert the message to unreadable format before sending the message to Mr B. When the message gets to Mr B, Mr B needs to convert the message to its original format for the message to be readable. The following are the terminologies from this example:

- **Sender**: Mr A that is sending a message to Mr B is a sender.
- **Receiver**: Mr B, that is receiving a message from Mr. is the recipient.
- **Intruder**: Mr C is an intruder who is interested in having access to Mr B message.
- **Plaintext**: Plaintext is the original message Mr A is sending to Mr B.
- **Ciphertext**: This is the output of an encrypted message from Mr B.
- **Encryption Algorithm:** Mr A will convert plaintext and encryption key to ciphertext. The encryption algorithm is a mathematical process that converts plaintext and encryption key to a ciphertext. In other words, the encryption algorithm takes plaintext and an encryption key as input and output a ciphertext. Later in this unit, I shall discuss some of the modern encryption algorithms.

- **Decryption Algorithm:** Mr B will reverse ciphertext and decryption key to having plaintext. Decryption algorithm is a mathematical process that changes ciphertext and decryption key to plaintext. In other words, the decryption algorithm takes ciphertext and decryption key as input and output a plaintext.

- **Encryption Key:** This is a value that is owned by Mr A. Mr A inputs the encryption key and plaintext into the encryption algorithm along with the plaintext to generate the ciphertext.

- **Decryption Key:** This is a value that is owned by Mr B. Mr B inputs the decryption key and ciphertext into the decryption algorithm along with the ciphertext to generate plaintext.

## 3.3 Types of Cryptography

There are two basic types of cryptography or cryptosystem. These two types determine how encryption and decryption are carried. In the next sub-sections, I shall discuss the two basic types, which include symmetric key cryptography and asymmetric key cryptography. It is important to note that symmetric key cryptography is also referred to as symmetric key encryption while asymmetric key cryptography is also referred to as asymmetric key encryption.

### 3.3.1 Symmetric Key Cryptography

Symmetric key cryptography or conventional cryptography is also known as secret-key cryptography or symmetric key Encryption. Symmetric key cryptography is a form of cryptosystem in which encryption and decryption are performed using the same key. In symmetry key cryptography, the sender and receiver of a message share a single, common key. In other words, symmetric-key cryptography is characterised only one key for both the sender and receiver. Let us consider the example given above to explain how symmetric key cryptography works. To prevent the intruder (Mr C) from reading Mr A message, Mr A inputs the plaintext (original message) and asymmetric key into the encryption algorithm. This produces the ciphertext. Mr A then sends the ciphertext to Mr B. Mr B then inputs the ciphertext and the same symmetric key into the decryption algorithm to generate the plaintext (original message). Symmetric-key ciphers fall into the following categories:

- **Block ciphers**: A block cipher takes a block of plain text and a key, and then outputs a block of ciphertext of the same size.
- **Stream ciphers**: A stream cipher creates an arbitrarily long stream of key material, which is combined bit-by-bit or character-by-character with the plain text.

### 3.3.2 Asymmetric Key Cryptography

Asymmetric key cryptography is also known as public-key encryption. Asymmetric encryption is a form of cryptography in which encryption and decryption are performed by using two different keys. Unlike symmetric key encryption, one key called the public key is used to encrypt a message and another key called the private key is used to decrypt the message in public-key encryption. In asymmetric key encryption, you can release your public key to anyone to send a message to you, while you keep your private key for the opening of the message.

## 3.4 Encryption Algorithms

In this sub-section, I shall discuss different modern encryption algorithms. These algorithms include both the symmetric and asymmetric algorithms.

### 3.4.1 Rivest-Shamir-Adleman (RSA)

In 1978 Ron Rivest, Adi Shamir, and Leonard Adleman designed Rivest-Shamir-Adleman encryption algorithm simply called RSA. RSA is one of the best known public-key encryption algorithms for key exchange. Of course, RSA is an asymmetric key encryption algorithm which is a widely used public-key encryption algorithm. RSA is characterised with the use of variable size encryption block and a variable size key. RSA operation is based on number theory. In generating public and private keys, RSA uses two prime number. The public key and private key are used for encryption and decryption, respectively.

Let us consider our earlier example for an explanation of how RSA works. Let again assume that Mr A is sending a message to Mr B. In RSA, Mr B, who is a receiver will send his/her public key to Mr A for encryption. Mr A will then encrypt the message with Mr B public key before releasing the message to Mr B. Mr B will then decrypt the message with his/her private key. There are three important steps involved in RSA cryptosystem. These are:

- Key generation
- Encryption with the public key
- Decryption with the private key

### 3.4.2 Data Encryption Standard (DES)

Data Encryption Standard is simply called DES. Data Encryption Standard often called DES is one of the most widely used and publicly available encryption algorithms. DES was developed by IBM in the year 1972. National Institute of Standards and Technology (NIST) later adopted DES as Federal Information Processing Standard (FIPS) in 1976. DES is a symmetry key encryption and is a block cipher. It is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key. In other words, DES receives data of 64-bit long ordinary message and 56-

bit key and comes up with a 64-bit block. The goal of the DES algorithm is to offer a strategy to secure crucial financial database. Despite DES being vulnerable to brute force attack, financial institutes and other industries worldwide find it difficult to migrate to another cryptosystem for protection of sensitive on-line applications.

### 3.4.3 Triple Data Encryption Standard (3DES)

DES is vulnerable to brute force attacks because it uses relatively small 56-bit key size. Hence, DES is not reliable for encryption of sensitive data. Consequently, instead of designing a completely new symmetry key encryption, Triple Data Encryption Standard or Triple Data Encryption Algorithm often represented as TDEA or 3DES was developed to address the weakness in DES. With three different keys, TDES extends the key size of DES by applying the algorithm three times in succession. Combination of DES 56-bit in three times will give 168-bit. TDEA uses three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode. This means that the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3.

### 3.4.4 Advanced Encryption Standard (AES)

In the year 2001, the Advanced Encryption Standard called AES was recommended by NIST as a more secure symmetric key encryption algorithm to replace DES. AES algorithm can support any combination of data (128 bits) with key sizes of 128, 192, and 256 bits. The algorithm comprises three block ciphers—AES-128, AES-192, and AES-256 depending on the key size. During the encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys to generate final ciphertext or to reverse the original plaintext.

Discussion

As discussed earlier in this module, confidentiality is one of the three security goals. **Discuss** the ways to achieve confidentiality of information whether on a system or on transmission.

## 4.0 Self-Assessment Exercise(s)

1. Cryptography deals with the secrecy of message; hence it has two types select the two.

A. Symmetric key cryptography
B. Encryption based cryptography
C. Asymmetric key cryptography
D. Decryption based cryptography

**Answer: A, C.**

2. From both ends of a cryptosystem, two functions must be performed at both ends to get a ciphertext-plaintext instance.

A. Senders function
B. Receiver's Function
C. Encryption
D. Decryption

**Answer C, D**

## 5.0 Conclusion

The unit has exposed you to the concept of cryptography. You have also seen different types of cryptography. Furthermore, some modern encryption algorithms (RSA, DES, 3DES and AES) have been discussed. By now, you are expected to have a better understanding of the concept.

## 6.0 Summary

The main points you have learnt in this unit are the definition of cryptography; different types of cryptography; how cryptosystem works with an example; different types of modern encryption algorithms.

## 7.0References/ Further Reading

https passwords/quickguide://uit.stanford.edu/service/accounts/

https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre

Jeetendra, P. (2017).*Introduction to Cyber Security*. Uttarakhand Open University.

# Unit 4: Access Control

## Contents

## 1.0 Introduction

In continuation of our discussion on security controls, I am going to discuss another important aspect of security controls in this unit. This aspect is access control. I will start the discussion with the definition of access control for you to have a good understanding of the concept. After that, I am going to explain the access control policy and models. My discussion in this unit will end with an explanation of different kind of access control models.

## 2.0 Intended Learning Outcomes (ILOs)

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

- explain access control
- manage access control towards goal achievement
- describe how various access control models work in achieving security goal.

# 3.0 Main Content

## 3.1 Understanding Access Control

What is Access control? Access control which is also known as authorisation is a process of determining whether a subject (e.g., process, computer) can perform an operation (e.g., read, write) on an object (e.g., a file, a resource in the system). Access control could also be defined as the technical strategy that restricts unauthorised subjects (examples, application, process, computer, human user and so on) from the system, grants access to authorised subjects to perform an operation (such as read, write, execute, search, delete and so on) and limits operation that authorised subject can perform on the system. In other words, Access control determines whether a subject will be able to perform an operation on an object (such as a database of any other resources of the system) in accordance with security policy. It is important to note that access control and security policy are the main components of information security. Why access control? The need for preservation of confidentiality, integrity and availability (though to some extent) of information gives an answer to the question "why access control?" In the next sub-section, I shall briefly discuss access control policy.

## 3.2 Access Control Policy

An access control policy is the set of rules built on an access control model that defines the subjects, objects, permissions, and other concepts within the computer system. Decisions on authorisation are based on access control policies. Security policies are made by the owner of a computer system or computing resources. This owner could be individual or cooperate organisation. Access control policy defines the subjects' permissions (the right to perform an operation on a system or object) in a computer system or computing resources for the purpose of enforcing the information security practice in an organisation. The literature has it that, development, deployment, reviewing, and enforcement of security policies is one of the fundamental best practices in information security.

## 3.3 Access Control Models

Access control model is the underlying model upon which security policies are built. To organise access control, the access control model defines concepts and relations between them. There are different ways in which an organisation can implement access control. Access control model establishes how separate entities (subject, object, operation and permission) relate. There are different categories of access control models. As depicted in figure 4.1 below

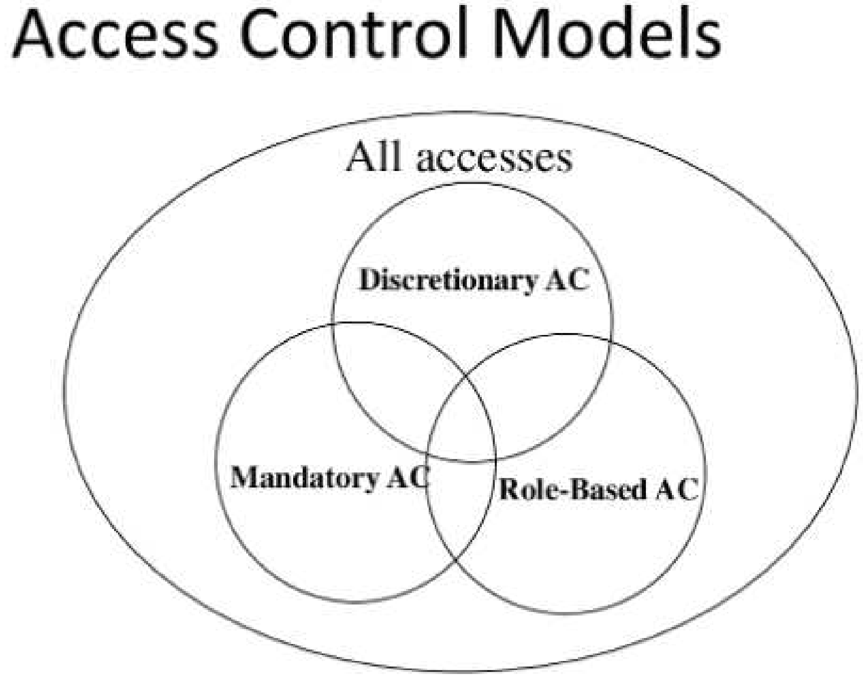


**Fig. 1.5: Access Control Model**

In the next sub-section, I shall discuss three main popular access control models which include a discretionary access control model; mandatory access control model and role-based access control, model.

### 3.3.1 Discretionary Access Control Model

Discretional access control model is often denoted as the DAC model. Discretionary access control is highly flexible, and one of the most widely used access control models. In Discretionary access control model, permissions are granted by the system owner. Under Discretional access control, the owner of resources or system can grant access to the users or even transfer ownership to the users. DAC model allows granting and revocations of permissions to the discretion of the owner of resources or system. A good example of where this access control model category is implemented is in the Unix/Linux operating system. The principle of the DAC model is implemented in the Unix/Linux operating system to control access to file. DAC model is not appropriate for high assurance system and many complex commercial security requirements. Private organisations use this model mostly.

### 3.3.2 Mandatory Access Control Model

With the DAC model, users are granted access to information or resources that do not belong to them, hence the possibility of a confidentiality breach. This poses a serious challenge to the critical confidentiality organisation. To overcome this challenge of DAC model, Mandatory access control model, which is often denoted as the MAC model, was designed.

Under the MAC model, the policy defines how permissions are granted to the subjects or users of the system or resources. MAC model is characterised with a process called clearance and labelling. Clearance and Labeling is a process whereby a user and a system or resource are assigned clearance and label, respectively. This is achieved by giving each user of a system clearance and by labelling each resource of a system.

The clearance and labelling process dictates the level of access a user has on a labelled system or resource. In other words, a user may access the system if and only if the user clearance is equal to or greater than the system or resource label. However, because of the increased overhead in achieving clearance and labelling of users and system resources, respectively, many private organisations move away from this category of access control model. Another good reason why many private organisations do not use this model is that the model surfers rigidity.

### 3.3.3 Role-Based Access Control Model

Role-base Access Control simply called RBAC to govern access to systems or resources based on the role of the subject or user. The main concept of RBAC is a role. What is the role? A role is a job function within the organisation with some associated semantics regarding the authority and responsibility conferred on a member of the role. In other words, roles are created for the various job functions in an organisation and users are assigned roles based on their responsibilities. Role-based access control supports access restrictions that derive from responsibilities an organisation assigns to roles.

The general idea of RBAC is that permissions are granted with roles, and users are assigned to appropriate roles. Roles are created for the various job functions in an organisation and users are assigned roles based on their responsibilities and qualifications. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed.

## 4.0 Self-Assessment Exercise(s)

1. Decisions on authorization are based upon access control
A. Policies
B. Procedures
C. Standards
D. Practices
**Answer: D**

## 5.0 Conclusion

Access control is a key concept in the arena of information security that you need to have a better understanding. Consequently, I have discussed the concept of access control in this unit. I have equally exposed you to various access control models which include: DAC model, MAC model and RBAC model. You are by now expected to master the main points addressed in this unit.

## 6.0 Summary

The main points I have addressed in this unit are the concept of access control, access control policy and access control, model. Access control model discussed they are DAC model, MAC model and Role-Based Access Control model. In our next unit, our focus will be on malicious software.

## 7.0References/Further Reading

http://www.ijecs.in/index.php/ijecs/article/view/1813

https://www.academia.edu/39692556/Introduction_to_Cyber_Security" https://www.academia.edu/39692556/Introduction_to_Cyber_Security

Lucas, I. (2009, July 10). Password Guidelines. Onttrek Oct. 24, 2015 uit Lockdown.co.uk: http://www.lockdown.co.uk/?pg=password_guide available under a Creative Commons Attribution-ShareAlike 2.0 License

# Unit 5: Malicious Software

## Contents

## 1.0 Introduction

Information security breaches are not only based on weakness in systems or resources authentication techniques, but Attackers also used other means to attack their victims. Attackers used different malicious software to carry out their various attack activities. In this unit, I will start the discussion from the definition of malicious software. After that, I am going to discuss different categories of malicious software.

## 2.0 Intended Learning Outcomes (ILOs)

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

- define malicious software
- describe the different threats posed by malware
- discuss malware countermeasure elements.

# 3.0 Main Content

## 3.1 Definition of Malicious Software

What do you understand by malicious software? Malicious software refers to malware. In other words, malware was derived from **MAL**icious soft**WARE**. Therefore, when you hear the word malware, you should know the same thing as malicious software. Malicious software or malware is a hostile program developed by computer programmers or cyber attackers that insert itself or being inserted on to your computer system without your consent. Malicious software could also be defined as a set of instructions that run on your computer without your knowledge and make your computer do something that an attacker wants it to do. An attacker may want to: steal your information on your system; cause damage to your system; use your system as relay and so on. In essence, any program or software that is intrusive or hostile and that is inserted into your computer without your knowledge is malicious software.

## 3.2 Categories of Malicious Software

In most cases, people referred to malicious software or malware as virus only. No, a virus is not the same as malware, although a category of malware, as shown in figure 5.1 below. In the next sub-sections, I am going to discuss different categories of malicious software or malware. Let us move to the next sub-section.

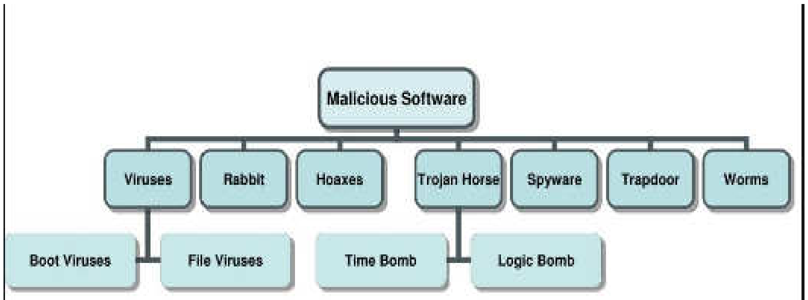


**Fig. 1.6: Categories of Malicious Software.**

### 3.2.1 Worm

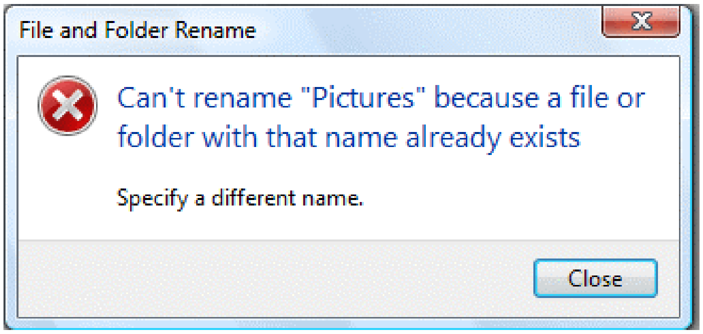
A worm is one of the categories of malware, and it is self-contained malicious software that propagates itself by sending a copyof itself to other machines over a network? In other words, a worm does not need any document to move from one machine to another. A worm is a program that spreads itself through a network and does not need to attach itself to an existing file or program. Worms spread themselves typically by exploiting existing vulnerabilities or weaknesses in an Operating System (OS) or application. Worm exploits vulnerabilities in operating systems or software. The Morris Internet worm of 1988 is a good example of a worm that exploited vulnerabilities in OS (UNIX systems). Another example is worms that exploited vulnerabilities in Microsoft Windows (Mydoom of 2004). The Morris Internet worm of 1988 and Mydoom of 2004 worm spread rapidly through the Internet and continued until the vulnerabilities they exploited were fixed.

### 3.2.2 Virus

A computer virus is a malicious software of executable code that propagates typically by attaching itself to a document or a file that will generally be an executable file. A virus is a software program that can copy itself from one file to another to infect a computer. A virus can also be defined as a piece of software that infects programs, modifying them to include a copy of the virus in the programs.

A virus is also programs that replicate itself between files, memory, hard disks, or other data storage device. With excursion or copying of an already infected file, a virus quickly spreads. Note that inserting a CDROM or thumb drive on some operating systems is equivalent to executing a program, and can also cause a virus to spread. Worm and virus are software that spread, what then differentiates them? The main difference between a virus and a worm is that a virus needs a file or document to propagate itself while a worm does not need a file or document to propagate itself. In other words, a worm does not need to attach itself to another program while a virus needs to do so.

**Scenario**: “Sometimes, when you see unusual error messages displayed on your computer repeatedly, as shown in the figure below in most cases is a virus attack.”



File and Folder Rename

Can't rename "Pictures" because a file or folder with that name already exists

Specify a different name.

**Fig. 1.7: Instance of a Virus Attack**

### 3.2.3 Logic Bomb

A logic bomb is one of the oldest malicious software. In Logic bomb, code is embedded in a legitimate software or program; this code will be activated when one or more specified condition(s) is met. This condition could be a particular time/date, presence of a file, absence of a file, and so on. A malicious logic is embedded in a valid executable program by its developer, integrator, distributor, or installer. When the program embedded with malicious logic triggered, modification or deletion of file, machine halting and system damages are the likely consequences. Time bomb and Trojan horse malicious software also share the same features with a logic bomb.

### 3.2.4 Trojan

A Trojan describes the class of malicious software that appears to perform a desirable function (as a state by the developer) but later performs undisclosed malicious functions that allow unauthorised access to the victim's computer. In other words, Trojan is an attractive software or application with hidden negative effects. This software could be game, free download application, software upgrade, and so on. When an attempt is made to run the attractive software, the software starts with an additional task such as virus infection, installation of backdoor program or destruction of victim's data. Backdoor malicious software will be discussed in the next sub-section.

### 3.2.5 Backdoor

Backdoor also is known as Trapdoor or Remote-Access Trojan is programs which allow an attacker to access a system in a way that bypasses normal authentication technique for the system. In this case, an attacker acts as a remote administrator to the infected machine. In an ideal situation, login to any system requires any means of authentication such as username and password. An infected backdoor system does not require login details before an attacker can gain access. The hidden software may be created by installing a new application or by modifying an existing application that gives access to a system.

### 3.2.6 Spyware

Spyware is malicious software that collects information about what a user does on a computer system. In other words, Spyware monitors the activities being carried out by a user of a computer system. Activities can be web browsing history, apps used, or messages sent. Spyware can be spread like a virus, worm, or through various other methods of delivering software such as drive-by-download, installation of software from the Internet, visiting a malicious website, and so on. The main goal of spyware is to track what you are doing on your computer and report that back to the attacker (another system). Spyware may transfer what you type, which sites you visit on the Internet, and even what information is presented. Spyware captures information of system user, which can include banking information, passwords, and other confidential and personal information. Some spyware may cause the victim computer system to become unstable. Apart from the monitoring function and collection of personal information, spyware also performs the following functions:

- Interference with user control of the computer through the installation of additional software.
- Redirection of browser activity.
- Reconfiguration of computer settings, resulting in slow connection speeds.
- Changing of home pages, Loss of Internet connectivity or functionality of other programs.

### 3.2.7 Adware

Adware is malicious software that automatically displays advertisement to the Internet user, resulting in unpleasant user experience. In other words, Adware displays unwanted advertisements to Internet users when browsing without their consent. Adware exactly does what it says on the advert. Each click by the victim brings about additional revenue to those that placed the advert. In most cases, the malicious software isn't there to steal data from the victim or cause damage to the device. However, too much pop-up as a result of adware annoys a computer user.

### 3.2.8 Keystroke Logger

Keystroke keylogger malicious software captures typing activities of a computer user to get sensitive information of the computer user. This malicious software is either install itself into a Web browser or being installs by the attacker without the consent of the user of the computer. In other words, keystroke keylogger monitors the data input by the user through the keyboard, and transfer the data to a control centre of the attacker. It is important to note that a piece of hardware also captures everything a user types on the computer keyboard.

### 3.2.9 Botnet

A botnet is a short form of robot network which is malicious software that is installed (without permission) on many different computers and is controlled remotely by the attacker. Botnets are a new evolution of malicious software and have become wide-spread. Botnet involves an attacker using malware to secretly control a network of computers in numbers, which can range from a handful to millions of compromised devices. Each member of the network of computers is called a robot or zombie. Each of the computers falls under the control of a single attacking operation, which can remotely issue commands to all of the infected computers from a single point. In other words, the software which infects the user’s computer waits for instructions on what to do from the remote system.

Meanwhile, this network of zombie can be used for many different coordinated attacks.  For instance, by issuing commands to all the infected computers in the zombie network, attackers can remotely carry out coordinated large-scale campaigns. These include DDoS attacks, which leverage the power of the army of devices to flood a victim with traffic, overwhelming their website or service to such an extent it goes offline. Other common attacks carried out by botnets are spam email attachment campaigns which can also be used to recruit more computers into the network, while smaller botnets have also been used in attempts to compromise specific targets.  Botnets are designed in such a way that the users are completely unaware that their computers are under the control of an attacker.

### 3.2.10 Rootkit

A rootkit is a collection of programs used by hackers to hide or evade detection while trying to gain unauthorised access to the victim's computer. With rootkit, attackers do many different undesirable things on their victims without being detected. Rootkits are a combination of malicious software that can include backdoors, keyloggers, and other malicious software that an attacker may find useful to hide their presence. Rootkits are designed to hide processes, files, or Windows Registry entries purposely. Attacks used rootkits to hide their tracks or to insert threats on their victims' compromised computers. An attacker installs rootkit by replacing system files or libraries, or by installing a specially crafted kernel module on the victim's computer.

To install a rootkit, the attacker must get access to the victim's computer by cracking login details of the victim computer or by exploiting a vulnerability in the victim's computer. The essence of this action and other action(s) that may be required is to obtain root or administrator privileges. Of course, by having access to the root of a computer, attackers can manipulate the victim computer to do anything they want. With the combination of other malicious software such as Trojan software, hackers use rootkits to change system settings and make use of the victim's computer without the user's knowledge. The worst part of it is that monitoring software such as firewalls or anti-virus programs will not be able to detect an attacker action(s).

## 3.3 Malicious Software Countermeasures

Malicious software or malware countermeasures are in two categories. They are:

1. Technology-based countermeasures
2. Information security policy-based countermeasures

In the next sub-section, I will discuss countermeasure that is based on technology.

### 3.3.1 Technology-based Malware Countermeasures

Technology-based malware countermeasures are divided into three categories which include: Detection, Prevention and Eradication. Each of these categories is described below.

a. **Detection**

Detection is the ability to recognise and find malware on a system, in a file on the system, and/or in software, hardware, or media not yet installed on the system. There are various detection techniques that academia, security vendor and professionals have offered to address malware detection. Some of these techniques are as follows:

**Signature-based detection**: This technique is based on analysing the behaviour of known and suspected malicious code.

**Behavioural-based detection**: This technique is based on signature matching.

**Anomaly-Based Detection:** This technique relies on indicators of unexpected and abnormal behaviour indicative of the trace of malicious code.

**Detection of Indirect Malware Indicators:** This technique relies on inference from indications of modifications to valid system contents or software code.

b. **Prevention**

Prevention approaches are required throughout the system life cycle to prevent malware during the developmental stage and operational stage of the system.

c. **Eradication**

Eradication has to do with removal and recovery from malware effects on operational systems.

Discussion

In your context identify the different categories of malicious software. Explain the impact they have on the society.

## 4.0 Self-Assessment Exercise(s)

1. Which of these definition best describe a computer virus?
A. A malicious software of executable code that propagates typically by attaching itself to a document or a file that will definitely be an executable file.
B. A collection of programs used by hackers to hide in order to evade detection while trying to gain unauthorised access to the victim's computer.
C. A short form of robot network which is a malicious software that is installed (without permission) on many different computers and is controlled remotely by the attacker.
D. A malicious software that collects information about what a user does on a computer system.
**Answer: A**

2. Malware countermeasures are based on two categories which include the following:
A. Technology-based countermeasures
B. Information security policy-based countermeasures
C. Antivirus based countermeasures
D. Antimalware based countermeasures
**Answer: A, B**

**Assignment 2**
Research of the various ways a rootkit is installed on a victim's system by the attacker, which is common in your environment and find out how to prevent rootkit attack.

## 5.0 Conclusion

In this unit, I have discussed malicious software by starting from the definition. I have also explained various categories of malware. Discussion on malicious software was rounded-up with malware countermeasures. I want to believe you now have a better understanding of malicious software.

## 6.0 Summary

In this unit, you have learnt what malicious software is and its categories. You have also learned how each category affects a victim's system and damages an attack causes to the victim’s system. More so, you have learned technology-based malware countermeasures which include detection, prevention and eradication. In our next unit, I am going to explain issues relating to database and cloud computing security.

## 7.0 References/Further Reading

Havercan, P. (2015, July 17). *A Plain Person's Guide to Secure Sockets Layer*. Retrieved on Sep. 26, 2015 from http://peter.havercan.net/computing/plain-persons-guide-to-secure-socketslayer.html

http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf

# Unit 6: Database and Cloud Security

## Contents

## 1.0 Introduction

Database and cloud computing require a high level of protection. Security of both the database and cloud computing is a thing of concerned for many organisations. In this unit, I will expose you to security threats to database and cloud computing environment. Also, I will discuss how to address these threats in both platforms.

# 2.0 Intended Learning Outcomes (ILOs)

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

- explain database security
- categorise approaches to database access control
- explain the security threat in database systems.
- manage the security issues related to cloud computing.

# 3.0 Main Content

## 3.1 An Overview of Database Security

Before we start a discussion on database security, let me quickly ask you a question. What is a database? A Database is an organised collection of integrated files. A database can also be defined as the storage areas for a large amount of related information. The nature of the information stored varies and depends on different organisations and companies. For instance, a company database might include files of all past and current employees of all the department. Now let us go back to the business. With your knowledge about security, what is database security?

Database security involves policies and techniques to protect data in the database and ensure that the data is not accessed, altered or deleted without proper authorisation. Database security methods focus on preventing unauthorised users from accessing the database because the Database Management System (DBMS) features that make the database easy to access and manipulate, also give a chance to intruders. Most DBMS's include security features that allow only authorised persons or programs to access data and then restrict the types of processing that can be accomplished once access is made.

Protection of a database becomes necessary as a result of the importance of data. For instance, if a database that houses credit card details of customers is being compromised, the attacker can make use of compromised credit card of customers to perform another transaction on another platform. The main security objectives of database security are the one we have discussed in Unit 1, which include confidentiality, integrity and availability. In essence, database, in summary, is defined as policies and mechanisms that ensure:

- Information is not disclosed to unauthorised users.
- Only authorised usersare allowed to modify data.
- Authorised users are not denied access.

## 3.2 Security Threats to a Database System

Before any discussion on how to secure our database, it is very important to first discuss security threats to the database system. The security threats to a database can be categorised into four which include people, malicious software, technological disaster and natural disaster. The threats are discussed in the next sub-section.

### 3.2.1 People

People can intentionally or unintentionally inflict damage, violation, or destruction to all or any of the database environment components which include people, applications, networks, operating systems, database management systems, data files or data. For instance, an unhappy employee of an organisation may decide to alter the organisation's database and delete data from the database. Examples of people are disgruntled employees, unpaid contractors, unpaid consultants, visitors with bad intention, hackers, terrorists etc.

### 3.2.2 Malicious Software

As discussed earlier, malicious software is an intrusive program developed by computer programmers or cyber attackers that insert itself or is inserted on to your computer system without your consent. Malicious software also serves as a threat to the database. Attackers, in most cases, intentionally insert malware to damage or violate one or more of the database environment components. An attacker can as well insert a line of codes in a database—for instance, Structural Query Language (SQL) injection.

### 3.2.3 Natural Disaster

A natural disaster like flood, fire, hurricanes, tornados, earthquakes, and so on can be a threat to the database system. In other word, calamities caused by nature, which can destroy any or all of the database environment components.

### 3.2.4 Technological Disaster

Technology disaster is often caused by some sort of malfunctions in equipment or hardware. Technological disasters can inflict damage to networks, operating systems, database management systems, data files or data.

# 3.3 Requirements for Database Protection

In line with the core security controls discussed in our previous unit, there are basic security requirements for database protection. These requirements include user authentication, protection from inference, protection from unauthorised access, Integrity of database and management and protection of sensitive data. These security requirements are discussed in the next sub-sections.

## 3.3.1 User Authentication

As we have defined user authentication earlier in our previous discussion, user authentication is a process of identifying a user based on authentication credentials which are usually username and password. User authentication requirement is used to enable only the authorised user to access the data. Don't forget, different user authentication techniques have been discussed in our previous unit.

## 3.3.2 Protection from Inference

Inference here refers to the protection of data from a type of threat where an unauthorised user tries to extract or retrieve confidential information from non-confidential data. In this case, the attacker usually targets the statistical databases; hence, precautions should be taken to protect each entity right from statistical aggregated information in order to prevent the statistical database from such threat.

## 3.3.3 Protection from Unauthorised Access

Protection from unauthorised access protects the data from being accessed by an unauthorised user. Any request sent by a user of applications to access a database or files should be verified by a database management system. It should check whether the user is authorised or not. Different access control models have been discussed in our previous unit. For the purpose of reminder, these access control models are DAC, MAC, and RBAC models.

## 3.3.4 Integrity of a Database

The integrity of a database may be breached as a result of unauthorised modification, insertions, and deletion of the content of the database. Integrity breaches may occur as a result of errors, malicious software infection and failures in the system or modification of contents present in the database. In essence, the database needs protection from the unauthorised user, which could be a human being, application, and so on.

### 3.3.5 Management and Protection of Sensitive data

This requirement entails preventing unauthorised users from accessing sensitive data. The database consists of the type of data which can either be sensitive, public or both. Thus, this requirement protects the contents of all types of data from attackers.

## 3.4 Approaches of Database Access Control

In Unit 4, I have extensively discussed different access control models how each of these models works has been discussed. These access control models constitute approaches of database access control. You are expected to go through Unit 4 for a better understanding.

## 3.5 Cloud Computing Security Overview

What is cloud computing? Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Computing resources, for instance, could be servers, application, networks and storage. Cloud computing is characterised by the following:

- On-demand self-service.
- Rapid elasticity.
- Measured service.
- Location independent resource pooling.
- Ubiquitous network access.

Meanwhile, Cloud computing security is defined as a combination of a set of policies, controls, processes and technologies that work together to protect cloud-based systems, data and infrastructure. Security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. Hence, there is a need to protect cloud computing environment. Let briefly discuss threats to cloud computing environment.

## 3.6 Threats to Cloud Computing

The following are common threats to the cloud computing environment.

- Misconfiguration of the cloud platform/wrong set-up
- Unauthorised access
- Insecure interfaces /APIs

- Hijacking of accounts, services or traffic
- External sharing of data
- Foreign state-sponsored cyberattacks
- Malicious insiders
- Malware/ ransomware
- Denial of service attacks

## 3.7 Security Technologies and Controls for Cloud Protection

In a data-driven environment, organisations must protect and secure workloads in the cloud. The threats to cloud computing listed above can all lead to data leakage if proper security technologies and controls are not in place. The following are security technologies and controls for cloud computing protection:

- Data encryption
- Network encryption
- (VPN, packet encryption, transport encryption)
- Intrusion detection and prevention
- Vulnerability assessment
- Access control (CASB/Cloud Access Security Brokers)
- Log management and analytics
- Privileged Access Management (PAM)
- Data leakage prevention
- Security Information and Event Management (SIEM)
- Trained cloud security professionals

Discussion

Discuss the main objectives of database security centred on the three security goals.

### 4.0 Self-Assessment Exercise(s)

1. In line with the core security controls discussed, there are basic security requirements for database protection; these include the following except. These requirements include
   A. User authentication.
   B. Protection from inference.
   C. Protection from unauthorized access
   D. Accounting.
   **Answer: D**

2. Cloud computing faces so many threat, which one of these is a type of threat faced in a cloud computing environment
   A. Misconfiguration of the cloud platform/wrong set-up
   B. Security Information and Event Management (SIEM)
   C. Data encryption
   D. Access control

   **Answer: A**

## 5.0 Conclusion

Database security and cloud computing security are important components for any data-driven organisation; hence, the need for their discussions in this unit. I have explained the concept of database security, a threat to a database system and approaches to database access control. Also, I have discussed cloud computing security from the definition of cloud computing. Threats and security technologies and controls to address these threats in the cloud computing environment have been discussed.

## 6.0 Summary

In this unit, you have learnt: security threats to a database; techniques to database access control; threats to cloud computing and technologies and control for cloud computing protection. In the next unit, I shall discuss Intrusion detection.

## 7.0 References/Further Reading

Dinniss, H. A. H. (2015). "The nature of objects: Targeting networks and the challenge of defining cyber military objectives." *Israel Law Review*, 48(1), 39-54.

Graham, J.; Howard, R.& Olson, R.(2011): *Cyber Security Essentials.* Taylor and Francis Group, LLC.

Thornton, R., & Miron, M. (2019). "Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom." *Journal of Cyber Policy,* 1-18.

https://www.forcepoint.com/cyber-edu/cloud-security

# Unit 7: Intrusion Detection

## Contents

## 1.0 Introduction

Hostile or unauthorised users or software trespass is a serious security problem for a networked system. User trespass can take the form of unauthorised logon to a machine or, in the case of an authorised user, acquisition of privileges or performance of actions beyond those that have been authorised. This is called intrusion. A software trespass can take the form of a virus, worm, or Trojan horse. The user of the software is referred to as an intruder in this content. This unit covers the subject of intrusion detection system. First, I am going to explain the concept of Intrusion detection. After this, Intruder pattern of behaviour, principles and requirements of intrusion detection and intrusion detection techniques will be discussed.

## 2.0 Intended Learning Outcomes (ILOs)

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

- distinguish among various types of intruder behaviour patterns
- explain the principles of and requirements for intrusion detection
- discuss the key features network-based and host-based intrusion detection systems.

# 3.0 Main Content

## 3.1 Understand Intrusion Detection Systems

Intrusion Detection Systems (IDS) are an essential component of defensive measures protecting the computer system and network against harm abuse. IDS can also be defined as a device or software application that monitors network and or system activities for malicious activities or policy violations and produces reports to the management station or administrator. The main idea of IDS is to detect attacks and provide the proper response. IDS can also be defined as the technique that is used to detect and respond to intrusion activities from network or host. In other words, IDS is hardware and/or software mechanisms that detect and log inappropriate, incorrect, or anomalous activities and report these for investigations. The following are the three components in IDS:

1. **Sensors**: they sense the network traffic or system activity and generate events.

2. **Console**: monitors events and alerts and control the sensors.

3. **Detection engine**: records events logged by the sensors in a database and uses a system of rules to generate alerts from the received security events.

## 3.2 Types of Intruder Behaviour patterns

The behaviour patterns of intruders are constantly changing, to exploit newly discovered vulnerabilities and to evade detection and countermeasures. A security administrator needs to have knowledge of behaviour patterns of intruders. In the following sub-section, I am going to discuss three types of intruder behaviour patterns.

### 3.2.1 Hackers Patterns of Behaviour

In most cases, those who hack into computers do so for the thrill of it or for status. The hacking community is a strong meritocracy in which status is determined by the level of competence. Hence, attackers often look for targets of opportunity and then share the information with others. The following are some examples of Hacker pattern of behaviour.

- Select the target using IP lookup tools such as NS Lookup, Dig, and others.
- Map network for accessible services using tools such as NMAP.
- Identify potentially vulnerable services (in this case, pcAnywhere).
- Brute force (guess) pcAnywhere password.
- Install remote administration tool called DameWare.
- Wait for the administrator to log on and capture his password.
- Use that password to access the remainder of the network.

**What can be done by organisations to counter this type of hacker?**
Intrusion detection systems and intrusion prevention systems (IPSs) are designed to counter this type of hacker threat. Let me use this medium to inform you that, in our next unit, I shall discuss IPSs. So don't worry yourself about IPSs for now. In addition to using IDSs and IPSs, systems, organisations can consider restricting remote logins to specific IP addresses and/or use virtual private network technology.

### 3.2.2 Criminals Patterns of Behaviour

Organised groups of hackers have become a widespread and common threat to Internet-based systems. These groups can be on the payroll of a corporation or government but often are loosely affiliated gangs of hackers. These gangs meet in underground forums with names like "DarkMarket.org" and "theftservices.com" to trade tips and data and coordinate attacks. A common target is a credit card file at an e-commerce server. Attackers attempt to gain root access. The card numbers are used by organised crime gangs to purchase expensive items and are then posted to carder sites, where others can access and use the account numbers; this obscures usage patterns and complicates the investigation. Whereas traditional hackers look for targets of opportunity, criminal hackers usually have specific targets, or at least classes of targets in mind. Once a site is penetrated, the attacker acts quickly, scooping up as much valuable information as possible and exit. The following are some examples of a criminal pattern of behaviour.

- Act quickly and precisely to make their activities harder to detect.
- Exploit perimeter through vulnerable ports.
- Use Trojan horses (hidden software) to leave back doors for reentry.
- Use sniffers to capture passwords.
- Do not stick around until noticed.
- Make a few or no mistakes.

IDSs and IPSs can also be used for these types of attackers but may be less effective because of the quick in-and-out nature of the attack.

### 3.2.3 Insider Attacker Patterns of Behaviour

Insider attacks are among the most difficult to detect and prevent. Employees already have access to and knowledge about the structure and content of corporate databases. Insider attacks can be motivated by revenge or simply a feeling of entitlement. The following are some examples of Insider attacker pattern of behaviour:

- Create network accounts for themselves and their friends.
- Access accounts and applications they wouldn't normally use for their daily jobs.
- E-mail former and prospective employers.
- Conduct furtive instant-messaging chats.
- Visit Web sites that cater to disgruntled employees, such as f'dcompany.com.
- Perform large downloads and file copying.
- Access the network during off-hours.

## 3.3 Principles and Requirements of Intrusion Detection System

Some principles are requirements for the implementation of any intrusion detection system. Intrusion prevention such as authentication facilities, access control facilities, and firewalls all play a role in countering intrusions. In case of failure in any of these intrusion preventions, another line of defense is intrusion detection. Intrusion detection system offers the following benefits:

- If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
- An effective IDS can serve as a deterrent, thus acting to prevent intrusions**.**
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen intrusion prevention measures.

However, there are some requirements for any IDS. These requirements are listed below. IDS must:

- Be running continually with minimal human supervision.
- Be fault tolerant in the sense that it must be able to recover from system crashes.
- Resist subversion. The IDS must be able to monitor itself and detect if an attacker has modified it.

- Impose a minimal overhead on the system where it is running.
- Be able to be configured according to the security policies of the system that is being monitored.
- Be able to adapt to changes in system and user behaviour over time.
- Be able to scale to monitor a large number of hosts.
- Provide graceful degradation of service in the sense that if some components of the IDS stop working for any reason, the rest of them should be affected as little as possible.
- Allow dynamic reconfiguration; that is, the ability to reconfigure the IDS without having to restart it.

## 3.4 Intrusion Detection Techniques

According to a source of data, IDS can be classified into two categories. These categories are Host-Based Intrusion Detection Systems (HIDSs) and Network-Based Intrusion Detection Systems (NBIDS).

### 3.4.1 Host-Based Intrusion Detection Systems

HIDSs are applications that reside on a single system or host and filter traffic or events based on a known signature list for that specific operating system. Host-Based Intrusion Detection Systems add a specialised layer of security software to vulnerable or sensitive systems. The HIDS monitors activity on the system in a variety of ways to detect suspicious behaviour. In some cases, an IDS can halt an attack before any damage is done. In other words, HIDSs detect intrusion activity at the host side. HIDSs include Norton Internet Security and Cisco Security Agent (CSA). Many worms and Trojans can turn off a HIDS. HIDSs can also be installed directly on servers to detect attacks against corporate resources and applications. Its primary purpose is to detect intrusions, log suspicious events, and send alerts.

### 3.4.2 Network-Based Intrusion Detection Systems

Network-Based Intrusion Detection Systems (NIDSs)are software-based appliances that reside on the network. They’re used solely for intrusion detection purposes to detect all types of malicious network traffic and computer usage that can’t be detected by a conventional firewall. This includes network attacks against vulnerable services; data attacks on applications; host-based attacks such as privilege escalation, unauthorised logins, and access to sensitive files; and malware. In other words, Network-based intrusion detection systems detect intrusion activity at the network side. This is done by sniffing packets from networks and passes it to detection engine. Network-based intrusion detection systems are passive. In comparison with host-based intrusion detection systems, Network-based intrusion detection systems are not able to process encrypted payload but can captures data from the entire network as compared to few hosts in case of HIDS.

## 4.0 Self-Assessment Exercise(s)

1. A component in IDS which senses the network traffic or system activity and generate events is referred to as………

A. Console

B. Sensor

C. Detecting engine

D. Network analyser

**Answer: B**

2. The two categories of intrusion detection techniques are

A. Host Base Intrusion Detection Systems

B. Device Base Intrusion Detection Systems

C. Component Base Intrusion Detection Systems

D. Network Base Intrusion Detection Systems

**Mini project**

An organisation approached you to make a presentation on how the intrusion detection system will be of benefits to the organisation since they are suffering from consistent intrusion attack. Write a proposal for this purpose.

## 5.0 Conclusion

Any form of user trespassing into a system or network is called an intrusion. User trespass can take the form of unauthorised logon to a machine or, in the case of an authorised user, acquisition of privileges or performance of actions beyond those that have been authorised. In any case, this is called Intrusion. Hence, intrusion detection becomes necessary. In this unit, I have discussed intrusion detection system. I also have explained different types of Intruder behaviour patterns which include hacker patterns of behaviour; criminal patterns of behaviour; and insider attacker patterns of behaviour. Similarly, I discussed the principles and requirements of the intrusion detection system and concluded with the discussion on different types of intrusion detection techniques.

## 6.0 Summary

You have learnt from this unit about Intrusion Detection Systems. You have also learnt different types of Intruder behaviour patterns such as hacker patterns of behaviour; criminal patterns of behaviour; and insider attacker patterns of behaviour. Also, you have learnt the principles and requirements of the intrusion detection system and different types of intrusion detection techniques.

## 7.0 References/Further Reading

Andress, J., & Winterfeld, S. (2013*). Cyber Warfare: Techniques, Tactics and Tools For Security Practitioners*. Elsevier.

Carr, J. (2011). *Inside Cyber Warfare: Mapping The Cyber Underworld*. O'Reilly Media, Inc.

Dinniss, H. A. H. (2015). “The nature of objects: Targeting networks and the challenge of defining cyber military objectives.” *Israel Law Review*, 48(1), 39-54.

Van Puyvelde, D., & Brantly, A. F. (2019). *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. John Wiley & Sons.

# Unit 8: Firewall and Intrusion Prevention Systems

## Contents

## 1.0 Introduction

The previous unit is on intrusion detection. In this unit, you will learn about firewalls and intrusion prevention systems. These comprise of explanation of firewall, firewall policies, policy actions, blacklists and white lists, types of firewalls, intrusion prevention system, differences between firewall and intrusion prevention system.

## 2.0 Intended Learning Outcomes (ILOs)

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

- explain the role of firewalls as part of a computer and network security strategy
- discuss the various basing options for firewalls
- distinguish between firewalls and intrusion prevention systems.

## 3.0 Main Content

## 3.1 Firewall Explained

A firewall is a network security device that monitors departing and arriving network traffic-flow and selects whether to allow or block precise traffic based on a distinct set of security guidelines. A firewall is a combined assembly of security procedures planned to avoid illegal electronic entree to a networked computer system. A network firewall is likening to firewalls in building construction. This is because in both cases, they are envisioned to separate one "network" or "compartment" from another.

### 3.1.1 Firewall Policies

A firewall can be hired to sieve incoming or outgoing traffic based on a predefined set of guidelines called firewall policies. This is to guard private networks and distinct machines from the hazards of the greater Internet, as shown in figure 3.1.

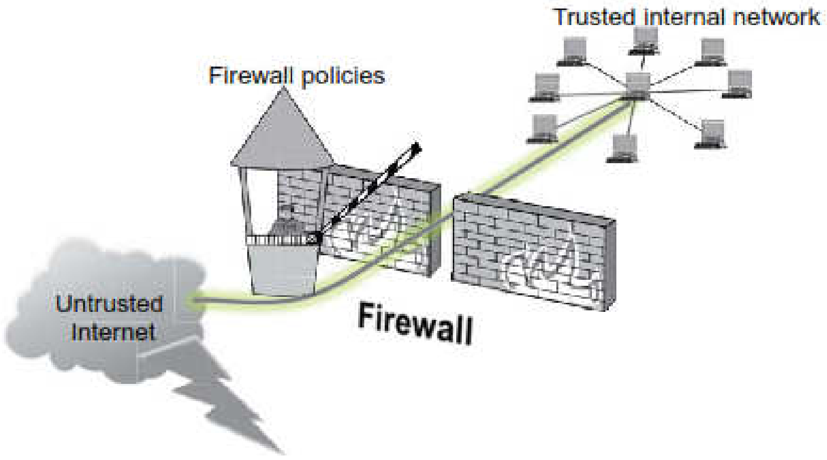


**Fig. 3.1: Firewall Policies Diagram**

### 3.1.2 Policy Actions

Packets flowing over a firewall might have one of three results:

(i) Accepted: allowable over the firewall.
(ii) Dropped: not allowable over firewall, with no sign of failure.
(iii) Rejected: not permitted over firewall, escorted by an effort to notify the source that the packet was forbidden.

Firewal policies used to handle packets are originated on many properties of the packets being checked, comprising the protocol utilized, like the following:

(a) Transmission Control Protocol (TCP) or UDP – the destination and source IP addresses
(b) the destination and source ports
(c) the application-level payload of the packet (like, whether it comprises a virus).

### 3.1.3 Blacklists and White Lists

There are two important methods to producing firewall policies (or rulesets) to efficiently lessen vulnerability to the external world even though preserving the anticipated functionality for the machineries in the reliable interior network (or separate computer).

(i) Black-list method: Excluding those that are suitable to the rules defined precisely in a blacklist, all packets are allowed through. This kind of configuration is extra flexible in guaranteeing that service to the interior network is not disturbed by the firewall, but is naïve from a security perspective in that it assumes the network administrator can count all of the properties of hateful traffic.
(ii) White-list method: A harmless method to setting a firewall ruleset is the default-deny policy, in which packets are rejected or dropped unless they are precisely permitted by the firewall.

## 3.2 Types of Firewalls

### 3.2.1 Proxy Firewall

A proxy firewall is an initial kind of firewall device which serves as the gateway from one network to another for a precise application. Proxy servers can offer additional functionality like content security and caching by discontinuing direct connections from external the network. Nonetheless, this also may influence throughput capabilities and the applications they may support.

### 3.2.2 Stateful Inspection Firewall

A stateful inspection firewall now thought of as a "traditional" firewall, allows or blocks traffic based on port, state, and protocol. It monitors all action from the starting of a connection until it is locked. As shown in figure 3.2, filtering decisions are made based on both administrator-defined guidelines as well as context, which signifies to using information from preceding connections and packets belonging to the similar connection.

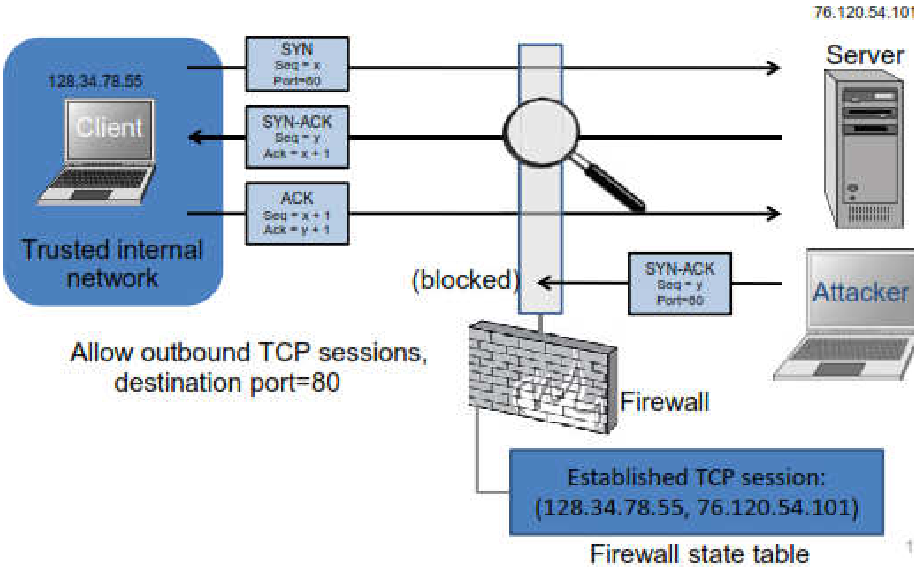


**Fig. 3.2: Stateful Inspection Firewall Diagram**

### 3.2.3 Unified Threat Management (UTM) Firewall

In a roughly coupled method, a UTM device classically combines the purposes of a stateful inspection firewall with intrusion prevention and antivirus. It may also encompass extra services and regularly cloud management. UTMs focus on ease and easiness of use.

**What do you understand by the term firewall?** A firewall is a network security device that monitors outgoing and incoming network traffic and chooses whether to block or allow specific traffic based on a well-defined set of security rules. A firewall is an integrated assembly of security procedures designed to avoid illegal electronic access to a networked computer system.

### 3.2.4 Next-Generation Firewall (NGFW)

Firewalls have changed outside simple stateful inspection and packet filtering. Most enterprises are deploying next-generation firewalls to block contemporary threats like advanced malware and application-layer attacks.

Gartner, Inc. defined a next-generation firewall to comprise:

a) Standard firewall competences such as stateful inspection
b) Integrated intrusion prevention
c) Application awareness and control to block and see risky apps
d) Upgrade paths to comprise upcoming information feeds
e) Methods to address developing security threats

Whereas these competencies are progressively becoming the standard for most corporations, NGFWs can do more.

### 3.2.5 Threat-Focused NGFW

These firewalls comprise all the competencies of a old-style NGFW and likewise offer progressive threat detection and remediation. With a threat-focused NGFW you can:

1) Distinguish which assets are greatest at risk with comprehensive context-awareness.
2) Rapidly respond to attacks with brainy security automation that hardens your defences and sets policies dynamically.
3) Well identify suspicious or elusive activity with endpoint and network event correlation.
4) Importantly decline the time from discovery to cleanup with reflective security that constantly monitors for suspicious action and behaviour even after the initial inspection.
5) Reduce complexity and ease administration with combined policies that guard across the whole attack continuum.

## 3.3 Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that scrutinises network traffic movements to avoid and identify vulnerability exploits. Vulnerability exploits classically originated in the form of malicious inputs to a service or target application that attackers use to interject and gain regulator of an application or a machine. Following a successful exploit, the attacker can incapacitate the target application (resultant in a denial-of-service state), or can perhaps access to all the consents and rights available to the conceded application.

### 3.3.1 Prevention

The IPS frequently sits straight after the firewall and offers a balancing layer of analysis that harmfully chooses for risky content. Different from its precursor the Intrusion Detection System IDS (which is a passive system that scans traffic and reports back on threats), the IPS is located aligned (in the direct communication track amid destination and source). It vigorously takes and analyses automated actions on entirely traffic flows that enter the network. Precisely, these activities encompass:

a) Transfer an alarm to the administrator (as would be seen in an IDS)
b) Dropping the malicious packets
c) Obstructive traffic from the source address
d) Resetting the connection

The IPS as an inline security constituent, must work proficiently to avoid degrading network performance. Also, it must work fast since exploits can occur in near real-time. Also, the IPS must respond and identify exactly, so as to eliminate threats and false positives (legitimate packets misjudged as threats).

### 3.3.2 Detection

A quantity of detection techniques for discovery exploits are in IPS, but statistical anomaly-based detection and signature-based detection are the two foremost mechanisms.

**Signature-based detection** is built on a dictionary of characteristically recognizable patterns (or signatures) in the code of respectively exploit. As an exploit is exposed, its signature is logged and kept in a constantly rising dictionary of signatures. Signature detection for IPS breakdowns into two kinds:

1. Exploit-facing signatures classify separate exploits by activating on the distinctive patterns of a specific exploit attempt. The IPS can recognize precise exploits by discovery a match with an exploit-facing signature in the traffic stream
2. Vulnerability-facing signatures are wider signatures that target the fundamental vulnerability in the system that is being targeted. These signatures permit networks to be protected from alternates of an exploit that may not have been directly observed in the wild, but also upsurge the risk of false positives.

**Statistical anomaly detection** takes examples of network traffic at chance and compares them to a pre-calculated reference point performance level. When the model of network traffic action is outdoor the parameters of reference point performance, the IPS takes action to handle the circumstances.

IPS was initially built and out as a standalone device in the mid-2000s. This, though, was in the advent of today’s applications, which are now normally combined into Unified Threat Management (UTM) solutions (for medium-sized and small companies) and next-generation firewalls (at the enterprise level).

## 3.4 Differences between Firewall and IPS

**Firewall**: A contemporary firewall is a rules-based engine that scrutinises packet header on source address, protocol kind, a destination address, destination port, and source port. Packets will be dropped, if the packets are not matched with firewall rules. There is somewhat called a Next-Generation Firewall (NGFW). This can make a sole device act as both a traditional Firewall and IPS.

**Intrusion-Prevention System** (IPS): The IPS positions among your firewall and the remain of your network meanwhile, the suspected traffic from getting to the rest of the network can stopped. The IPS screens the incoming packets and what they are actually being utilized for before decisive to let the packets into the network. An IPS will inspect contents of the request and be able to drop, alert, or perhaps clean a malicious network request based on that content. The willpower of what is malicious is based either on through the use of signatures or behaviour analysis.

Discussion

As the want for application consciousness rose, numerous vendors added application perceptibility and other hardware or software 'blades' into their stateful inspection firewall and traded the offering as a Unified Threat Management (UTM). UTMs did not improve security because the functions were retrofitted into the firewall, and not natively integrated.

Different from UTM, a Next Generation Firewall is application aware and makes decisions based on user, application and content. It's simply integrated plan streamlines operation and advances security. Given its achievement, the term NGFW has now become identical with firewall. Can you say that NGFW are intelligent firewalls?

# 4.0 Self-Assessment Exercise(s)

(1) Explain when you think the intrusion prevention system will take action on the traffic in a network? ___________________________

Answer:
Statistical anomaly detection takes samples of network traffic at random and likens them to a pre-calculated baseline performance level. When the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation.

## 5.0 Conclusion

In this unit, you have learnt about the meaning of firewall. You also learnt about the firewall policies, policy actions, blacklists and white lists, types of firewalls, intrusion prevention system. The unit also covered the differences between firewall and intrusion prevention system.

## 6.0 Summary

This unit explained firewall, firewall policies, policy actions, blacklists and white lists. The unit also covers types of firewalls such as proxy firewall, stateful inspection firewall, Unified threat management (UTM) firewall, Next-generation firewall (NGFW) and threat-focused NGFW. The unit also covers Intrusion Prevention System (IPS), prevention and detection. Finally, the unit explained the differences between firewall and IPS.

## 7.0 References/Further Reading

Ashoor A. S. & Gore, S. (2011). "Importance of Intrusion Detection System (IDS)", *International Journal of Scientific and Engineering Research*, vol 2, issue 1.

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Hils, A., D'Hoinne, J., & Kaur, R. (2017).*Magic Quadrant for Enterprise Network Firewalls*. Gartner.

Sandhu, U. A., Haider, S., Naseer, S. & Ateeb, O. U. (2011). "A Survey of Intrusion Detection and Prevention Techniques", International Conference on Information Communication and Management IPCSIT: IACSIT Press, Singapore.

Scarfone, K. & Mell, P. (2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)." Recommendations of the National Institute of Standards and Technology: NIST Special Publication, February 2007.

Verizon (2017). *Data Breach Investigation Report*. Retrieved from https://www.knowbe4.com/hubfs/rp

# Module 2: Software Security and Trusted Systems

## Module Introduction

In module 1 you learnt about security technology and principles, which comprises security fundamentals, user authentication, cryptography tools, access control, Malicious software, database and cloud security, intrusion detection, firewall and intrusion prevention systems. This module has to do with software security and trusted systems. It covers software security and operating system security. This module is made up of two (2) units.

Unit 1: Software Security
Unit 2: Operating System Security

## Unit 1: Software Security

### Contents

# 1.0 Introduction

In this unit, you will learn about software security. You will also learn about how programming practices lead to vulnerability, software vulnerabilities, a computer program with potential points of vulnerability, starting exploits, defensive programming approach and problems with defensive programming.

# 2.0 Intended Learning Outcomes (ILOs)

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

- examine how programming practices lead to vulnerability
- describe an abstract view of a program, and detail where potential points of vulnerability exist in this view
- discuss the defensive programming approach.

# 3.0 Main Content

## 3.1 Software Security Explained

Software security is about the procedure of designing, constructing, and testing software for security. It contains taking the pro-active method in building security into the software as opposite to securing it afterward building it. It is all about building secure software. What it means for software to be secure is the key issue. One probable definition is that a software system is secure if it satisfies a specified or an implied security objective. This security objective specifies confidentiality, integrity and availability necessities for the system's functionality and data. Reflect, for instance, a social networking service. The security objective of such a system might comprise the succeeding necessities:

(i) Pictures sent by a user might only be gotten by that user's friends (confidentiality).
(ii) A user might like any given post at most once (integrity).
(iii) The service is working more than 99.9% of the time on regular (availability).

Diverse security necessities might be at probabilities with apiece other, for instance, barring down a system on the appearance of an attack is good for integrity and confidentiality of the system, but bad for availability.

## 3.2 How Programming Practices Lead to Vulnerability

The quantity of software systems is growing each day, so also the number of vulnerabilities. A software vulnerability might be alleged as a flaw, weakness or even a fault in the system that might be exploited by an attacker in order to adjust the usual behaviour of the system. Additionally, if you reflect that most of the systems are unprotected to numerous users (internet) and surroundings (operating systems for example), then it is just a matter of time that someone might launch an attack (sequence of actions) whose consequences are unpredictable in cost and damages. Generally, the aim of an attacker is to gain some rights in the system to obtain valuable information for his own return or take control of it. Then it is important for the general public and the developers to know about vulnerabilities and their detection and prevention.

### 3.2.1 Software Vulnerabilities

Attackers can exploit a vulnerable software system and the system might be conceded. The attacker may take control of the system to damage it, to launch new attacks or get some privileged information that might be used for personal profit. It is significant to know in view of this, the varied kinds of vulnerabilities, their detection and prevention in order to try to evade their existence in the last software version of the system and then decrease the likelihood of costly damages and attacks.

Utmost of the known vulnerabilities are connected to an improper way of dealing with the inputs provided by a user of the system; if these inputs are not correctly treated before using them within the program, they can yield unforeseen behaviour of the system. For instance, some recognized and recurrent vulnerabilities are:

1) **Buffer overflow**: it typically arises with fixed-length buffers as soon as some data is going to be written above the limits of the present defined ability. This might lead to malfunctioning of the system because, the new data might corrupt the data of other processes or buffers. The buffer overflow can also be used to insert malicious code, and then the execution order of the program may be changed in order to execute the injected code and take control of the system.
2) **XSS or cross-site scripting**: typically related with web applications, contains in the insertion of code in the pages accessed

by other users. If exploited, an attacker can do phishing, avoid access controls, expose connections or identity theft.

3) **SQL injection**: it contains in the inoculation of code with the intension of exploiting the content of a database. Typically occurs since the inputs are not held properly; the attacker might get delicate information from the database.

Nevertheless, some other popular vulnerabilities that might be stated are:

1. **Format string bugs**: it occurs when exterior data is supplied to an output function as a format string argument. The output function, for example, *printf* in C language, produces an output according to the stipulations of the format string, some directives can write to memory locations. Hence the attacker can use the *printf* to write malicious code and alter the control flow to execute it.
2. **Integer overflows**: might be of two varied kinds, arithmetic overflows and sign conversion bugs. The second ensues when a signed integer is transformed to an unsigned integer; while in the first the result of an arithmetic operation is an integer greater than the maximum integer, and it is stored in an integer variable.

## 3.3 Computer Program with Potential Points of Vulnerability

A computer program is secure when it exactly does what it supposed to do. A program is secure when it does not do bad things. Bad things can include; deleting or corrupting important files; crash the system; send user's password over the Internet and send threatening e-mail to others.
Intricate systems virtually continuously comprise unintentional functionality "weird machines". An **exploit** is a mechanism by which an attacker triggers unintended functionality in the system. Security desires understanding not just the envisioned, but also the unintentional functionality current in the implementation such as developers' blind spot, which is the attackers' strength.

**Explain the key issue of what it means for software to be secure**? One likely definition is that a software system is secure if it satisfies implied or a specified security objective - this security objective specifies confidentiality, integrity and availability requirements for the system's data and functionality. Consider, for instance, a social networking service.

### 3.3.1 Starting Exploits

You start with low-level details of how exploits work. How can a remote attacker get **your** machine to execute **their** code?

The threat model:
Victim code is **handling input** that comes from across a security boundary

Instances:
Image viewer, word processor, web browser.
You want to protect the integrity of execution and confidentiality of internal data from being compromised by malicious and highly skilled users of our system.

Simplest instance: **buffer overflow:**
Provide input that ”overflows” the memory  the program has allocated for it

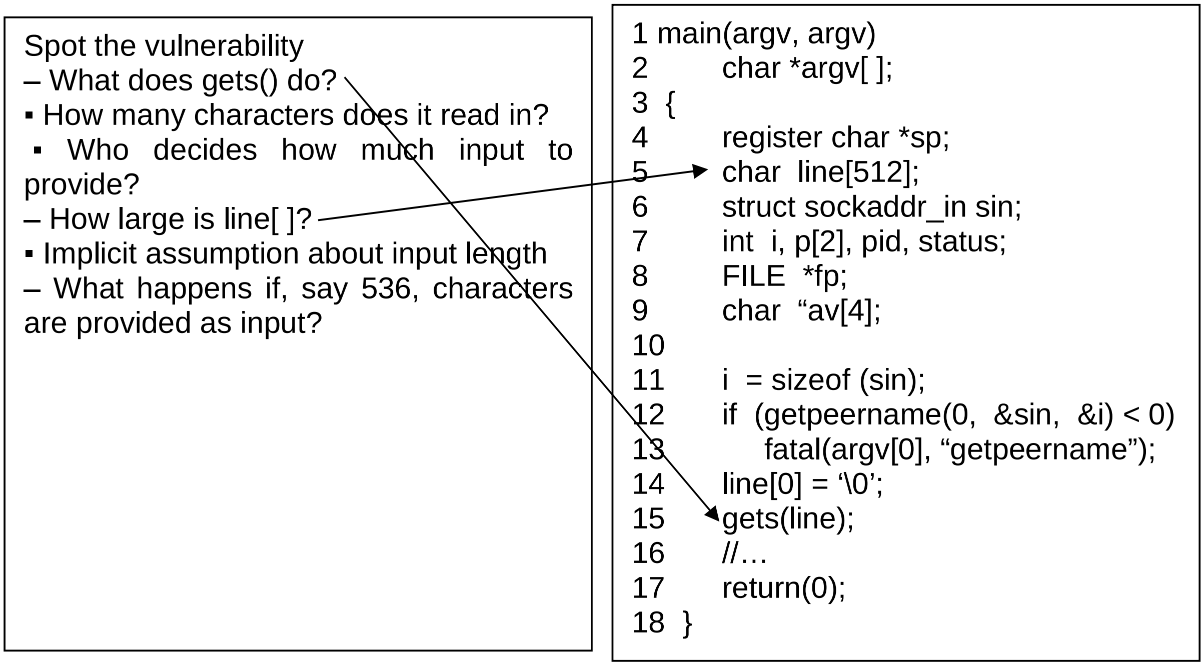
Buffer Overflow is an anomaly that occurs when a program writes data beyond the boundary of a buffer.

Archetypal software vulnerability. Ubiquitous in system software (C/C++).
Operating systems, web servers, web browsers, embedded systems, etc.
If your program crashes with memory faults, you probably have a buffer overflow vulnerability.

A rudimentary core concept that allows a broad range of likely attacks – Occasionally a single byte is all the attacker needs.

An ongoing arms race between defenders and attackers – Co-evolution of defences and exploitation techniques.
Note the followings:

1) No automatic bounds checking in C/C++. Developers should know what they are doing and check access bounds where necessary.
2) The problem is made more acute/more likely by the fact many C standard library functions make it easy to go past array bounds.
3) String manipulation functions like gets(), strcpy(), and strcat()all write to the destination buffer until they encounter a terminating ‘\0’ byte in the input. – Whoever is providing the input (often from the other side of a security boundary) controls how much gets written



Spot the vulnerability
– What does gets() do?
▪ How many characters does it read in?
▪ Who decides how much input to provide?
– How large is line[ ]?
▪ Implicit assumption about input length
– What happens if, say 536, characters are provided as input?

```
main(argv, argv)
        char *argv[ ];
{
        register char *sp;
        char  line[512];
        struct sockaddr_in sin;
        int  i, p[2], pid, status;
        FILE  *fp;
        char  "av[4];

        i  = sizeof (sin);
        if  (getpeername(0,  &sin,  &i) < 0)
            fatal(argv[0], "getpeername");
        line[0] = '\0';
        gets(line);
        //…
        return(0);
}
```

**Avoiding Buffer Overflows**

(i) Train the developers to write secure code.
− Provide developers with tools that make it easier to write secure code.

(ii) Avoiding buffer overflow vulnerabilities requires validating the lengths of untrusted input before performing read or write operations into buffers.

(iii) Common libc string functions do not encourage this practice and make it easy to introduce buffer overflow vulnerabilities.

(iv) However, better alternatives are available.

(v) Aside: default ways of doing something are often insecure.

Investigate security aspects of tools, frameworks, libraries, APIs, that you are using and understand how to use them safely.

## 3.4 Defensive Programming Approach

Defensive coding or defensive programming is a style of writing computer software that tries to be extra tough in the occasion of unforeseen behaviour. Generally, this unexpected behaviour is measured to be an outcome of existing bugs in the software but can be due to other problems for example, hardware failures, corrupted data, or even bugs introduced by later software changes. Normally, the code attempts to do the most sensible thing with no or little performance consequence and without adding new error-conditions.

Instance: The archetypal example of defensive programming rises in just about all C program ever written, wherever the terminating condition is written as a test for inequality ( < ) rather than a test for non-equality ( != ). For example, a typical loop is written like this:

```
size_t len = strlen(str);
for (i = 0; i < len; ++i)
    result += evaluate(str[i]);
```

rather than this:

```
size_t len = strlen(str);
for (i = 0; i != len; ++i)
    result += evaluate(str[i]);
```

Obviously, these both should do exactly the same thing, because the variable 'i' is only ever incremented and might not ever skip having the same value as 'len'. Thus why are loop end conditions continually written in the first manner?

Initial, the penalties of the "impossible" condition are bad, maybe resultant in all kinds of unwanted consequences in production software, for example an infinite loop or a memory access violation. The "impossible" condition might happen for any number of explanations such as:

i) Bad hardware or a wandering gamma ray photon means that one of the bits of 'i' is flipped arbitrarily.

ii) Extra errant procedure (in a system without hardware memory protection) or thread changes memory that does not fit to it.

iii) Bad supervisor level code (for instance, a device driver or the operating system) changes the memory.

iv) The 'evaluate' function has a rogue pointer that changes the value of 'i'.

v) The 'evaluate' function corrupts the stack frame pointer and the location of 'i' is now at some random place on the stack.

vi) later code changes introduce bugs, for instance:

```
    for (i = 0; i != len; ++i)
    {
        while (!isprint(str[i]))          // bad code change means that 'i'
may never be equal to 'len'
            ++i;
        result += evaluate(str[i]);
    }
```

The last few of course, caused by bugs are the most popular in the software, which is the reason defensive programming is typically connected to protecting against bugs.

### 3.4.1 Scope

A portion of the misperception around defensive programming originates about since the scope of control is not constantly clearly defined. For instance, if you have a function that takes a string (const char *) parameter, if it never makes sense to do so, you may want to assume that you are never passed a NULL pointer. If it is a private function you may be able always to safeguard it; but you can't assume that unless you clearly document that a NULL pointer may not be used, if its use is outside the scope of your control.

If you anticipate the condition to be unbearable, in any case, it is wise to allow for the likelihood of using defensive programming. If unexpectedly passed a NULL pointer, many functions do this by simply returning.

### 3.4.2 Symptoms

The signs of defensive programming are seen frequently, when using buggy software, (but may be discharged as operator fault). Like flash a window, everybody has at some time seen software that did something a little strange, disregard a command or even show a message about an "unknown error". Classically this is produced by a bug which triggered a problem from which the software tried to recover.
This recovery might occasionally be fruitful but classically outcomes in the program limping along. It can silently cause huge difficulties in the worst case, like corruption or data loss.

### 3.4.3 Problems with Defensive Programming

It is pretty clear that defensive programming has a main problem. It hides the existence of bugs. Many people might reason it is good to hide bugs. Surely, for released software in use, you do not need to force the user to deal with a problem that they do not understand. Sloppily enduring on the other hand, when something is broken can be hazardous. Similarly, some effort should be made to inform someone of the problem - at least write a fault message to a log file.

Though, what is worse is that defensive coding has been identified to hide bugs throughout development and testing. Nobody might contend that this is a decent thing. The alternate is to use what has been called "offensive programming" and occasionally "fail fast". This means to make sure someone recognizes about problems rather than hiding them.

Discussion

Thus any conversation of defensive programming must evidently describe the scope of the code being well-thought-out. This is unique problem with some of the article on defensive programming. Is there any difference to error-handling since no error value is generated?

## 4.0 Self-Assessment Exercise(s)

(1) Explain how you can address buffer overflow.

Answer:

- The best way to deal with any bug is not to have it in the first place.
  - Use memory-safe languages.
  - Train the developers to write secure code and provide them with tools that make it easier to do so.
- Language choice might not be an option (it frequently isn't), and people still make mistakes. So, we must also be able to find these bugs and fix them.
  - Manual code reviews, static analysis, adversarial testing, etc.
  - More on this later in the course.
- Failing all of the above, make remaining bugs harder to exploit.
  - Introduce countermeasures that make reliable exploitation harder or mitigate the impact

(2) What should be the security objective of a secure software?

Ans:

The security objective of such a system could comprise the following requirements:

(i) Pictures posted by a user can only be seen by that user's friends (confidentiality).

(ii) A user can like any given post at most once (integrity).

(iii) The service is operational more than 99.9% of the time on average (availability).

## 5.0 Conclusion

In this unit, you have learnt that software security is about the process of designing, building, and testing software for security. You also learnt about how programming practices lead to vulnerability, software vulnerabilities, a computer program with potential points of vulnerability, starting exploits, defensive programming approach and problems with defensive programming.

The next unit is on operating system security.

## 6.0 Summary

This unit explained software security. It also covers how programming practices lead to vulnerability, software vulnerabilities, a computer program with potential points of vulnerability, starting exploits, defensive programming approach and problems with defensive programming.

## 7.0 References/Further Reading

Meer, H. (2010). *Memory Corruption Attacks: The Almost Complete History*. , Black Hat USA. Retrieved from http://www.youtube.com/watch?v=stVz9rhTdQ8 ▪ Code Injection in C and C++ :

Piessens, F. Younan, Y. & Joosen, W. (2019). *A Survey of Vulnerabilities and Countermeasures.* Retrieved from https:// www.cs.kuleuven.be/publicaties/rapporten/cw/CW386.pdf

Peter S. D. (2019). *An Introduction to Computer Networks* Retrieved from http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf.

https://devmethodologies.blogspot.com/2012/05/defensive-programming.html.

Robert C. S. (2018): *Secure Coding in C and C++* (2nd ed.). U.S.A.

# Unit 2: Operating System Security

## Contents

## 1.0 Introduction

The previous unit 1 is on software security. In this unit, you will learn about how to secure a system, techniques for securing the Operating System (OS) such as user accounts, account policies, file system, network services, system patches, OS minimisation, logging and monitoring as well as system integrity. You will also learn about the need for planning system security.

## 2.0 Intended Learning Outcomes (ILOs)

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

- describes the steps for securing a system.
- examine the need for planning system security.

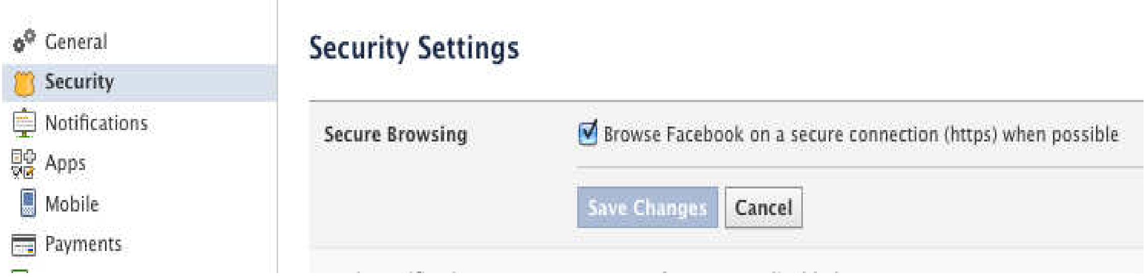
# 3.0 Main Content

## 3.1 How to Secure a System

The following describes how you can secure your system:

**a. Encrypt your network connection**

At least some of the time, best general sites concession HTTPS connections. In Gmail, click the gear icon in the top-right corner and select "Always use https" under the General tab. To select Facebook's HTTPS setting, click the down arrow in the top-right corner and choose Account settings. Select Security in the left pane and Edit in the Secure Browsing section of the main window. Check "Browse Facebook on a secure connection (https) when possible" and click Save Changes to activate the feature.



Security Settings

Secure Browsing ☑ Browse Facebook on a secure connection (https) when possible

Choose Facebook's HTTPS option by clicking "Browse Facebook on a secure connection (https) when possible." Screenshot by Dennis O'Reilly

The Electric Frontier Foundation's HTTPS Everywhere extension for Firefox does not encrypt all page you browse to, but it mechanically needs an encrypted connection for those sites that support HTTPS and that have been added to the program's rules. After you install HTTPS Everywhere, the extension's icon appears in the top-right corner of Firefox. Click it to view the encrypted and nonencrypted content served by the current page.

**b. Encrypt sensitive files stored locally**

The file-encryption features assembled into Mac OS and Windows leave plenty to be wanted. The Apple Support site defines Mac OS X 10.6's FileVault encryption feature, and Macworld's Roman Loyola affords a primer on Mac OS Lion's FileVault 2.

**c. Encrypt private information stored in the cloud**

If you request cloud-storage vendors, how safe is the data you store in the cloud? it is.

d. **Use a free VPN service to protect public Wi-Fi connections**

Even though if you only hardly sign in to Web accounts over a public Wi-Fi link, you might stop lurking snoops by means of a free VPN service to secure the connection.

e. **Prevent keystroke loggers, other data snoops**

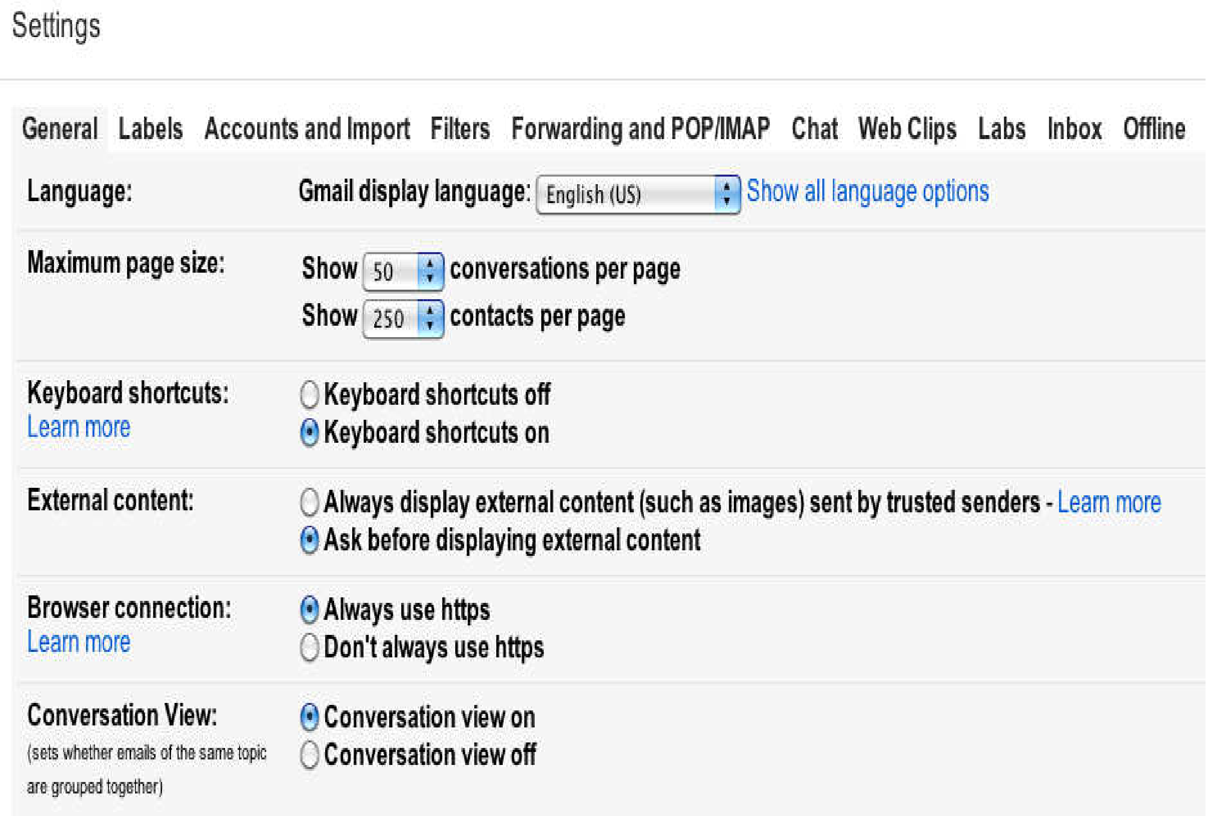
Computer criminals tend to attack the most vulnerable systems by searching for that path of least resistance. Make sure your firewall and real-time antivirus software are at work to evade being one of their victims and keep all your software up-to-date.

f. **Perform a manual virus scan with the free Malwarebytes Anti-Malware**

Even with automatic software updates and regularly arranged malware scans, viruses might sneak over your defences. That is the reason it is a good impression to use Malwarebytes' free Anti-Malware program to scan your system manually.

g. **Disable images in the e-mail**

The persons who send you e-mail may recognize when you open their messages and click links they comprise. Programs for example Zendio posture a grave security threat, mainly in view of that the program also discloses your wide location (through your IP address) when the message is unlocked. To stop e-mail snoops, disable images in your received messages. This evades the HTML beacons used by the detectives from being triggered. In Gmail, click the settings icon in the top-right corner, choose Mail settings, and select "Ask before displaying external content."



Language: Gmail display language: English (US) Show all language options

Maximum page size: Show 50 conversations per page
Show 250 contacts per page

Keyboard shortcuts: Learn more
○ Keyboard shortcuts off
● Keyboard shortcuts on

External content:
○ Always display external content (such as images) sent by trusted senders - Learn more
● Ask before displaying external content

Browser connection: Learn more
● Always use https
○ Don't always use https

Conversation View: (sets whether emails of the same topic are grouped together)
● Conversation view on
○ Conversation view off

Block spying beacons embedded in the messages you receive by setting Gmail to ask before displaying external content. Screenshot by Dennis O'Reilly

h. **Be wary of e-mail attachments**

The current rise in spear-phishing has made it difficult to trust that an e-mail was really sent by the individual whose name appears in the From: field. The safe method to open e-mail attachments: right-click downloaded files and select the option to scan the file manually with whatsoever security program you use.

i. **Use a standard (non-administrator) account in Windows**

When you use your Windows PC nine times out of ten, without installing a new program, altering any settings, or performing some additional action that needs an administrator account. Yet few persons use a standard Windows account, which is one of the best approaches to keep malware from contaminating your system.

j. **Destroy old data**

The last time you recycled a storage device or gave an old computer, you perhaps did not show concern about someone stealing your identity by lifting delicate data off the machine. It may not happen frequently, but it occurs. A safer and simpler way that is just as effective is to run a free secure-erase utility.

## 3.2 Techniques for Securing the Operating System

The physical environment where your application runs is the operating system. The security of the application could be concessioned if there is any vulnerability in the operating system. You make the environment steady by securing the operating system, control access to resources and control outside access to the environment. The physical security of the system is vital. Threats may arise through the Web, but they might also arise from a physical terminal. If an attacker gets physical access to a server, even if the Web access is very secure, breaking into a system is much easier. Appraisal of security policies and recommendations for your operating system. Contemplate implementing the succeeding security best practices.

### 3.2.2 User Accounts

Bound the number of user accounts on the server computers: legacy and unnecessary user accounts increase system complexity and might give system vulnerabilities. The length of time administrators spend on account administration might be reduced by fewer user accounts. Be sure that only a few reliable users have administrative access to the server computers. It easier to maintain accountability with fewer administrators. The administrators must be proficient. For the account that runs the application assign the minimum required access permissions. If attackers get access to the application, they have the consents of the user who runs the application.

**Computer criminals look for that path of least resistance; how can you avoid this?** Computer criminals search for that path of least resistance, so they tend to attack the most vulnerable systems. To avoid being one of their victims, make sure your real-time antivirus and firewall software are working, and retain all your software up-to-date.

### 3.2. 2 Account Policies

Administer and develop password policies that aid operating system security. Examples of such policies are the password change schedule and the robust password rule. By breaking the passwords, you can test the strength of users' passwords. The users who do not conform with the strong password rule obtain a notification to update their passwords according to the organization password policy. To help you with this task, software is obtainable. Activate the shadow password file, on a UNIX operating system. Passwords are stored in the /etc/password file on UNIX. Everyone which presents a security risk, this file is open to. Activate the shadow password file named /etc/shadow, to improve password security. If this file is obtainable, passwords are kept in it in its place of the password file. Since consents for the /etc/shadow file are more preventive, the security risk is lesser.

### 3.2.3 File System

Offer the users read-only consents for compulsory directories. If attackers obtain access to an application, they have user consents. Disprove access by default.

Access to resources is denied for single and entirely apart from for the users to whom access is permitted openly. For all directory structures for all users, you can refute write and read permissions. Solitary users to whom these consents are approved explicitly have access to the files and directories. This policy also defends any resources that were ignored by an administrator.

### 3.2.4 Network Services

On the server computer, network services offer the minimum number of required services. Only the services that you need to run the application should be used. Entry point for a malicious attack is a possible by each service. Your system is extra manageable by decreasing the quantity of running services. For instance, you might not need the rlogin, ftp or ssh services. Decline the level of access consents for the network services users.

Network services are noticeable to the public. Assurance that the user accounts that have access to the Web server do not have entree to the shell functions. Verify that unused services do not happen in the rc0 through to rc6, rc files, in the /etc directory on Linux and UNIX operating systems. Verify that idle services are not working and that they do not start mechanically on Microsoft Windows operating systems. Verify that obligatory services are running on UNIX. You can use the netstat and ps utilities to see the running services. The ps utility gives a list of procedures presently running on the computer. The netstat utility offers a list of ports that are presently in use. Decrease the number of reliable ports stated in the /etc/services file.

### 3.2.5 System Patches

Execute the latest, vendor-recommended patches for the operating system. The patches may be core OS patches or patches compulsory by additional applications. Schedule consistent maintenance of security patches.

### 3.2.9 Operating System Minimisation

Eliminate nonessential applications to decline likely system vulnerabilities. Limit local services to the services essential for operation. Implement protection for buffer overflow. Third-party software may be needed to do this.

### 3.2.10 Logging and Monitoring

Log security associated actions, comprising failed and successful logons, logoffs, and differences to user consents. Monitor system log files. Use a time server to relay time for forensics. Safe the system log files by curbing access consents to them. Logs are important for everyday maintenance and as a disaster recovery tool. Hence, they must be protected from system failures and user altering. Use IPF logging to build a more sophisticated logging system. To upsurge the security of the log file system, in one location, on one server you can place all logfiles. This rationalizes the administration of log files; set up manifold logging servers for redundancy; use a remote server for logging. This protects the logs if the system is conceded and, for example, the hard drive is damaged. Since an IPF server is regained over the network, it can be located wherever in the world. Safe the logging configuration file. The configuration file encompasses settings that, if changed, can concession the dependability of the log system. For instance, incorrectly setting the log level may cause some letdowns not to be logged. Allow logging of access demands on the Web server. This might be valuable in recognizing malicious action.

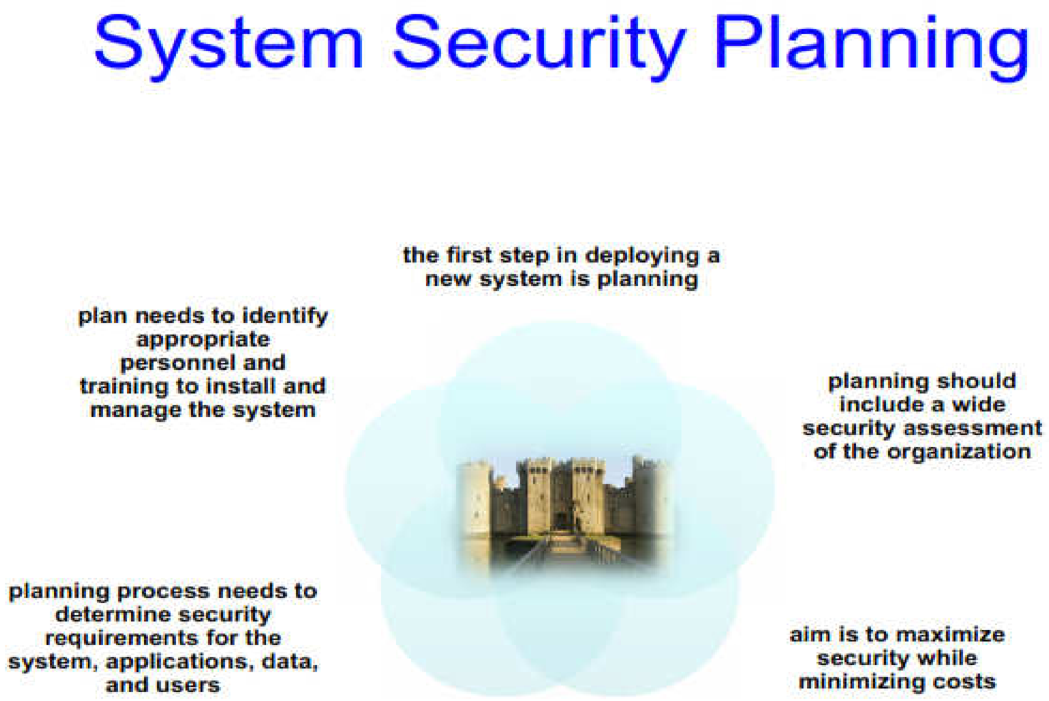
### 3.2.11 System Integrity

Build production systems from a repeatable and recognised process to guarantee system integrity. Check systems infrequently against snapshots of the original system. Use available third-party auditing software to check the system integrity.

Back up the system resources on a steady basis.

## 3.3 Need for Planning System Security

Through the security accreditation and certification process, the system security plan is updated, analysed and accepted. The security controls defined in the system security plan are reliable, the certification agent settles that. With the security class determined for the information system and that the threat and vulnerability identification and initial risk determination are recognised and documented in the system risk assessment, security plan or equivalent document. The results of a security certification are used to reassess the risks, develop the plan of action and milestones (POA&Ms) which are essential to track remedial update and actions, the system security plan, therefore providing the realistic basis for an approving official to render a security



System Security Planning

the first step in deploying a new system is planning

plan needs to identify appropriate personnel and training to install and manage the system

planning should include a wide security assessment of the organization

planning process needs to determine security requirements for the system, applications, data, and users

aim is to maximize security while minimizing costs

## 4.0 Self-Assessment Exercise(s)

(1) Explain what will happen if your employee reveals your logins to your system to an attacker.

Answer:
The administrators must be capable. Assign the minimum required access permissions for the account that runs the application. If attackers obtain access to the application, they have the permissions of the user who runs the application.

(2) Why do you think it is necessary to secure your operating system?

Answer:
The operating system is the physical environment where your application runs. Any vulnerability in the operating system could concession the security of the application. By securing the operating system, you make the environment stable, control external access to the environment and control access to resources. The physical security of the system is essential. Threats can come through the Web, but they can also come from a physical terminal.

## 5.0 Conclusion

In this unit, you have learnt about software security. You also learnt about how to secure a system, techniques for securing the Operating System (OS) such as user accounts, account policies, file system, network services, system patches, OS minimization, logging and monitoring as well as system integrity. Finally, you learnt about the need for planning system security.

## 6.0 Summary

This unit explained software security, how to secure a system and techniques for securing the operating system. It also discussed the need for planning system security. The next module is on network security.

## 7.0 References/Further Reading

https://cdn.ttgtmedia.com/rms/security/The-Basics-of-Information-Security-Ch11.pdf

https://www.techopedia.com/definition/24774/operating-system-security-os-security

https://www.ibm.com/support/knowledgecenter/en/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.crn_arch.10.2.1.doc/c_securing_the_operating_system.html

https://www.cnet.com/how-to/how-to-secure-your-pc-in-10-easy-steps/

Silberschatz, A; Galvin, P. B. & Gagne, G. (2012). *Operating System*

John, N. J. (2015). *Concepts*. Hoboken, Wiley & Sons.

Silberschatz, G. & Gagne, G. (2014): Operating system concept

C-DAC. (2014). National Intelligence Grid : NATGRID.

CERT-In. (2014). Indian Computer Emergency Response Team.

Chander, M. (2013). National Critical Information Infrastructure Protection Centre

Email Tips. Retrieved on Oct. 29, 2015 from https://survival.tacticaltech.org/internet/email/tips

*How to Reveal a Fake Facebook Account.* Retrieved on Sep. 27, 2015 from http://www.wikihow.com/Reveal-a-Fake-Facebook-Account

# Module 3: Network Security

## Module Introduction

In Module 2, you learnt about software security and trusted systems, which comprises of software security and Operating System security. This module is on network security. It is made up of Internet security protocols and standards, wireless network security and cellular network security. The units under this module are three.

Unit 1: Internet Security Protocols and Standards
Unit 2: Wireless Network Security
Unit 3: Cellular Network Security

## Unit 1: Internet Security Protocols and Standards

### Contents

# 1.0 Introduction

This unit is on internet security protocols and standards. You will learn about Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL) Overview, Key SSL Characteristics and Hypertext Transfer Protocol Secured HTTPS (HTTP over SSL).

# 2.0 Intended Learning Outcomes (ILOs)

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

- explain the functionality of S/MIME
- explain the key components of SSL
- discuss the use of HTTPS

# 3.0 Main Content

## 3.1 Secure/Multipurpose Internet Mail Extensions (S/MIME)

Multipurpose Internet Mail Extensions (MIME): Extension to the old RFC 822 specification of an Internet mail format – assumes ASCII text format – RFC 822 describes a simple heading with To, From, Subject– offers a number of new header fields that describe information about the body of the message.

Secure/Multipurpose Internet Mail Extensions (S/MIME), defined in IETF RFC 2311, offer a steady method to receive and send secure MIME data. Based on the general Internet MIME standard, S/MIME offers the succeeding cryptographic security services for electronic messaging applications: message integrity, authentication and non-repudiation of origin (using digital signatures), and privacy and data security (using encryption).

S/MIME can be used by old-style mail user agents (MUAs) to add cryptographic security services to mail that is sent and also interpret them in the mail that is received. Nevertheless, S/MIME is not limited to mail; it can be used with any transport mechanism that transports MIME data, like HTTP. In this technique, S/MIME takes advantage of the object-based features of MIME and allow secure messages to be exchanged in mixed-transport systems.

Additionally, S/MIME can be used in automatic message transfer agents that use cryptographic security services that do not require any human interference, like the validation of software-generated documents and the encryption of FAX messages sent through the Internet. The S/MIME content kinds are defined in Table 3.1.

**Table 3.1: S/MIME Content Types**

| Type | Subtype | SMIME Parameter | Description |
|---|---|---|---|
| Multipart | Signed | | A clear-signed message in two parts: one is the message, and the other is the signature |
| Application | pkcs7-mime | signedData | A signed S/MIME entry |
| | pkcs7-mime | envelopedData | An encrypted S/MIME entry |
| | pkcs7-mime | degenerate SingedData | An entity containing only public-key certificates |
| | pkcs7-mime | compressedData | A compressed S/MIME entry |
| | pkcs7-signature | signedData | The content type of the signature subpart of a multipart/signed message. |

### 3.1.1 Typical S/MIME Process

The typical S/MIME process is made up of five stages, as shown in figure 3.1.

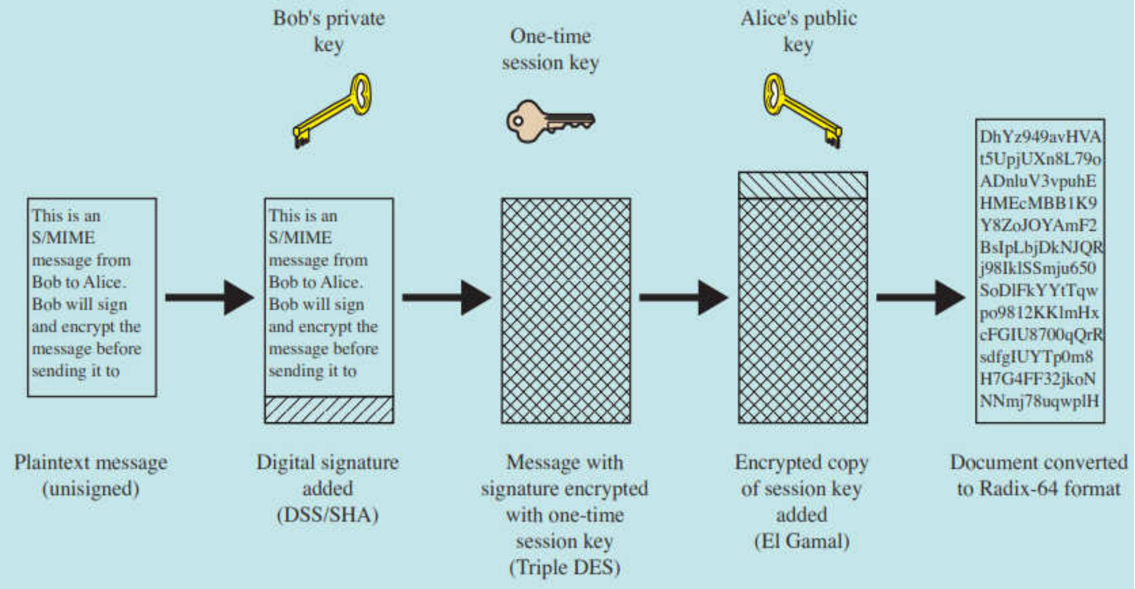

Bob's private key
One-time session key
Alice's public key
This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to
This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to
DhYz949avHVA
t5UpjUXn8L79o
ADnluV3vpuhE
HMEcMBB1K9
Y8ZoJOYAmF2
BsIpLbjDkNJQR
j98IklSSmju650
SoDlFkYYtTqw
po9812KKlmHx
cFGIU8700qQrR
sdfgIUYTp0m8
H7G4FF32jkoN
NNmj78uqwplH
Plaintext message (unisigned)
Digital signature added (DSS/SHA)
Message with signature encrypted with one-time session key (Triple DES)
Encrypted copy of session key added (El Gamal)
Document converted to Radix-64 format

**Fig. 3.1: Typical S/MIME Process**

### 3.1.2 S/MIME Cryptographic Algorithms

DSS and SHA-1 are default algorithms used for signing messages. RSA public-key encryption algorithm may be used with the MD5 or SHA-1. Message digest algorithm for forming signatures. Base64 or Radix-64 mapping is used to map the signature and message into printable ASCII characters.

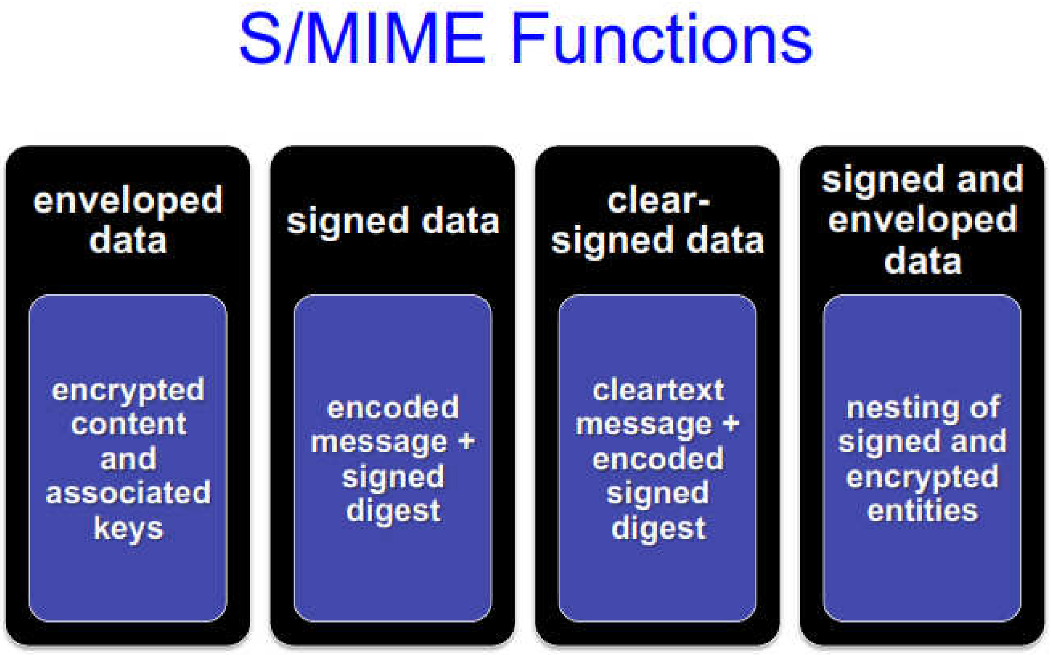
**Explain Multipurpose Internet Mail Extensions?** Multipurpose Internet Mail Extensions (MIME): Extension to the old RFC 822 specification of an Internet mail format – RFC 822 defines a simple heading with To, From, Subject – assumes ASCII text format – provides a number of new header fields that define information about the body of the message.

### 3.1.3 S/MIME Public Key Certificates

3DES and EIGamal are default algorithms used for encrypting S/MIME messages – EIGamal is based on the Diffie-Hellman public key exchange algorithm. If encryption is used alone, radix-64 is used to convert the ciphertext to ASCII format. A basic tool that allows widespread use of S/MIME is the public-key certificate. S/MIME uses certificates that conform to the international standard X.509v3.

### 3.1.4 S/MIME Functions

S/MIME functions are in four parts; enveloped-data, clear-signed data, signed-data, and signed and enveloped data. They are described in figure 3.2.



S/MIME Functions

enveloped data

encrypted content and associated keys

signed data

encoded message + signed digest

clear-signed data

cleartext message + encoded signed digest

signed and enveloped data

nesting of signed and encrypted entities

**Fig. 3.2: S/MIME Functions**

## 3.2. Secure Sockets Layer (SSL) Overview

SSL is one of the greatest generally used security services. General purpose service implemented as a set of protocols that trust on TCP. SSL consequently became Internet standard RFC2246: Transport Layer Security (TLS). The main goal of the SSL Protocol is, of course, to offer privacy and reliability between two communicating applications. SSL is considered to reside on top of TCP at the transport layer in the OSI Reference Model and interfaces to a user application through an SSL socket as part of an SSL connection establishment. SSL is made up of three protocols, and each SSL transaction comprises of two distinct and typically sequential parts. The two chief protocols are The SSL Handshake Protocol and the SSL Record Protocol. See figure 3.3.

The third protocol is the Alert Protocol and is used to specify questionable conditions. At the lowest level, layered on top of a reliable transport protocol (e.g., TCP), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of numerous higher-level protocols. One such encapsulated protocol is the SSL Handshake Protocol, which permits the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys earlier the application protocol receives or transmits its first byte of data. One advantage of SSL is that it is application protocol independent. A higher-level protocol can layer on top of the SSL Protocol transparently. The SSL protocol delivers connection security that has three rudimentary properties:

(i) The connection is private — encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES, RC4, etc.).

(ii) The peer's identity can be authenticated using asymmetric (or public-key) cryptography (e.g., RSA, DSS, etc.).

(iii) The connection is reliable — message transport includes a message integrity check using a keyed message authentication code (MAC).

Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations. The Handshake Protocol demonstrates the key communicating exchanges between the client and the server.

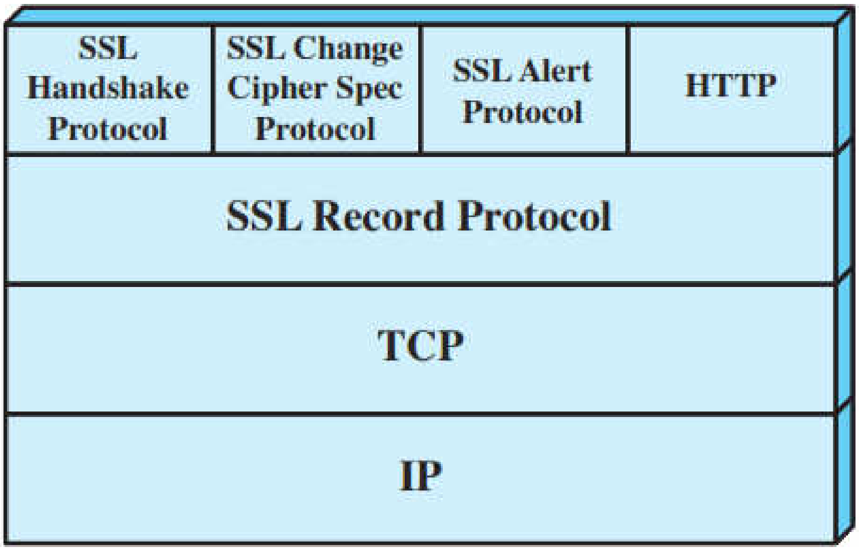


**Fig. 3.3: SSL Protocol Stack**

## 3.2.1 The Record Protocol

The encryption for all messaging in SSL is handled in the Record Protocol. This protocol delivers a common format to frame all Alert, Change Cipher Spec, Handshake, and application protocol messages. The SSL Record Protocol receives uninterrupted data from higher layers in non-empty blocks of arbitrary size. The Record Protocol fragments the information blocks into SSL plaintext records of $2^{14}$ bytes or less. Client message boundaries are not conserved in the recording layer (i.e., multiple client messages might have coalesced into a single SSL plaintext record). Once the handshake is complete, the two parties have shared secrets that are used to encrypt records and compute keyed MACs on their contents. The techniques used to perform the encryption and MAC operations are defined by the Cipher Spec. The encryption and MAC functions translate an SSL-compressed structure into an SSL ciphertext. The decryption functions inverse the process. Transmissions also comprise a sequence number so that missing, altered, or extra messages are detectable.

## 3.2.2 SSL Change Cipher Specific Protocol

One of three SSL specific protocols that use the SSL Record Protocol is the simplest. It contains a single message which contains a single byte with the value 1. The sole purpose of this message is to cause the pending state to be copied into the current state, hence updating the cipher suite in use.

### 3.2.3 The Alert Protocol

The Alert Protocol handles any questionable packets. If either the server or client detects an error, it sends an alert comprising the error. There are three types of alert messages: warning, critical, and fatal. Based on the alert message received, the session can be restricted (warning, critical) or terminated (fatal).

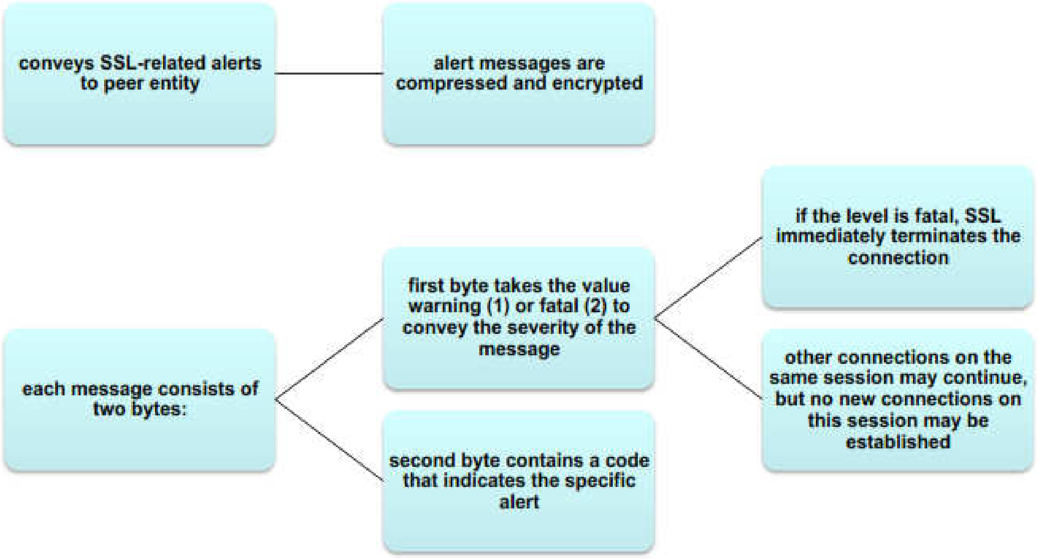
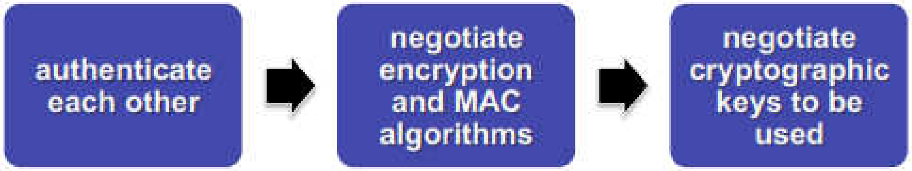

conveys SSL-related alerts to peer entity
alert messages are compressed and encrypted
if the level is fatal, SSL immediately terminates the connection
first byte takes the value warning (1) or fatal (2) to convey the severity of the message
each message consists of two bytes:
other connections on the same session may continue, but no new connections on this session may be established
second byte contains a code that indicates the specific alert

Fig. 3.4: SSL Alert Protocol

### 3.2.4 SSL Handshake Protocol

The greatest complex part of SSL is used earlier; any application data are transmitted. It lets server and client to:


authenticate each other
negotiate encryption and MAC algorithms
negotiate cryptographic keys to be used

It includes a series of messages exchanged by client and server. The exchange has four phases.

## 3.3 Key SSL Characteristics

The following are key characteristics of the SSL implementation:

i. The digital signature produced by hashing a message with a public key is sent over to the other side and likened against the locally generated hashed message for a match.
ii. The client normally authenticates the server, and the server can optionally authenticate the client.
iii. The Handshake Protocol is explained as follows: the client sends ClientHello, the server sends ServerHello, the server sends Certificate, the client sends ClientKeyExchange, the client sends CertificateVerify, both send ChangeCipherSpec, and both send Finished.
iv. The Record Protocol is explained for bulk data transfer.
v. The Alert Protocol handles questionable packets.
vi. Server processing bottleneck: Public-key cryptographic operation, encryption of SSL records, and MAC signature operations are all computation-intensive operations. To reach performance improvement, accelerators that are connected to switches are usually deployed for such applications as content distribution. These are usually known as SSL accelerators. Physically external SSL accelerators are sometimes called SSL termination devices.
vii. SSL modes: SSL can work in transparent and nontransparent (the client address is not sent over to the server, but cookies can be used to return client information) modes. The nontransparent mode is more flexible and more scalable.
viii. The use of SSL accelerators or other SSL optimization techniques is especially important in data centres.

## 3.3 Hypertext Transfer Protocol Secured HTTPS (HTTP over SSL)

This is the mixture of HTTP and SSL to implement secure communication amid a Web browser and a Web server. It is made into all modern Web browsers. Search engines do not support HTTPS. The URL addresses start with https:// It is documented in RFC 2818, *HTTP Over TLS.* An agent acting as the HTTP client also acts as the TLS client. The closure of an HTTPS connection requires that TLS close the linking with the peer TLS entity on the remote side, which will include closing the underlying TCP connection.

Discussion

Crime is an act omitted or committed in violation of a law commanding or forbidding it and for which punishment is levied upon conviction. So you can say in easy term that, “crime is something that is against the law.” Crime is a social and economic phenomenon and is as old as the human society. Crime is a lawful concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment. What are the reasons why cyber-criminals are

## 4.0 Self-Assessment Exercise(s)

(1) What provision is available for MIME in S/MIME?

____________________________________________________________

Answer:

Secure/Multipurpose Internet Mail Extensions (S/MIME), defined in IETF RFC 2311, offer a consistent method to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures), and privacy and data security (using encryption).

(2) The importance of SSL protocol on connection security cannot be over-emphasized. Explain? ____________________

Answer:

The SSL protocol provides connection security that has three basic properties:

(i) The connection is private — encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES, RC4, etc.).

(ii) The peer’s identity can be authenticated using asymmetric (or public-key) cryptography (e.g., RSA, DSS, etc.).

(iii) The connection is reliable — message transport includes a message integrity check using a keyed message authentication code (MAC).

## 5.0 Conclusion

In this unit, you have learnt about Secure/Multipurpose Internet Mail Extensions (S/MIME), such as typical S/MIME Process, S/MIME cryptographic algorithms, S/MIME public key certificates and S/MIME Functions. You also learnt about Secure Sockets Layer (SSL), Key SSL characteristics and HTTP over SSL. You will learn about wireless network security in the next unit.

## 6.0 Summary

This unit explained Secure/Multipurpose Internet Mail Extensions (S/MIME), such as typical S/MIME Process, S/MIME cryptographic algorithms, S/MIME public key certificates and S/MIME Functions. You also learnt about Secure Sockets Layer (SSL) such as The Record Protocol, SSL Change Cipher Specific Protocol, the Alert Protocol and SSL Handshake Protocol. It also covers Key SSL characteristics and HTTP over SSL.

## 7.0 References/Further Reading

*How to Set up 2 Step Verification in Gmail*. Retrieved on Oct. 24, 2015, from http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail

*Introduction to Digital Forensics*. (2011, Nov. 16). Retrieved on Sep. 28, 2015 from https://en.wikibooks.org/ wiki/Introduction to _Digital Forensics

Jeetendra, P. (2017). *Introduction to Cyber Security.* Uttarakhand Open University.

Westfall, J.E. et al. (2012). "Locking the virtual filing cabinet: A researcher's guide to Internet data security." *International Journal of Information Management.* Retrieved from http://dx.doi.org/ 10.1016/j.ijinfomgt.2012.01.005

Cisco Subscriber Edge Services Manager (SESM) document, 2003.

Application Security SDK, Hewlett Packard document, 2003.

Deploying Scalable, Secure, Dynamic Virtual Private Networks, White Paper, NetScreen Technologies, May 2003.

IETF RFC 2743 (obsoletes 2078): Generic Security Service Application Program Interface, Version 2, Update 1, J. Linn, January 2000.

Intranet and Extranet VPN Business Scenarios, Cisco Document, January 20, 2003.

Configuring a GRE Tunnel over IPSec with OSPF, Cisco Document, January 14, 2003.

IETF RFC 2246: The TLS Protocol Version 1.0, T. Dierks, C. Allen, January 1999.

IETF Internet-Draft: EAP Tunneled TLS Authentication Protocol (EAP-TTLS), Paul Funk and Simon Blake-Wilson, February 2002.

*Router Security Configuration Guide by System and Network Attack Center*(*SNAC*), National Security Agency, Updated: March 25, 2002, Version: 1.0k,Report Number: C4-054R-00.

A Framework for Denial of Service Analysis, C. Meadows, Third Information Survivability Workshop — ISW-2000, October 24–26, 2000.

The CERT ® Guide To System and Network Security Practices, Julia Allen, May30, 2001.

VoIP traversal of NAT and Firewall, Cisco Document, March 26, 2003.

IETF RFC 2328 (obsoletes 2178): OSPF Version 2, J. Moy, April 1998.

Wireless LAN Security, Cisco White Paper, 2003.

IETF RFC 2311: S/MIME Version 2 Message Specification, S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka, March 1998.

Burt Kaliski, "Raising the Standard for RSA Signatures: RSA-PSS," RSA Laboratories, February 26, 2003.

# Unit 2: Wireless Network Security

## Contents

## 1.0 Introduction

This unit is on wireless network security. Wireless security is the deterrence of unauthorised damage or access to computers using wireless networks. The utmost common kinds of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. You will learn about wireless threats and attacks, securing wireless Network (countermeasures) and network auditing.

# 2.0 Intended Learning Outcomes (ILOs)

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

- describe the security threats and countermeasures for wireless networks.

# 3.0 Main Content

## 3.1 Wireless Threats and Attacks

### 3.1.1 Ad-hoc Networks

Ad-hoc networks pose a security threat. Ad-hoc networks can be defined as peer-to-peer networks among wireless computers that do not have an access point amid them. While these kinds of networks typically have little protection, encryption approaches can be used to offer security.

### 3.1.2 Identity Theft (MAC Spoofing)

MAC spoofing (or Identity theft) happens when a cracker is able to eavesdrop in on Network traffic and recognise the MAC address of a computer with network rights. Most wireless systems permit some kind of MAC filtering to only allow authorised computers with specific MAC IDs to gain access and utilise the network. Nevertheless, a number of programs exist that have network “sniffing” abilities. Conglomerate these programs with additional software that permit a computer to be imaginary it has any MAC address that the cracker wants, and the cracker can effortlessly get around that hurdle.

**Explain a security threat that can be posed by ad-hoc networks?** Ad-hoc networks represent a security threat. Ad-hoc networks can be defined as peer-to-peer networks among wireless computers that do not have an access point amid them. While these kinds of networks typically have little protection, encryption approaches can be used to offer security.

### 3.1.3 Man-in-the-middle Attacks

A man-in-the-middle attacker lures computers to log into a computer which is set up as a soft Access Point (AP). Once this is completed, the hacker connects to a real access point through another wireless card offering a stable flow of traffic through the clear hacking computer to the real network. The hacker can then sniff the traffic. A unique type of man-in-the-middle attack trusts on security errors in the challenge and handshake protocols to execute a "de-authentication attack". This attack forces AP connected computers to drop their connections and reconnect with the cracker's soft AP. Man-in-the-middle attacks are improved by software such as LAN jack and Air Jack, which automate multiple steps of the process. What once required some skill can now be done by script kiddies. Hotspots are mainly vulnerable to attack somewhat since there is tiny to no security on these networks.

### 3.1.4 Denial of Service

A Denial-of-Service attack (DOS) happens when an attacker repeatedly bombards a Targeted AP (Access Point) or network with bogus requests, untimely successful connection messages, failure messages, and/or other commands. These cause genuine users not to be able to get on the network and might even cause the network to crash. These attacks depend on the misuse of protocols.

### 3.1.5 Network Injection

In a network injection attack, a cracker can make use of access points that are unprotected to non-filtered network traffic, precisely broadcasting network traffic like "Spanning Tree" (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

## 3.2 Securing Wireless Network (Countermeasures)

### 3.2.1 Use of Encryption

The most effective method to secure your wireless network from intruders is to scramble or encrypt, communications over the network. Utmost wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router does not have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on.

### 3.2.2 Use Anti-virus and Anti-Spyware Software and a Firewall

Computers on a wireless network require the same protections as any computer connected to the Internet them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

### 3.2.3 Turn Off Identifier Broadcasting

Utmost wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the neighbourhood announcing its existence. You do not need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

**Explain encryption as one of the countermeasures to wireless network security?** The most effective method to secure your wireless network from intruders is to scramble or encrypt, communications over the network. Utmost wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router does not have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on.

### 3.2.4 Change your Router's Pre-set Password for Administration

The manufacturer of your wireless router perhaps assigned it a standard default password that permits you to set up and operate the router. Hackers know these default passwords, so change it to somewhat only you know. The longer the password, the tougher it is to crack.

### 3.2.6 Do Not Assume that Public "hot spots" are Secure

Numerous cafés, hotels, airports, and other public establishments offer wireless networks for their customers' use.

## 3.3 Network Auditing

Wireless network auditing is a vital part of Wireless Local Area Network (WLAN) security policy. The network desires to be frequently audited for rouge hardware. In this technique, the network is scanned and mapped for all access points and WLAN nodes. Then this is likened with previous network map. Regularly available network mapping tools like nets tumbler and Waveland-tool can be used to do this. Particular tools like Air snort can be used for WEP cracking and auditing the network for weak keys, key reuse and WEP security settings. These approaches comprise the same tests as those carried out by hackers for breaking into the network.

Discussion

Most access points use a single key or password that is shared with all connecting devices on the wireless LANs. A brute force attack can be applied on sniffing packets captured by the attacker in order to obtain the key. What is the simplest way to get a key? The simplest way to get a key is to see someone as he enters the password. One solution is to keep the key inside the computer. The problem with this approach is that, if the computer is stolen, the key is inside and the thief can gain access by masquerading as a user. The problem for the attacker is that the data is encrypted.

## 4.0 Self-Assessment Exercise(s)

(1) Describe how you can use your system to perpetrate man-in-the-middle attack.

___________________________________________________

Answer:

A man-in-the-middle attacker lures computers to log into a computer which is set up as a soft Access Point (AP). Once this is completed, the hacker connects to a real access point through another wireless card offering a stable flow of traffic through the clear hacking computer to the real network. The hacker can then sniff the traffic. A unique type of man-in-the-middle attack trusts on security errors in the challenge, and handshake protocols to execute a "de-authentication attack". This attack forces AP connected computers to drop their connections and reconnect with the cracker's soft AP. Man-in-the-middle attacks are improved by software such as LAN jack and Air Jack, which automate multiple steps of the process.

(2) Why is turning off identifier broadcasting is one of the countermeasures to wireless network attacks? _______________

Answer:

Utmost wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the neighbourhood announcing its existence. You do not need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

## 5.0 Conclusion

In this unit, you have learnt about wireless threats and attacks, securing wireless network (countermeasures) and network auditing. You will learn about cellular network security in the next unit.

## 6.0 Summary

This unit explained wireless threats and attacks, such as Ad-hoc Networks, Identity Theft (MAC Spoofing), Man-in-the-middle Attacks, Denial of Service and Network Injection. It also covers securing wireless network (countermeasures) such as the use of Encryption, use Anti-virus, Anti-Spyware Software and a Firewall, turning off identifier broadcasting, changing Router's Pre-set Password for Administration and not assuming that Public "hot spots" are Secure. The unit at end discussed Network Auditing.

## 7.0 References/Further Reading

Aneja, A., & Sodhi, G. (2016). "A Study of Security Issues Related With Wireless Fidelity (WI-FI)". *International Journal of Computer Science Trends and Technology (IJCST), vol.* 4, 2, pp. 346-350.

Beard, C. & Stallings, W. (2016). *Wireless Communication Networks and Systems*. London, England: Pearson.

Bilolikar, D. & Gaikwad, S. Y. (April 2015). "Spoofing Attackers Using Cluster Analysis in Wireless Network". *International Journal of Innovative Research in Computer and Communication Engineering, Vol*. 3, 4.

Bartolic, I. (2017). on the.best wireless internet.com, Retrieved from http://thebestwirelessinternet.com/how-wlan-works.html.
the tutorials website. [Online]. Available:http://etutorial.org.

Bhatia V. et al. (November 2012). "Security And Vulnerability Analysis Of Wireless Networks". *International Journal of Neural Networks*, Vol. 2, Issue 1, pp. 10-13, 16. A. Angela, I. (July 2014). "Evaluation of Enhanced Security Solutions in 802.11Based Networks*".*

*International Journal of Network Security and Its Applications (IJNSA),* Vol.6, No.4, pp. 29-42,

Coleman, D. D., Westcott, D. A. & Harkins, B. E. (2016). *CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205*. (2nd ed.). New Jersey, US: Wiley Publishing.

Deotare, V. Wani, S. & Shelke, S. (March 2014). "Wired Equivalent Security Algorithm for Wireless LAN". *International Journal of Emerging Technology and Advanced Engineering*. Vol. 4 Issue 3, pp. 66-69,

Edney, J. & Arbaugh, W. A. (2004). *Real 802.11 Security*. Massachusets, USA: Addison Wesley.

Habib Sardar, T., Ansari, Z. & Khan, A. (2014). "A Methodology for Wireless Intrusion Detection System ". *International Journal of Computer Applications (0975 – 8887), pp. 12-15, 2014*

Kanawat, S.D. & Parihar, P.S. (May 2011). "Attacks in Wireless Networks". *International Journal of Smart Sensors and Adhoc Networks (IJSSAN),* vol. 1, 1, pp. 113-116,

Lackner, G. (2013). "A Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMAX", *International Journal of Network Security,* Vol.15, No.6, pp.420-436.

Malgaonkar, S. et al., "Research on Wi-Fi Security Protocols". *International Journal of Computer Applications (*0975 – 8887), Vol.164, No 3, pp. 30-36, April 2017

Md. Waliullah, & Diane Gan, "Wireless LAN Security Threats & Vulnerabilities", *International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1*, pp.176-13, 2014.

Prastavana, M. & Praveen, S. (January 2016). "Scientific Engineering and Applied Science (IJSEAS)", Vol 21, pp. 374382.

Sari, A. & Karay, M. (December 2015). "Comparative Analysis of Wireless Security Protocols: WEP vs WPA". *International Journal Communications, Network and System Sciences,* Vol.08 No.12, pp. 483-491.

Tony, B. (2018). on Lifewire. [Online]. Retrieved from https://www.lifewire.com/introduction-to-intrusiondetection-systems-ids-2486799.

Wang, S., Wang, J., Feng, C., & Pan, Z. (2016). “Wireless Network Penetration Testing and Security Auditing”, 2016, ITM Web of Conferences, 7, 03001

# Unit 3: Cellular Network Security

## Contents

## 1.0 Introduction

This unit is on cellular network security. The increased use of cellular devices has led to an uptick in cellular security threats. People tend to look at cellular security threats as an all-encompassing threat. But the truth is, there are different types of cellular security threats to be aware of. They include application-based, web-based, network-based and physical threats. You will learn about these threats and their countermeasures.

## 2.0 Intended Learning Outcomes (ILOs)

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

- describe the security threats and countermeasures for cellular networks.

## 3.0 Main Content

## 3.1 How Cellular Security Threats Works

### 3.1.1 Application-Based Threats

These happen when people download apps that look legit but actually skim data from their device. Examples are spyware and malware that steal personal and business information without people realising what's going on.

### 3.1.2 Web-Based Threats

These are subtle and tend to go unnoticed. They happen when people visit affected sites that seem fine on the front-end but in reality, automatically download malicious content onto devices.

### 3.1.3 Network-Based Threats

These are especially bad because cybercriminals can steal unencrypted data while people use public WiFi networks.

### 3.1.4 Physical Threats

These happen when someone loses their mobile device or has it stolen. Because hackers have direct access to the hardware where private data is stored or where they have access to data, this threat is especially dangerous to enterprises

## 3.2 Types of Cellular Threats and Countermeasures

### 3.2.1. Malicious Apps

When you visit Google Play or the App Store to download apps that look innocent enough, the apps ask for a list of permissions before you are allowed to download them. These permissions generally require some kind of access to files or folders on the mobile device. Most people just glance at the list of permissions and agree without reviewing them in great detail. This lack of scrutiny leaves devices and enterprises vulnerable to mobile threats.

**Countermeasure:** Check the permissions apps request before you approve any download. If the list of permissions seems too invasive, you should skip the download

### 3.2.2. Spyware

Whether you have an iOS or Android device, your devices are targets for threats focused on mining user data and your private corporate data. For example, Apple realized it had three zero-day vulnerabilities that left its devices open for spyware attacks. Pegasus spyware was discovered back in August 2016 and was used to hack into Apple devices and surveil users. Apple had to release a patch with updates that would protect users against the Trident iOS vulnerabilities.

**Countermeasure:** Choose a mobile security app and ask all of your employees to download it onto their devices. Next, make it a requirement for employees to update their device software regularly. Regular updates ensure that their devices are protected against the latest spyware threats.

### 3.2.3. Public WiFi

As more companies offer remote work options, access to unsecured WiFi is becoming more widely available in public places. Be it coffee shops, co-working spaces or the library, public WiFi is convenient, but the downside is that the devices your employees use are vulnerable to attacks sent through these networks. Instead of connecting directly to a network, people are tricked into accessing a network that looks authentic but is actually controlled by a hacker.

**Countermeasure:** Ask employees to create unique passwords for every new account they create when they use their mobile devices. Because hackers assume people use the same password for everything, employees should never default to standard logins used for their personal accounts. Even if their phone is hacked, private, password protecting data can't be.

### 3.2.4. Lack of End-to-end Encryption

Depending on the platforms employees use to access corporate data on their phones, a lack of mobile app security doesn't bode well for you. For example, a lot of communication happens electronically. You send, share and receive countless amounts of data every day, so leaving that unencrypted leaves the door open for anyone to look at what's being said or done in your company. And it's not just hackers who'll have access, your service provider and any online applications that host your conversations with employees will have access to view and collect private data.

**Countermeasure:** Use communication apps that encrypt data transfers to make sure that communication between you and your employees can't be accessed by anyone outside of the business. Use an encryption-based application to help manage communication.

### 3.2.5. Inactive Apps

Google and Apple remove apps from their stores regularly, but the thing is, they don't offer much explanation about why. We can assume, though, that these occasional purges have something to do with security threats and privacy breaches.

In Google's case, they found apps that forced users to click on ads by making it hard to use the app otherwise. When a user clicks on the ad, it runs in the background without the user knowing while the ad accumulates automated clicks to generate income for the app developer.

**Countermeasure:** There should be more transparency for users *and* enterprises, so they know what apps could threaten their devices. You and your employees should be proactive and regularly check the apps on devices to see if they're still active. If apps aren't active, users should delete them to limit the threat to data access and privacy.

### 3.2.6. IoT Mobile Security Threats

Mobile devices are branching out from cell phones and tablets to include wearable tech, like smartwatches or devices in the office, like video conferencing tools. Basically, anything that's used to improve workplace efficiency, productivity and service quality has a product for that purpose. Cybercriminals are aware of this expansion; after all, Gartner predicts the number of connected devices will reach 20.8 billion by 2020.

A big part of what makes the growth of IoT pose a threat is the proliferation of ransomware. A lot of the latest mobile devices have IP addresses, which means that they can be hacked through the internet. Anyone looking to gain access to your corporate data can find and use mobile devices to access corporate networks and the information within them. That's why mobile security shouldn't just be about the network and the data; it should extend to include securing the devices.

**Countermeasure:** Educate employees on where threats can come from and how to use their devices safely. Get them to read blog posts, send them email newsletters and news updates or start a video series. The point is to get across the fact that you expect employees to take mobile security seriously and that threats can come from almost anywhere.

### 3.2.7. Botnets

Depending on sites employees visit on their mobile devices, malware can be downloaded onto mobile devices that aren't protected by antivirus software or a mobile security app. This gives hackers full access to the device so that they can control affected devices remotely.

All devices with the malware on them are added to a network of other affected devices — called a botnet — that allow hackers to send spammy emails and other click fraud campaigns that spread the malware to even more devices. As an enterprise, it's harmful to you that malware can disrupt networks or steal confidential customer information.

**Countermeasure:** Put in place BYOD policies to protect your enterprise network. For example, give employees options on which mobile security apps to download to make sure that botnets don't have a chance to spread. Educate employees on the policies and what's expected of them to ensure that internal data is kept safe.

### 3.2.8. No Password Protection

With all of the ways to secure mobile devices, it might be shocking to know that 34% of people don't use a password to lock their phone. If these devices are lost or stolen, it gives thieves easy access to all the information stored on the phone.

For people who do go through the effort of creating a password or PIN, they typically default to codes that are easy to crack. Like 0000, 1234 or birthday month and day. Unlike secure sites, mobile devices don't force users to create a password or PIN. And even when users do create them, devices don't confirm the strength of the password or PIN.

**Countermeasure:** If employees are going to use their own devices to access your data, make your identity access management requirements clear to them. For example, layout what your password standards are. Take it one step further and require 2-factor authentication to access internal tools.

### 3.2.9 Phishing Attacks

This happens all too often in enterprises where hackers send what looks like legit emails or SMS to get employees to hand over private information. For example, let's say the finance department in an insurance company gets an email from what looks to be a genuine B2B customer email account. The email might inform finance about a change to the “customer's” banking information and ask that all payments be re-routed to the new account. It all looks and sounds above board until the actual customer confirms that they haven't been receiving payments.

**Countermeasure:** To fight against this, enterprises need strict processes for employees to follow when customers request changes and processes to alert the right people when red flags are spotted.

Discussion

WiFi, and now mobile networks, allow users to connect from a relatively wide coverage radius. In the case of mobile networks, the user is able to connect from any point where there is cellular coverage. Finding the exact location of a specific user requires special equipment, and a very rapid response when searching for them.

Mobile operators offering data services to their subscribers face a number of threats from anonymous users who intend to abuse the service and its network. There are a number of typical threats to third parties such as spam, hacking of third party sites, copyright infringement, and illegal communications. Mobile operators are not accustomed to dealing with these threats. However, solutions have been developed by Internet service providers (ISPs) that are relatively simple to deploy into the mobile environment.

## 4.0 Self-Assessment Exercise(s)

(1) Describe spyware as a cellular threat and its countermeasure.

_______________________________________________

Answer:

Whether you have an iOS or Android device, your devices are targets for threats focused on mining user data and your private corporate data. For example, Apple realised it had three zero-day vulnerabilities that left its devices open for spyware attacks. Pegasus spyware was discovered back in August 2016 and was used to hack into Apple devices and surveil users. Apple had to release a patch with updates that would protect users against the Trident iOS vulnerabilities

**Countermeasure:** Choose a mobile security app and ask all of your employees to download it onto their devices. Next, make it a requirement for employees to update their device software regularly. Regular updates ensure that their devices are protected against the latest spyware threats

(2) What is countermeasure to phishing attacks? __________________

Answer:
To fight against this, enterprises need strict processes for employees to follow when customers request changes and processes to alert the right people when red flags are spotted.

## 5.0 Conclusion

In this unit, you have learnt about how cellular security threats works and types of cellular threats and countermeasures.

## 6.0 Summary

This unit explained how cellular security threats works such as application-based threats, web-based threats, network-based threats and physical threats. Also, it discussed **t**ypes of cellular threats and countermeasures, such as malicious apps. Spyware, public WiFi, lack of end-to-end encryption, inactive apps, IoT mobile security threats, botnets, no password protection and phishing attacks.

## 7.0 References/Further Reading

Becher, M.; Freiling, F.C.; Hoffmann, J.; & Holz, T. (2011). "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices." In Proceedings of the 2011 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 22–25 May 2011.

Itwire Web Page. (2013). Asia Pacific Mobile Data Revenues Tipped to Exceed Voice in 2016. Retrieved on 28 July 2013 from http://www.itwire.com/your-it-news/mobility/49878-asia-pacific-mobile-data-revenuestipped-to-exceed-voice-in-2016

Nagy, M.; & Kotosová, M. (2012). "An IP Based Security Threat in Mobile Networks." In Proceedings of the 35th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2012.

Ricciato, F. (2006). "Unwanted traffic in 3G networks." *ACM SIGCOMM Comput. Commun. Rev.,* 2006, 36, 53–56.

Ricciato, F.; Coluccia, A.; & D'Alconzo, A. (2010). "A review of DoS attack models for 3G cellular networks from a system-design perspective." *Comput. Commun. 2010*, 33, 551–558.

Serror, J.; Zang, H.; & Bolot, J.C. (September 2006). “Impact of Paging Channel Overloads or Attacks on a Cellular Network.” In Proceedings of the ACM Workshop on Wireless Security (WiSe 06), Los Angeles, CA, USA, 29.

The European Telecommunications Standards Institute (ETSI). Technical Specification: 3GPP TS 25.331; version 8.1.0; ETSI: Valbonne, France, 2008. Retrieved on 28 July 2013 from http://www.etsi.org/deliver/etsi_ts/125300_125399/125331/08.01.00_60/ts_125331v080100p.pdf.

Mobile Marketer Web Page. (2013). *Top Mobile Security Threats for 2013*. Retrieved on 28 July 2013 from http://www.mobilemarketer.com/cms/news/strategy/14518.html.