Unit 17: Network Security

Unit code	**L/615/1646**
Unit level	**5**
Credit value	**15**

Introduction

“Who is accessing my network?" A bank was hacked last week? Did you hear about that? Last night l blocked my neighbours from accessing their internet because they did not have a Wireless Equivalent Protection (WEP) or WPA (Wi-Fi Protected Access) key on their wireless.”

It is estimated that Network Security (NS) breaches occur every second worldwide from small home networks to massive corporate networks. The cost to businesses is in billions, if not trillions. There are several methods, techniques and procedures that need to be implemented on a network in order for it to be ‘secure’. Sometimes basic procedures such as locking your network room, changing your password regularly, as well as putting a password on all your network devices, is all that is needed to achieve some basic network security.

This unit introduces students to the fundamental principles of Network Security practices. As Systems Administration and Management are important tasks in the day-to-day functioning and security of Information Systems, poor or improper practices can lead to loss of data, its integrity, performance reductions, security breaches or total system failure. Special planning and provisions needs to be made for ongoing support of systems and networks, which account for a significant proportion of the IT budget. With the widespread use of computers and the internet for business customers and home consumers, the topic of security continues to be a source for considerable concern.

Among the topics included in this unit are: historical Network Security (NS) principles and associated aspects such as Firewalls, Routers, Switches, MD5, SSL, VPN, AES, SHA-1/2, RSA, DES, 3DES; different types of public and private key cryptography such as Caesar Cipher, IPSec; types of attacks that can be done on a network and methods of preventing such attacks such as Man-In-the-Middle (eavesdropping), Denial of Service (DoS), Distributed Denial of Service (DDoS) (ping); Certificate Authority (CA); ‘The Cloud’ Security aspects and associated counter-measures such Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud, Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), phishing, spoofing, DNS attack, SQL Injection, MAC Address spoofing/control. Firewalls and other Gateways can be used as a tool for Intrusion Detection and Prevention as they can be situated on the perimeter of the Network to provide security.

On successful completion of this unit students will be able to discuss with confidence several types of Network Security measures as well as associated protocols, cryptographic types and configuration settings of Network Security environments. Finally, students will be able to test the security of a given network to identify and fix vulnerabilities.

As a result they will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1. Examine Network Security principles, protocols and standards.

LO2. Design a secure network for a corporate environment.

LO3. Configure Network Security measures for the corporate environment.

LO4 Undertake the testing of a network using a Test Plan.