**COE 510: COMPUTER SECURITY TECHNIQUES (3, 0, 0) 3 UNITS**

**Course Description**

This course covers fundamentals of computer security i.e. the confidentiality, integrity, and availability (CIA) and other concepts, attacks and security services. Malicious programs such as viruses and worms, propagation, effects, countermeasures and related issues will be covered. Intrusion detection, prevention, firewalls and other access controls mechanism will be studied. The course also covers security ethics and policy, strategy, personnel and training. Fundamentals of cryptographic, different encryption methods, digital signatures, and organisational security. Overview of security audit, risk assessment, analysis, vulnerability scan and penetration testing.

**Learning Outcomes**

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

* Prevent internal and external attacks
* Demonstrate knowledge of malware and protection/prevention
* Demonstrate knowledge of security threats
* Create security policies to secure both physical and computer files, and resources.
* Perform encryption and decryption
* Demonstrate knowledge of organisational security

**Grading**

Assignment + Home work/Quiz = 20%

Mid-Semester Test = 20%

Final Exam = 60%

**Class Note 1- Introduction to Computer Security**

**Brief History**

The need for computer security—that is, the need to secure physical locations, hardware, and software from threats—arose during World War II when the first mainframes, developed to aid computations for communication code breaking (German code machine Enigma), were put to use.

During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage.

The 1960s - During the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to enable these mainframes to communicate via a less cumbersome process than mailing magnetic tapes between computer centers. This birth the ARPANET (predecessor to the Internet), developed by Larry Roberts.

The 1970s and 80s - ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1973, Robert M. “Bob” Metcalfe (credited for Ethernet), identified fundamental problems with ARPANET security. Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorization to the system. Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET.

Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was referred to as network insecurity.

Thereafter, movement toward security that went beyond protecting physical locations began by a single paper sponsored by the Department of Defense (the Rand Report R-609), which attempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system. This started the study of computer security.

This paper signaled a pivotal moment in computer security history—when the scope of computer security expanded significantly from the safety of physical locations and hardware to include the following:

* Securing the data
* Limiting random and unauthorized access to that data
* Involving personnel from multiple levels of the organization in matters pertaining to information security.

MULTICS (Multiplexed Information and Computing Service) - first operating system to integrate security into its core functions. It was a mainframe, time-sharing operating system developed in the mid-1960s by a consortium of General Electric (GE), Bell Labs, and the Massachusetts Institute of Technology (MIT).

UNIX (mid-1969) – created by several of MULTICS’ developers. While the MULTICS system implemented multiple security levels and passwords, the UNIX system did not. Its primary function, text processing, did not require the same level of security as that of its predecessor. In fact, it was not until the early 1970s that even the simplest component of security, the password function, became a component of UNIX.

Microprocessor (1970s) - brought the personal computer and a new age of computing. The PC became the workhorse of modern computing, thereby moving it out of the data center. This gave rise to networking—that is, the interconnecting of personal computers and mainframe computers, which enabled the entire computing community to make all their resources work together.

The 1990s, close of the twentieth century - networks of computers, and the need to connect this networks became more common. This gave rise to the internet. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN). Early Internet deployment treated security as a low priority. In fact, many of the problems that plague e-mail on the Internet today are the result of this early lack of security. Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

2000 to Present - Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer’s stored information is now contingent on the level of security of every other computer to which it is connected. The growing threat of cyber-attacks have made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure.