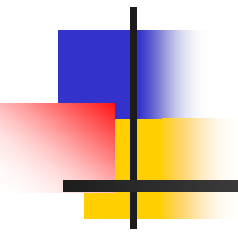

Information Security Course

Prof. Mona Mursi

Course Description

Upon successful completion of the course, the student will be knowledgeable of network security principles and implementation, including the technologies used and principles involved in creating a secure computer networking environment; authentication, types of attacks and malicious code that may be used against a network; threats and countermeasures for e-mail, Web applications, remote access, and file and print services; security topologies; technologies and concepts used for providing secure communications channels, secure internetworking devices, and network medium; intrusion detection systems, firewalls, and physical security concepts; security policies, disaster recovery, and computer forensics; and daily tasks involved with managing and troubleshooting security technologies.

Course Objectives

- To provide the student with basic knowledge of general security concepts, including authentication methods, common network attacks and how to safeguard against them.
- To provide the student with basic knowledge of communication security, including remote access, e-mail, the Web, directory and file transfer, and wireless data.
- To provide the student with basic knowledge of infrastructure security, including various network devices and media, and the proper use of perimeter topologies such as DMZs, Extranets, and Intranets to establish network security.
- To provide the student with basic knowledge of cryptography basics, including the differences between asymmetric and symmetric algorithms, and the different types of PKI certificates and their usage.
- To provide the student with basic knowledge of operational/organizational security