DBLN CPSI 4497

This course is being offered at Griffith College, CAPA's academic partner in Dublin. The Irish academic system differs from the US, particularly with grading. Griffith College professors expect students to undertake a good deal of independent study to achieve a high mark in their classes. For additional information about this class, please contact the Boston Program Advising Team at 1-800-793-0334.

Network Security

Continuous Assessment: 40%
Exam: 60%

Intended Module Learning Outcomes

On successful completion of this module learners will be able to:

1. Develop an understanding of information systems security.
2. Security vulnerabilities, threats and risk assessment and security policies.
3. Gain familiarity with prevalent network and distributed system attacks, defences against them, and forensics to investigate the aftermath.

4. Security problems in computer operating systems, distributed systems, networks and applications
5. A basic understanding of cryptography, and some key encryption techniques used today.
6. Understand wireless security standards.

Module Objectives

This module provides the learner with a detailed understanding of computer and information security. They learn fundamentals of computer security, security models, aspects of information systems security such as access control, security attacks, systems and programs security, intrusion detection, networks and distributed systems security, worms, and viruses, and other Internet secure applications. They develop the skills necessary to formulate and address the security needs of enterprise and personal environments.

Module Curriculum

Introduction to network security

- Security vulnerabilities,
- risk,
- attacks,
- detection,
- protection,
- response and recovery policies.

Cryptography

- Introduction to cryptographic systems,
- encryption and decryption of data,
- conventional encryption,
- public key encryption.
- Encryption standards.

Security services

- Confidentiality,
- availability,
- integrity,
- authenticity,
- non-repudiation.
- Hashing,
- digital signature,
- digital certificates.

Network security

- Database security,
- Operating systems and programming languages security problems.
- Network security tools,

- network ports and services,
- firewalls

Internet security

- Internet Protocol Security (IPsec),
- Transport Layer Security (TLS),
- Secure Sockets Layer (SSL)

Wireless security

- Concepts of wireless security.
- WPA,
- WAP,
- WTLS.

Organisational policies

- Organisational security policies.
- Password policies,
- user training and education,
- environment control,
- backups and redundancies,
- monitoring,
- Risk Assessment and Risk Mitigation.