COT 4930 Introduction to Security and Cryptography

Credits: 3 credits


Specific course information

Catalog description: This is a course on computer security and cryptographic algorithms. The following components are covered in the course: (a) Overview of computer security concepts (b) Computer security technology and principles, (c) Software security and trusted systems, (d) Management issues, (e) Cryptographic algorithms, and (f) Network security

Prerequisites: MAD 2104 and COP 3014. Knowledge of linear algebra, number theory and computer programming would be of great help. The instructor also reviews some of the necessary background materials

Specific goals for the course: Enable the students to learn fundamental concepts of computer security and cryptography and utilize these techniques in computing system

Brief list of topics to be covered:
The following concepts and topics will be covered with different levels of emphasis. Some topics will be covered in-depth and some other topics will be reviewed briefly.

1. Overview of Computer Security Concepts
2. Computer Security Technology and Principles
   - Cryptographic Tools
   - User Authentication
   - Access Control
   - Database and Cloud Security
   - Malicious Software (Trojans, Phishing, Spyware)
   - Denial-of-Service Attacks
Intrusion Detection
Firewalls and Intrusion Prevention Systems

3. Software Security and Trusted Systems
   Buffer Overflow
   Software Security
   Operating System Security
   Trusted Computing and Multilevel Security

4. Management Issues
   IT Security Management and Risk Assessment
   IT Security Controls, Plans and Procedures
   Physical and Infrastructure Security
   Human Resources Security
   Security Auditing
   Legal and Ethical Aspects

5. Cryptographic Algorithms
   Symmetric Encryption and Message Confidentiality
   Public-Key Cryptography and Message Authentication

6. Network Security
   Internet Security Protocols and Standards
   Internet Authentication Applications
   Wireless Network Security