CS 6210: COMPUTER SYSTEMS SECURITY

Course Description

Security issues in the realm of computers, communications, and the internet. Algorithms for encryption, cryptography, authentication, key exchange protocols, virus detection, database security, and secure internet communication. Models of security policies and computer systems certification. Prerequisites: Admission to MS in CS program, or consent of department, plus CS 3270 and CS 3350 or equivalent.

Course Syllabus

- **Basics of computer security**
  - Overview
  - Definition of terms
  - Security goals
  - Shortcomings
  - Attack and defense

- **Encryption and cryptography**
  - Ciphers and codes
  - Public key algorithms
  - Key distribution
  - Digital signatures
  - Pretty good privacy

- **Authentication and key exchange protocols**
  - Directory authentication service
  - Diffie-Hellman key exchange
  - Kerberos

- **Software security**
  - Malicious code
  - Worms
  - Intruders
  - Error detection and correction
  - OS protection policies

- **Trusted systems**
  - Memory protection
  - Access control matrix
  - User authentication
  - Security models
  - Disaster recovery

- **Database security**
  - Integrity constraints
  - Multi phase commit protocols

- **Network security**
  - Threats in networks
  - Privacy enhanced email
  - DS authentication
• Web and electronic commerce
  o Threats on the web
  o Secure socket layer
  o Client-side certificates
  o Applet security model
• Security policy: case study
  o Unix
  o Windows NT
  o Browsers and Java/scripts