

## CS 6210 : COMPUTER SYSTEMS SECURITY

---

<i>Semester Hours:</i>	3.0	<i>Contact Hours:</i> 3
<i>Coordinator:</i>	Yan Wu	
<i>Text:</i>	Various	
<i>Author:</i>	VARIOUS	
<i>Year:</i>	Various	

### SPECIFIC COURSE INFORMATION

#### *Catalog 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: Full Admission to MS in CS program or consent of department.

Course type: **ELECTIVE**

### SPECIFIC COURSE GOALS

- I understand how basic cryptographic algorithms work.
- I can explain the inner workings of a variety of security protocols.
- I can critically evaluate one or more research papers in certain subdomains of computer security.
- I can explain some common software vulnerability issues and classifications mechanisms.
- I understand security models for compute systems security, example: BLP, Ring, Chinese Wall.
- I understand the differences between certain access control models.
- I can compare and contrast Windows and Unix security architecture.
- I understand the benefits and drawbacks of firewall and intrusion detection architectures.
- I understand language security architectures.
- I can use certain language mechanisms for resource protection under program control.

## LIST OF TOPICS COVERED

- 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
- Networks Security
  - Threats in networks
  - Privacy enhanced email
  - DS authentication
- Web and Electronic Commerce
  - Threats on the web
  - Secure socket layer
  - Client-side certificates
  - Applet security model
- Security Policy: Case Study

- Unix Windows NT
- Browsers and Java/scripts