

**Course Designator/ Course Number:** CprE 531

**Course Title:** Computer Systems Security

**Course Length:** 45 hours in 15 weeks, 3 one-hour meetings per week

**Course Description:**

Computer and network security: basic cryptography, security policies, multilevel security models, attack and protection mechanisms, legal and ethical issues.

**ISU Catalog Description:**

CprE 531. Information Systems Security. (3-0) Cr. 3. F. Prereq: CprE 489 or CprE 530 or ComSci 586 or MIS 535. Computer and network security: basic cryptography, security policies, multilevel security models, attack and protection mechanisms, legal and ethical issues.

**Recent Text:**

Security in Computing, 2<sup>nd</sup> Edition. William Pfleeger. Prentice-Hall PTR 1997. ISBN: 0-13-337486-6.

**Course Learning Objectives:**

Upon completing this course a student will:

- Understand the varied types and sources of threats to computer security
- Be able to choose appropriate security mechanisms given the value of the data and the types of threats anticipated
- Understand the different categories of cryptographic algorithms and be able to explain or demonstrate the underlying mathematical problem they are based on, explain their strengths and weaknesses, and determine appropriate uses
- Understand authentication and access control, as implemented in different information models and real-life operating systems. Be able to analyze a real computer system and note exploits in the authentication and access control policies and implementation that could lead to a security exploit.
- Understand the capabilities and limitations of contemporary security technology and determine it's appropriate use.
- Understand local and state code, and rules of evidence, as it pertains to computer crime
- Understand the issues the various perspectives in the ongoing debate about security and privacy

**Major Topics:**

- Sources for security threats; risk analysis; appropriate reactions
- Cryptographic techniques: alphabetic ciphers, one-time pads, block ciphers, etc.
- Secure encryption systems: RSA, DES, Clipper, public and private key systems
- Key exchange schemes and more elaborate protocols (arbitrated, adjudicated, and self-enforcing protocols)
- Authentication mechanisms: Kerberos, X.509, etc.
- Trusted computer systems; TCB OS design; TSEC evaluation (Orange Book, Common Criteria)
- Access control mechanisms and information models: DAC, MAC, BLP, Biba, Chinese Wall, Principle of Least Privilege, lattice models
- Security technology: PGP, packet filtering, TCP wrappers, firewalls
- Network and system intrusion detection
- Policy and legal aspects of computer security

**Method of Instruction:**

The course is taught using lectures which are video taped for off campus students. Emphasis is placed on designing solutions to open-ended problems using in-class and out of class teams.

**Evaluation Methods:**

In-class examinations

Weekly problems

A substantial student-chosen report or software project

Class and team participation

**Student Enrollment:**

Taught each fall. Typical enrollment:

On campus: 60-70 students per year

Off campus: 25-35 students per year