

ICS 171: Introduction to Computer Security

Examines the essentials of computer security, including risk management, the use of encryption, activity monitoring, intrusion detection; and the creation and implementation of security policies and procedures to aid in security administration.

Course Student Learning Outcomes

- List the first principles of security and describe why each principle is important to security and its relationship to the development of security mechanisms and security policies.
- Describe why good human machine interfaces are important to system use, the interaction between security and system usability and the importance for minimizing the effects of security mechanisms.
- Analyze common security failures and identify specific design principles that have been violated, and the needed design principle, when given a specific scenario.
- List the fundamental concepts of the Information Assurance/ Cyber Defense discipline and describe how they can be used to provide system security.
- Identify the elements of a cryptographic system and describe the differences between symmetric and asymmetric algorithms, which cryptographic protocols, tools and techniques are appropriate for a given situation, and implementation issues.

Credits: 3

Lecture Hours: 3

Prerequisites: ICS 184 with a C or better, or concurrent enrollment, or consent of the instructor.