CS 370: Introduction to Security

Catalog Description: Introductory course on computer security with the objective to introduce concepts and principles of computer systems security. Notions of security, basic cryptographic primitives and their application, basics of authentication and access control, basics of key-management, basics of malware and software security.

Credits: 4  Terms Offered: Fall

Co-requisites: CS 344

Courses that require this as a prerequisite: CS 478/ECE 478, CS 445 (recommended)

Structure: On campus, three 50-minute lectures per week or two 75-minute lectures per week

Instructors: Rakesh Bobba

Course Content:
- Key Notions of Security: confidentiality, privacy, integrity, availability, accountability
- Terms and Definitions: asset, threat, vulnerability, exploit, attack, adversary, risk
- Principles of Security: least-privilege, separation-of-duty, complete-mediation etc.
- Cryptographic Primitives and their Application:
  - Symmetric-key Cryptography: historical ciphers, modern block ciphers and modes of operation, hash functions, HMAC
  - Asymmetric-key Cryptography: RSA, Diffie-Hellman Key Exchange, Digital signatures
- User Authentication: passwords, tokens, biometrics
- Access Control
  - Discretionary Access Control (DAC): ACLs & Capabilities
  - Role-based Access Control (RBAC)
  - [Optional] Mandatory Access Control: Bell-LaPadula, Biba, Chinese-Wall
- Malware: introduction to types of malware and overview of defense strategies
- Software Security: common software security issues such as buffer overflows and mitigation/defense strategies

Learning Resources:
- Lecture notes from the instructor

Measurable Student Learning Outcomes:
At the completion of the course, students will be able to…
1. **Understand** the need for cyber security, key notions of security, and well established security principles and security mechanisms/controls
2. **Apply** security controls including cryptographic primitives to secure systems while adhering to applicable security principles
3. **Critically evaluate** system designs and security controls in place to **identify** security weaknesses
4. **Assess** security requirements of systems and **select** security controls that are appropriate
5. **Describe** common security properties and requirements, common security issues in systems and their implications

**Evaluation of Student Learning:**
- Homeworks/Quizzes/Participation (approx. 20%)
- Programming Assignments (approx. 20%)
- Exams (approx. 60%)

**Students with Disabilities:**
Accommodations are collaborative efforts between students, faculty and Disability Access Services (DAS). Students with accommodations approved through DAS are responsible for contacting the faculty member in charge of the course prior to or during the first week of the term to discuss accommodations. Students who believe they are eligible for accommodations but who have not yet obtained approval through DAS should contact DAS immediately at 737-4098.

**Link to Statement of Expectations for Student Conduct**, i.e., cheating policies [http://oregonstate.edu/studentconduct/offenses-0](http://oregonstate.edu/studentconduct/offenses-0)

Revised: Winter 2015