CSE 4272 Computer and Information Security (3 credits

Primary instructor: William Allen

Textbooks and references:

Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, 4th edition. Prentice-Hall, 2006. 0132390779, 978-0132390774. (T)

Course information:

2014–2015 Catalog description: CSE 4272 Computer and Information Security (3 credits). Introduces the fundamentals of computer security. Includes vulnerability analysis, threat modeling and risk assessment, and techniques for asset protection. Discusses economic, legal and ethical issues in computer security. Focuses on a system-wide view of security and discusses trends in current literature. Prerequisites: CSE 2010 or ECE 2552.

Prerequisites by topic: Computing ideas through algorithms and data structures.

Place in program: Advanced elective

Course outcomes & related student outcomes: The student will be able to

1. Understand the risks involved in computing and be able to classify specific threats as a risk to confidentiality, integrity or availability. (1: Fundamental knowledge)
2. Describe common software vulnerabilities and explain secure design and programming techniques that can mitigate those vulnerabilities. (1: Fundamental knowledge & 4c: Tradeoffs in design choices)
3. Describe common threats to networks, operating systems and databases and explain techniques and technologies that can protect against those threats. (1: Fundamental knowledge)
4. Understand issues related to private information, including disclosure, data sensitivity, and the dimensions of privacy. (5: Awareness of professional issues and responsibilities & 6: Analyze computing's impact)
5. Explain requirements and techniques for the administration of security, including risk analysis, security policies, controls, and physical threats. (5: Awareness of professional issues and responsibilities)
6. Understand issues related to the economic impact of security. (6: Analyze computing's impact)
7. Describe legal protections for programs and data and understand the difference between legal and ethical viewpoints. (5: Awareness of professional issues and responsibilities)

Topics covered:

1. Attacks, vulnerabilities, and defenses
2. Program protection

3. Protection of operating systems
4. Network security
5. Database security
6. Elementary cryptography
7. Threat modeling and risk assessment
8. The economics of cybersecurity
9. Legal, ethical, and privacy issues

Approved by: William Allen, Associate Professor

Signature: ______________________________ **Date:** 2/26/2015