CLEMSON CPSC 4200

Computer Security Principles

CATALOG DESCRIPTION

Covers principles of information systems security, including security policies, cryptography, authentication, access control mechanisms, system evaluation models, auditing, and intrusion detection. Computer security system case studies are analyzed.

PRE-REQUISITES

- Clemson Students: **CPSC 3220** with a C or better or **ECE 3220** with a C or better; and **CPSC 3600** with a C or better or **ECE 4380** with a C or better.
- Transient/Visiting Students: A course each in operating systems & networking; C++ familiarity.

COURSE LEARNING OUTCOMES

1. Identity physical attacks and counter measures
2. Specify requirements and mechanisms for identification and authentication and identify related threats.
3. Explain common network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms.
4. Explain the requirements of real-time communication security and issues related to the security of web services.
5. Identify the appropriate defense mechanism(s) and its limitations given a threat.
6. Describe the cost and tradeoffs associated with designing security to a product.
7. Develop a conceptual vocabulary for applied cryptography.

BRIEF LIST OF TOPICS

Physical security, operating systems security, malware, mobile platform security, network security, software security, web security, cryptography, security models and practice.

TEXTBOOK

(Recommended) Goodrich & Tomassia. Introduction to Computer Security. ISBN-13: 978-0133575477

Please note that this syllabus is a general plan for the course; a finalized syllabus will be distributed on the first day of classes with additional information


School of
COMPUTING
SUMMER of CYBER