

CpE 691 Information Systems Security Syllabus

Catalog Description:

CpE 691 Information Systems Security (3-0-3)

History of network security; Classical information security; Cryptosecurity; Kerberos for IP networks; Private and public keys; Nature of network security; Fundamental framework for network security;; Analysis and performance impact of network topology;; Vulnerabilities and security attack models in ATM, IP and mobile wireless networks; Security services, policies, and models; Trustworthy systems; Intrusion detection techniques - centralized and distributed; Emulation of attack models and performance assessment through behavior modeling and asynchronous distributed simulation; Principles of secure network design in the future; Projects in network security and student seminar presentations. Cross-listed with NIS 691.

Recommended Text Books:

Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World," Wiley, ISBN 0-471-25311-1

---, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley, ISBN 0-471-11709-9.

Instructor:

Bruce McNair, Distinguished Service Professor of ECE.

Goals:

The goal of Information Systems Security is to familiarize students with the security issues and technologies involved in modern information systems, including computer systems and networks. Students will gain an understanding of the various ways in which information systems can be attacked and tradeoffs in protecting networks. Students will gain an appreciation of the need to develop an understanding of underlying system applications and potential security issues early in the design process.

Recommended prerequisites by topic:

Probability and random variables
Systems Theory
Switching Theory and Logical Design
Operating Systems

Grading Policy:

- Two research papers 20% each (individual effort)
- One research paper seminar presentation 20% (individual effort)
- Final project report: 20% (individual or small group effort)
- Final project presentation: 10% (individual or small group effort)
- Participation in class discussions (WebCT discussion groups): 10%

All assignments provide opportunities for extra credit work. Work that goes significantly beyond what is asked will be graded accordingly.

For completely on-line sections of the course (e.g., Stevens WebCampus), seminar and project presentations will be delivered by students using standard presentation tools (e.g., Powerpoint) with text or voice annotated slides

Course Components:

- *Engineering - 100%*

Course Web Site:

<http://koala.ece.stevens-tech.edu/~bmcnair/ISS-xxx> where xxx is current semester (e.g., S04)

Schedule of Topics

This is the list of detailed topics and likely order. The specific schedule will vary by semester, depending on current issues.

Introduction

- Definition of security
- Assessing security
- Security terminology
- Historical developments
- Structure of security

Cryptography

- Applications of cryptography
- Terminology
- Evolution of cryptography, Caesar ciphers, one-time pads
- Operation of DES, AES
- Public-key cryptosystems

Topics in Information Systems Security

- Minimum privilege
- Compartmentalization
- Dual controls
- Security perimeters
- Trustworthy software, proof of design correctness
- Single-points-of-failure
- Covert channels
- Inference
- Security models
 - Requirements
 - Types
 - State-machine models
 - Mandatory/Discretionary controls
 - Information-flow models
 - Informal models

Kerberos Authentication

Authentication in centralized systems

Distributed Authentication

Denial of Service attacks

Security vs. ATM, IP, wireless mobile networks

QoS

- Traffic modeling
- Network topology

Security Protocols

- Zero-knowledge proofs
- Subliminal channels

Oblivious transfer
Digital signature schemes
Bit commitment
Digital cash
Secure contract signing
Secure voting
Digital certified mail
Anonymous message broadcast
TEMPEST and related topics

Last revised: October 12, 2006