



Stevens Institute of Technology

WebCampus.Stevens

Syllabus

Course Number: CS 694WS

Course Name: Enterprise Security and Information Assurance

Overview

Paragraph description of course objectives and requirements:

Information assurance and security are recognized as very important issues in electronic business transactions and financial systems from the managers, users, and providers viewpoints. This course addresses the security of e-business and cyber environments from an end-to-end perspective. The information security methodologies of inspection, protection, detection, reaction, and reflection are addressed in detail. Topics include: security at network, transport, and application levels, firewalls, virtual local area networks (VLANs), secure financial transaction techniques, backup and disaster recovery techniques, smart card security, estimation and management of risks associated with security.. The course includes a project.

Prerequisites: CPE 678/CS 666 (Information Networks 1) or CS 521 (TCP/IP Networking) or TM 610 (Business Information Networks) or Mgt 776 (Managing Information Networks), or equivalent

Cross-listed with. None

Learning Goals

After taking this course, the student will be able to:

- Understand the nature and value of information, information security and information assurance, information security plan and its phases, and information security architecture
- Understand security services, and mechanisms, including cryptographic techniques, Digital Certificate, digital signatures, and message integrity techniques
- Understand and design the phases of a security plan, including Security Inspection, Security Protection, Security Detection, Security Reaction, and Security Reflection
- Recognize security threats, vulnerabilities, and attacks
- Describe information availability models, and backup and recovery methods
- Describe the intrusion process, intrusion detection methods
- Understand incident response philosophies and design an incident response plan
- Understand firewalls, their types, and applications
- Understand IP security, the IPSec protocol, and Virtual Private Networks (VPNs)
- Understand Web security and Secure Socket Layer (SSL)/TLS
- Design application security
- Understand Smart Cards and their Security issues

Pedagogy

The course will employ lectures, class discussion, and individual homework. Students will also have individual or team projects and will make one team presentation during the class. The course includes a midterm exam and a final exam.

Required Text(s)

William Stallings, *Network Security Essentials, Applications and Standards*, Third Edition, Prentice Hall, ISBN: 0-13-238033-1, 2007

Required Readings

Reading will be assigned for each week, posted on the course website.

Assignments

1. Reading assignment – posted weekly
2. Class Participation - To enhance the learning experience, all students are expected to participate in class discussion board by responding to the posting by the professor and other students. A minimum of 3 substantive postings is expected from each student each week.
3. Homework – Homework must be completed and submitted on WebCT by the required date each week.
4. Project presentation - Each student team will choose a project, submit a project report by the end of the semester and make a slide presentation online.

The assignments and their weights are as shown below:

- 20% for Homework Assignments (due via the WebCT Submission tool on Sunday every week; 50% penalty per week if delayed for any reason)
 - 20% for Project
 - 20% for Participation in online technical discussions (15% for Discussions, 5% for Chat)
 - 20% for Midterm Exam
 - 20% for Final Exam
- TOTAL** **100%**

Please note that assignments in this class may be submitted to www.turnitin.com, a web-based anti-plagiarism system, for an evaluation of their originality.

Course Schedule (Sample)

To be posted September 10, 2006:

- Assignment 1** (due September 17)
- Unit 1: Introduction**
 - E-commerce, e-business, and e-services
 - Nature and value of information
 - Security issues in e-business
 - Information security
 - Information Assurance
 - Information security plan and its phases
 - Information security architecture

To be posted September 17:

- Assignment 2** (due September 24)
- Unit 2: Security Overview, Part 1**
 - Security attacks, services, and mechanisms
 - Cryptographic techniques
 - Secret-key cryptography
 - Data Encryption Standard (DES), 3DES, and AES
 - Symmetric key distribution

To be posted September 24:

- Assignment 3** (due October 1)
- Unit 2: Security Overview, Part 2**
 - Public-key cryptography
 - Key management
 - Digital Certificate and Certification Authority

To be posted October 1:

- Assignment 4** (due October 8)
- Unit 3: Security Inspection**
 - What is Security Inspection?

- Identifying resources and their value
- Security threats and their assessment
- Security attacks and their types
- Security vulnerabilities
- Evaluating losses
- Security safeguards
- Appendix: Web spoofing

To be posted October 8:

- ❑ **Assignment 5** (due October 15)
- ❑ **Unit 4: Security Protection, Part 1**
 - What is Security Protection?
 - Security vision, strategy, and procedures
 - Access security
 - Identification
 - User authentication
 - Authorization
 - Digital signature and non-repudiation
 - Role-based Access Control (RBAC)
 - Firewalls

To be posted October 15:

- ❑ **Assignment 6** (due October 22)
- ❑ **Unit 4: Security Protection, Part 2**
 - Information availability models
 - Backup and recovery
 - Appendix – A Web attack scenario
- ❑ **Unit 5: Security Detection, Part 1**
 - What is Security Detection?
 - Intruders types
 - Intrusion methods
 - Intrusion process

To be posted October 22:

- ❑ **Assignment 7** (due November 5)

To be posted October 29:

- ❑ **Unit 5: Security Detection, Part 2**
 - Intrusion detection
 - Honey pots
 - Message integrity detection

October 30: Midterm Exam, 9:30-11:30 PM EST (covers Units 1 through 4)

To be posted November 5:

- ❑ **Assignment 8** (due November 12)
- ❑ **Unit 6: Security Reaction**
 - What is Security Reaction?
 - Incident response philosophies
 - Incident response plan
 - Incident determination
 - Incident notification
 - Incident containment
 - Assessing the damage
 - Some good practices

- ❑ **Unit 7: Virtual Local Area Networks (VLANs)**
 - E-business reference architecture
 - E-business “providers”
 - Data centers and Web hosting models
 - Overview of Local Area Networks (LAN) protocol architecture
 - Virtual LANs (VLANs)
 - VLAN standardization (IEEE 802.10)
 - Using VLANs in data centers for traffic separation

To be posted November 12:

- ❑ **Assignment 9** (due November 19)
- ❑ **Unit 8: IP Security**
 - Overview of IP and its security
 - Tunneling and its protocols
 - The IPSec protocol
 - Virtual Private Networks (VPNs)

To be posted November 19:

- ❑ **Assignment 10** (due December 3)
- ❑ **Unit 9: Security at the Transport Level**
 - Web security considerations
 - Secure Socket Layer (SSL) architecture
 - SSL protocols
 - SSL phases
 - SSL exchanges
 - Transport Layer Security (TLS)

November 26: Project reports due

To be posted November 26:

- ❑ **Unit 10: Security at the Application Level**
 - *Security within the application*
 - *Privacy issues*
 - *Secure Electronic Transaction (SET)*
 - *The dual signature technique*
 - *SET message processing*
 - *Certificate management*
 - *Implementation issues*
 - *Email Security*
 - *Pretty Good Privacy (PGP)*
 - *S/MIME (Secure MIME)*

To be posted December 3:

- ❑ **Unit 11: Smart Cards and their Security**
 - Smart card characteristics
 - Smart card classification
 - Smart card life cycle
 - Authentication in smart cards
 - Multi-application smart cards
 - Smart card standards
 - Attacks on smart cards

December 11: Final Exam: 9:30-11:30 PM EST (covers Units 5 through 11)