



Stevens Institute of Technology

WebCampus.Stevens

Syllabus

Course Number: CS 573WS

Course Name: Fundamentals of Cybersecurity

Overview

Paragraph description of course objectives and requirements:

This course provides an overview of Information Security and Assurance. Students will be exposed to the spectrum of security activities, methods, methodologies, and procedures with emphasis on practical aspects of Information Security. Topics include: security principles, threats, attacks, security models, security policies, overview of authentication, encryption, and certifications, security detection, security in Unix and Windows environments, business risk analysis, protection of information assets, examination of pre- and post-incident procedures, and an overview of the information security evaluation. The course includes a project.

Prerequisites: CS 520 (Introduction to Operating Systems) or equivalent

Cross-listed with. None

Learning Goals

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

- Understand security principles, threats and attack techniques
- Describe authentication and access control
- Describe lattices, reference monitors, and security models
- Understand basic cryptography
- Authentication in distributed systems
- Understand network security and operating system security
- Understand software security and database security
- Design protection measures

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)

Computer Security, 2nd ed.
Author: Dieter Gollmann
Publisher: John Wiley & Sons, 2006
ISBN: 0-470-86293-9

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)

| Posting date and instructor | Textbook chapter references | Topic to be covered | Assignment and due date |
|-----------------------------|--|--|-------------------------|
| Week 1 | Chapters 1 and 2 | Security principles, threats and attack techniques <ul style="list-style-type: none"> • Introduction to security • Information security • Security triad: Confidential, Integrity, Availability • Focus of control • Security threats and attacks • Security management | |
| Week 2 | Chapter 3 and part of Chapter 4 | Authentication and access control <ul style="list-style-type: none"> • Identification • Authentication • Authentication by passwords • Protecting passwords • Access control structures • Types of access control | |
| Week 3 | Remaining part of Chapters 4 and Chapter 5 | Lattice and reference monitors <ul style="list-style-type: none"> • Security levels and categories • Lattice diagram • Reference monitors • Security kernel • Hardware security features • Protecting memory | |
| Week 4 | Chapters 8 and 9 | Security models <ul style="list-style-type: none"> • Bell-LaPadula • Biba • Non-deducibility • Non-interference • Other models | |
| Week 5 | Chapter 11 | Cryptography <ul style="list-style-type: none"> • Cryptographic mechanisms • Digital signatures • Encryption • Certificates | |
| Week 6 | Chapters 12 | Authentication in distributed systems <ul style="list-style-type: none"> • Key establishments and authentication • Kerberos | |

| | | | |
|---------|--------------------|--|--|
| | | <ul style="list-style-type: none"> • Public key infrastructures • Single sign-on | |
| Week 7 | | Mid Term Exam Includes material covered so far. | |
| Week 8 | Chapters 13 | Network security <ul style="list-style-type: none"> • Protocol design principles • ISO architecture • IP security • SSL/TLS • Firewalls • Intrusion detection | |
| Week 9 | Chapters 6 and 7 | Unix security and Windows security <ul style="list-style-type: none"> • Subjects, objects and access control • General security principles • Access components • Access decisions • Administration and management issues | |
| Week 10 | Chapters 14 and 17 | Software security and database security <ul style="list-style-type: none"> • Memory management • Data and code • Relational databases • Access control in databases • Statistical database security | |
| Week 11 | Chapters 15 and 16 | Java Security, Mobile Security <ul style="list-style-type: none"> • GSM security • Wireless LAN security | |
| Week 12 | Chapter 10 | Protection measures <ul style="list-style-type: none"> • Business risk analysis • Prevention, detection and response • Information classifications • Security evaluation | |
| Week 13 | | Discussions on project reports | |
| Week 14 | | Final Exam Includes material covered after the Midterm exam. | |