CS695 -- Network and Computer Security for Business
(Online Course, Fall 2006)
Revised October 24th, 2006

Textbooks:

"Security Engineering: A Guide to Building Dependable Distributed Systems", Ross Anderson, Wiley, 2001. ISBN: 0-471-38922-6 (*For Weeks 1 – 3*)
This book is available online chapter by chapter at
http://www.cl.cam.ac.uk/~rja14/book.html

"Network Security Essentials: Applications and Standards" , THIRD EDITION, William Stallings, Prentice-Hall, 2007. ISBN: 0132380331 (*For Weeks 4 – 6 and Week 3 's Lecture on Cryptography*)

Course Description

The goal of the course is to present and explain formal and technical aspects of computer security on examples of real world systems and thus enable the student to relate theoretical approaches and technical implementations to the security requirements of the problem domain. The course provides an in-depth presentation of security issues in computer systems, networks, and applications. Formal security models are presented and illustrated on operating system security aspects, more specifically memory protection, access control and authentication, file system security, backup and recovery management, intrusion and virus protection mechanisms. Application level security focuses on language level security and various security policies; conventional and public keys encryption, authentication, message digest and digital signatures. Internet and intranet topics include security in IP, routers, proxy servers, and firewalls, application-level gateways, Web servers, file and mail servers. Discussion of remote access issues, such as dial-up servers, modems, VPN gateways and clients.

Course Syllabus

Week 1 -- Introduction and Security Overview (10/30/06 – 11/5/06)

Introduction
Threats & Targets
What can you do?
Security Overview
Functional Classification of Security
Application Level Security
  Examples - Web Applications, SQL Injection, CSS, Buffer Overruns
Famous Examples (Blaster, Slammer, etc.)

Week 2 – Access Control and Operating Systems Security (11/6/06 – 11/12/06)

Operating Systems Security
    Memory and Address Protection
Access Control
    Access Control Matrix, Access Control Lists, Capability Lists, etc.
Administrative Tasks in Access Control Methods
    Groups and Permissions, Protection Rings, RBAC, and Lattices
Security Models
    Bell-LaPadula, Biba, Chinese Wall, Clark-Wilson
UNIX Operating Systems Security and Role Based Access Control

Week 3 – Windows Security, Application Security and Cryptography (11/13/06 – 11/19/06)

Windows Security
    Users and Groups, Access Control Model, Registry,
    Domains and Trust Relationships, Active Directory,
    Identification and Authentication, Role Based Access Control
Application Security
    More on Buffer Overflows
    Java Security
Cryptography
    Encryption, Decryption, Symmetric and Asymmetric
    Public/Private Key, DES, RSA
    Message Digests, Digital Certificates

Mid Term Exam (3 Hour Exam) 11/20/06 – 11/26/06
    Will cover all the above material but only a part of Cryptography.
    Cryptography questions will also be included in the Final Exam.

Week 4 -- Network Security Principals and Authentication Protocols (11/27/06 – 12/3/06)

1. Fundamentals of Network Security
   - 1.1. Introduction
   - 1.2. Rational for Network Security
   - 1.3. Objectives of Network Security
   - 1.4. Overview of Network Architectures
     - 1.4.1. OSI Network Model
     - 1.4.2. Internet Network Model
   - 1.5. Network Security Issues
   - 1.6. Security of Network Layers
   - 1.7. Security Threats, Risks, Safeguards and Vulnerabilities
   - 1.8. Network Threats and Safeguards:
     - 1.8.1. LAN
     - 1.8.2. WLAN
     - 1.8.3. MAN
     - 1.8.4. WAN
     - 1.8.5. Internet
   - 1.9. Network Security Mechanisms
   - 1.10. Models of Network Security

2. Authentication
   - 2.1. Introduction
   - 2.2. Authentication Applications
     - 2.2.1. Introduction
     - 2.2.2. Kerberos
     - 2.2.3. X.509 Authentication Service
   - 2.3. Summary
   - 2.4. References

Week 5 -- Network Layer Security (12/4/06 – 12/10/06)

1. IP Security
   - 1.1. IPsec Architecture
   - 1.2. Authentication Headers
   - 1.3. Encapsulating Security Payload
   - 1.4. IPsec implementation
   - 1.5. Combining Security Associations
   - 1.6. Key Management
   - 1.7. Summary

2. Firewalls
    2.1. Firewall Design Principles and Configurations
    2.2. Firewall Types
        2.2.1. Packet-filtering routers
        2.2.2. Application-level gateways
        2.2.3. Circuit-level gateways
    2.3. Firewall Configurations
    2.4. Summary
    2.5. References

Week 6 -- Higher Layers Security (12/11/06 – 12/17/06)

1. Web Security
    1.1. Introduction
    1.2. SSL and TLS
    1.3. Secure Electronic Transfer

2. Email Security
    2.1. Introduction
    2.2. PGP
    2.3. S/MIME

3. Summary

Final Exam (3 Hour Exam) 12/14/06 – 12/18/06

Will include questions from Weeks 4 – 6 and from the Cryptography lecture from Week 3.