CIS 221 Introduction to Computer Architecture

Co/Prerequisites

Prerequisite(s): Comp 150, CIS 192

Textbooks

1. Security Engineering: A guide to Building Dependable Distributed Systems; Ross Anderson; John Wiley & Sons, Inc; ISBN: 0-471-38922-6
2. IETF Requests for Comments (RFCs)
3. W3C Standards
4. The World Wide Web

Course Description

This course provides an introduction to proven techniques for protecting information systems from intruders, while allowing the required access to authorized users. This course is introductory and is designed to provide an overall view of security in the modern information world. Several hands-on lab projects will be completed using Linux-and/or Windows-based computer systems.

Instructor: Daniel Harris
Email: dan.harris@ucfv.ca

Learning Outcomes

This course provides students with a clear picture of information security engineering, a subject that covers a wide area of computer science and social engineering. By the end of this course, students will have studied:

1. Basic cryptology such as encryption, authentication and key management
2. Building secure protocols
3. Access control, Security Policy Models, Nuclear Command and Control
4. Distributed Denial and Service Attacks, Intrusion Detection and Firewalls
5. Secure networking and internetworking (e.g., IPSec, SSL, VPN, firewalls)
6. Digital content protection (e.g. S/MIME, XML digital signature and XML encryption)
7. Physical security and biometrics (e.g. tamper resistance, emission security, secure tokens)
8. Password protection and password based protocols
9. Management issues
10. System evaluation and assurance
11. Wireless security (e.g. Bluetooth, IEEE 802.11, and WAP) - an optional reading assignment

Syllabus:

- Introduction
- What is Information Security Engineering?
- Protocols
- Password, Access Controls, and Distributed Systems
- Password and psychology issues
- Technical protection of passwords
- Operating system access control
- Fault-tolerance and failure recovery
- Basic Cryptology
- Symmetric encryption: DES, TDES, AES
- Symmetric authentication
- Asymmetric encryption and digital signature: RSA, DSA
- Key management and Public Key Infrastructure
- Security policy models, Nuclear command and control
- Multilevel Security
- Banking and Bookkeeping
- Monitoring Systems
- Nuclear Command and Control
- Physical security and biometrics
- Biometrics
- Physical tamper resistance
- Smart cards
- Emission security
- Network and Internetworking security, digital content protection
- The most common attacks
- Distributed Denial of Service Attacks (DDoS)
- Intrusion detection
- Firewall
- IETF protocols (IPSec, VPN, IKE, S/MIME)
- XML digital signature, XML encryption
- eCommerce Security, Copyright, and Privacy
- Protecting eCommerce systems
- Copyright and privacy
- Management Issue, and System Evaluation and Assurance
- Management Issues
- System Evaluation and Assurance
- Wireless Security
- Bluetooth
- IEEE 802.11
- Wireless Application Protocols (WAP)

Week 2:
Chapter 1 and 2. Basics of information security engineering through studying several examples.

Week 3:
Chapters 3, 4, 6. Passwords, access control and distributed systems.

Week 4:
Chapter 5. Basic cryptographic algorithms.

Week 5:
(Chapter 7, pp 137-160, Chapter 8 (Sections 8.1 and 8.2) pp 161-172, Chapter 9, pp185-206, Chapter 10 (Sections 10.1 and 10.2) pp 207-216, Chapter 11, 231-241. Security policies, multilevel security, monitoring systems, and nuclear command and control.

Week 6:
Chapter 13 (skim sections 13.5-13.7), Chapter 14, Chapter 17 (Section 17.1 and 17.2)
Biometrics, identity-based public cryptosystems, physical tamper resistance devices, emission security, and telecom system security

Week 7:
Midterm Exam

Week 8, 9, 10:
Chapter 18
The most common attacks, distributed denial of service attacks, intrusion detection, firewalls, IETF security protocols, and XML security.

Week 11:
Chapter 19 (skim section 19.5), Chapter 20 (skim sections 20.4.1, 20.4.3, 20.4.4)
E-commerce systems, copyright and privacy.

Week 12:
Chapter 22-23. Management issues, system evaluation and assurance.
Project assigned.

Week 13:
Course review.

Grading Scheme

Component	Percentage

Assignments	20%
Group Mark	10%
Midterm exam	35%
Final exam	35%
Total	100%

You **must pass the final exam** to pass the course.

Letter Grades

Course Percentage	Letter Grade
95% or greater	A+
90% or more, less than 95%	A
85% or more, less than 90%	A-
80% or more, less than 85%	B+
75% or more, less than 80%	B
70% or more, less than 75%	B-
65% or more, less than 70%	C+
60% or more, less than 65%	C
55% or more, less than 60%	C-
50% or more, less than 55%	P
Less than 50%	NC