CSCI 451 Computer Security

by Hui Chen, Ph.D.

Overview

This course focuses on communication security in computer systems and networks. It is intended to provide students with a comprehensive introduction to the field of network security. The course covers critical network security services such as authentication and access control, integrity, and confidentiality of data, routing, firewalls, virtual private networks, and web security. Where appropriate, we examine threats and vulnerabilities to specific a nchitecture and protocols.

*Prerequisites:*CSCI 358 Introduction to Information Assurance or approval of the instructor

Syllabus

Download it in a PDF file

Textbook

You may access VSU's Safari's Book Online subscription from using VSU library's off-campus access service.

- Matt Bishop, Introduction to Computer Security, Addison-Wesley Professional, October, 2004, ISBN-13: 978-0-321-24774-5.

Reference Books

- Matt Bishop, Computer Security: Art and Science, Addison-Wesley Professional, October, 2004, ISBN-13:978-0-321-24744-5. *This book is a version of the book with more formal and mathematical treatment of the subject than the textbook. If you wish more formal and mathematical treatment, read this book instead.*
- Dorothy Elizabeth Robling Denning. 1982. Cryptography and Data Security. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA.
- Bruce Schneier. 1996. Applied Cryptography. John Wiley & Sons.
- Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. 2010. Cryptography Engineering. John Wiley & Sons.

Class Schedule and Material

08/17 Course Overview and Introduction to Computer Security

Topic: Overview of basic computer security concepts

Reading:

- Chapter 1 of Textbook
- The matasano crypto challenges

Assignment:

- Lab 1 (Due 08/24)
- Reading and Oral Presentation: Comparing Expert and Non-Expert Security Practices *(1-student presentation in class on 08/24)*.

08/19 - 08/21 Access Control Matrix

Topic: Access Control Matrix

Reading:

- Sections 2.1 and 2.2 of Textbook
- Sections 2.3, 2.4, and 2.5 of Textbook

Assignment:

- (Homework L2-1) questions 1(a), 1(c), 1(e) and 1(g) in exercises 1.11 in the textbook (page 22) and question 1(a) in exercises 2.6 in the textbook (page 35)

08/24 Students' Presentation and Discussion

Reminder: Lab 1 is due

- Students' Presentation: Comparing Expert and Non-Expert Security Practices

08/26 Security Policies

Topic: Overview of Security Policies

Assignment:

- See lecture notes

Reading:

- Chapter 4 of Textbook

08/28 Examples of Policy Models

Topic: Policy Examples: The Bell-LaPadula Model; Biba Integrity Model; Clark-Wilson Integrity Model; Chinese-Wall Model

Assignment:

- See lecture notes

Reading:

- Chapter 5 of Textbook
- Chapter 6 of Textbook
- Chapter 7 of Textbook

08/31 - 09/04 Basic Cryptography I

Topic: Transposition Ciphers; Substitution Ciphers; Vigenere Cipher; Simple Cryptanalysis;

Reading:

- Sections 8.1 - 8.2.2 of Textbook
- The instructor's notes on Index of Coincidence

Program:

- Making Vigenere Tableau in: C++; C; Java; and Matlab/Octave
- *Attacking Caesar Cipher*: attackcaesar.m
- *Attacking Vigenere Cipher*: readline.m findcommonsubstrings.m computeic.m guesskey.m vigenere.m computeletterfreq.m;

Assignment:

- See lecture notes.
- *Ciphertext for Exercise L5-5*: pg.txt tc.txt;
- (Homework L5-1) question 8 in exercise 8.7 in the textbook (page 120)

09/07 Labor Day Holiday. University Closed. No Class.

09/09 Basic Cryptography I (Continued)

Topic: continue the lectures from 08/31 - 09/04

09/11 Basic Cryptography II

Topic: DES; AES; RSA; Cryptographic Checksums;

Reading:

- Sections 8.2.3 - 8.6 of Textbook

Assignment:

- Exercises in lecture notes
- Reading and Oral Presentation: Side-Channel Attacks on AES Implementations [It's all a question of time – AES timing attacks on OpenSSL and A shared cache attack that works across cores and defies VM sandboxing—and its application to AES] *(1-student presentation in class on 10/07)* .

9/14 - 09/18 Key Distributions

Reading:

- Sections 9.1 and 9.2 of Textbook

Assignment:

- See lecture notes

09/21 - 09/25 Public Key Infrastructure

Reading:

- Section 9.3 of Textbook

Assignment:

- Mini-Project 1 on PKI and Mini-Project 2 on PGP (due two weeks after it has been posted. Submit your work to Blackboard.)

Resources for Mini-Project 1 The Mini-Project 1 is based on the PKI lab developed by Professor Wenliang Du at Syracus University. You may download the lab manual from this site. Download a Debian Linux virtual machine prepared for this lab from either Dropbox or OneDrive. Both the username and password are "debian" (without the quotation marks).

09/28 Midterm Review

09/30 Midterm Exam

10/02 Recap on Midterm Exam

10/05-10/09 Fall Break. No Class.

10/12 Cipher Techniques: Common Problems

Reading:

- Section 10.1 of Textbook

Assignment:

- Students' Presentation: Side-Channel Attacks on AES Implementations [It's all a question of time – AES timing attacks on OpenSSL and A shared cache attack that works across cores and defies VM sandboxing—and its application to AES]

10/14 Cipher Techniques: Stream and Block Ciphers

Reading:

- Section 10.3 of Textbook

Assignment:

- Mini-Project 2 on PGP and Mini-Project 2 on PGP (due two weeks after it has been posted. Submit your work to Blackboard.)

10/17 Cipher Techniques: Networks, Cryptography, and Example Protocols

Reading:

- Section 10.4 of Textbook

10/19 Design Principles

Reading:

- Chapter 12 of Textbook

Assignment:

- (Homework L12-1) Answer questions 2, 3, 7, and 10 in Chapter 12 of the textook (page 208 - 209)

10/19 - 10/23 Representing Identity

Reading:

- Sections 13.1 - 13.5 of Textbook

10/26 -10/30 Identify and Anonymity on the Web

Reading:

- Section 13.6 of Textbook

Assignment:

- (Homework L14-1) Answer questions 1 in Chapter 13 of the textook (page 234).

Note: to answer this question, you may want to consult references on web cookies, e.g., Document.cookie Web API , and IETF RFC 6265 .

11/02 - 11/06 Controlling Access to Files

Reading:

- Sections 14.1 - 14.2 of Textbook

Assignment:

- See lecture notes

11/11 - 11/13 Ring-based Access Control

Reading:

- Section 14.4 of Textbook

11/09 - 11/13 Introduction to Assurance

Reading:

- Chapter 17 of Textbook

11/25 Thanksgiving Holiday. University Closed. No Class.

11/30 Review for Final Exam

12/02 Class Project; Q & A; Last Day of Classes

12/03 Reading Day. Senior Project Presentation.

12/04 - 12/10 Final Examination Week

CSCI451 Final Exam:

10:30 - 12:30PM, Monday, December 7, 2015