Computer Security

CIS 5370, Fall 2014
Department of Computer Science, Florida State University

Class time and location

Monday, Wednesday and Friday, 10:10 – 11:10 AM, LOV 103

Instructor

- Instructor: Xiuwen Liu (pronounced as Shu-wen Lea-l)
- Email: liux@cs.fsu.edu (most effective way to contact me)
- Home page: http://www.cs.fsu.edu/~liux
- Office: 166 Love Building (LOV); Phone: (850) 644-0050
- Office hours: Monday and Wednesday, 1:15 PM – 2:15PM and by appointments

Teaching Assistant

- Grader: Nigel Nye
- Email: nye@cs.fsu.edu
- Office: TBA
- Office hours: Monday, 11:30AM-12:30PM and 1:00PM-2:00PM

Class Home Page

http://www.cs.fsu.edu/~liux/courses/cis5370-2014/index.html.
This web site contains the up-to-date information related to this class such as news, announcements, assignments, lecture notes, and useful links to resources that are helpful to this class. Besides the web pages, Blackboard will be used to communicate changes and updates and post grades for this class; in particular, I will send emails using email addresses in the Blackboard system and please make sure that your email address on record is current.

Rationale

With affordable desktop and laptop computers, large storage devices (e.g., hard drives), hardware, wide availability of the high speed internet connections, and more recently Internet-capable 3G and 4G smartphone and similar devices, the earth becomes highly connected that almost everyone can reach any other one on the planet as long as they are connected to the Internet. The unprecedented connectivity has unleaded unique potentials of computer technology (e.g., huge storage spaces and fast computing), leading to new services that were not imagined ten years ago. Not only our daily life activities heavily rely on the Internet, and government and the critical infrastructures we take for granted rely on the intended behaviors of computers and the underlying network. Unfortunately, the high connectivity has also created new problems, from spyware to steal data, computer viruses and worms to destroy data, to network-enabled weapons, to cyber wars that can disable companies and even countries (such as Stuxnet). All these problems are related to computer security. Due to its paramount importance, computer security is not just one academic research area. Many security products are installed on typical computers; in the United States, there are multiple federal agencies dedicated to computer security; the computer security is a multi-billion industry that is estimated to grow steadily (just click https://www.google.com/#q=computer+security+industry+growth and see). Computer security related issues have been widely recognized in software development companies. As computer security techniques evolve continuously along with product improvements and new service opportunities, computer security is and will remain to be an important and valuable area in the perceivable future with new career opportunities; in recent years, computer security has enjoyed a zero and low unemployment rate (see http://www.techjournal.org/2011/07/information-security-analysts-unemployment-rate-zero/ and http://www.bls.gov/oes/current/oes151122.htm).

Course Description

This course provides introductory but comprehensive coverage of fundamental problems, principles, techniques, and algorithms in computer security, including basic cryptographic algorithms, symmetric key cryptography, public key cryptography, hash functions, authentication methods, authorization mechanisms, authentication protocols, real-world security protocols, malware and software attacks, malware analysis and software reverse engineering, secure software development, insecurity in operating system and software, trusted computing approaches to secure and trusted computer systems, and web security. Additionally, as computer security relies on many interdependent components, this course will also cover real world policy and implementation issues through case studies and papers in the literature. It also offers opportunities to explore implementation, research, and applications of computer security techniques to solving real world problems.

Prerequisites

COP 4610 – Operating Systems and Concurrent Programming or consent of the instructor; basic knowledge and experience with computer systems; basic knowledge and understanding of modular mathematics, permutations, probability, and linear algebra. Proficient programming skills are not required; but students need to be able to understand C/C++ programs, write simple programs to call library and other implemented functions, make changes to such programs, and be able to use debuggers to analyze programs.

Course Objectives

Upon successful completion of this course of study, the student will:

- Know how to encrypt and decrypt simple substitution cipher methods and how to break a simple substitution cipher
- Know how to encrypt and decrypt using stream ciphers (A5/1 and RC4) for symmetric key cryptography
- Know how to encrypt and decrypt using block ciphers (Feistel Cipher, DES (Data Encryption Standard), and AES (Advanced Encryption Standard))
- Know how to encrypt and decrypt using RSA public key cryptography
- Know how to apply Diffie-Hellman for key exchange
- Know how to encrypt and decrypt using elliptic curve cryptograghy
- Know how to use public key cryptography to achieve confidentiality, digital signatures, and non-repudiation
- Know how to use cryptographic hash functions (SHA-1) and hashed message authentication code (HMAC)
- Know how to use different methods to achieve authentication
- Know how to apply access control matrix and multilevel security models (Bell-LaPadula and Biba models)

- Know how to apply authentication protocols
- Know how to achieve zero knowledge proofs
- Know how to apply SSL, IPSec, and Kerberos security protocols
- Know how to exploit software flaws (such as buffer overflow)
- Know how to perform software reverse engineering and software analysis
- Know how to achieve secure coding
- Know how to secure operating systems for computer security applications
- Know how to achieve physical and emanations security
- Know how to achieve computer security assurance
- Know how to identify and analyze web security
- Have some experience with research in computer security

Textbook and Course Materials

Required textbook: "*Information Security*," 2nd Edition, (ISBN 978-0-470-62639-9), Wiley, 2011, by Mark Stamp.

In addition to the textbook, papers and notes from the literature will be distributed along the lectures.

Student Responsibilities

Attendance is required for this class. Unless you obtain prior consent of the instructor, missing classes will be used as bases for attendance grading. In case that it is necessary to skip a class, students are responsible to make up missed materials. Participation in in-class discussions and activities is also required. All submitted assignments and projects must be done by the author(s). It is a violation of the Academic Honor Code to submit other's work and the instructor of this course takes the violations very seriously.

As this course will cover certain techniques to break down known systems in order to demonstrate their vulnerabilities, it may be illegal, however, to practice these techniques on others' systems. The students will be liable for their behaviors and therefore consequences.

Assignments and Projects

About nine homework assignments will be given along the lectures and they need to be turned in; they include problems in the textbook at the end of chapters as well as understanding/using/modifying existing implementation of covered algorithms. There will be a term project, which can be an implementation project that involves extensive programming, an analysis project on policy and fundamental issues, or an in-depth literature survey on a particular topic. There will be about five in-class quizzes, a midterm exam and a final exam.

Grading Policy

Grades will be determined as follows:

Assignment	Points	Assignment	Points
Class Attendance & Participation	5 %	Midterm Exam	20 %
Homework Assignments	25 %	Term Project	10 %
Final Exam (cumulative)	30 %	Quizzes	10%

Grading will be based on the weighted average as specified above and the following scale will be used (suppose the weighted average is *S* in 100 scale)

Score	Grade	Score	Grade	Score	Grade
$93 \le S$	A	$80 \le S < 83$	B-	$67 \le S < 70$	D+
$90 \le S < 93$	A-	$77 \le S < 80$	C+	$63 \le S < 67$	D
$87 \le S < 90$	B+	$73 \le S < 77$	C	$60 \le S < 63$	D-
$83 \le S < 87$	B	$70 \le S < 73$	C-	$S < 60$	F

Late Penalties

Assignments are due at the beginning of the class on the due date. Assignments turned in late, but before the beginning of the next scheduled class will be penalized by 10 %. Assignments that are more than one class period late will **NOT** be accepted.

Submission and Return Policy

All tests/assignments/projects/homework will be returned as soon as possible after grading but no later than two weeks from the due date.

Tentative Schedule

- Week 1: Introduction (Chapters 1 and 2)
  - General introduction to computer security.
  - Fundamental problems, principles, and methods in computer security.
  - Basic cryptographic algorithms and cryptanalysis.
  - Introduction to modern cryptography.
- Week 2: Symmetric key cryptography (Chapter 3 and Chapter 6).
- Weeks 3 and 4: Public key cryptography and public key infrastructure (Chapter 4 and Chapter 6).
- Week 5: Hash functions (Chapter 5)
- Week 6: Authentication (Chapter 7).
- Week 7: Authorization (Chapter 8).
- Weeks 8 and 9: Simple authentication protocols (Chapter 9).
- Week 8: Midterm exam (October 17, 2014)
- Weeks 10-11: Real-world security protocols (Chapter 10)
- Week 12: Software flaws, malware, software reverse engineering, and secure software development (Chapters 11 & 12)
- Week 13: Software security (system security) (Chapter 13)
- Week 14: Web security (from the literature and other sources)
- Week 15: Introduction to Emanations Security (TEMPEST), Summary and Case studies
- Final exam (cumulative), Wednesday, 12:30-2:30 PM, December 10, 2014

Academic Honor Code

The Florida State University Academic Honor Policy outlines the University's expectations for the integrity of students' academic work, the procedures for resolving alleged violations of those expectations, and the rights and responsibilities of students and faculty members throughout the process. Students are responsible for reading the Academic Honor Policy and for living up to their pledge to ". . . be honest and truthful and . . . [to] strive for personal and institutional integrity at Florida State University." (Florida State University Academic Honor Policy, found at http://dof.fsu.edu/honorpolicy.htm)

Assignments/projects/exams are to be done individually, unless specified otherwise. It is a violation of the Academic Honor Code to take credit for the work done by other people. It is also a violation to assist another person in violating the Code (See the FSU Student Handbook for penalties for violations of the Honor Code). The judgment for the violation of the Academic Honor Code will be done by the instructor and a third party member (another faculty member in the Computer Science Department not involved in this course). Once the judgment is made, the case is closed and no arguments from the involved parties will be heard. Examples of cheating behaviors include:

- Discuss the solution for a homework question.
- Copy programs for programming assignments.
- Use and submit existing programs/reports on the world wide web as written assignments.
- Submit programs/reports/assignments done by a third party, including hired and contracted.
- Plagiarize sentences/paragraphs from others without giving the appropriate references. Plagiarism is a serious intellectual crime and the consequences can be very substantial.

Penalty for violating the Academic Honor Code: A 0 grade for the particular assignment/quiz/exam and a reduction of one letter grade in the final grade for all parties involved for each occurrence. A report will be sent to the department chairman for further administrative actions.

Accommodation for Disabilities

Students with disabilities needing academic accommodations should: 1) register with and provide documentation to the Student Disability Resource Center (SDRC), and 2) bring a letter to the instructor indicating the need for accommodation and what type. This should be done within the first week of class. *This syllabus and other class materials are available in alternative format upon request.*

For more information about services available to FSU students with disabilities, contact the Assistant Dean of Students:

Student Disability Resource Center
97 Woodward Avenue, South
108 Student Services Building
Florida State University
Tallahassee, FL 32306-4167
(850) 644-9566 (voice)
(850) 644-8504 (TDD)
sdrc@admin.fsu.edu
http://www.disabilitycenter.fsu.edu/