COMPUTER SECURITY FUNDAMENTALS

CIS 4360, Spring 2019

Department of Computer Science, Florida State University

General Information

— Place and times: HCB 0316, TuTh 8:00-9:15am.
— Course URL: http://www.cs.fsu.edu/_burmeste/cis4930.htm
— Instructor: Mike Burmester
— TAs: Md Reaz Murshed Masud (mm18ka@my.fsu.edu), Joyeep Das (jd14w@my.fsu.edu)
— Office: 268 Love Building
— Office hours: TuTh 9:30-10:30pm, and by appointment
— email: burmester@cs.fsu.edu
— Class Home page: www.cs.fsu.edu/~burmeste/cis4360.htm

This web site contains up-to-date information related to this class such as, announcements, assignments, lecture notes, and useful links to resources that are helpful to this class. Besides the web pages, Blackboard will be used to announce changes and updates and post grades for this class; in particular, emails will be sent using the Blackboard email addresses: please make sure that your email address on record is current.

Prerequisites

COP4530 -- Data Structures. You should be familiar with basic arithmetic and basic statistics. Thinking out-of-the-box will help a lot!

Textbook and course materials

There is no required textbook for this course. Lecture slides, written notes, and papers from the literature will be provided. The following books can be helpful to understand some of the basic concepts thoroughly.

- Handbook of Applied Cryptography, by A. Menezes, P. Van Oorschot, S. Vanstone (free)
- A Graduate Course in Applied Cryptography, D. Boneh and V. Shoup (free)
- Cryptography and Network Security: Principles and Practice, 6th Edition, William Stallings, Pearson, ISBN-10: 0133354695 • ISBN-13: 9780133354690©2014 (not free!)

Rationale

Do you want anyone to be able to read your emails? How about accessing your bank account for some cash? Do you mind somebody pretending to be you on the Internet? Do you think cyber warfare can really hurt us? Do you worry about spyware, computer viruses, worms, zero-day threats?

Do you think security-by-obscurity is good protection? If you were an anchovy would you prefer a bait-ball to a go-it-alone strategy against sharks? How should we defend our infrastructure? Do you care?

Do you think blockchain consensus accounting and distributed ledgers technology will be the next breakthrough technology? Do you think Bitcoin is cheap today?

As more communications are conducted via mobile and cellular technologies, these technologies have become critical. It is important to understand how data is processed and transmitted using these ubiquitous devices. Mobile devices are increasingly subject to threats from malware, threats associated with data theft and more generally threats that exploit physical and cyber components. Do you think your cell phone is secure?

Course Description

The course will introduce the fundamental security and design principles for cyber space, cyber defense operations and the basic theory and practice of cryptographic techniques for computer and network security. It will cover topics such as: confidentiality, integrity, authentication, digital signatures, public-key infrastructure,

digital rights management, trust relationships, fundamental security design principals, and cellular/mobile networks.

Course Objectives. The objective of this course is to study techniques for the protection of computer and communication systems from attacks by hackers and fraudsters, and cryptographic systems that can be used for secure multiparty computation. The goal is to become familiar with the foundations of these techniques, and the security design principles.

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

- Know how to recognize the common vulnerabilities of cryptographic algorithms.
- Know the basic conventional symmetric cryptographic systems and how to use them.
- Know the basic public-key cryptographic systems and how to use them.
- Know the basic network protocols work at the infrastructure, network and application layers.
- Know the major network protocols for communication and data transfer.
- Become familiar with the basic techniques to protect computer and communication systems against a range of threats.
- Know the range of security objectives, and the levels of security that can be achieved.
- Know the technologies and methods used to defend systems and networks.
- Understand the principles underlying cyber security, and how they are used to achieve solutions.
- Become familiar with the basics of cellular and mobile technologies, their operating systems, wireless technologies, the encryption standards and location services.

Student Responsibilities

Attendance. Attendance is required for this class. Participation in in-class discussions and activities is also required. Unless you obtain prior consent from the instructor, missing classes will be used as basis for attendance grading.

University Attendance Policy. Excused absences include documented illness, deaths in family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities. These absences will be accommodated in a way that does not arbitrarily penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness.

Make up missed materials. In case that it is necessary to skip a class, students are responsible to make up missed materials. You are responsible for all information explained in class, some of which will not be available in written form. I will not feel obligated to repeat homework assignments, schedule changes, or other material presented in class. If you are forced to miss a class, it is your responsibility to get good class notes from a friend and check with me for handouts.

Assignments & Honor Code. 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.

Assignments & Grading

The only way to learn this material thoroughly is to work through the details and examples, pencil and paper in hand, on your own. Treat graded homework assignments as take-home tests. Do the work yourself: no one else should look at your work. Giving or accepting help on graded homework assignments is a violation of the student honor code.

Homework Assignments. About five homework assignments will be given. These will have to be done individually and turned in at the beginning of class to be graded. You should be prepared to make oral presentations of your answers in class, as part of such a review. Solutions to the assignments will be provided.

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.

***Projects*.** You will be assigned one project, on a specific cryptographic topic. This will involve researching the particular topic, finding appropriate background material.
Cyber Ops Projects will focus on Mobile and Cellular technologies (the last part of the course), and in particular on exploits of mobile devices. A hands-on approach is desirable although not essential.

***Quizzes*.** There will be several 5 min quizzes on material covered during class: these will consist of simple or multiple choice questions, typically handed out five minutes before the end of class.

***Midterm*.** There will be one midterm.

***Grading*.** The final grade may be raised for exceptional class participation, exceptional projects, marked improvement over the term, or in cases where the grading formula appears skewed by a few exceptionally low grades or work missed for verifiable excusable reasons.

***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.

Grading Policy

Homework Assignments, Projects, and Quizzes will contribute 50% to the final grade. The midterm and final examination will contribute 25% each:

Assignment	Points
Quizzes/Class Attendance Participation	20 %
Homework Assignments	15 %
Projects	15%
Midterm	25%
Final	25%

Grading will be based on the weighted average as specified above and the following scale will be used ("S" is the weighted average on a 100-point scale):

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

Tentative Schedule

Week 1. Brief introduction and motivation

a. Confidentiality, Integrity, Availability, Cryptography and Steganography, Cryptography and Cryptanalysis, Unconditional vs computational security, secret key cryptography, cryptographic hash functions and public key cryptography.

b. A brief history of classical cryptography. From antiquity to Caesar, Bacon, Chaucer, Vigenere, Jefferson, Cipher Machines, mono and poly alphabetic ciphers, transposition ciphers, product ciphers, Enigma.

Week 2. Classical encryption techniques, an overview

a. Symmetric ciphers, substitution, transposition, examples

b. Block ciphers, Feistel cipher, Stream ciphers, examples

Week 3. Classical encryption techniques

a. The Data Encryption Standard (DES)

Week 4. Basic Concepts in Number Theory

a. Modular arithmetic, Euclidean algorithm, groups, rings, fields, finite field arithmetic

b. Advanced Encryption Algorithm (AES), AES structure

Week 5. Advanced Encryption Algorithm (AES), Block Ciphers, modes of operation

a. Key expansion, substitute bytes, shiftrows, mixcolumns, addroundkey, implementation aspects

b. Multiple encryption, 3-DES, modes of operation of block ciphers

c. Modes of operation: ECB, CBC, CFM, OFM, CTM, and XTS-AES for storage devices

Week 6. Public Key Cryptography

a. Asymmetric ciphers, the Rivest-Shamir-Addleman (RSA) protocol

b. Principles of Public Key Cryptosystems

Week 7. Pseudorandom Number Generators

a. Random Numbers, Unpredictability, entropy

b. True Random Numbers, PRNG, BBS

Week 8. Pseudorandom Number Generators and Stream Ciphers

a. Using Block Cipher modes, Stream Ciphers, RC4

b. Hash functions, other public-key cryptosystems

Week 9. Other Public-Key Cryptosystems

a. Digital signatures, Elliptic Curve Cryptography

b. Revision: Classical encryption techniques, Block ciphers, Block Cipher operation, Public Key Cryptography

Week 10. Midterm

a. Midterm
b. Other public-key cryptosystems

Week 11. Spring Break

Week 12. First Principals & Cyber Defense

a. Domain separation, Process isolation, Resource encapsulation, least privilege, layering, abstraction, data hiding, modularity, simplicity and minimization
b. Anomaly/Intrusion detection and identification, malicious activity detection
c. Network security techniques and components, defense in depth
d. Trust relationships, distributed cloud, virtualization

Week 13. Cellular and Mobile Technologies

a. Overview of smart phone technologies & embedded operating systems (IOS, Android)
b. Wireless technologies (GSM, WCDMA,CDMA200, LTE, Internet 802.11b/g/n)
c. Infrastructure components (fiber optic network, evolved packet core, lPLMN)

Week 14. Cellular and Mobile Technologies

a. Mobile protocols (SS7, RR, MM, CC)
b. Logical channel descriptions (BCCH, SDCCH, RACH, AGCH)
c. Registration procedures and encryption standards

Week 15. Cellular and Mobile Technologies, Revision

a. Mobile identifiers (IMSI, IMEI, MSISDN, ESN, Global Title, E.164)
b. Mobile and location-based services
c. Revision

Week 16. Exam week

Academic Honor Policy

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://fda.fsu.edu/Academics/Academic-Honor-Policy).

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 /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 accommodation should: (1) register with and provide documentation to the Student Disability Resource Center; and (2) bring a letter to the instructor indicating the need for accommodation and what type. This should be done during 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: Student Disability Resource Center 874 Traditions Way 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/.

Additional Information

Free Tutoring from FSU: On-campus tutoring and writing assistance is available for many courses at Florida State University. For more information, visit the Academic Center for Excellence (ACE) Tutoring Services' comprehensive list of on-campus tutoring options at http://ace.fsu.edu/tutoring or contact tutor@fsu.edu. High-quality tutoring is available by appointment and on a walk-in basis. These services are offered by tutors trained to encourage the highest level of individual academic success while upholding personal academic integrity.

Syllabus Change Policy: Except for changes that substantially affect implementation of the evaluation (grading) statement, this syllabus is a guide for the course and is subject to change with advance notice.