

ECE 404

INTRODUCTION TO COMPUTER SECURITY

School of Electrical and Computer Engineering
Purdue University
Spring 2019

Instructor: Avi Kak

Office: EE 340

Phone: 494-3551

E-mail: kak@purdue.edu

Office Hours: TuTh 1:30-2:30
(prefer by appointment)

Class hours: TuTh 3:00 – 4:15

Classroom: Matthews Hall 210

Teaching Assistants

Constantine Roros

Office: EE209
e-mail: croros@purdue.edu
Office Hours: Tuesdays: 12:00 PM – 1:00 PM
Wednesdays: 12:00 PM – 2:00 PM
Thursdays: 12:00 PM – 1:00 PM
and by appointment at any time

Shayan Akbar

Office: EE208
e-mail: sakbar@purdue.edu
Office Hours: Mondays: 3:00 PM – 5:00 PM
Wednesdays: 3:00 PM – 5:00 PM
and by appointment at any time

Somrita Chattopadhyay

Office: EE 209
e-mail: chattops@purdue.edu
Office Hours: Mondays: 11:00 AM – 1:00 PM
Fridays: 11:00 AM – 1:00 PM
and by appointment at any time

Course Objective:

Beyond question, computer and network security has emerged as one of the most important subjects of study in modern times.

Even the minutest details of our lives now depend on computers and networks working with our trust that the information that is private to us will not fall in the hands of those with ill intent.

The two major components of computer and network security are cryptography and what is known as systems-oriented security.

For a good education in computer and network security, you have no choice but to learn them both.

For that reason, here is the goal of this class: To provide a balanced introduction to both cryptography and the systems-oriented issues.

In cryptography, we will cover the most important algorithms used today for data encryption and decryption. And in the systems-oriented issues we will cover in this course include Denial-of-Service attacks, DNS Cache Poisoning attacks, Buffer Overflow attacks, Dictionary attacks, attacks with viruses, worms, and Trojans, etc.

Course Outcomes:

- i. sufficient understanding of TCP/IP to understand vulnerabilities of and defenses for TCP/IP. [1,4,6]
- ii. an introductory level of knowledge on secure protocols, their use and their limitations. [1,4]
- iii. knowledge of how to access and understand CERT, IETF and SANS advisories. [4]
- iv. an ability to implement and design basic rule-based firewall/intrusion detection systems. [1,2,4,6]

Homework and Exam Credit

You'll earn 50% of your credit from homework assignments (including programming assignments) and 50% from three exams.

There will be at least one homework assignment every week which could either be just theoretical in nature or could involve programming. In some weeks, you may get a small theoretical homework assignment in addition to the programming assignment.

Attendance Policy

1. Each class will begin with a 3-minute, 3-question quiz.
2. The purpose of this quiz is for me to see how comfortable you are in quickly articulating the major concepts covered in the previous lecture.
3. Although the quiz will not be graded, it will serve as a record of your attendance in class.
4. **If you miss more than three classes during the course of the semester, your grade may be lowered by one full letter.**

Homework Submission Policy

1. If your programming homework does not compile, do not turn it in.
2. You must turn in both hardcopy and electronic versions of your programming homework.
3. The instructions for turning in the electronic version of your programming homework will be posted on the course web page.
4. The hardcopy version of your programming homework is due at the **beginning** of class.
5. The electronic copy of your programming homework is due **before** the beginning of the class. The system will not let you make an electronic submission after the start of the class.
6. Actual grading of most programming homework assignments will take place on the hardcopy version. The electronic copy may be used by the TA to test the workings of your program. This will be done on some subset of the assignments turned in.
7. If you only turn in the electronic version of a programming assignment, that will be the same as not turning in the homework since the homework submissions will be kept track of only through their hardcopy versions. As mentioned before, the electronic versions are meant to be used for verification purposes only.

8. If a programming assignment is relatively easy, it is possible that the grader will not actually look at the electronic version of your submission. However, as a matter of policy, if at any point during the semester it is discovered that you did not submit the electronic version of a homework for which you received a grade, **that grade will be zeroed out.**

Exams

There will be three midterm exams. (There will be no final exam.) Each exam will carry the same weight in the final evaluation. The exams have been scheduled for the following dates and times:

<i>Exam dates</i>		<i>Exam time</i>	<i>Location</i>
Exam 1:	Thursday February 7	8 pm	LILY 1105
Exam 2:	Tuesday March 5	8 pm	CL50 224
Exam 3:	Wednesday April 17	8 pm	EE 129

Additional Information:

1. Your course grade will be determined from the total points that you obtain from homework assignments and exams, and will be

based on a combination of relative and absolute scaling. You determine your own grade by your homework and exam performance.

2. There will be no extra credit projects.
3. If you do not show up for an exam you will receive a zero, unless you obtain prior authorization from the TA to be absent from the exam. (The authorization **MUST** come from the TA. Asking your instructor for the authorization to be absent does not count.)
4. If a medical or some other emergency keeps you away from an exam, you must notify the TA within 8 hours after the exam. NO PUSH notes will be accepted. Absolutely no late exams will be given after the exams are handed back in class.
5. Course exams will be given in the evenings. Each exam will cover approximately one third of the course material. (Exams will not be cumulative, but you will be expected to know all the material up to an exam in order to be successful in that exam.)
6. You are responsible for all information given in class verbally and/or in writing. All information about the course (including but not limited to exam dates, office hours, and course schedule) may be superseded by the information given in class at any time.
7. **Cooperative efforts at understanding the material and the assignments of the course are encouraged.**

However, what you finally present for any given homework must be done individually. Submitting any work that is not a student's own work is considered cheating. If you cheat, the Dean of Students will be notified.

8. You may ask to have an assignment or exam re-graded, the result of which may be an increase or a decrease in your grade. To have an assignment or a test re-graded, you must speak with the TA within **two days** after receiving the graded material.

9. The course web site:

`https://engineering.purdue.edu/ece404/`

Note that, in general, homework assignments and their solutions will NOT be posted at the course web site. However, useful information, including a solution, may be posted on the web site for homework assignments that are particularly challenging.

The rest of this document presents the syllabus for
this class.

Computer and Network Security

by
Avinash Kak

Think of these lecture notes as a living textbook that strives to strike a balance between the systems-oriented issues and the cryptographic issues. Without the latter, many aspects of the former cannot be fully comprehended, and, without the former, the latter are too dry to appreciate.

Note for instructors using these slides/notes:

It is not uncommon for the instructors who use these notes/slides to want to know how exactly I use them in class since there is much more information on a typical slide than you will usually find in a powerpoint presentation.

Here is the answer: When I teach the theoretical portions of this course, I actually work out the formulas on the chalkboard and, when I do so, I follow the derivations presented in these lecture notes. On the other hand, when I teach the systems portion of the course, I spend quite a bit of time demonstrating the issues on my Linux laptop, again in the manner described in these lecture notes. These lecture notes are intended as much for showing in class in the form of slides as they are for focused reading by the students on their own. When used as slides, these serve as backdrop to the explanations provided on the chalkboard or through demonstrations on a computer.

Regarding homework assignments:

Homework assignments typically involve writing Perl or Python scripts *in order to gain a deeper understanding of the ideas through actual implementation*. (From a pedagogical standpoint, scripting is much more efficient for this than writing code in raw C.) In the part of the course that deals with encryption and hashing, students write scripts for implementing DES, AES, RC4, SHA1, SHA512, etc. In the part of the course that deals with more system related issues, the students are asked to write scripts that carry out DoS attacks, buffer overflow attacks, etc., against servers (for buffer overflow attacks, that would be a socket program in C with intentionally embedded buffer-overflow vulnerability).

If you are an instructor and you'd like to see these homework assignments (*along with the two best solutions submitted by the students at Purdue*), send me a note at kak@purdue.edu. If you do so, please place the string "requesting security homework" in your subject line to get past my merciless spam filter. **VERY**

IMPORTANT: Your email request for this material must establish two things: that you are an instructor and that you are using these lecture notes to teach your class. An anonymous email request (using, say, a gmail or a yahoomail address) that does not indicate your institutional affiliation will be ignored.

Useful resources for homework assignments:

1. The [BitVector class](#) in Python is useful for creating compact implementations for hash functions (see Lecture 15 for an example) and for writing scripts for block and stream ciphers.
2. The [BitVector class](#) in Perl that lets you do everything in Perl that the above mentioned class does in Python.
3. If you are writing Perl and/or Python scripts for solving homework problems or for course projects, you will find the book ["Scripting with Objects"](#) a useful resource for this course. Chapters 2 and 3 of the book provide quick and easy-to-follow introductions to Perl and Python, respectively.
4. If you'd rather do your homework in C++ or Java, you will find the book ["Programming With Objects"](#) a useful resource. This book is now being used at a number of universities for teaching object-oriented programming in both C++ and Java simultaneously.

If you would like to know about the **OBJECTS TRILOGY PROJECT** that led to the two books mentioned above, [click here](#).

The third book in the Objects Trilogy is:
["Designing with Objects"](#)

When will this material be updated next?:

The 2018 update of the lecture notes is finished. The next major update of this material is scheduled for the January - April 2019 time frame.

Lecture Notes			
1.	Introductory material, course administration handout, etc.		
2.	Some Basic Vocabulary of Computer and Network Security and a Brief Review of Classical Encryption Techniques	Updated January 10, 2019	download code <small>Updated: January 13, 2016</small>
3.	Block Ciphers and the Data Encryption Standard	Updated January 11, 2019	download code <small>Updated: January 15, 2018</small>
4.	Finite Fields (PART 1): Groups, Rings, and Fields	Updated January 17, 2019	
5.	Finite Fields (PART 2): Modular Arithmetic	Updated January 22, 2019	download code <small>Updated: February 28, 2016</small>

6.	Finite Fields (PART 3): Polynomial Arithmetic	Updated January 24, 2019	
7.	Finite Fields (PART 4): Finite Fields of the Form $GF(2^n)$	Updated January 29, 2019	download code <small>Updated: February 5, 2016</small>
8.	AES: The Advanced Encryption Standard	Updated January 31, 2019	download code <small>Updated: February 2, 2018</small>
9.	Using Block and Stream Ciphers for Secure Wired and WiFi Communications	Updated February 5, 2019	download code <small>Updated: February 11, 2016</small>
10.	Key Distribution for Symmetric Key Cryptography and Generating Random Numbers	Updated February 8, 2019	download code
11.	Prime Numbers and Discrete Logarithms	Updated February 14, 2019	download code <small>Updated: February 28, 2016</small>
12.	Public-Key Cryptography and the RSA Algorithm	Updated February 20, 2019	download code <small>Updated: February 28, 2016</small>
13.	Certificates, Digital Signatures, and the Diffie-Hellman Key Exchange Algorithm	Updated February 23, 2019	download code <small>Updated: February 28, 2016</small>
14.	Elliptic Curve Cryptography and Digital Rights Management	Updated February 23, 2019	download code <small>Updated: February 28, 2016</small>
15.	Hashing for Message Authentication <small>(Starting in 2018, this lecture now includes material on crypto currencies that I explain with the help of my Python-based CeroCoinClient module that you can access by clicking here.)</small>	Updated March 1, 2019	download code <small>Updated: April 8, 2018</small>
16.	TCP/IP Vulnerabilities and DoS Attacks: IP Spoofing, SYN Flooding, and The Shrew DoS Attack	Updated March 7, 2019	download code <small>Updated: March 12, 2016</small>
17.	DNS and the DNS Cache Poisoning Attack	Updated March 5, 2019	download code <small>Updated: March 23, 2016</small>
18.	Packet Filtering Firewalls (Linux)	Updated March 7, 2019	download code
19.	Proxy-Server Based Firewalls	Updated March 22, 2019	download code <small>Updated: March 24, 2016</small>
20.	PGP, IPSec, SSL/TLS, and Tor Protocols	Updated March 21, 2019	
21.	The Buffer Overflow Attack	Updated April 9, 2018	download code <small>Updated: April 3, 2017</small>
22.	Malware: Viruses and Worms	Updated April 10, 2018	download code <small>Updated: April 8, 2016</small>
23.	Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing	Updated April 3, 2018	
24.	Dictionary Attacks and Rainbow-Table Attacks on Password Protected Systems	Updated April 16, 2018	

25.	Security Issues in Structured Peer-to-Peer Networks	Updated April 17, 2018	
26.	Small-World Peer-to-Peer Networks and Their Security Issues	Updated April 18, 2018	download code
27.	Web Security: PHP Exploits, SQL Injection, and the Slowloris Attack	Updated April 16, 2018	download code <small>Updated: April 14, 2017</small>
28.	Web Security: Cross-Site Scripting and Other Browser-Side Exploits	Updated April 15, 2018	download code
29.	Bots, Botnets, DDoS Attacks, and DDoS Attack Mitigation	Updated April 13, 2018	download code <small>Updated: April 11, 2018</small>
30.	Mounting Targeted Attacks for Cyber Espionage with Trojans and Social Engineering	Updated April 12, 2018	
31.	Filtering Out Spam	Updated April 6, 2018	download code
32.	Security Vulnerabilities of Mobile Devices	Updated April 19, 2018	download code <small>Updated: April 25, 2015</small>
33.	Index (HTML)	Updated April 24, 2018	

Follow me on Twitter if you want to be automatically informed of when the updates to these lectures are completed each year.

A BRIEF HISTORY: These lecture notes, at least several of them, made their first appearance on the web in 2006. They have so far gone through nine revisions. With each revision I have attempted to improve the explanations on the basis of the feedback I receive from the students at Purdue and from other users of these notes. Regarding the notes that deal with the systems side of security, I have continually endeavored to find the best ways to combine the explanation of the concepts involved and their demonstration on a laptop keeping in the mind the time constraints of a typical lecture period.

HOW CAN YOU BE SURE YOU HAVE THE LATEST UPDATED VERSION OF A LECTURE: As I am thinking about the material and teaching it in class, a lecture may go through as many as a dozen updates. If you are tracking my updates, the only way you can be certain you have the final version of an updated lecture is to check at the end of April when I am usually done with all the updating. When I am done, I post a notice to that effect on Twitter.

EXPERIENCING PROBLEMS? If you experience any problems with downloading or using any of these PDF files, please send an email to kak@purdue.edu with the string "Problem with computer security notes" in the subject line to get past my spam filter.

FEEDBACK WELCOME! If you have any comments or any suggestions for improving these notes, please send an email to kak@purdue.edu with the string "Comments on computer security notes" in the subject line to get past my spam filter. Any suggestions that I incorporate would be duly acknowledged.

WOULD YOU LIKE TO CONTRIBUTE A HOMEWORK PROBLEM OR A PROJECT? My goal is for these notes to become self-contained as a medium of instruction in computer and network security. Toward that end, I'd like to end the notes for each lecture on a set of homework problems and/or projects. If you send me a problem or a project, your name will be mentioned as the author of that problem or project. If you submit a project, please make sure that it can be done in one or two weeks' time in some high-level language. I'll certainly include the problems and projects I currently give out when teaching this material, but any contributions made by others using these lecture notes would add to the variety. If you choose to send me a problem or a project, email it to kak@purdue.edu with the string "homework for computer security notes" in the subject line.

SAVE THIS INFORMATION IN A SAFE PLACE: If you are a frequent user of this material, note that occasionally the web server hosting this material may be down for system maintenance. If you cannot access this material but you have an urgent need to do so, send an email immediately to kak@purdue.edu with the string "Unable to access computer security notes" in the subject line to get past my spam filter. I should be able to provide you with a URL to another web server hosting this material.

