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 2023 update of the lecture notes has been completed. The next major update of this material is scheduled for the January – April 2024 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 11, 2024	download code Updated: January 13, 201
3.	Block Ciphers and the Data Encryption Standard	Updated January 16, 2024	download code Updated: January 15, 201
4.	Finite Fields (PART 1): Groups, Rings, and Fields	Updated January 25, 2024	
5.	Finite Fields (PART 2): Modular Arithmetic	Updated January 25, 2024	download code Updated: February 28, 20
6.	Finite Fields (PART 3): Polynomial Arithmetic	Updated January 29, 2024	
7.	Finite Fields (PART 4): Finite Fields of the Form $GF(2^n)$	Updated January 30, 2024	download code Updated: February 5, 201
8.	AES: The Advanced Encryption Standard	Updated February 7, 2024	download code Updated: February 2, 201
9.	Using Block and Stream Ciphers for Secure Wired and WiFi Communications	Updated February 7, 2024	download code Updated: February 11, 20
10.	Key Distribution for Symmetric Key Cryptography and Generating Random Numbers	Updated February 8, 2024	download code
11.	Prime Numbers and Discrete Logarithms	Updated February 13, 2024	download code Updated: February 28, 20
12.	Public-Key Cryptography and the RSA Algorithm	Updated February 15, 2024	download code Updated: February 28, 20
13.	Certificates, Digital Signatures, and the Diffie-Hellman Key Exchange Algorithm	Updated February 20, 2024	download code Updated: February 28, 20
14.	Elliptic Curve Cryptography and Digital Rights Management	Updated February 22, 2024	download code Updated: February 28, 20

15.	Hashing for Message Authentication (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.)	Updated March 24, 2024	download code Updated: April 8, 2018
16.	TCP/IP Vulnerabilities and DoS Attacks: IP Spoofing, SYN Flooding, and The Shrew DoS Attack	Updated February 29, 2024	download code Updated: March 12, 201
17.	DNS and the DNS Cache Poisoning Attack	Updated March 7, 2024	download code Updated: March 23, 201
18.	Packet Filtering Firewalls (Linux)	Updated March 7, 2024	download code
19.	Proxy-Server Based Firewalls	Updated March 21, 2024	download code Updated: March 24, 201
20.	PGP, IPSec, SSL/TLS, and Tor Protocols	Updated March 21, 2024	
21.	The Buffer Overflow Attack	Updated March 26, 2024	download code Updated: April 3, 2017
22.	Malware: Viruses and Worms	Updated March 28, 2024	download code Updated: April 6, 2022
23.	Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing	Updated April 9, 2024	
24.	Dictionary Attacks and Rainbow-Table Attacks on Password Protected Systems	Updated April 11, 2024	
25.	Security Issues in Structured Peer-to-Peer Networks	Updated April 18, 2024	
26.	Small-World Peer-to-Peer Networks and Their Security Issues	Updated April 18, 2024	download code
27.	Web Security: PHP Exploits, SQL Injection, and the Slowloris Attack	Updated April 16, 2024	download code Updated: April 14, 2017
28.	Web Security: Cross-Site Scripting and Other Browser-Side Exploits	Updated April 16, 2024	download code
29.	Bots, Botnets, DDoS Attacks, and DDoS Attack Mitigation	Updated April 9, 2024	download code Updated: April 11, 2018
30.	Mounting Targeted Attacks for Cyber Espionage with Trojans and Social Engineering	Updated April 9, 2024	
31.	Filtering Out Spam	Updated Apil 4, 2024	download code
32.	Security Vulnerabilities of Mobile Devices	Updated April 11, 2024	download code Updated: April 25, 2015
33.	Index (HTML)	Updated July 23, 2023	

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. Since then I have revised them anually during the Spring semester when I teach this class at Purdue. 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.