Introduction to Cybersecurity

CSCI 4621/5621 (Fall 2020)

Phani Vadrevu

Dept. of Computer Science, University of New Orleans

About me

- Graduated from University of Georgia
    - 2017 PhD in Computer Science

- Research areas: Web security, network security, malvertising, malware

- Email: phani@cs.uno.edu

- Office: Math 329-C (GNOCIA)

- Office hours: Mon, Tue, Wed 02:00 PM to 04:00 PM

Course Objectives

- A solid foundation of security concepts, backed by concrete examples

- Security mindset
  - How to think like an attacker or security engineer?
  - Looking beyond the system’s intended functionality, what it can be made to do?

- Understanding how computer systems work, how they break, and how to fix them
  - Technical details of vulnerabilities, attacks, and defenses

Course Prerequisites

- *CSCI 2467 (Systems Programming Concepts)*

- You are expected to have a basic understanding of
  - C and x86 assembly language
  - Programming in a lighter weight language such as Python or Ruby
  - Linux
  - Computer architecture
  - Networking

Course Contents

- Following topics will be covered in the class
  - Overview of Computer Security
  - Cryptographic tools
  - Buffer Overflow
  - User Authentication / Access Control issues
  - Malware
  - Network Security
  - Web Security
  - Other CTF-oriented topics such as steganography, forensic analysis
  - Adversarial Machine learning (if time permits)

You will play CTFs!

CTF

- Capture the Flag (CTF) competitions
- Hacking games that **test** and **improve** knowledge of security concepts
- Have a “learn-as-you-solve” methodology
- Two formats:
  - Attack – defense
  - Jeopardy
- Categories:
  - Binary Analysis, Crypto, Web, Network, Forensic, Steganography
- Good resource for lots of CTF-related information: https://ctftime.org/

Jolly Roger Insecurity

- Our university CTF team
- https://ctftime.org/team/25932
- **Submit request to join the team**
- **Join Slack Channel #ctf** (https://acmuno.slack.com/)
- Upcoming CTFs will be discussed here.

Grading components

- Midterm exam: 20%
    - October 8, 2020 (Tentative date)

- Final exam: 20%
    - December 3, 2020 (Thursday) – 10 AM to 12 PM

- Semester-long CTF: 60%
    - Assignment-1: September 27 (Cryptography, Steganography)
    - Assignment-2: October 14 (Binary Analysis, Reverse Engineering)
    - Assignment-3: November 1 (Network security, Forensics)
    - Assignment-4: November 22 (Web security)

Approaching CTFs

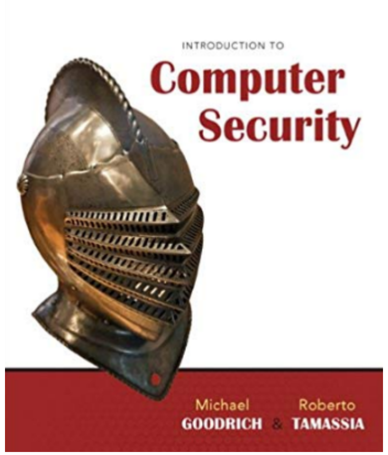
- Ability to learn on your own – new tools, techniques and concepts.
- Requires Google-fu!
- Needs problem solving skills.
- Needs patience and persistence to solve tough problems.

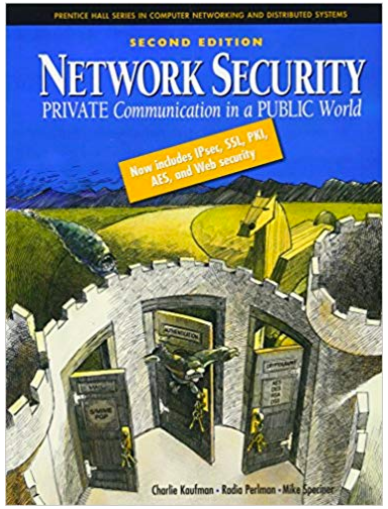
Textbooks

- There is no required textbook

- If you want additional reading:
  - ***Optional***: Introduction to Computer Security
    by Goodrich & Tamassia

  - ***Optional***: Network Security: Private Communication in a
    Public World
    by Kaufman, Perlman & Speciner




PRENTICE HALL SERIES IN COMPUTER NETWORKING AND DISTRIBUTED SYSTEMS
SECOND EDITION
NETWORK SECURITY
PRIVATE Communication in a PUBLIC World
Now includes IPsec, SSL, PKI, AES, and Web security
Charlie Kaufman · Radia Perlman · Mike Speciner

Recommended Readings

- https://medium.com/@DRX_Sicher/ctf-explained-6c7d4417305e