ECE 455: Cybersecurity

The Cooper Union
Daniel Gitzel, Instructor
gitzel@cooper.edu

Fall 2020

Course Description

This course covers both attacker and defender perspectives of applied information security. Topics will include networked and embedded applications, access control systems and their failure modes, privilege escalation, intrusion detection, privacy and data breaches and applied cryptography. Each topic will be approached through analysis and discussion of historical cybersecurity incidents and possible mitigations. Safe coding practices and OS flaw mitigation will be explored through case studies and reinforced through security sensitive programming projects. Coursework will include penetration testing, code auditing, and independent projects.

Prerequisites

Required:

- ECE303 (Communications Networks)
- ECE357 (Operating Systems)

Useful:

- Knowledge of Unix-like OS
- Comfortable in command-line interface
- C and x86 assembly experience
- A curious mind!

Lecture Schedule

The following is an outline of the course schedule and may be subject to change.

- **08/31** *Introduction*: foundations of security, threat modeling, security and risk management
- **09/07** *Labor Day*: No class
- **09/08** *Add/Drop Deadline*: FYI
- **09/14** *Identification and Authentication*: login, spoofing, social engineering, multi-factor
- **09/21** *Access Control*: controls, groups, and permissions
- **09/28** *Monitoring and detection*: hardware and OS integrity, protecting memory
- **10/05** *Basics of Unix & Windows Security*: principles, subjects, access control, management issues
- **10/05** *Software & Database Security*: common vulnerabilities and defenses

- **10/12** *Cryptography*: background, block ciphers, symmetric key encryption, hashes (Project Proposals Due)
- **10/19** *Cryptography*: public key exchange, common pitfalls, crypto-currencies
- **10/26** *Midterm Exam*: Covers all topics from Lectures 1–7.
- **10/28** *Withdraw Deadline*: FYI
- **11/02** *Network Security*: background, threat model, protocol design, lower layers
- **11/09** *Network Security*: TCP, DNS, and TLS, firewalls, detection (Project Check-in)
- **11/16** *Web Security and Privacy*: Web browsers, cookies, Javascript
- **11/23** *Web Security and Privacy*: Tor network, privacy, tracking, mobile devices
- **11/30** *Selected Topics*: IoT devices and security, side channel and hardware attacks
- **12/07** *Selected Topics*: continued, and review of course material
- **12/14** *Final Project Presentations*

Reading Material

The primary textbook for is course is Dieter Gollman's "Computer Security" 3rd edition [4]. For the cryptography portion of the class, I'll be referencing both "Applied Cryptograpy" by Bruce Schneier [5] and "Cryptography Engineering" by Ferguson, Schneier, and Kohno [6]. I'll also reference industry white papers on actual implementations of these systems.

I may reference a few supplementary texts, these are optional resources, check if the library has a copy. "The Tangled Web" by Michal Zalewski [7] is a guide on securing web applications and browsers. "Practical Malware Analysis" by Sikorski and Honig [9] is a discussion on Windows malware. Finally, "Silence on the Wire" by Michal Zalewski [8] is a fun read on side channel and indirect attacks (some not so practical, others interesting).

The paper by Diffie and Hellman [1], describes their key exchange mechanism which is widely used to establish an encrypted communications channel. Their method describes one of the first public-key protocols later described by Merkle [2]. Students may also find various documented historical attacks [3] against network infrastructure of interest.

Coursework

Homework

Problem sets and programming assignments will be issued roughly every-other week. These might be collected and graded, but are primarily for your benefit to try out some of the things you've learned. Many of the pitfalls of security are in the execution and implementation; the cryptography is bullet-proof, but the code might have bugs!

Quizzes

Short quizzes will be based on both textbook and research paper reading assignments. These will cover landmark developments in security and may be sourced from academic or industrial research.

Final Project

The final for this class will be a research project into a known security vulnerability. Students are encouraged to look for interesting papers during the semester to attempts to replicate and extend. We'll present the findings during the last class session.

Grading Policies

- Homework (10%), Quizzes (30%), Midterm Exam (30%), Project (30%)
- All assignments are due at the start of lecture.
- Late homeworks will receive a 0.
- Late projects will receive a 10 point penalty per day.
- Collaboration between teams is allowed and encouraged; however, explicit copying of code is prohibited. Any code that you did not write yourself, excluding standard libraries, must be attributed. Failure to do so will result in a 0 on the project.
- Missed exams or quizzes will receive a grade of 0 without prior arrangements or an explanatory note.

Exams are supposed to be hard, not a simple regurgitation of homework problems; however, they are graded on a curve.

References

[1] Whitfield Diffie and Martin Hellman, "New directions in cryptography." *IEEE Transactions on Information Theory 22*, no. 6 1976: p. 644-54.

[2] Ralph C. Merkle, "Secure communications over insecure channels." *Communications of the ACM 21*, no. 4 1978: p. 294-9.

[3] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin, "Breaking 104 bit WEP in less than 60 seconds." *Cryptology ePrint Archive, Report 2007/120*, `https://eprint.iacr.org/2007/120`, 2007.

[4] Dieter Gollman, "Computer Security." Wiley, 2011.

[5] Bruce Schneier, "Applied Cryptography." Wiley, 1996.

[6] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, "Cryptography Engineering." Wiley, 2010.

[7] Michal Zalewski, "The Tangled Web." No Starch Press, 2011.

[8] Michal Zalewski, "Silence on the Wire." No Starch Press, 2004.

[9] Michael Sikorski and Andrew Honig, "Practical Malware Analysis." No Starch Press, 2012.