ECE 458 - Computer Security, Spring 2020 (Online)

Instructor: Professor G. Gong
Office: E7 5436, x45650, ggong@uwaterloo.ca
https://uwaterloo.ca/scholar/ggong
Office hours: TBD

Webpage: UW-LEARN

Course Description This is an introductory course for computer security. The course will consist of five modules and cover the topics of models of security, attacks on program and operation system, practical cryptography, threats to networks and wireless system, web security, secure design principles, evaluation, privacy, and applications.

Objectives: A primary objective of this course is that the student should gain wide-ranging knowledge of many aspects of computer security and think adversarially about computer systems.

Prerequisites ECE 254 or SE 350; Level at least 4A Computer Engineering or Electrical Engineering or Software Engineering.

Antirequisites CS 458.

Textbooks

- There is **NO** required text book. If you want additional reading:
  - C. Pfleeger, S. Pfleeger, and J. Margulies, Security in Computing, 5th edition, Prentice Hall, 2015. ISBN: 0134085043.
  - W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th edition, Pearson, 2017. ISBN: 0134794109.
  - S. Smith and J. Marchesini, The Craft of System Security, Pearson, Addison Wisely, 2007. ISBN: 9780321434838.
- Lecture Notes: Available on UW-LEARN.
- Some revised contents for the book, *Communication System Security*, CRC, 2012, by L.D. Chen and G. Gong, will be provided.
- Some additional readings links will be provided.

Course Outline

1. Basics of Security: trust and threat model, memory safety, program and OS security, trust platform, and attacks on processors.

2. Practical Cryptography: pseudorandom generation, symmetric-key crypto, public-key cryptography, and digital signature.
3. Network and Wireless Security: TLS/SSL, tunnel model, firewalls and intrusion detection; and WiFi, 4G-LTE/5G, and attacks on location services.
4. Web Security: attacks on browser, SQL injection, password based authentication, Kerberos, and open-authorization.
5. Applications: RFIDs, IoT, blockchain, and privacy preserving machine learning.

Teaching Assistants

- Guiwen Luo (full TA, 1.00 load), g27luo@uwaterloo.ca.
- Akshay Goyal (0.6 load), a49goyal@uwaterloo.ca.
- Rongzhi Gu (0.5 load), rongzhi.gu@uwaterloo.ca.

Course Logistic

- The lectures will be in asynchronous mode. Each lecture is provided by a 50-minute video. I will divide each video into 2 or 3 small pieces for your easy to download.
- In this term we will be using Piazza for discussions on course related questions and comments. So please send them there. Find our class page at: `https://piazza.com/uwaterloo.ca/spring2020/ece458/home`. Access code can be downloaded from LEARN.
- Avoid public posts that reveal solutions to homeworks/projects.

Course Grading

- 5 homework assignments (30% total). Done individually.
- 2 course projects (25%). Done individually or in groups of 2.
- A comprehensive open book final exam (45%).

Other Resources

- Schneier on Security, `http://www.schneier.com/blog/`. A blog covering current computer security and privacy issues.
- Kevin Du, Seed Labs, University of Syracuse, `https://seedsecuritylabs.org/lab_env.html`. The lab contains many hand-on experiments and some crafted attacks can be launched under their specific environment for better understanding them.
- BugTraq, `http://www.securityfocus.com/archive/1`. A full disclosure moderated mailing list for the detailed discussion and announcement of computer security vulnerabilities.