EE 418: Network Security and Cryptography

Autumn 2017

Instructor: Xuhang (Shaun) Ying
Teaching Assistant: Zhipeng (Leo) Liu
Course Information

• **Time & Location:**
  - Tuesdays and Thursdays, 2:30pm – 3:50pm, EEB 003

• **Instructor:** Mr. Xuhang (Shaun) Ying
  - Email: xhying(at)uw(dot)edu
  - Office hours: Tue and Thu, 4:00pm – 5:00pm (or by appointment), EEB M406

• **Teaching Assistant:** Mr. Zhipeng (Leo) Liu
  - Email: zhipliu(at)uw(dot)edu
  - Office hours: Mon and Wed, 4:00pm – 5:00pm, SIEG128.

• **Course website:**
  - Any course related info: lecture notes, homework and project.
  - Link: [https://class.ee.washington.edu/418/2017aut/](https://class.ee.washington.edu/418/2017aut/)
  - Others: discussion board, Dropbox, reading materials.
Course Overview

• **What is covered?**
  - Fundamental principles of cryptography, and its applications in network and communication security.
  - Basic cryptographic theory and techniques.
  - No prerequisite required.
  - Basic knowledge in discrete math and algorithm would be helpful, but this course is pretty much self-contained.

• **Two key themes of this course**
  - How to think about security and privacy
  - Technical aspects of security and privacy
Course Syllabus

• **Week 1**: Course overview. Introduction to security and privacy.
• **Week 2**: Classic **cryptosystems** (e.g., how to encrypt/decrypt plaintext/ciphertext)
• **Week 3**: Cryptanalysis of classical cryptosystems (e.g., how to attack/break a cipher).
• **Week 4**: From symmetric/shared key cryptography to public key cryptography.
• **Week 5**: Public key cryptography. Two examples: RSA, ElGamal.
• **Week 6**: Diffie-Hellman key distribution. **Midterm** (Nov 2, in-class).
• **Week 7**: Hash functions to generate fingerprints: from confidentiality to integrity.
• **Week 8**: Iterated hash functions. Example: message authentication codes.
• **Week 9**: Digital signatures: another application of public key cryptography.
• **Week 10**: Public key infrastructure: manage and distribute public/private keys.
• **Week 11**: Web security. Emerging technologies. Ethics and course wrap-up.
• **Final Week**: **Final exam** (Tue, Dec 12, 4:30-6:20pm, EEB 003)
Grading

• Homework: 20%
• Projects: 30%
• Mid-term exam: 20%
• Final exam: 20%
• In-class activities + online discussions: 10%
Homework

• **Up to 5 homework assignments.**
  • If four are given, each will carry 5%.
  • If five are given, the best four are counted.

• **Format:**
  • Mix of written questions, coding and simulations.
  • For coding, choose your favorite language (e.g., Matlab, Mathematica, Python), but please submit your source code.
  • Sample code, if any, will be provided in Matlab (or Python?).

• **Submission:**
  • Due in-class on the date indicated in the assignment.
  • No homework will be due during exam weeks.
Projects

- **Objective:**
  - Better understand security and privacy concepts through hands-on experience.

- **Format:**
  - There will be two group projects. Each carries 15% (total is 30%).
  - Written questions + coding/simulation.
  - The maximum allowed group size is three.

- **Submission:**
  - Submit written report and source code through Dropbox.
  - You will have several weeks to complete them.
Exams

• **Mid-term:**
  • November 2, in-class (2:30pm-3:50pm), EEB 003

• **Final-term:**
  • Tue, Dec 12, 4:30-6:20pm, EEB 003

• **Format:**
  • Open book, open notes, and open homework
  • Sample exams will be provided for preparation.
In-Class Activities + Online Discussions

• **Possible in-class quiz** at the beginning of class
  • Help you review the materials from last lecture.
  • You may discuss with your classmates to solve them.
  • Students will be invited to explain them.

• **Online discussions:**
  • Ask & answer homework/project questions etc.
  • **Share & comment** interesting news/articles/papers/stories in security & privacy, e.g.,
    • Equifax data breach: how did it happen? how does it affect you?
    • Two-factor authentication is a mess (**Link**): what is the weakest point? How do you, as a user, learn from this article?
    • iPhone 8 face recognition: how do you like the feature?
  • **Proposal:** 5-min presentation (2 or 3 slides) in the second half
Course Materials

• **Textbook:**

• **Reference books:**
  - W. Stallings, *Cryptography and Network Security*
  - B. Schneier, *Applied Cryptography*
  - A. Menezes, P. Van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*
Questions?