ECE 443/518 – Computer Cyber Security
Lecture 01 Introduction

Professor Jia Wang
Department of Electrical and Computer Engineering
Illinois Institute of Technology

August 19, 2024

Outline

Reading Assignment

- This lecture: Course Syllabus, ICS 1
- Next lecture: UC 1

Outline

Instructor

- Professor Jia Wang
- E-Mail: jwang34@iit.edu
- Office hours: TBD

Lectures

- Mon./Wed. 11:25 AM – 12:40 PM
- IIT Tower 16E4-1
- Course website:
  `http://www.ece.iit.edu/~jwang/ece443-2024f`

Textbooks

- Required Textbook

  UC "Understanding Cryptography: A Textbook for Students and Practitioners" C. Paar and J. Pelzl, Springer, 2010. ISBN-13: 978-3642446498
  `https://link-springer-com.ezproxy.gl.iit.edu/book/10.1007/978-3-642-04101-3`

- Recommended Textbook

  ICS "Introduction to Computer Security"
  M. Bishop, Addison-Wesley, 2005. ISBN: 0321247442

Useful Websites

- `https://www.cryptography-textbook.com/first-edition/`
  - Website of the textbook UC, with lecture slides and videos from the authors.
- `https://www.schneier.com/`
  - Schneier on Security, with a lot of blog and news articles.

Prerequisite

- Computer programming
- Digital logic and computer organization
- Probability

Course Outline

The Security Mindset

- Computer cyber systems: software and hardware, collaboration via (network) communications.
- Secure communication: introductory cryptography.
- Secure collaboration: advanced cryptography.
- System security and hardware security.
- Digital forensics.
- Languages and libraries for cryptography applications.

Course Objectives (ABET)

After completing this course, you should be able to:

1. Describe computer cyber security as threats and defense mechanisms.
2. Understand stream ciphers, block ciphers, cryptographic hash functions, and public-key cryptography.
3. Explain authenticated encryption, man-in-the-middle attack, perfect forward secrecy, and their impact on secure communication protocol designs.
4. Understand system security concepts including security policies and access control.
5. Describe vulnerabilities in software and hardware systems.
6. Explain digital forensics processes.

Homeworks/Projects

- 4 Homeworks
  - 5 points each for a total of 20 points
- 6 Projects
  - 15 points each for a total of 90 points
- Submit online in Canvas only.
- Late homeworks and projects will not be graded.

Exams

- Midterm: 11:25 AM – 12:40 PM, Wed., 10/9
  - 30 points
- Closed book/notes, cheat sheet allowed
- Makeup exams will NOT be given.

ECE 443 Grading

- A: 90
- B: 80
- C: 60
- D: 55

ECE 518 Grading

- A: 110
- B: 90
- C: 75

Project Setup

- Please install VSCode and Go following the instructions on: `https://docs.microsoft.com/en-us/azure/developer/go/configure-visual-studio-code`

Ethics (Very Seriously)

- Read "IIT Code of Academic Honesty" and "IEEE Code of Conduct" (posted on the course website).
  - Projects/homeworks should be done individually.
  - Discussions on homeworks/projects are encouraged.
  - Interactions with AI assistants (prompts and answers) should not be shared since they are considered as your own work.
  - Source code from the lectures and instructions in this course can be used directly.
  - Source code from other online sources not directly related to this course may be used with proper references.
- All other writings and code should be BY YOURSELF.
  - NEVER SHARE YOUR WRITINGS/CODE WITH OTHERS!
  - NEVER USE WRITINGS/CODE FROM OTHERS!
  - NEVER POST YOUR PROJECT CODE OR ASK FOR HELP DIRECTLY ONLINE!
- Please review our Academic Honesty Guidelines.
  `https://web.iit.edu/ugaa/academic-honesty`

Outline

Any Risk?

- Passwords
  - Use simple passwords.
  - Use the same password for many websites.
- Emails
  - Click links in emails.
  - Open attached files in emails.
- Computers (desktop, laptop, smart phones, etc.)
  - Use USB drives.
  - Send your laptop or cell phone for repair.
  - Install applications.
  - Throw out broken Wifi bulbs.
- Can you prevent others to fall into similar traps that may affect you?

More Questions to Answer

- How to protect our (online) privacy?
  - With a lot of our photos and videos posted online?
  - When our names, addresses, phone numbers, credit cards, and even government-issued id numbers are already leaked?
- What is cryptocurrency?
  - How to safely store Bitcoin? Is it the same as safeguarding money in a bank?
  - Are CBDCs (central bank digital currencies) also a kind of cryptocurrency?
- If you have nothing illegal to hide, why you encrypt your data?

CIA: Basic Components of (Computer Cyber) Security

- A king need to send messages to a general fighting in a war.
  - War and banking are two most common recurring themes when discussing security.
- Confidentiality
  - Only the king and the general can read the messages.
- Integrity
  - The general should only accept messages sent by the king.
- Availability
  - Some of the messages must be able to reach the general.
- We will focus on confidentiality and integrity for this course, and discuss other important components including authentication, authorization, and nonrepudiation later.

Threats and Attacks

- Threats: potential violation of security
  - E.g. snooping, alteration, spoofing, repudiation of origin, denial of receipt, delay, denial of service in a messaging system.
  - And many more.
- Attacks: what cause violations to occur
- Need to guard against attacks that might happen.
  - Before an attack actually happens.
- The security mindset: can you envision an attack to a system even before the existence of the attack?

Security Policy and Mechanism

- Policy: what is, and what is not, allowed.
  - E.g. only the king and the general can read the messages.
- Mechanism: how to enforce the policy.
  - E.g. to encrypt the messages using a secret key known only to the king and the general.
- In many cases, it is impossible to enforce the policy without a proper mechanism.
  - E.g. how to enforce the policy that only the king and the general can read the messages without encryption?
- The use of a mechanism may require additional policies.
  - E.g. neither the king nor the general should tell anyone else about the secret key, and they should choose a complex secret key.

Assumptions and Trust

- But how could we be sure that a policy together with the mechanism will correctly guarantee desired security?
- We need assumptions!
  - E.g., we assume that attackers cannot decrypt the messages without the secret key.
  - We have to make additional assumptions if the king and the general use computers and networks to communicate.
- Trusts: assumptions based on other assumptions
  - Hardware is secure. By secure we mean that it computes correctly and will not leak key or messages.
  - OS and libraries are secure.
  - Software implementations are secure.
  - And so on.
- Assumptions may be undermined over time.
  - What if we could factor large integers efficiently tomorrow?

Practical Issues

- Policy and mechanism that are good in theory may still fail in practice.
- Operational Issues
  - Some mechanisms are too costly to enforce
  - Some subsystem needs less protection than others
  - What if encryption is illegal?
- Human Issues
  - Underestimating the loss, responsibility vs. power, lack of workforce and resource
  - Attacks from insiders, lack of training, human errors

Summary

- Computer cyber security as threats and defense mechanisms.
- Practical issues.