Lecture 1: Course Overview

Kehuan Zhang

IERG4130 2022

Brief introduction to the course

- Topics to be covered in this course
- Student Evaluations
- Landscape of Cyber Security

Brief self-introduction

- Joined CUHK in 2012
- Focus on system security research
    - Mobile device security
    - Embedded system security
        - E.g., Internet of Things (IoT)
    - Machine Learning Security, Web, Cloud computing, Operating System, etc.
    - Recent work got accepted on top international conference in security area
    - Also got wide media coverage:
        - Mobile Payment
        - Face Flashing
- More information at lab home page:
    - LASR: Lab for Applied Security Research
    - `http://lasr.ie.cuhk.edu.hk`
    - Or my personal web site `https://staff.ie.cuhk.edu.hk/~khzhang`
- Office hour:
    - Thursday 2:30pm - 3:30pm, or by appointment

Tutors

- Zirui Song
  - office: SHB726
  - email: sz019@ie.cuhk.edu.hk
- Ke Zhang
  - office SHB 726
  - email: zk019@ie.cuhk.edu.hk
- Jiuqin Zhou
  - office SHB 726
  - email: zj021@ie.cuhk.edu.hk
- Yikang Chen
  - office SHB 826B
  - email: cy021@ie.cuhk.edu.hk
- Office hour: To be determined

Teaching Activity

- Lecture
  - Twice a week, on Tuesday and Thursday
  - Mainly Face-to-Face mode
  - Given the COVID-19, will also provide ZOOM and recorded videos
    - https://cuhk.zoom.us/j/99456640851
    - Meeting ID: 994 5664 0851
    - Passcode: lasr
    - NOTE:: you need to log into ZOOM with CUHK account first
    - However, it is hard to have interactions via ZOOM
    - So if you may need to talk tutors or me offline if you have any questions
- Tutorial
  - You need to attend one and only one session
  - Provide extra material, helping on assignments, etc.
  - The time will be decided later
- Office hours
- Assignments & Labs
- Mid-term and final-term exams

Evaluation

- Assignments - 30%
  - Three assignments
- Labs - 15%
  - Two hands-on experiments (offline, do it on your own computer)
- Mid-term - 15%
  - Date is schduled on Oct 20 (Thursday), 9:30am – 11:15am
- Final-term - 40%

Interactions and Communication Channel

- You can get basic course information and schedule from course web
  - https://course.ie.cuhk.edu.hk/~ierg4130/
- Lecture notes, assignments, announcements, tutorials, etc., will still use Blackboard
  - Blackboard System: `https://elearn.cuhk.edu.hk`
- For Q&A, we use piazza.com:
  - You can enroll with the URLs later (to be activated)
  - `https://piazza.com/cuhk.edu.hk/fall2022/ierg4130`
  - An extra three

Topics to be covered

- Part I: Basic Concepts and Tools
  - CIA Triangle, Security Principles
- Part II: Software Security
  - Buffer overflow and defenses, malicious code, secure coding
- Part III: Cryptographic Algorithms
  - Encryption algorithms: concepts, symmetric key encryption, asymmetric key encryption, stream cipher vs. block cipher, etc.
  - Message integrity: Hash, Message Authentication Code, Digital Signature, certificate, etc.
- Part IV: Network Security
  - Basic concepts, typical attacks
  - Firewall, Intrusion Detection Systems, De-militarized Zone, etc.
  - Web Security: Same-Origin-Policy, Cross-Site-Scripting (XSS), Cross-Site-Request-Forgery (CSRF), SQL Injection, etc.
  - Wireless Security: WEP/WPA/WPA2 Protocols, Sniffing Attack, etc.
  - Secure Networking Protocols (IPSec, TLS, PGP, etc.)
- Part V: System Security
  - Access Control, Adversary Model, etc.
  - Mobile Security, etc.

Tentative Teaching Schedule

- Please refer to our course home page
  - `https://course.ie.cuhk.edu.hk/~ierg4130/`
- The schedule may be changed based on our learning progress
- Pay attention to the date of mid-term – start to prepare early
- Assignments and Lab instructions will be announced later (through Black-board system)

Expected Learning Outcome

- Acquire the ideas and concepts of common cyber security problems
  - Be able to understand common attack and defense techniques
  - Be able to perform security analysis on some real world cases
  - Be able to deploy necessary defense technologies

Acknowledgements

- Slides in this course have used materials following sources
  - Most are adapted from slides by Prof. Wing C Lau in previous years
  - Others
    - ★ William Stallings, “Cryptography and Network Security, 3rd Edition”
    - ★ Simon Garfinkel, Gene Spafford, “Web Security, Privacy and Commerce”
    - ★ Charlie Kaufman, Radia Perlman, Mike Spenciner, “Network Security”
    - ★ Prof. Vern Paxson, UC Berkeley
    - ★ Prof. Vincent Costa, Hofstra University
    - ★ Prof. Henning Schurzinne of Columbia University
    - ★ Prof. Felix Wu, UC Davis
    - ★ Prof. Dan Boneh, Stanford
    - ★ Prof. Wenke Lee of Georgia Tech
    - ★ Prof. Yehuda Afek, Tel Aviv Univeristy
    - ★ Prof. Giovanni Vigna, UC Santa Barbara

Textbook and References

- We mainly rely on the lecture notes
  - Since none single textbook satisfy our requirements
- Any copy of following textbooks will be helpful (but not mandatory):
  - Computer Security: Principles and Practice (3rd ed. or later)
    - by William Stallings and Lawrie Brown, Prentice Hall, 2014.
    - **both Chinese and English version are available in mainland China**
    - E.g., `https://item.jd.com/12682948.html`
  - Introduction to Computer Security, 1st Edition
    - by Michael Goodrich, Roberto Tamassia
  - Cryptography and Network Security - Principles and Practice (6th ed. or later)
    - by William Stallings, Prentice Hall, 2013.
- Old versions are also OK

The landscape of Cyber Security

- Study the security problems related to **Cyber Space**
    - What is Cyber Space? A digital world within interconnected computing devices
- Cyber Security is important
    - At country level, it is a new (the 5th) battle ground besides traditional land, sea, air, and space
    - For company and organizations, it means economic and reputation gain and loss
    - Also big influence on each individuals (e.g., privacy, digital assets, metaverse . . .)
- Cyber Security is challenging
    - No perfect technology
    - Always make trade-offs among multiple constrains: cost, market share, usability, . . .
        - ★ Example: history of Android
    - Law and policy will always lag behind
        - ★ Example: 2018 European Union's General Data Protection Regulation (GPDR)
    - Weakness of human natures: e.g., curiosity, love *free* things, . . .

The landscape of Cyber Security - My understanding

- The Science, technology, and Engineering of attacking and defending computing systems
  - What is **Science**?
    - Science is to find existing but unknown laws and patterns
    - A typical element of science in cyber security is crypto algorithms
  - What is **Technology**?
    - Technology is to create new methods and things that were not existing before
    - Many technologies in cyber security, e.g., encryption, authentication, firewall, . . .
  - What is **Engineering**?
    - Engineering is to apply or deploy technologies in larger scale and lower cost
- A question: why cyber security should also include **attack**, why not only defense?
  - Defending is not the whole story of cyber security
  - Attacking is the driving force for cyber security
  - No attack → no defense → no existence (or improvement) of security

Why Do People Want to Attack?

- For fun
  - Hackers in old days
  - Amateur hackers
- For profit
  - Hackers in modern days
  - Especially for professional and organized hackers
- For national security
  - Cyber war
  - Critical infrastructure
  - Another meaning of “the best defense is to attack” Benign attacks can find vulnerabilities before the been exploited by adversaries.
- Attacking techniques are evolving in cyber space
  - Steal money:
    - Traditional: Pick-up wallet from someone’s pocket or bag
    - Cyber version: pick-up the mobile wallet
  - Door access:
    - Traditional: open a door with paper clip
    - Cyber version: hack into a smart lock

How Many Attacks Are There?

- Unlimited, and more to come everyday
  - Hackers are really innovative
  - Why?
- But fundamentally, most attacks are similar
  - E.g., malware families, virus variants, vulnerability exploits, etc.
  - Except some really new ones
- Open Discussion
  - What kind of Attacks you may know or have even experienced?

How to Protect Ourselves in Cyber Space

- Take this course :)
  - So you will know potential security risks
- Thinking through the phenomenon
  - Try to link what would have learned in this course with real world cases
  - Try to understand the hidden reasons, principles and technologies
- Apply the techniques learned in this course
- Pray!
  - There are many things we cannot control
  - E.g., companies may leaked our personal information
  - An real world incident: Cathay Pacific data leakage

Summary

- Brief introduction of this course
    - topics, evaluations, etc.
- My thoughts on the cyber security at high level
- Next time:
    - Basic Concepts and Tools for Cyber Security