Introduction to Cyber Security

Fall 2017 | Sherman Chow | CUHK IERG 4130

香港中文大學
The Chinese University of Hong Kong

信息工程學系
Department of Information Engineering

My Contact

- Office: Room 808, Ho Sin Hang Engineering Building
- Email: smchow [at] ie.cuhk.edu.hk
  - Prepend subject of the email with [IERG4130]
  - Use your institutional email (@cuhk.edu.hk) for correspondences
  - I will not check my junk mail box
- Course website: https://course.ie.cuhk.edu.hk/~ierg4130
  - We also use blackboard for delivering materials and discussion
  - It is your responsibility to check these web resources and emails

What this course is mostly about

- **Cryptography**
  - quickly introduce probability, number theory, abstract algebra, *etc.*
- **Network security**
  - How crypto can be used to ensure network security
  - Other non-crypto techniques, e.g., firewall
  - Prerequisite: IERG 3310 Computer Networks
  - or CSCI4430 Data Communication and Computer Networks
  - (Note that CSCI4430's Prerequisite is:

    CSCI3150 Introduction to Operating Systems)

What the rest of this course is about

- System security
  - You should know what is an operating system before learning operating system security.
- Application security (buffer overflow attack)
  - You should know some basic *principles of programming languages*, such as C function *stack*, then you can study how to smash the stack.
- Web security
  - You should know how the browser, DNS server, and web server inter-operate, how HTTP and DNS packets look like, then you can start to think about what could go wrong.
- *etc.*

Cyber Security Stream for BEng(IE)

- Operating Systems
- This course will also be offered in the next semester (Spring 2018)
- IERG 4210 Web Programming and Security (concurrently)
- IERG 4220 Secure Software Engineering (2nd time of offering, in Spring 2018)
- IERG 5240/ENGG 5383: Applied Cryptography (concurrently, had UG's)
- IERG 5310 Security and Privacy in Cyber Systems
- IERG 5320 Digital Forensics (had undergraduate students)
- http://www.ie.cuhk.edu.hk/programmes/ierg_streams.shtml

Information Security Certifications

- International Information Systems Security Certification Consortium, a.k.a. (ISC)²
  - e.g., CISSP
- International Council of E-Commerce Consultants (EC-Council)
  - e.g., Certified Ethical Hacker (CEH)
- SANS Institute: Global Information Assurance Certification (GIAC)
  - e.g., Forensic Analyst
- many others

Certified Information Systems Security Professional

- **Access control; Telecommunications and network security**
- Information security governance and risk management
- Software development security
- **Cryptography; Security architecture and design;** Operations security
- Business continuity and disaster recovery planning
- Legal, regulations, investigations and compliance
- Physical (environmental) security

What this course is *not* about

- We will not cover the basics in details (except Cryptography)
- (In contrast, it is not like IERG4210, which covers Web Programming first, *then* its Security.)
- We will not focus on only hacking (we will have some though)
- We will not focus on writing secure code

What you need for this course

- Hands-on skills to perform the attack
- Mathematical aptitude and maturity to understand cryptography a.k.a. the sciences of "secret writing"
- Do your reading (textbook, other web resources, etc.)
  - We cover a large number of topics and there can be some which you may not master well

Required Textbook (any 1)

- Cryptography and Network Security - Principles and Practice, by William Stallings, 6th ed., Prentice Hall, 2013.
- Computer Security: Principles and Practice, by William Stallings and Lawrie Brown, 2nd ed., Prentice Hall, 2011.
- Network Security: Private Communication in a Public World, by Charlie Kaufman, Radia Perlman, and Mike Spenciner, 2nd ed., Prentice Hall, 2002.
- [Slides are designed for teaching, not tailor-made for revision]
- Consult us (the teaching staff) in case you “missed” any lecture

Tentative Rundown

- Landscape of Cyber Security
- Applications security: buffer-overflow attacks
- System security
- Web-applications security
- (This means you can start your hands-on assignment/lab early)

Tentative Rundown (cont.)

- Overview of Cryptography: modern application, classic ciphers, symmetric ciphers, stream vs. block ciphers
- Symmetric key cryptography: 3DES, AES, mode of operations
- Hashes, message digests and message authentication codes
- Public key algorithms: RSA and Diffie-Hellman
- More public key schemes; Elliptic curve cryptography; Public key infrastructure; Authentication
- (So your mid-term examination will be mostly about Cryptography)

Tentative Rundown (end)

- Key Management and Kerberos
- Network security: sniffing, spoofing, hijacking, denial-of-service
- Firewall, DMZ, VPN, intrusion detection
- Secure networking protocols
  - e.g., IPSec, SSL/TLS, S/MIME, PGP
- (We will still have some labs for you to try on something, say, sniffing and spoofing)

Tentative Assessment

- Participation: tutorial attendance, take-home reading, *etc.* (5%)
- Assignment x 4 (15%)
- Labs (with written part and hands-on part) x 4 (15%)
- Mid-Term x 1 (20%)
  - Open cheat-sheet (single sided)
- Final examination (45%)
  - Open cheat-sheet (both side of an A4 paper)

Learning Outcomes

- Obtain an introductory level of understanding of major areas of cyber security, including cryptography, network security, system security, and web security
- Gain experiences in network security and web security
- Able to apply the learning outcomes of this course towards a potential career in the governance of system, network, and websites (for the last one, also take IERG4210)
- (Foundation for taking advanced classes: IERG5240/5310/5320)

Special Arrangement (or lack thereof)

- Lecture time:
  - Tuesday 12:30-2:15pm (LT2)
  - Wednesday 10:30-11:15am (LT1)
- There is no holiday in this semester on Tue/Wed
- 13 weeks in Sep, Oct, and Nov (4 + 4.5 + 4.5)
- I may hold Cantonese (& Mandarin) extra tutorial on crypto

Teaching Assistant

- TAI, Ka Ho Raymond (tkh016@ie, SHB801)
  - Took this course 2 years ago
  - 2nd time TA-ing this course
  - My year-2 MPhil student
- Email for appointment

What you see in every courses

- Honesty in Academic Work
  - http://www.cuhk.edu.hk/policy/academichonesty/
- Anti-Plagiarism
  - http://www.cuhk.edu.hk/clear/tnl/Plagiarism_English.html
  - http://www.cuhk.edu.hk/clear/tnl/Plagiarism_Cantonese.html