Chapter 0
Logistics
Sherman S. M. CHOW

- Associate Prof., Dept. Information Engineering (Nov ’12 – now)
- Research: Cryptography, Privacy, Distributed System Security
- 4th time teaching this course

Research Fellow
Dept. of Combinatorics and Optimization

Research Intern
MSR Redmond
W.A., USA

PhD, MS
Courant Inst. of Math. Sciences

MPhil, BEng (1st Hon.)
Department of Computer Science
Our Contacts

- My Email: sherman [at] cuhk.edu.hk
  - Prepend subject of the email with [DSME6788i]
  - Use your institutional email (@cuhk.edu.hk) for correspondences
  - (My Office: Room 808, Ho Sin Hang Engineering Building)

- We use blackboard for delivering materials and discussion
  - It is your responsibility to check these web resources and emails

- TA: Harry Wong (harrywhwong [at] link.cuhk.edu.hk)
  - My senior Ph.D. student working on cryptography
What this course is mostly about

- **Security**
  - Security management
  - Software security, System security
  - Database security, Web security
  - Intrusion detection, Firewall

- **Cryptography**
  - We will introduce the necessary mathematics background
  - Yet, we will try to minimize the reliance on mathematics
  - Cryptocurrency and Blockchain
What this course is *not* about

- We will not cover the basics in detail (except Cryptography)
  - We will try to quickly recall some technical background though.

- We will not focus on only hacking (we will see some though)

- We will not talk about (secure) programming
  - But some related elements may appear (*e.g.*, SQL)
Information Security Certifications

- International Information System 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

1: Security and Risk Management – 15%
2: Asset Security – 10%
3: Security Architecture and Engineering – 13%
4: Communication and Network Security – 14%
5: Identity and Access Management (IAM) – 13%
6: Security Assessment and Testing – 12%
7: Security Operations – 13%
8: Software Development Security – 10%
What you need for this course

- Some hands-on skills to perform the attack
- Some 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
  - Probably there are some which you may not master well
Computer Security: Principles and Practice
by William Stallings and Lawrie Brown
takes 2-3 working days to order
from Commercial Press
(other editions should be helpful too)
Other Relevant Textbooks


- Slides are designed for teaching, not tailor-made for revision
- “Extra” materials will appear which are not from textbook
- Consult us (the teaching staff) in case you “missed” any lecture
I. December 6:
- Introduction (1 // Chapter number of Stallings-Brown textbook)

II/III/IV. December 13, 20, 3/1:
- Cryptography (2)
- Symmetric Encryption and Message Confidentiality (20)
- Public-Key Cryptography and Message Authentication (21)
- Internet Authentication Applications (Key Management) (23)
V. January 8:

- User Authentication (3), Access Control (4)

VI. January 10:

- Database and Data Center (5), Malicious Software (6)

VII. January 17:

- IT Security Management and Risk Assessment (14)
VIII. January 24:
- Software Security and Web Security (11)
- Security Principles (General, no textbook correspondence)

IX. February 7:
- Mid-term examination (tentatively)

X. February 14:
- Denial of Services (7), Intrusion Detection (8), and Firewall (9)
XI. February 21:

- Cryptocurrency and Blockchain

XII. February 28:

- Other Special Topics
Tentative Assessment

- Participation (10%)
  - class participation, take-home reading, end-of-lecture-quiz, etc.
- “Lab” Assignment (both written and hands-on parts) (15%)
- Written Assignment (15%)
- Mid-Term Examination (30%)
- Group Project (30%)
4-5 students as a group, investigate a topic related to security

(group size depends on the final number of enrollment)

A group report, the usual format includes but not limits to

- executive summary (or abstract), (general) introduction,
- technical preliminary (if any, not covered by this course),
- technical details (the “meat”),
- comparison with “competitor”, “friend/relative”, whatever appropriate
- your own evaluation, etc.

Evaluation based on quality, not length
Possible Topics

- Technical reflection of a real-world security incident
- Technical survey of the security features of some app/service
- New product idea with security as its key feature(s)
- Examining the current infrastructure and practices of a small- to medium-sized organization, justify its appropriateness or propose new tools/infrastructure/practices for “better” security
- Studying 1/2 recent academic papers in security/cryptography
Proposed/Tentative Timeframe

- Group formation by January 8
- Topic declaration by January 17
- Proposal/Preliminary report due on February 8
- Peer Evaluation (early March?)
- Final Report (early March?)
  - I would like to give you more time
  - but I have to fulfill my own grade submission deadline
uReply (Interactive Classroom App)

- https://www.web.ureply.mobi
Learning Outcomes

(1) assess the current security landscape and the likely consequences of security failures;

(2) apply the practices, technologies, and protocols of cyber security to secure business operations;

(3) assess the security challenges in the virtual, cloud, and mobile processing environments;

(4) understand the legal, ethical, and regulatory issues associated with cyber security policy development, implementation, and administration.
What you see in every courses

â† Honesty in Academic Work
  â† http://www.cuhk.edu.hk/policy/academichonesty

â† Anti-Plagiarism
  â† http://www.cuhk.edu.hk/clear/tnl/Plagiarism_English.html
  â† http://www.cuhk.edu.hk/clear/tnl/Plagiarism_Cantonese.html