IEMS5710 Cryptography, Info. Security & Privacy

Sherman Chow
Chinese University of Hong Kong
2nd Trimester, 2023-24
Lecture 0: Logistics

Contacts

- smchow[at]ie.cuhk.edu.hk
  - Prepend subject of the email with [IEMS5710]
  - Use your institutional email for correspondences
- Office: 808, Ho Sin Hang Engineering Building (SHB)
  - Please make a prior appointment
- Teaching assistant:
  - Yat-Long KEI (kyl022, SHB726)
- http://staff.ie.cuhk.edu.hk/~smchow/5710
- Piazza for online discussion
  - be constructive and friendly
- Blackboard for course material
- Announcement sent via Blackboard to your CUHK mail

Tentative Assessment

- Preparatory "Lab Assignment" (5%)
  - due by the add-drop period / "soon"
- 2 Written Assignments (30%)
- Mid-Term Exam × 1 (25%)
  - open cheat-sheet (1-sided A4)
- Final Exam × 1 (35%)
  - open cheat-sheet (2-sided A4)
- Attendance (5%)
- (Online) Class Participation ?
  - (tiny bonus for top 10% participants?)

Tentative Schedule

Cryptography

1. 6/12: Logistics & Overview
2. 13/12: OTP & Stream Cipher
3. 20/12: Block Cipher
4. 27/12: Hash, Password, MAC
5. 3/ 1: Digital Signatures & RSA
6. 10/ 1: Public-key encryption
7. 17/ 1: [Mid-term Exam], Possibly a Small Special Topic

Information Security and Privacy

8. 24/1: Access Control, KDC vs. PKI
9. 31/1: DNS, Database Security
10. 7/2: Web Security
11. 21/2: General Security Principles & Risk Managements
12. 28/2: Special Topics
13. TBD: [Final Exam]

OTP: **O**ne-**T**ime **P**ad
MAC: **M**essage **A**uthentication **C**ode

KDC: **K**ey-**D**istribution **C**enter
PKI: **P**ublic-Key **I**nfrastructure
DNS: **D**omain **N**ame **S**ever

“Prerequisites”: Mathematically inclined

- No advanced math. background is assumed
- However, “mathematical maturity” is expected
- Knowledge of Basic Logics
  - *e.g.*, logic operators (AND, OR, XOR), inference: *e.g.*, contrapositivity
- Knowledge of Basic (Discrete) Probability
- You should recall/revisit your middle-school (?) math
  - *e.g.*, power arithmetic
- A quick review of Number Theory will be given
  - revisit your primary-school (?) math, *e.g.*, simple modular arithmetic

What you need and what you will learn

- Some hands-on skills to try things out to learn concretely
- Do your assignment/revision early
  - We cover a large number of topics
  - You may not master some of them well

- Expected outcomes:
  1. gain conceptual knowledge in cryptography, security, & privacy
  2. do case studies in contemporary topics in cryptography, security, and privacy, such as security audit, and digital right management
  3. (be interested in the subject!)

Crypto. as a scientific discipline

- Crypto is taught at most major universities
- Received the ultimate seal of approval from the CS community
  - Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, 2002
  - Silvio Micali and Shafi Goldwasser, 2012
- IACR Conferences: *Crypto, EuroCrypt, AsiaCrypt (flagship)*
  - *CHES (Cryptographic Hardware and Embedded Systems)*
  - *FSE (Fast Software Encryption)*
  - *PKC (Public Key Cryptography)*
  - *TCC (Theory of Cryptography Conference)*
- Conferences in Cooperation with IACR: *AfricaCrypt, CANS, Financial Crypt., InsCrypt, LatinCrypt, MyCrypt, Post Quantum, Selected Areas in Crypto, …*
- Others: *ACISP, ACNS, CT-RSA, ECC, ICICS, ICISC, IndoCrypt, ISC, ISPEC, SCN, ProvSec, QCrypt, SCIS, SEC, SEcrypt, WISA, …*

Information Security Certifications

- Intl' Information System Security Certification Consortium, a.k.a. $(ISC)^2$
  - *e.g.*, CISSP
- Intl' 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 Info. Systems Security Professional

1. *Security and Risk Management – 15%*
2. *Asset Security – 10%*
3. *Security Architecture and Engineering – 13%*
4. *Communication and Network Security – 13%*
5. *Identity and Access Management (IAM) – 13%*
6. Security Assessment and Testing – 12%
7. Security Operations – 13%
8. Software Development Security – 11%

Textbooks / References

- The Joy of Cryptography
  - joyofcryptography.com
- Introduction to Modern Cryptography
  - www.cs.umd.edu/~jkatz/imc.html
- Handbook of Applied Cryptography
  - cacr.uwaterloo.ca/hac
- Cryptography and Network Security: *Principles and Practice*
- Computer & Internet Security: *A Hands-on Approach*
- Network Security: *Private Communication in a Public World*
- Counter Hack Reloaded: *A Step-by-Step Guide to Computer Attacks and Effective Defenses*
- Hardly any textbook covering all topics at the "right" level
  - "whatever it takes…" remember?

What this course is *not* about

- How to make your computer "secure"
- How to hack, *e.g.*, crack a password-protected account

- We do not discuss specific crypto software or Internet protocols
  - *e.g.*, HTTPS, SSH, SSL/TLS, IPsec, PGP, Tor, Signal, Bitcoin, BitLocker, …
- What caused the vulnerabilities in TEE (*e.g.*, Intel SGX), *etc*.

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

Class Policy

- Read the textbook
  - the slides, while using the same style and terminology, are meant for teaching but *not* for other purposes, say, revision cram notes
- No plagiarism
  - at the very least, you need paraphrasing
- Work independently
  - discussion is allowed, but write your own solution
- The use of AI: use only with *explicit* acknowledgement
  - departmental policy at the moment, subject to change