정보보호이론
(Information Security Theory)

이 형 태

Spring 2025

Course Overview

- Course Title: 정보보호이론 (Information Security Theory)
- Course No.: 18927
- Class No.: $\begin{cases} 01 \text{ if Tue } 09{:}00 - 10{:}50, \text{ Thu } 10{:}00 - 10{:}50 \\ 02 \text{ if Tue } 11{:}00 - 12{:}50, \text{ Thu } 11{:}00 - 11{:}50 \end{cases}$
- Instructor: 이 형 태 (Hyung Tae Lee)
  (Room 506, Building 208, 02-820-5613, hyungtaelee@cau.ac.kr)
- Office hour: By an appoinment via email
- Lecture Room:
  $\begin{cases} \text{Room 728 (Tue), Room 728 (Thu) in Building 310 if Class No.=01} \\ \text{Room 723 (Tue), Room 728 (Thu) in Building 310 if Class No.=02} \end{cases}$

Textbook

- Textbook: Lecture slides uploaded to the eclass
- References:
  - W. Stallings & L. Brown, Computer security: Principles and practice, 3rd edition, Pearson, 2014.
  - C. Paar & J. Pelzl, Understanding Cryptography, Springer, 2010.
  - Additional materials will be introduced during the class if necessary.

Information Security

- System Security: System management, Access control
- Network Security: DoS, DDoS, Sniffing, Spoofing,...
- Web Security: Web hacking, HTTP, SQL Injection, XSS (Cross-Site Script)
- Code Security: Buffer overflow attack, Format string attack,...
- Malware: Virus, Worm, Trojan horse,...
- Mobile Security: Mobile OS security, IoT security
- Cryptography: Encryption, Signatures, Hash, MAC, Zero-Knowledge proofs...
- Security System: Authentication, Firewall, Intrusion prevention,...
- Electronic Commerce Security: Public key infrastructure, Cryptocurrency, Blockchain
- Digital Forensics

⋮

Tentative Schedule (I)

Week	Subject
1	Course overview Introduction to information security and cryptography
2	Classical encryption algorithms
3	Symmetric encryption I (DES)
4	Symmetric encryption II (AES)
5	Symmetric encryption III (Stream cipher & Modes of operations)
6	Public-key encryption I (RSA)
7	Public-key encryption II (Diffie-Hellman & ElGamal)
8	Mid-term exam

Tentative Schedule (II)

Week	Subject
9	Digital signature & Elliptic curve cryptography
10	Hash function & Message authentication codes
11	User authentication
12	Internet security protocols and authentication applications
13	Zero-knowldege proof
14	Blockchain
15	Mobile security
16	Final exam

Grading

- Follow the policy of Relative Evaluation A (A: $\leq$ 35%, A+B: $\leq$ 70%)
- Midterm: 45%, Final: 45%, Attendance: 10%
  - It may be changed if some assignments are given.
    (e.g., Midterm: 40%, Final: 40%, Assignment: 10%, Attendance: 10%)
- Attendance: (3 latenesses) = (1 absence), (2 absences) = (-1) point
  - Absence from more than 1/4 of all classes $\rightarrow$ F
- **The cases that grades 'F' without any consideration**
  - Absence from any exam
  - Cheating on exams or assignments
  - Absence from more than 1/4 of all classes
  - Attendance-related misconduct such as leaving after attendance or proxy attendance

Important Dates & Homepage

- Exam Dates
  - Mid-term Exam: (**Hopefully**) **April 22** (Thursday) 7pm – 9pm
  - Final Exam: (**Hopefully**) **June 17** (Thursday) 7pm – 9pm
  - **The exam dates may be changed depending on the classroom allocation during the exam period with high probability**.
- Homepage: A board in the eclass (eclass3.cau.ac.kr)
  - All announcements will be posted on the eclass.
  - Please send an email if you have any inquiries because I do not check eclass messages frequently.

Question?

hyungtaelee@cau.ac.kr