Introduction to Software Security

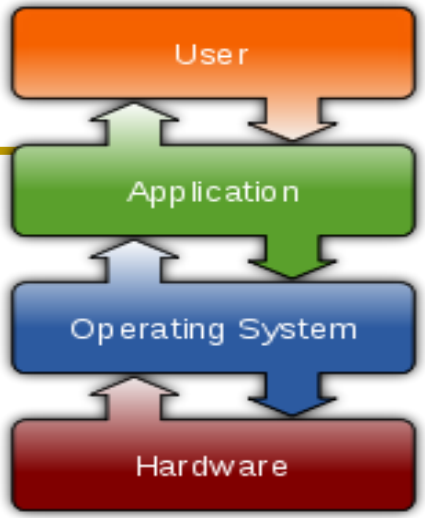
(524660)

Computer Security & OS Lab
Dept. of Software Science, DKU

Cho, Seong-je (조성제)

Spring, 2019

Teaching Team



- **Instructor**
  - **Prof. Cho, Seong-je (조성제 교수)**
    - Room **510**, SW·ICT Building
    - Computer Security & OS Lab.
    - Faculty advisor of the Aegis, Information Security Club
    - Email) sjcho@dankook.ac.kr
    - **Course webpage**
      - » http://SecureSW.dankook.ac.kr
      - » **Lecture notes, Exam schedule, Assignments**

AEGIS

- **TA**
  - **Jaemin Jung (정재민), Minjae Park (박민재)**
    - Room 504 / 505, Media Center Building

    Email) s17orlax@gmail.com, souling4you@gmail.com

Course Overview

- **Course: Introduction to Software Security**
- **Time & Classroom:**
  - **1st Class (1분반)**
    - 10:30-11:45 on Mondays → Room 406, SW·ICT Building
    - 16:00-17:15 on Wednesdays → Room 301, SW·ICT Building
  - **3rd Class (3분반)**
    - 13:00-14:15 on Mondays → Room 303, SW·ICT Building
    - 14:30-15:45 on Wednesdays → Room 509, Media Center
- **Credit: 3 hours/week**
- **Related courses**: Programming, Computer architecture, System programming, OS, Computer network, Other courses for software security track
- **Course webpage:**
  - http://securesw.dankook.ac.kr/ → courses
  - The latest announcement and schedule updates

Target students & Course goal

- **For those who**
  - Are interested in information security, software security track, and
  - Are familiar with programming languages (C, Java, …), basic computer architecture and system programming, Unix/Linux, and
  - Are preparing to investigate more details in selected topics and recent developments in system, networks, and information security including software security track

- **Course Objective (related to Engineering Accreditation 공학 인증)**
  - The Objective of this course: to provide students with comprehensive knowledge of information security.
    1) Understanding of major cybersecurity threats
    2) Understanding the importance of secure coding
    3) Understanding basic malware analysis and reverse engineering

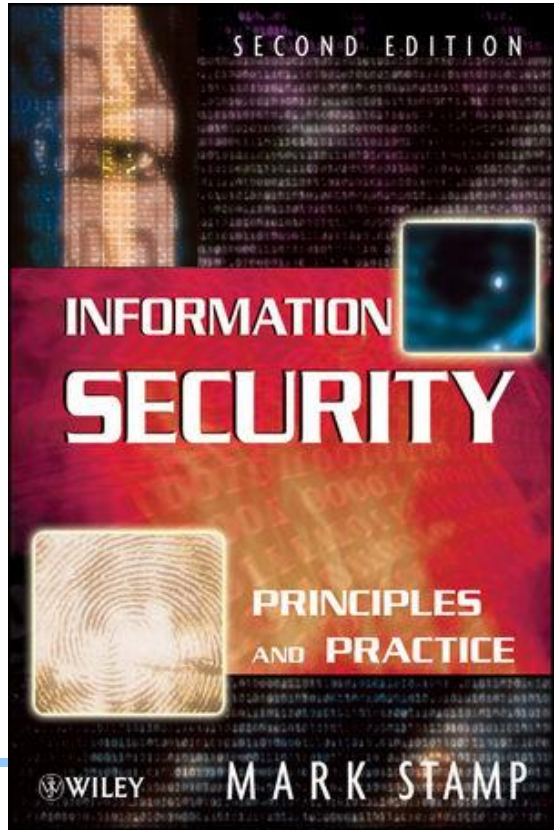
SW 중심대학 (College for SW-centric society)

- **SW Security Track**
  - Introduction to SW Security (SW보안 개론)
  - Secure Coding (시큐어 코딩)
  - Operating System Security (운영체제 보안)
  - Information Security Theory (정보보호 이론)
  - Malicious Code Analysis (악성코드 분석, Malware Analysis)
  - Internet Security (인터넷 보안)

- **Requirement for the SW security track (트랙 이수 조건):**
  - Must complete three or more courses in the track (valid for new freshmen students entering college in 2018)
  - 해당 트랙의 3개 과목 이상 이수 (2018년 입학생부터 졸업장에 명시)

Resources

- **Textbook**
  - ***Information Security: Principles and Practice*, 2nd edition by Mark Stamp, Wiley, 2011**
  - http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470626399,miniSiteCd-BSG.html
  - http://onlinelibrary.wiley.com/book/10.1002/9781118027974
  - It would be better to check if online chapters and appendices are available
- **References:**
  - ***Introduction to Computer Security*** by Michael Goodrich and Roberto Tamassia, Pearson
  - ***Computer Security: Principles and Practice*, 4th Edition** by William Stallings and Lawrie Brown, Pearson, 2017
    - http://williamstallings.com/ComputerSecurity/
  - **Information Security: Principles and Practices, 2nd Edition** by Mark S. Merkow, Jim Breithaupt, Pearson, 2014



Teaching

- **Lectures**
- Experience sharing from previous seniors and the industry
- **About three homework assignments and one term project**
  - Homework should be turned in within two weeks
  - Project should be turned in within four weeks
- **One mid-term exam & One final exam**

- **Homework & Term project: system development or topical surveys**
  - ☞ You must do your homework by yourself. But, For term project, you should perform the term project with your team members after organizing a project team (2~4 members)
  - How can intruders attack our systems?
  - What kinds of security tools are available?
  - How do we protect against attacks?
  - E.g.) Malware analysis, SQL injection, BoF, Format string, Secure coding

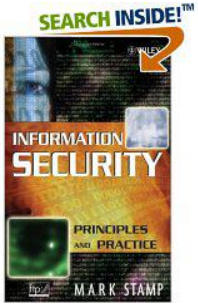
Grading Policy

- Coursework will consist of assignments & project, a midterm exam, and a comprehensive final exam.
- **(Tentative) grading policy:**
  - 35% from the midterm exam
  - 35% from the final exam
  - 20% from assignments/project
  - 10% from attendance and participation
  - Bonus: 10% from presentations & discussions (Technical Reports)
- **"A/B/C/D/F" Grading systems**
  - Grade percentage can be variable
  - Only 10% to 20% of all students may receive grade 'A'
- **No cheating (No make-up tests will be given.)**
- **Some points will be deducted for late homework or project**

Course Description

- Introduction to basic concepts in information security and their applications
  - Background
    - Key concepts, Threat model, Key terms, …
  - Basic Cryptography
    - Encryption, hash function
  - Software & System Security
    - Malware (Virus), Buffer overflow, Integer overflow
    - Overview of secure coding
  - SQL injection
  - Overview of Intrusion and Firewall
  - Network security applications
    - Packet capture, HTTPS, DoS, e-mail security,

Textbook (Table of Contents)



Information Security: Principles and Practice

- **Introduction**
- Chapter 1: Introduction

- **Cryto**
  - Chapter 2: Crypto Basics
  - Chapter 3: Symmetric Key Crypto
  - Chapter 4: Public Key Crypto
  - Chapter 5: Hash Functions and Other Topics
  - Chapter 6: Advanced Cryptanalysis

- **Access Control**
  - Chapter 7: Authentication
  - Chapter 8: Authorization

- **Protocol**
  - Chapter 9: Simple Authentication Protocols
  - Chapter 10: Real-World Security Protocols

- **Software**
  - Chapter 11: Software Flaws and Malware
  - Chapter 12: Insecurity in Software
  - Chapter 13: Operating Systems and Security

(Tentative) Schedule : Plan of the textbook

- Introduction/Background (Ch. 1-2) : 2-3 wks
- Cryptography : 3-4 wks
  - Symmetric Key Crypto (Ch. 3)
  - Public Key Crypto (Ch. 4)
  - Cryptographic Hash Functions (Ch. 5)
  - Advanced Cryptanalysis (Ch. 6)
- Access Control : 1 wks
  - Password, Authentication (Ch. 7), Authorization (Ch. 8)
- Protocol and Internet Security : 2-3 wks
  - Packet capture, Firewall, SQL injection, HTTPs
  - Simple Authentication Protocols (Ch. 9), Real-World Security Protocols (Ch. 10)
- Software (Ch. 11-13) : 3-4 wks
  - Software Flaws and Malware (Ch. 11)
  - Insecurity in Software (Ch. 12), Secure coding overview
  - OSs and Security (Ch. 13)
- Term project presentation: 1-2 wks

Course Schedule *(tentative)*

W	Contents	W	Contents
1	Introduction / Key concepts	8	Symmetric Key Crypto (AES)
2	Threat modeling	9	Cryptographic Hash Function
3	Defense techniques / Software Flaws(1)	10	Packet capture, HTTP/HTTPS & Telnet/ssh, Firewall
4	Software Flaws(2) / Secure coding overview	11	Public Key Crypto (Diffie-Hellman)
5	Malware	12	User authentication (password)
6	Malware detection (Reversing)	13	DoS, SQL injection
7	Review/Mid term Exam.	14	Review/Final Exam.
		15	Presentation (Term project, …)

The class also offers hands-on experience using open source software by TA.
(E.g., Webgoat, Tripwire, gdb)

Outline & Schedule (Cont')

- **Due to the time limits, we will try to cover most of the major topics without going into too much detail**
  - E.g.:
    - Mathematical parts such as number theory and finite fields (Ch.2 & Ch.5)
    - Theoretical parts in cryptography
    - Details of information security standards, protocols, RFCs
  - A broad overview, and then focus on selected topics in depth

- **Notice:** March 13, Major conference/meeting
  → TA (Assignment introduction), Special lecturer invitation (특강)

- **Mid-term exam: April 17 or 22, 2019**
- **Final exam: June 10 or 12, 2019**
  - **If the exam date is changed, notify it on the course web site.**

Additional Resources

- **Online resources at Pearson and by Stallings**
  - **Useful Websites and documents**
  - **Online chapters (if available)**

- **Glossary (Terms) through Google search**
  - NISTIR 7298 Revision 2 (Glossary of Key Information Security Terms), NIST
  - NICCS Glossary (Explore Terms: A Glossary of Common Cybersecurity Terminology)

- **SEED labs**
  - **Hands-on Labs for Security Education**
  - **http://www.cis.syr.edu/~wedu/seed/index.html**
  - **SEED: A Suite of Instructional Laboratories for Computer SEcurity EDucation**

- **Review questions, problems, and programming problems (at the end of each chapter)**

More on Assignments & Term Project

- **Vulnerability analysis, Malware analysis, or System development using security libraries**
  - Software Vulnerability Analysis & Secure Coding
  - Malware Analysis ← Term project
  - Packet capture, Web security (SQL injection)
  - Implementation of security algorithms (AES, RSA, …)

- **Topical surveys in information security-related topics, e.g.:**
  - Demonstration on how to use a security tool to defend against recent attacks
  - Analysis of potential security weakness in systems, and possible solutions or countermeasures
  - Focused survey on the latest technical developments in security
    - **Specific issues in mobile security, cloud security & privacy, big data security, …**

- **Late homework:** ≥48 hours: no credit
- **Focus on the quality and technical depth of your presentation**

Example of Term Project - Tentative Plan

- **Team-based malware analysis**
  - **Android malware analysis (Aidra worm/botnet analysis in 2018)**
- **Proposal: required before midterm (Due: April 10, 2019)**
  - Two-page description of your planning for term project, and responsibilities of your team members
  - More details to be announced in class
- **Final report: (Due: May 15, 2019)**
  - **Presentation files, documentation, …**
  - Late project: <24 hours: -10%, <48 hours: -20%, <72 hours: -40%, ≥72 hours: no credit
- **Presentation: Optional but Encourage it**
  - You can present your research/result from May 20 to June 19, 2018

Hint

- **Keys to success: Do the homework and attend class**
- **Cheating will not be tolerated...**
  - Never share solutions, code, etc. or let other students see them.
  - Work on your own unless it is a group assignment
- **It's better not to use our slides to answer questions during class**
- **...but working together is encouraged**
- **Student must be respectful of the teacher and other students; for example**
  - No chatting or talking
  - Turn off cell phones
  - Class begins on time
  - Class is not over until I say it's over

How to become an information security expert ...

Most security professionals come out of computer science and engineering programs. It's really important to have a solid, well-rounded IT background. Fields you should specifically explore in your studies include networking, OS, architecture, compiler, databases and application development.

Every effort makes the next effort easier and more enjoyable

Attention! Any questions?

- Do not try attacks at home or school!
- Our goal is to learn about information security