

# Introduction to Software Security

(524660)

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

Cho, Seong-je (조성제)

Spring, 2018

Many photos/pictures in presentation licensed from textbook, google images or Wikipedia.

Thus, please do not duplicate or distribute this in whole or in part

# Teaching Team

## ● Instructor

### ■ Prof. Cho, Seong-je (조성제 교수)

- Room 511, Natural Science Hall
- Computer Security & OS Lab.
- Faculty advisor of the Aegis, Information Security Club
- Email) sjcho@dankook.ac.kr
- Course webpage

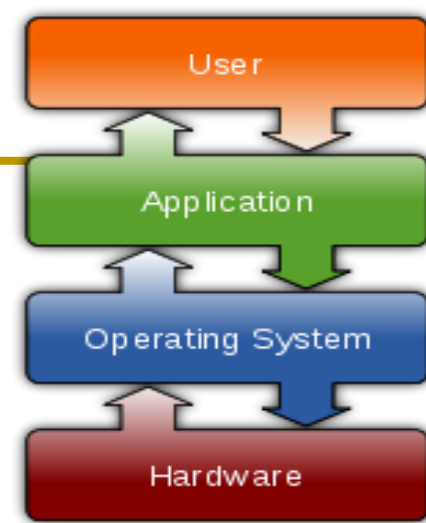
» <http://SecureSW.dankook.ac.kr>

» **Lecture notes, Exam schedule, Assignments**

## ● TA

### ■ Jaewoo Shim (심재우)

- Room 505, Media center building
- tlawodn94@gmail.com



# Course Overview

---

- **Course: Introduction to Software Security**
- **Time: 4:00-5:15 pm on Mondays and Wednesdays**
- **Classroom: R 517, SW-ICT Building**
- **Credit: 3 hours/week**
- **Related courses: Programming, Computer architecture, System programming, OS, Computer network, Other courses for software security track**
- **Course webpage:**
  - <http://seuresw.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 (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 security 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)

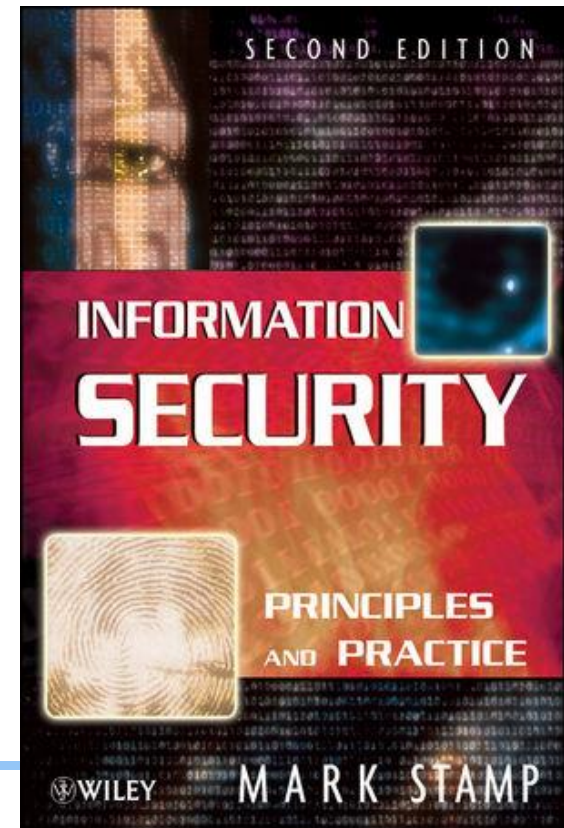
# Resources

## ● Textbook

- *Information Security: Principles and Practice*, 2<sup>nd</sup> 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*, 4<sup>th</sup> 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, after project team organization, you should perform the term project with your team members
  - How did 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

---

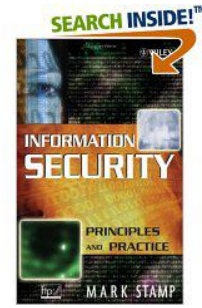
- Coursework will consist of assignments & project, a midterm exam, and a comprehensive final exam.
- (Tentative) grading policy:
  - 30% from the midterm exam
  - 30% from the final exam
  - 20% from assignments/project
  - 10% from presentations & discussions (Technical Reports)
  - 10% from attendance and participation
- “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

- **Crypto**

- 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**
- **Mid-term exam: April 18 or 23, 2018**
  - **Notice:** Overseas business trip from April 8 to 14.
    - Special guest lecture (대강), or Supplementary lesson (보강)
- **Final exam: June 15, 2018**
  - **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)
- **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**



# More on Term Project

---

- **Team-based malware analysis**
  - Aidra worm (Aidra botnet) analysis
- **Proposal: required before midterm (Due: April 4, 2018)**
  - 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 2, 2018)**
  - 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 result from May 16 to June 20, 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 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**



# Any questions?

---

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

