Operating Systems Security

(524870)

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

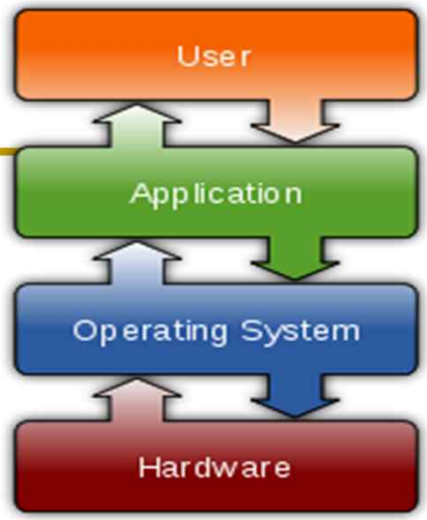
Cho, Seong-je (조성제)

Fall, 2018

sjcho at dankook.ac.kr

DKU
DANKOOK UNIVERSITY

Teaching Team



- **Instructor**
  - Prof. Cho, Seong-je (조성제 교수)
    - Room 510, SW·ICT Hall
    - Computer Security & OS Lab.

      Dept. of Software Science, Dankook Univ.
    - Faculty advisor of the Aegis, Information Security Club
    - Email) sjcho at dankook.ac.kr
    - http://SecureSW.dankook.ac.kr
      - » Lecture notes, Exam schedule, Assignments

- **TA**
  - Jaemin Jung & Minjae Park (정재민 & 박민재)
    - Room 504/505, Media center building

What is Operating Systems?

What is Computer Security?
Which types of threats are there?

What is Computer Security?

- Allow intended use of computer systems
- Prevent unintended use that may cause harm
- Protect information and systems from security threats
  - Protect computing resources and system assets from security threats

※ Security threats: STRIDE

Operating Systems & Security

- **Threats / Attacks**
  - Password cracking for root ID
  - Bootkit, Rootkit, keylogger, backdoor, …
  - Privilege Escalation Attacks (User → Super user)
    - Buffer overflows, Frame Pointer overwrite attack, Ret2Libc, ROP
    - Android rooting, iOS jailbreaking
  - Race condition vulnerabilities
  - DLL injection, GOT overwrite, …

- **Defenses**
  - Secure boot, Measured boot, …
  - Stack Guard (Canary), Stack Shield, NX bit, DEP, PAX/ExecShield, ASLR
  - SELinux/SEAndroid, AppArmor, SMACK, TOMOYO, grsecurity, …
  - Sandbox, Trusted Execution Environment (TEE), Secure OS, …
  - Audit log, Computer forensics, …

What is This Class About?

Learn About Security

Make a Difference

Topics Covered in Intro to SW Security, Spring Semester, 2018

- Basic security threats and properties
  - Microsoft STRIDE vs. CIA Triad
- Primary concepts for Cryptography
  - Symmetric Cryptography vs. Public-key Cryptography
  - Cryptographic Hash Functions
- C secure coding overview
  - BoF overview, Integer overflow, Format string overview
- Malware analysis, Reverse Engineering
- Web Security: SQL injection

- Malware
  - Backdoor, Logic bomb, Viruses, Worms

- Network security basics
  - Sniffing, Spoofing, Firewall, DDoS attacks

Possible Topics Covered in Class of this Semester

- Basic system security attacks and defense
  - Authentication, Password cracking, Logging
  - Buffer overflow, Ret2Libc, ROP ↔ Stack canary, LibSafe, ASLR, Guard page
    - Privilege escalation, Code injection attacks, Code reuse attacks
    - Control flow hijacking ↔ Control flow integrity (CFI)
- Linux Security Framework / Access Control
  - Access control (DAC/MAC/RBAC)
    - Multilevel Security (MLS), Type Enforcement (TE)
  - SELinux, SMACK, AppArmor, grsecurity, …
- Malware / Rooting
  - Keylogger, Backdoor, Rootkits
  - Android rooting
- Other OS security
  - Command injection, DLL injection, Hooking
  - Race condition, PLT/GOT overwrite
  - Sandbox, Virtualization

Course Format

- Lecture: 15 weeks (including midterm/final exam)
  - Lecture + Practical exercise (roughly 70:30)
  - Midterm exam: Oct. 30 or Nov. 5
    Final exam: Dec. 11 ~ Dec. 17
- Students can get extra credit (or bonus points)
  - Presentation about recent security issues
    - E.g.: Android/iOS Security, Tizen Security, …
  - Reporting after a field trip to an expo
  - Technical report including hands-on experience (practical exercises) in current systems

Assignments and Labs

- Tentative plan
  - Two types of homework
    - 2~4 Labs + Team-based term project
- Usually 2-3 weeks long

- Lab & Team-based term project
  - Lab environment: TOAST Cloud, or Linux
  - Term project: will be done in groups of 3~4 (Pick partners soon!)

- Expected Assignment/Lab
  - PLT/GOT overwrite, ROP, DLL injection
  - Android malware analysis (Reverse engineering)
  - Rootkit (Hooking), Rooting detection, Network security
  - Comparison of SELinux, AppArmor, and SMACK

Grading

- Coursework will consist of homeworks and a midterm exam, and a comprehensive final exam.
- The overall grade will be determined as follows:
  - 35% from the midterm exam
  - 35% from the final exam
  - 10% from assignments
  - 10% from lab, 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'

Cheating policy

- Performance must be 100% individual effort on all exams, that is, no collaboration is allowed on exams. Any collaboration or copying will be considered cheating.
- Group work on lab is permitted, but each student must list his or her collaborators in writing for each problem, using a phrase like "In collaboration with *Gildong Hong*...". If a student turns in a solution without listing the others who helped produce this solution, this act will be considered cheating (for it is plagiarism).
- Late homework assignments will not be accepted without a medical or other life-emergency excuse.
- Students caught cheating will be given a zero on the homework or exam in question and have a letter filed with their associate dean for academic affairs.

Cheating policy & Course Requirements

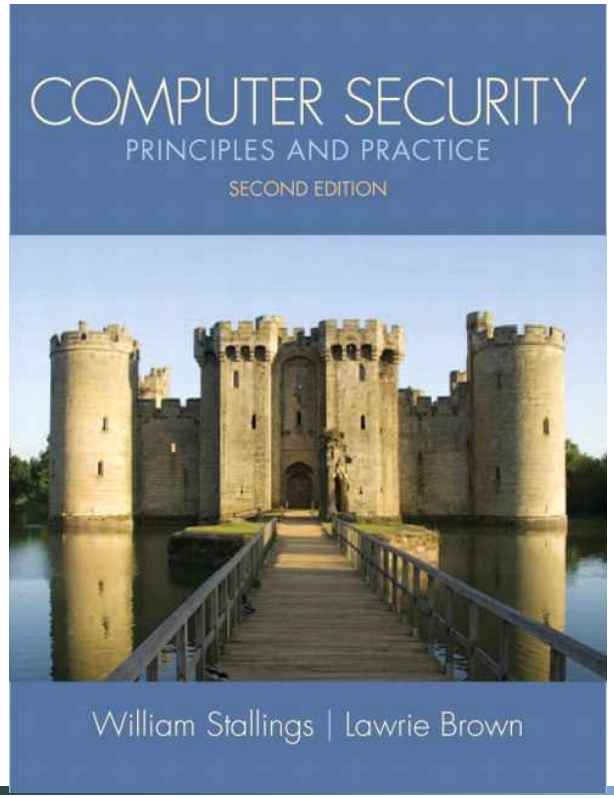
- No cheating
  - What is cheating?
    - Sharing code: either by copying, retyping, looking at, or supplying a copy of a file.
  - What is NOT cheating?
    - Helping others use systems or tools.
    - Helping others with high-level design issues.
    - Helping others debug their code.
  - Penalty for cheating: F grade

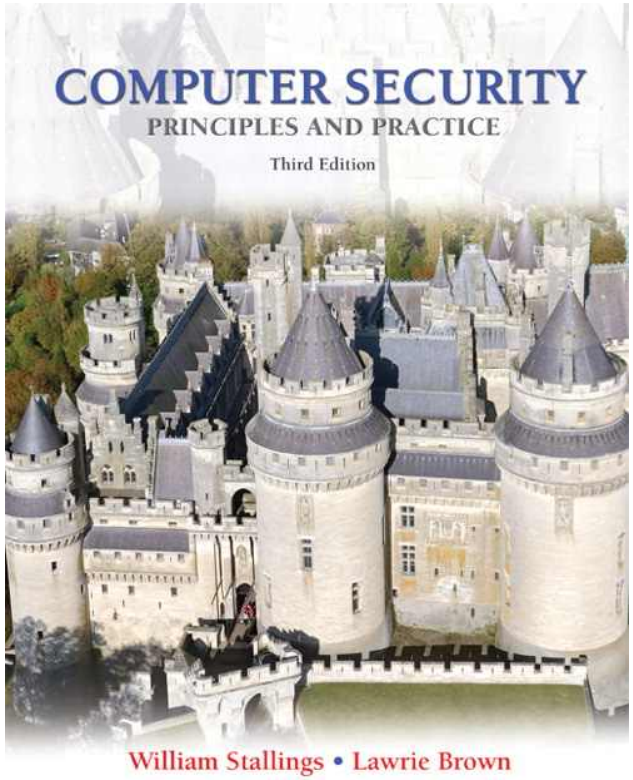
- Active class participation
  - Question
  - Presentation & Discussion
  - Feedback

- Read newspapers including "보안뉴스" (http://www.boannews.com/)

Textbook

- William Stallings and Lawrie Brown, *Computer Security: Principles and Practice*, 2/E or 3/E, Prentice Hall, 2011/2014, Pearson' International Edition
  - http://williamstallings.com/ComputerSecurity/
  - http://www.pearsonhighered.com/educator/academic/product/1,,0132775069,00.html
  - http://www.pearsonhighered.com/educator/product/Computer-Security-Principles-and-Practice/9780133773927.page





Contents of Text

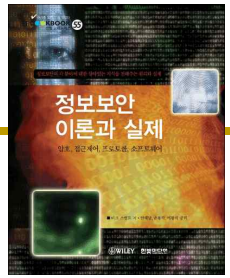
Tentative Schedule *(subject to change)*

- Week 1: Course introduction, Threats, Overview of OS & Security
- Week 2: User authentication, Password cracking
- Week 3: Buffer overflow, Privilege Escalation, BoF exercise
  - Stack overflow / Heap overflow / Data overflow
- Week 4: Buffer overflow attack, BoF exercise
- Week 5: Defense of BoF attacks: *ASLR, Guard page,* Ret2Libc, PLT/GOT overwrite
- Week 6: Race conditions, Return Oriented Programming (ROP)
- Week 7: Defenses against control flow hijacking, Examples for term project
- Week 8: Midterm exam
- Week 9: Access control: DAC, SetUID program, RUID/EUID
- Week 10: Access control: MAC, Privilege escalation, SELinux overview
- Week 11: Access control: RBAC, SELinux TE & RBAC & MLS
- Week 12: Malware (Keylogger, Backdoor)
- Week 13: Malware (Rootkit, …), Rooting, Practical exercise for malware
- Week 14: Injection (Command, DLL), Trusted OS, Presentation
- Week 15: Final exam, Presentation

Tentative schedule

Week	Lecture	Hands-on Exercise(s)
1	Introduction	Password cracking
2	User authentication	
3	Buffer Overflow (BoF)	LoB (Lord of Buffer overflow)
4	Buffer overflow attacks	
5	Defense for Buffer overflow, Ret2Libc	PLT/GOT overwrite
6	Race condition & ROP	Race condition or ROP
7	Defenses against control flow hijacking	
8	Mid-term exam	
9	Discretionary Access Control (DAC)	SELinux (basic commands, user addition, policy insertion & change)
10	Mandatory Access Control (MAC)	
11	Role-based Access Control (RBAC)	
12	Malware (keylogger, Backdoor)	
13	Malware (Rootkit), Android rooting	TiwelRoot v3.0 APK
14	Injection, Smartphone security issues	Android library injection
15	Final exam	

Reference 1 (Table of Contents)



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
- You can find out online chapters and appendices are available

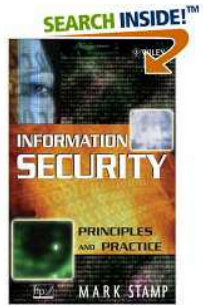
- **Introduction**
- Chapter 1: Introduction

- **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

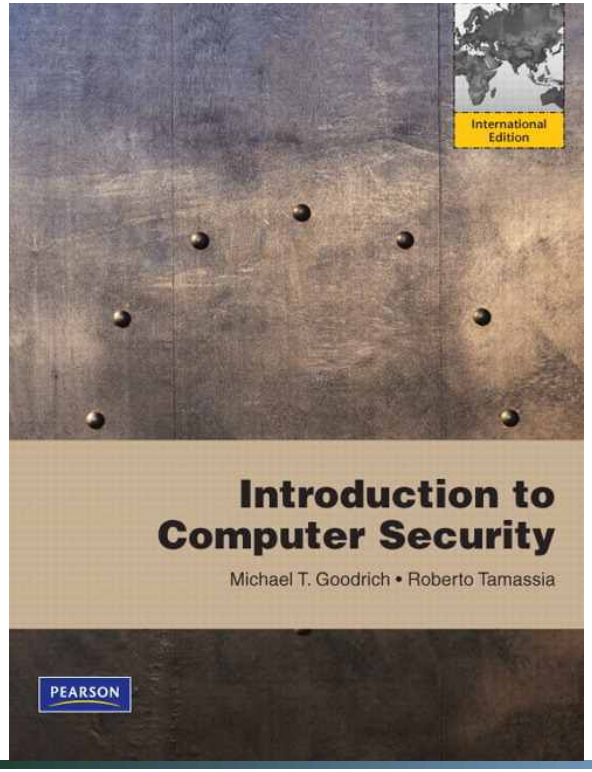
- **Protocol**
  - Chapter 9: Simple Authentication Protocols
  - Chapter 10: Real-World Security Protocols

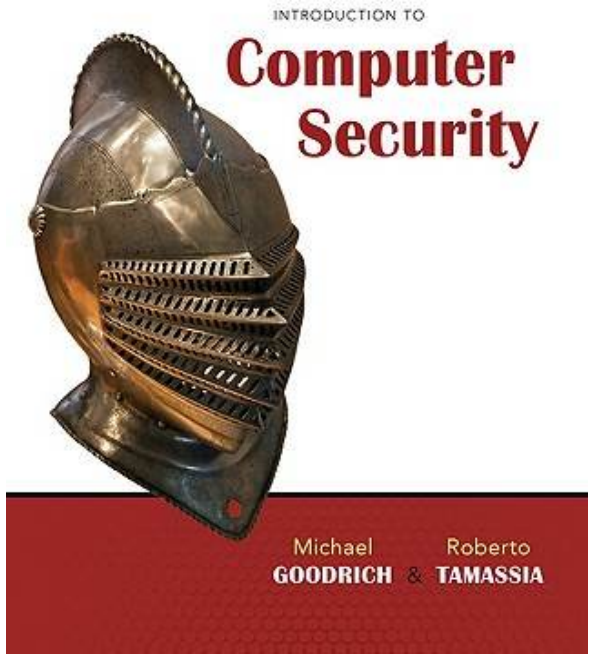
- **Software**
  - Chapter 11: Software Flaws and Malware
  - Chapter 12: Insecurity in Software
  - Chapter 13: Operating Systems and Security



Reference 2

- M.T. Goodrich and R. Tamassia, *Introduction to Computer Security*, Pearson' International Edition (Addison-Wesley), 2011
  - http://www.securitybook.net/
  - http://www.ics.uci.edu/~goodrich/teach/ics8/syll.html
  - http://www.pearsonhighered.com/educator/product/Introduction-to-Computer-Security/0321512944.page



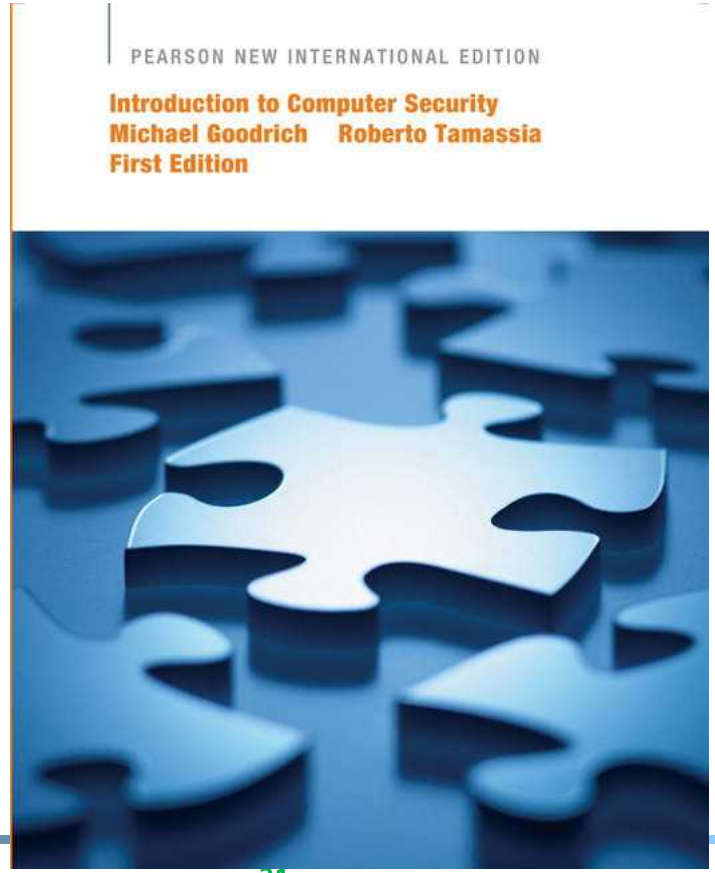


Contents of Textbook

	International Edition	Original Edition
Chap.1:	Introduction	Introduction
Chap.2:	Cryptography	Physical Security
Chap.3:	Operating Systems Security	Operating Systems Security
Chap.4:	Malicious Software	Malware
Chap.5:	Network Security I	Network Security I
Chap.6:	Network Security II	Network Security II
Chap.7:	Browser Security	Web Security
Chap.8:	Physical Security	Cryptography
Chap.9:	Security Models and Practice	Security Models and Practice
Chap.10:	Application Security	Distributed Application Security

Reference 3

- **M.T. Goodrich and R. Tamassia, *Introduction to Computer Security* : Pearson New International Edition (Addison-Wesley), 2013**
  - http://catalogue.pearsoned.co.uk/educator/product/Introduction-to-Computer-Security-Pearson-New-International-Edition/9781292025407.page
  - ISBN-10: 1292025409 • ISBN-13: 9781292025407



Other References

- crackmes.de - A great site for testing your reversing skills. Crackmes range from Very Easy to Very Hard [1-9] for many Operating systems !
  - Reverser's playground: www.crackmes.de

- tdhack.com - a lot of challenges including cryptographic riddles, hackmes and software applications to crack for both Windows and Linux. Polish and English languages are supported.
  - Hacking, cracking, wargames, cryptography

- **Lord of the Root**
  - **https://www.vulnhub.com/entry/lord-of-the-root-101,129/**
  - **https://www.vulnhub.com/** **https://research.g0blin.co.uk/lord-of-the-root-vulnhub-writeup/**

- **양대일, 정보보안 개론과 실습: 시스템 해킹과 보안(개정판), 한빛미디어, 2011 http://hack.pe.kr/321**

Notice / Notification

- Be careful that only the attendee can download the lecture notes
  - Copyright of all lecture notes should be protected
- Please do not distribute/upload the lecture notes (PDF slides) via the Internet, blog, usb, email, …
  - We are strictly prohibited from distributing the PPT/PDF slides written by the authors of textbooks

Everyone is invited, regardless of skill

Contact: Cho, Seong-je <sjcho at dankook.ac.kr>

or

Visit: http://securesw.dankook.ac.kr

We need great diligence and effort.

Every effort makes the next effort easier and more enjoyable

A Key Comment

- Do not try attacks at home or school!
- Our goal is to educate so you can defend, not attack

Summary

- Prerequisites
  - C language, Computer architecture
  - System programming (Debugging)
- Related courses
  - Introduction to SW Security
  - Introduction to operating systems, Computer networks
- http://securesw.dankook.ac.kr

Any questions?

- Hardships, The way of suffering
  - Diligence, An unremitting effort, Sincerity, Passion

- Expert, Specialist

- Black hat vs. White hat