Operating Systems & Security

(478550)

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

Cho, Seong-je (조성제)

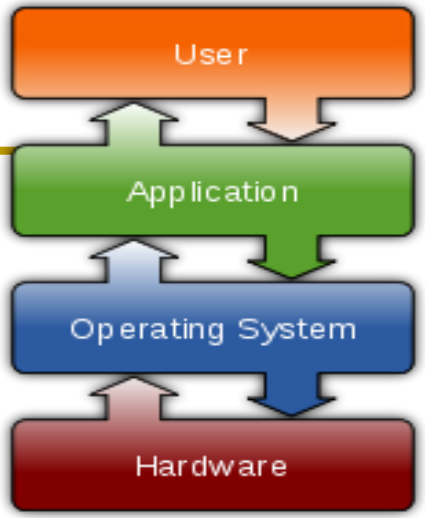
Fall, 2015

sjcho at dankook.ac.kr

DKU
DANKOOK UNIVERSITY

Many photos/pictures in presentation licensed from google images or wikipedia

Teaching Team



- **Instructor**
  - Prof. Cho, Seong-je (조성제 교수)
    - Room 511, Natural Science Hall
    - Computer Security & OS Lab.

      Dept. of Computer 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

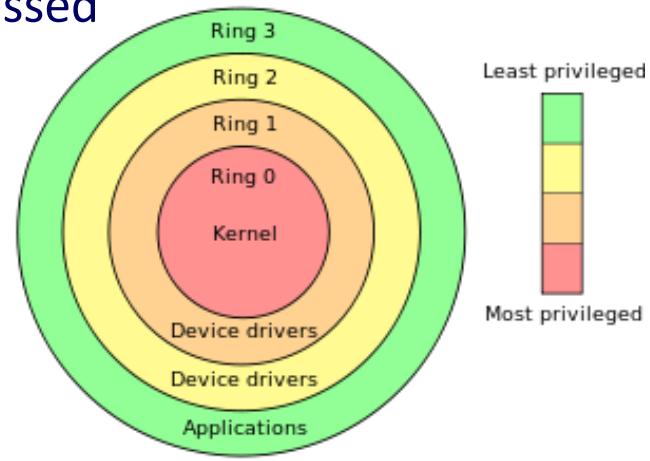
- **TA**
  - Kyeonghwan Lim and Nak-young Kim (임경환 & 김낙영)
    - Room 504/502, Media center building

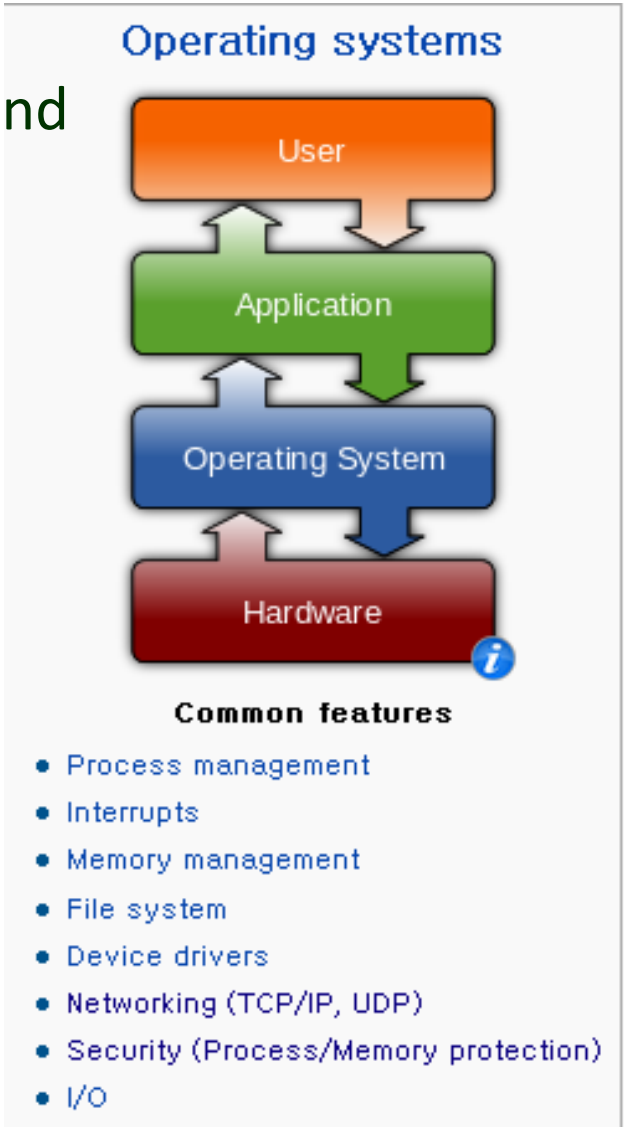
What is Operating Systems?

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

Operating Systems

- a collection of software that manages computer hardware **resources** and provides common services for computer programs
  - Kernel provides the most basic level of control over all of the computer's hardware devices
  - OS must be capable of distinguishing between requests which should be allowed to be processed, and others which should not be processed





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

What is This Class About?

Learn About Security

Make a Difference

Topics Covered in Class of Spring Semester, 2015

- 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
- Web Security: SQL injection, XSS, …
- Network security basics
  - Sniffing, Spoofing, Firewall, DDoS attacks
- Malware
  - Backdoor, Logic bomb, Viruses, Worms
  - Reverse engineering (Reversing)

Topics Covered in Class of this Semester

- **Basic system security attacks and defense**
  - Authentication, Access control (DAC/MAC), Logging
  - Buffer overflow, Ret2Libc ↔ Stack canary, ASLR, Libsafe
  - Privilege escalation
- **Malware**
  - Reverse engineering (Reversing)
  - Keylogger, Backdoor, Rootkits
- **OS security**
  - Command injection, DLL injection, Hooking
  - Password cracking
  - Multilevel security (MLS), Virtualization
- **Linux Security Framework**
  - SELinux, SMACK, AppArmor, grsecurity, …

Course Format

- Lecture: 15 weeks (including midterm/final exam)
  - Lecture + Practical exercise (roughly 60:40)
  - Midterm exam: Oct. 27 or Nov. 02
    Final exam: Dec. 16
- Students can get extra credit (or bonus points)
  - Presentation about recent security issues
    - E.g.: Android/iOS Security, SNS 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
    - Several Labs + Team-based term project
- Usually 2-3 weeks long
- Lab
  - Done in groups of 3~4 (Pick partners soon!)
- Expected Assignment/Lab
  - Buffer overflow, Ret2Libc, DLL injection
  - Malware analysis (Reversing), Android malware analysis
  - Rootkit (Hooking), Network security

Grading

- Coursework will consist of homeworks and a midterm exam, and a comprehensive final exam.
- The overall grade will be determined as follows:
  - 30% from the midterm exam
  - 30% from the final exam
  - 10% from assignments
  - 20% 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 plagarism).
- 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

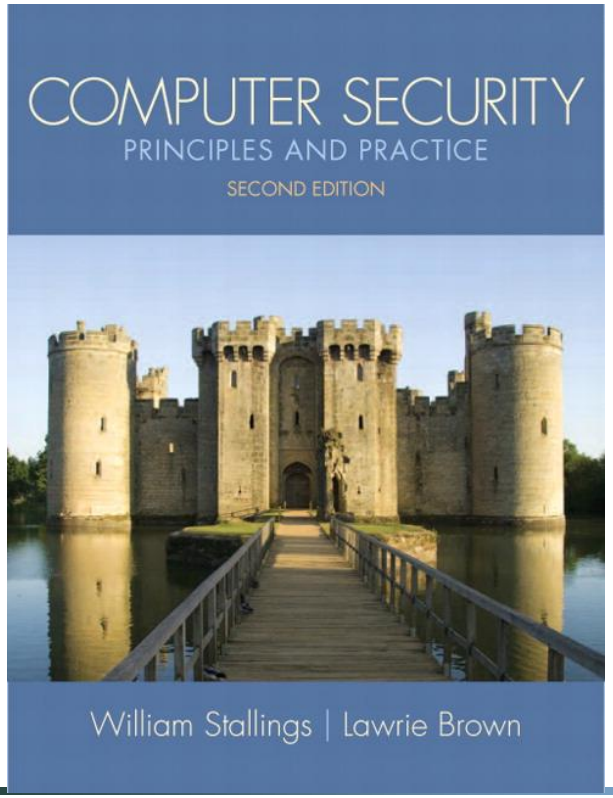
- No cheating
  - What is cheating?
    - Sharing code: either by copying, retyping, looking at, or supplying a copy of a file.
  - What is NOT cheating?
    - Helping others use systems or tools.
    - Helping others with high-level design issues.
    - Helping others debug their code.
  - Penalty for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

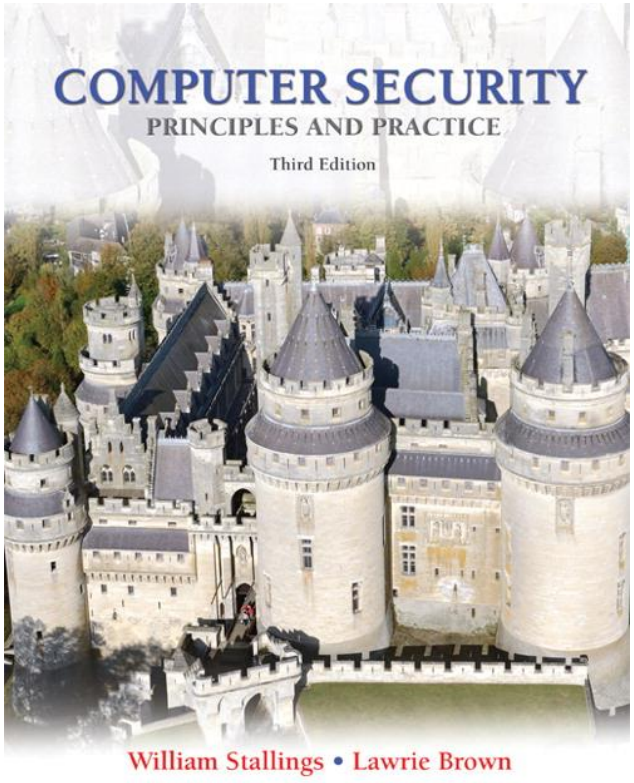
- Active class participation
  - Question
  - Presentation & Discussion
  - Feedback

- 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
- Week 2: Overview of (OS + security)
- Week 3: User authentication, /etc/{passwd, shadow}, Password cracking
- Week 4: Access control: DAC, SetUID program, RUID/EUID
- Week 5: Access control: MAC, Privilege escalation, SELinux overview
- Week 6: Access control: RBAC, SELinux TE & RBAC & MLS
- Week 7: Comparison of SELinux, AppArmor, and SMACK
- Week 8: Midterm exam
- Week 9: Malware (Keylogger, Backdoor)
- Week 10: Malware (Rootkit, …), Practical exercise for malware
- Week 11: Buffer overflow attack, BoF exercise
- Week 12: Defense of BoF attacks: *ASLR, Guard page, LibSafe*, Ret2Libc
- Week 13: Race conditions, Return Oriented Programming (ROP)
- Week 14: Injection (Command, DLL), Trusted OS, Presentation
- Week 15: Final exam, Presentation

Tentative schedule

Week	Lecture	Hands-on Exercise(s)
1	Introduction	OWASP Top 10 WebGoat
2	**Overview of (OS + security)**	
3	User authentication	Password cracking
4	Discretionary Access Control (DAC)	SELinux (basic commands, user addition, policy insertion & change)
5	Mandatory Access Control (MAC)	
6	Role-based Access Control (RBAC)	SMACK (basic commands, policy insertion & change)
7	Comparison of SELinux, AppArmor, SMACK	
8	Mid-term exam	
9	Malware (keylogger, Backdoor)	Rootkit & Its defense
10	Malware (Rootkit)	
11	Buffer overflow attacks	Buffer Overflow
12	Defense for Buffer overflow, Ret2Libc	
13	Race condition & ROP	Race condition or ROP
14	Injection, Smartphone security issues	Android library injection
15	Final exam	

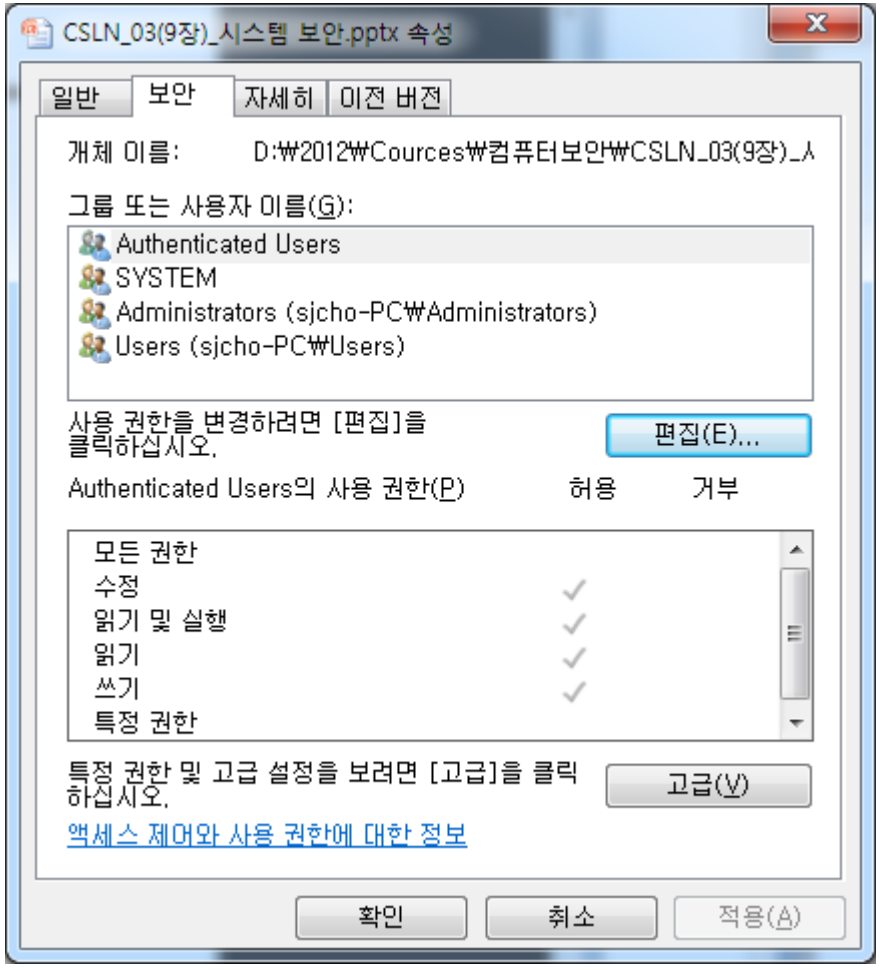
OS Security Example: File Permissions

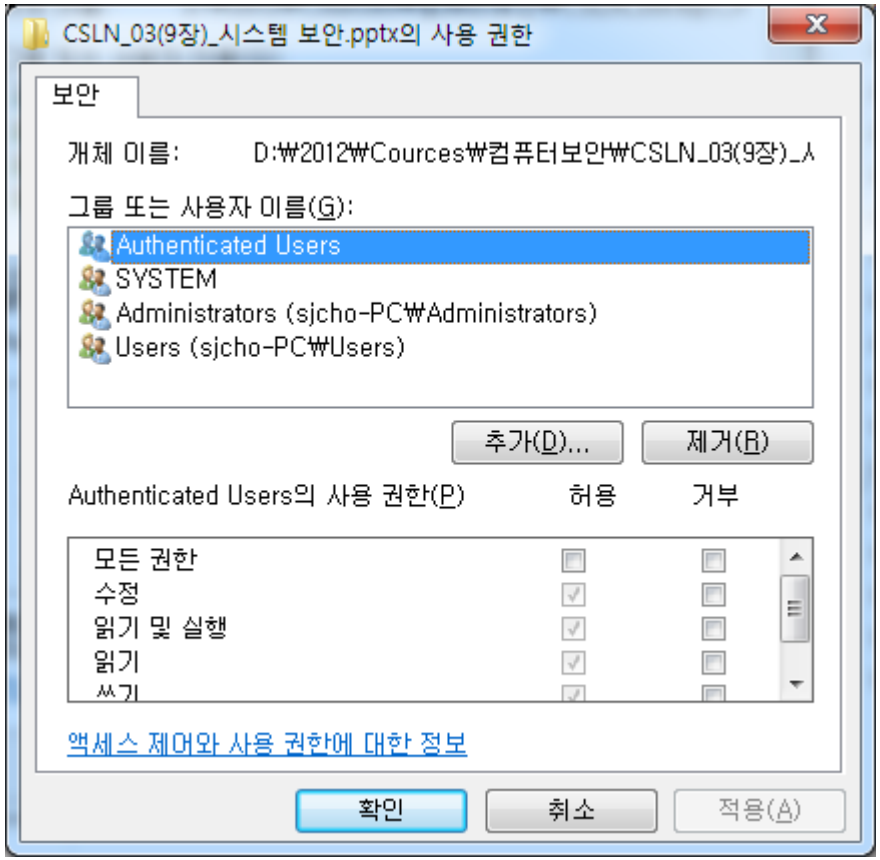
- **File permissions (Authorization)**
  - **Readable/Writeable/eXecutable by a user or group of users**
- **In Unix-like OS's, a file permission matrix shows who is allowed to do what to the file.**
  - **Files have owner permissions, which show what the owner can do, and group permissions, which show what some group id can do, and world permissions, which give default access rights.**

-rw-rw-r--	1 pbg	staff	31200	Sep 3 08:30	intro.ps
drwx------	5 pbg	staff	512	Jul 8 09.33	private/
drwxrwxr-x	2 pbg	staff	512	Jul 8 09:35	doc/
drwxrwx---	2 pbg	student	512	Aug 3 14:13	student-proj/
-rw-r--r--	1 pbg	staff	9423	Feb 24 2003	program.c
-rwxr-xr-x	1 pbg	staff	20471	Feb 24 2003	program
drwx--x--x	4 pbg	faculty	512	Jul 31 10:31	lib/
drwx------	3 pbg	staff	1024	Aug 29 06:52	mail/
drwxrwxrwx	3 pbg	staff	512	Jul 8 09:35	test/

OS Security Example: File Permissions

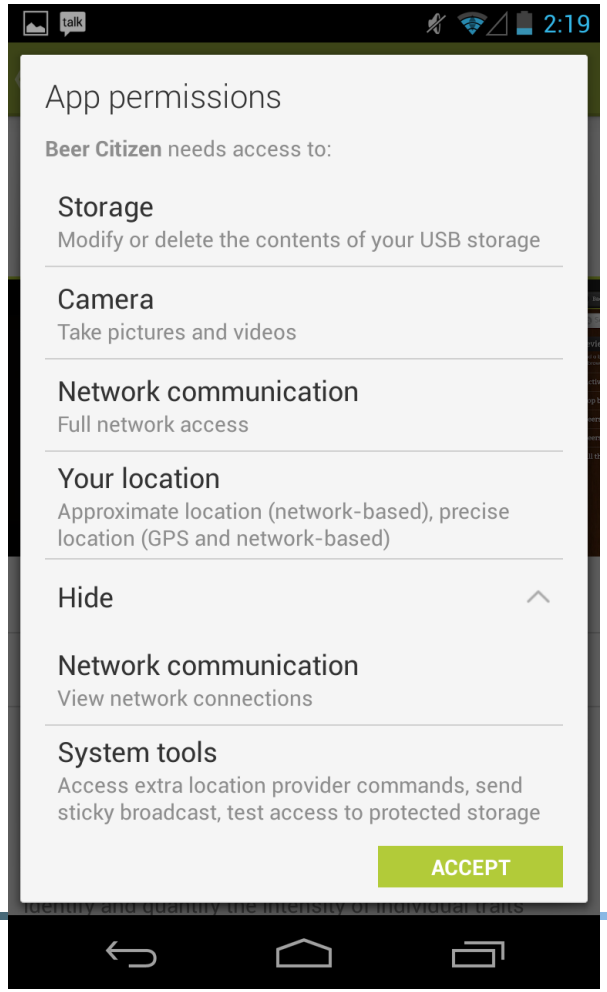
- **Authorization on Windows 7**

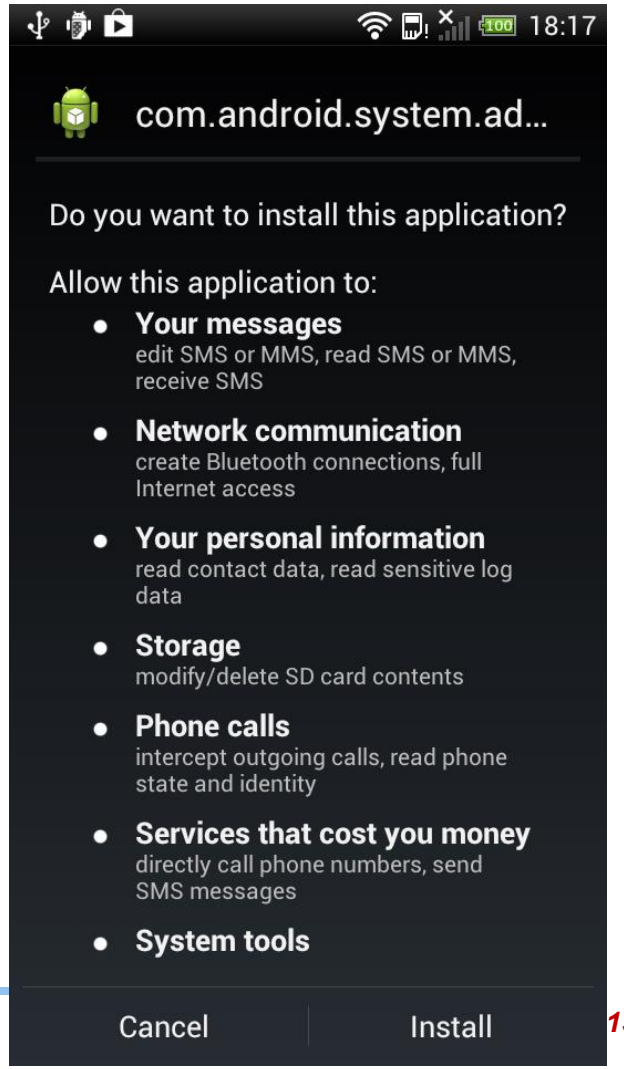




OS Security Example: File Permissions

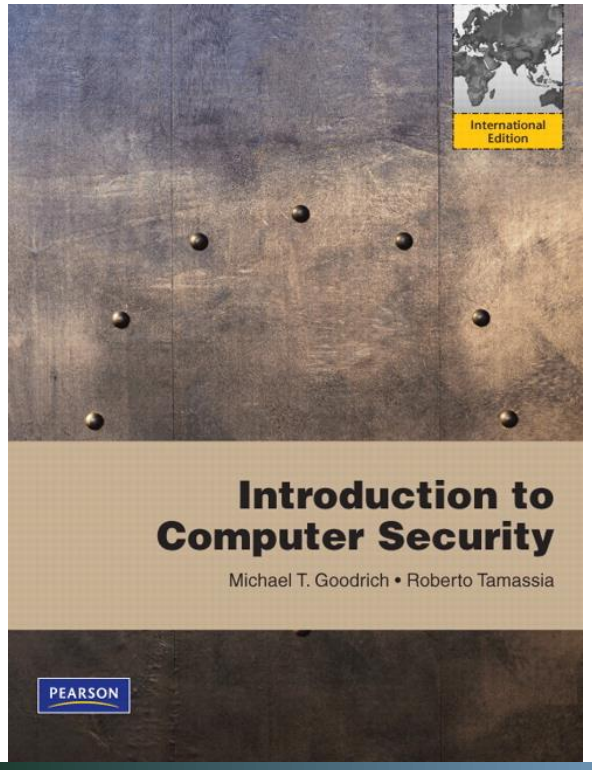
- Android 2.2는 134개의 permission을 정의
  - Such as dialing (CALL_PHONE), taking pictures (CAMERA)
- Ask which permissions is accepted at install time

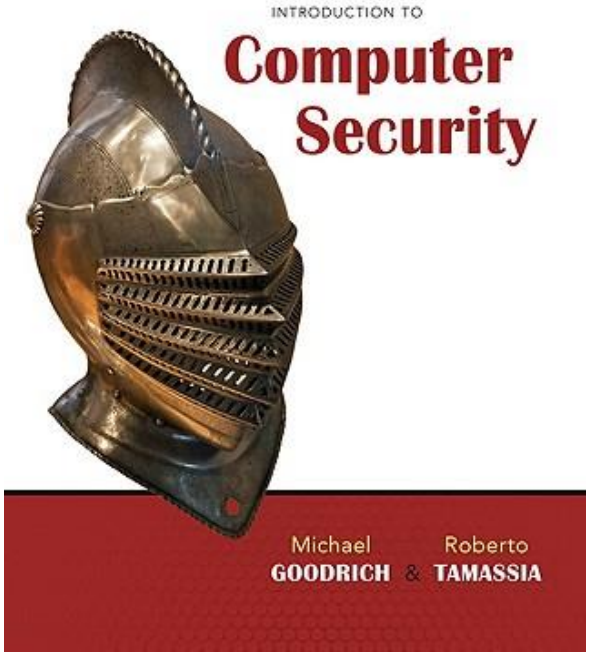




Auxiliary Textbook

- 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



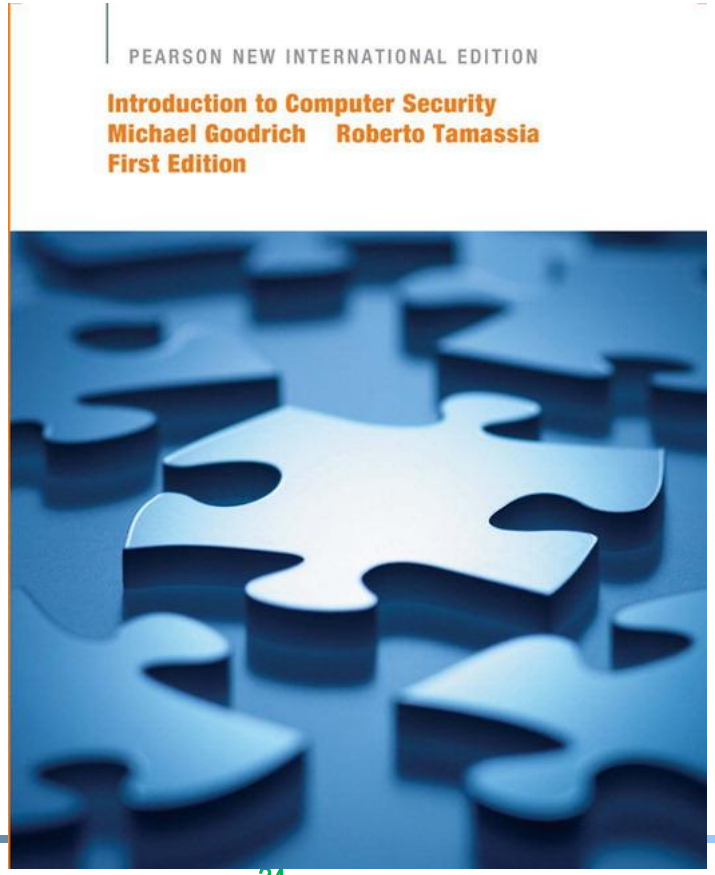


Contents of Textbook

	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

Auxiliary Textbook

- **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



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

- **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**
  - Computer 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