Syllabus

고려대학교 (Korea Univ.)

사이버국방학과 (Dept. of CYDF) · 정보보호대학원 (CIST)

사이버무기시험평가연구센터 (CW-TEC)

보안성분석평가연구실 (Security Analysis aNd Evaluation Lab.)

김 승 주 (Seungjoo Kim)

www.KimLab.net

고려대학교 정보보호대학원 KOREA UNIVERSITY

This integrated syllabus is for those taking Prof. **Seungjoo Kim**'s class.

(e.g.) Security Engineering, IT Security Evaluation Methods, Operating System, etc.

Who am I?

보안성분석평가연구실

Security Analysis aNd Evaluation Lab

www.KimLab.net / www.SecEng.net

김승주 교수 (skim71@korea.ac.kr)

로봇융합관 306호

연구분야

- Security Eng. for High-Assurance Trustworthy Systems
- High-Assurance Cryptography
- Security Verification (e.g. Formal Specification/Verification, Automated Vulnerability Finding) and Security Evaluation Standards (e.g. CMVP, CC, C&A, SSE-CMM)
- Usable Security

주요 경력 :

1990.3~1999.2) 성균관대학교 공학 학사·석사·박사
1998.12~2004.2) KISA 암호기술팀장 및 CC평가1팀장
2004.3~2011.2) 성균관대학교 정보통신공학부 부교수
2011.3~현재) 고려대학교 사이버국방학과·정보보호대학원 정교수
Founder of (사)HARU & SECUINSIDE
2017.4~현재) 고려대학교 사이버무기시험평가연구센터 부센터장

前) 육군사관학교 초빙교수
前) 선관위 DDoS 특별검사팀 자문위원
前) SBS 드라마'유령'및 영화'베를린'자문 / KBS '명견만리' 강연

現) 한국정보보호학회 이사
現) 대검찰청 디지털수사 자문위원
現) 개인정보분쟁조정위원회 위원

- '96: Convertible group signatures (AsiaCrypt)
- '97: Proxy signatures, revisited (ICICS): 670회이상 인용
- '06: 국가정보원 암호학술논문공모전 우수상
- '07: 국가정보원장 국가사이버안전업무 유공자 표창
- '12,'16: 고려대학교 석탑강의상
- '13,'17: Smart TV Security (Black Hat USA, Hack In Paris): 삼성 및 LG 스마트TV 해킹(도청·도촬) 및 해적방송 송출 시연

주요 R&D 성과

삼성전자와 공동으로
국내 최초 프린터복합기 보안 인증 획득 (2008년)

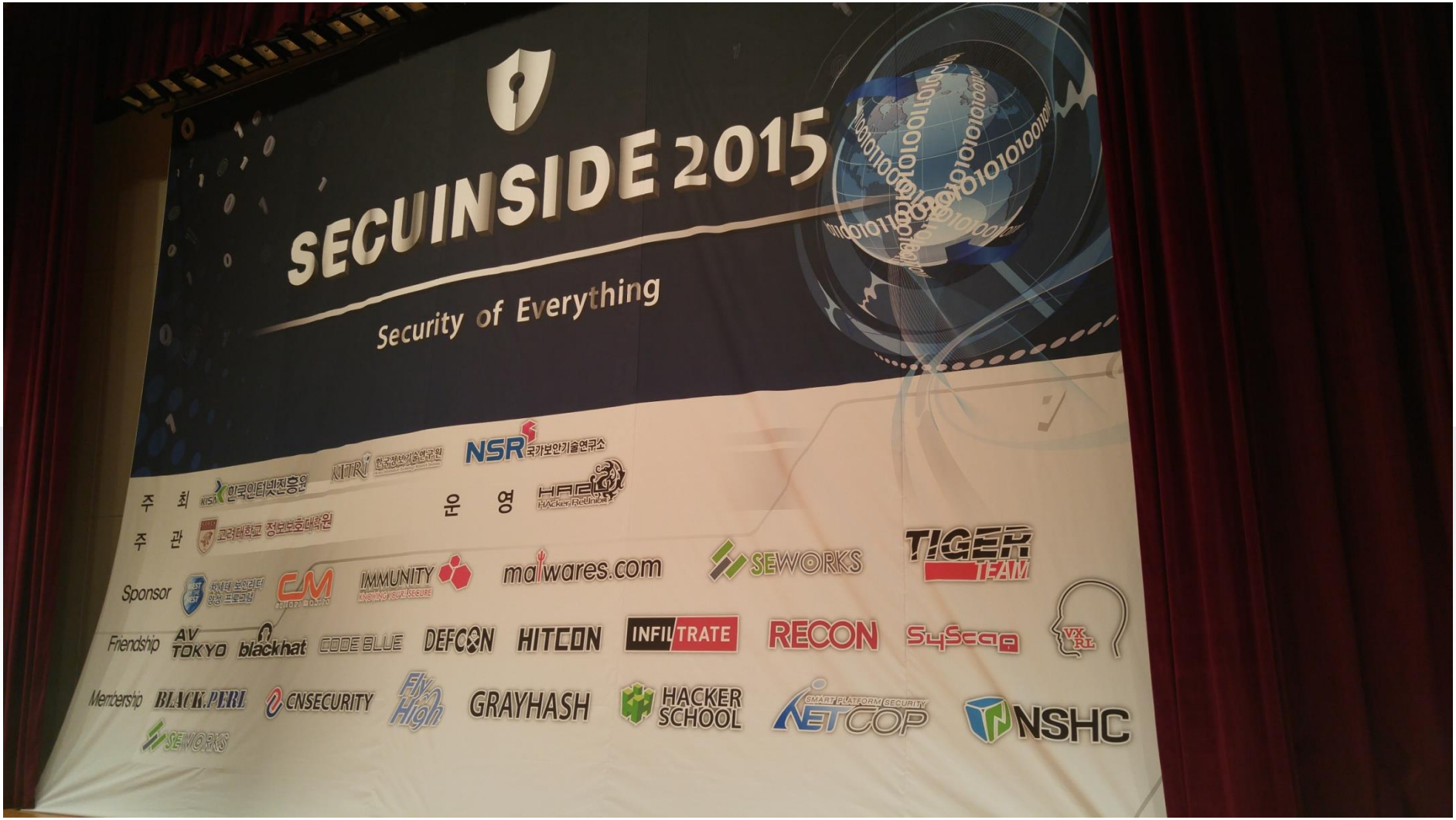
LG전자와 공동으로
세계 최초 스마트TV 보안 인증 획득 (2015년)

CyKoR @ DEFCON CTF 2015

(**Advisor :** Seungjoo Kim)

KOREA UNIVERSITY

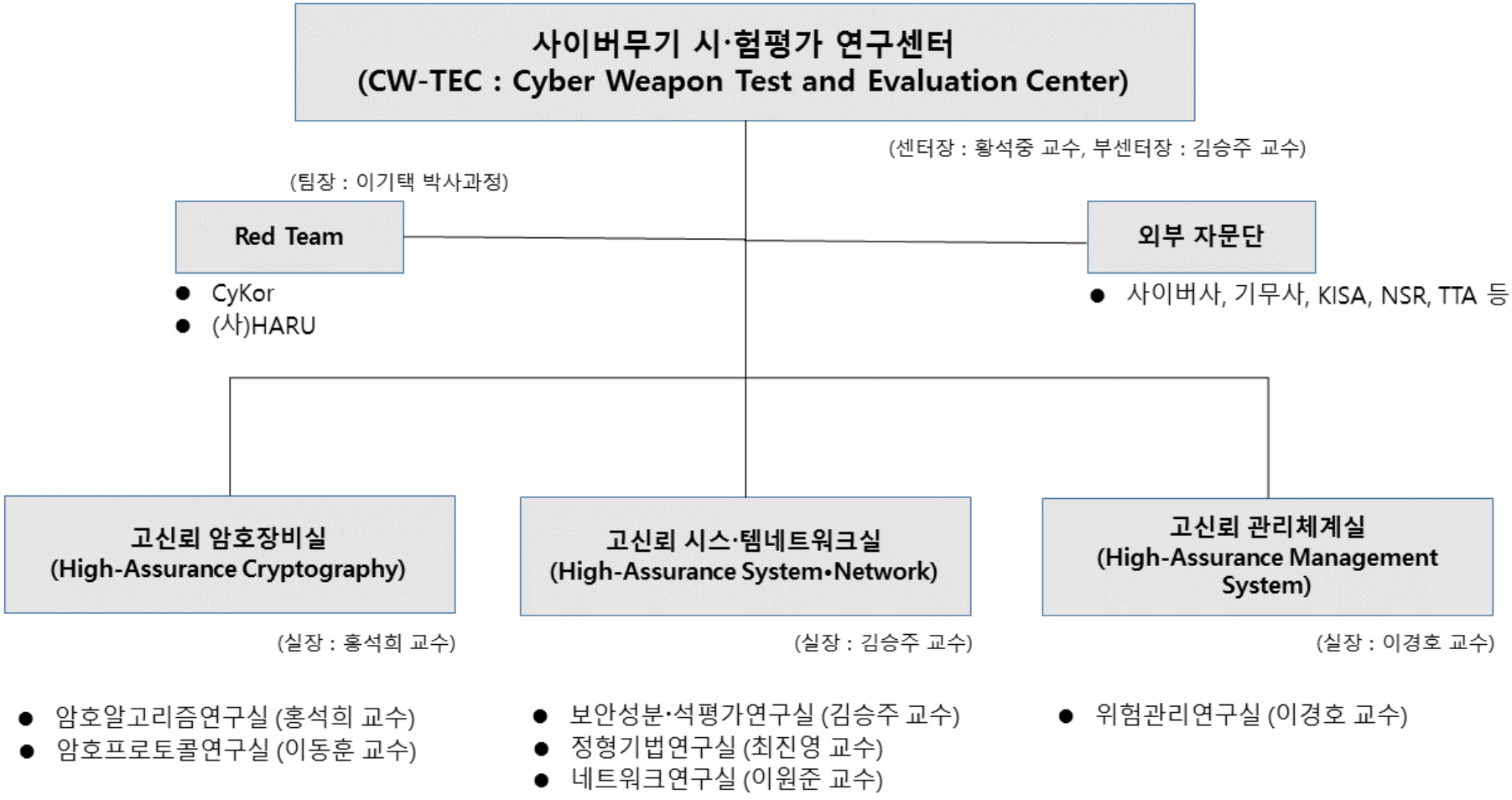
(사)화이트해커연합 HARU



(**Founder & Board Member :** Seungjoo Kim, 2011)

KOREA UNIVERSITY

사이버무기시험평가연구센터 (CW-TEC)



KOREA UNIVERSITY

Course Syllabus

KOREA UNIVERSITY

Brief History of Computer Security

- **1959) Timesharing** was proposed by MIT Prof. John McCarthy in 1959, and by other computer scientists about the same time.

- **1961)** One of the **first timesharing systems, CTSS**(Compatible Timesharing System), was developed at the MIT, and first demonstrated in November 1961.

Brief History of Computer Security

- **1964)** The original **BASIC**(Beginner's All-purpose Symbolic Instruction Code) language was released on May 1, 1964 by John G. Kemeny and Thomas E. Kurtz.
  - **Apple II** was released in 1977,and had BASIC as their primary programming language and operating environment.
- **1965~2000) Multics**(Multiplexed Information and Computing Service) by MIT, Bell Labs, and GE. **First OS created with security as its primary goal.** It was programmed **in PL/I**. http://www.multicians.org/
  - Many of the concepts of UNIX and other modern OS came directly from Multics.

Brief History of Computer Security

- **1967)** Bernard Peter (@ NSA) realized that timesharing computer system posed security issues that went beyond the traditional concerns for secure communications and **suggested several directions**.
- **1969) Adept-50** : The **first** practical attempt to **apply a mathematical model of multilevel security** with support from ARPA.
- **1969)** Ken Thompson wrote the first **UNIX** system **in assembly** language on a PDP-7.

Brief History of Computer Security

- **1972)** The **C programming language** is released. Ken Thompson and Dennis Ritchie created C and soon after **re-wrote** the source code for **Unix in C**.
  - The migration from assembly to the higher-level language C resulted in much more portable software, requiring only a relatively small amount of machine-dependent code to be replaced when porting Unix to other computing platforms.

Brief History of Computer Security

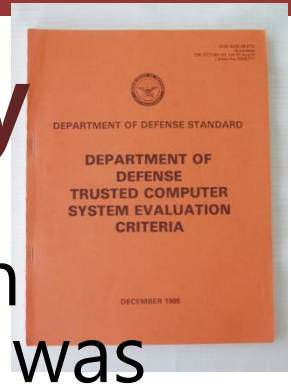
- **1972) James P. Anderson's Report** determining the requirements for U.S. government computer systems to execute securely in the presence of malicious users. http://dx.doi.org/10.1109/MSP.2008.15
  1. The reference validation mechanism must always be invoked (**complete mediation**).
  2. The reference validation mechanism must be tamperproof (**tamperproof**).
  3. The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (**verifiable**).

Brief History of Computer Security

- **1981)** The DoD Computer Security Center was founded in 1981 and renamed the **NCSC**(National Computer Security Center) in 1985. NCSC was part of NSA.

- **1981) MS-DOS**(Microsoft Disk Operating System) resulted from a request in 1981 by IBM for an operating system to use in its IBM PC range of personal computers. It modified 86-DOS of Seattle Computer Products.

Brief History of Computer Security



- **1983)** **TCSEC**(Trusted Computer System Evaluation Criteria, a.k.a. Orange Book) was issued by NCSC(National Computer Security Center) : TCB Concept
  - **Mid 80s ~ Mid 90s)** Canada, UK, European Community develop standards similar to and beyond the TCSEC.
- **1985)** Microsoft introduced an operating environment named **Windows** on November 20, 1985.
- **1989)** Military Standard 1785 on **System Security Engineering** was released.

KOREA UNIVERSITY

Brief History of Computer Security

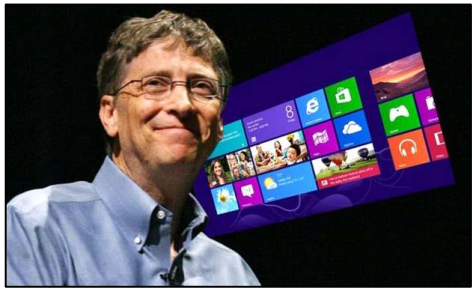
- **1991)** **Linux** kernel was released on September 17, 1991 by Linus Torvalds.

- **1996)** The international **CC**(Common Criteria) emerged.

KOREA UNIVERSITY

Brief History of Computer Security

- **2002)** Bill Gates wrote "**Trustworthy Computing**" memo early 2002.

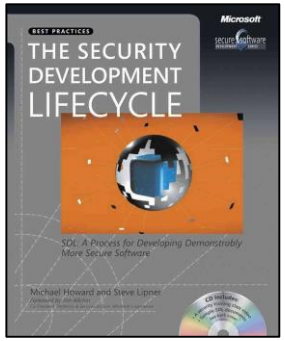


- **2002)** Unix-based graphical OS, **macOS (Mac OS X or OS X)** was developed and marketed by Apple Inc.

KOREA UNIVERSITY

Brief History of Computer Security

- **2004)** Microsoft Senior Leadership Team agreed to require **SDL**(Security Development Lifecycle) for **all** products. https://www.microsoft.com/en-us/SDL



- **2007) Window Vista** : The **first** OS to go through **full SDL** cycle

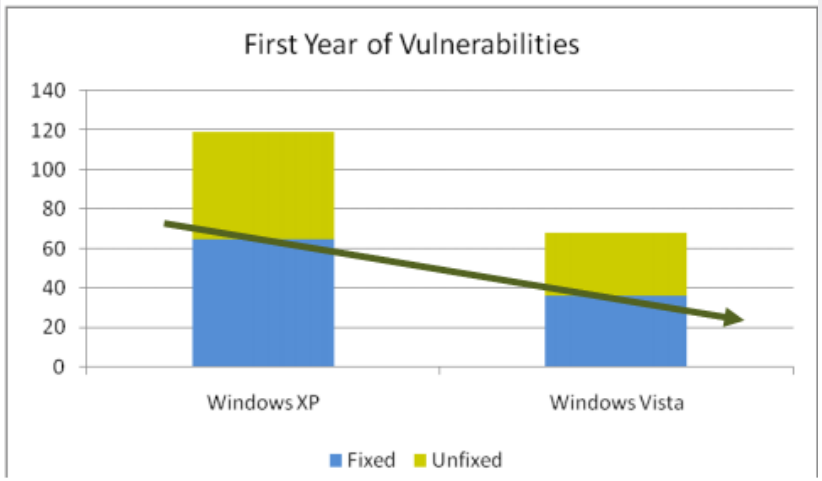


Figure 3: Side-by-side First Year Vulnerabilities for Windows Vista and Windows XP

KOREA UNIVERSITY

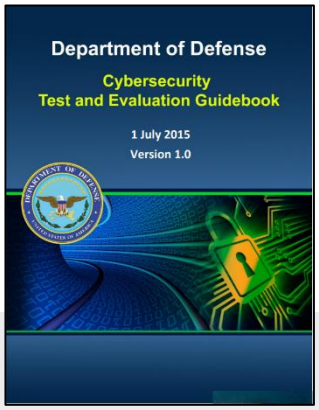
Brief History of Computer Security

- **2007) Android** : Initially developed by Android Inc., which Google bought in 2005, and unveiled in 2007.

- **2009) seL4**(Secure Embedded L4) : The **first**-ever general purpose OS kernel that is **fully formally verified** for functional correctness by NICTA https://sel4.systems/

Brief History of Computer Security

- **2015)** DoD Cyber Chief, "Cybersecurity now key requirement for all weapons."
  - **DoD(Department of Defense) Cybersecurity Test and Evaluation Guidebook** was released.



- **2016)** NIST rolled out **NIST Special Publication 800-160: Systems Security Engineering**.

Brief History of Computer Security

- **2017)** The BASIC(British American Security Information Council) found the **U.K.'s Trident nuclear submarine fleet** is vulnerable to various cyberattacks

- **2017) Kakao Bank** launched.
  - "What is different in Kakao Bank security?" http://amhoin.blog.me/221084472531

What I Teach

- C Programming Language (undergraduate)
- Operating System (undergraduate)
- Security Engineering (graduate)
- Security Evaluation (graduate)

KOREA UNIVERSITY

What I Teach

- C Programming Language (undergraduate)
- Operating System (undergraduate)
- Security Engineering (graduate)
  - ☞ How to build (provably) secure things
- Security Evaluation (graduate)
  - ☞ How to check it

KOREA UNIVERSITY

What I Teach

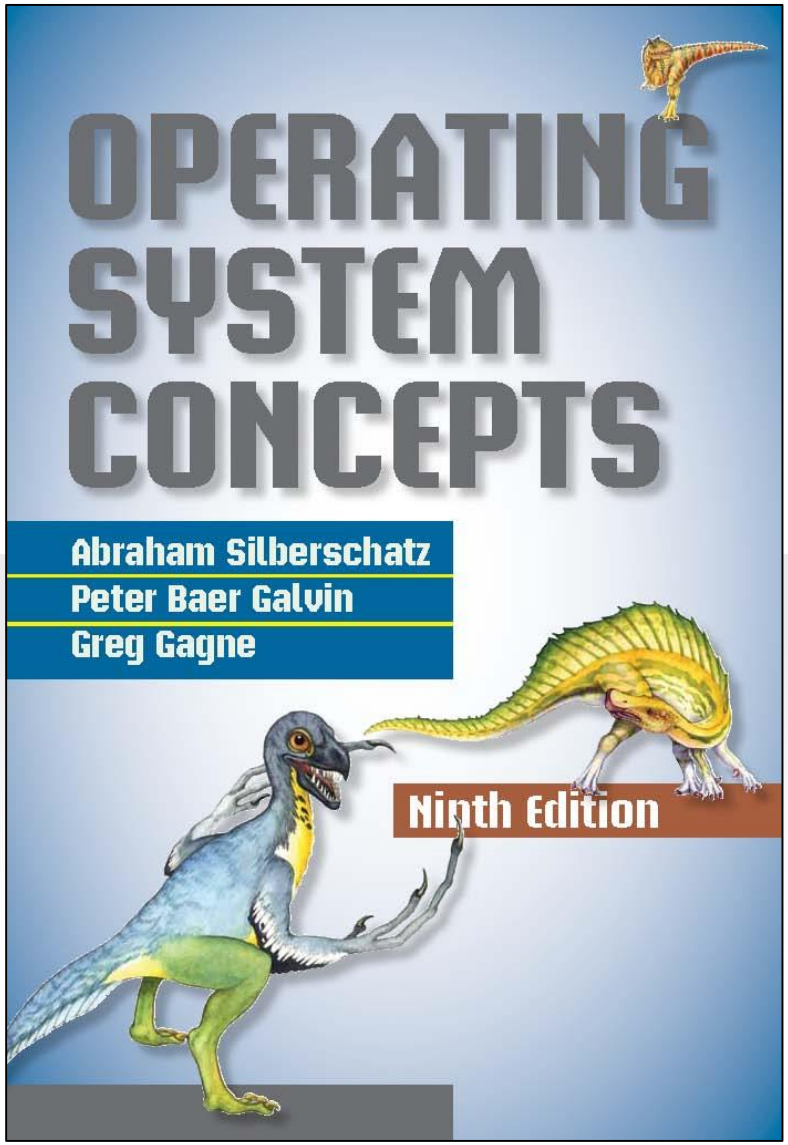
- C Programming Language (undergraduate)
- Operating System (undergraduate)
- Security Engineering (graduate)
  + Intro. to IA & SE (undergraduate)
- Security Evaluation (graduate)

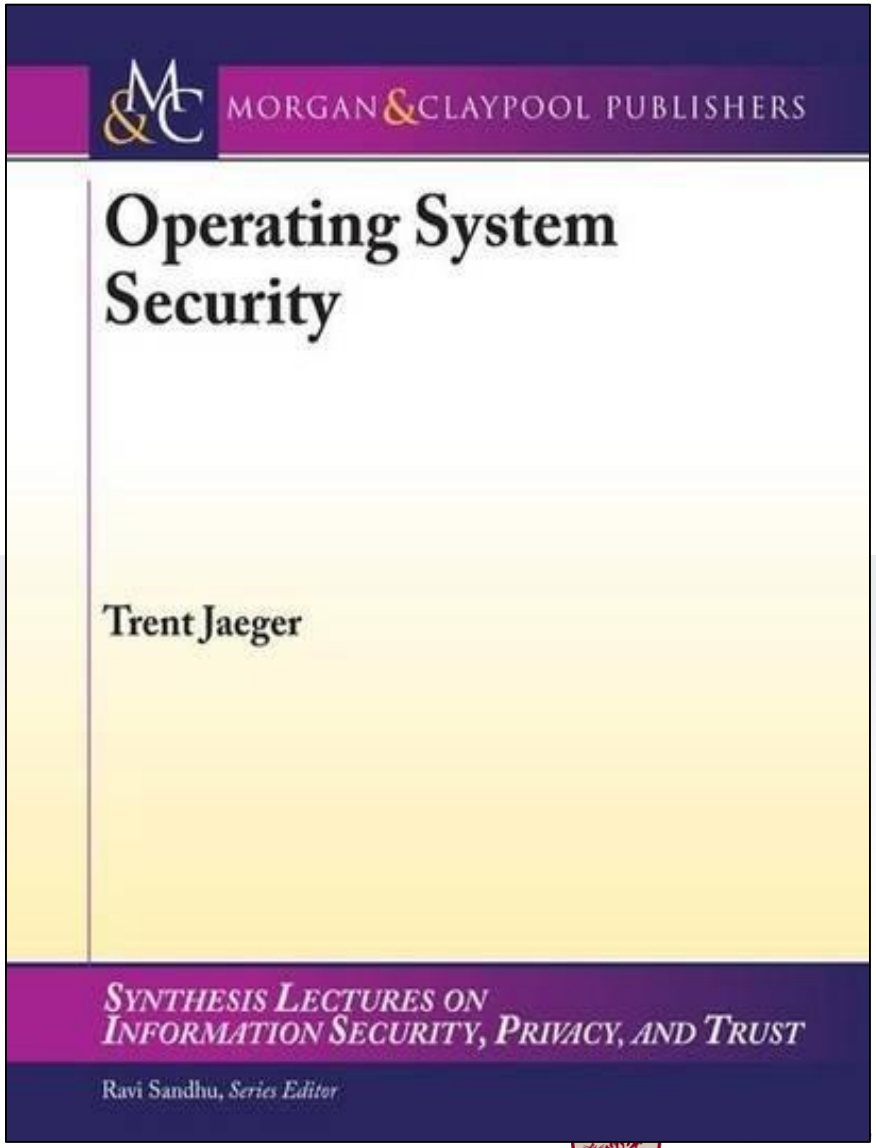
KOREA UNIVERSITY

Download Course Materials

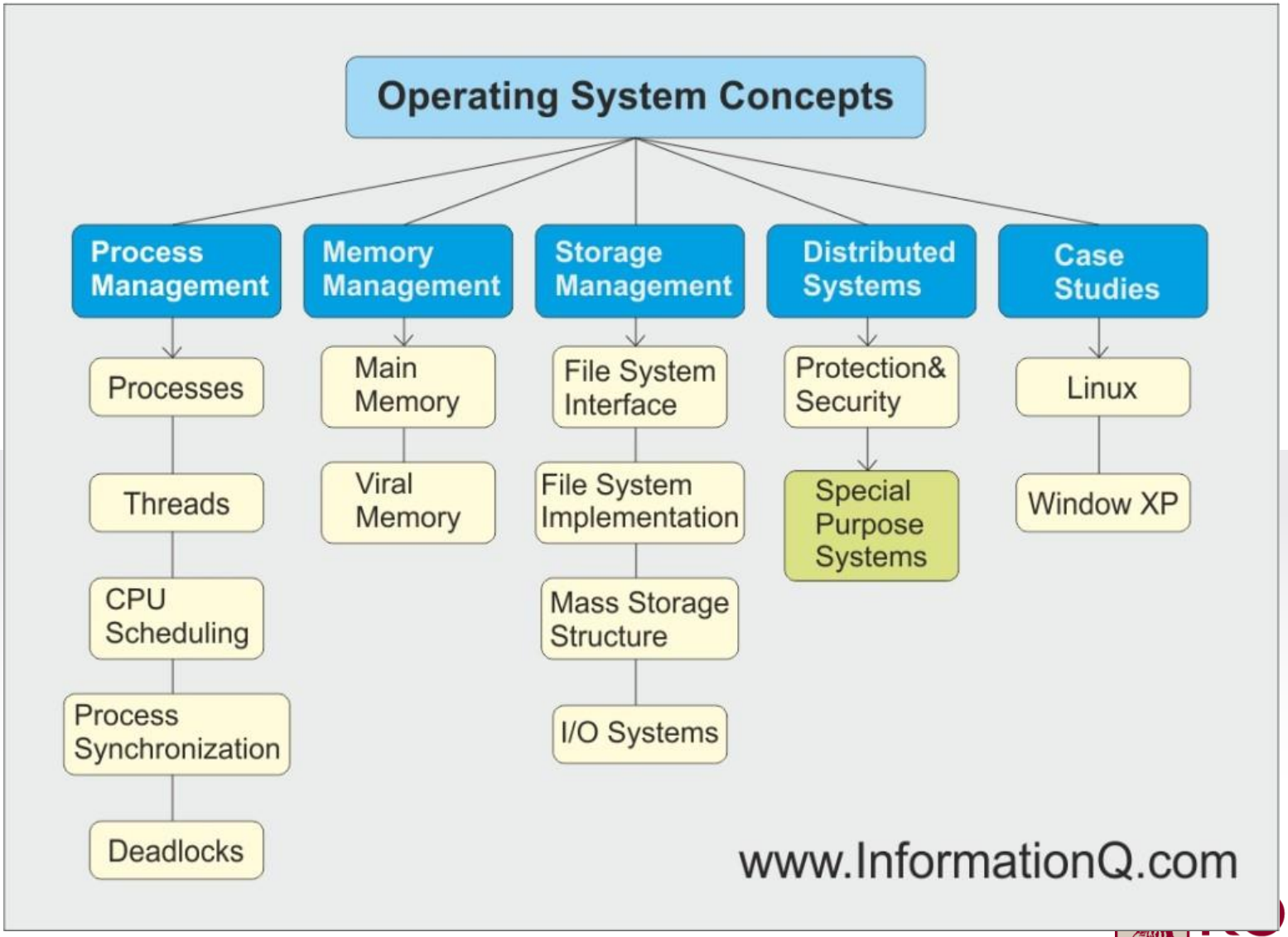
- http://www.skim.name -> Lecture
- http://www.kimlab.net -> Lecture

Textbooks


OPERATING SYSTEM CONCEPTS
Abraham Silberschatz
Peter Baer Galvin
Greg Gagne
Ninth Edition


MORGAN & CLAYPOOL PUBLISHERS
Operating System Security
Trent Jaeger
SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, AND TRUST
Ravi Sandhu, Series Editor

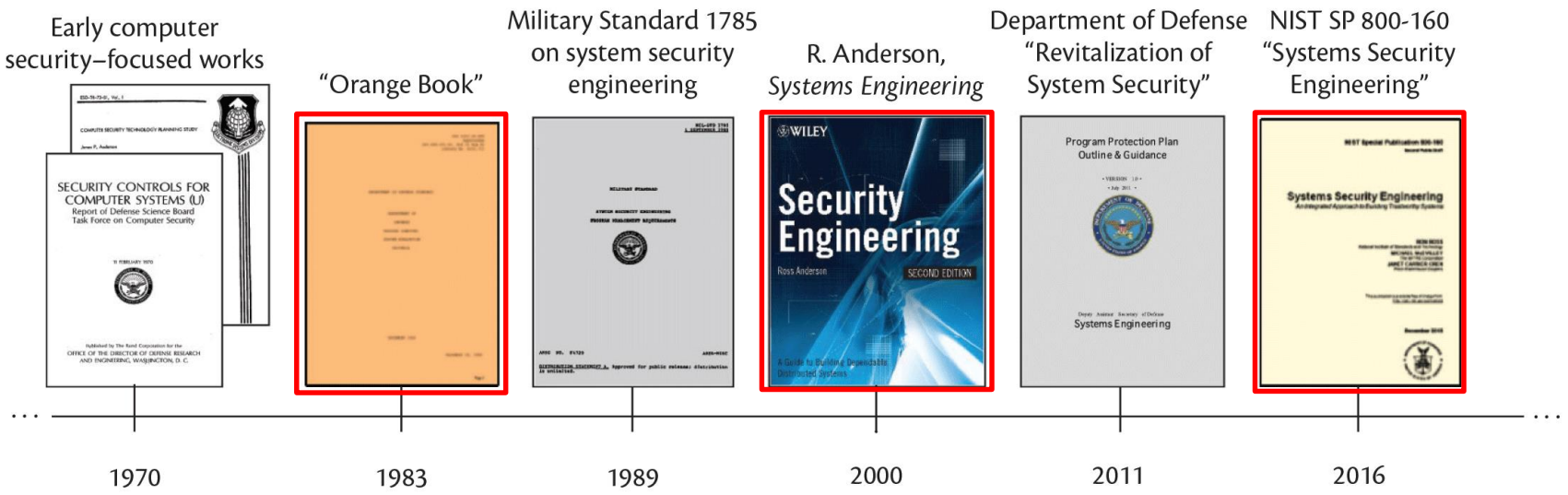
[Note] Operating System: Concepts



[Note] Operating System Security

- Access Control Fundamentals
- Multics
- Security in Ordinary OS
- Verifiable Security Goals
- Security Kernels
- Securing Commercial OS
- Case Study : Solaris Trusted Extensions
- Case Study : Building a Secure OS for Linux
- Secure Capability Systems
- Secure Virtual Machine Systems
- System Assurance

Textbooks



KOREA UNIVERSITY

Textbooks

많은 기관과 정부부처에서는 CC인증을 획득한 제품을 필요로 하며, 구매 과정에서 공통평가기준 방법론을 사용한다. 하지만 시중에는 IT 보안성 평가를 위한 공통평가기준이 설명된 자료가 턱없이 부족한 실정이다.

"국제공통평가 기준을 이용한 보안 평가론"은 IT제품, 시스템, 네트워크, 서비스계약의 구매, 개발, 평가시 공통평가기준을 이용하는 이유와 방법에 대해 설명하고 있다.

이 책에서는 공통평가기준방법론에 대해 서술하고 있는데 이는 주요 과정 및 단계, 활동, 의미, 관련용어 그리고 공통평가기준방법론이 시스템의 생명주기 동안 어떻게 사용되는지에 대해 서술하고 있다.

이 책은 FAA, the Federal Reserve Bank, DoD, NATO, NASA, 그리고 정보기관들과 같은 곳에서 운영되는 중요 기반시설 시스템에 필요한 모든 것에 관한 중요한 참고서이다.

공통평가기준을 준수하기 위해 구성된, "국제공통평가 기준을 이용한 보안 평가론"은 3개의 다른 시나리오(COTS 제품, 시스템 또는 네트워크, 서비스 계약)에 방법론이 어떻게 적용될 수 있는지 설명하기 위해 각 장마다 예제를 제공한다. 또한, 각 장의 끝에는 토의 문제를 두어 본문의 이해를 돕고 교육상 효과를 높이고자 하였다.

특징

1. PP에서 보안 요구사항을 서술하는 방법 설명
2. ST에서 보안 구조를 설계하는 방법 설명
3. 보안기능요구사항이 만족되었는지, 그리고 정확히 서술되었는지 검증하는 방법 설명
4. 정보의 무단노출, 수정, 손실을 막는 방법 설명
5. 신뢰적인 system 개발 지원

국제공통평가 기준을 이용한 보안 평가론

저자 DEBRA S. HERRMAUN
역자 김승주

홍릉과학출판사

Using the Common Criteria for IT Security Evaluation

국제공통평가 기준을 이용한

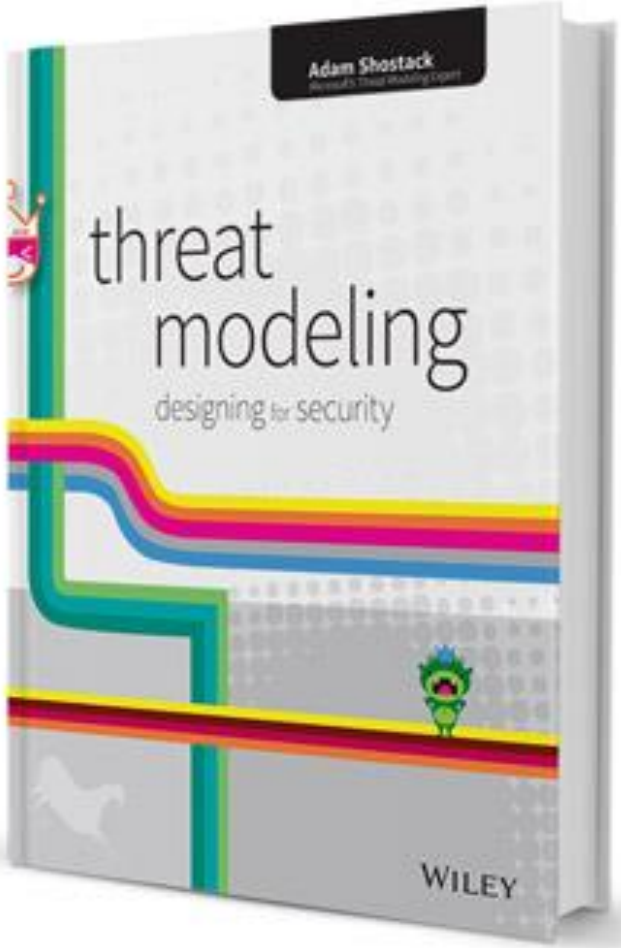
보안 평가론

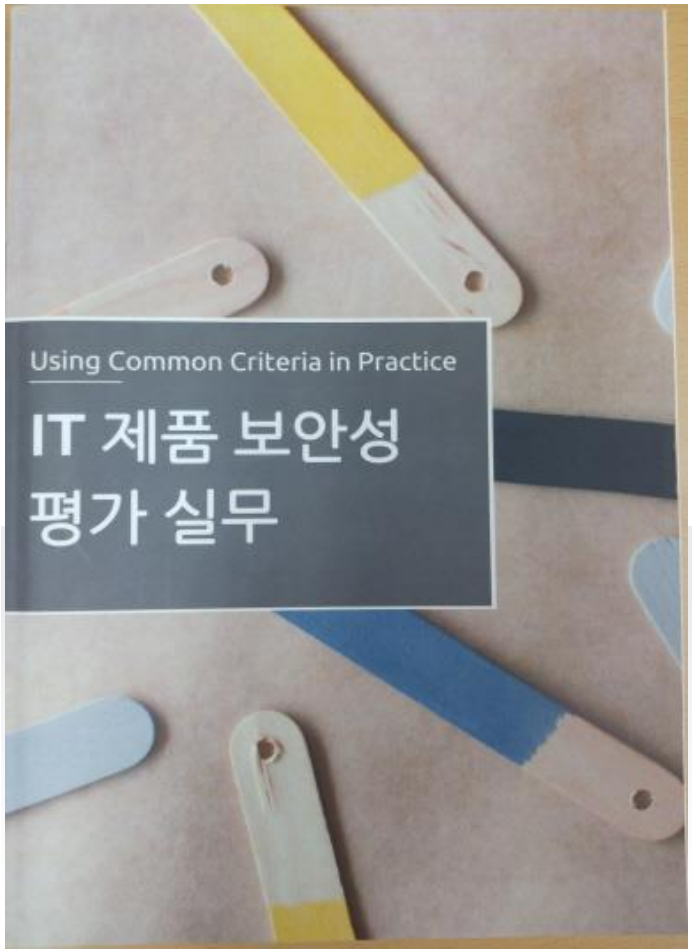
저자 DEBRA S. HERRMAUN 역자 김승주

홍릉과학출판사

KOREA UNIVERSITY

Textbooks





KOREA UNIVERSITY

ICCC (International CC Conference)

ICMC (International Crypto Module Conf)

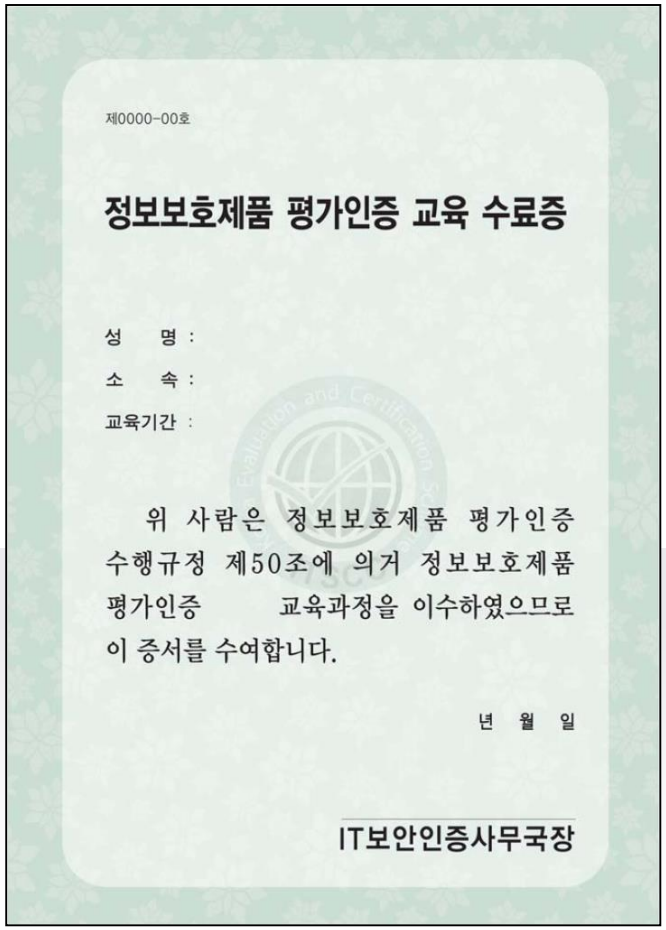
KOREA UNIVERSITY

Certifications

My CSSLP Certification

KOREA UNIVERSITY

Certifications



제0000-00호

정보보호제품 평가인증 교육 수료증

성 명 :
소 속 :
교육기간 :

위 사람은 정보보호제품 평가인증 수행규정 제50조에 의거 정보보호제품 평가인증 교육과정을 이수하였으므로 이 증서를 수여합니다.

년 월 일

IT보안인증사무국장

정보보호제품 평가인증 교육 수료증

제0000-00호

정보보호제품 평가자 자격증

성 명 :
소 속 :
자 격 :
평가범위 :

위 사람은 정보보호제품 평가인증 수행규정 제34조에 의거 평가자 자격을 부여합니다.

년 월 일

IT보안인증사무국장

정보보호제품 평가자 자격증

KOREA UNIVERSITY

Syllabus

고려대학교 (Korea Univ.)

사이버국방학과 (Dept. of CYDF) · 정보보호대학원 (CIST)

사이버무기시험평가연구센터 (CW-TEC)

보안성분석평가연구실 (Security Analysis aNd Evaluation Lab.)

김 승 주 (Seungjoo Kim)

(FB) www.fb.com/skim71 (Twitter) @skim71