Security Evaluation Standards

고려대학교 (Korea Univ.)
사이버국방학과 · 정보보호대학원 (CIST)
보안성분석평가연구실 (Security Analysis aNd Evaluation Lab.)

김 승 주 (Seungjoo Kim)

www.kimlab.net

고려대학교 정보보호대학원 KOREA UNIVERSITY

보안성분석평가연구실

Security Analysis aNd Evaluation Lab

www.KimLab.net / www.SecEng.net

Seungjoo Kim
PROFESSOR, KOREA UNIVERSITY
CNN
North Korean government website hacked

김승주 교수 (skim71@korea.ac.kr)

로봇융합관 306호

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

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): 670회 이상 인용
- '06: 국가정보원 암호학술논문공모전 우수상
- '07: 국가정보원장 국가사이버안전업무 유공자 표창
- '12, '16: 고려대학교 석탑강의상
- '13: Smart TV Security (Black Hat USA): 스마트TV 해킹(도청·도촬) 및 해적방송 송출 시연

연구분야

- Security Eng. for High-Assurance Trustworthy Systems
- High-Assurance Cryptography
- Security Testing (including End-to-End Provable Security, Formal Verification) and Security Evaluation (e.g. CMVP, CC, C&A, SSE-CMM)
- Usable Security

주요 R&D 성과

Common Criteria Certification for Samsung Multifunction Printers

WHITE PAPER

Common Criteria Certification for Samsung Multifunction Printers

Introduction

[illegible]

Overview

[illegible]

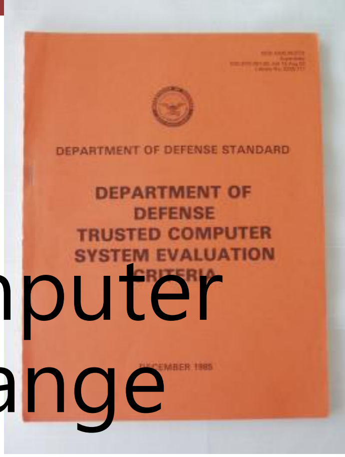
삼성전자와 공동으로
국내 최초 프린터복합기 보안 인증 획득 (2008년)

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

Security Evaluation Begins

- In 1967, realized that ( ) system posed security issues that went beyond the traditional concerns for secure communications. ( ) (@ NSA) talked 3 important issues :

DoD’s TCSEC


DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

DECEMBER 1985

- In ( ), DoD’s **TCSEC** (Trusted Computer System Evaluation Criteria, a.k.a Orange Book) was made.
  - Specifies evaluation classes ( )
  - **A1 : ( )**
    - It had been expected that a higher, A2, incorporating ( ), would eventually be added, but the addition was never made.

Rise of NSA NCSC

- In (   ), DoD CSEC was elevated to NSA **NCSC** (   ) because :
  - The growing interconnection of computers into networks (   ) between COMSEC and COPUSEC.
  - High-level computer security market was never really as large as people expected. They need to (   ) by including in it sectors that were nonmilitary but had computer security concerns : Other departments of government and the commercial sector, especially banking.

In Mid 80s - Mid 90s

- The Red Book (Trusted Network Interpretation (TNI) of the Orange Book)
- Series that expanded on Orange Book in specific areas was called "(   )".
- Canada, UK, European Community develop standards similar to and beyond the Orange Book.

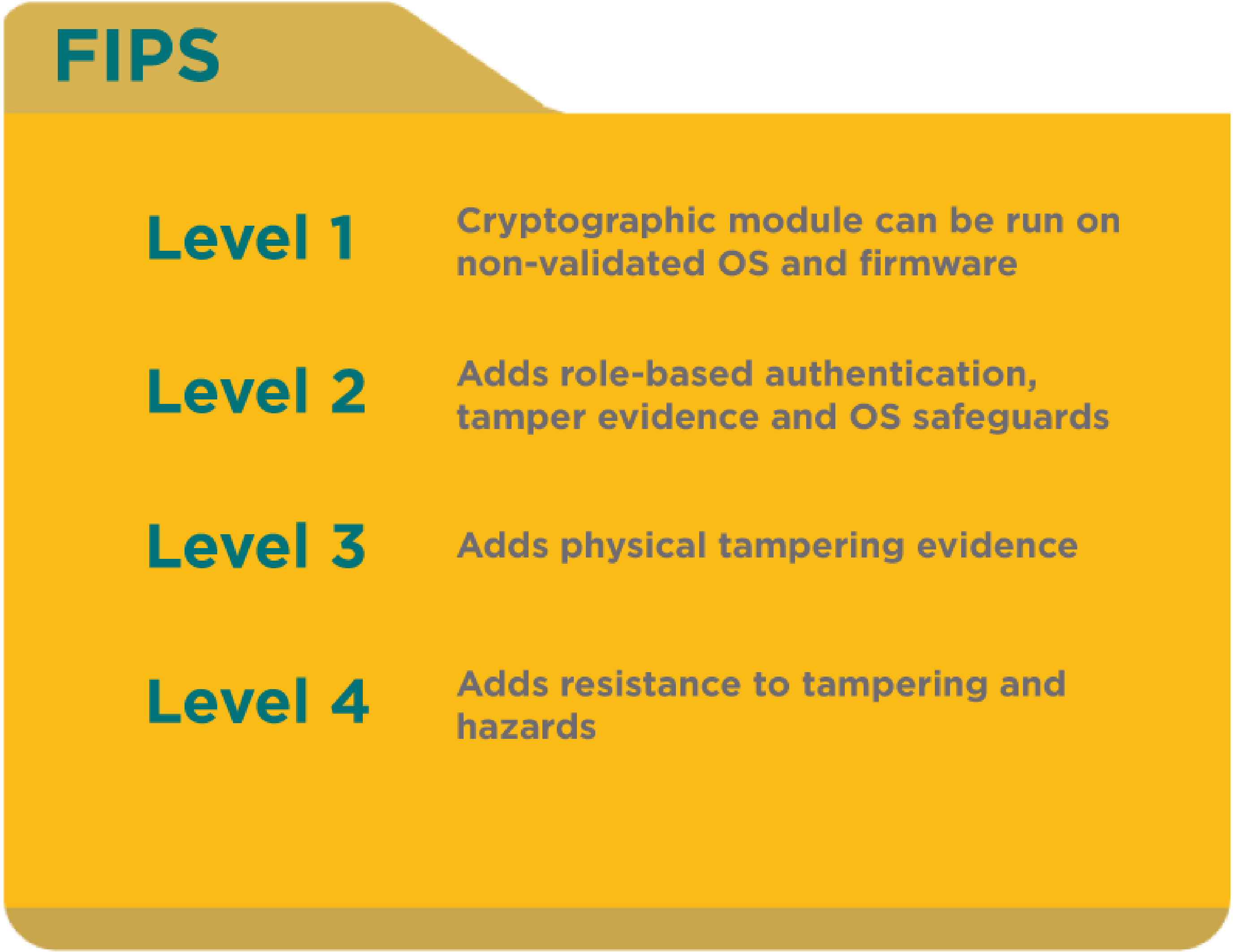
CMVP

- **CMVP** : to test and validate cryptographic modules to
  - FIPS 140-1 (1994, developed by a government and industry working group)
  - FIPS 140-2 (2001, supersedes FIPS 140-1)
  - Draft FIPS 140-3 (Revised Draft 09/11/09, will supersede FIPS 140-2)
    - 11 Security Sections
    - 4 Security Assurance Levels
  - Joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada.
  - All cryptographic modules used by US Federal Government to protect ( ) information go through CMVP validation program.

CMVP

- Works jointly with the NIST ( ).
  - ( ) algorithmic validation is a ( ) for ( ) module validation.
- International Standards Organization
  - ISO/IEC 19790 Security Requirements for Cryptographic Modules
    - Published March 2006
  - ISO/IEC 24759 Test requirements for cryptographic modules
    - Published July 2008
  - ( ) was the editor for both international standards.

CMVP



FIPS

Level 1	Cryptographic module can be run on non-validated OS and firmware
Level 2	Adds role-based authentication, tamper evidence and OS safeguards
Level 3	Adds physical tampering evidence
Level 4	Adds resistance to tampering and hazards

CMVP

Country	CST Lab
USA	• ÆGISOLVE, INC. (USA - CA) • Aspect Labs, a division of BKP Security, Inc. (USA - CA) • atsec Information Security Corporation (USA - TX) • CEAL: a CygnaCom Solutions Laboratory (USA - VA) • COACT Inc. CAFE Laboratory (USA - MD) • Computer Sciences Corporation (USA - MD) • ICSA Labs, An Independent Division of Verizon Business (USA - PA) • InfoGard Laboratories, Inc. (USA - CA) • SAIC Accredited Testing & Evaluation (AT&E) Labs (USA - MD) • SAIC Accredited Testing & Evaluation (AT&E) Labs (USA - VA) • Underwriters Laboratories, Inc. (USA - IL)
Canada	• DOMUS IT Security Laboratory (Canada) • EWA - Canada IT Security Evaluation & Test Facility (Canada)
Germany	• TÜV Informationstechnik GmbH (Germany)
Japan	• ECSEC Laboratory Inc. (Japan) • Information Technology Security Center (Japan)
Spain	• Epoche & Espri (Spain)
Taiwan	• TTC IT Security Evaluation Laboratory (Taiwan, R.O.C.)

※ http://csrc.nist.gov/groups/STM/testing_labs/index.html

※ **CST Lab :** Cryptographic and Security Testing Lab accredited by NVLAP(National Voluntary Laboratory Accreditation Program)

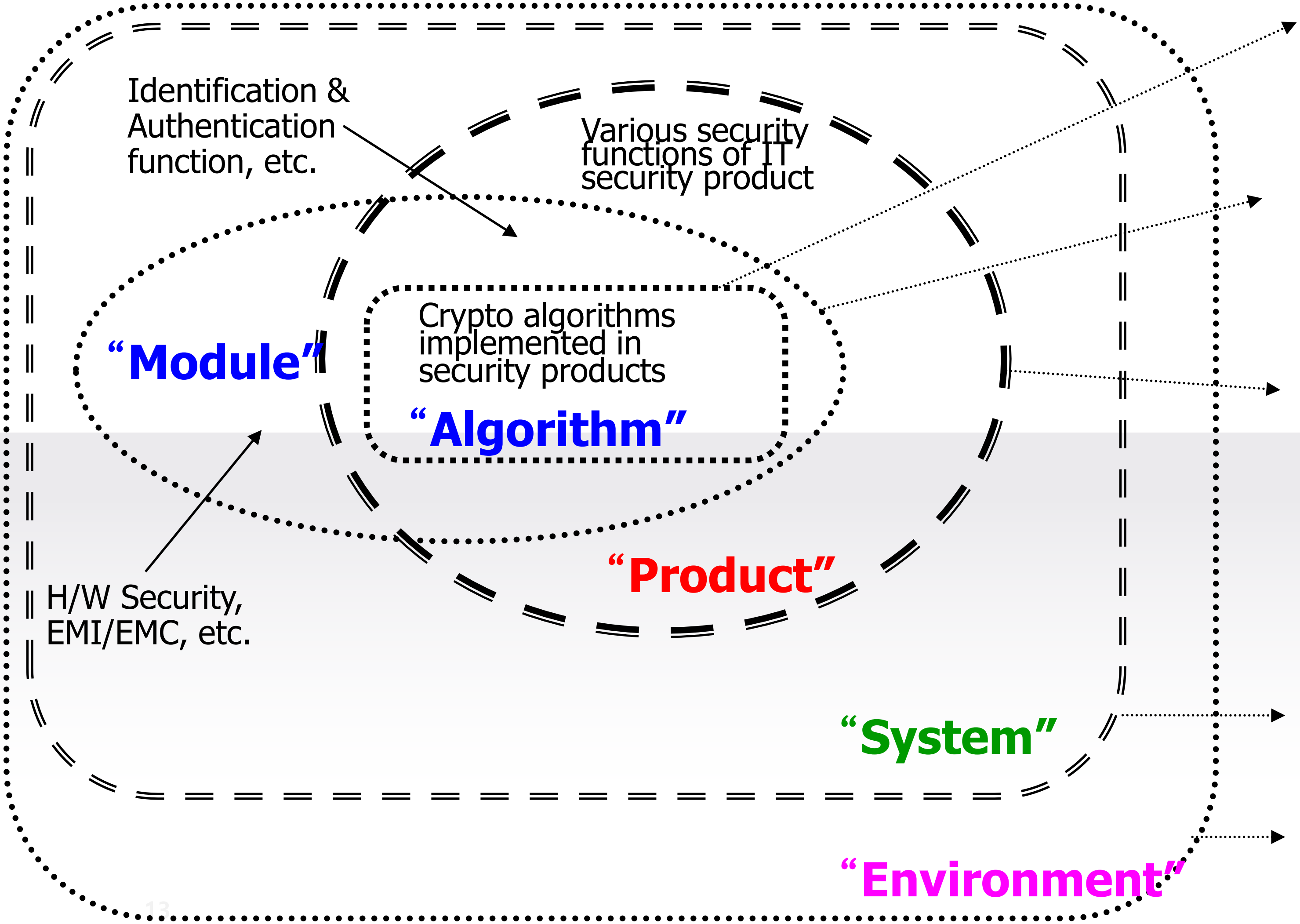
International Standard, CC

- The international **CC** (   ) emerged because :
  - Extending the computer security market by internationalizing the market.
  - The orange book had serious flaw : The problem with bundling functionality and assurance.
    - It ruled out systems that had simple functions but high assurance of the correctness of those functions.
    - Thus CC reflects the (   ) unbundled approach rather than (   ) bundled one, although there is a provision for bundled PPs.

Sample Products Evaluated by CC

VMware® ESXi Server 3.5 and VirtualCenter 2.5	EAL4+	24-FEB-10
Microsoft Windows Mobile 6.5	EAL4+	09-FEB-10
Apple Mac OS X 10.6	EAL3+	08-JAN-10
Red Hat Enterprise Linux Ver. 5.3 on Dell 11G Family Servers	EAL4+	23-DEC-09
Windows Vista Enterprise; Windows Server 2008 Standard Edition; Windows Server 2008 Enterprise Edition; Windows Server 2008 Datacenter Edition	EAL4+ ALC_FLR.3	31-AUG-09
Oracle Enterprise Linux Version 5 Update 1	EAL4+ ALC_FLR.3	15-OCT-08
Green Hills Software INTEGRITY-178B Separation Kernel, comprising: INTEGRITY-178B Real Time Operating System (RTOS),	EAL6+	01-SEP-08

After CC, C&A



Identification & Authentication function, etc.

Various security functions of IT security product

"Module"

Crypto algorithms implemented in security products

"Algorithm"

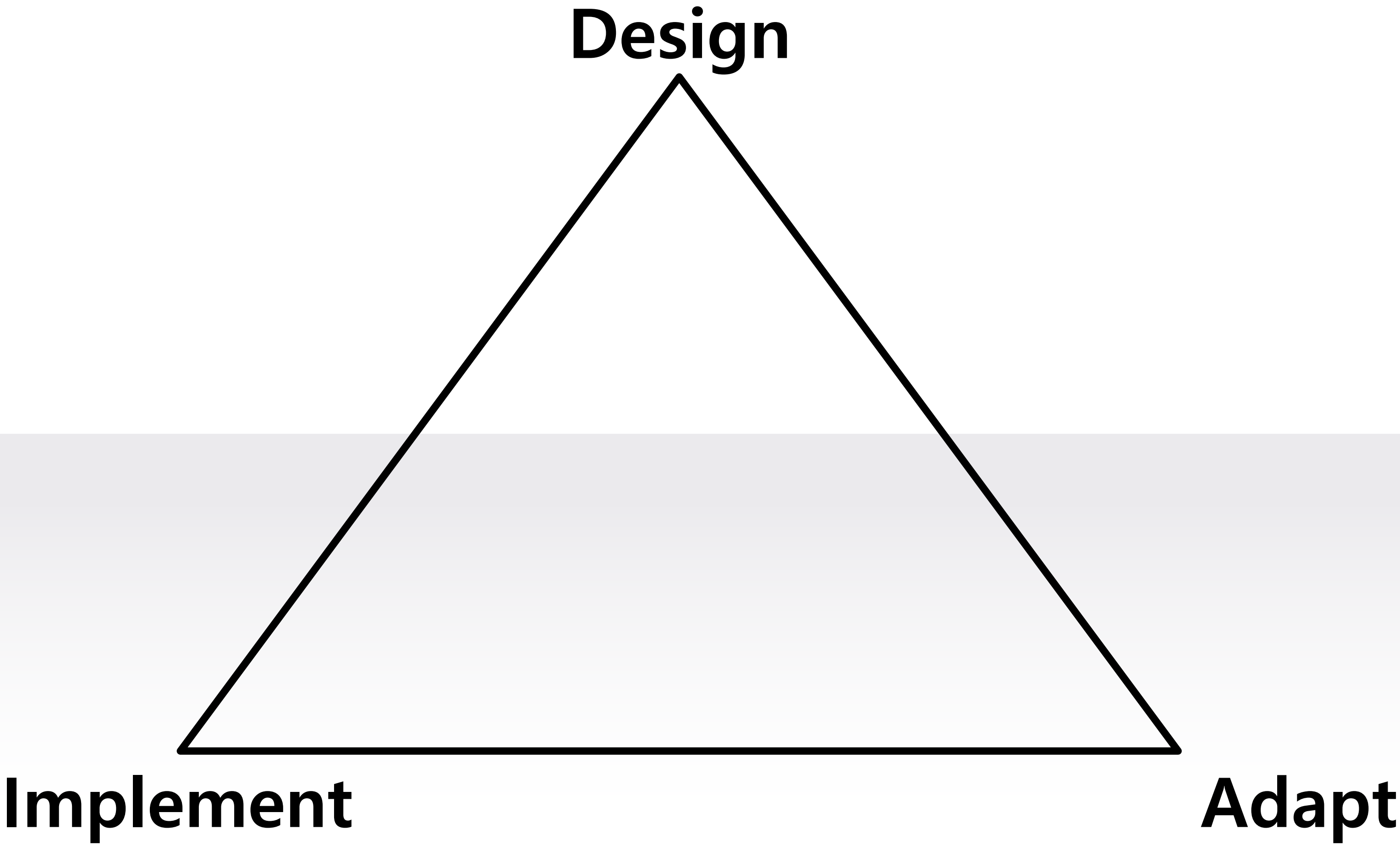
H/W Security, EMI/EMC, etc.

"Product"

"System"

"Environment"

After CC, C&A



Design

Implement

Adapt

C&A

- Title III of the E-Government Act (Public Law 107-347), entitled ( ), requires that all federal agencies develop and implement an agency-wide information security program designed to safeguard IT assets and data of the respective agency.

C&A

- There are generally 3 methodologies used by government organizations in order to satisfy the requirements set forth by (   ) :
  -
  -
  -

C&A

DIACAP

DITSCAP

It's all just C&A to me...

NIACAP

C&A

- Processes used to evaluate and approve a system for **government** or **military** use
  - Or a highly regulated industry like **pharmaceuticals** or **aeronautics**
  - Not normally used in businesses

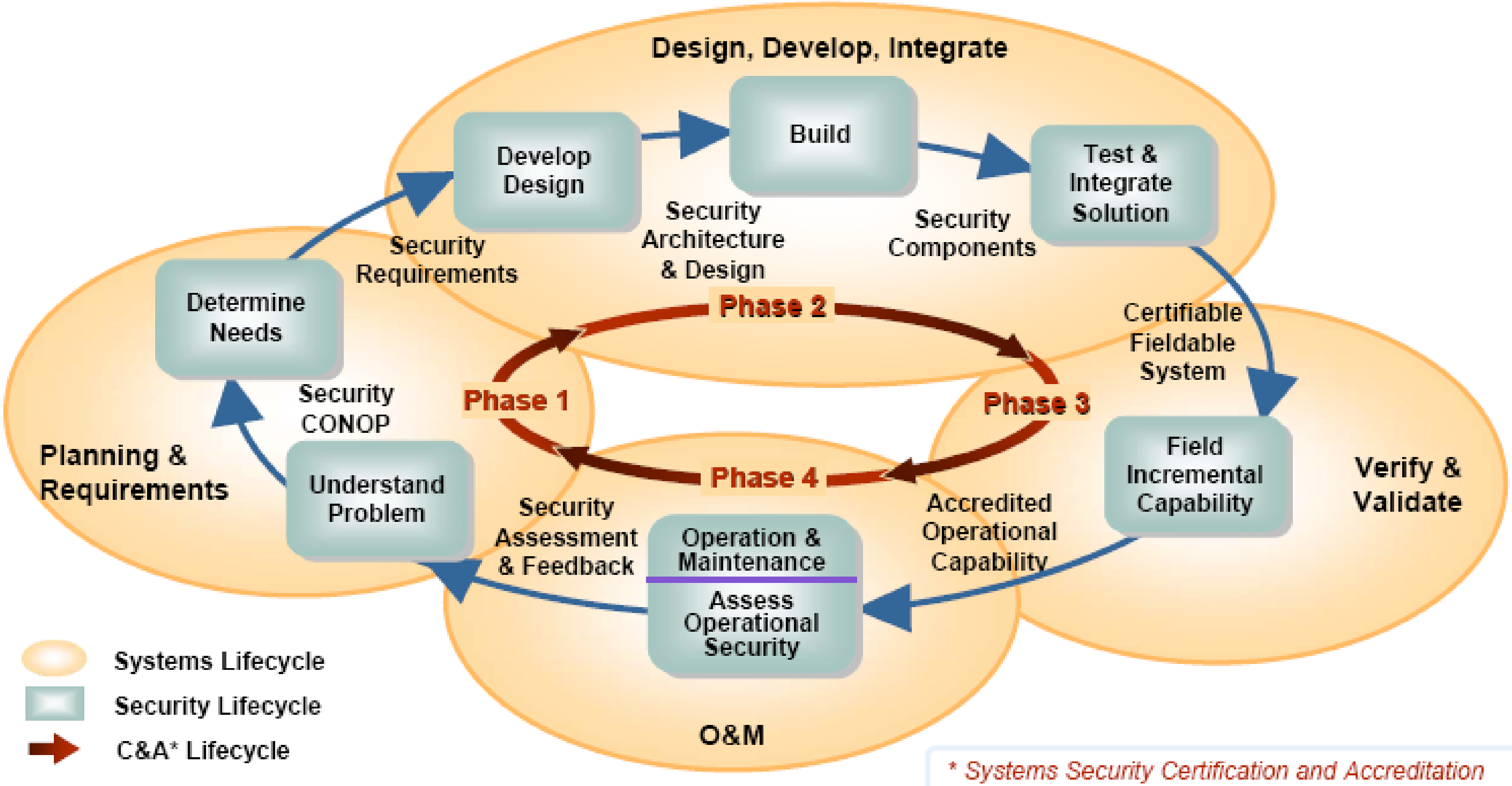
C&A

- It is a process for ( ) that a given system is safe to operate (security-wise) in its ( ).

- A process that ensures systems maintain their ( ) throughout their ( ).

C&A

Integrating security engineering into the systems engineering lifecycle enables successful information assurance implementation

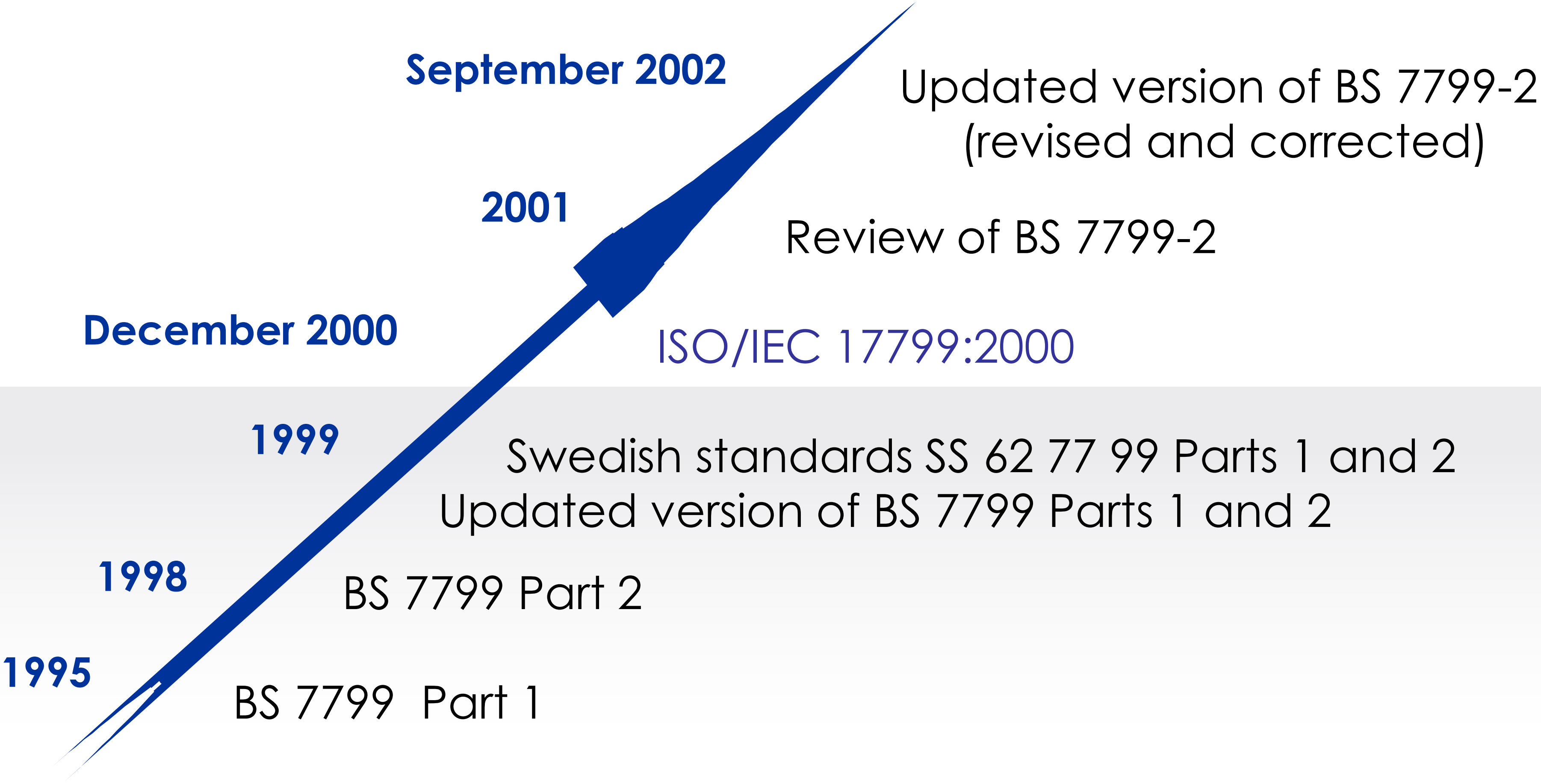


* Systems Security Certification and Accreditation

After CC, BS7799/ISO 17799

- An international standard covering **every** aspect of information security :
  - Equipment
  - Management policies
  - Human resources
  - Legal aspects

After CC, BS7799/ISO 17799



1995 BS 7799 Part 1

1998 BS 7799 Part 2

1999 Swedish standards SS 62 77 99 Parts 1 and 2
Updated version of BS 7799 Parts 1 and 2

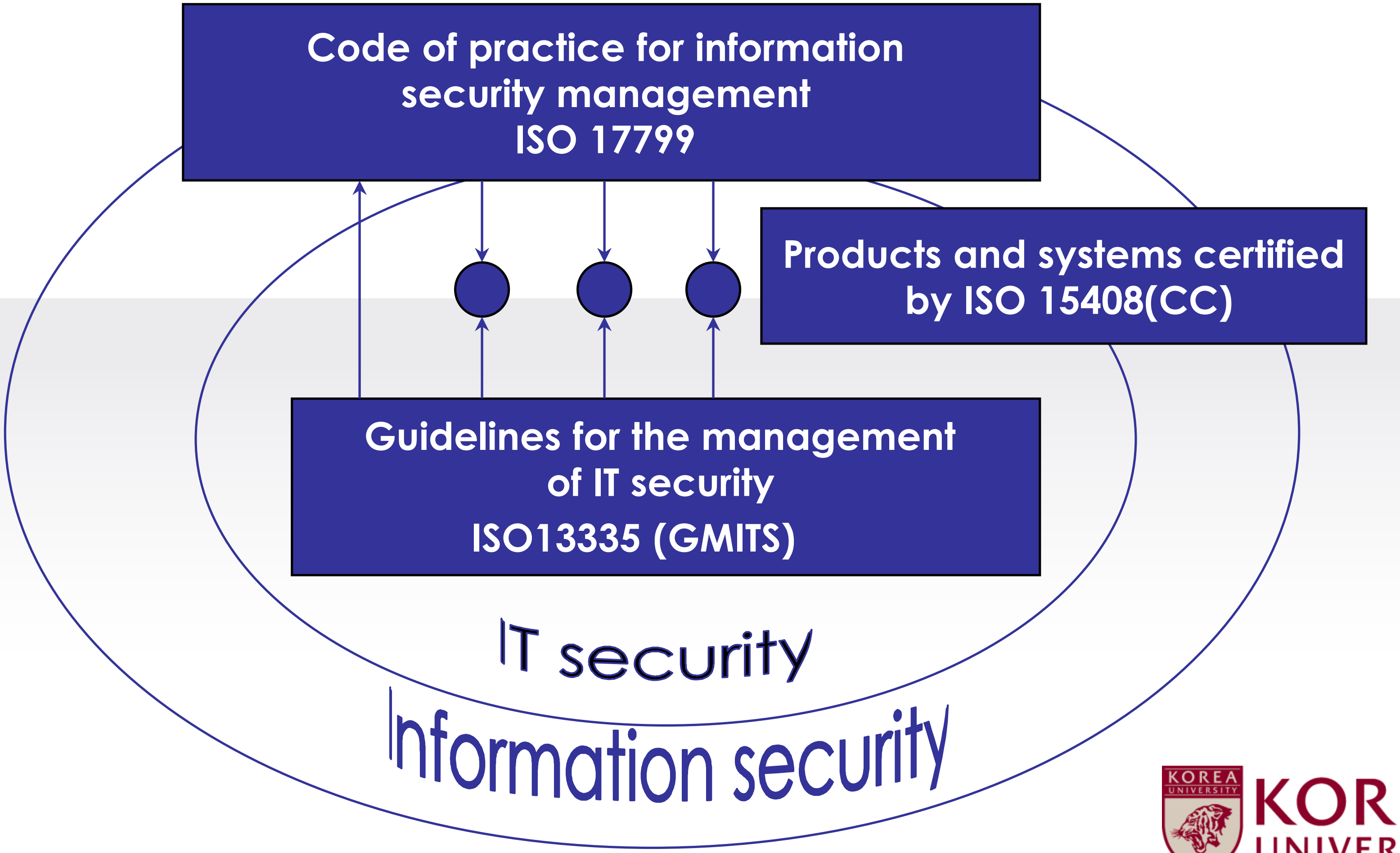
December 2000 ISO/IEC 17799:2000

2001 Review of BS 7799-2

September 2002 Updated version of BS 7799-2 (revised and corrected)

After CC, BS7799/ISO 17799

- Complementarity with Other ISO Standards



Code of practice for information security management
ISO 17799

Products and systems certified by ISO 15408(CC)

Guidelines for the management of IT security
ISO13335 (GMITS)

IT security

Information security

But Testing Is Still Required…

- CC, even at EAL7(“formally verified design and tested), relies on (   ).
  - Although mathematical proofs are required for security properties of the system’s API, there is no proof that these properties hold for the actual implementation. This is why testing is still required.
  - Testing, as Dijkstra famously stated, (   )
- Hence, even a system certified at EAL7 must be suspected to contain security flaws.

But Testing Is Still Required…

- Formal Proofs are (   )
  - It does not matter which process was used to implement the software.
  - Shifting from (   ) to (   ) certification has an immense potential for simplification, saving costs, and making certification more meaningful at the same time.

Security Evaluation Standards

고려대학교 (Korea Univ.)
사이버국방학과 · 정보보호대학원 (CIST)
보안성분석평가연구실 (Security Analysis aNd Evaluation Lab.)

김 승 주 (Seungjoo Kim)
(FB) www.fb.com/skim71 (Twitter) @skim71