Foundations

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
Source: CNN

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

SAMSUNG
Common Criteria Certification for Samsung Multifunction Printers
WHITE PAPER

Common Criteria Certification for Samsung Multifunction Printers

Introduction

Overview

SAMSUNG

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

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

Definitions

Risk

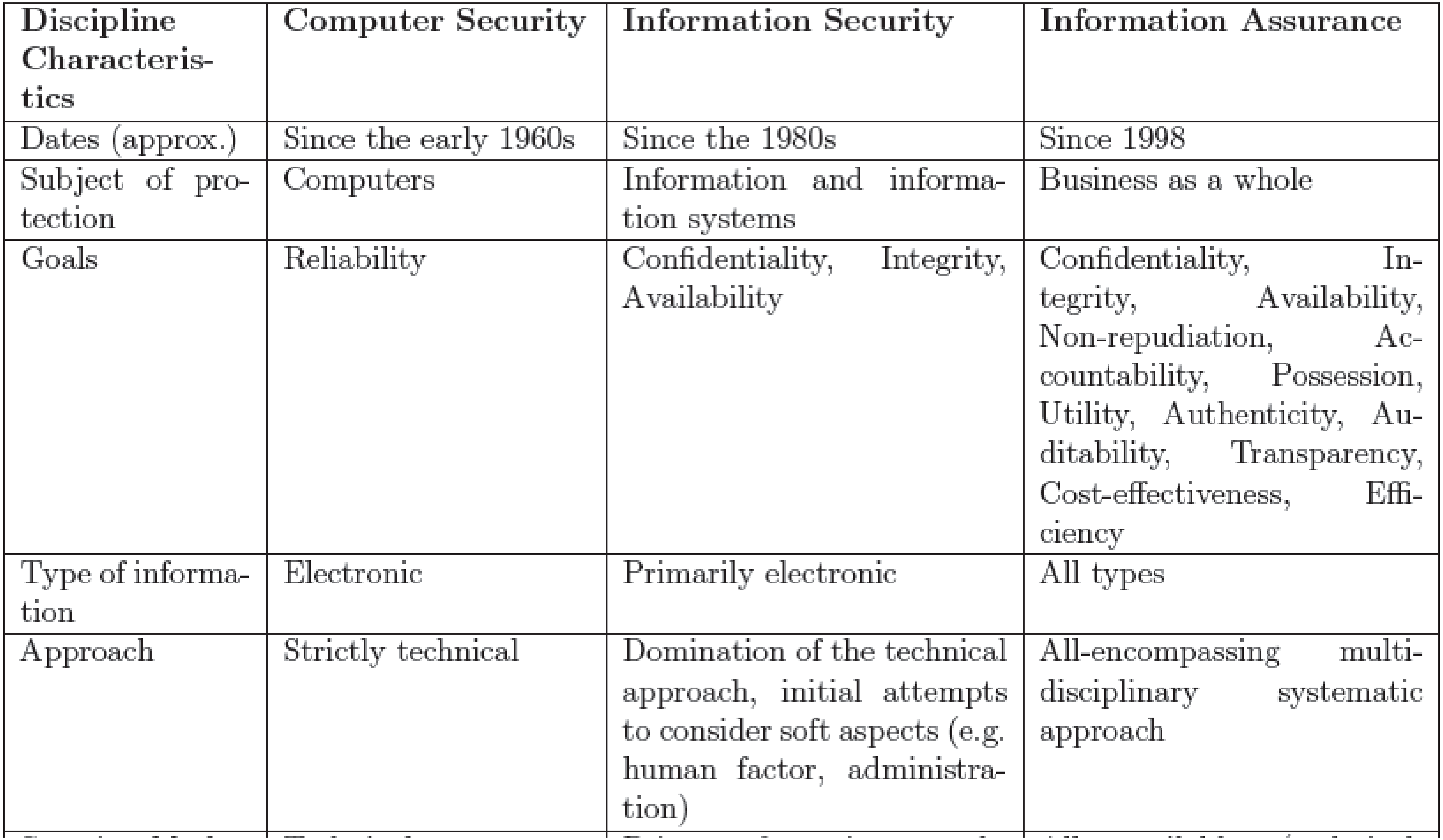
- Risk = Expected Asset Loss * Vulnerabilities * Threats
- ALE (Average Loss Expectancy) = probability of loss * total loss potential

Assets

- Software
- Hardware
- Data and Information
- Reputation

- Identification easy, valuation difficult
- Data, Information, Reputation – difficult to measure

Assets



Discipline Characteristics	Computer Security	Information Security	Information Assurance
Dates (approx.)	Since the early 1960s	Since the 1980s	Since 1998
Subject of protection	Computers	Information and information systems	Business as a whole
Goals	Reliability	Confidentiality, Integrity, Availability	Confidentiality, Integrity, Availability, Non-repudiation, Accountability, Possession, Utility, Authenticity, Auditability, Transparency, Cost-effectiveness, Efficiency
Type of information	Electronic	Primarily electronic	All types
Approach	Strictly technical	Domination of the technical approach, initial attempts to consider soft aspects (e.g. human factor, administration)	All-encompassing multidisciplinary systematic approach

Vulnerabilities

- Vulnerabilities = An error or a weakness in the design, implementation, or operation of a system.
  - Badly configured accounts
  - Programs with known flaws
  - Weak access control
  - Weak firewall configuration
  - Can be rated according to impact

Threats & Threat Agents

- Threats = Actions by adversaries who try to exploit vulnerabilities to damage assets

- Threat Agent = An adversary that is motivated to exploit a system vulnerability and is capable of doing so

Security Countermeasures

- Security countermeasure is about protecting assets. This involves:
  - Prevention
  - Detection
  - Reaction (recover/restore assets)

Confidentiality

- Prevent unauthorized disclosure of information.

- Confidentiality can be achieved through :

Integrity

- Prevent unauthorized modification of information.

- Integrity can be achieved through :
    -
    -

Availability

- For Computer Systems this means that :
  - Services are accessible and useable (without undue Delay) whenever needed by an authorized entity.
  - For this we need fault-tolerance.
  - Faults may be accidental or malicious (Byzantine).
  - Denial of Service attacks are an example of malicious attacks.

Accountability

- Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.

- For this,
  - Audit information must be kept and protected,
  - Access control is needed.

Non-repudiation

- Provide unforgeable evidence that a specific action occurred.

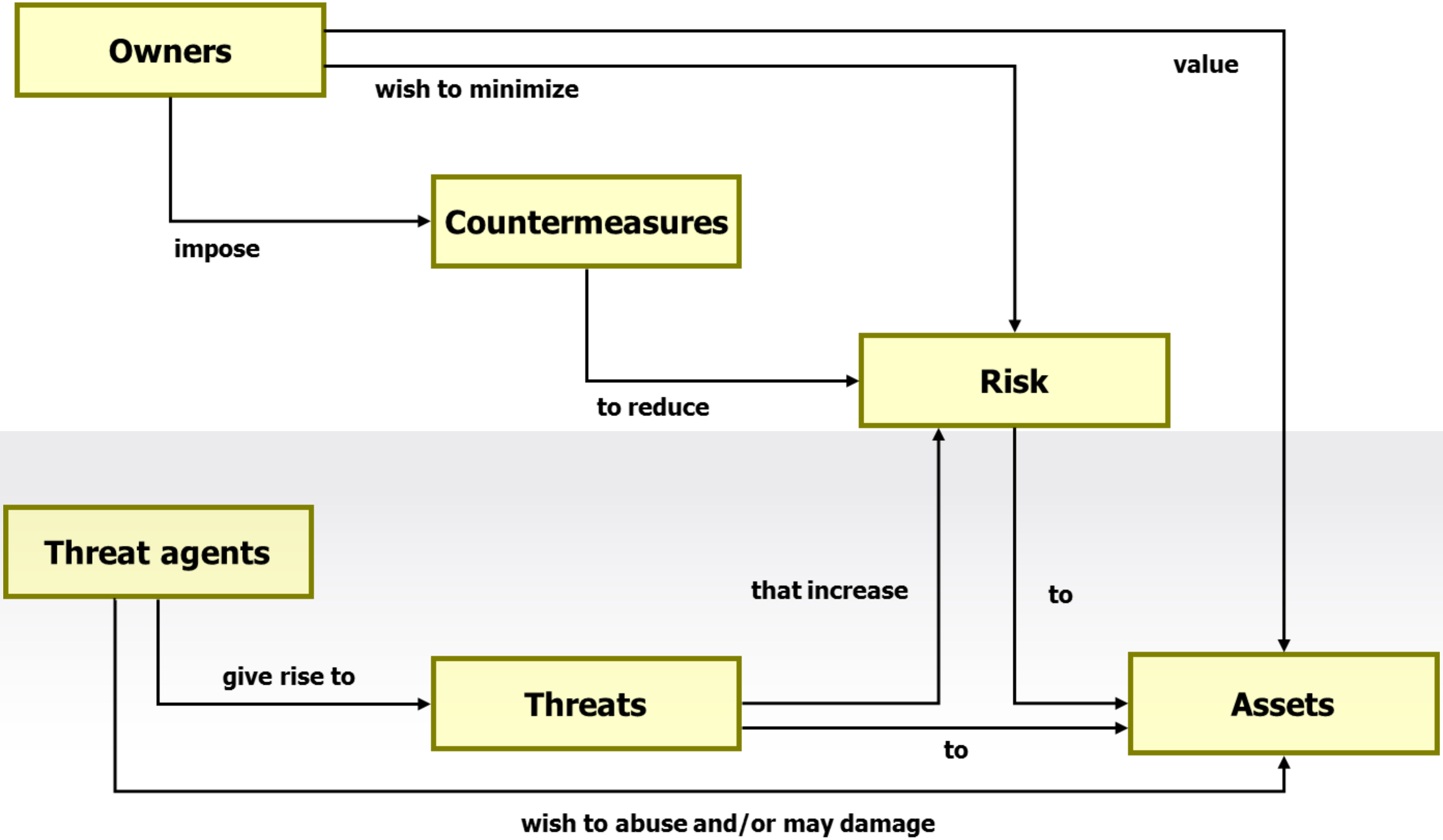
Dependability

- Dependability = Reliability (Accidental Failures) + Security (Intentional Failures)

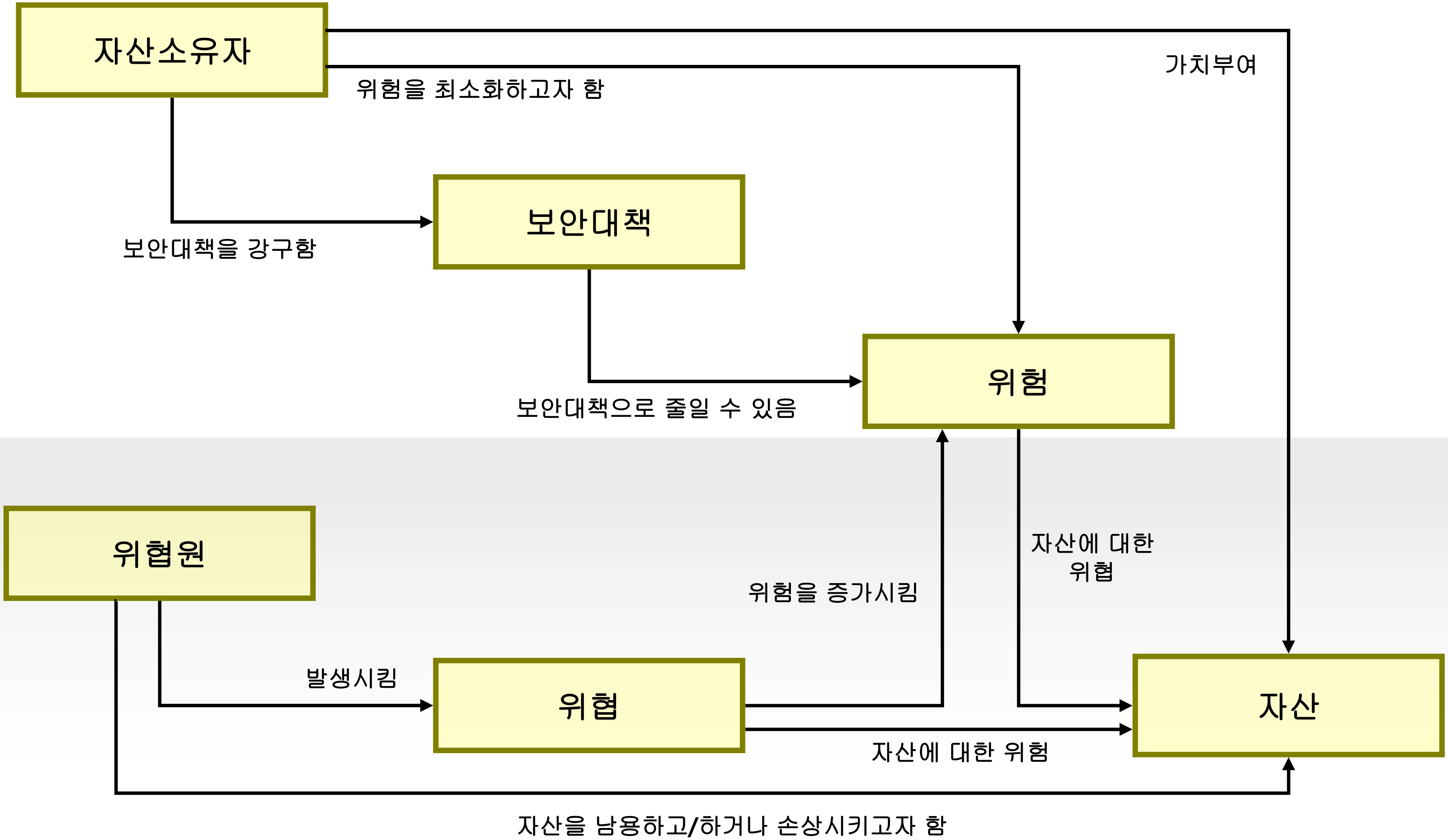
Survivability

- Deals with the recovery of the system after massive failure.

Relationships



Relationships



자산소유자

가치부여

위험을 최소화하고자 함

보안대책을 강구함

보안대책

위험

보안대책으로 줄일 수 있음

위협원

위험을 증가시킴

자산에 대한 위협

발생시킴

위협

자산

자산에 대한 위험

자산을 남용하고/하거나 손상시키고자 함

References

- Even at this general level there is disagreement on the precise definitions of some of the required security aspects.

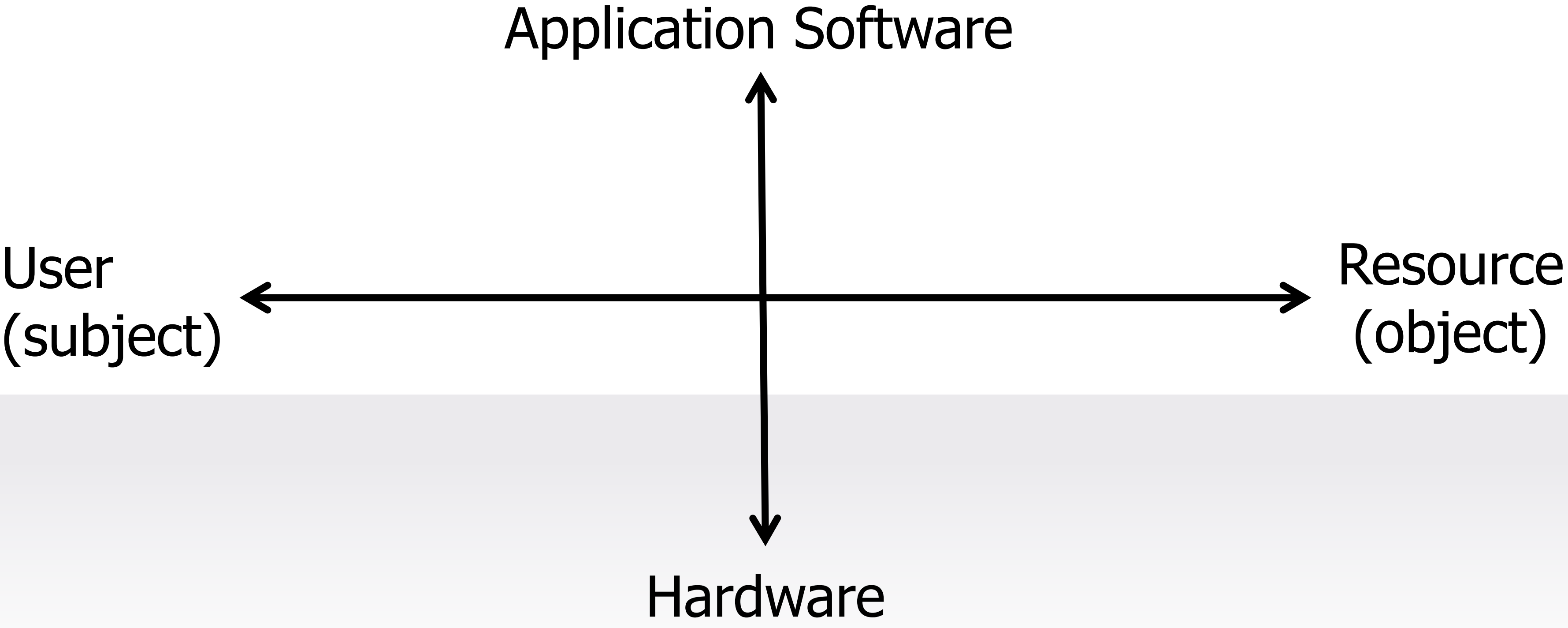
- References :
  - TCSEC or Orange book – US Dept of Defense, Trusted Computer System Evaluation Criteria.
  - ITSEC – European Trusted Computer System Product Criteria.
  - CTCPEC – Canadian Trusted Computer System Product Criteria

Fundamental Design Parameters

1st Design Decision

- **Focus of Control :** Should protection focus on data, operations or users?

1_{st} Design Decision



Application Software

User (subject)

Resource (object)

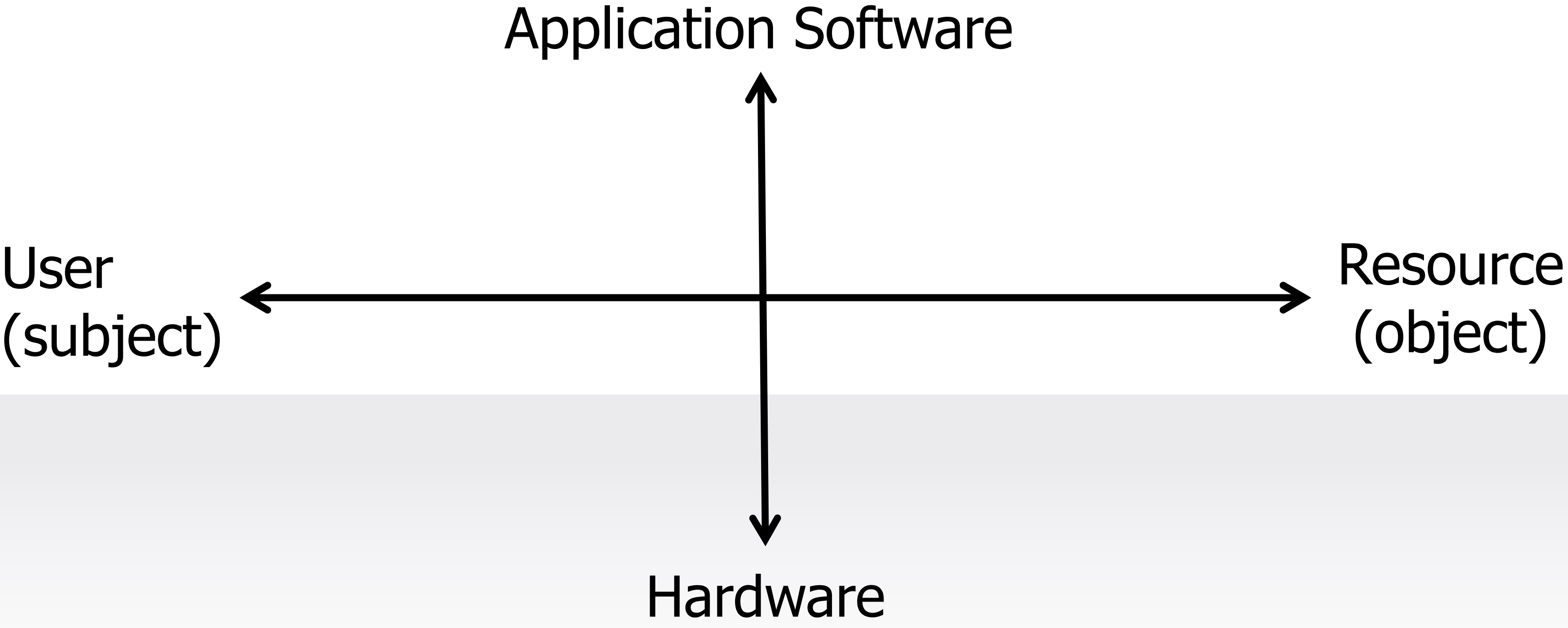
Hardware

The Dimensions of Computer Security

2nd Design Decision

- **The Man-Machine Scale :** In which layer should security be placed?

2nd Design Decision



Application Software

User (subject)

Resource (object)

Hardware

The Dimensions of Computer Security

3rd Design Decision

- **Complexity v.s. Assurance :** Should security focus on simplicity or security?
    - To achieve a high degree of assurance, the security system has to be examined in close detail and as exhaustively as possible. Hence there is an obvious trade-off between complexity and assurance. The (   ) an assurance level you aim for, the (   ) your system ought to be.

4th Design Decision

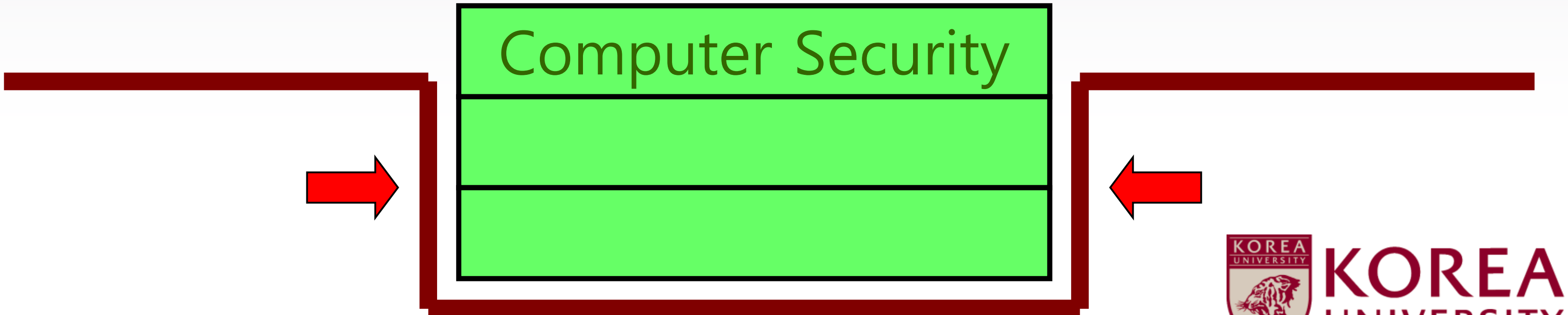
- **Centralized v.s. Decentralized :** Should security control tasks be given to a central entity of left to individual components?

5th Design Decision

- How to prevent the attacker from accessing the layer below the protection boundary?

5th Design Decision

- The Layer Below
  - An attacker with access to the (   ) is in a position to subvert protection mechanisms further up.
  - When you reach the stage where you cannot apply computer security mechanisms or do not want to do so, you can still put in place physical or organizational security mechanisms.



Physical and organizational security measures controlling access to the layer below

Foundations

고려대학교 (Korea Univ.)

사이버국방학과 · 정보보호대학원 (CIST)

보안성분석평가연구실 (Security Analysis aNd Evaluation Lab.)

김 승 주 (Seungjoo Kim)

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