Foundations

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

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

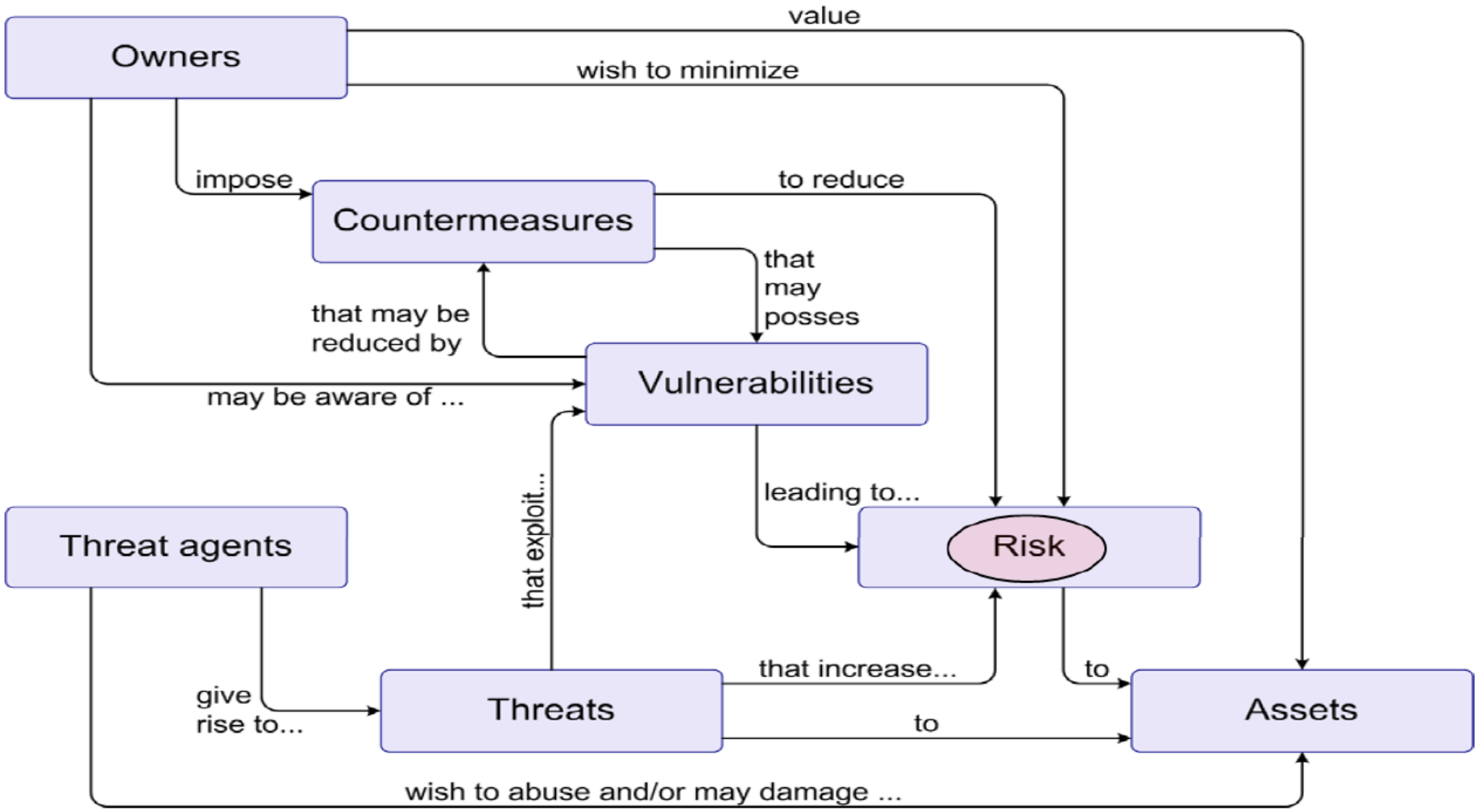
주요 R&D 성과

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

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

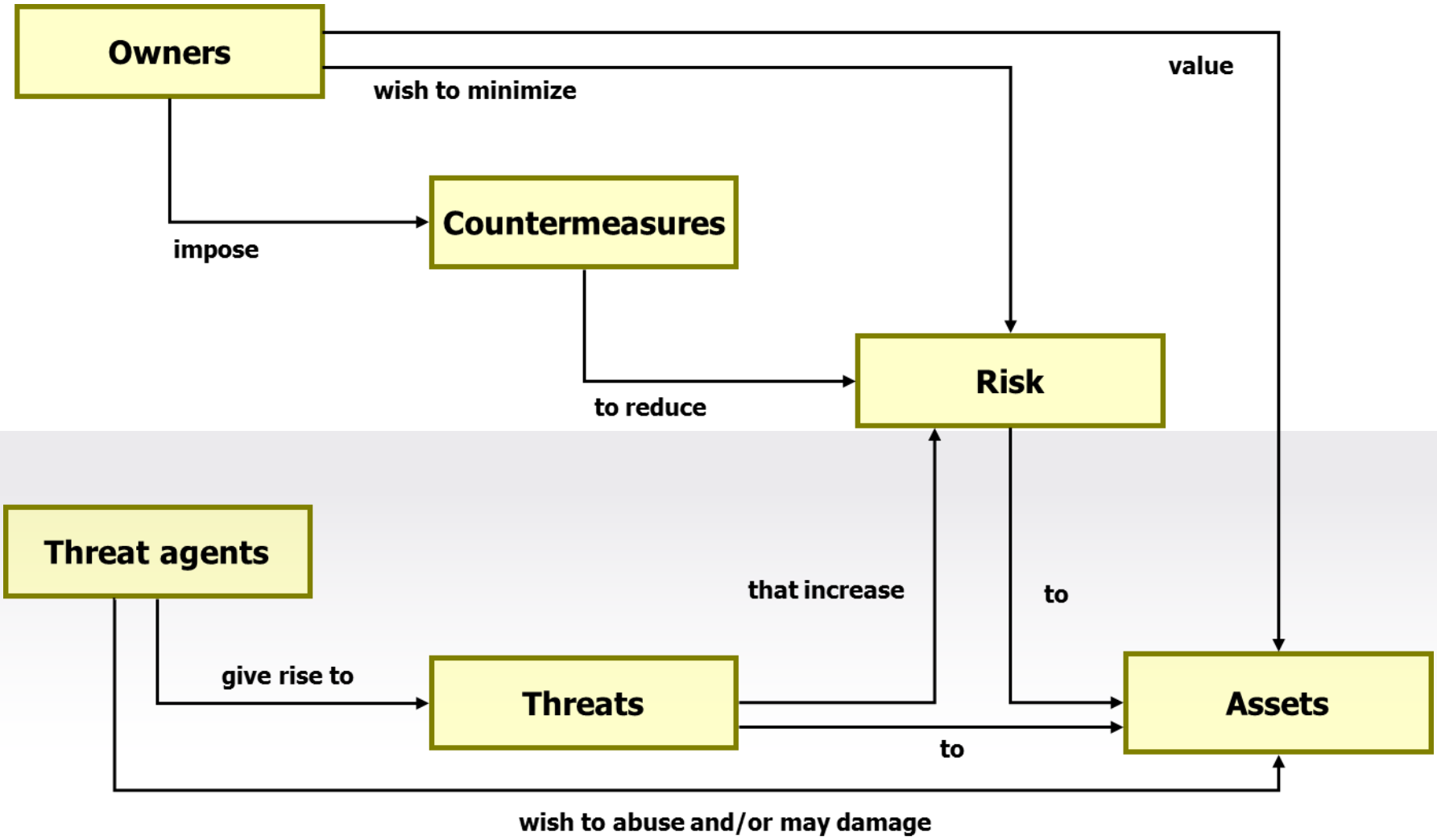
Definitions

The Security "Big Picture"



SOURCE: ISO/IEC 15408-1:2005, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*, Common Criteria v2.3, http://www.iso.ch

The Security "Big Picture"



KOREA UNIVERSITY

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

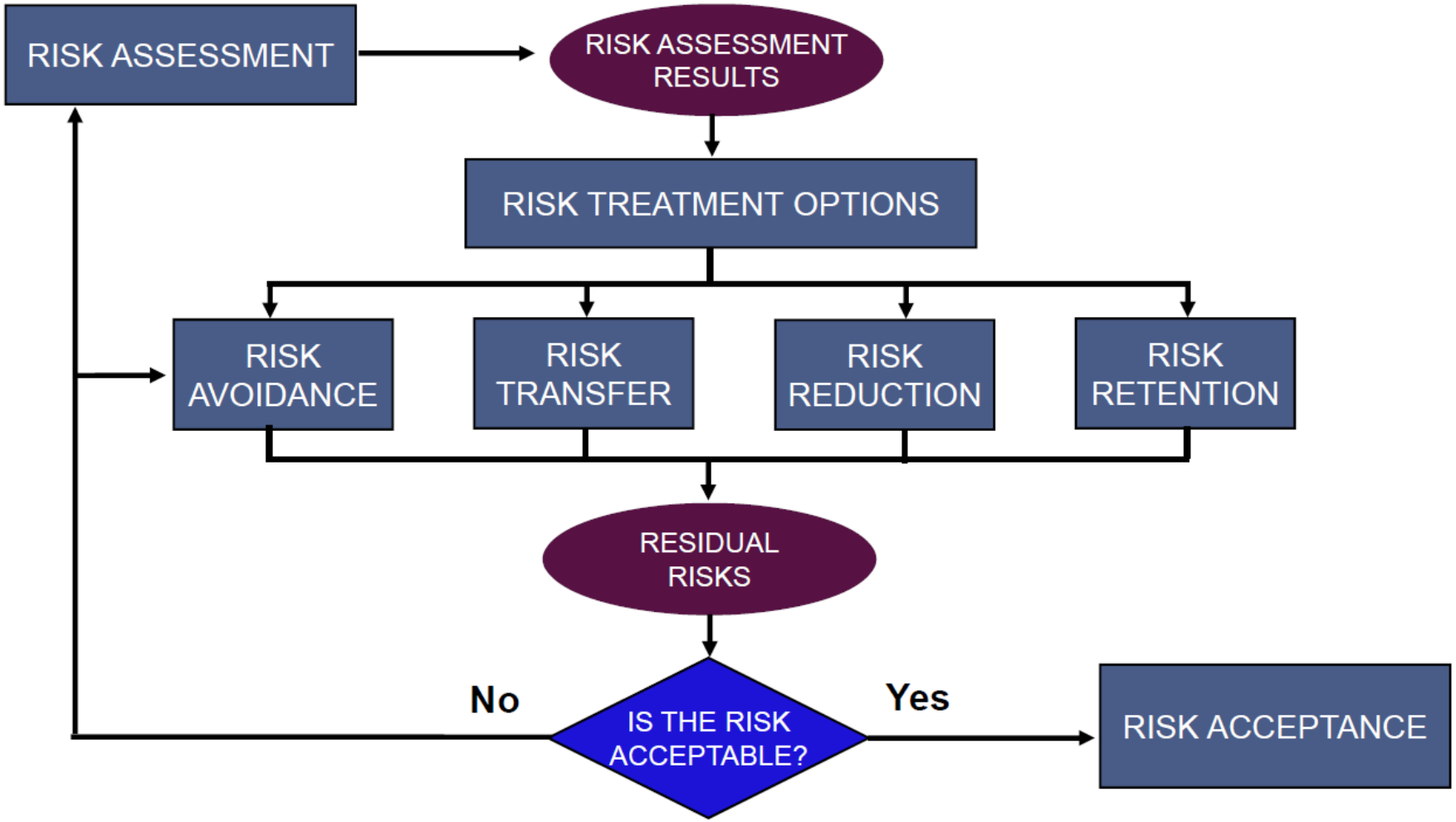
- **Vulnerabilities** = An error or a weakness in the design, implementation, or operation of a system.
  - Badly configured accounts
  - Programs with known flaws
  - Weak access control
  - Weak firewall configuration
  - Can be rated according to impact

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

Risk Treatment Decision-making Process



BASED ON: ISO/IEC 27005:2008, *Information technology -- Security techniques – Information Security Risk Management*, http://www.iso.ch

Trusted & Trustworthy

- **Trusted** system or component is one whose failure can break the security policy.

- **Trustworthy** system or component is one that won't fail.

Security Engineering

- Security engineering is about building systems to remain dependable in the face of **malice**, **error**, or **mischance**.

- As a discipline, it focuses on the tools, processes, and methods needed to **design**, **implement**, and **test** complete systems, and to **adapt** existing systems as their environment evolves.

Security Engineering

- Security engineering requires **cross-disciplinary expertise**, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of economics, applied psychology, organizations and the law.

Fundamental Design Principles

Saltzer's 8 Fundamental Principles

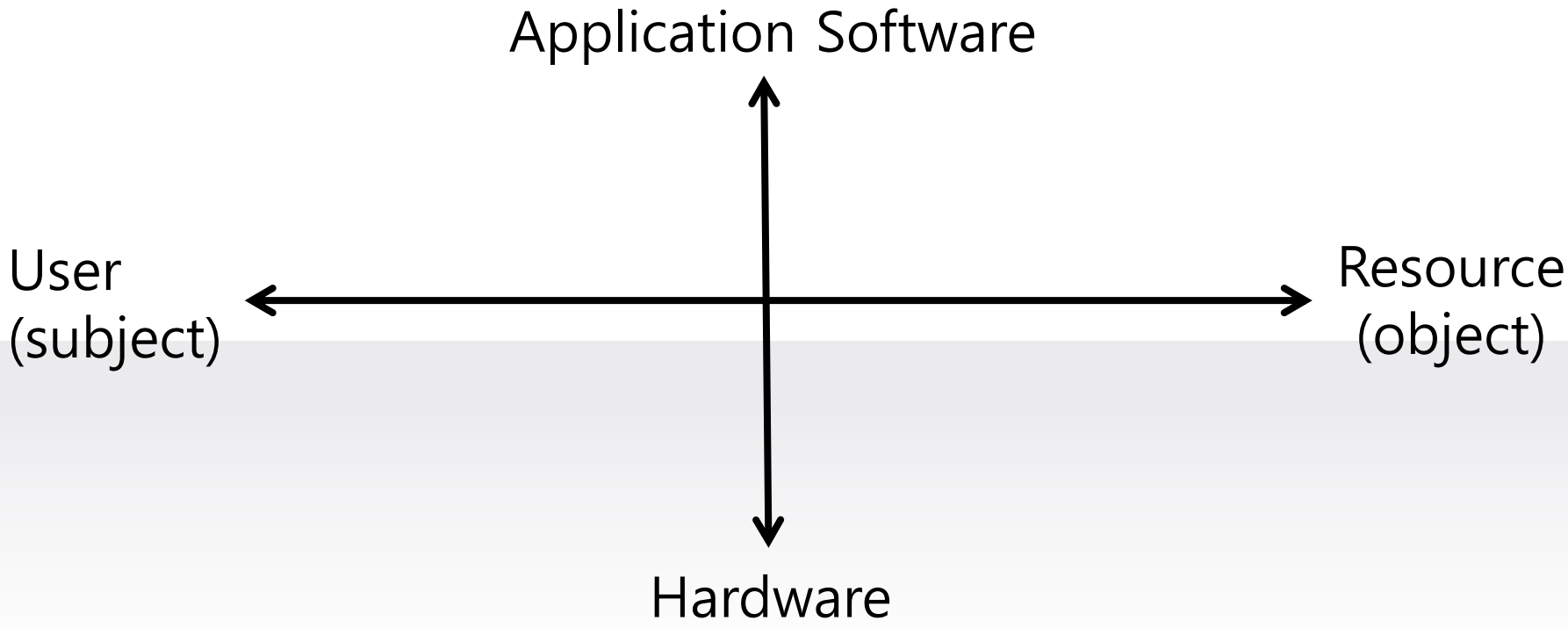
- Saltzer and Schroeder describe eight principles for the design and implementation of security mechanisms. The principles draw on the ideas of **simplicity** and **restriction**.

☞ J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems," Proceedings of the IEEE 63 (9), pp. 1278–1308 (Sep. 1975).

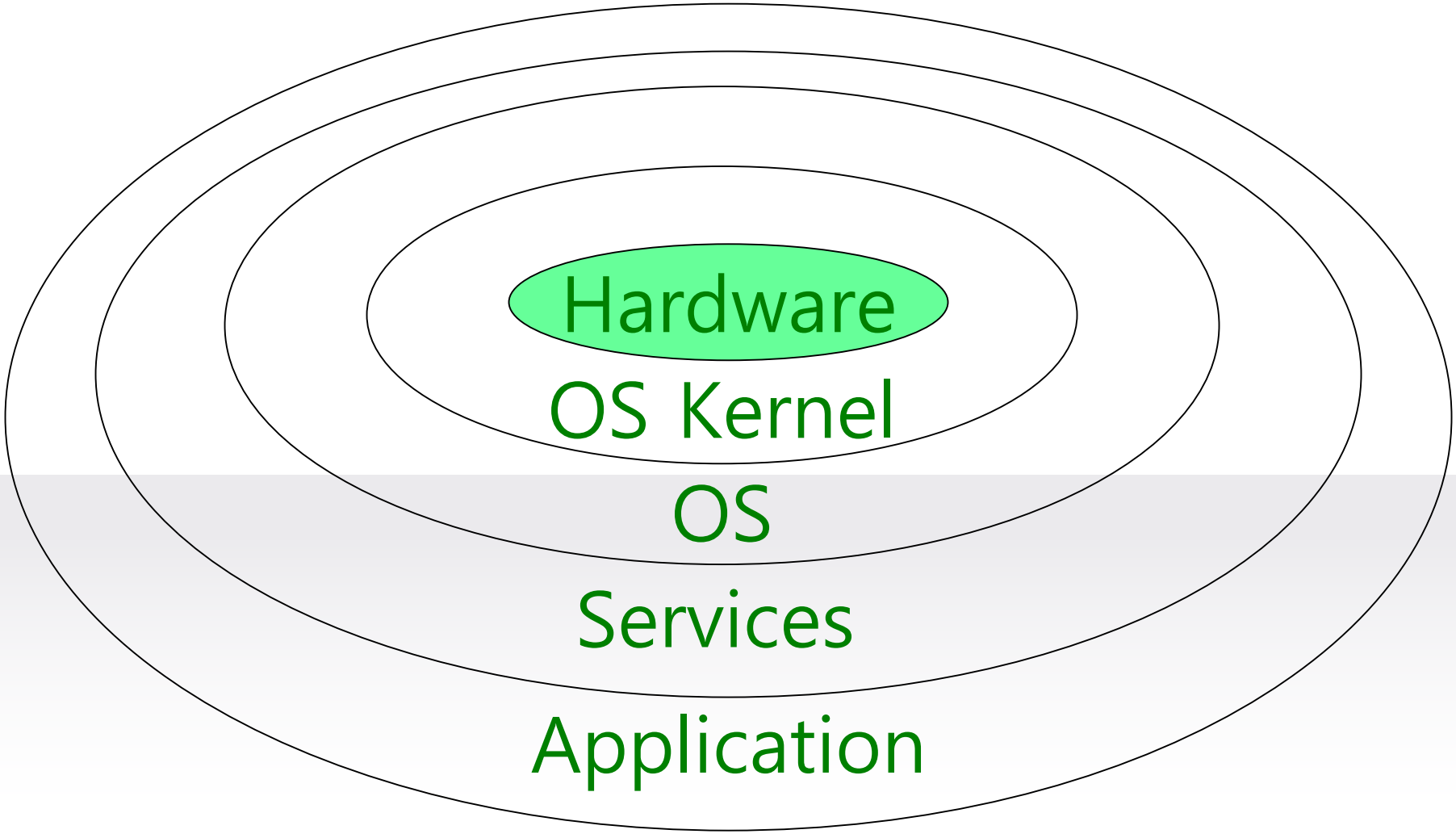
Saltzer's 8 Fundamental Principles

1. Principle of Least Privilege
2. Principle of Fail-Safe Defaults
3. Principle of Economy of Mechanism
4. Principle of Complete Mediation
5. Principle of Open Design
6. Principle of Separation of Privilege
7. Principle of Least Common Mechanism
8. Principle of Psychological Acceptability

Ext.1 The Dimensions of COMPUSEC



Ext.2 Onion Model of Protection



Ext.3 Centralized v.s. Decentralized

- Should security control tasks be given to a central entity of left to individual components?

Foundations

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