Foundations

고려대학교 (Korea Univ.)

사이버국방학과 · 정보보호대학원 (CIST)

보안성분석평가연구실 (Security Analysis aNd Evaluation Lab.)

김 승 주 (Seungjoo Kim)

www.kimlab.net

보안성분석평가연구실

Security Analysis aNd Evaluation Lab

sane.korea.ac.kr / www.kimlab.net

김승주 교수 (skim71@korea.ac.kr)

로봇융합관 306호

연구분야

- Security Engineering for Building High-Assurance Systems (e.g. End-to-End Provably Secure Micro Kernel)
- Recent Security Threat Analysis and Security Evaluation (e.g. CMVP, CC, ISMS)
- All Areas of Security, from Crypto to Hacking, and Policy

주요 연구성과

MBC 뉴스데스크
(2013.5.10.)

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 조교수, 부교수
2011.3~현재) 고려대학교 사이버국방학과·정보보호대학원 정교수
Founder / Advisory Director of SECUINSIDE

前) 선관위 디도스 특별검사팀 자문위원
前) SBS 드라마 '유령' 및 영화 '베를린' 자문
現) 한국정보보호학회 이사
現) 대검찰청 디지털수사 자문위원
現) 방송통신위원회 정보통신망침해사고 민관합동조사단 위원
現) 육군사관학교 초빙교수

- '96: Convertible group signatures (AsiaCrypt)
- '97: Proxy signatures, revisited (ICICS): 630회이상 인용
- '06: 국가정보원 암호학술논문공모전 우수상
- '07: 국가정보원장 국가사이버안전업무 유공자 표창
- '12: 고려대학교 석탑강의상
- '13: Smart TV Security (CanSecWest 및 Black Hat): 스마트TV 해킹(도청·도촬) 및 해적방송 송출 시연

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.
  -
  -
  -

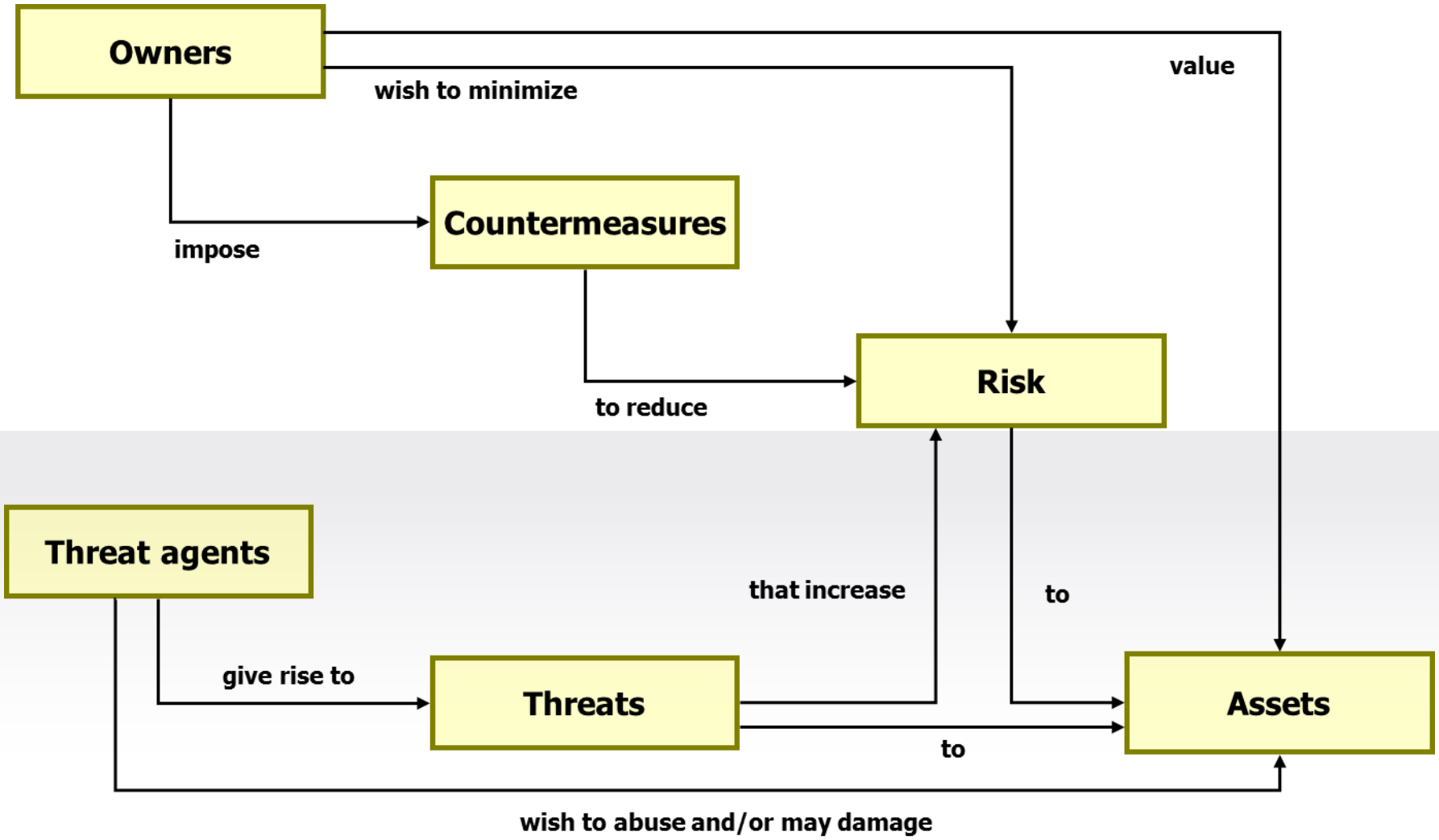
Dependability

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

Survivability

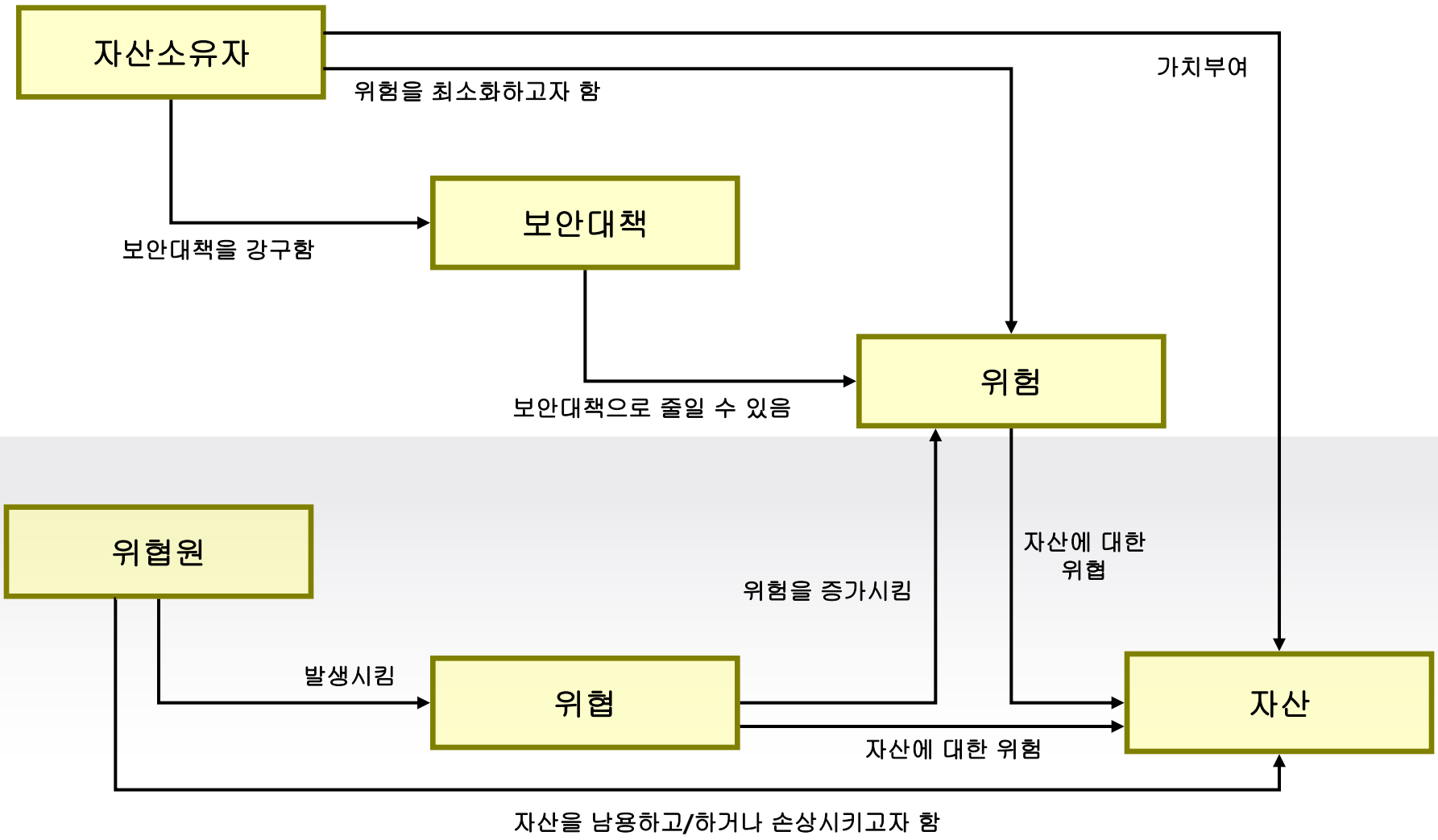
- Deals with the recovery of the system after massive failure.

Relationships



KOREA UNIVERSITY

Relationships



KOREA UNIVERSITY

References

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

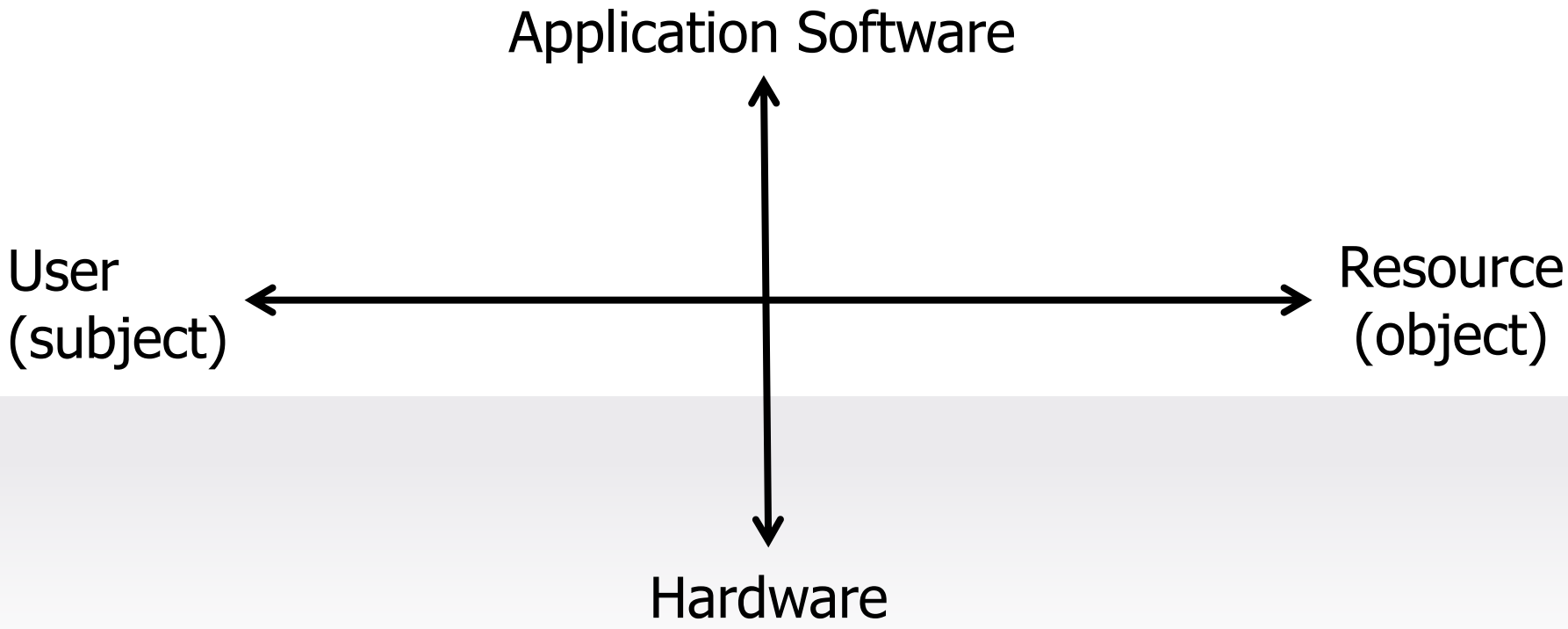
- References :
  - TCSEC or Orange book – US Dept of Defense, Trusted Computer System Evaluation Criteria.
  - ITSEC – European Trusted Computer System Product Criteria.
  - CTCPEC – Canadian Trusted Computer System Product Criteria

Fundamental Design Parameters

1_{st} Design Decision

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

1_{st} Design Decision

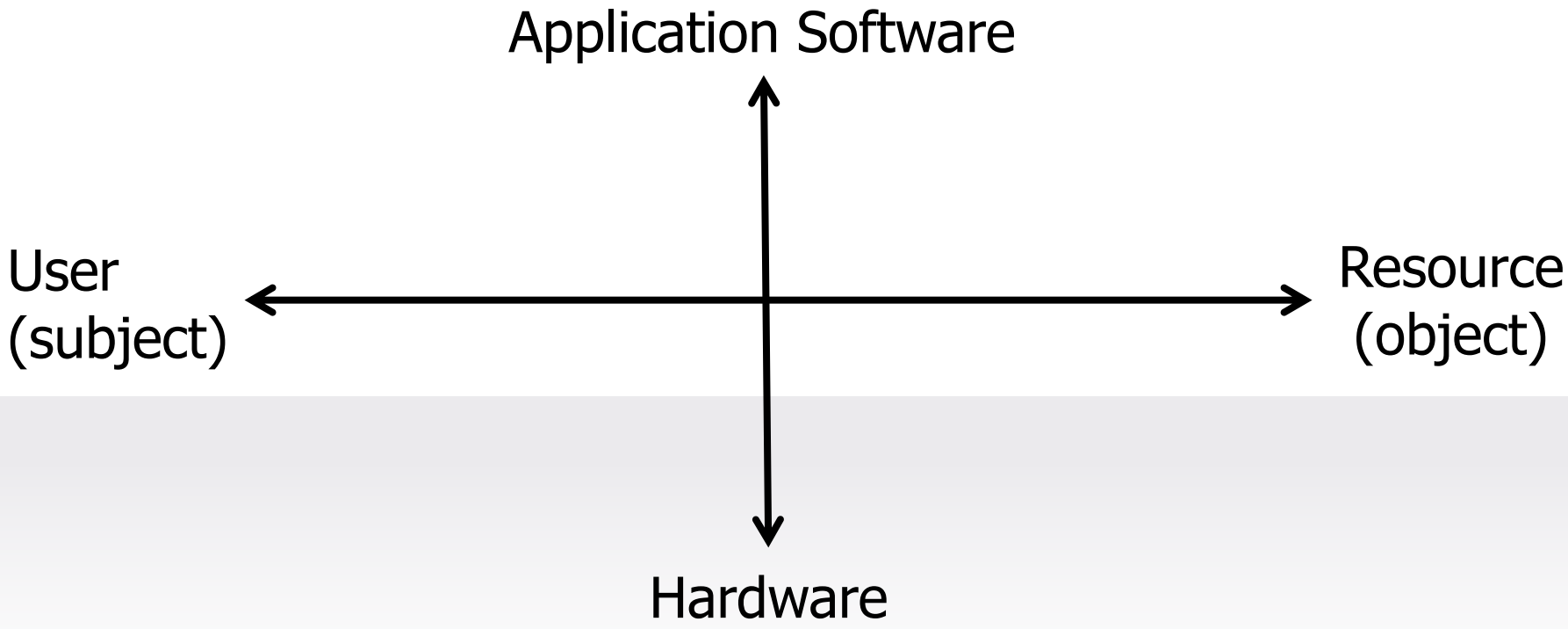


The Dimensions of Computer Security

2_{nd} Design Decision

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

2_{nd} Design Decision



The Dimensions of Computer Security

3_{rd} 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.

4_{th} Design Decision

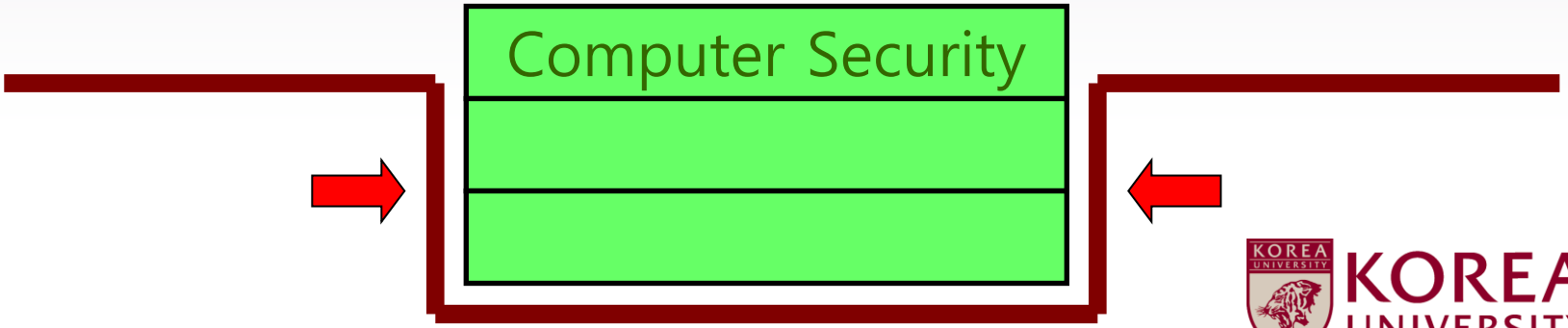
- **Centralized v.s. Decentralized :** Should security control tasks be given to a central entity of left to individual components?

5_{th} Design Decision

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

5_{th} 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

고려대학교 정보보호대학원 KOREA UNIVERSITY