<FISC 2008>

# Security Issues in Future Internet

2008. 8. 26

School of EE
Seoul National University
Seung-Woo Seo

CNS Lab

# Contents

- Review on security
- Crypto and authentication protocols
- Security in TCP/IP
- Motivations for security researches for FI
- Integrated dependability and security evaluation
- Conclusions

CNS Lab

# What is Security?

- Managing a malicious adversary
- Guaranteeing properties even if a malicious adversary tries to attack

- Basic security analysis
  - What are we protecting?
  - Who is the adversary?
  - What are the security requirements?
  - What security approaches are effective?

# Security Goals

- Confidentiality: restricted to legitimate members
- Integrity: no modification or deletion in any unauthorized way
- Authentication: verification of the actual sender
- Access Control: access allowed to only authorized parties
- Non-repudiation: The sender cannot deny sending the message
- No denial-of-service: sustaining of the service
- And many others …

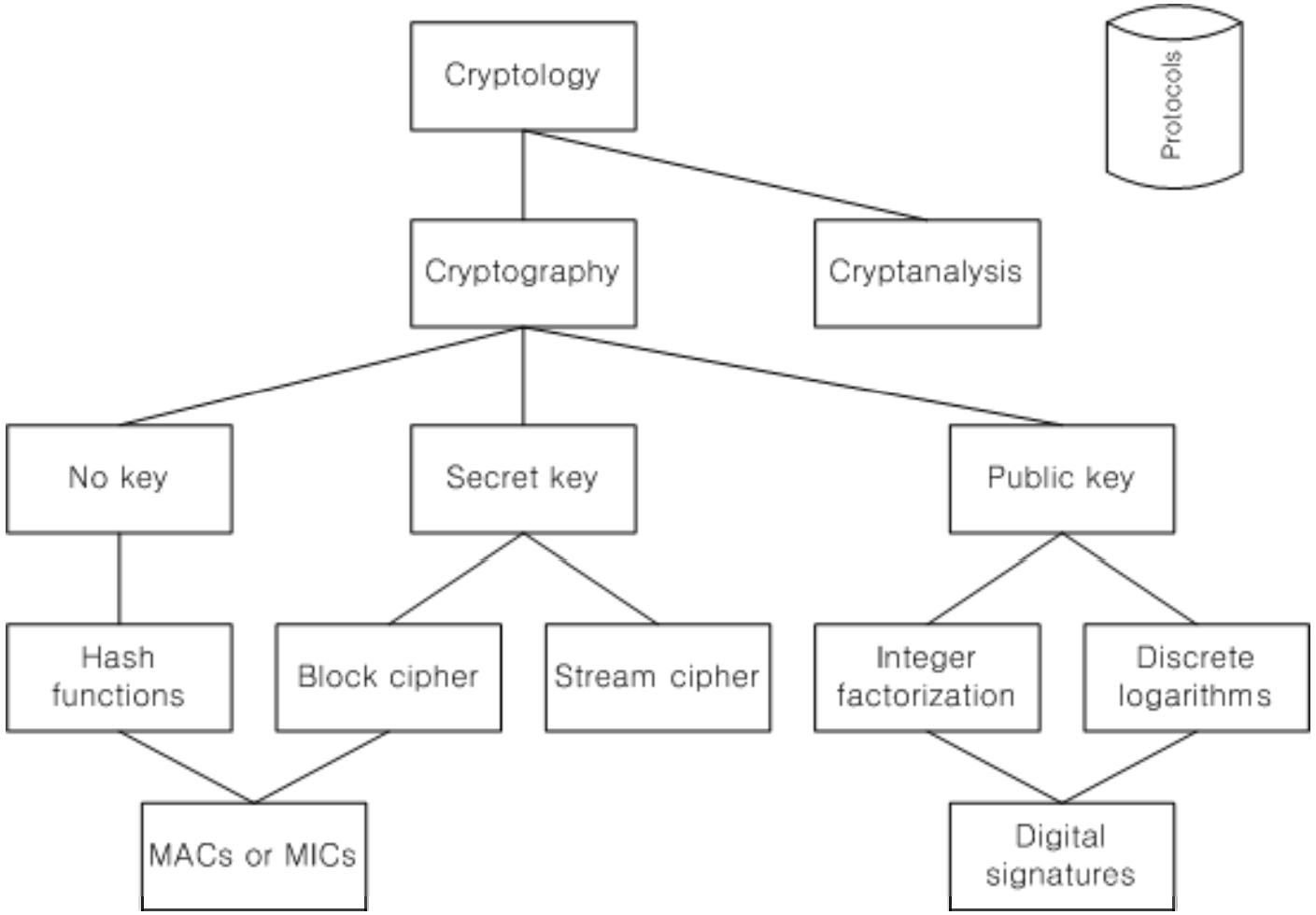
# Basic Approaches for Security

- Prevention
  - Attack prevention mechanisms used to prevent or complicate specific attacks
- Detection and recovery
  - Attack detection mechanism is in place, recovery phase initiated after attack detected
- Resilience
  - Despite undetected attacks, security property continues to hold
- Deterrence
  - Use of legal system to provide disincentive for attacks
- How can these approaches be used to achieve secrecy, integrity, availability?

# Crypto and Authentication Protocols

CNS Lab

# Taxonomy of Cryptography




From "Information Assurance" by Qian, et al.

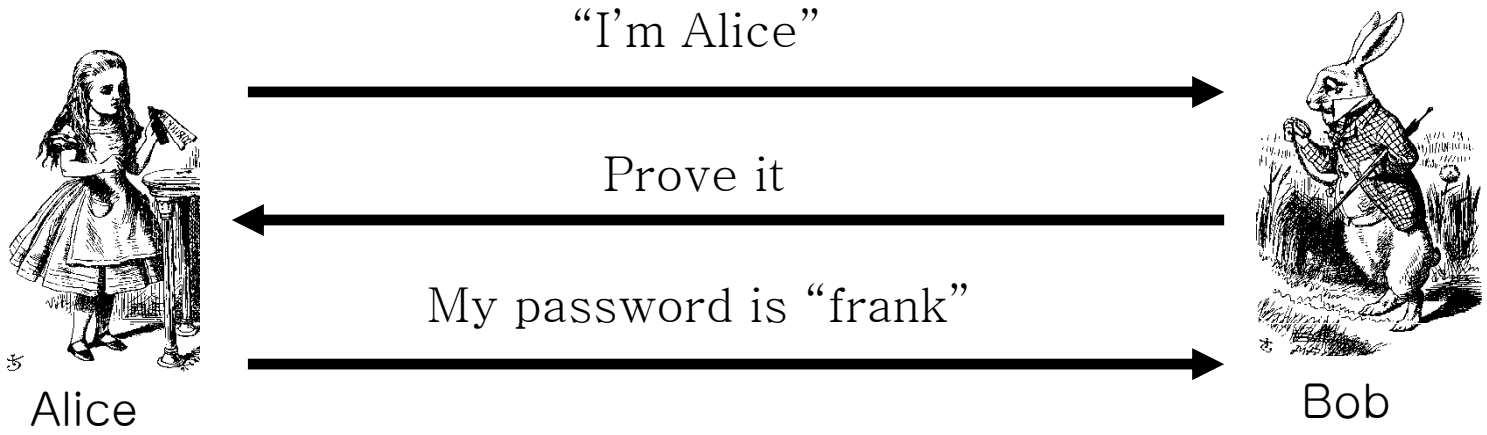
# Authentication

- Alice must prove her identity to Bob
  - Alice and Bob can be humans or computers
- May also require Bob to prove he is Bob (mutual authentication)
- May also need to establish a session key
- May have other requirements, such as
  - Use only public keys
  - Use only symmetric keys
  - Use only a hash function
  - Anonymity, plausible deniability, etc., etc.

# Authentication

- Authentication on a stand-alone computer is relatively simple
  - "Secure path" is the primary issue
  - Main concern is an attack on authentication software
- Authentication over a network is much more complex
  - Attacker can passively observe messages
  - Attacker can replay messages
  - Active attacks may be possible (insert, delete, change messages)

# Simple Authentication

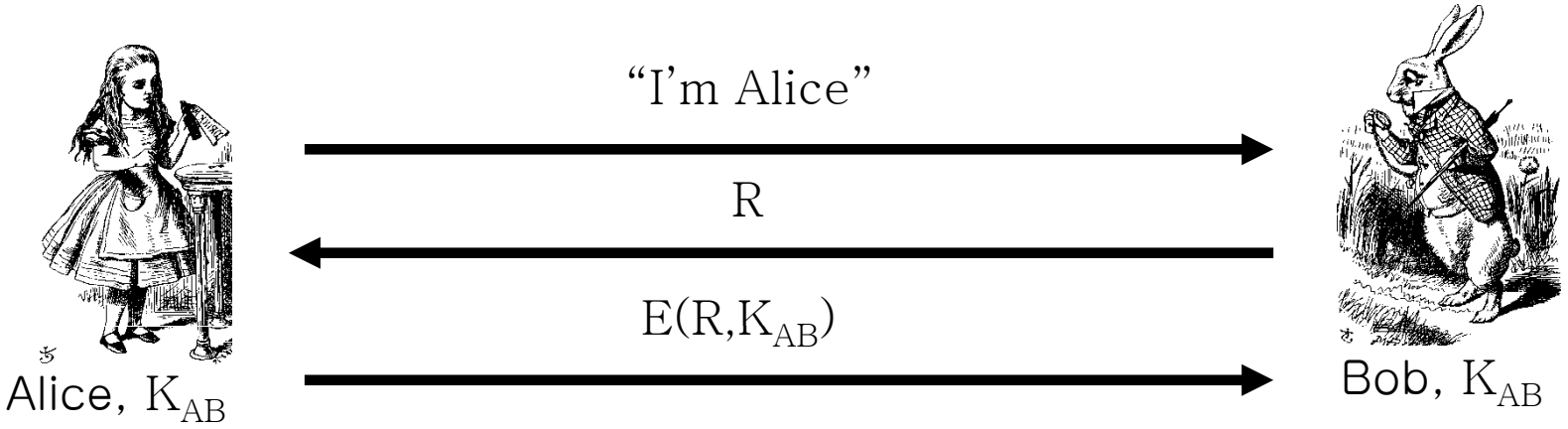



- Simple and may be OK for standalone system
- But insecure for networked system
  - Subject to a replay attack
  - Bob must know Alice's password

# Challenge-Response

- To prevent replay, challenge-response used
- Suppose Bob wants to authenticate Alice
  - Challenge sent from Bob to Alice
  - Only Alice can provide the correct response
  - Challenge chosen so that replay is not possible
- How to accomplish this?
  - Password is something only Alice should know…
  - For freshness, a "number used once" or **nonce**

# Authentication with Symmetric Key




- Secure method for Bob to authenticate Alice
- Alice does not authenticate Bob
- Can we achieve mutual authentication?

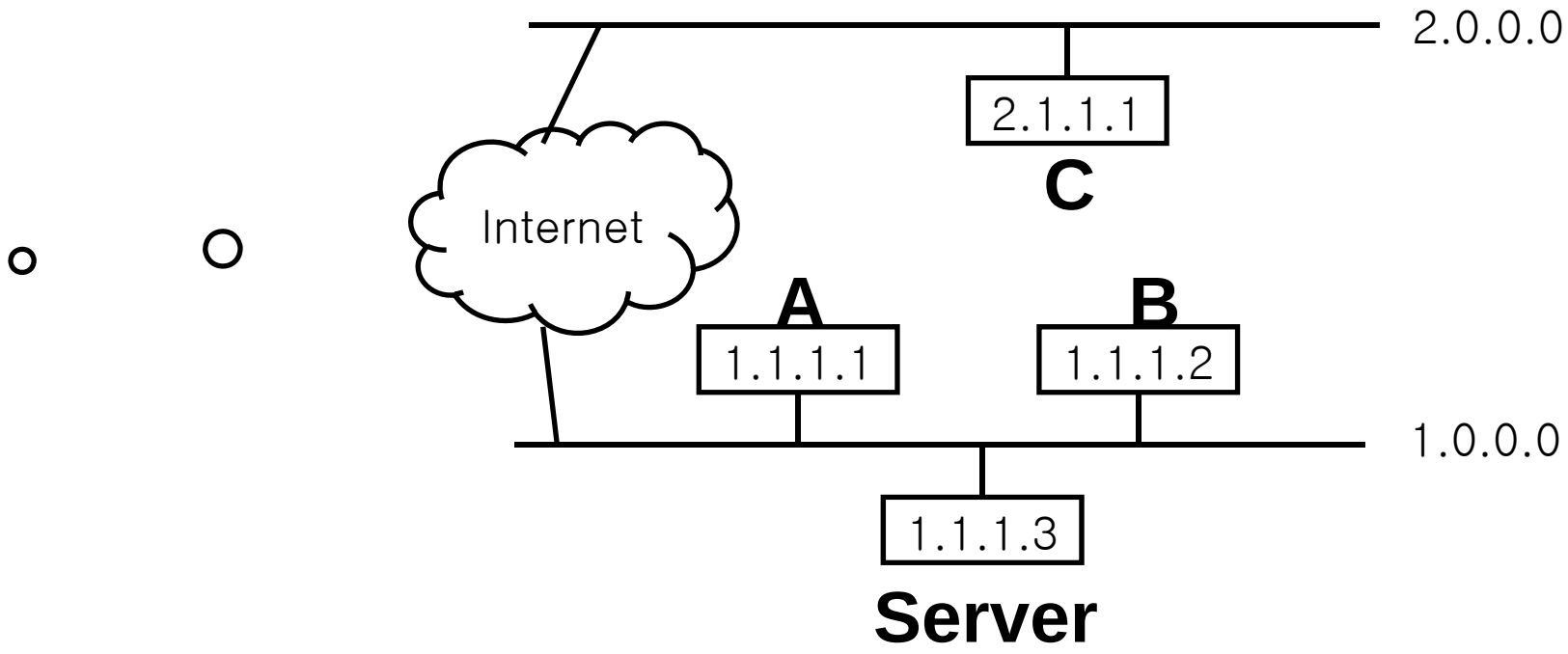
# Security in TCP/IP

Slides by Adrian Perrig

# "Security Problems in the TCP/IP Protocol Suite"

- Paper by Steven Bellovin
- Interesting historical perspective
- Wakeup call for networking researchers, listing many security vulnerabilities
- Some of the possible attacks
  - IP level attacks
  - TCP level attacks
  - Routing attacks
  - ICMP attacks
  - Application-level attacks

# Security Issues in Broadcast Networks




- Security issues for communication between A, B, C, and Server?

# Other IP Level Attacks

- IP fragment attack
  - Host stores fragments until entire packet arrives
  - Attack: send individual fragments only, host wastes memory to store them
  - Countermeasure?
- Smurf attack
  - Send packet with broadcast address to network, spoofing victim
  - All hosts on the network will send reply packet to victim
  - This is called a reflector attack, in this case the reflector also performs traffic amplification

# TCP Level Attacks: TCP Primer

- TCP provides reliable data transfer using the best effort IP service
- Typical TCP packet exchange
  - A → B: SYN($ISN_A$)
  - B → A: SYN($ISN_B$), ACK($ISN_A$)
  - A → B: ACK($ISN_B$)
  - A → B: data …
- Issues?

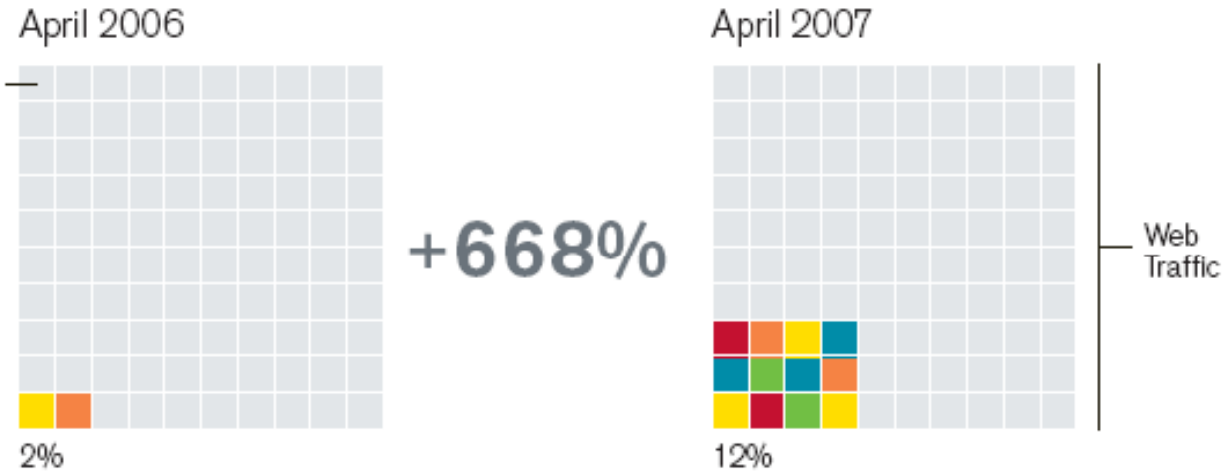
# Other TCP Level Attacks

- TCP SYN flooding
  - Exploit state allocated at server after initial SYN packet
  - Extensive flooding exhausts server's memory
- TCP hijacking
  - If TCP sequence numbers are known, attacker can inject malicious information into TCP stream
- TCP poisoning
  - Inject random data into TCP stream to shut down TCP connection
  - Does sequence number need to be known?
  - How many packets are required?

# Motivation for Security Research in FI

# Status of Internet

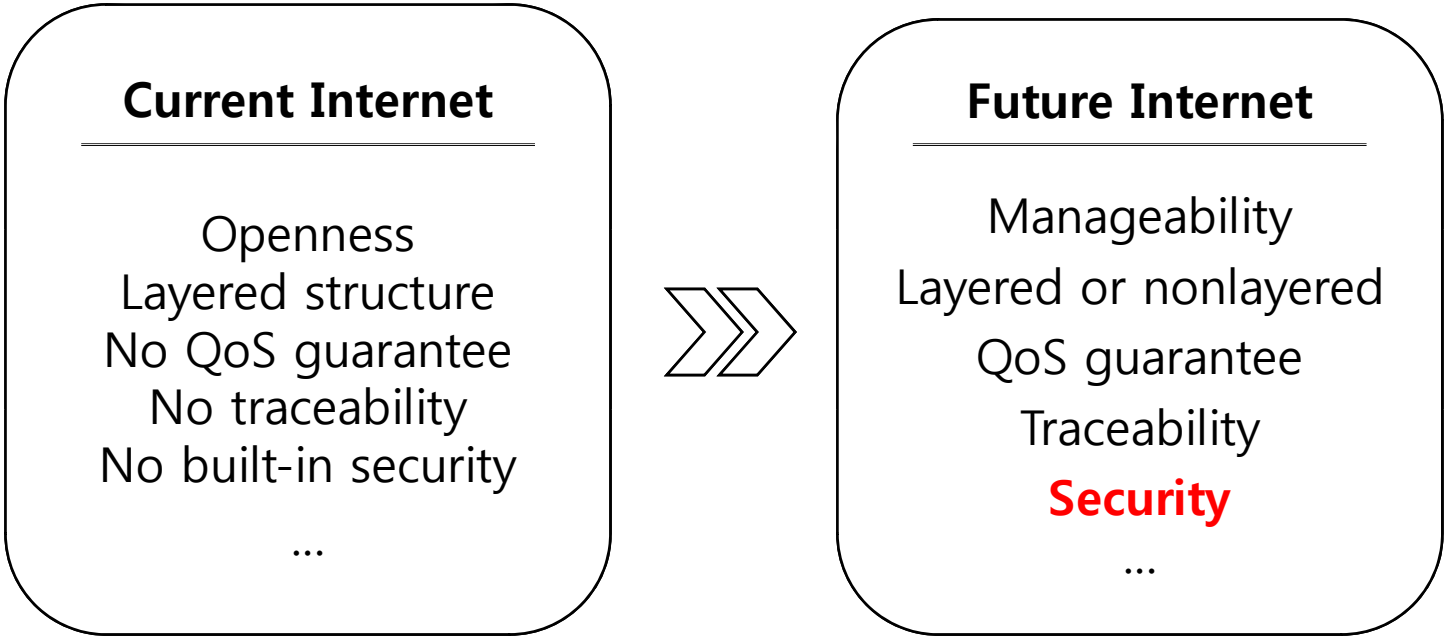
- Driving engine for economy and social networking
  - In Korea, market size has grown  up to $5370Billion in 2006
  - Social networking traffic like CyWorld has increased up to 12% of total Web traffic in 2007 (BusinessWeek, 2007.6.)




- Very diverse requirements for Internet

CNS Lab

# Necessity of Future Internet



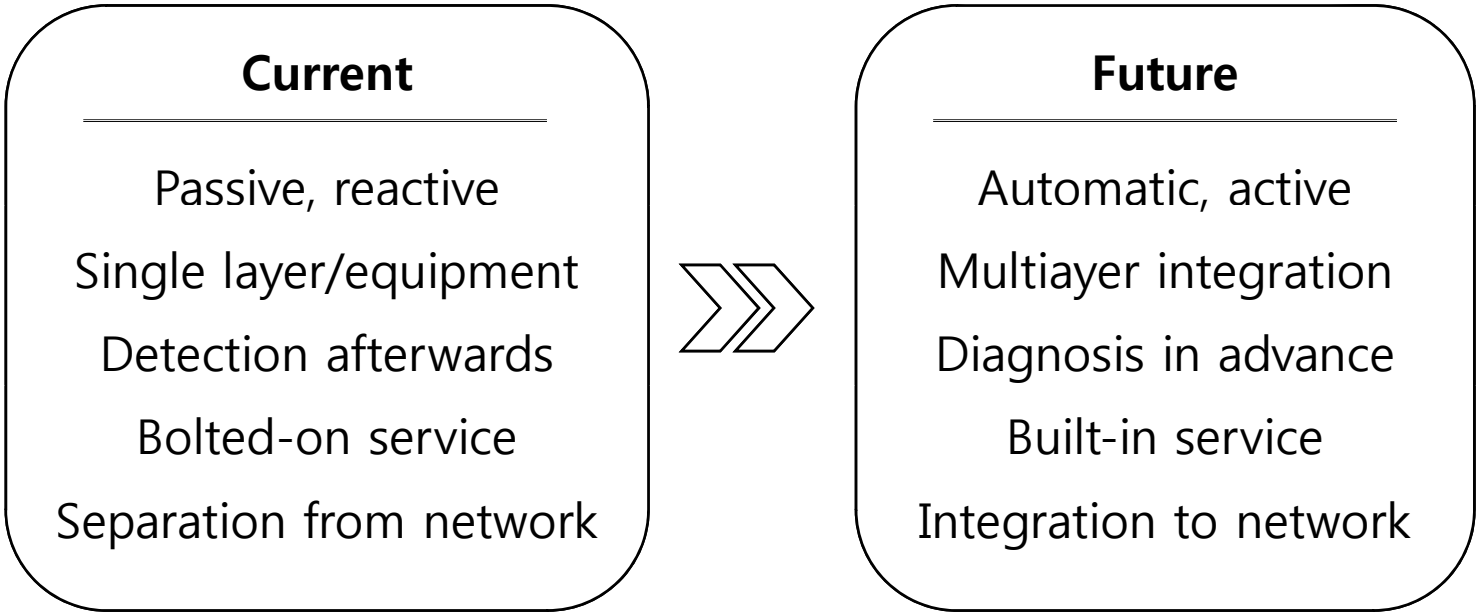

- Research on Future Internet under diverse requirements has just begun

CNS Lab

# Current Status of Internet Security

- Limitation on current security technology
  - Separation of security function from network
    - Independent deployment of virus vaccine, spam filter, IDS, Firewall, VPN, etc. in each layer and application whenever necessary
  - Passive detection and prevention
    - Passive reaction by relying on the decision of human
    - Long delay until action, which allows additional attacks
  - More importantly, integrated end-to-end security measures are not available
    - Local detection of worm, DDoS and Bot
    - Each domain has its own security measures
    - No correlation among security technologies
    - No integrated end-to-end security measures

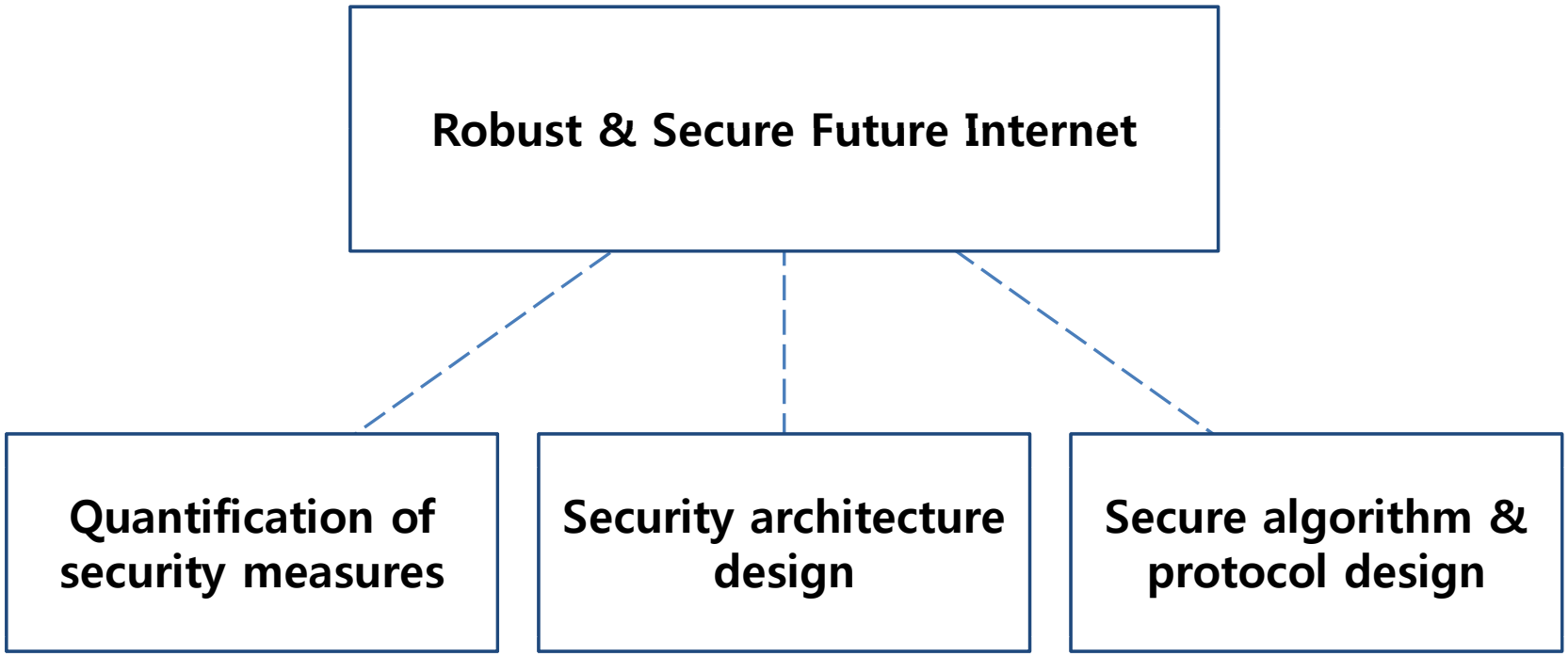
# Change of Security Service Paradigm




⇒ Security is no more an option, but a necessity that should be considered at the initial stage of network design.

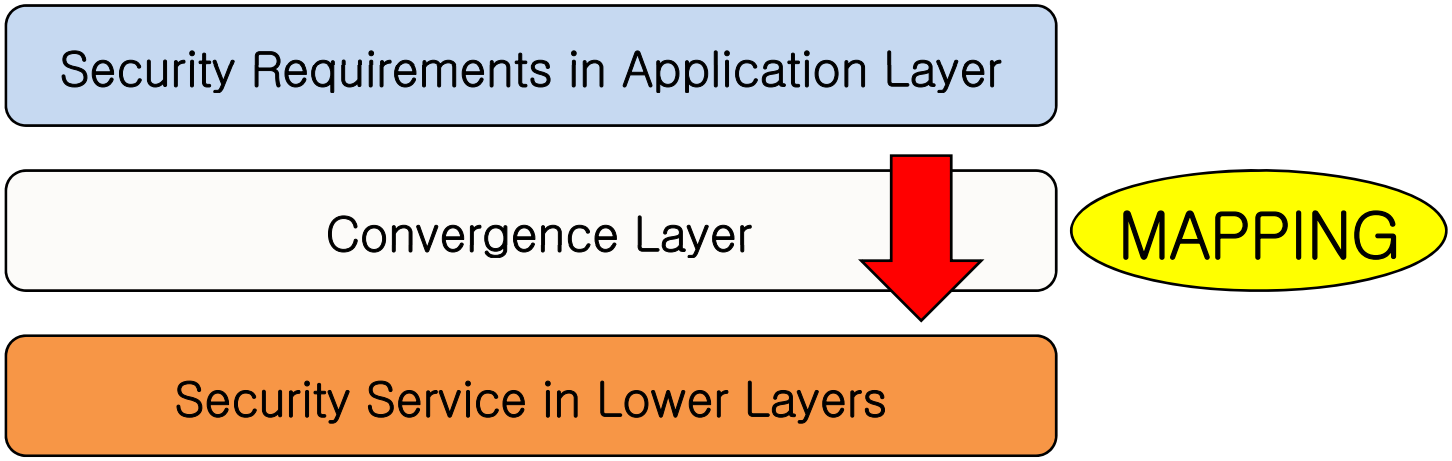
CNS Lab

# Direction of Security Research for FI




CNS Lab

# Mapping of Security Requirements




- Classification of security levels
  - Service profiling for security requirements
  - Classification and mapping to network configurations
- Network service
  - Secure and robust service in network layer which is resilient to external perturbation

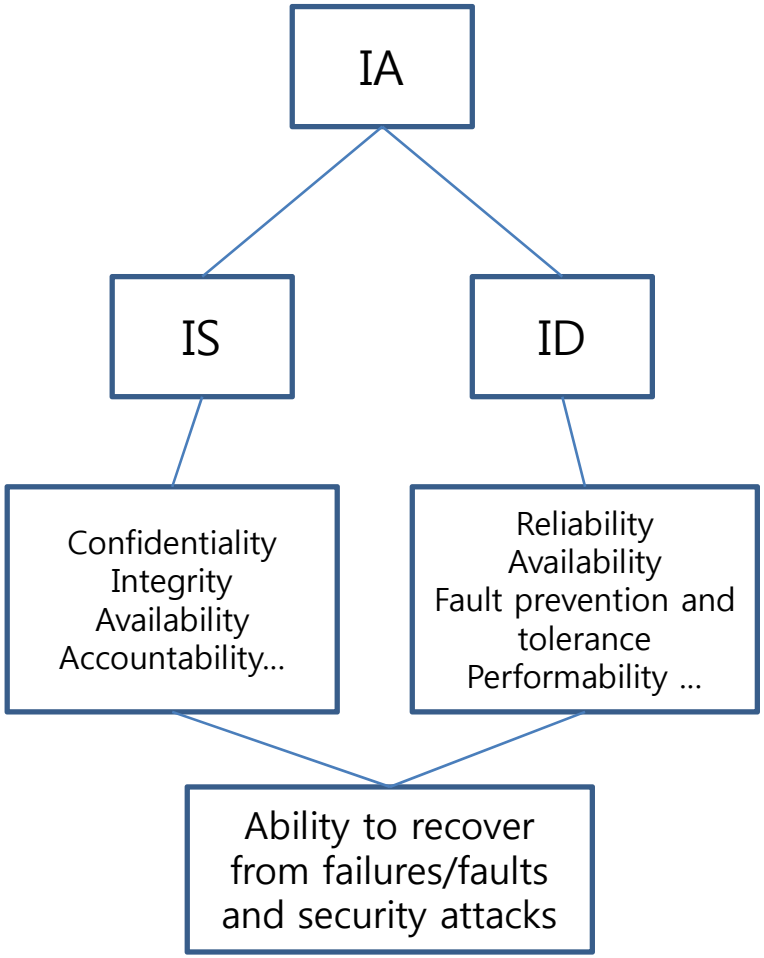
CNS Lab

# Design Considerations

- Non-overlapped security service
- Configurability
- Balance between privacy and security
- Balance between availability and security
- Automated diagnosis (self-diagnosability)
- Security audit

# Information Assurance

- Convergence of security and dependability
  - Protection of critical information and resources must be provided
  - Networked information systems must function correctly in various operational environments
- Ensuring to provide an assured level of functionalities in the presence of disruptive events
  - Survivability, resilience, disruptive tolerance, etc.
- **Integrated framework for security and dependability**




CNS Lab

# Integrated Dependability and Security Evaluation

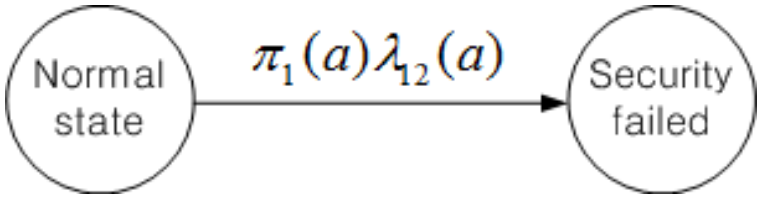
# Failure Process

- "*Fault-Error-Failure*" Pathology
  - Can be used to model security failures in a similar way as the dependability community
  - *Fault* : an atomic phenomenon that can be either internal or external, which causes an *error* in a system
  - *Error* : a deviation from the correct operation of a system, which may lead to a *failure* of a system
  - *Failure* : an event that causes a system service to deviate from its security requirements
- *Intrusion*
  - The result of the external malicious human-made faults
  - Because they are intentional in nature, intrusions cannot be modeled as truly random processes.
  - Even though the time, or effort, to perform an intrusion may be randomly distributed, the decision to perform the action is not

# Modeling Intrusion as Transitions

- Modeling failure rate
  - $\pi_i(a)$ : the probability that an attacker will choose action $a$ when the system is in state $i$
  - $\lambda_{ij}(a)$ : the accumulated failure intensity if all $n$ potential attackers always take action $a$
  - failure rate between $i$ and $j$

$$q_{ij} = \pi_i(a)\lambda_{ij}(a)$$




- System measures
  - Based on CTMC model, measures, i.e., MTFF, MTTF can be obtained

# Model Parameterization

- Accidental failure, repair rate
  - The procedure has been practiced for many years in traditional dependability analysis.

- *Obtaining* $\lambda_{ij}(a)$ is challenging
  - To let security experts assess the intensities based on subjective expert opinion, empirical data, or a combination of both.
  - To collect information from a number of different sources in order to predict attacks

- *Obtaining* $\pi_i(a)$ is more difficult
  - To use game theory as a means for computing the expected attacker behavior

# Predicting Attacker Behavior

- Motivation for attacks
  - Financial gain : credit card theft, blackmailing, or extraction of confidential information
  - Entertainment : hacking web sites or rerouting Internet browser requests
  - Ego : overcoming technical difficulties or finding innovative solutions
  - Ideology : likely to increase in the future
  - Entrance to a social group of hackers : writing a particular exploit, or breaking into a particularly strong computer security defense
  - Status : the most powerful motivation factor

- Demotivation
  - Attackers may be risk averse
  - The illegal aspect of actions (criminal offense) may prevent even remote attackers to use available tools to exploit vulnerabilities in corporate networks

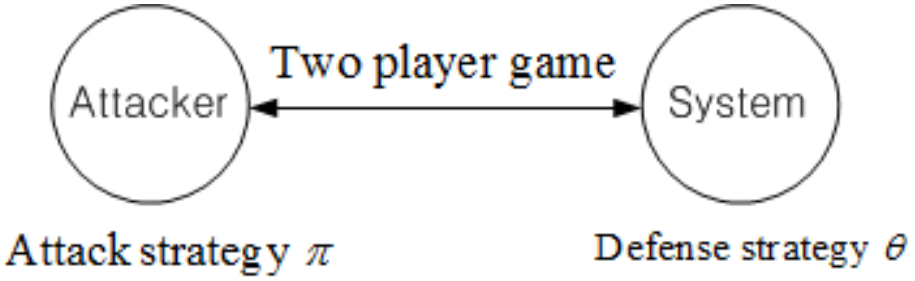
# Reward and Cost Concept

- Reward
  - An attacker accumulates reward during the events of an attack
  - Whenever an attacker performs an attack action, he receives an immediate reward.
  - If the action succeeds, an additional reward (expected future reward) may be gained.
  - The expected amount of recovery effort required from a system administrator
  - The degree of bandwidth occupied by a DDoS attack

- Cost
  - A negative reward is used to quantify the impact on an attacker as an attack action is detected and reacted to.
  - Risk-averse attackers may sometimes refrain from certain attack actions due to the possible consequences of detection.

# Modeling Interactions as a Game

- The interaction between an attacker and a system modeled as a game




- A two-player, zero-sum stochastic game
  - Compute the expected attacker behavior in terms of a set of attack probability vector $\pi$.
  - Since the game is zero-sum, an attacker's gain is the system's loss.
  - Does not assume that the attackers know the system outcome values.
  - The purpose of the game model is to predict the behavior of attacker and not to perform any cost-benefit optimization of system defense strategies.

# Conclusions

Goal of Security Research:

Design of Security Architecture for Future Internet with ~100% guarantee of C, I, A, and A

- Find the most fundamental prevention mechanisms against security attacks
- Desirable if self-restoration feature is incorporated
- Must develop efficient security policies for Future Internet

CNS Lab