Future Internet Security Research in Korea

2011. 3. 09

Kyung-ho Chung, Information Security PM
Korea Communications Agency

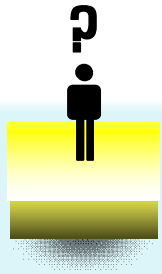
Contents outline

- Overview
- Technology Trends
- Complicated Problem
- Network
- Authentication
- User Privacy
- Attacker Tracer
- Virus & DDoS
- Discussion

Overview－1

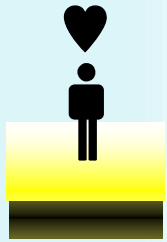
❑ Future Internet security background

Internet security



- System and Network security becomes very complex issues
  - ➢ Cyber attacks for profit and national agenda
  - ➢ New computing technologies, a variety of security threats and privacy problems
- Independent of security technologies add additional burdens on the Internet
  - ➢ Security is not considered at the design stage

Need for Future Internet Security



- Internet, as a trusted communication infra
  - ➢ Overcome the limitations of Internet and add new security requirements
  - ➢ Security-embedded network for trusted communication
- Trust communication structure at the initial design phase of Future Internet
  - ➢ Compatibility with existing Internet vs. Innovative concepts (Clean-slate)

Overview－2

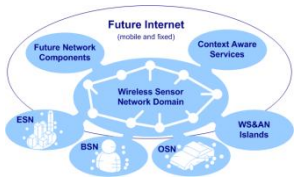
- **Standards**
  - ➢ Leadership for Future internet Technology
  - ➢ Technological competitiveness
  - ➢ New information security market

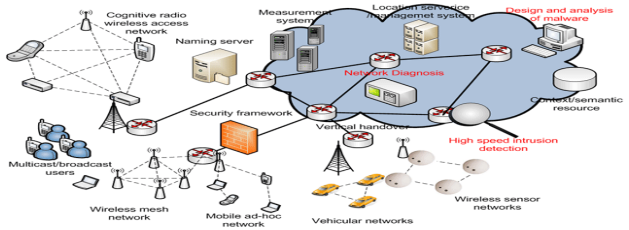
Information Security for Future Internet In KOREA

- **Technology**
  - ➢ Convergence of Broadcasting and Telecommunication
  - ➢ Hybrid attack against system and network

- **Policy**
  - ➢ Long-term national research
  - ➢ A systematic approach with business perspectives

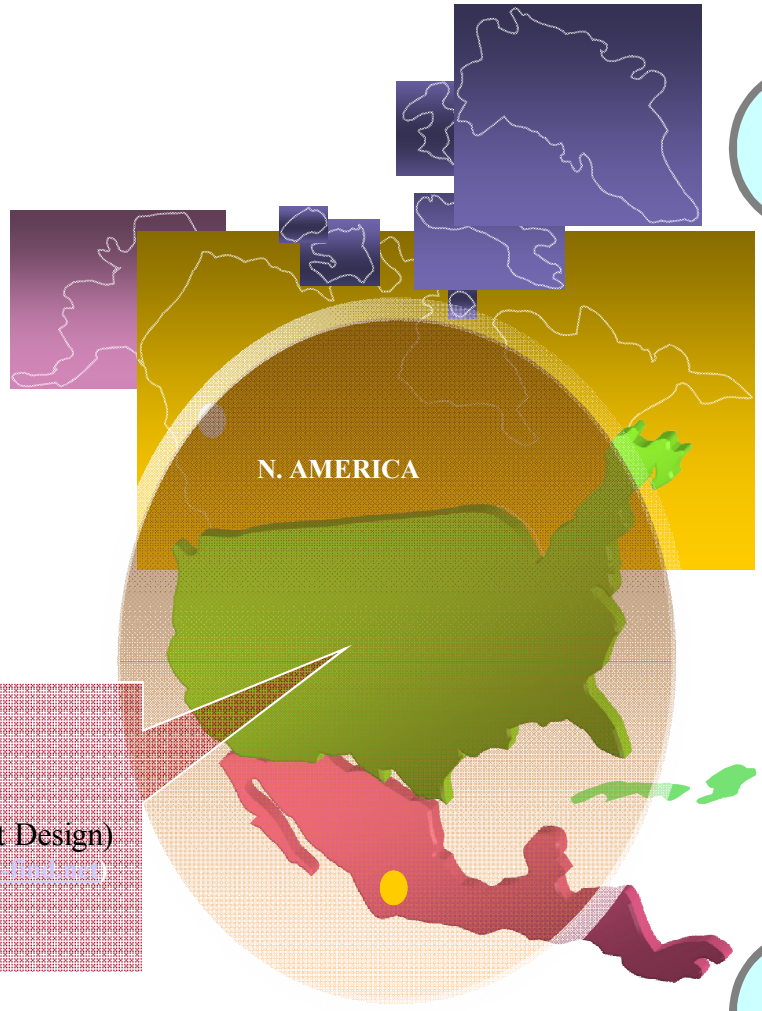
방송통신위원회
KOREA COMMUNICATIONS COMMISSION





Technology Trends (US)

❑ NSF Projects



NSF Next Generation Internet in 2005 for developing and testing innovative Internet structure

Routing / Forwarding. Security, Wireless, Sensor Naming and identifier technology and core technology research and development

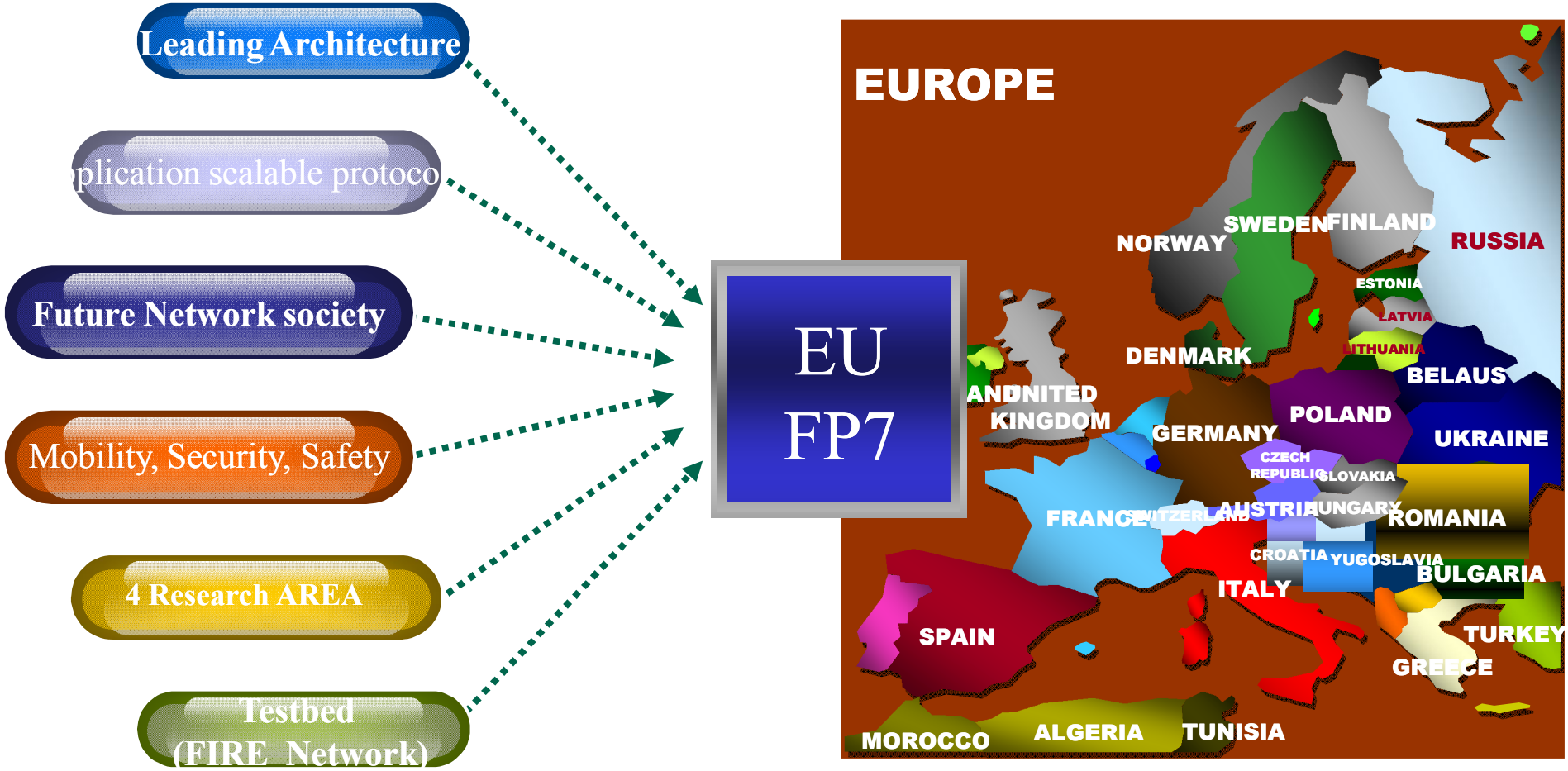
48 more projects
FIND Security Projects (6)

Standford, MIT, UC berkely, CMU,.etc

In 2020, Future Internet Design

FIND
(Future Internet Design)
(http://www.nsf.gov/find)

Technology Trends (EU)



Technology Trends (Kr)

· 1150 KRW = 1 USD

1	Future internet Core technology research	● Seoul national university (future growth engine projects) ● 2007 ~ 2009 (National funding 3.13M$) ● Algorithm, Standardization ● Cooperation with GENI, EU-ICT FP7, Asia FI, etc
2	Development of future Internet Infra platform & core technology	● ETRI ● 2009 ~ 2013 (total 9.47M$) ● Programmable platform, Virtualization ● 'Broadcasting & Communication network Long term Plan'
3	Development of future internet network model	● Development of future internet model (National Institute for Mathematical Sciences) ● 2008.12 ~ 2014.12 (total 14.78M$) ● Mathematical model, Network structure ● Korea Research Council of Fundamental Science & Technology
4	Development of future internet Quality of Service Technology	● Seoul National University ● 2008 ~ 2010 (Total 782K$) ● Real-time intrusion prevention system, Network diagnosis, Source authentication

Technology Trends (Kr)

Future Internet Infra Technology

- Virtualization Support Programmable Platform technology
- Network virtualization control technology
- Infra management Technology
- Wireless Access infra technology

Future Internet Architecture Technology

- Integration Architecture Technology
- Address & Routing Technology
- Future Security Architecture
- Network management and mobility management technology

Future Internet Application and Service Technology

- Service architecture technology
- Service Adaptability technology
- Service Transmission Technology
- Service virtualization & Transforming information into knowledge

Technology level compared to advanced countries (Low)

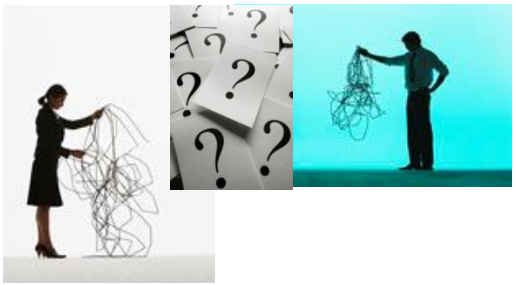
Technology level compared to advaced countries (Lower)

※ Source from 'Analysis Report on Future Internet Issues', KISA, 2011.

Complicated Problem

✓ A Complicated Problem (Nobody goes that way)

A pile of cable,
totally mixed up! ☹



Sorting through
a pile of cable

Holding one end first!

Holding opposite ends of a long cable

Long way… but, a better approach

Holding ends of a cable
and putting them together ☺

***Possible?
… might be
impractical***

Network (1)

✓ **Openness VS. Security**

➔ One good strategy is fairly tuning two objectives for achieving a balanced performance

Preparing expected benefits

Functionality, Sharing, Transparency, Convenience, Compatibility, Anonymity, Performance, Operability, and so forth

Coping with potential risks

Confidentiality, Integrity, Availability, Concealment, Protection, Privacy, Identification, Trustworthiness, etc.

Emerging technologies and services, and one-to-one communications come us with unpredictable threats and attacks

Risky-ignored Internet

Security costs too much

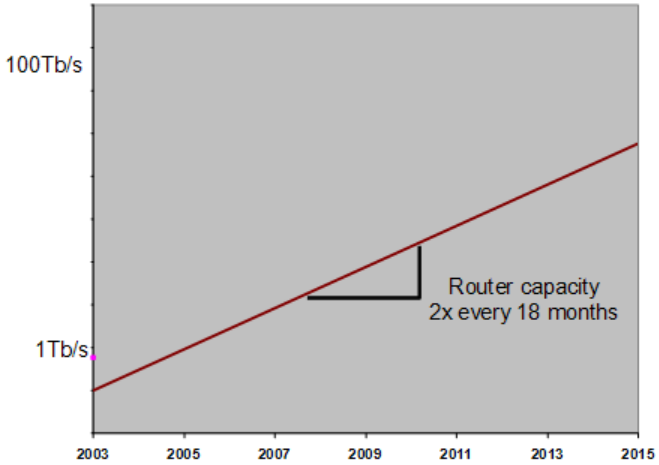
Should be equally fair??

We're going the same way together

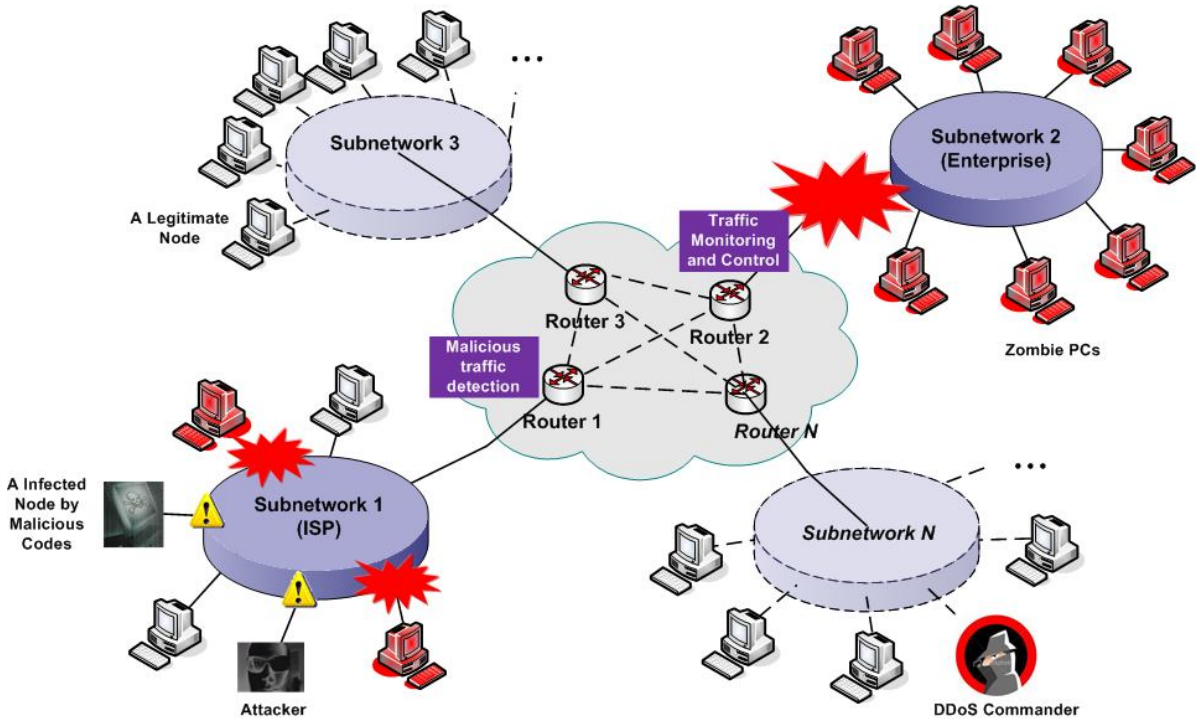
Network (2)

- ✓ **Building free networks from malicious codes and DDoS attacks**
- ➔ One suggestion is that individual routers could be equipped with detection, blocking, and other relevant functions coping with serious threats and attacks.
- ➔ This cooperative network is able to play a role of the global sensorium for the future Internet.

A Linear (Pessimistic) Expectation in the Router Capacity Growth



*Source from Stanford Univ.

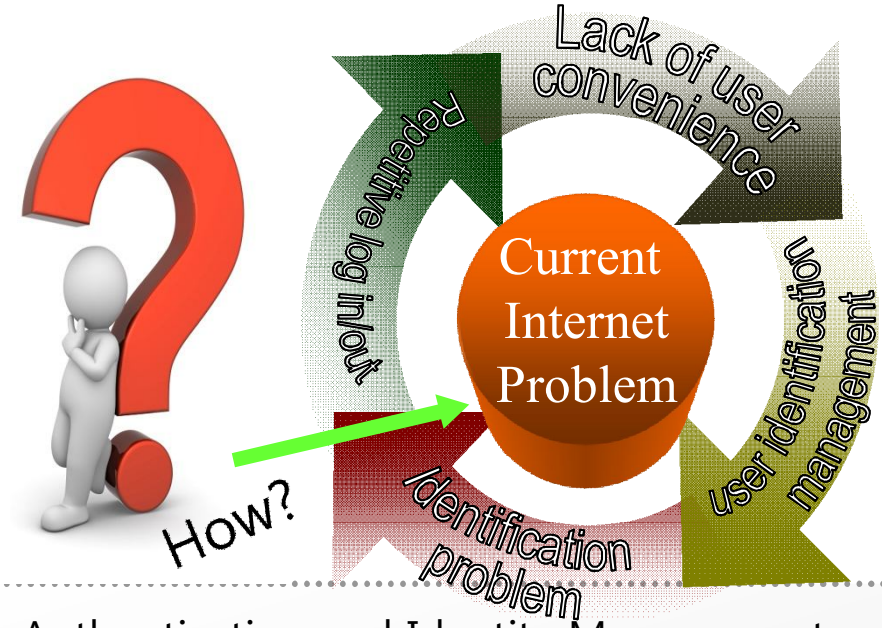


Authentication

Authentication in Future Internet

- Auth. based on bio-info.
- Interactive auth.
- Evaluation of auth. system
- Legal system

High-cost and low-efficiency



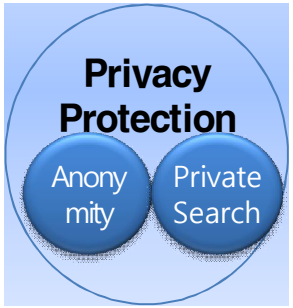
◆ Development of New Authentication and Identity Management

- MS - Cardspace, Liberty Alliance - Federal Identity Management System, etc.
- Each solution is dedicated for a particular service
  - Full interaction between entities may not be supported

◆ Development requirements and issues

- Authentication-related information and system sharing, and user convenience
- Expansion of conventional authentication system for new services

User Privacy

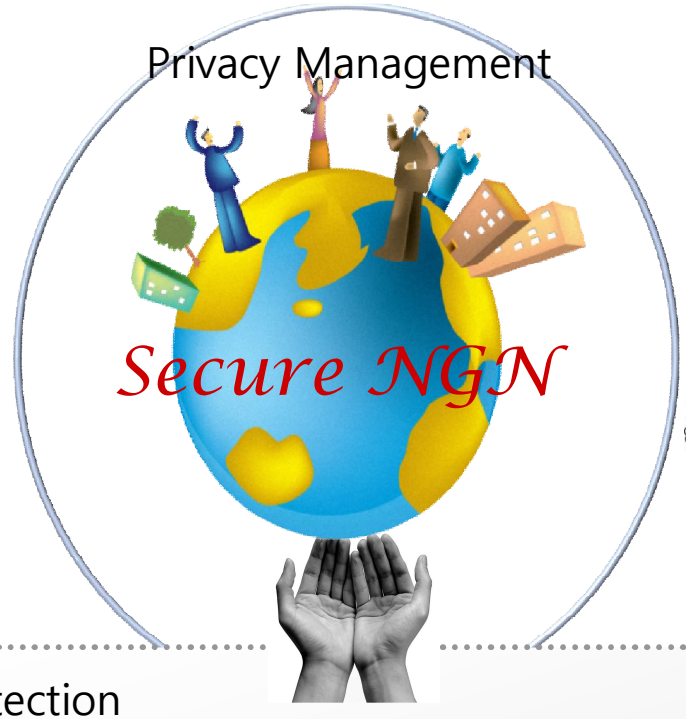


Privacy

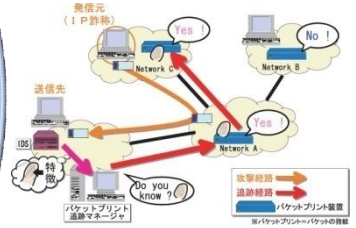
- Decentralization
- Data Randomization
- Group anonymity

Privacy Management

User Privacy Protection



Privacy Control



◆ Reliable Privacy Protection

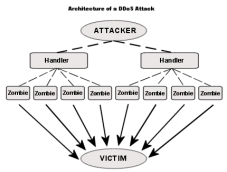
- Privacy-preserving Data mining
- Group anonymity with Generic identity management

◆ Private information retrieval

- Private search and information retrieval
- Various techniques using the public key or symmetric key approach

Attacker Tracer

Countermeasure after Attacks << Prevention



Network Security System → Tracking Attackers → Blocking the Predicated Attacker's Behaviors

Coping with violations from attacks

- Concurrent and multiple connections
- Immediate data recovery
- Pre-intervention of collaborated attacks

Tracking Attackers	Predicting and Blocking Attackers
IP based attacker trace	Other way than IP-based attacker trace
Passive solution after some attacks	Risk verification of unknown threats or vulnerabilities
Various vulnerabilities on network security products	Attack prediction and blocking technique
	Developing the security product feasible in various environments

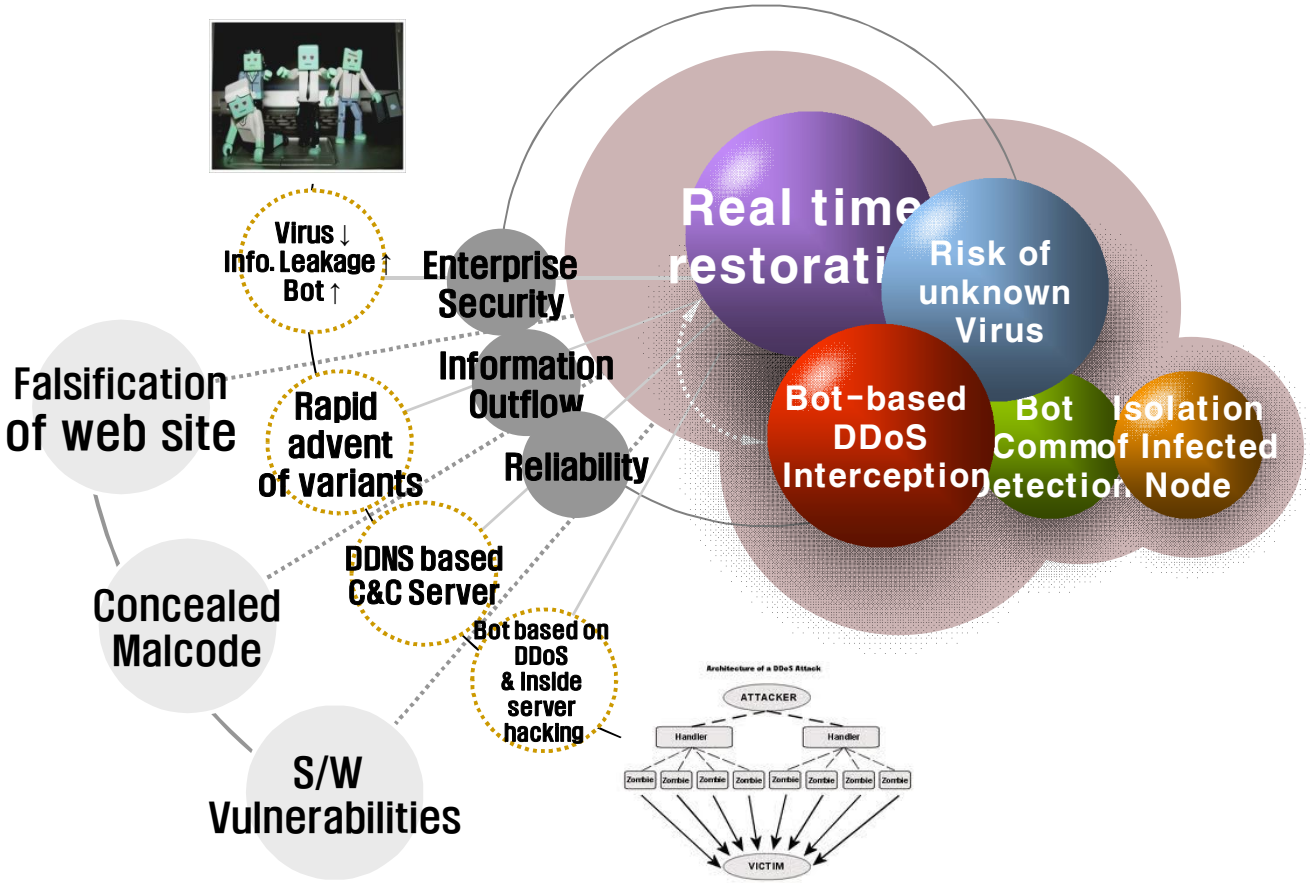
Economic Efficiency and Practical Feasibility

Virus, DDoS and malicious code

Automatic Attack/Passive Countermeasure << Pre-interception & Active Protection

Coping with Virus & DDoS

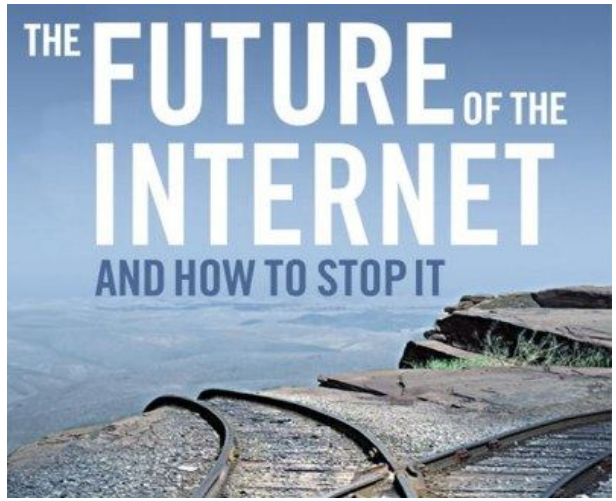
- Analysis on unknown virus and bot
- Sophisticated analysis technique
- Protecting privacy
- Protection scheme for the business confidential



How to protect…?

Discussion


HOW SAFE IS YOUR
COMPUTER?


THE FUTURE OF THE
INTERNET
AND HOW TO STOP IT