Creating Trust in Critical Network Infrastructures:

Korean Case Study

Chaeho Lim

Professor, KAIST

chlim@if.kaist.ac.kr

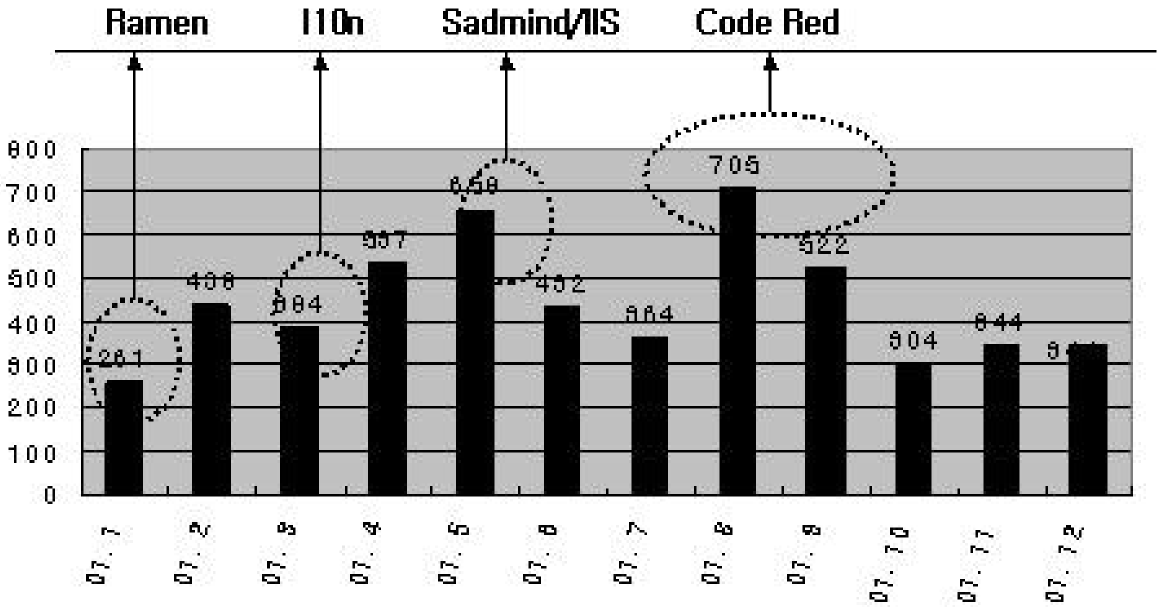
KAIST
ISC 정보보호교육연구센터
Information Security Center

Table of Contents

- Introduction
- Korean Environment
- Telecommunication and Networks Services
- Types and impact of threats to Critical Network Infrastructures
- Key Initiatives to Protect Critical Network Infrastructures
- Conclusion and possible areas for further studies

Introduction

- The Major Security Threats in Korea, 2001
  - Over 10 times traffic than the normal
  - How was the critical infrastructure ?



Korean Environment

- Korea’s Geographical Structure
- The Korean Economy

Telecommunication and Networks Services

- Facilities-Based Telecommunication Services
  - Domestic Telecommunication Services
  - International Telecommunication Service
  - Wireless Telecommunication Service
- Non-facilities-based telecommunication service providers
  - Specially Designated Telecommunication Services
  - Value-added Telecommunication Services
  - Internet Connection Services

Telecommunication and Networks Services

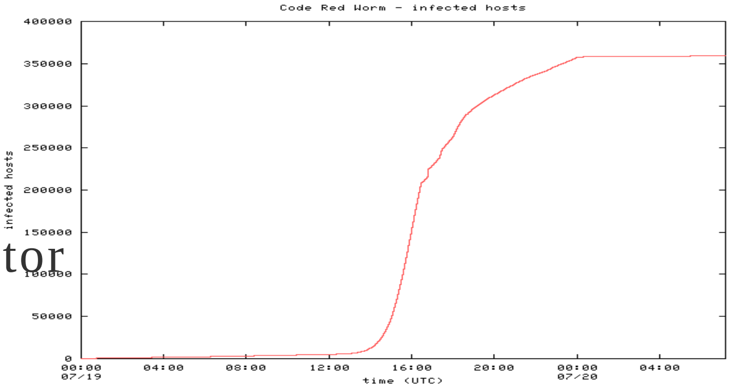
- Internet Infrastructures in Korea
  - Internet eXchange (IX)
  - Internet Backbone Network
  - Access Networks
    - Wired Services
      - Dialup Modem / ISDN, Cable Modem, XDSL,
    - Wireless Service
      - Internet via Cellular, B-WILL, Satellite

Types and Impact of Threats to Critical Network Infrastructures

- The Worm Attacks in 2001
- Internet Attacks Statistics
- Computer Virus Attacks

The Worm Attacks in 2001

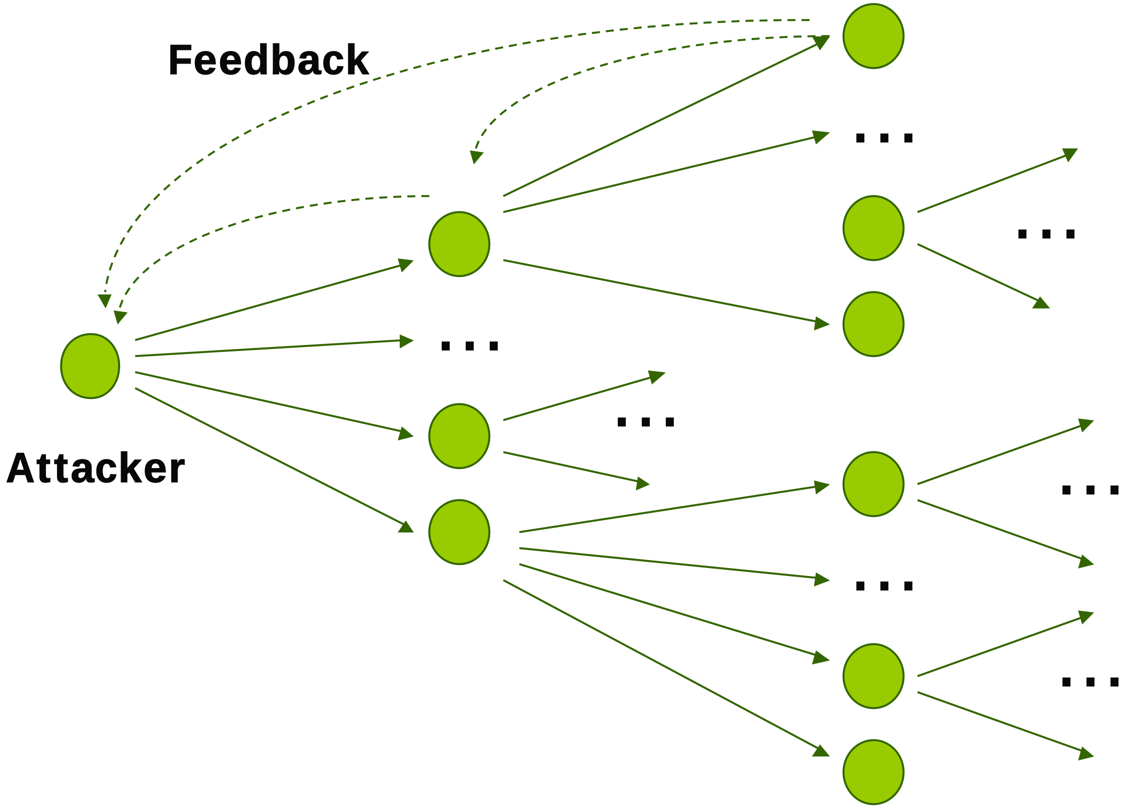
- The Worms in 2001
  - Ramen, Li0n, Carko, Sadmin / IIS, Cheese, Red, CodeRed, CodeBlue, Nimda
  - Cheese Worm,
    - Found in Korea only
    - Found in Real Time Scan Detector



  - We found
    - Indication & Warning is very important
    - International Cooperation is very important
    - System should be vulnerable

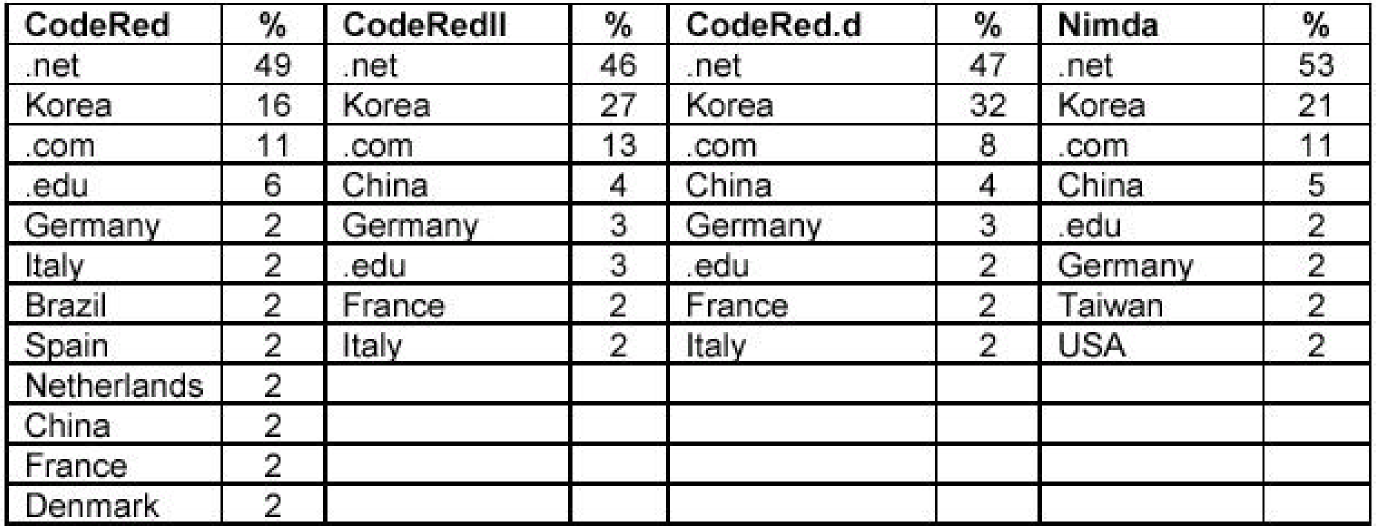
The Worm Attacks in 2001

- Worm Model



The Worm Attacks in 2001

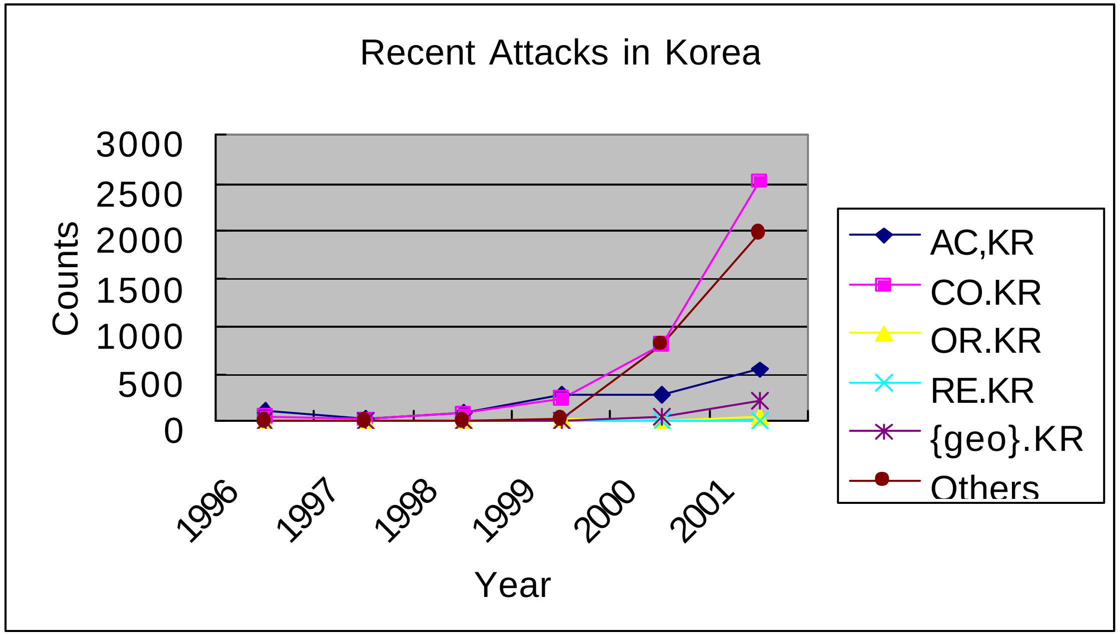
- Abor Networks, “A Snapshot of Global Internet Worm Activity”, Nov 2001



CodeRed	%	CodeRedII	%	CodeRed.d	%	Nimda	%
.net	49	.net	46	.net	47	.net	53
Korea	16	Korea	27	Korea	32	Korea	21
.com	11	.com	13	.com	8	.com	11
.edu	6	China	4	China	4	China	5
Germany	2	Germany	3	Germany	3	.edu	2
Italy	2	.edu	3	.edu	2	Germany	2
Brazil	2	France	2	France	2	Taiwan	2
Spain	2	Italy	2	Italy	2	USA	2
Netherlands	2						
China	2						
France	2						
Denmark	2						

Internet Attacks Statistics

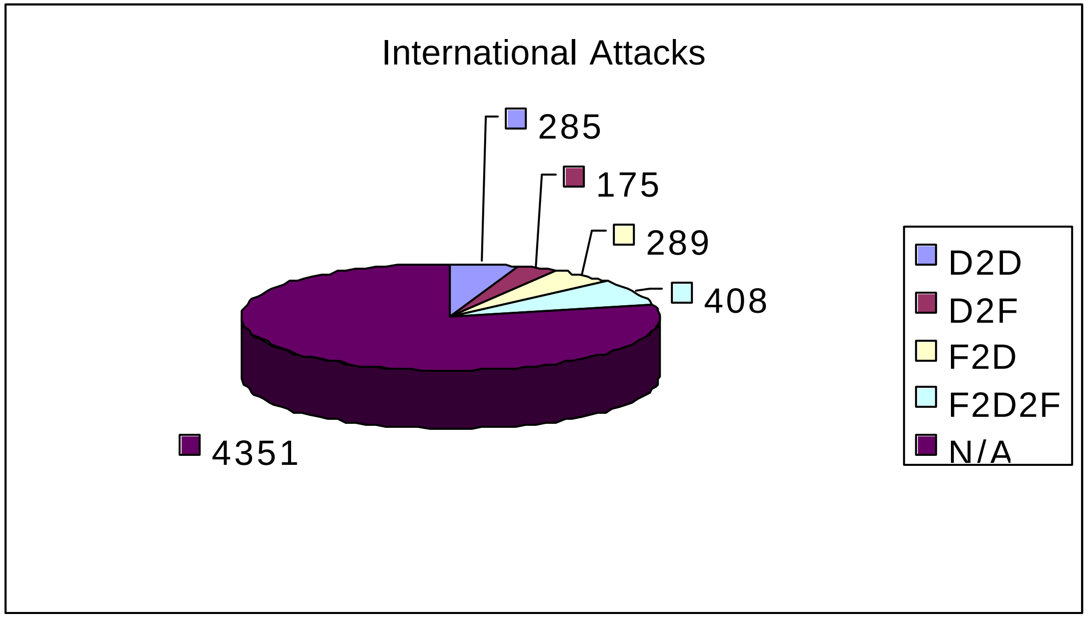
- Recent Attacks Statistics
  - Reported to CERTCC-KR/KISA
  - Increased very rapidly



Internet Attacks Statistics

◆ International Attacks

- D2D : From Korea to Korea, D2F : From Korea to Foreign
- F2D : From Foreign to Korea
- F2D2F : From Foreign to Korea to Foreign
- N / A : Not Available



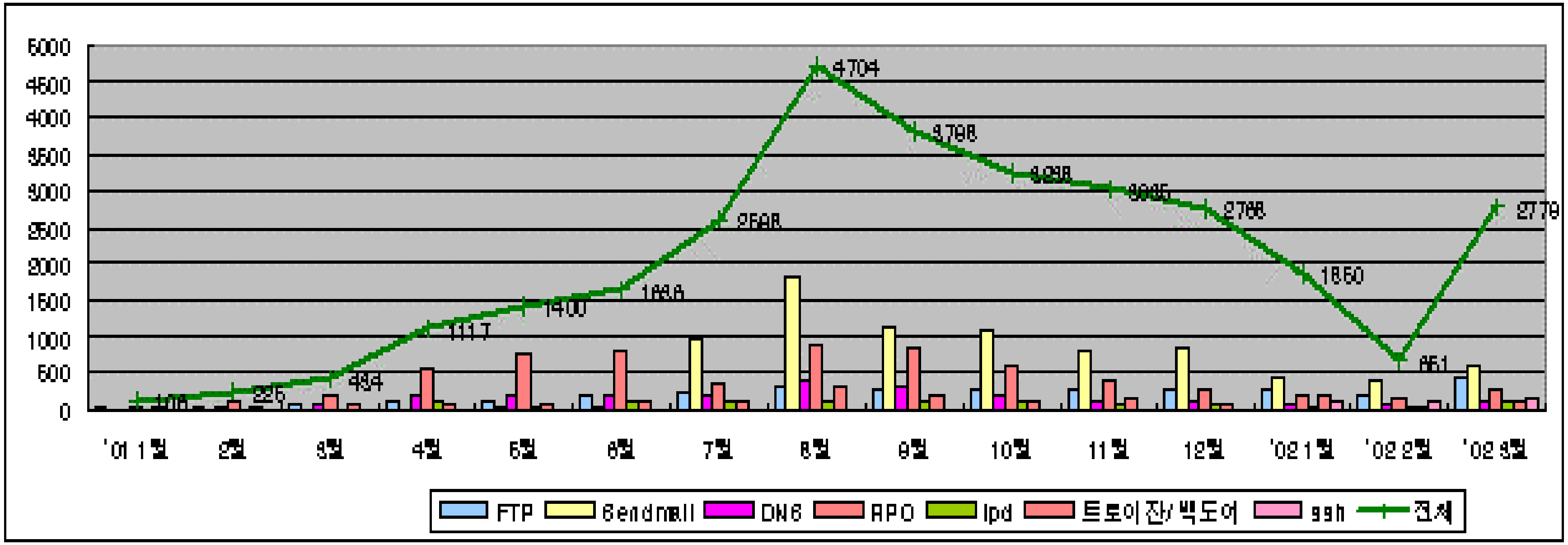
Internet Attacks Statistics

- What Countries ?

Country Name	Counts	Country Name	Counts
France	707	Japan	615
Australia	600	Brazil	310
Germany	220	United Kingdom	107
Malaysia	76	Thailand	61
USA	51	Poland	30
Netherland	24	Canada	21
Austria	7	Spain	5
Slobenia	3	Chile	1
Italy	1	Hongkong	1

Internet Attacks Statistics

- Real Time Scan Detector(RTDS), Jan ’01 – Mar ‘02



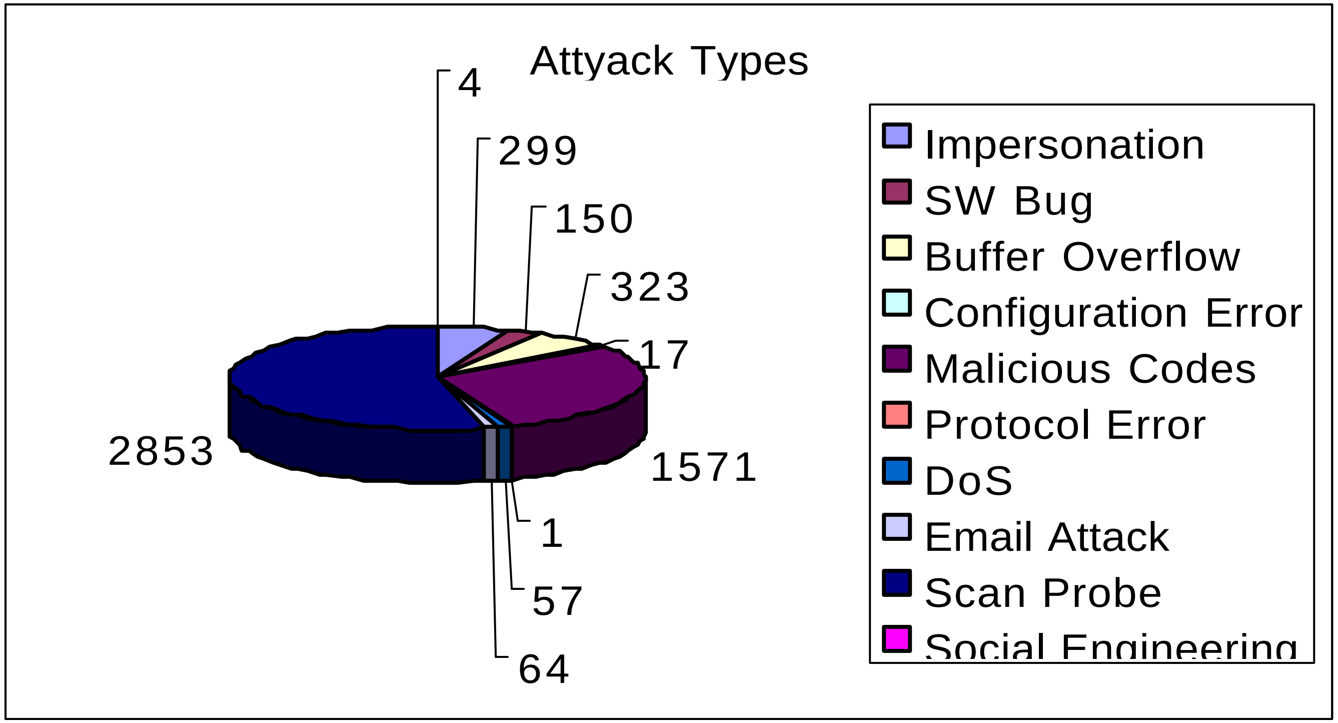
Internet Attacks Statistics

- Countries in RTDS

					ISP/NET		
	EDU	ORG/GOV	RE	COM	PPP user	Unknown	Total*
KOREA	420	80	15	517	589	79	1700
U.S.	47	7		142	408	3	607
CHINA	9	2	1	32	66	3	113
TAIWAN	11	2		33	63		109
ITALIA	1			6	75		82
JAPAN	3	5		28	35		71
CANADA	6	1		15	38	1	61
GERMAN	1			16	37	1	55
HongKong	2	1		24	22		49
U.K.	3	1		9	31		44

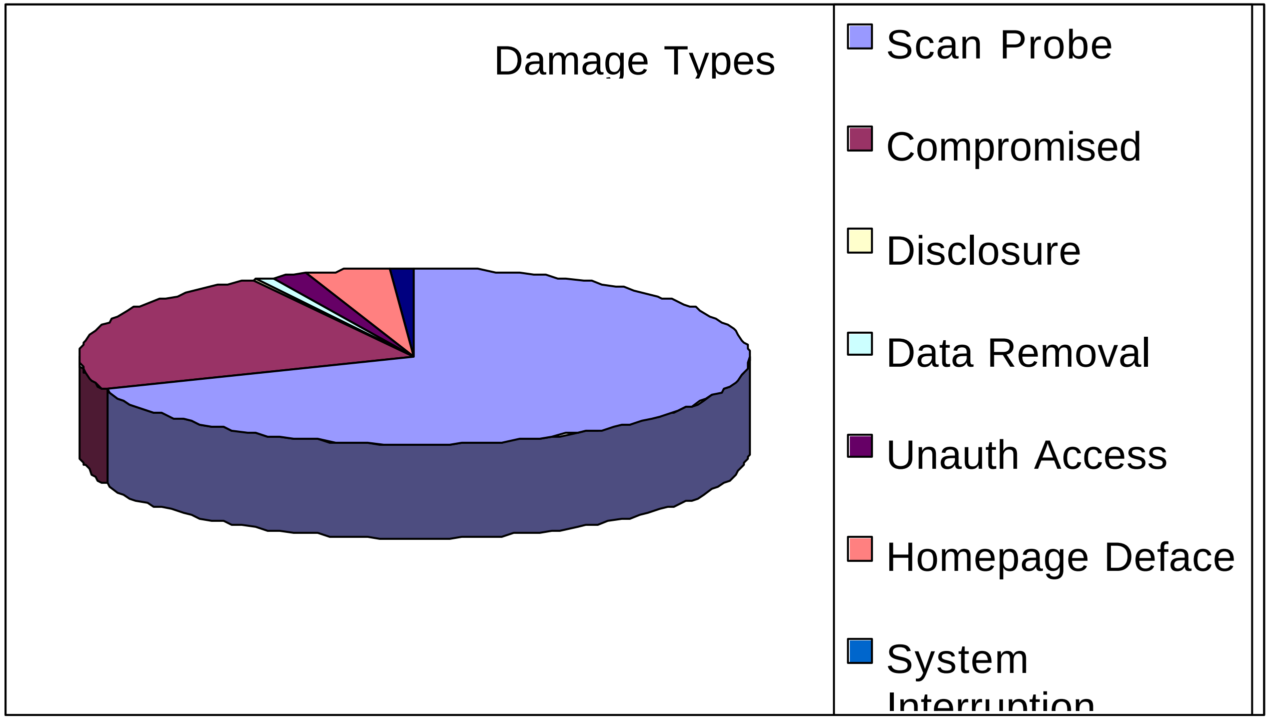
Internet Attacks Statistics

- Attack Type

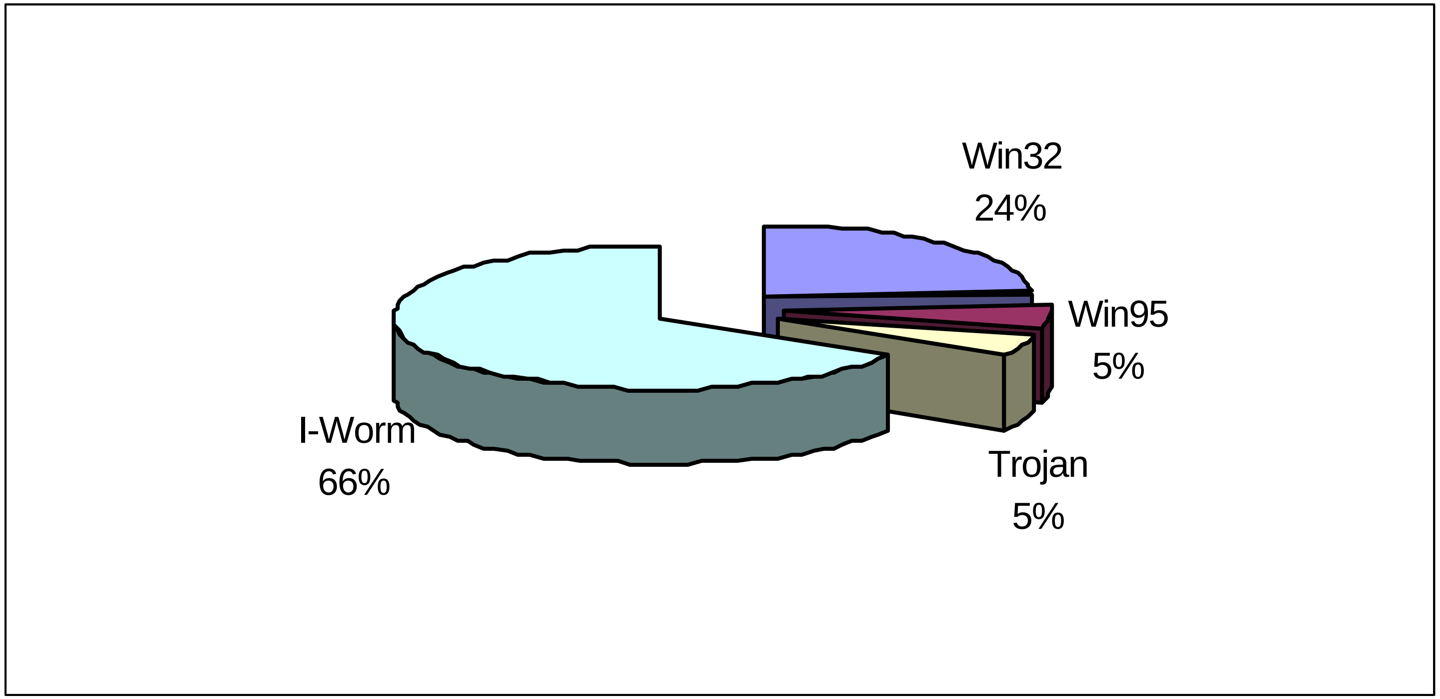


Internet Attacks Statistics

- Damage Types

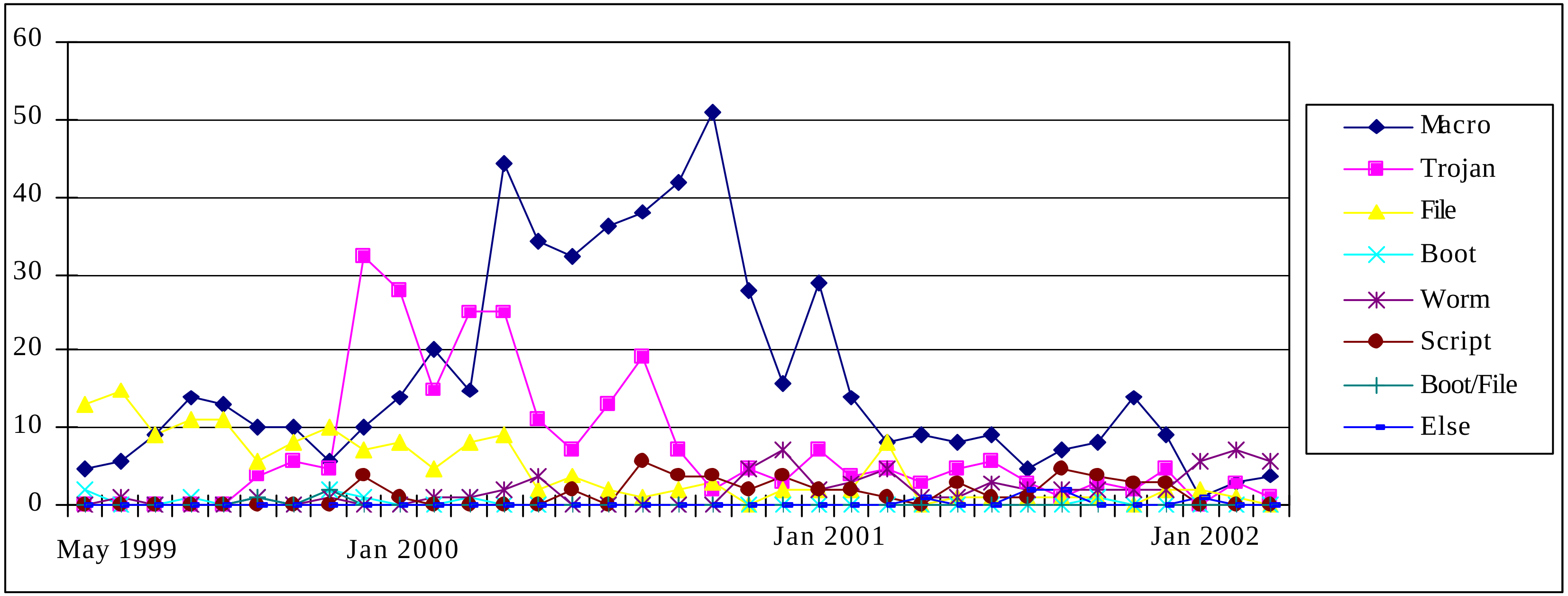


Computer Virus Attacks

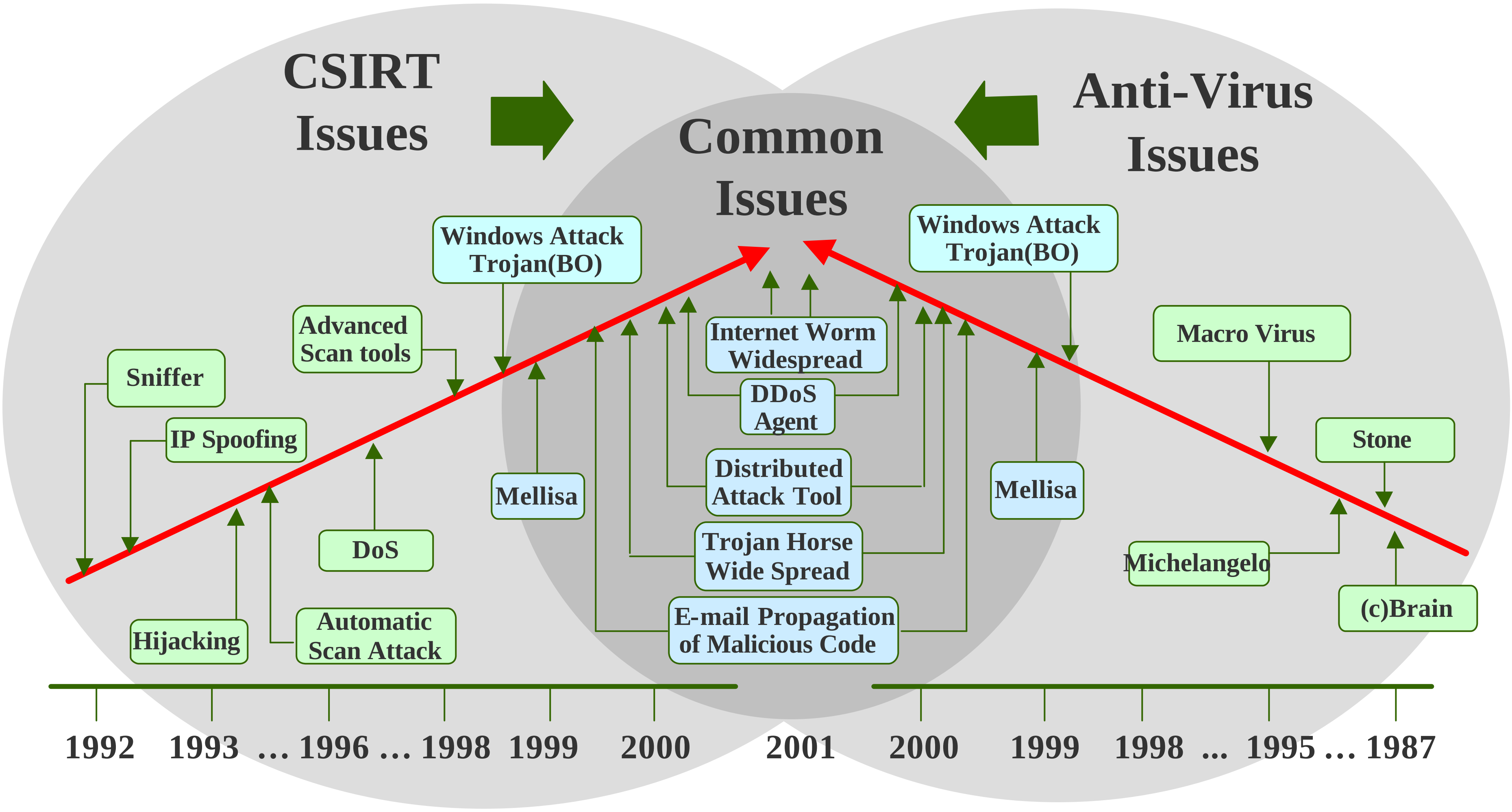


Computer Virus Attacks

What Kinds of Virus were reported?



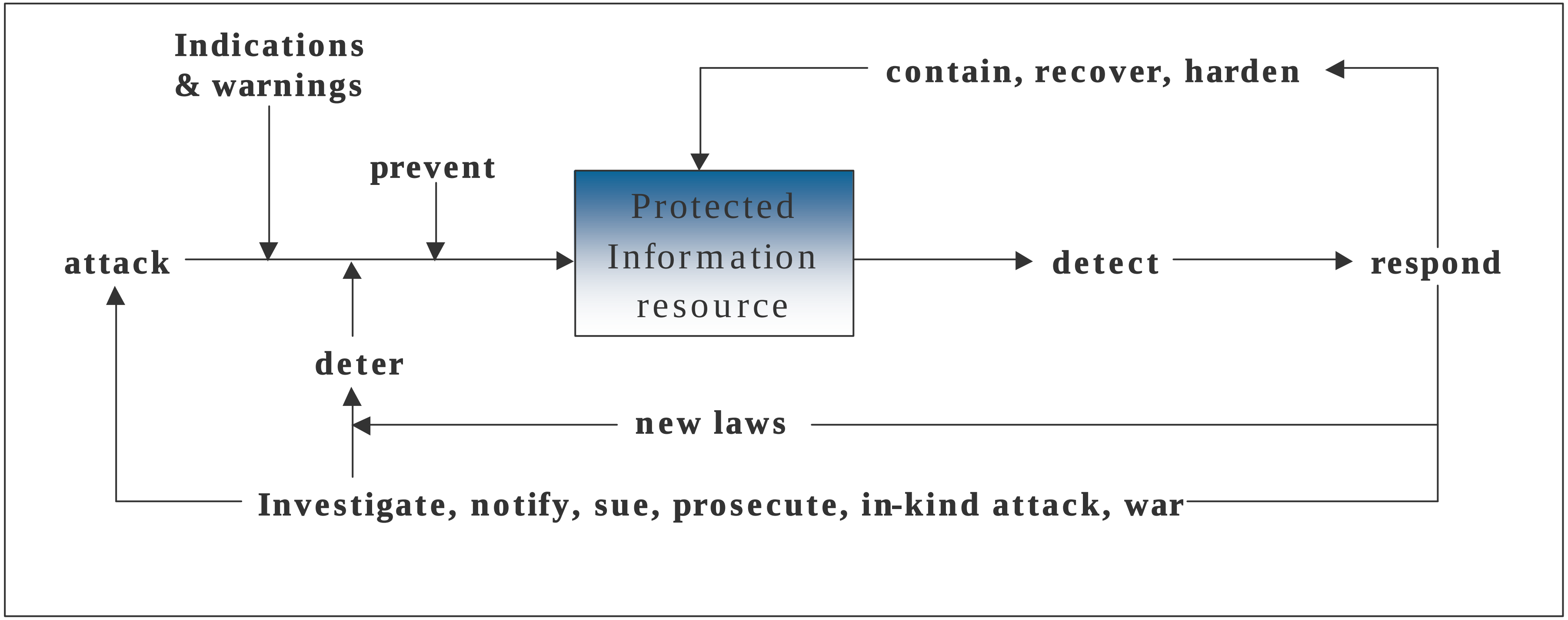
Computer Virus Attacks



Key Initiatives to Protect Critical Network Infrastructures

- The General Approaches for Incident Response
- The Structure of Security in Korea
- The Act of Critical Communication & Telecomm Protection
- Regional Level Cooperation
- Other Activities

The General Approaches for Incident Response


Indications & warnings
contain, recover, harden
prevent
Protected Information resource
attack
detect
respond
deter
new laws
Investigate, notify, sue, prosecute, in-kind attack, war

The Structure of Security in Korea

- The National Intelligence Security and Public
  - National security ;
    - National Intelligence Service, NIS
    - Ministry of National Defense, NMD
    - National Security Research Institute, NSRI(Under ETRI)
  - The Public ;
    - Ministry of Information and Communication, MIC
    - Korea Information of Security Agency, KISA
    - ETRI
    - CONsortium of CERT
  - Law Enforcement
    - Supreme Public Prosecutor's Office, SPPO
    - National Police Agency, NPA

The Act of Critical Information & Telecommunication Protection

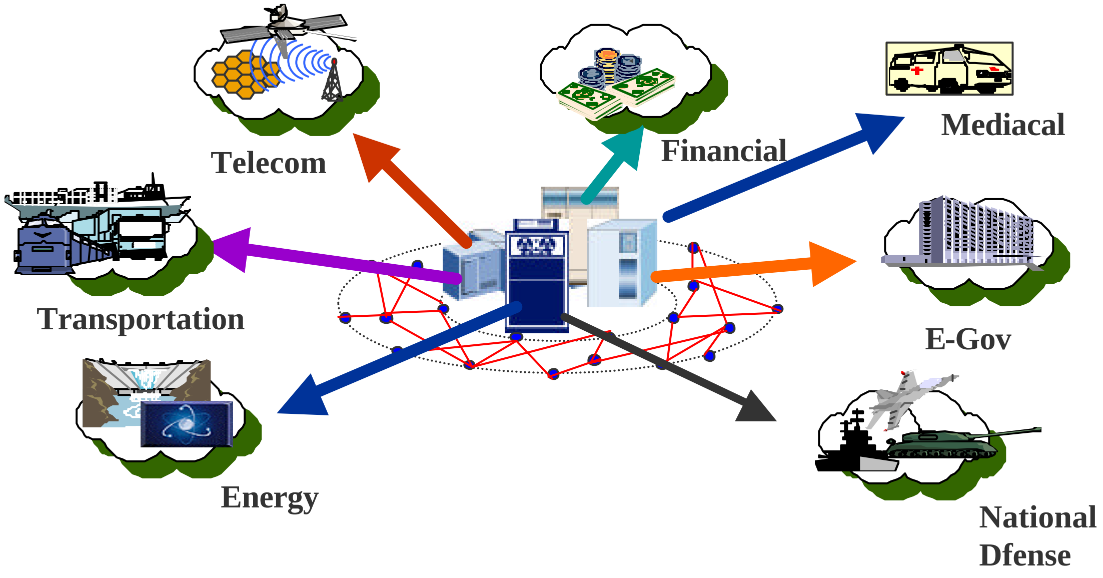
- What is the Critical Communication & Telecomm?
  - Modern Information Society all ITs are interconnected through the communication networks
  - Recently computer intrusion and virus attack could be attacked to critical system
  - Especially if social infrastructure system could be attacked?
  - Serious Damages Occurred !!

The Guidance to Critical Infrastructure

-The Importance of the mission's sociality
-The dependence of Information & Communication Infra
-The Interdependence of other Information & Comm Infra
-The Damage Level of the Compromise and Interruption
-The Easy of the Compromise and Recovery

The Act of Critical Information & Telecommunication Protection

- What is Critical Information and Telecommunication?
  - Electronic Government & General Administration
  - National Defense
  - Medial Service
  - Financial Service
  - Gas and Energy
  - Transportation
  - Telecommunication



The Act of Critical Information & Telecommunication Protection

- What CITP Sites are Decided?
  - MOFAT : 1
  - MOGAHA : 2
    - General Administration Network,
    - Local Authority Network
  - MIC : 17
    - Comm Infra Net 11,
    - Internet 4,
    - postal Financial 1
  - MOHA : 3(Citizen Security)

The Act of Critical Information & Telecommunication Protection

- How to decide CIT Site
  1. Select the Potential CIT Sites by the President of Major Government
  2. Evaluate the Possibility of CIT site
  3. Check the report of the evaluation of CIT by the Major Government
  4. Discussion of the Result of the Check inside of the committee of the CITP
  5. Announcement

The Act of Critical Information & Telecommunication Protection

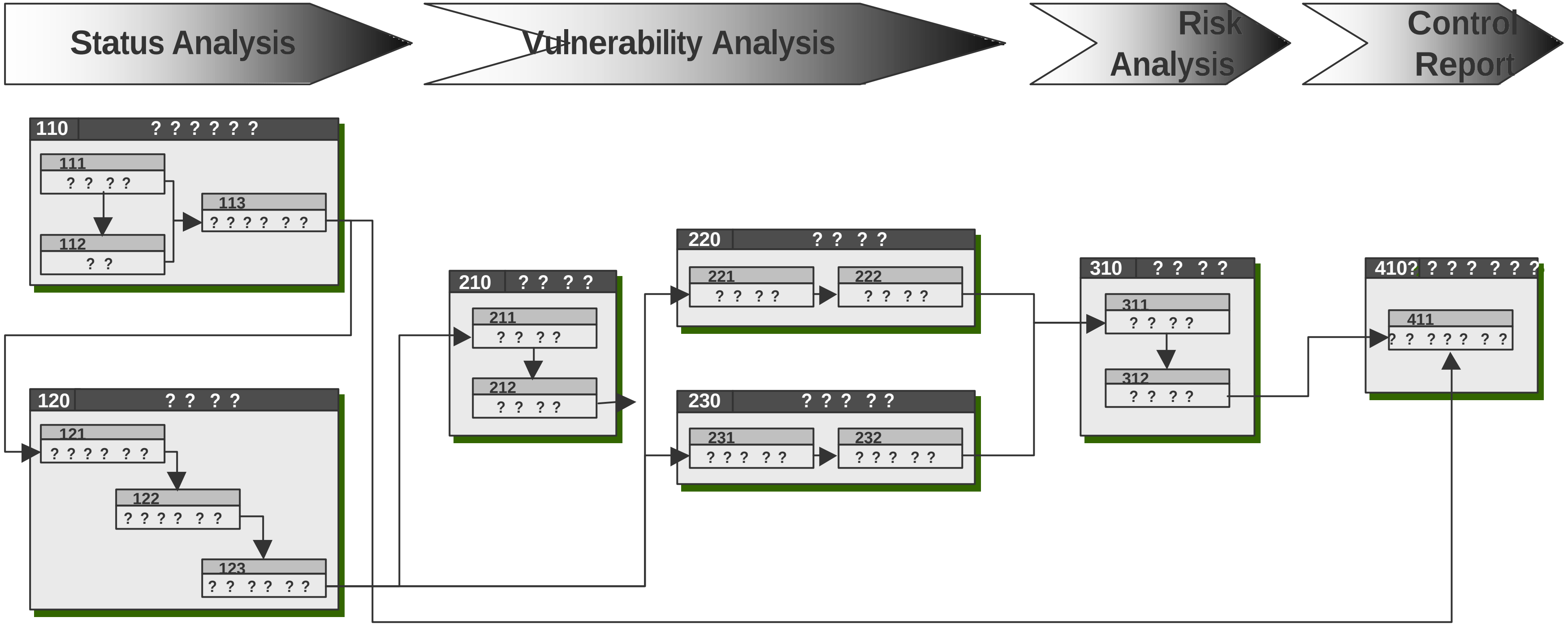
- ISAC & Special Information Security Company
    - Information Sharing and Analysis Center
        - Provide the Early Indication & Warning, solution to their subscribers
        - Financial and telecommunication ISAC was being settled
    - Special Information Security Company
        - Provide the analysis and evaluation of CIT Sites
        - 7 Companies were Decided in Nov 2001
        - Hackerslab, Inzen, A3SC, S-Cube, Secure Soft, SecureI.com, MacroTech

The Act of Critical Information & Telecommunication Protection

- The Analysis of Vulnerability of CIT Site
  - **GMITS**
  - **ISO/IEC 17799**
  - **IAM**
  - **VAF**
  - **OCTAVE**
  - **IPAK**
  - **CSE**
  - **NIST(SP 800-30)**

The Act of Critical Information & Telecommunication Protection

- KISA’s Model



Regional Level Cooperation

- We found :
  - Almost attacks are from foreign sites
  - Almost attacks are done suddenly and deeply
  - The first indication is most important for identify and warning the serious attacks
- APSIRC in Feb 2001
  - Almost countries come
  - Decides the cooperation between counties

  - http://www.apng.org/apsirc
  - http://www.jpcert.or.jp/apsirc

Other Activities

- The Evaluation the ISMS
  - Information Security Management
  - Like BS7799
- The Evaluation the IDC Security Requirement
  - Number of IDC : 48
  - The Number of Performs : 30
- Promotion of Security Related Manpower
  - The 5 Information Security Center
  - Support Security Related Clubs of Underground : 40
- Promotion of the Security Related Industry
  - Support the Development
  - Assist the Related Lab

Conclusion and possible areas for further studies

- Integrated National Information Security System, under construction
- Establishing common criteria for evaluating security products

Integrated National Information Security System, under construction

- Cyber Intelligence for Local/Regional
  - It's important to gather the indication information
  - If a country can analyze the attack signature, it's rather to share it regional
  - It's to study and cooperate the information to share
    - ftp://ftp.cert.dfn.de/pub/docs/csir/
- National Cyber Command Center
  - Gathering information
  - Analyze the attack and Assessment
  - Warning it nation wide

Establishing common criteria for evaluating security products

attacker	Target	Level of Damage	Classification
Individual (Hacker)	PC	Individual privacy, property loss	D
Organization (Terrorist, Crime Org)	Enterprise Network, Financial network, Power infra. Medical info Network, National geography, Information system, etc	Damage on enterprise, Public losses (damage on the public) National commerce loss, Damage public organization (loss to national economy	C B
Country	National defense network, Foreign affair network, Public peace network	Damage on the important national facility	A

Final Remarks

- Regional or Global Information Sharing
  - What Information?
  - What Jobs ?