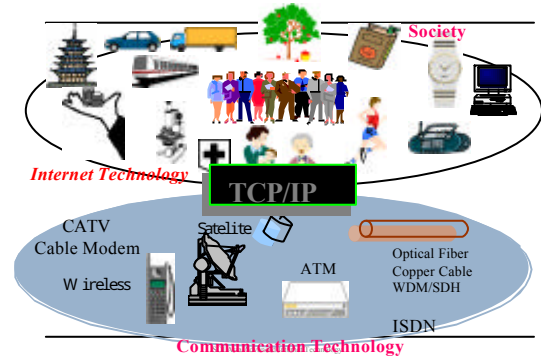


Security (1)

Suguru Yamaguchi
Nara Institute of Science and Technology

SOI Asia/Advanced Internet Technology

Internet: Global and Ubiquitous Infrastructure for Communication



Why we need SECURITY?

- Protect your activities on your information systems as well as network infrastructure
 - Information asset
 - Information processing environment
- Any damages on information systems and network infrastructure make impact directly on your "business" activities
 - Dependable infrastructure
 - Earning profit directly through these systems

SOI Asia/Advanced Internet Technology

Overview of technical trend observed as recent Security incidents

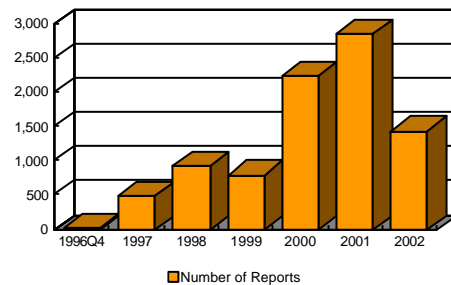
SOI Asia/Advanced Internet Technology

Frequently Observed

- Port Scanning & Probe
 - Almost every hour.
 - This can be considered as a prologue followed by other security incidents such as intrusion, we have to watch port scanning and probe trials at least at firewall.
- Intrusion
 - Still intrusions by password cracking are observed frequently.
 - However, one time password or other advanced method to protect login session makes them reduced.
 - Normally, buffer overflow is a main course to make intrusions to systems
 - Implanting "shell code" into network servers that have buffer overflow security hole.
 - Try to take whole control of the targeted system from the Internet
 - Many attack tools are using this method.
- Denial of Services (DoS)
 - Send excessive amount of traffic to the target, then try to stop its service
 - Distributed DoS is becoming more popular
- SPAM
- Computer Viruses via E-mail or other networking method

SOI Asia/Advanced Internet Technology

Statistics@JPCERT/CC



SOI Asia/Advanced Internet Technology

Technical trend

- Advanced attack method are widely deployed
 - Recently reported that **only 48 hours** duration when we can get attack tool using a specific security hole from the time when the vulnerability was reported.
 - Attack tools are very popular and traded in the Internet
 - Many developers
 - Traded in the Internet
 - Various kinds of information about security holes, attack methods and attack tools are available and aggressively exchanged among the community
 - E.g. "bugtraq"
 - Through WWW and IRC
 - Professionally developed
 - Give actual damage on the system

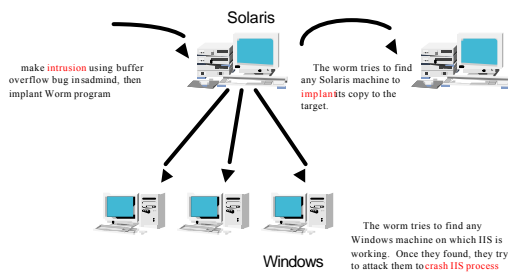
SOI Asia/Advanced Internet Technology

Buffer Overflow Attack

- Recognized as the most dangerous security hole, especially cases when we can find them in network service servers.
 - Major course for intrusion
 - Try to make "process crash (core dump)"
 - Implanting "shell code"
 - Obtain backdoor access with administrator privilege
- Reported buffer overflow found in many service servers
 - wuftp, Netscape Enterprise Server, Microsoft IIS,
 - Caused by functions in standard library that do not make boundary check of memory assignment.
 - Internet Worm (1988) used this method, so quite classic but can't be eliminated

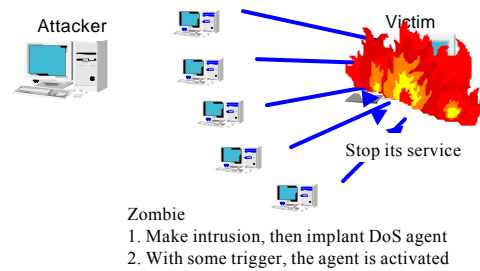
SOI Asia/Advanced Internet Technology

Multiple OS involved



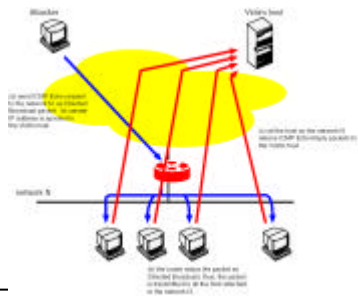
SOI Asia/Advanced Internet Technology

DDoS



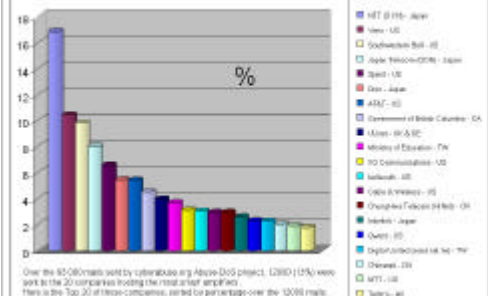
SOI Asia/Advanced Internet Technology

Smurf Attack



SOI Asia/Advanced Internet Technology

Percentage of Smurf amplifiers in the Top 20 of the most visited companies by cyberbase.org



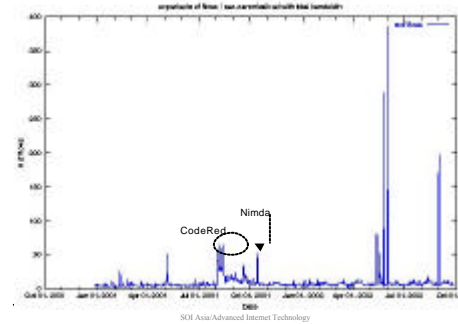
Over the 95,000 mails sent by cyberbase.org Abuse-DOS project, 1280 (1.5%) were sent to the 20 companies listing the most visited amplifiers. Here is the Top 20 of these companies, sorted by percentage over the 12000 mails.

DDoS

- In Nov. 2002, root DNS servers were attacked by DDoS
 - 13 top level DNS server (serving TLD) for the whole Internet
 - No major damage
 - The design of DNS already concerns DoS attack
- For other application servers....
 - Major risk/threat we have to protect

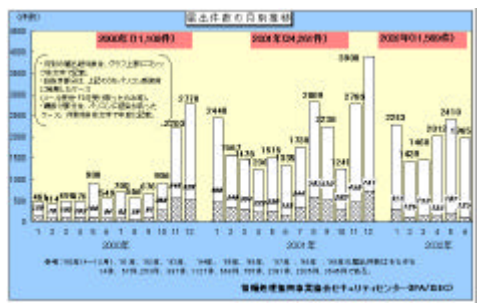
SOI Asia/Advanced Internet Technology

Actual DoS traffic



SOI Asia/Advanced Internet Technology

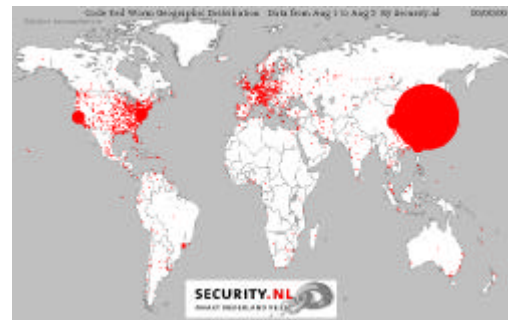
Computer Viruses



<http://www.ipa.go.jp/>

SOI Asia/Advanced Internet Technology

CodeRed



SOI Asia/Advanced Internet Technology

High tech crime

The number of arrested suspects by "high tech crime"

	2001	delta (2001 / 2000)	2000	1999	delta (2000 / 1999)
Computer crime	63	10	44	110	66
illegal	48	13	33	98	65
interferences	4	2	2	5	3
modify data	11	2	9	5	4
Ordinary crime using network	712	228	484	242	237
iconspionage	102	81	154	142	7
child porn / juveniles prostituit	248	124	121	9	112
illegat	102	50	53	23	30
defamation	42	12	30	12	18
IP infringement	28	11	28	21	7
Threat	46	28	17	35	6
misc.	151	71	80	31	49
Unauthorized access	38	4	31	31	0
合計	810	251	559	357	202

http://www.ipa.go.jp/hightech/arrest_reporokekyo_2000.htm

SOI Asia/Advanced Internet Technology

Recent research for Security

SOI Asia/Advanced Internet Technology

Threats (1)

- passive attack
 - eavesdropping, wire tapping
 - traffic analysis
- active attack
 - packet stream modification
 - Denial of Service
 - masquerading
 - unauthorized access
 - Packet spoofing
 - Replay attack
 - Others....

SOI Asia/Advanced Internet Technology

Threats (2)

- In systems
 - File and data modifications
 - Unauthorized account creation
 - Virus
 - Unauthorized copy of information
 -

SOI Asia/Advanced Internet Technology

Components we have to look into

- Information Processing Systems
 - Computers and attached devices (hardware)
 - OS and application programs (software)
- Communication System / Computer network
 - routers, switches, several datalinktechnologies (hardware)
 - Communication protocols
 - Implementation of protocols (software)

SOI Asia/Advanced Internet Technology

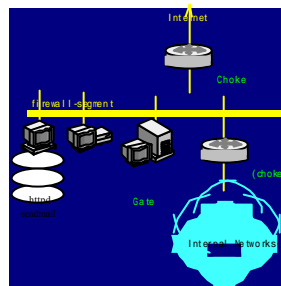
Ordinary method to protect systems

- Drop "evil" traffic
 - Packet filtering
 - SPAM filtering
 - Firewall
- Re-route traffic
 - Add resiliency against DoS
 - Check the content of the traffic
- Inspection
 - IDS, virus check,
 - Monitoring & analysis
- Cheating
 - Honeypot
- Load balancing
 - Load splitting
 - Anti-DoS configuration
- Network re-configuration
 - Out-band management

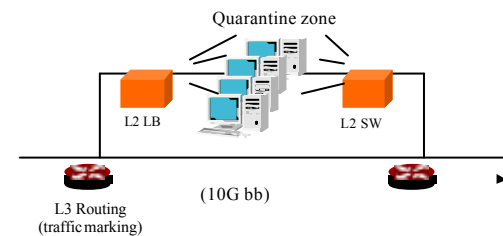
SOI Asia/Advanced Internet Technology

Firewall

- Configuration
 - "Choke & Gate" style
 - Choke
 - Filtering
 - Gate
 - Services
 - Access Control
 - Firewall-segment
 - DMZ (Demilitarized Zone)

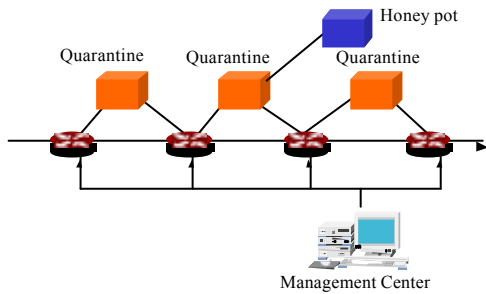


High performance FW (1)



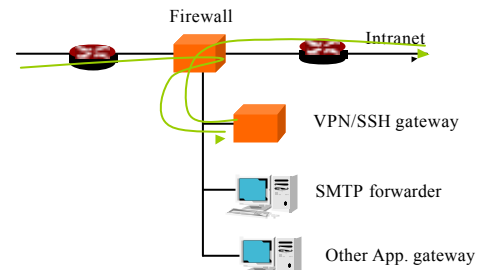
SOI Asia/Advanced Internet Technology

High performance FW (2)



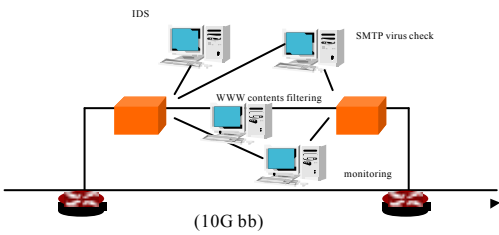
SOI Asia/Advanced Internet Technology

Multifunctional FW



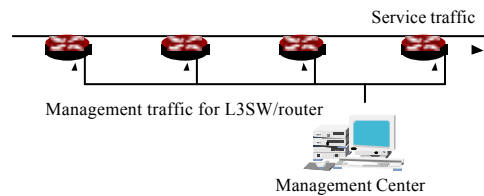
SOI Asia/Advanced Internet Technology

Ex: functional distribution at firewall



SOI Asia/Advanced Internet Technology

Out-band Management



SOI Asia/Advanced Internet Technology

Research area (1)

- Technology and engineering for network operation as well as operations of service servers
 - Adding more capacity
 - Adding more sophisticated functions
 - Adding more manageability
 - Adding more rich functionality

SOI Asia/Advanced Internet Technology

Research Areas (2)

- Technologies against attackers
- AAA
 - Authentication, authorization, accounting
 - PKI
 - Secure operating system and service servers
- Confidentiality management
 - Cipher (data encryption technology)
 - IPsec, PGP, SSH, SSL,
 - VPN, NAT, secure gateway,

SOI Asia/Advanced Internet Technology

Research Area (3)

- Digital Forensics
 - IP Traceback
 - Monitoring and recording
 - Data mining from huge information repositories
 - Logging