Cyber Attack: Urgent Demand for Protecting our Infrastructure

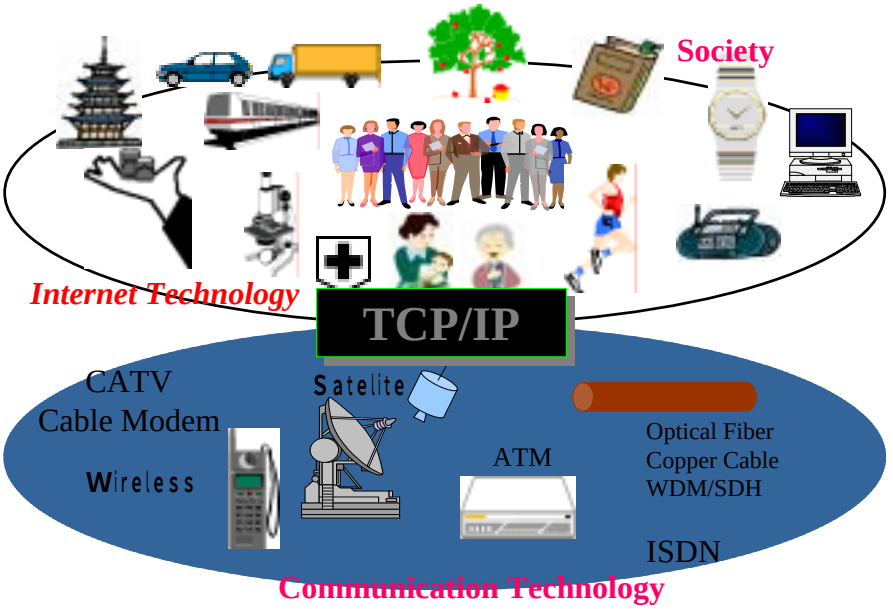
Suguru Yamaguchi
Nara Institute of Science and Technology
Japan

Overview

- Security Incidents, current situation
  - Widely & rapidly spread
  - Installing protection mechanism is required for everybody
- Role of Standardization
  - Quick development of security mechanism
  - Quick deployment of security conscious systems and protocols
  - And more…

Current situation we are facing

Internet: Global and Ubiquitous Infrastructure for Communication



Internet is now available everywhere

Source: http://www.soumu.go.jp/hakusyo/tsushin/h13/index.htm

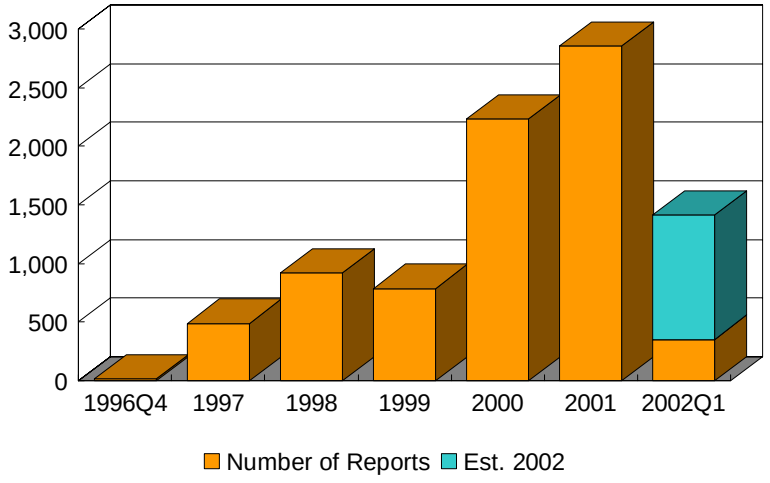
What has IT changed?

- Dedicated Internet access service
  - 20 USD / mo.
  - global IP address assignment (dynamic / static)
  - multiple Mbps to 100Mbps
  - using xDSL and Ethernet technology
  - both home and office environment
- Impact
  - FEBA: home
    - Tons of non-protected PC and other computers in home environment can be used as DoS handler, SPAM relay, packet amplifier, and others.
    - In many cases, home environment has better access than office environment. Therefore, it is quite likely to have security incidents at home environment more than office environment.

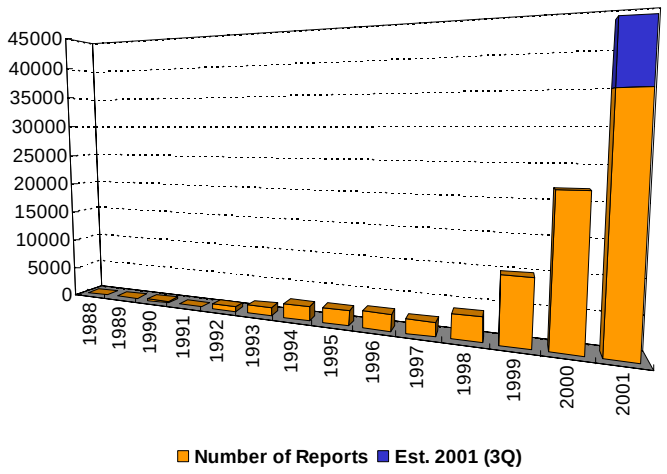
Observation

- Speed of changes
  - What we are using has been changed rapidly.
    - Only the technology can provide counter measures, in "on-time" manner.
    - It's quite good idea that regulations and laws does not touch technologies in detail. Otherwise, light-weight updating mechanism of regulations / law should be developed.
- Attacks
  - Techniques of security attacks have been developed rapidly.
  - New method has been distributed freely and widely, via the Internet
    - script kiddy can easily use the leading edge tools.
  - It is impossible to develop counter measures for each attack method, one by one.
    - core mechanism of computers and the Internet should be improved.

Statistics@JPCERT/CC



Statistics@CERT/CC



Security Incidents observed recently

- Port Scanning & Probe
  - This happen everyday in any environment.
  - Recognized as a prologue to more significant incidents
- Intrusion, break-in
  - Using weak and/or cracked password to login directly to the system.
    - But, it is quite rare in these days because of widely spread of usage of One Time Password system (challenge-response type).
  - Using “Buffer Overflow” security hole to implant and execute “shell-code” on the targeted system.
    - Almost all of the attack tools are using this method.
- Amplifier and Open relay
  - SPAM, packet smurfing, …
- Denial of Services (DoS)
  - Generate excessive load on the targeted system
  - Distributed DoS
  - Targeting major WWW, IRC server, and other services

Why attack can be conducted

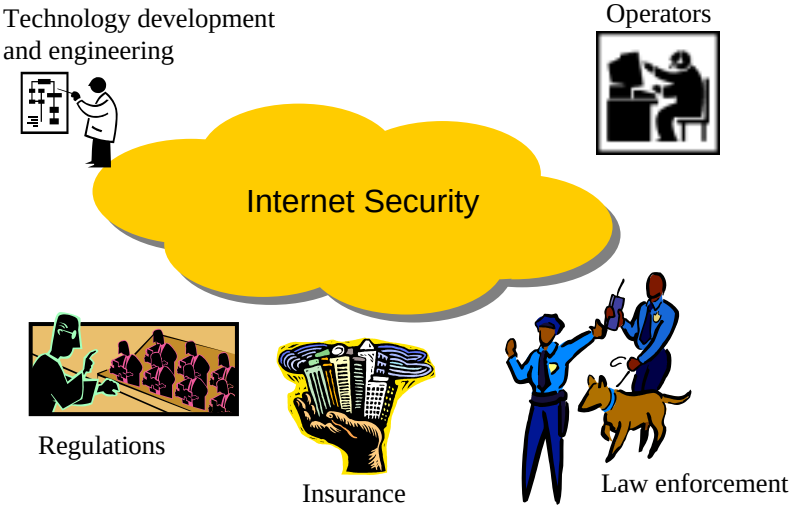
- Bad design and implementation of Operating System
  - non-protected stack
- Few security conscious protocols
  - Still non-secure protocols are existing and widely utilized.
  - Still we don't have practical protocol testing method, in terms of security
  - Many protocols is now being improved, but more efforts are required.
- Applications which security mechanisms are built in, but not as default
  - encourage vendors by market, government, community, ...
  - Let's say "We need more security stuff."
- Less focus on eliminating security holes
  - Encourage vendors to use comprehensive software testing and debug techniques

Protect Your System

- Setting up your "security policy" and operational rules for all the people involved to the network / system operations
  - Continuously applying security patches submitted by software vendors
  - Auditing and system updating in proper manner
  - It's quite rare to face attacks by unknown method.
- Making it as "business as usual"
  - Clearly defined procedures for all of us.
- Using technology
  - IDS, Firewall, audit tools, ….

More works required on “Network Security”

Who is involved?



What is issue?

- Still more technology development is required
  - Many systems and protocols are not security conscious.
  - Major working area for standardization bodies.
- There are many areas where standard is required.
  - System testing and evaluation in terms of security measures
  - Risk assessment method
  - Training for engineers, lawyers, politicians, law enforcement
  - Human resource development
  - ….

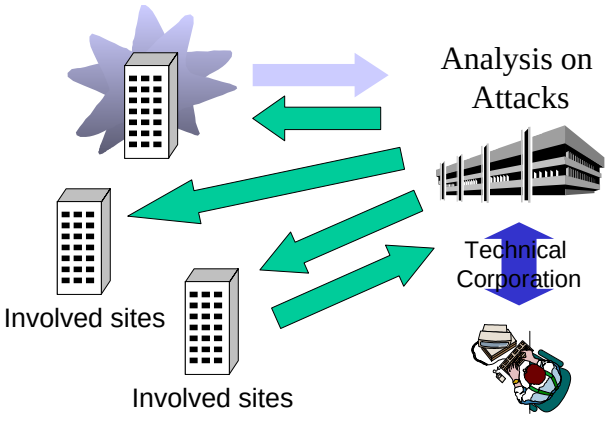
Ex: Critical Infrastructure Protection

- Many infrastructure depends on Internet and other computer oriented communication infrastructure.
  - possibility of “Cyber terrorism”
  - But, there is quite tough for developing protection mechanism of the critical infrastructure protection
    - There is no method to evaluate the system, because infrastructure is quite huge complicated & sophisticated system.
    - There are many regulations and laws directly related to its operation.
    - Sometimes, government is running the infrastructure, therefore, it is slow on decision making.
    - Normally, many ministries and department in the government should be involved when we discuss this issue. (slow enough)
    - In many cases, infrastructure uses its own proprietary systems

Ex: CSIRT

- Computer Security Incident Response Teams
  - Organization focused on computer security incidents
    - Technical professionals for analysis, assistance on problem solution, and accelerating information exchange among organization involved to the specific security incidents
    - CERT/CC, JPCERT/CC, CERT/CC-KR, AusCERT, …
  - Coordination
  - Information Switchboard

Coordination



- Providing help on problem solutions
  - Information
  - Coordination
  - confidentiality

Ex: CSIRT

- Information sharing among CSIRT is highly required when working on cases
  - No standardized way for information sharing.
  - It is hard to make the process semi-automated by IT.

More work required

- Technology is required for protecting our infrastructure, but other mechanisms are also required.
  - Operation & Social Infrastructure
  - Technology is only one of parts we need.
- Standardization is considered good, but…
  - Its process takes long time
  - Series of BCP (Best Current Practice) is more valuable for operators.