R&D Efforts on CIIP in Japan Police

Ko Ikai
Cyber Force Center,
National Police Agency, Japan
Agenda

- Duties of Japan Police
- Efforts on CIIP
- R&D Efforts on CIIP
  - Outline
  - Facilities
  - Topics
- Challenges
Duties of Japan Police

Goal:
- Maintenance of Public Safety and Order

Method:
- Crime Prevention
- Crime Containment
- Crime Investigation

Activities on CIIP:
- Prevention of Cyber Attack
- Incident Response
- Cyber Attack Investigation
Efforts on CIIP

- Quarterly Site Visit for 500 Critical Infrastructure Entities (CIE)
- Mailing List among CIE and Police
- Security Assessment for CIE systems
- Conference and Training for CIE
- 24/7/365 Centralized Monitoring
- Incident Response Support for CIE
- Research & Development on CIIP
R&D Efforts on CIIP

- **Outline**
  - Started in 2001FY
  - Total budget until 2004FY: $17.8M
  - Background:
    “If necessary technology for police is not available, develop it by ourselves.”
Facilities

- R&D System
  - Huge set of network devices such as servers, routers, firewalls, IDS and so on
  - Also used as “network device library”
Facilities

Monitoring System

- Cyber Force Center
- Router
- Dumb hub
- IDS
- Sensor (Firewall)
- VPN device
- Connection with fixed IP address registered anonymously

The Internet

x57 police sites
Topics

- Risk assessment
  - Development of a risk assessment system for critical infrastructure entities (CIE)
  - Trend analysis of malicious activities on the Internet
  - Reverse engineering of malicious codes, such as viruses, worms and exploits
  - BM on network scanner products
Topics

- Protection
  - Development of prototype firewall and anti-DoS reverse proxies
  - BM on security devices such as firewalls, IDS and anti-cyberattack features on OS and applications.
  - Literature research on incident response
Topics

- Logging
  - Development of prototype secure logging system
  - Development of supporting system for massive log analysis
Challenges

- Environmental
  - Unpopularity of the topics in Japanese academia
  - Lack of evaluation methods
- Internal
  - Lack of basic research resource
  - Little awareness inside police
Any Questions?

- Thank you.

- [http://www.cyberpolice.go.jp/](http://www.cyberpolice.go.jp/)