Research Direction for Cybersecurity

Hidehiko Tanaka

Cybersecurity No.192 Committee Chair, JSPS

Institute of Information Security

Index

1. Japanese Organization for Cyber Security
2. Needs of Basic Research for Cybersecurity
3. Research Topics
   A) Tightening of Basic Systems
   B) Development of Automatic Detection of Attacks
   C) Advancement of Management Methodology
   D) Clarification of Law Systems
   E) Information Sharing among Organizations
4. Research Cooperation
   A) JSPS (Japan Society for the Promotion of Science)
   B) Cybersecurity No.192 Committee
   C) International Cooperation

1. Japanese Organization for Cybersecurity

- Government
  - – Basic Law for Cyber Security: 2014.11/2015.1
  - – Cyber Security Strategic Headquarter : Policy Decision
  - – NISC(National center of Incident readiness and Strategy for Cybersecurity) : Practice Affairs as Control Tower
- Mid-Organization
  - JPCERT/CC, GSOC, CSSC, IPA, ACTIVE, J-SCIP, JC3
- Industry
  - SOC, CSIRT, Telecom-ISAC, Financial-ISAC, JNSA
- Research Activity
  - University, Research Institute

2. Needs of Basic Research for Cybersecurity

- Status of Current Countermeasures for Cybersecurity
  - Inherent Vulnerability of Base Systems: Non-decreasing Bugs in Computers, Operating Systems, Networks, and Software
  - The Cybersecurity of Critical Systems is at the beginning.
  - Countermeasures for each Vulnerability are Similar to a Game of whack-a-mole
  - Number of Corresponding Professionals is limited.
- Age ”Internet of Things” is coming.
  - Enormous Number of Sensors, Cars, Systems, etc. will be connected through Internet.
  - Systems under Different Design Principles will be Connected.
  - Integrated Control of Total System will be difficult.

Complexity Problems

- Clear interface definition of subsystems is required for integrity , but a difficult task in reality.
  - Information Subsystems
  - Transportation Subsystems
  - Electric Power Subsystems
  - Factory Control Subsystems
  - Financing Subsystems
  - Consumer Electronics: Vulnerable Devices(Router)
- Difficult to predict precisely the behavior of connected systems
  - system design principles of both sides differ with each other
- The connection of ambiguous subsystems induces a lot of Vulnerabilities.

The Time of Basic Research

1. Design Principle Research for Wide Area Applications
    - Establishment of Correct Systems
        - Using Formal Method of Software Design
    - Handling Methods of Connected Subsystems
        - Termination Techniques of Subsystems
        - System Continuation even at Malware Infection
    - Revisited Research
        - From New Point of View: not only of Complex Systems but of Cybersecurity
2. Expected Methodologies for Cybersecurity Research
    - Big Data Analysis
    - Artificial Intelligence
    - Growing Computer Power: Many Cores

3. Research Topics

A) **Firm Basic Systems**

a. Processing Systems
   - Hardware: Simultaneous Monitoring/Status Capturing, Hardware-assisted Taint capability
   - Operating Systems:
     - ➢ Trusted Platform Module TPM bootstrapping + Online Status Guaranty (Firm Process History, Firm System Calls)
     - ➢ Embedded Garbage Collection Facility
   - Formal Verification of Software: Detection of Vulnerability

b. Networking Systems
   - Firm Router
   - All-Time Use of Cryptograph

c. Authentication/Authorization
   - Frequent Use of User and System Level

B) Automatic Detection of Attacks

a. Present Status
   - Visualization of Activities in a System and Check by Correlation Analysis with Assist of Human Professionals

b. Automatic Detection of Malicious Activity
   - Automatic Linking of Activities in PC: Mail/System-Call by Exec Code/Process/File Access/System-Call for Sending
   - Detection of Malicious Activity through Inference of the Meaning of Each Activities-Set
   - Detection of Attacks Using Definition of Malice

c. Development of Automatic Attack Detection Systems

C) Advancement of Management Technology

a. Present Status
   - Information Security Management Systems are widely used, but unsatisfactory.

b. Need to Take Other Features into Account
   - Internal Crime/Offense Prevention
   - More Simple and Practical Selection scheme of Countermeasures
   - Useful for Persuading Executives

c. An Example of Countermeasure Selection Scheme
   - Collect Incidents/Costs in the Organization
   - Selection of Countermeasures through Evaluation of the Effectiveness in terms of Cost

D) Clarification of Law Systems

a. Present Status
   - Privacy of Correspondence, Illegal Virus Creation, Revealing of Personal/Secrecy Information

b. Clarification Required: Test and Evaluate cycle
   - Definition of Personal Information: Usage Oriented (at the Second Stage of Personal Information Protection)
   - Analysis of Header and Control Information of Message Transmission, and Computer Analysis of Secrecy Information in Blackbox: permitted or prohibited ?

c. System Example in Research
   - Encrypted Data Base with Access Policy Matching Retrieval
   - Attribute-based Encryption

E) Information Sharing Among Organization

a. Present Status

- Information Sharing and Analysis Center(ISAC) Sectors: Telecom/Heavy Industry/Financial
- CEPTOARs for Critical Information Infrastructure Protection : Cybersecurity Strategic Headquarters, Government JAPAN
- 13 Sectors: Information-Communication/Finance/Aviation/ Railway/Electricity/Gas/Gvmt/Medicine/Water/Logistics/Credit/Oil
- J-CSIP: Initiative for Cyber Security Information Partnership of Japan, 6 SIGs. for heavy industries. IPA is the Hub of sharing.

b. Enhancement of Information Sharing System

- Raising the Level of Measures and Cyber-Attack Response Capability Reflecting the Increasing Complexity, Sophistication of Cyber-Attacks

c. Public Relations Activity and International Cooperation

- Enhancement of Publicity and Bilateral Cooperation

4. Research Cooperation

R&D Structure of Japan

1. Near Term Countermeasure for Cybersecurity
   - Strategic Innovation Promotion SIP Program: National Project of Cybersecurity for Critical Information Structures
2. Mid/Long Term Research
   - Basic Research: Grant-in-Aid for Scientific Research (Competitive Funds) at JSPS, and Innovation Program of Japan Science and Technology Agency(JST)
   - University-Industry Research Collaboration scheme at JSPS: 68 operational Committees
3. JSPS Program for International Scientific Exchanges
   - Bilateral Cooperation: Joint Research Project, Joint Seminar and Researcher Exchanges

SIP Project for Cyber Security

- Countermeasure for Cybersecurity
  - Security Technology, Monitor/Analysis/Defense System
  - Target: 2020 Tokyo Olympic/Paralympic Games
  - Just Started in 2015: Prof. Goto (IISEC) Program Director
- R & D Items
  - Countermeasure Technology of Control/Communication Equipment, and Control Network
  - Realization of Common Platform for Rapid Social Implementation
  - Development of Human Resources of Security Professionals

JSPS

A) JSPS: Japan Society for the Promotion of Science

- Japan's leading funding agency and is largely funded through annual subsidies from the Japanese Ministry of Education, Culture, Sports, Science and Technology.
- University-Industry Cooperative Research Committees: Bottom-Up Scheme for Bridging Seeds and Needs

B) Cybersecurity No.192 Committee

- After 3 Years of Preliminary Research, it was Established on October 1, 2015.
- Member: From Academies and Industries (17+15)
- Objectives: Research for Assuring Infra-System Security and Information Security, from the Viewpoint of Technical and Global Governance

Research Issues of No.192 Committee

a. Analysis and Countermeasure of Information Security Risks, inside and outside Japan

b. New Technological Themes and Countermeasures for Global Open Systems

c. Technical R&D Strategy and Roadmap for Information Security in Japan

d. Security Professional Raising Strategy of medium and Long term

e. Cooperative System between Academy and Industry against Cyber Attacks

Expected Results of Activities

- Technological Development Items will be shown for Cybersecurity at the Globalized Cyber Society
- Planning such as Cooperation among Organizations, and Mechanisms of System Regulation
- Planning for the Development of Security Professionals at Universities, Government, Industries, and Public Organizations

→ Secure and Stable Operation of Cyber-Infrastructures

→ Contribution to the Globalization of Industries

C) International Collaboration

a. Bilateral Collaboration Scheme
   - Call for Proposals 05/29/2015 (closed), 11/14/2014(closed)
   - With Memorandum of Understanding : Joint Research Projects, Joint Seminar, and Researcher Exchange

b. Formation of Cooperation Groups between 2 Countries funded by each Country
   - Group of Core Members
   - Provisional Work toward the Acceptance of Application

c. Cooperated Activities
   - Periodic Workshop of Cybersecurity: Information Exchange such as Situation of Attacks, Countermeasures and R&D Results

d. Researcher Exchange: Personal Basis
   - Collaborative Research between Excellent Researchers
   - Nominates and Acceptance basis

Fin

Thank you for your attention.