Study Group on Next-Generation Information Security Policies—3rd Meeting

Summary of Minutes

1. Date and Time

Thursday, December 20, 2007; 10:00–12:00

2. Location

Special Conference Room 4, Mita Kaigisho

3. Attendees (honorifics omitted)

(1) Study Group Members (in order of Japanese alphabet)

Koichi Arimura (Telecom-ISAC Japan), Yasuo Ayazuka (NTT DoCoMo), Hiroyuki Ogura (Mitsubishi Electric Corporation, standing in for Suga), Takumi Onodera (Microsoft Corporation, standing in for Takahashi), Akira Kato (University of Tokyo), Takashi Kimura (NIFTY), Shingo Koya (Trend Micro Incorporated), Satoru Koyama (NTTPC Communications Inc), Mamoru Saito (Internet Initiative Japan Inc.), Masahiro Sata (WILLCOM, Inc.), Yoichi Shinoda (Japan Advanced Institute of Science and Technology), Masahiro Shimomura (Japan Network Security Association), Hiroki Takakura (Kyoto University), Satoru Tezuka (Hitachi, Ltd.), Koji Nakao (KDDI Corporation), Masaya Norifusa (NEC Corporation), Michikazu Fukuchi (SOFTBANK BB Corp), Toshiro Fujii (Matsushita Electric Industrial Co., Ltd.), Masayo Fujimoto (Fuji Xerox Co., Ltd.), Ichiro Mizukoshi (Nippon Telegraph and Telephone East Corporation), Hiroshi Yasuda (Tokyo Denki University), Masashi Yamauchi (Symantec Japan Research Institute, Inc.), Takahiro Yokota (KDDI Corporation), Yoshiaki Watanabe (IBM Japan, Ltd., standing in for Tokuda)

(2) Secretariat

Matsui (Deputy Director-General), Takeuchi (Director, Telecommunications System Division), Yanagishima (Director for Policy Planning, Computer Communications Division), Kawauchi (Director, IT Security Office), Murakami (Deputy Director, IT Security Office), Tanabe (Security Measures Chief, IT Security Office)

4. Agenda

(1) Opening

(2) Agenda

(i) Threats to and issues in information security

(ii) Measures against major threats and issues in the current telecommunications environment

(iii) Changes in the telecommunications environment and security measures

(iv) General discussion

(3) Others

(4) Closing

5. Summary of meeting

(1) Opening

The Secretariat reviewed the minutes of the 2nd meeting.

(2) Agenda

(i) Threats to and issues in information security

a. Current status and issues regarding digital home information appliances (Fujii)

Fujii gave an explanation based on Document 3-2.

Summary of the question-and-answer session

- Is information about incidents shared among manufacturers?

→ There is no system for sharing information. Announcements of vulnerability are made by organizations such as IPA and JPCERT/CC. Expanding the public database is one of the challenges for the future.

- Are you conducting a vulnerability analysis based on the common architecture by standardizing the home network?

→ We haven't reached the stage of actually standardizing. Each company has been working on this issue, including closed-environment services. With services provided collectively, the specifications are being unified through one-to-one discussions between companies.

- I have often heard that they cannot put expensive processor chips in home information appliances, which is why they cannot use powerful ciphers. What is the trend recently?

→ Stronger security is also requested by users, so we have been working on it. However, for expensive appliances such as TV sets, we can use a powerful cipher with high-performance components. However, I wonder if the same level of security is needed in cheap devices such as simple network cameras. Therefore we should carry out measures on an as-needed basis determined through vulnerability analyses. However, it is certain that home information appliances compare unfavorably to personal computers in terms of future expandability.

b. The effects of “major environmental changes” and new issues (Tezuka)

Tezuka gave an explanation based on Document 3-3.

Summary of the question-and-answer session

- I have the impression that the shift to a more powerful cipher due to the current cipher becoming less effective involves various processes including exchanging IC cards with those incorporating the new encryption method. What do we actually need to do?

→ The entire process involves a whole range of things. During the shift, the new and old encryption systems will coexist. Therefore we must clarify the transition procedure.

c. State of ID management in the ITU-T (Nakao)

Nakao gave an explanation based on Document 3-4.

Summary of the question-and-answer session

- What is the purpose of discussing ID management?

→ I think the purpose of the discussion is to promote partnerships among the entities that manage IDs and broaden the fields of business by unifying the framework and structure for managing IDs.

- Have you considered the point of contact between the Internet and NGN?

→ We haven’t specifically discussed it.

- What is the relationship with privacy?

→ We are currently reviewing the ID management frameworks and ID use cases, and determining what the difference with the present circumstances will be. We haven’t got to the point of discussing the relationship with privacy.

(ii) Measures against major threats and issues in the current telecommunications environment

The Secretariat gave an explanation based on Document 3-5.

(iii) Changes in the telecommunications environment and security measures

The Secretariat gave an explanation based on Document 3-6.

(iv) General discussion

(A summary of the discussion is provided separately.)

(3) Others

The Secretariat explained the future schedule.

(4) Closing

6. Summary of the general discussion

A summary of the general discussion follows.

- Promoting the “exchange of people” and the “formation of communities” is as important as reinforcing the partnerships among the parties concerned. It may be not easy to share information among companies but it is relatively easy between individuals. It is preferable to create cross-industrial and cross-company communities.
- The concept of platform services is an important one. It is crucial to clarify up to what point the responsibility lies with the user connected to the network and from which point is the control in the hands of the platform.
- When the platform certifies a device, it would be better if the platform can refuse to connect to a device that is not maintained properly as well as determine whether the device is valid.
- It is necessary to implement a mechanism that can recognize through which home gateway the communication path passes. From the viewpoint of taking measures against specific abuses and raising the awareness of users, it is vital to create and save a log that the carrier can use to trace the communication path backward.
- Does certification include “certification of trustworthiness” that indicates, for example, that this platform is trustworthy? Some kind of proof is required for network managers at least.
- Home electric appliances are often used for 10 years. In a home network or even in a ubiquitous network, we should consider an architecture that assumes a long span of time.
- Mission-oriented activities are important where the authorities and the telecommunications industry make a concerted effort to accomplish a common mission.
- The issue of how to adapt to changes is important. In Japan, many manufacturers often try to support older versions. However, making older versions obsolete is easier in terms of maintenance. Including this issue, we should consider how to respond to changes.
- A credential system, under which information security insiders can speak with frankness in an environment of trust, might be one possibility.
- As threats diversify, you have to spend money on maintaining security. We must inform the general public of this.
- To address new threats it is essential that organizations continue to operate. We need a mechanism to maintain the sustainability of organizations.
- The cost for maintaining roads is covered by taxes. I think it is not a bad idea to spend tax money to retain the security of telecommunications.

- There has been mention of a common platform. Rather than a common platform, we need, for example, to draw up guidelines for the systems that have authenticating and charging functions, so as not to inhibit individual business models.
- For the common platform, it might be necessary to require a common interface and functions as mandatory.
- Regarding the “platform,” we still have a lot of details to work out including what our basic assumptions will be. We have to brainstorm and organize our ideas.