Study Group for Next-Generation Information Security Policies—8th Meeting

Summary of Minutes

1. Date and Time

Friday, May 23, 2008, 9:30–12:00

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, Inc.), Hisao Iizuka (NEC BIGLOBE, Ltd.), Hiroyuki Ogura (Mitsubishi Electric Corporation), Akira Kato (Keio University Graduate School), Takashi Kimura (NIFTY Corporation), Satoru Koyama (NTTPC Communications Inc.), Mamoru Saito (Internet Initiative Japan Inc.), Masahiro Shimomura (Japan Network Security Association), Kazuyuki Suzuki (WILLCOM, Inc., standing in for Sata), Hiroki Takakura (Kyoto University), Ikuo Takahashi (Lawyer), Ikko Takahashi (Trend Micro Incorporated, standing in for Koya), Masakazu Takahashi (Microsoft Corporation), Satoru Tezuka (Hitachi, Ltd.), Toshifumi Tokuda (IBM Japan, 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.)

(2) Secretariat

Nakata (Director-General for Policy Planning), 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), Nagaya (Security Measures Chief, IT Security Office)

(3) Presenters

Secure Brain Corporation, NEC Corporation

4. Agenda

(1) Opening

(2) Agenda

(i) Results of opinion solicitation for the Interim Report

(ii) Threats of malware in the mobile environment and the Linux system

(iii) Activities of ISPs and the secrecy of communications

(iv) General discussion

(3) Others

(4) Closing

5. Summary of meeting

(1) Opening

The Secretariat reviewed the minutes of the 7th meeting.

(2) Agenda

(i) Results of opinion solicitation for the Interim Report

The Secretariat gave an explanation based on Document 8-2 and the members agreed on the stance of the Study Group on public comments.

(ii) Threats of malware in the mobile environment and the Linux system

a. Research of malware, etc. in the mobile environment (SecureBrain Corporation)

An explanation was given based on Document 8-3.

Summary of the question and answer session

- A description is provided on the scenario of threats. Attacks on PCs using images are emerging. This is also happening in the mobile environment, since there are many websites with images, such as profiles, which users can access, but there may be threats of being hooked in a certain manner with such websites.
- The presentation referred to collecting malware by using Bluetooth. Collection at ticket wickets at stations may be effective, apart from whether or not it is feasible. Since a commuter pass function is incorporated into mobile phones and the traffic volume is extremely high, it must be very efficient.

b. Research study on threats of malware in the Linux system (NEC Corporation)

An explanation was given based on Document 8-4.

Summary of the question and answer session

- There are various methods for attacking. Which type is more frequently used—a manual one or an automatic one?

→Presently, attacks are being made using a tool and I think there are more cases where intruders manually operate this tool.

- Provided that research and development are conducted with the initiative of the Ministry of Internal Affairs and Communications, which items do you think should be promoted?

→Currently, the secured VM project is being carried out at the Ministry of Internal Affairs and Communications. We may use technologies related to the project. There is also the fact that, even if antivirus software for the Linux system is developed, such software may actually be inoperable due to the differences in distribution and other factors. Even in cases of open source software, standardization of specifications will be necessary so that antivirus functions can be embedded by vendors as a standard option.

(iii) Activities of ISPs and the secrecy of communications

a. Activities of ISPs and the secrecy of communications (Takahashi)

Takahashi gave an explanation based on Document 8-5.

Summary of the question and answer session

- On page 46, “guidelines for large volume communications, etc.” and “guidelines concerning operation standards for bandwidth control” are listed. Those guidelines are not the official view of the government but voluntary guidelines in the private sector.

→Approaches to these guidelines are not in accordance with the current conventional context. They are not the official view of the government but they have a strong impact on telecommunications carriers and other operators, and within that limitation they are listed to show the trend in recent reviews.

→In that sense, the Ministry of Internal Affairs and Communications has already made its opinion clear on OP25B concerning nuisance mails, which may be more appropriate.

- If rights of management are granted to telecommunication carriers, the responsibilities and obligations of telecommunication carriers will be incurred as well. What do you think of the obligation to inform users of the risks as well as the responsibility in the event of occurrences of incidents?

→As far as network management is concerned, it will always be a matter of the degree of rights granted in a sense. This applies also to the relation with legal enforcement bodies.

Another example is how, and to what extent, ISPs can control communications data. However, as long as it is understood that ISPs play a certain role, a code of conduct should be established and a mechanism should be built whereby verification can be made after the fact even in the worst case. While ISPs are playing a certain role, balancing their rights and duties will be the most significant theme in the future.

- Communications content is discussed by classifying it as real time content and recorded content. As for recorded content, how should ISPs store the records? Recording content may make some users feel uncomfortable. Are discussions going to be necessary on the technical aspect, such as a method whereby records cannot be seen by anyone except for the relevant parts, which will be available when permitted by a legal enforcement body?

→Within the scopes of law, I think that individual ISPs preserve at least records at their discretion in their business. In the EU, data must be preserved in the context of national security. However, surveys have not been sufficiently conducted as to what extent such functions are implemented as business practices and what kind of impact they have.

→Preserving data is a very sensitive issue. The issue includes what percentage of data should be acquired and who can guarantee the integrity of the data. Placing the obligations of such matters, for example, on telecommunication carriers will cause a significant problem. It will be necessary for the government to provide some kind of guideline and framework indicating to what extent telecommunication carriers should be able to do this.

- As a general rule, I think that a free and open Internet is also important. However, with the mechanism that is currently in place in Japan, it will probably be difficult to achieve while maintaining healthy social and economic activities. I want discussions to be continued on the responsibility of freedom and the obligations and incurrence of costs that come with that responsibility to be carried out by relevant parties, including users, though such discussions will be held somewhere outside of this Study Group.
- On page 48, there is a mention of “clarification of the definition.” I definitely want the definition clarified. At the very least, the concept of “utilization without permission” must be clarified. Otherwise, no further action can be taken. This term is hard to use unless it is clearly defined by giving a point by point explanation like in the case of the Telecommunications Business Act.
- In order to find out how telecommunications carriers in foreign countries manage their daily operations in accordance with the relevant laws, we may be able to provide assistance by relying on our connections with telecommunications carriers’ associations

and ISPs in those countries.

- From the perspective of the telecommunications carriers, we have to deal with (1) communications that interfere with carriers' facilities and (2) communications that cause disruptions to facilities that receive the communications. Where in the table on page 8 can we find this kind of perspective?

→Interpretative books do not usually refer to such matters, and research has not covered such areas yet.

- When the standardization project at ITU-T finalized the recommendation concerning information security management guidelines for telecommunications carriers, secrecy of communications was included in its items. However, since the term, "secrecy of communications," was used only in the UK and Japan, this term has been changed to "nondisclosure of communications," meaning that information obtained during the exchange of communications shall not be disclosed to a third party. In conducting surveys on legal systems and such, one option will be to have a questionnaire where this type of activity is conducted.

→In the case of an international comparison survey, the best method will be to first make a thorough survey of the country's system—which could be the standard for an international framework—and then send out a questionnaire to various countries concerning the potential problems of that country's system in comparison with Japan's system and then visit the relevant country to find out where a survey in further detail is necessary.

(iii) General discussion

No discussion was held.

(3) Others

The Secretariat explained the future schedule.

(4) Closing