Study Group for Next-Generation Information Security Policies—5th Meeting

Summary of Minutes

1. Date and Time

Thursday, March 6, 2008, 10:00–12:00

2. Location

Special Conference Room 1, Ministry of Internal Affairs and Communications

3. Attendees (honorifics omitted)

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

Yuu Arai (LAC Co., Ltd.), Koichi Arimura (Telecom-ISAC Japan), Yasuo Ayazuka (NTT DoCoMo, Inc.), Hisao Iizuka (NEC BIGLOBE, Ltd.), Hiroyuki Ogura (Mitsubishi Electric Corporation, standing in for Suga), Takumi Onodera (Microsoft Corporation, standing in for Takahashi), Shingo Koya (Trend Micro Incorporated), Satoru Koyama (NTTPC Communications Inc.), Mamoru Saito (Internet Initiative Japan Inc.), Masahiro Sata (WILLCOM, Inc.), Masahiro Shimomura (Japan Network Security Association), Hiroki Takakura (Kyoto University), 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.), Ichiro Mizukoshi (Nippon Telegraph and Telephone East Corporation), Hiroshi Yasuda (Tokyo Denki University), Suguru Yamaguchi (Nara Institute of Science and Technology), Masashi Yamauchi (Symantec Japan Research Institute, Inc.)

(2) Secretariat

Nakata (Director-General for Policy Planning), Matsui (Deputy Director-General), Yanagishima (Director for Policy Planning, Computer Communications Division), Araki (Chief for Planning, Telecommunications Systems 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) Issues regarding information security in the future

(ii) Outline of the Interim Report

(iii) General discussion

(3) Others

(4) Closing

5. Summary of meeting

(1) Opening

The Secretariat reviewed the minutes of the 4th meeting.

(2) Agenda

(i) Threats to and issues regarding information security in the future

a. Information security in the near future – from the perspective of fourth generation mobile communications and ubiquitous networks – (Ayazuka)

Ayazuka gave an explanation based on Document 5-2.

Summary of the question and answer session

- What is the reason for the decreasing number of reported viruses over the past several years?

→We have no proven findings of it although the number is made public by the IPA Security Center. While scattering viruses had often been a form of attack in the past, recent hackers are more likely to intensively target particular individuals rather than scatter a number of viruses. We assume that such a trend is reflected in the decreasing number of viruses.

- It is suggested in your document that international cooperative measures as well as technological measures will be effective. What kinds of specific international cooperative measures do you have in mind?

→One of the approaches will be to share information of incidents and the various ways in which they occur and take cooperative measures in dealing with them. Defensive measures will be limited. It is necessary to promote studies, including offensive measures to be taken against the hacker.

- What does “making terminals open” mean?

→In the context here, it means making the terminal platform open. Terminals capable of accommodating various applications without limitation are becoming available.

- From the viewpoint of the Internet, perimeter defense does not function effectively any longer. It may be necessary to seek measures that can take advantage of the mobile

environment.

- There are increasing cases where resources are abused and, for example, used as a stepping-stone for hacking. These cases include bots. It is necessary to expose the possibility of ubiquitous devices being used to cause problems for other people.

b. Present status of increasingly-sophisticated malware (Takakura)

Takakura gave an explanation based on Document 5-3.

Summary of the question and answer session

- I have heard that problems caused by Allaple included DDoS attacks on a specified IP in Estonia, which caused an extremely significant incident there last year. Are such behaviors identified in this analysis?

→Such a function could not be identified at all. Those versions, which are scattered to deceive analyzers, are almost all garbage. However, there are a few that are different from the other tens of thousands, which seem to be tactically used for attacks. Ordinarily, analysts cannot catch up with such situations.

- Can anything about the attacks be calculated, for example, which country or territory do they operate from, based on such factors as terminal functions and network speeds?

→After checking the kind of environment the hijacked machines are from and the level of their attacking power, we see that DDoS attacks are made by focusing on the target in a pin-point manner. Because broadband is widely deployed in Japan, individual terminals in general households are estimated to have considerable attacking power.

- You mentioned the necessity of a domestic observation network. It is surely difficult to take measures without information. But what kind of network do you have in mind?

→It used to be that, wherever a honey pot was placed, it was accessed from the hackers' side. However, it is known that malware is now likely to be found if action is taken vigilantly on our side; for instance, malware is located somewhere on the web and if a user steps on it, a problem starts developing and the malware disappears after. So, what is required is a kind of tracking system that tries to step on it as if on a landmine. The most essential problem is the lack of information, which is caused by the lack of technical ability of SEs and CEs. This is due to the fact that, when asked whether a customer's important data obtained through troubleshooting experiences can be brought back to the company in order to train young SEs, most customers say no. Young engineers cannot accumulate experience at all because they are not put in an environment where they can

handle actual data.

c. Measures necessary to be taken for information security in response to future changes in the information communications environment (Fukuchi)

Fukuchi gave an explanation based on Document 5-4.

Summary of the question and answer session

- While there are certain criteria for the evaluation of regular market competition, there are no certain indices for the introduction of competitive principles in security. Therefore, in introducing competition principles in security, the competition principle may not function well unless a study is first made on such criteria. After such a process, consideration will have to be given to the relationship between market competition in business and market competition in terms of security, for example, situations in which the market share is high but the security level is low, or vice versa. It is necessary to find how to interpret or let users interpret such situations. Unless the issues are summarized in a user-oriented manner and information related to the issues is provided to users, the whole scenario will not work well.

→I agree. What I meant to say here was that a competitive relationship in the market is important because a single point of failure is likely to occur in the environment of a single system specification. The next stage would be competition in security, and it is exactly true that an evaluation system is necessary to move to that stage.

- As for suggestions that suppliers shall be responsible for security measures, I can understand that the responsibility naturally lies on the supply side in terms of protecting users or increasing the security level of individual products. On the other hand, if, for example, there are some people whose computers are infected by bots and who are informed of that fact by the CCC yet do not take any action as they have no practical problems, it may be an option to shut out such people to protect other users. What do you think is the scope of the responsibility on the providers' side?

→To the question of whether an ISP should be blamed if a user, informed of an infection by the CCC, takes no action, the answer is no. Security measures must be taken on in a hierarchical manner, where ISPs take some while PC venders take others. It is necessary to build such a kind of comprehensive framework. Efforts made by telecommunications carriers or by ISPs alone are not enough. In this sense, we should assume that security measures be maintained as a whole by building up everyone's best efforts in a multilayered

way.

(ii) Draft Outline of the Interim Report

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

(iii) General discussion

Opinions were exchanged on the “Draft Outline of the Interim Report.”

(A summary of the discussion is provided separately.)

(3) Others

The Secretariat explained the future schedule.

(4) Closing

6. Summary of the general discussion

- It will be better to first describe in detail the concept of the allocation of roles between industry and government. In 2003 or 2004, for example, measures for security were still at a low level, in which the government played a large part of the role of problem recognition compared to the industrial sector. In considering the recent results of the liberalization of and competition within the market, it is necessary, in my opinion, to formulate a system where various factors, including security, are carefully incorporated in the market principle. To this end, discussions will be necessary to specify the role of the industrial sector. It is required of the government to prepare an environment that facilitates the industrial sector’s actions, for example, by extending support to independent organizations such as Telecom-ISAC Japan.
- It may be better to specify measures for cracking down on crimes as an item for discussion. Up to now, the focus on security has been a technical discussion; however, considering the reality of increasing criminal practices, it will be necessary to clarify relationships between ISPs and consumers with the police.
- The role of academia has not been discussed much to date and it would be a good idea to clarify it.
- Five or ten years ago, there were not as many engineers involved in criminal organizations as there are now. Measures for increasing incentives for those who are engaged in sound security technology should be clearly described as well.
- Awareness campaigns are continuously required to let the general public better understand real threats to present security, including the actuality of increasing security risk.
- As can be most easily understood in the case of nuisance mails, freedom and fairness are important for the Internet. However, public interests and public nature are also required now

that the Internet has become a public domain. It may be better to consider strengthening penalties against those who infringe public interests and public nature.

- I think that personal authentication and terminal authentication are two of the more important factors in the network. In this context, I hope that emphasis is placed on the current status of the exposure to risks of secret codes, on which such authentications are based.
- What constitutes a crime; for example, making malware, transmitting malware, or placing malware somewhere in the web is not well clarified. It is necessary to add these items concerning the improvement of the legal system, including the definition of criminal acts.
- The market is now in a helpless mood due to its ineffectiveness in consulting with the police even if you are the victim of a crime. It is necessary to further encourage victims of crime to submit a criminal report.
- Considering the fact that more and more attacks are coming from abroad, I think that the issue of international cooperation, or in other words, a system of teamwork with police forces from other countries, will seem more important when we consider our own country's security.
- With NICT's Traceback Technology Development Project, a study has been conducted covering technical, operational, and legal aspects, and a practical use of such technology is becoming more viable. Since this is very important in terms of one of the frameworks of communications infrastructure, I hope this item will be added.
- Even if the address and phone number of the person who committed a crime are technically identified, it does not necessarily mean that the carrier knows who made the relevant communications. This obscurity is caused by various factors, such as the business configuration, contractual relationship and existence of public terminals. In order to pursue measures against crime, it is necessary to hold in-depth discussions again on whether anonymous communications are allowed and how relevant communication logs are and how they should be handled.
- While the role of users is referred to in the document, it would be better, in my opinion, if their role were to be described in a specific manner after having discussed what we should expect or should not expect of users in the future. There are two points to the discussion. One is whether consumers can continue to protect themselves and the other is whether those causing trouble for others, for example, functioning as stepping stone unknowingly should be criminally liable.
- I agree that it is important to discuss how the role of the user should be regarded, but I think that we should develop a mechanism to solve disputes, including ADR and a third party

arbitrating body. For example, there are various issues beyond the reach of discussion in this study group. It is desirable that a framework is in place that can be dynamically applied to those issues using a legal mechanism instead of technical standards or the like. I feel that society is becoming excessively sensitive to privacy and consumers' rights. On the other hand, the security mechanism now in progress is a very sophisticated technological matter. With a disparity between these two factors emerging now, it may be impossible to settle disputes in a classical manner. In this sense, I think that ADR and a third party arbitrator should be considered. The areas that I particularly want added include the roles of individual consumers, protection of privacy, the sophistication of technology, and the increasing complexity of disputes.

- The document suggests making it obligatory to report an incident. I think that this part should be a highlighted a little more. In my experience through the activities of Telecom-ISAC, I felt that sharing information was actually nothing but an illusion. It is no longer the case that damage is inflicted concurrently and is, thus, less likely to be clearly identified. Considering such factors, I think that a mechanism or organization like the Accidents Investigation Commission, which was established to deal with aircraft and railway accidents, will be necessary, whereby third party personnel conduct thorough investigations of incidents in accordance with changes in an increasingly sophisticated environment with the results available to the people who need them.
- In order for the industrial sector to voluntarily take action, it is very important for telecommunications carriers to perceive that they are conducting lawful business practices. For example, if eliminating spam mails is perceived as reducing the load of mail servers, security measures may be promptly promoted regardless of monetary matters. It will be necessary to have in-depth discussions on lawful business practices because telecommunications carriers may eventually be able to adopt such practices and compete with others as well.
- In managing the university's network, we are in a situation similar to that of ISPs, meaning that users often strongly claim their right to use. The method we usually use in cases where a computer is obviously infected by a virus is to notify the user and seek permission to observe the computer for another week or so and give a final notice if infection is confirmed. It may be better if an ISP notifies the user at once that his/her computer may be infected with a virus and, with permission, ISP is allowed to monitor the situation for a while if the user denied or neglected the notice. Today's discussion is focused on whether or not we should cut the line

immediately. However, I feel that such a way may put the relevant ISP in trouble because the user may switch from one ISP to another. I think such a flexible way will work even though it may seem like a lukewarm compromise.