

**Study Group for Next-Generation Information Security Policies—9th Meeting**  
**Summary of Minutes**

1. Date and Time

Wednesday June 18, 2008, 10:00–12:00

2. Location

Special Conference Room 3, Ministry of Internal Affairs and Communications

3. Attendees (honorifics omitted)

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

Koichi Arimura (Telecom-ISAC Japan), Yasuo Ayazuka (NTT DoCoMo, Inc.), Hiroyuki Ogura (Mitsubishi Electric Corporation), Takashi Kimura (NIFTY Corporation), 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), Masakazu Takahashi (Microsoft Corporation), Satoru Tezuka (Hitachi, Ltd.), Toshifumi Tokuda (IBM Japan, Ltd.), Koji Nakao (KDDI Corporation), Noriaki Harada (NEC Corporation, standing in for Norifusa), Toshiro Fujii (Matsushita Electric Industrial Co., Ltd.), Masayo Fujimoto (Fuji Xerox Co., Ltd.), Jun Matsukuma (SOFTBANK BB Corp., standing in for Fukuchi), Ichiro Mizukoshi (Nippon Telegraph and Telephone East Corporation), Akira Murakami (LAC Co., Ltd., standing in for Arai), Hiroyuki Mochizai (NEC BIGLOBE, Ltd. standing in for Iizuka), Hiroshi Yasuda (Tokyo Denki University), Masashi Yamauchi (Symantec Japan Research Institute, Inc.), Takahiro Yokota (KDDI Corporation)

(2) Secretariat

Nakata (Director-General for Policy Planning), Matsui (Deputy Director-General), Suzuki (Director, General Policy 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

NTT Information Sharing Platform Laboratories, Nara Institute of Science and Technology

#### 4. Agenda

##### (1) Opening

##### (2) Agenda

- (i) Trend in the survey study and the research and development of information security
- (ii) Draft Report
- (iii) General discussion

##### (3) Others

##### (4) Closing

#### 5. Summary of meeting

##### (1) Opening

The Secretariat reviewed the minutes of the 8th meeting.

##### (2) Agenda

##### (i) Trend in the survey study and the research and development of information security

- a. Survey of the actual situation of botnets (NTT Information Sharing Platform Laboratories)

An explanation was given based on Document 9-2.

Summary of the question and answer session

- According to your explanation, in most cases of botnets, IRC is used in the closed environments and HTTP is used in the open environments. It is not surprising that IRC is mainly used in closed environments because no downloading is involved. It seems that command-control communications are not distinguished from download communications, and a simple comparison between bots samples may lead to misunderstanding.

→Most HTTP-based bots have the same command system as BOBAX using HTTP-based C&C servers. Also in some other cases, it seemed according to their behavior that not only additional bots were downloaded but some bots were created through communications with C&C servers. Therefore, we reported that 1,226 samples used HTTP-based C&C.

- A considerable number of bots seems to have been collected. Through your analysis, what is the percentage of bots you've collected versus the number of bots spreading throughout the world? Various types of bots with various behaviors have also been observed. How many types of bots do you think there are?

→Since the types of samples spreading vary depending on individual countries and ISPs,

we have not, to this date, covered those throughout the world. The information analyzed in a single PC is not sufficient either. So, another means is to classify the types based on a sequence of activities of dynamic bots.

b. Approach to traceback technology (Nara Institute of Science and Technology)

An explanation was given based on Document 9-3.

Summary of the question and answer session

- IP traceback is technology in a comparatively low layer. Is it possible that the technology develops into the model usable in higher layers, such as personal authentication for websites or e-mails described at the beginning of the document?

→There are two aspects; one is a technological scenario and the other includes a legal scenario. Technically, even communications translated at the transport layer, such as those via NAT or steppingstones, can be traced. This technology has a mechanism whereby a unique value such as a hash value is inquired and it is transferred between ISPs. So, if the XML-based scheme is expanded to some extent, not only the hash value of each IP packet but also, for instance, a user ID can be inquired. In a sense, this mechanism can, presumably, be generalized and expanded into an application layer. This mechanism is expected to be applied to measures against information leakage and the NICT is now engaged in this kind of activity. However, once it reaches a legal scenario, the scenario is quite different, and research and discussions are conducted in the context of the secrecy of communications. But I think that if a hash value is limited to that of the header part of each IP packet, it will not cause any problems when randomly calculating and inquiring it. On the other hand, within the scope of the current interpretation, it may be illegal to process the payload content of a packet, such as user names and main e-mail texts. Legal interpretation of these areas may become a little different if IP traceback becomes more widely used and its necessity is recognized in the future.

-International standardization at ITU has been described. If we look at, for example, the reference model of OSI, communications are divided by function and the function module is classified in the service interface, the protocol interface, and the process model showing how to process the service function. Can those modules, including BTM (Border Traceback Manager), proposed as traceback modules be general function modules? If Japan and other countries have quite different systems, a significant difference in this model will cause difficulties.

→I think that modularization of the current DTM (Domain Traceback Manager) and BTM will be workable if not limited to the traceback function. Since different operation systems are usually used for the module exploring the organization and area where the provider's border is sorted out, such modularization is possibly applicable, without limitation, to traceback. One more thing is that if the respective traceback mechanisms of individual countries have more in common than usually assumed, standardization will be easier. On the other hand, if those mechanisms created by individual countries are quite different from one another, it will be difficult to merge them for standardization.

- You refer to international standardization activities in ITU "with a seven layer model for OSI as an exemplar." Does this mean that traceback is in a different layer or it is defined as a function across different layers?

→The NICT Research Center makes various modules, and we think that rough concept reference models may be created there. Such models are not limited to those with a traceback function but also include, for example, a detection system and an analysis system related to measures against bots, as well as a cooperation module that facilitates their mutual cooperation. I think that, using the analogy of a human body, there will be modules that work as the eyes, the hands, and as the brain, respectively.

## (ii) Draft Report

The Secretariat gave an explanation based on Document 9-4.

## (iii) General discussion

Discussion was mainly focused on the Draft Report.

- Terms not understandable for those without advanced ICT knowledge are used. If the target readers include the general public, it will be necessary to give consideration to them, such as attaching a glossary

→In compiling the Report, we will attach a glossary as an attached document or add the explanation of terms in footnotes.

- In Section (iii) "Enhancement of foundational research and development of cryptographic and authentication technology" on page 59, it states that, "it is necessary to continue to develop domestic technology." However, since this kind of technology cannot be implemented into products unless internationally usable, it will be better to also add some phrases like "international standardization will be promoted" or "efforts will be made so

that the technology be widely used on an international basis.”

- Figure 3-10 on page 38 reads that attacks are made intensively by a specific country rather than by various countries. It will be better to replace it since appropriate data are separately available.
  - Do ICT service providers described on page 2 include providers of products? It does not seem that they are included at first glance. It will be better to modify the expressions.
  - In the paragraph dealing with promoting the development of human resources to be engaged in information security measures on page 63, cooperation between industry and academia is not much emphasized. It will be necessary to modify the expression to one with a little more emphasis like “cooperation needs to be promoted.”
  - While adults know the history of the development of ICT, children, these days, have been surrounded by mobile phones and PCs all their lives. It will be necessary to make users aware of the risks through education.
  - The description on page 32 that suggests that “targets are more worth being attacked” will be inappropriate in the expression.
  - I think that the threats indicated on page 20 are not limited to ICT but also applicable to the whole of society. However, in Section 6, “Closing,” on page 67, the expression “secure and safe ICT environment” is used. It will be better to clarify whether the aim of this Report is limited only to the ICT environment or related to something more like social infrastructure.
- There are various threats including external ones. This Study Group has focused attention particularly on threats of malware such as bots and threats making full use of social engineering in conducting the study. There is a description also on page 21 that this Study Group focuses attention on threats brought about via this kind of network in conducting the study. So, we believe that the target of the study has been clarified.
- Traceback technology is referred to in the paragraph discussing utilization of the most advanced security technology on page 63. However, it will be better to describe the necessity of traceback technology in terms of, for instance, a deterrent power thanks to its capability of identifying the sender.
  - What kind of set do you plan to use for the release of this Report.
- We plan a set of two parts, the full text of the Report with reference documents such as a glossary attached to it and the summary version of the Report.
- I feel that the current description may lead to a scenario in which perpetual beginners can

feel secure because they are protected by the government. However, perpetual beginners cannot be 100 percent protected. It will be necessary to provide education to users to let them recognize, as well as to create, the framework to communicate the message to users, that they do not have to protect themselves alone but, also, that the government cannot protect everything.

(3) Others

The Secretariat explained the future schedule.

(4) Closing