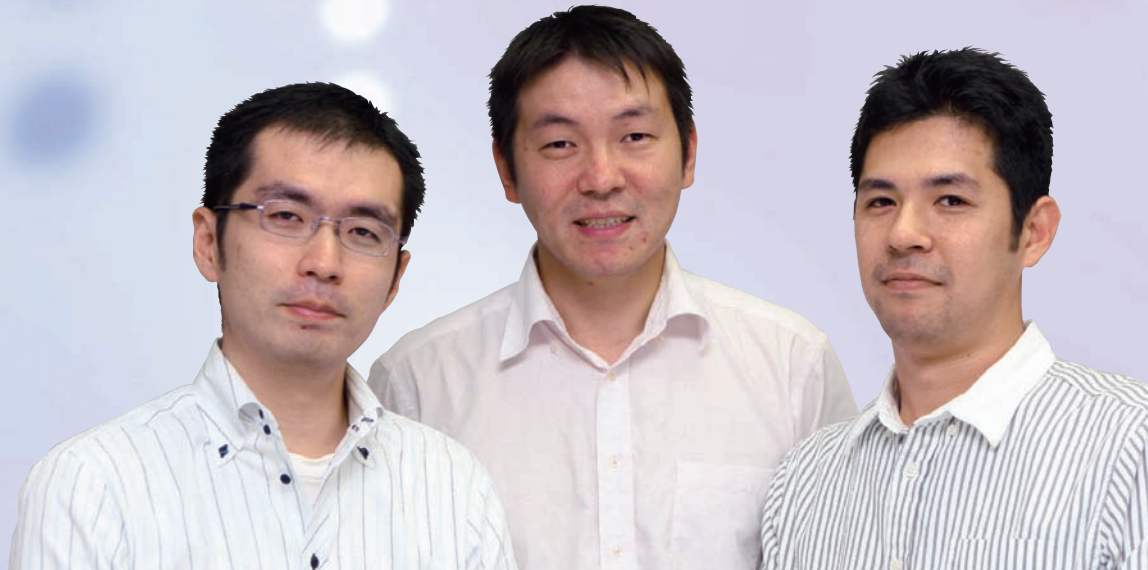
NICT 独立行政法人 情報通信研究機構 NEWS
National Institute of Information and Communications Technology
2010 OCT No.397 10

Special Feature: Traceable Network (2/2)



NiCT

P2P Network Monitoring System

Towards Traceability of Confidential File Leakage

Ruo Ando

Senior Researcher, Traceable Secure Network Group, Information Security Research Center

In March 2006, Ruo Ando completed the Media and Governance Advanced Doctoral Course at the Graduate School of Media and Governance, Keio University (Ph.D. in media and governance). In April 2006, he joined the National Institute of Information and Communications Technology (NICT) and has been engaged in the research activities on information security, cloud computing authentication, access control, and application layers network monitoring.

P2P Network Monitoring System

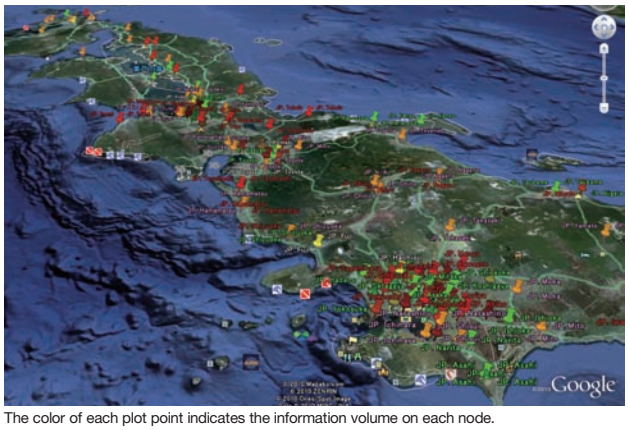
The peer-to-peer (P2P) information network leakage*[1] (of unintentional divulgence of confidential files) has given rise to social issues in recent years. While a P2P network contributes to enhancing convenience of the Internet owing to the high speed and efficiency of file transfers, it is not compatible with the monitoring approach of conventional client server models, resulting in the difficulty in determining the network operating status indicating what is happening on the network. Additionally, the issues of security incidents such as extensive distribution of illegal files containing viruses and the information leakage through P2P networks are significant. Since monitoring of P2P network needs to be a broad area, efficient monitoring is enabled by detecting supernodes with massively collected information. Traceable Network Group has developed a "probe network" for tracing and verifying the file distribution status and alteration histories on P2P networks, and is surveying the status of nodes linked to the P2P networks.

Algorithm for Accelerating the Tracing of Information Leakages

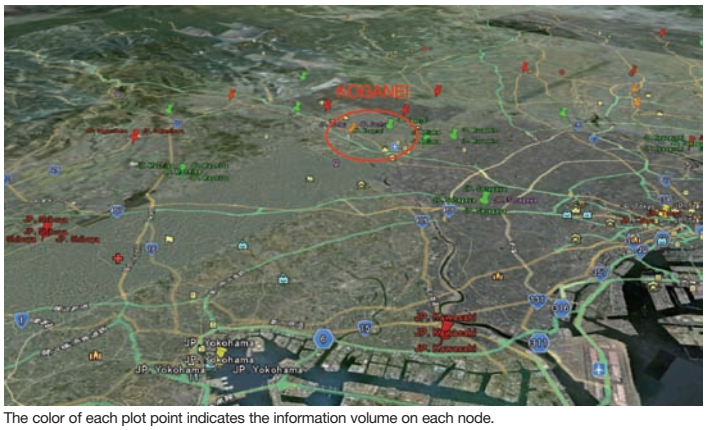
What our group is now considering as critical points in tracing information leaks on a P2P network includes the following two approaches:(1) to detect supernodes and query them to identify the file distribution status and (2) to detect altered or re-issued files by applying an algorithm to determine the degree of similitude.

Detecting Supernodes and Tracing the Status of File Distribution Status

On a P2P network, there is a single functional element called "supernode" that works at the center of a cluster (the agglomerated content of similar files). The P2P network monitoring system aims at monitoring and grasping the file distribution status in accordance with the details of a leaked file, by detecting and querying the supernode.



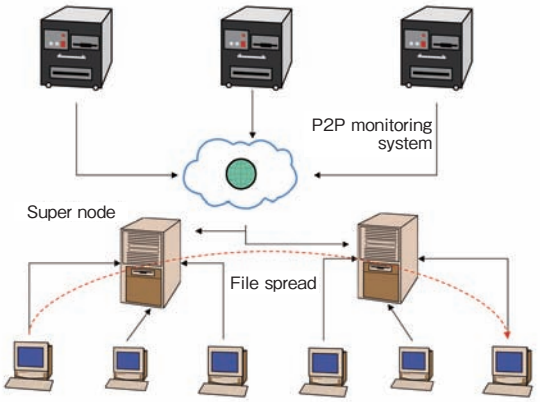
The color of each plot point indicates the information volume on each node.



The color of each plot point indicates the information volume on each node.

Figure 1●An Example of Visualizing the Distribution of Nodes

The Information Security Research Center works on the visualization of traffic monitoring log and database construction to monitor the file distribution and/or alteration status of leaked files on a P2P network.



This irradiation chart indicates the magnitude in number of node connections.

Figure 2●Detecting and Visualizing Supernodes
By monitoring supernodes, altered files are detected and their transfer status can be traced and verified. Crawling is performed to identify supernodes, and hash comparison as well as data mining*2 is conducted to detect and verify altered files.

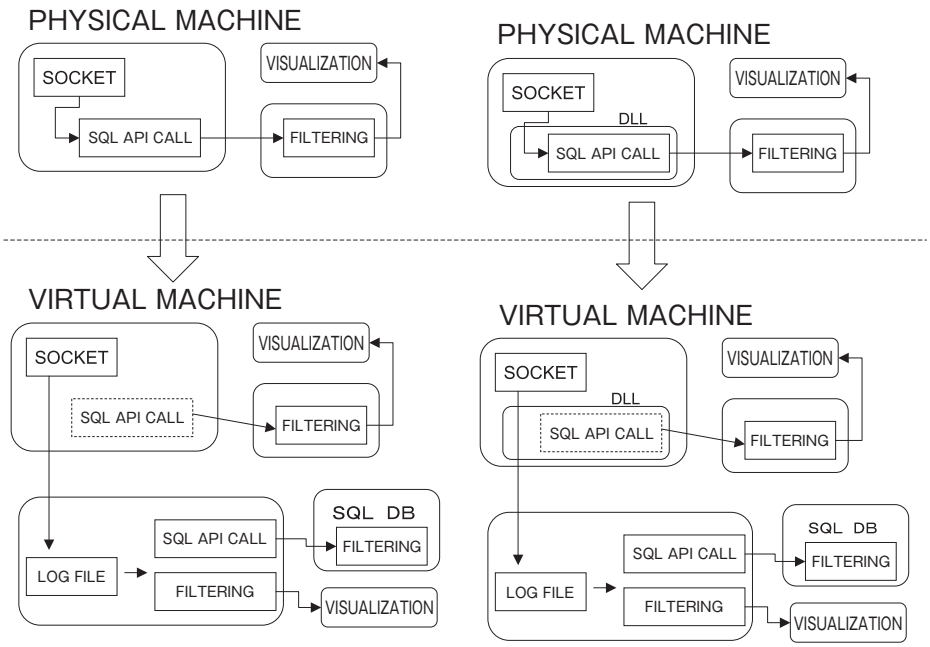


Figure 3●Strengthening the Monitoring System

Reinforcing the Systems for Wide-Area Network Monitoring

Since the P2P network that covers a wide area generates an enormous volume of monitored data, providing virtual monitoring nodes is an effective means to enhance the intensity of data accumulation. Thus, the system enables the provisioning*3 for a monitoring task of which traffic log varies dynamically and thus can hardly be assessed.

Supporting the Visualization of P2P File Distribution and Offering Public Services of Databases and Retrieval Systems

NICT is currently studying the feasibility of offering public services for P2P monitoring, databases, and retrieval systems. For details, refer to the following Web site:http://blink.nict.go.jp

Terminology

∗1 P2P network
Two or more computers on a P2P network are allowed to communicate on a direct and mutually equal basis. This system requires no such server that controls the network as a whole.

∗2 Data mining
This is a technology to analyze voluminous data accumulated on a data mining database to identify the interrelationships between items and patterns embedded in the database.

∗3 Provisioning
In such a field as voice communication and computers, the term provisioning refers to an act to enable services as required by the user.

TBNAN, a Network Traffic Monitoring and Analysis System

Towards New Generation Traceable Networks

Tao Ban

Expert Researcher, Traceable Secure Network Group, Information Security Research Center

Dr. Tao Ban received his Ph.D. degree in Engineering from Kobe University, Japan, in 2006 and since then he has been working as an expert researcher in NICT. His current research interests include network monitoring and analysis, network attack countermeasures, malware analysis, data mining, and machine learning. Ph.D. (Engineering)

Background

Traceable Network Group is now working on the development of IP traceback technology to fight against cyberterrorism attacks such as (distributed) denial of service (DDoS). By smoothing the collaboration and coordination among interconnecting ISP networks, IP traceback technology enables discovery of the attack path for an attack with spoofed IP address. However, as a reactive tool to locate attack sources and alleviate the impact of DDoS, an IP traceback system cannot operate autonomously but rely on other entities for attack detection. Moreover, performing IP traceback needs to intercept the communication channel and thus is subject to user privacy violation; it may impose load (more or less depending on specific implementation) on the traceback servers and line capacity and thus affects the performance of user network. In the following, we introduce our recent study of the Trace Back Network Analyze (TBNAN) – a starting system for the IP traceback. Equipped with attack-identifying and abnormality-detecting functions, TBNAN seeks to ensure the legitimacy and improve the effectiveness of an IP traceback system.

The TBNAN system, as a network monitoring and analyzing system (NMAS), is equipped with a function that detects the anormaly status or performance drop in the monitored computer network in an intellectual manner and sends system warnings to the network administrator. Hence, an NMAS could contribute to the protection from threats adversely affecting the network and minimization of risk and loss caused by malware[*1] or abuse of important Internet resources. NMASes often find useful applications in: (1) network server load monitoring and management, (2) intrusion sensing against external intrusions, (3) IP traceback for locating attackers using IP address spoofing, and (4) system monitoring for tracking virus propagation, malware activities, and botnet[*2] motions.

Mechanism of TBNAN

TBNAN has been developed to be an NMAS for high-speed networks and complex protocols. The TBNAN system is composed of a packet processor, a computation server, a database server, and a web server (Figure 1).

(1)The packet processor

The packet processor captures traffic going through an access

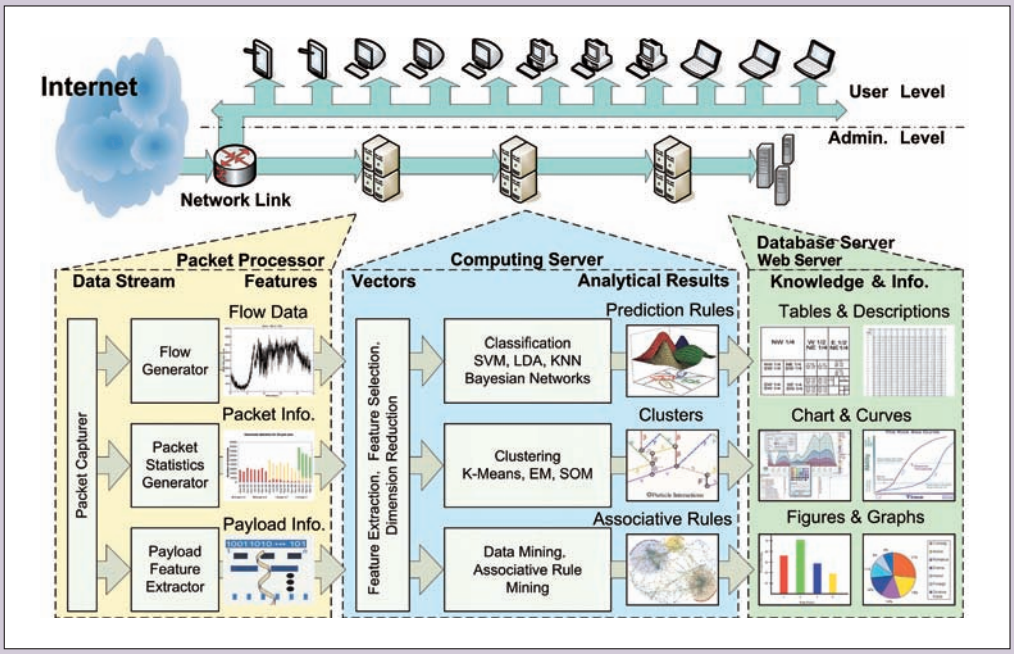


Figure 1●Configuration of TBNAN

point, extracting statistical information from the traffic, and the forword the data to the computation server. Here, statistical quantities of time, space, and flow rate are extracted from the data link layer, network layer, and transport layer. The packet processor does not inspect the payload information to protect user privacy. Therefore, it circumvents reverse engineering of protocols with encrypted payload and meets the performance requirement of real-time monitoring in a next generation broadband network.

(2)The computation server

This server creates prediction models by applying the data mining technology to received data.

[Statistical classification] This is a statistical process to categorize network streams into known classes based on their statistical characteristics. In the case shown in Figure 2, the system identifies whether or not the involved host pertains to P2P nodes by referring to the traffic related to the host. The classification is performed based on the two quantities with respect to a host, namely, (a) the number of kept connections in a unit time frame and (b) the packet volume with in the same time window. The decision function indicated with the white dotted line predicts the probability of a host being a P2P host. In the figure, nodes on the right side of the dotted line are predicted as P2P hosts.

[Anomaly detection] This method builds a model of normal network streams and detect deviations from the normal model in observed streams and predict them as anomaly states. In the case of Figure 3, the anomaly detection algorithm helps to identify port scan attackes by monitoring the communications between a host and the Internet, The detection refers to the following two quantities: (a) the number of source ports that have appeared in a unit time frame and (b) the type of TCP-Flags that have appeared in the same time window. Anomaly spots can be detected during the port scan in reference to the decision function indicated by the threshold plane (normal traffic under the plane and port scan above the plane) given in Figure 3.

In addition to the above mentioned methods, we are positively incoorperating other intelligent analytical tools such as statistical analysis and clustering metods[*5] into the TBNAN system.

(3)Database and web server

These units provide the user with the indexing and visualization services of the data imported from the computation server.

Future Perspective

In the opening age of cloud computing, computer applications will depend more heavily on networks, and at the same time, the network infrastructure and protocols will presumably gain further complexity. Therefore, the monitoring and analysis of network traffics will become an increasingly challenging task. Striving for the objective to realize the new generation networks with further enhanced stability and reliability, we aim at enabling realtime incident response under the broadband environment. To this end, we plan to incorporate the latest achievements in the theoretical field of data mining and machine learning as well as the paractical technologies such as parallel computing, hardware realization, and GPGPU computing into the TBNAN system.

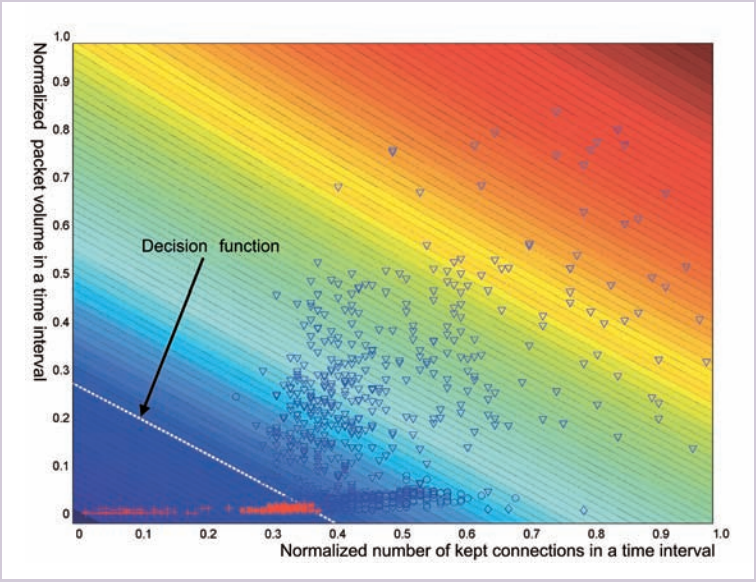


Figure 2●Grouping P2P hosts through statistical learning

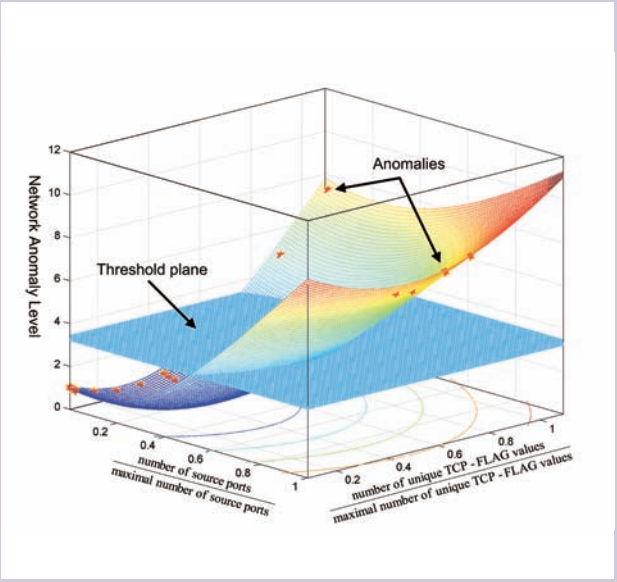


Figure 3●Sensing the port scan by detecting anomaly values

Terminology

*1 Malware
A generic name of software with malicious intent and harmful actions

*2 Botnet
This is a network that is composed of computers that have come to be manipulated by a vicious external person and remote controlled by commands issued through the Internet.

*3 Payload data
This term refers to the body data within a communication packet except such administrative data (header data) as recipient's address and source address.

*4 Reverse engineering
This is the process of discovering the specific mechanism, specifications, structuring, and/or source codes of a piece of hardware or software by disassembling the hardware or analyzing the operation of the software.

*5 Clustering
This term refers to an approach to assign a set of observations into subsets by analogy (or similarity) between data elements. Each subset is called a cluster.

An Oblivious Secret Key Encryption Scheme and Its Applications

Toward Privacy-Preserving Traceable Networks

Ryo Nojima

Senior Researcher, Traceable Secure Network Group, Information Security Research Center

Ryo Nojima received the Ph.D. degree in the Information Science in 2005. In 2005, he jointed as a postdoctoral fellow of Tokyo University. In 2006, he joined as a researcher of the Information Security Research Center, National Institute of Information and Communications Technology (NICT). His interests include applied cryptography and network security.

Background of the Research Activities

With the rapid progress of the Internet, the network security related issues such as computer viruses and denial of service (DOS) attacks are increasingly taken up. Among those issues, we, the Traceable Network Group, have so far paid attention to the specific technology called "IP-Traceback technology" for tracing illegal users who have committed the DOS attack. While the IP-Traceback technology is said to be very useful, it has the potential risk of depriving not only illegal users but also legitimate users of their privacy. Our group has thus carried on the research and development of such an IP-Traceback technology that can preserve the privacy.

The issues in the conventional IP-Traceback and the privacy-preserving IP traceback can be simplified as follows: First, imagine two users (Hanako and Taro). Let us assume that Taro keeps the set of IP addresses A= $\{a_1, \ldots, a_n\}$, while Hanako has an IP address "a". The intent of Hanako is to find whether "A" contains an "a". This problem can be resolved by Hanako sending the "a" to Taro, and Taro checking whether "a" is included in "A". In actual IP-Traceback practice, a similar interaction is performed by assuming Hanako being at the send end and Taro at the receive end. In contrast, privacy-preserving IP-Traceback raises somewhat more difficult issues. To implement this technology, it is imperative to ensure that Taro does not disclose "A" and Hanako "a" to check whether "a" is included in "A". Our group has successfully resolved this apparently insoluble problem by developing and applying a technology called Oblivious Secret Key Encryption Scheme. The following summarizes the Oblivious Secret Key Encryption Scheme and introduces its applications.

Secret Key Encryption Scheme

In the Secret Key Encryption scheme, message "M" can be encrypted by using a secret key "SK". This encrypted message is represented with the abbreviation "Enc" (SK, M) where only the person who keeps the secret key SK can extract M from Enc (SK, M). Conversely, any person without SK cannot get any piece of information relevant to M. Typical Secret Key Encryption scheme includes DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

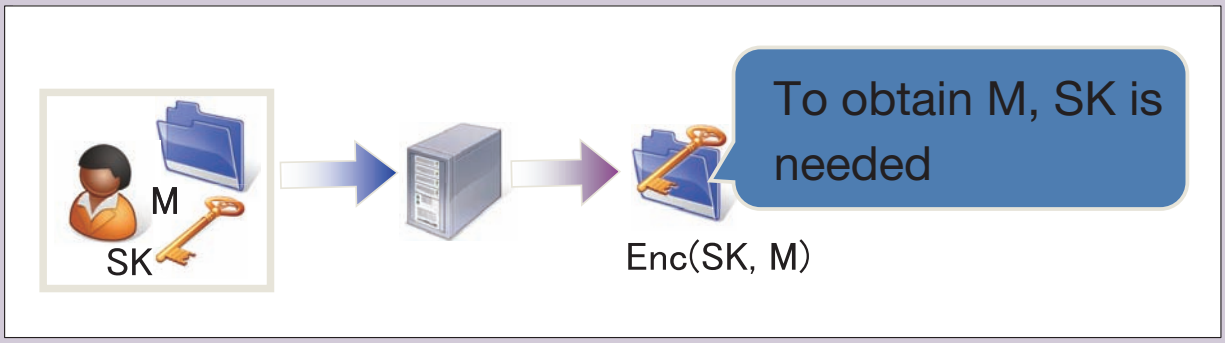


Figure 1●Illustration of Secret Key Encryption

Oblivious Secret Key Encryption Scheme

The Oblivious Secret Key Encryption Scheme (hereafter abbreviated as OEP) is a cryptographic protocol between two parties (Taro and Hanako).

Taro keeps the secret key SK to the secret key encryption, while Hanako has the message M. This protocol enables the computation of the ciphertext C = Enc (SK, M), while keeping SK and M in secret. In this protocol, Hanako can obtain C, whereas Taro cannot get any piece of information on C (Figure 2).

Our group has succeeded in the design and development of the OEP of the Secret Key Encryption scheme DES.

In this case, the term "oblivious" literally means "unaware". Since each of Taro and Hanako is "unaware" of the other party's input, the term "oblivious" has been employed for this protocol.

Applications of the OEP
IP-Traceback

In the privacy-preserving IP-Traceback technology, each of Taro and Hanako has to conceal information pertaining to the other party when verifying whether "a" is included in A = $\{a_1, \ldots, a_n\}$. This problem can simply be resolved by using the OEP in the following way:

(1) Taro selects the secret key SK of the Secret Key Encryption Scheme and sends "Enc (SK, a_1),…, En c(SK, a_n)" to Hanako.

(2) Hanako uses the OEP to get Enc (SK, a). Then, when "Enc (SK, a_1),…, Enc (SK, a_n) includes any item that will be identical with Enc (SK, a), she concludes that "a" is included in "A".

Since the use of OEP prevents the mutual leak of SK and "a", the secret data "a" of Hanako will never be leaked to Taro. Further, since SK is not leaked to Hanako, there is no risk that Taro's secret data A should be leaked from n pieces of ciphertexts to any party (Figure 3).

Cloud Storage

The technology for storing files in external servers is currently attracting interest to minimize investments in the infrastructure including servers and to realize the data consolidation. When an enterprise or other organization is to store files in external servers, the encryption of those files is obviously required. In view of user-friendliness, keyword-based retrieval may be employed. However, how can the retrieval process be applied to those files that are encrypted? The OEP enables the keyword retrieval of a text that remains encrypted.

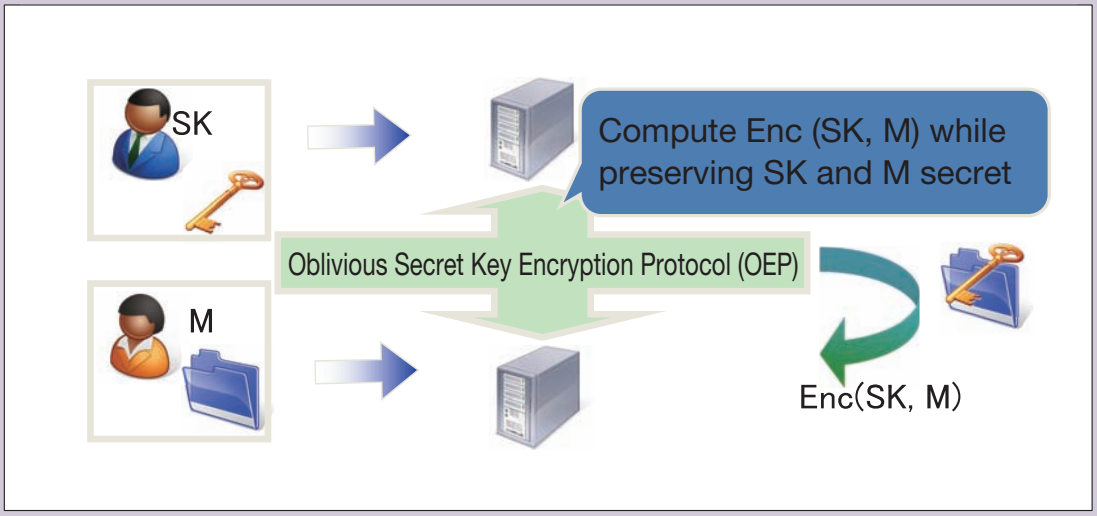


Figure 2●Illustration of OEP

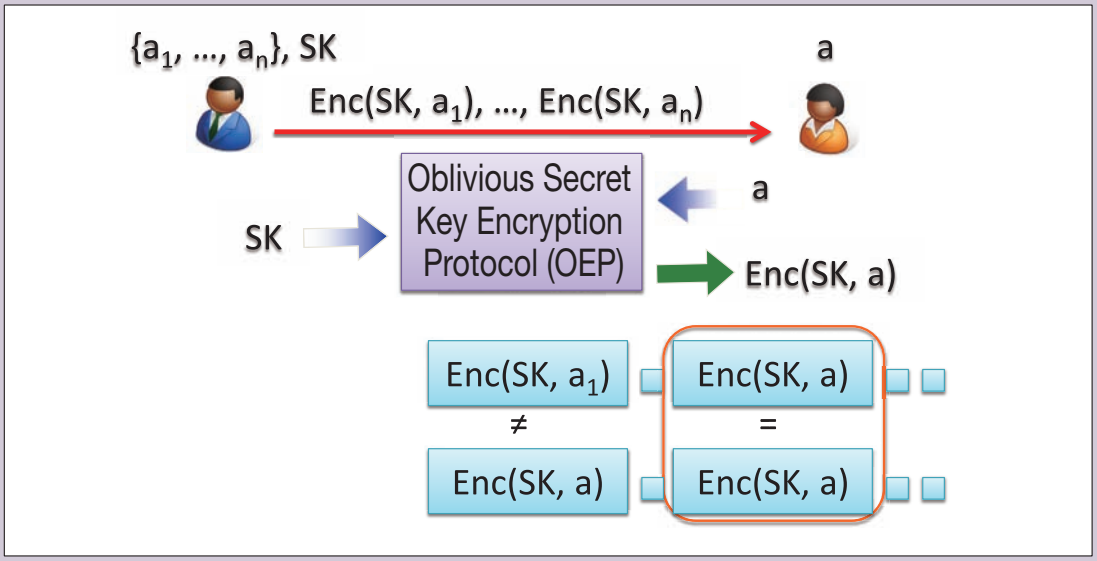
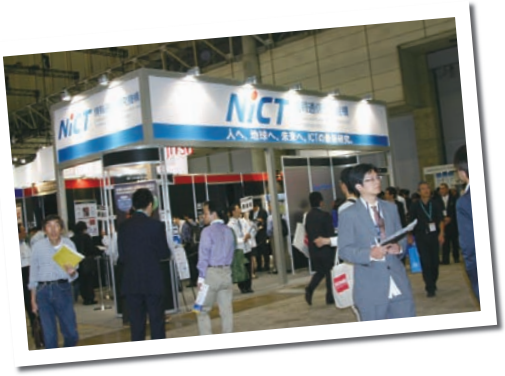


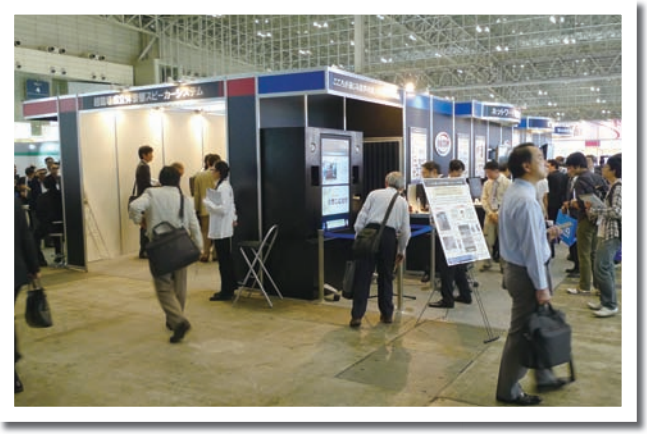
Figure 3●Illustration of Privacy-Preserving IP-Ttraceback System

Report on Our Exhibits Presented at “CEATEC JAPAN 2010”
- Universal Media Research Center and Knowledge

At "CEATEC JAPAN 2010" (Cutting-edge IT and Electronics Comprehensive Exhibition), being one of the largest exhibitions in IT and electronics fields, our exhibits were presented for this year as well (Tuesday, 5th through Saturday 9th October). Similarly to the last year and before, we held the theme "The latest ICT studies for the people, the earth, and the future" and exhibited the results of our research activities by both the Universal Media Research Center and Knowledge Creating Communication Research Center.

Of the total visitors to CEATEC as a whole of approximately 180 thousand, about 40 percent, approximately 72 thousand, called on NICT booths. A majority of visitors to this year's CEATEC watched the 3D-related exhibits that have been focused more than last year including NICT's leading-edge research results.





Exhibits from the Universal Media Research Center
-Experiencing ultra realistic communication technology, such as "stereoscopic images", "sounds" ,"tactile feelings", up to "scents"-

Multi-sensory Interaction System

A Shosoin treasure "gin-kunro", a silver incense burner, was reproduced as a 3D image.Visitors were allowed to enjoy an interactive experience of "watching, touching, listening to a sound when touched, and sniffing a imitated scent of ‘kyara’ agilawood".

World’s First 62-Channel 3D Sound System

The world’s first sound system capable of representing a moving sound source in three dimensions. This new system is able to create a 3D representation including sound source orientation and motion by emitting acoustic signals from 62 independently driven channels in different directions to compose the sound source in space.

Electronic Holography

By using a 33 million pixels ultra-high definition display device and originally developed viewing-zone enlargement technique, we demonstrated the world's first "color moving holography images with a viewing zone angle of 15° and display size of 4-cm diagonal".

Creating Communication Research Center Presented Exhibits -

Standard Test Content for 3D Images

Ultra high-definition three-dimensional live images are displayed with a 4K 3D display. Additionally, three-dimensional image content that is produced, and distributed by NICT to accelerate and support the research and development of 3D images was demonstrated.

Lectures were Given at the Exhibitor's Seminar.

Exhibitor's Seminar
Wednesday, Oct. 6, 11:00 a.m. – noon

(1) Electronic Holography Using Ultra High-definition Display Device
Kenji Yamamoto, Senior Researcher, 3D Spatial Image & Sound Group

(2) Overview of Ultra-realistic 3D Sound System
Michisato Katsumoto, Senior Researcher, 3D Spatial Image & Sound Group

(3) 4K-3D Technology and Content
Yoshiki Arakawa, Senior Researcher, Project Promotion Office

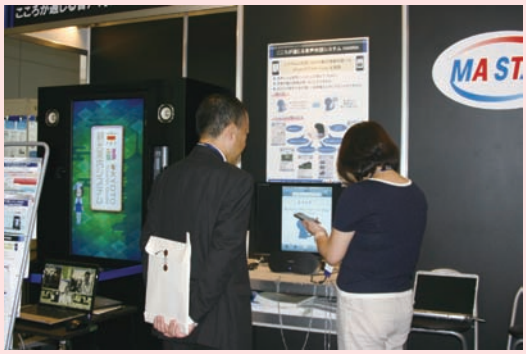
Exhibits Presented by the Knowledge Creating Communication Research Center
- Exhibits based on the leading-edge technologies of "retrieval", "recognition", and "analysis" for experiencing -

Network-based Multilingual Translation

Demonstration of iPhone applications "Textra" (text translation) and "VoiceTra" (voice translation), which are globally offered on a royalty-free basis

Voice Dialog System "HANNA"

A visitor experiences a sight-seeing guide system by posing a question before the display screen, while the system understands the user's intension of conversation and performs a natural dialog with him or her in the same way as a human guide would do.



Concept Dictionary

Beyond the keyword retrieval, this system enabled the retrieval through "category (or concept)".

Knowledge Cluster System

This system can associate the results of a retrieval using arbitrary keywords through the Internet with knowledge GRID platform, and discover its connection between phenomena and events on a combined time-space of maps and time axis.

Web Information Credibility Analysis System WISDOM (Web Information Sensibly and Discreetly Ordered and Marshaled)

This is an information analysis system designed to help users to judge the credibility of information on the Web by analyzing them from various perspectives. Visitors can input arbitrary keywords and realize its analyzing quality.

Youngster's Science Festival Halts Young Learners Move Away from the Sciences

—Report on the Exhibits at the 2010 Tokyo "Youngster's Science Festival" in Koganei—

The "2010 Youngster's Science Festival Tokyo Convention in Koganei" was held on Sunday, Sept. 12, at the Koganei Campus of Tokyo Gakugei University, where NICT presented its exhibits.

Despite such a hot day above 34℃, a number of children and their family members visited the venue. Since 1992 this Youngster's Science Festival (National Convention) has been held each year for junior high and high school students to stop moving away from science, and to offer experiencing fascination of science. Amidst various events organized throughout the nation, this regional event (Tokyo Convention), allows youths to experience the exciting aspects of natural science and thereby foster their sensibility and sharp intellect. Thus, a number of organizations, associations, and individual volunteers living in Tama area, centered around Koganei City, participated in the event.

NICT gave three presentations: "Let's watch the space weather -- Weekly Spatial Weather News --", "Let's enjoy the multi-sensory interactions!" and "Let's create clouds!"

"Let's watch the space weather -- Weekly Space Weather News --", children were curious to unusual "Space Weather Forecast" and intently stared at the screen. Similarly at the booth of "Let's enjoy the multi-sensory interactions! ", visitors experienced the multi-sensory interaction system, which has been developed by NICT to convey the multi-sensory information such as visual, acoustic, and tactile sense. It let each visitor feel the stereoscopic images, tactile sense, and touched sound of the "Kaiju-budo-kyo", a mirror with the design of animals, birds, insects and grapes (important cultural properties), which was unearthed from the "Takamatsuzuka Kofun", an ancient burial mound. The visitors appeared to be attracted to the virtual experience because they had touched such an important cultural property that could never be realized. At the "Let's create clouds! " booth, visitors experienced the joy and wonder of science by creating a small cloud of water vapor. The pressure built up inside the special container turns water (mouthwash at this time) to steam.

We gratefully acknowledge visitors including junior high school students who volunteered to help us in conducting experiments with appreciation.

Opening ceremony

creating clouds

A visitor enjoying the Multi-Sensory Interaction System

Visitors watching the Weekly provide the unit here.

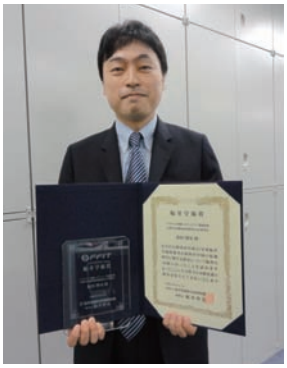
Prize Winners

Prize Winner ● Hiroshi Harada　Group Leader, Ubiquitous Mobile Communication Group, New Generation Wireless Communications Research Center

◎DATE : April 17, 2010
◎NAME OF THE PRIZE :
Funai Prize for Science
◎DETAILS OF THE PRIZE :
Achievement on Research and Development, and Standardization for Software defined and cognitive radio
◎NAME OF THE AWARDING ORGANIZATION :
FUNAI Foundation for Information Technology

◎Comments by the Winner :

I feel greatly honored that the achievement of our research and development of software radio and cognitive radio technologies has been recognized. I also gladly find that our research and development efforts have turned out to be part of the infrastructure that contributes to the build-up of the integrated network of new generation wired and wireless communications. I would like to extend my cordial appreciation to all the people who offer support to us and the members of the Ubiquitous Mobile Communication Group who are further improving the results of our studies to bring them up to a commercial stage.



Prize Winner ● Hirotaka Terai　Nano ICT Group, Kobe Advanced ICT Research Center

◎DATE : April 22, 2010
◎NAME OF THE PRIZE :
Japan Society for the Promotion of Science 146th Committee prize
◎DETAILS OF THE PRIZE :
For making significant contributions in the field of superconducting electronics
◎NAME OF THE AWARDING ORGANIZATION :
Japan Society for the Promotion of Science

◎Comments by the Winner :

We are very much honored that our research and development activities in the fields of superconductance electronics and super-conductance integrated circuits have been awarded. I extend my sincere gratitude to my colleagues as well as my superiors and seniors who have supported the subject study. Thank you very much.

Prize Winner ● Tsukasa Iwama　Research Manager, Space-Time Standards Group, New Generation Network Research Center

◎DATE : May 17, 2010
◎NAME OF THE PRIZE :
The ITU Association of Japan Award for International Activities Promotion
◎DETAILS OF THE PRIZE :
For a major contribution to the realization of the world information society through international cooperation activity in ITU and the field of information, communication, and broadcasting.
◎NAME OF THE AWARDING ORGANIZATION :
The ITU Association of Japan, Inc.

◎Comments by the Winner :

We have been awarded the ITU Association of Japan Award for the International Activities Promotion. Over the past decade, since we first attended a local ITU-R meeting (with a 3-year absence for replacement), the major agenda point during that period has been "UTC's future issues", on which we have worked and positively submitted reports from Japan. Concurrently, we have dealt with a wide variety of issues such as recommendations concerning "time for time stamping". We are indebted to those people in Japan who have supported our activities abroad by sending us encouraging e-mail messages. I would like to take this opportunity to thank all of them.

Prize Winner ● Thomas Hobiger　Researcher, Space-Time Standards Group, New Generation Network Research Center

◎DATE : May 26, 2010
◎NAME OF THE PRIZE :
EPS Award 2009
◎DETAILS OF THE PRIZE :
Ray-traced troposphere slant delays for precise point positioning (Author: Thomas Hobiger, Ryuichi Ichikawa, Tomoji Takasu, Yasuhiro Koyama, and Tetsuro Kondo)
◎NAME OF THE AWARDING ORGANIZATION :
The Society of Geomagnetism and Earth, Planetary and Space Sciences / The Seismological Society of Japan / The Volcanological Society of Japan / The Geodetic Society of Japan / The Japanese Society for Planetary Sciences

◎Comments by the Winner :

It is a great honor that my research and our resulting paper has been given the 2009 EPS Award. In the awarded paper, we propose a sophisticated ray-tracing method based on data from a high-resolution 4D meteorological model to correct for propagation delays which enables us to realize highly accurate GPS positioning. We are planning to continue this research as we expect improvements for other applications as well.

Report on Our Exhibits Presented at the "Welcome Party" of the IEICE Communications Society 2010

Daisuke Inoue, Planning Manager, Strategic Planning Office, Strategic Planning Department

The 2010 convention of the Societies of Engineering Sciences, Communications, and Electronics of the Institute of Electronics, Information and Communication Engineers (IEICE) was held on Tuesday, 14 through 17 September 2010 at the Osaka Prefecture University (Nakamozu campus).

NICT exhibited posters illustrating the overview of its activities and performed demonstrations on the "TexTra" multi-language text translator developed by the Knowledge Creating Communication Research Center and the "nicter" that is a real-time cyber attack monitoring and analyzing system developed by the Information Security Research Center for the global Internet.

The "Welcome Party" of the Communications Societies has been serving as an exchange opportunity for students as well as young engineers and researchers on actual services in the information and communications fields since 2008. NICT, as the Japan's sole research institution in information and communications fields, presents the exhibits with the aim of contributing to the relations with academia and fostering talented youths in the fields. For this year, the event had 80 or more participants in the students sector alone and a total of over 250 visitors. A number of students visited NICT's booth and posed enthusiastic questions on the NICT's R&D activities and details of the demonstrations.

A staff member answering visitors' questions

Information for Readers

The next issue will feature some of the successfully commercialized examples of research and development results and details of studies at the Keihanna Research Laboratories.

NICT NEWS No.397, October 2010 ISSN 1349-3531

Published by
Public Relations Office, Strategic Planning Department,
National Institute of Information and Communications Technology
<NICT NEWS URL> http://www.nict.go.jp/news/nict-news.html

Editorial Cooperation: Japan Space Forum

4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
Tel: +81-42-327-5392 Fax: +81-42-327-7587
E-mail: publicity@nict.go.jp
<NICT URL> http://www.nict.go.jp/index.html