ISSN 1349-3531

NiCT NEWS

National Institute of Information and Communications Technology

2005 JUN.
《No.351》

Activities of the Information Security Unit

"Toward the establishment of a nationwide research and development system"

Yuichi Matsushima, Unit Executive Director, Information Security Unit

As reported in the April issue, NICT has decided four strategic areas and established six "units" with the aim of concentrating the allocation of resources for research and development activities. This month, we will discuss the "Information Security Unit," one of the six newly established units.

1. A safe and secure ICT society

NICT has chosen a safe and secure ICT society as one of its four strategic areas in focus. To this end, we are engaged in research and development to ensure safety and security of people's lives in national and international societies, and the global environment in the future ICT society.

In the information and telecommunication fields, safety and security are based on information security technologies. In NICT's wide variety of information security activities, we emphasize the lateral coordination of research and development projects from basic to applicational stages among the related departments, as well as coordination with external organizations. This emphasis is designed to promote the unit's target of contributing to the establishment of efficient nationwide research and development systems.

2. Implementation of results

Under the direction of the Ministry of Internal Affairs and Communications, this unit has actively tackled policy tasks, enhanced international collaboration, and expedited the implementation of results. These efforts are aimed at improving information security in Japan, and include participation in international standardization efforts, practical experiments using large-scale laboratory facilities, and more (Fig. 1).

To help accomplish this objective, we have promoted coordination among projects and external organizations, uncovered new information security research and development themes, planned and supported research and development projects, and applied the results in practical settings. In promoting these research and development efforts, we hold regular information security support meetings attended by external specialists to discuss possible directions for research and development, as well as schemes for enhancing our cooperation with external organizations, from comprehensive viewpoints.

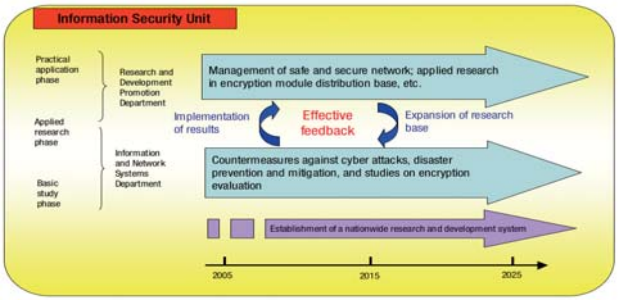
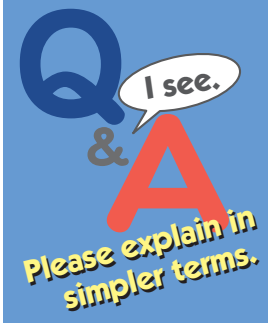


Figure 1: **Information Security Unit**

As one of the themes of the Priority Issue Solution Type in Special Coordination Funds for Promoting Science and Technology, as promoted by the Ministry of Education, Culture, Sports, Science and Technology, in fiscal 2004, our program, "Analysis of security information and development of shared systems" was adopted, and the supported researches are in progress. One of the goals of this program is to establish a cooperative system among various research organizations concerning information security in Japan (with a total of 14 such organizations, including the National Institute of Advanced Industrial Science and Technology (AIST), the Information-Technology Promotion Agency (IPA), and Keio University) to promote research and development through information sharing and effective allocation of responsibilities. NICT plays a significant organizational role in this system.



Q What are information security technologies?

A Information security technologies are designed to ensure the safety and reliability of information by preventing leaks, misinformation, unauthorized use, etc. Japan has lagged behind other advanced countries in recognizing the importance of information security and encryption techniques, as well as in establishing methods of response in these fields. However, with the rapid proliferation of the Internet, commercial transactions have become truly global in nature, and payment systems have become more and more complicated. Accordingly, various efforts have rapidly been devoted to enhancing information security, through various technologies now in daily use: ATM cards with IC chips, fingerprint authentication systems, watermark authentication, and more.

Q What is CRYPTREC?

A CRYPTREC is an acronym for the Cryptography Research and Evaluation Committee, a joint project to evaluate cryptographic techniques under the auspices of three committees: the CRYPTREC Advisory Committee (formed by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry), the CRYPTREC Evaluation Committee, and the CRYPTREC Module Committee (both jointly formed by NICT and the IPA). This project's aim is to provide information on the safety of encryption techniques used in the information and telecommunications field. Among the project's responsibilities, participants report on evaluations of cryptographic techniques and monitor e-Government-recommended cipher lists.

3. For safer and securer information and telecommunications networks

This unit is engaged in research and development in the following four fields.

• **Countermeasure technologies against cyber attacks**

Realization of sophisticated analyzing functions for early warning capabilities and technologies to enhance the security of the network itself

• **Construction of test beds**

Realization of test beds, such as devices for reproducing large-scale unauthorized access, to help unify nationwide efforts to establish a research and development system

• **Evaluation of encryption techniques**

Maintenance of robust encryption in e-Government through research and development about the design of encryption and authorization algorithms, evaluation of robustness, etc.

• **Disaster prevention and mitigation technologies**

Research and development in ad-hoc communication in disasters, information collection technologies for disasters, congestion control technologies, etc., as well as enhancing coordination with related organizations to realize large-scale proving fields of application

These research and development efforts are made in close collaboration with external implementation bodies through joint research and training, as well as studies of near practical themes entrusted to private enterprises (Fig. 2).

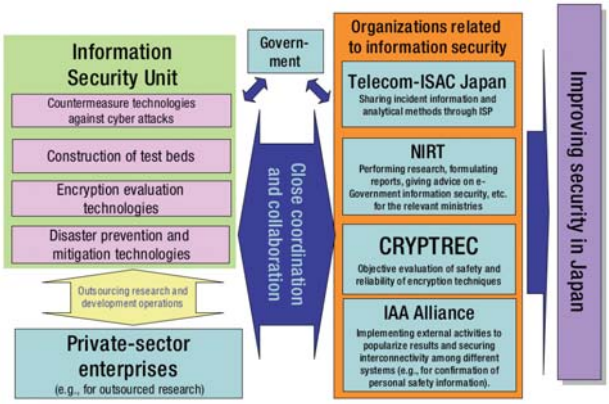


Figure 2: **Coordination of research and development with external parties**

4. Activities and research results

Since the inauguration of the unit in December 2004, we have engaged in a variety of activities, the results of which can be summarized as follows.

- Implementation of demonstration experiments for emergency/priority communication technologies required in disasters, side-channel attacks, etc.
- Basic studies on countermeasure technologies against cyber attacks, platform-building technologies for high-security services, technologies to improve safety of contents utilization, etc.
- Implementation of the verification of trace-back technologies to ensure security in large-scale networks
- Theoretical studies of encryption protocols etc, such as public key cryptography common key cryptography based on new principles, and secret sharing schemes.
- Evaluation and establishment of encryption modules, and organization of information-sharing infrastructural technologies
- Implementation of the verification of analog-tolerant electronic watermark technologies
- Information security strategy symposium held in March on joint research achievements, based on the Special Coordination Funds for Promoting Science and Technology, with Keio University, the AIST, and the IPA.

Specifically, NICT led a series of CRYPTREC surveys of a reported compromised hash function detected in the summer of 2004. As this issue impacts the very basis of the information and telecommunications society, such as electronic signatures, and time stamping, in danger of affecting services requiring high-security, we have undertaken specific, meticulous safety evaluations, through the addition of new investigation systems and so on.

As a preliminary step, the unit has made adjustments to enhance the technical review process, and has transferred CRYPTREC secretariat operations formerly handled primarily by the Research and Development Promotion Department (an outgrowth of the former Telecommunications Advancement Organization of Japan (TAO)) to the Information and Network Systems Department.

5. Establishing a nationwide research and development system

Next fiscal year, NICT starts to promote research and development based on the new mid-term plan. Threats to information security are increasingly sophisticated, often damaging many users, against a background of the progress of ICT technologies. The mid-term plan will be drawn up to drive nationwide coordination efforts, primarily led by the Cabinet Secretariat National Information Security Center (NISC), and to enable flexible responses to these threats. Another general aim of the plan is to foster greater efficiency in R&D activities through the exchange of information with various private-sector organizations.

Life & Technology

● Cryptographic techniques indispensable in a network-based society

The activities of the Information Security Unit (including those of CRYPTREC), and the specific cryptographic techniques developed, may not seem to impact our daily lives directly. However, the network society is already here, as seen in the immense use of the Internet. To take the next step toward a true e-Government, in which safety and reliability are critical, high security based on cryptographic techniques must be firmly maintained. Cryptographic techniques thus form an indispensable foundation for information security technologies, supporting the entire network society.

High-Performance Internet Data Transport Technology

"An Internet Infrastructure Extending beyond the Earth"

Kiyohide Nakauchi, Ph.D

Researcher, Internet Architecture Group
Information and Network Systems Department

Received Ph.D. degree from Department of Information and Communication Engineering, the University of Tokyo and entered CRL (NICT as of April 1, 2004) in 2003. Currently engaged in research on next-generation Internet architecture and high-performance data transport technologies, among others.

Introduction

With the widespread implementation of broadband technologies in Internet access links for home users with ADSL and FTTH (data communication services for home use), expectations are high for high-performance network applications requiring bandwidths (transmission speeds) from 100 Mbit/s to 1 Gbit/s. These applications include large-volume data delivery, high-quality video streaming, academic and professional network collaboration (remote cooperation through wide area networks), and grid computing (technology to distribute computer resources over wide area networks). Even before the full implementation of these applications, high-speed links at 1–10 Gbit/s are already in general use on the Internet backbone all over the world.

A current challenge thus lies in the development of high-performance data transport technologies through which these applications can maximize use of the bandwidths of high-speed links on the Internet .

Approaches to infrastructure technologies

Transport protocols are the foundation of communication technologies, sustaining countless exchanges of information on the Internet. These protocols perform a wide variety of important functions, such as "retransmission control," to retransmit information lost in communication pathways, "flow control," to adjust transmission timing according to a receiver's reception capability, "congestion control," to adjust transmission timing to minimize missing data due to congestion by monitoring congestion in the communication paths, and "window control," to adjust how much data should be transmitted at one time, to name but a few.

In the current Internet environment, transport protocols such as TCP (a data transport system that guarantees reliability by confirming transmission) and UDP (a data transport system without any procedures such as transmission confirmation), the prototypes of which were developed more than 20 years ago, are used as standards. However, as views of the future Internet emerge, conventional transport protocols are beginning to be found insufficient. For example, in an ultra-high-speed long-distance link at 10 Gbit/s with a round trip time of 100 ms (corresponding to the distance between Japan and the U.S.), conventional TCP can use only about 40% of bandwidth, a significantly low efficiency of bandwidth use. This problem will become even more serious for communications taking much longer round trip times, as in future interplanetary communications.

The Internet Architecture Group is currently proposing and verifying the SIRENS system (Simple Internet Resource Estimation and Notification Scheme), an explicit router feedback system supporting more advanced and flexible data transport, as an infrastructure technology for high-performance data transport. The SIRENS technology is characterized by collecting real-time information on the precise status of network resource use on the Internet, including

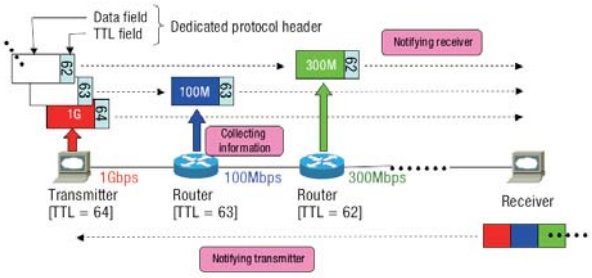
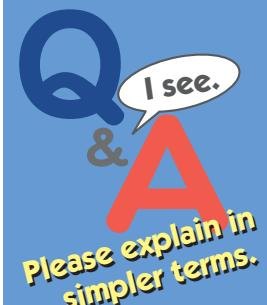


Figure 1: **Outline of SIRENS, explicit router feedback system**
In SIRENS, the sender and the receiver collect and analyze network resource information at frequencies determined by hops and packets. In this sense, SIRENS is highly versatile, robust, and simple, and is easily applicable to a wide variety of transport protocols.



Q Is there a Gigabit-level high-speed link available in Japan?

A Since April 2004, NICT has operated JGN (Japan Giga Network) II, an R&D test bed network with access points in all prefectures and in the U.S. High-speed transmission at 20 Gbit/s is available between Tokyo and Osaka and between Tokyo and Kanazawa; transmission at 10 Gbit/s is available between Osaka and Fukuoka, Kanazawa and Fukuoka, and Tokyo and Sendai. In addition, seven research centers have been established all over the country. JGN II is a successor of the R&D test bed (JGN) used from 1999 to the end of 2003 .

Q What is an emulator? Isn't it the same as a simulator?

A An emulator is different from a simulator. The former is a program for the virtual reproduction of communications with host computers, the same as in standard terminals, or of specific environments, in order to emulate procedures on a general-purpose computer (PC). On the other hand, a simulator is a device or a program to conduct simulations when actual trials are difficult due to limitations of cost, space, time, etc.

available bandwidths, link bandwidths, buffer sizes (temporary memory for packet storage within a router), and packet loss rates.

In conventional transport protocols, end-hosts conduct transmission and reception while estimating network status and its changes. In transport protocols based on SIRENS, however, end-hosts are explicitly notified of network status and its changes by each router in the path, and are capable of instantaneous and accurate recognition of these situations. Each parameter of congestion control and window control can always be optimized based on notification results, which will enable the maximum use of network resources . The basic operations of SIRENS are illustrated in Fig. 1.

Performance improvements at the time of TCP communication start

As a representative SIRENS application, we have studied an optimized limited slow start mechanism for TCP. The usual limited slow start mechanism was devised to lighten performance drops due to the burst packet drops at the time of TCP communication start in high-speed networks. However, window control parameters are set fixed, and the effective use of network resources is not achieved.

On the other hand, in the limited slow start mechanism using SIRENS, parameters can be optimized using two items of feedback information: the available bandwidth and the buffer size. At the initial stages of the TCP slow start phase and the congestion avoidance phase, much shorter convergence time and higher throughput (data volume to be transmitted within a specified time) can be achieved than in a conventional limited slow start mechanism.

First, we have developed a high-precision network (NW) emulator based on the Intel IXP2400 programmable general-purpose network processor, for high-precision evaluation and demonstration experiments of a high-performance transport protocol using SIRENS on a 1-Gbit/s high-speed network. The basic specifications of the high-precision NW emulator are shown in Table 1. The high-precision NW emulator has 1,000 times finer settable granularity (microsecond unit) and delay jitter precision (about 100 nanosecond) than Dummynet, a general-purpose software NW emulator installed as a standard in FessBSD (an open source OS similar to UNIX). Figure 2 shows a local experimental network build for its performance evaluation.

Setting item	Specifications
Bandwidth	Target bandwidth
Jitter	Target delay (in micro-seconds)
Packet loss rate, duplication rate, re-sequencing rate	1/N (1 ≤ N ≤ 2^30)
Bandwidth control system	Leaky packet system Token packet system
Header processing	Bitmax, bit comparison, overwrite (12 Bytes)

Table 1: Basic specifications of high-precision network emulator

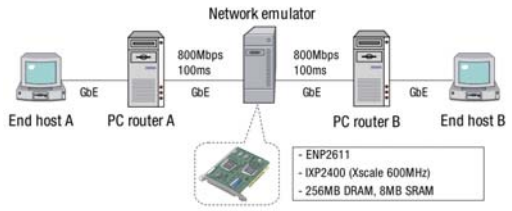


Figure 2: Experimental environment for high-performance transport protocol

The measurement results of TCP performance using the optimized limited slow start mechanism under the above experimental conditions are shown in Fig. 3. The vertical axis represents throughput, and the horizontal axis time. In the emulation environment with maximum 800 Mbit/s, the proposed system is capable of increasing throughput quickly to a maximum transmission rate of 300 Mbit/s, enabling communication without packet loss just after the time of communication start. In addition, high-level throughput is maintained even through congestion avoidance phase until congestion is first detected.

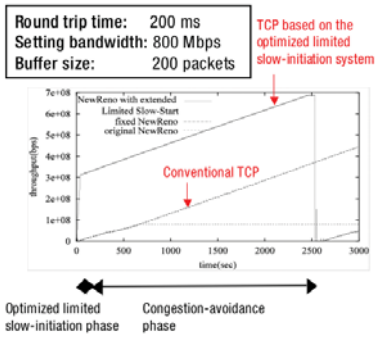


Figure 3: Performance measurement results for high-performance transport protocol

Conclusion

SIRENS can be applied to the wide variety of transports that will be newly developed, and holds great potential for further development. We plan to continue the verification of SIRENS' effectiveness in other transport protocols, and to promote its application both in Japan and abroad, with a view to its eventual adoption as a worldwide standard.

Life & Technology

● Gigabit-level backbone networks drawing attention with the evolution of the high-speed Internet society

New modes of Internet applications are continually emerging, as seen in current music and video download services. Such services require networks capable of high-speed, large-volume data transmission, for which Gigabit-level backbone networks will be indispensable, as stated above. At present, these networks are available only to researchers and specialists, but with the rapid spread of new Internet services, it is only a matter of time before this world of large-volume communications is connected directly with our daily lives.

Makoto Kusakai
Group Leader, Science and Technology Information Group
Research Support Division, General Affairs Department

Report on Science and Technology Lecture 2005

The Science and Technology Lecture 2005 was held on Saturday, April 23, at the NICT Koganei Headquarters. This week (Monday through Sunday), including Invention Day on April 18, was designated Science and Technology Week, part of a campaign to promote science and technology in Japan by deepening the general public's awareness of issues in science and technology. By this purpose, NICT holds an annual science and technology lecture at the time of year to provide easy-to-understand presentations on the achievements of our daily research. Residents in the community and their children can thus become more familiar with science and technology, hopefully countering the recent trend toward greater indifference to science among Japanese youth.

Luckily, the weather for the exhibition was as refreshing as an early summer day. Even before the scheduled opening, visitors had already gathered around the permanent exhibition rooms and the adjacent exhibition halls. When the opening announcement was made, the lecture hall was so full that many participants had to watch the lectures on a video display set up outside the hall.

The lecture session began with opening remarks from Vice President Nakata of NICT, who introduced a variety of research on information and communications conducted at NICT, with reference to familiar examples such as cell phones, the Internet, and satellite broadcasts. Nakata also touched on the relationship between our research and applications in outer space, this year's theme.

Following the opening remarks, a lecture entitled "Protect Our Spacecraft and Satellites! Robots in Space," was presented by Dr.

Dr. Shinichi Kimura (Group Leader of the Smart Satellite Technology Group) giving a lecture

Shinichi Kimura, Group Leader of the Smart Satellite Technology Group, Wireless Communications Department. Dr. Kimura showed numerous animations and slides to describe space robots designed to recover obsolete satellites and to repair malfunctioning ones. In the subsequent question-and-answer session, the children asked a number of sharp questions likely to stump even specialists, such as, "What is the total area of the solar panels used on the international space station?" "How many satellites are there around the earth?" Showing a keen concern over the problem of waste in space, children asked question such as, "What happens to broken satellites after they're put in a 20-km orbit?"

Participants assembling model rockets

The second lecture was entitled, "Reach for Outer Space," and was given by Mr. Makoto Yamada, the President of the Japan Association of Rocketry (JAR). He called the participating children "candidate astronauts," as he touched on theories of rocketry and future dreams of outer space, stimulating young imaginations throughout the afternoon program.

After the lunch break, workshops to make model rockets were held in two halls. As even small children took part in the workshops, it took longer than planned, but after all of the rockets were assembled, the finale was a splendid occasion: a launching competition among the children's creations. Three, two, one, ignition—at the moment everyone pushed their launch buttons, the air was filled with anticipation and excitement.

We hope that this event provided an opportunity for children to become more interested in science and technology.

As a final note, we would like to express our gratitude for all those who attended, cooperated in, and contributed to the success, of this event.

Launch of the model rockets

Public Relations Division, General Affairs Department

Report on Participation in Exhibitions at the Tokyo Ubiquitous Network Conference

On May 16 and 17, 2005, the "Tokyo Ubiquitous Network Conference," a WSIS (World Summit on the Information Society) Thematic Meeting on a Ubiquitous Network Society, was held at the Keio Plaza Hotel (Shinjuku Ward, Tokyo). The WSIS is held to establish and promote understanding shared visions about the information society, and to discuss, formulate, and try to realize declarations and strategic action plans for the coordinated development.

Plenary statement by President Nagao of NICT

The first summit was held in December 2003 in Geneva. Prior to the second WSIS to be held in Tunis, the capital of Tunisia, this Tokyo Conference was jointly assembled by the Japanese government (Ministry of Internal Affairs and Communications), the International Telecommunication Union (ITU), and the United Nations University. Participants included approximately 600 people from various local governments, international organizations, the private sector, NGOs, and civic groups from 82 countries around the world.

Mr. ASO, Minister of Internal Affairs and Communications of Japan, visiting the NICT exhibition

Ms. Noda, former Minister of Posts and Telecommunications, visiting an exhibition booth

At the plenary session after greetings by Mr. Aso (Minister of Internal Affairs and Communications) and Mr. Utsumi (Secretary-General of the ITU) keynote addresses were given by leading world figures, followed by various sessions. President Nagao of NICT also presented a plenary statement.

Lively discussions took place at each session and working group, and are summarized in the Chairman's report.

In the exhibition held in parallel with the conference, along the theme "Toward a Ubiquitous Network Society," NICT also presented displays on three topics: (1) interactive interface robots, (2) barrier-free maps, and (3) ubiquitous communication technologies in disaster prevention. Many conference participants from around the world, including foreign dignitaries and eleven Diet members, such as Mr. Taro Aso (Minister of Internal Affairs and Communications), former Prime Minister Yoshiro Mori, and Seiko Noda (former Minister of Posts and Telecommunications), visited the exhibitions of NICT's achievements. The mass media coverage was quite favorable, including both TV and newspaper reports.

NICT is now preparing to participate in the exhibition to be held in parallel with the second WSIS in Tunis in November. Based on the valuable experience gained in Tokyo, we are working to ensure that this next occasion will represent an even more fruitful opportunity to publicize our achievements.

Greetings from Newly Appointed Vice Presidents

— Joining National Institute of Information and Communications Technology as Vice Presidents —

As of April 1, 2005

Mutsumi Nakata

[General Affairs]

There is no doubt that information and communications technologies will rise to predominance in future international competition, a predominance that will be as evident in our daily living environments as in the international arena. While there may be an infinite number of R&D themes to be tackled, our financial and human resources are limited.

To accomplish the missions of NICT, as the only public research institute in the field of information and communications, I am determined to facilitate the continued evolution of the organization, with your assistance and encouragement.

Shingo Omori

[Core R&D]
(Information and Network Systems Department)

A few years ago, I read a newspaper article stating that a research institute is like a zoo. The contention seemed to be that the value of a research institute lies in its star residents: excellent researchers, with excellent research achievements.

NICT is a research institute, and its existence depends on its achievements, the researchers responsible for these achievements, and the support environment that surrounds them.

As the Vice President in charge of Core R&D, I intend to dedicate myself to making our institute even more highly valued by the citizens of Japan.

Facilities of National Institute of Information and Communications Technology Opened to the Public

Full of technologies that make dreams come true

Free of Charge

Annual open facility events are again planned this year to introduce our activities and research achievements, and to deepen our communication with the local community. Visitors of all ages, including primary school and junior high school students, are welcomed to gain first-hand experience of our facilities and to enjoy a range of experiments. Please feel free to drop by our facilities.

Open facilities	Opening date/time	
Koganei Headquarters	July 22, 23	10:00 am–4:00 pm
Hiraiso Solar Observatory	July 30	10:00 am–4:00 pm
Kashima Space Research Center	July 30	10:00 am–4:00 pm
Keihanna Human Info-Communication Research Center	July 30	10:00 am–4:00 pm
Kansai Advanced Research Center	July 30	10:00 am–4:00 pm
Okinawa Subtropical Environment Remote-Sensing Center	July 31	10:00 am–5:00 pm

For more details, please visit "http://www2.nict.go.jp/so/f484/2005kokai/index.html."

NiCT NEWS
Jun. 2005 No. 351

Published by:
Public Relations Division, General Affairs Department
National Institute of Information and Communications Technology

4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795 Japan
■ Tel: (042) 327-5392 ■ Fax: (042) 327-7587
■ e-mail: publicity@nict.go.jp ■ URL: http://www.nict.go.jp/

NICT NEWS at: http://www.nict.go.jp/overview/news/nict-news.html