ISSN 1349-3531

NICT NEWS

独立行政法人
情報通信研究機構

No.379
APR
2009
4

National Institute of Information and Communications Technology

Special Issues Featuring the Information Security Research Center

Aiming at the Realization of Safe the and Secure Networked Society

Information Security Research to be Promoted through Four Approaches
Yoichi Shinoda 1

Aiming at a Secure Network Environment

Introduction of Network Incident analysis Center for Tactical Emergency Response (nicter)
Kazuhiro Ohtaka 3

Measuring Security Level of Cryptographic Technologies

Missions of CRYPTREC and activities of Security Fundamentals Group
Hidema Tanaka 5

ICT Useful for Information Collection during Any Disaster

Osamu Takizawa 7

NiCT

Leadoff Interview

Information Security Research to be Promoted through Four Approaches

Aiming at the Realization of the Safe and Secure Networked Society

Yoichi Shinoda

Executive Director
Information Security Research Center

After completing a doctoral course of postgraduate school, worked for Tokyo Institute of Technology as a research fellow, and Japan Advanced Institute of Science and Technology (JAIST) as an associate professor in School of Information Science, and later, as a professor and has been working for the Institute. Also joined National Institute of Information and Communications Technology in 2006 as Executive Director in Information Security Research Center. Doubles as Advisor to National Information Security Center since 2007. Doctor of Engineering.

Information Security Research Center aims at realization of the safe and secure networked society through information communication technologies. Currently, four groups are promoting advanced researches looking ahead to the future.

Establishing a safe and secure society through information communication technologies

What researches is Information Security Research Center engaged in?

Shinoda: You might imagine computer viruses or intrusion via networks from the term "security," but we understand the concept of security as broader meaning like "safety" and "security." The relation between information communications, and technologies for safety and security has two aspects, and we are pursuing researches in these two fields: "research of safety and security technologies through information communications" and "research of safety and security technologies for information communications."

"Research of safety and security technologies through information communications" is for protecting lives and properties of people in Japan by using information communication technologies to establish a safe and secure society, which is engaged by "Disaster Management and Mitigation Group." "Research of safety and security technologies for information communications" is around cryptography of communications and tracking of data falsification, which is engaged by "Network Security Incident Response Group" and "Traceable Secure Network Group." In addition to these groups, "Security Fundamentals Group," a group mainly handling basic theories, is in charge of activities relating to both researches.

Four research groups constituting the center

What kind of research is Disaster Management and Mitigation Group pursuing?

Shinoda: Information communication technology is infrastructure for all infrastructures, in other words "meta infrastructure." Information communication technologies are used even for telephone calls, electricity distribution, and operation of transportation means. The objective of this research is how to support other infrastructures by using emergency communication systems when a disaster occurs. When an electric cable is cut, for example, the telephone switch does not work, resulting in interruption of telephone communications. The group studies how to recover the communication network in such a case. "Providing required information to the people or place which require it at required time" is a catchphrase of this group.

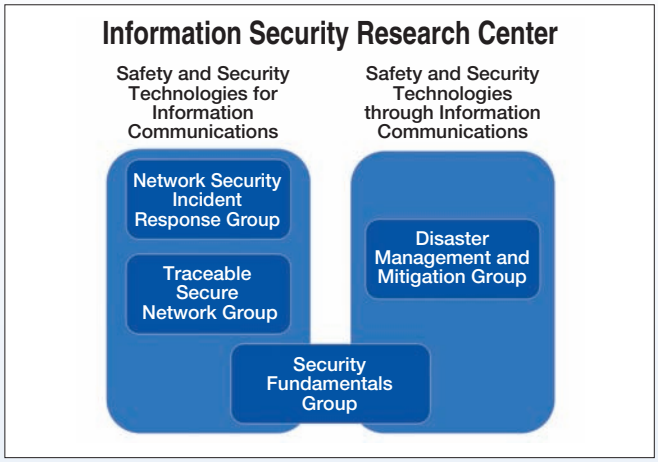
Is Security Foundations Group engaged in the research of cryptography?

Shinoda: The group aims at establishment of safe and secure communication technologies through cryptographic technology. You might think that cryptography is related to numeric figures, but in addition to that, this group is in charge of various other activities including researches for encrypting cipher itself and supporting electronic government of the central government.

Are the existing cryptographic technologies secure?

Shinoda: Verification whether the cipher system currently used is secure or not is one of their missions. The group also examines the security of various applications using cryptographic technologies developed as a system. Of course, the group is providing their technologies to other groups in our center.

Furthermore, we can identify what behaviors the electronic devices such as mobile phones or personal



Four Research Groups in Information Security Research Center

Network Incident analysis Center for Tactical Emergency Response (nicter)

computers are currently doing by analyzing the leaked electromagnetic waves of these devices. The group also studies the electromagnetic and physical security technologies to prevent information leakage.

Establishing a safe and secure tractable network

What do you mean by incident measures?

Shinoda: Incident measures mean detecting and analyzing cyber attacks of pecuniary motives or for the purposes to steal confidential information, and taking countermeasures for the resolution.

Network Security Incident Response Group is engaged in the research and development for comprehensive technologies against cyber attacks, including real-time monitoring of actual attacks which are occurring nation-wide to take direct actions, forecast of the trend on how these attacks are changing, and study of countermeasures based on the forecast. Network Incident analysis Center for Tactical Emergency Response (nicter) is a platform for real-time and automatic analysis and visualization of attacks monitored and detected on the network.

What kind of research is Traceable Secure Network Group pursuing?

Shinoda: The purpose of this group is to track problems beyond time and space. You may know a scene in a drama or movie of a telephone call tracing. That is a case of tracing the person on the other side of the telephone beyond space. While the tracing is available immediately with telephones currently used, it is not appropriately achieved with data networks represented by the Internet. Traceable Secure Network Group is aiming to overcome this issue at first to be able to trace beyond space.

The group is also engaged in the research for tracking problem occurrences beyond time. For example, when a virus activity emerges, we can prevent the same problem from its occurring if we can reproduce important moments of this incident such as the status of the moment when the virus intrudes the system.

These two groups are studying countermeasures against cyber attacks, aren't they?

Shinoda: Our center establishes a concept of "tractable network," by integrating the activities of these groups. Something like a network containing a lot of systems is likely to be unstable and subject to problems. While we can't avoid and do accept occurrence of these problem, we can detect and analyze the problems, and take actions to them, as well as tracing the source of problem and preventing its reoccurrence. The tractable network is a concept to establish a network equipping such capabilities.

"Security" is interesting because it is a comprehensive science

What about characteristics of the security research?

Shinoda: The research on security is very special. The field is complex and interesting, but it has a character that the problem itself disappears when the security technology completes. In addition, the security technology itself does not work without other technologies, such as a technology concerning information and communications, for example. In other words, the single study field of "security" does not exist, and it is a so-called comprehensive science, collecting and reconstructing knowledge accumulated so far by the research and development in other fields. Security is the mathmatics, concerning cryptography, and database and communication technologies, concerning calculation between databases. In the research of disaster management and mitigation, we are focusing on how much information human beings can receive when they are in panic, which is related to the fields of human ethology, psychology and social ethology. In addition to those, security has aspects of high performance computing technology, and the study of artificial intelligence handling "probability and analogism." Like this, we are pursuing comprehensive security researches by integrating various research fields.

Thank you very much for your cooperation today.

Aiming at a Secure Network Environment

Introduction of Network Incident analysis Center for Tactical Emergency Response (nicter)

Profile

Kazuhiro Ohtaka

Research Manager, Network Security Incident Response Group, Information Security Research Center

Joined Radio Research Laboratory (current NICT) in 1980. Was engaged in the research of ionospheric radiowave propagation, and the development of Antarctic aurora radar. Participated in the 31st and 36th Antarctic wintering teams. After being engaged in the research of space weather forecasting, is currently in charge of the research and development of Network Incident analysis Center for Tactical Emergency Response (nicter).

For protect Internet in Japan

Internet has become an indispensable tool in our daily lives. On the other hand, there is occurrence of various incidents (security accidents) everyday, including expansion of malware via Internet and associated information leakage, a huge amount of spam mails inducing users to fishing sites, and information falsification or service interruption attacks to Web servers. As countermeasures for these incidents, antivirus software and personal fire walls are introduced at user levels, and companies apply security technologies such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). These measures are security technologies to protect individual users and organizations like companies on local "points" for them. However, when we think about the entire Internet as social infrastructure, the security by protecting it on local points is not enough.

Aiming at the research and development to protect Internet in Japan, Network Security Incident Response Group of Information Security Research Center establishes and maintains Network Incident analysis Center for Tactical Emergency Response (nicter), for monitoring attacks to networks not on "points" but in "area."

Overview of nicter

The nicter consists of "Macro Analysis System" to monitor and analyze nation-wide network attacks, "Micro Analysis System" to analyze malware which is a cause of network attacks, and "Correlation Analysis System" to connect the attack status and its cause to be malware for identifying the cause (Fig. 1).

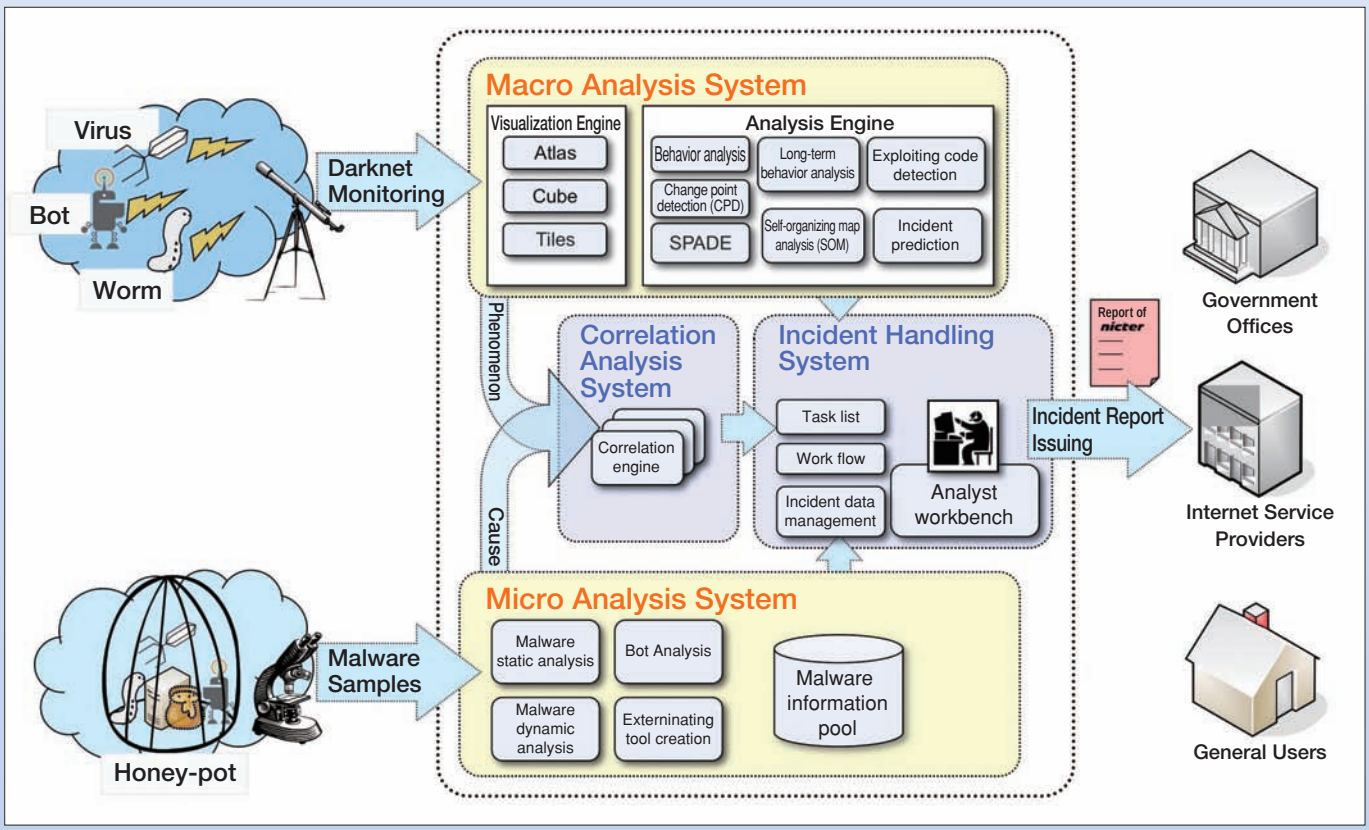


Fig.1: nicter Overview

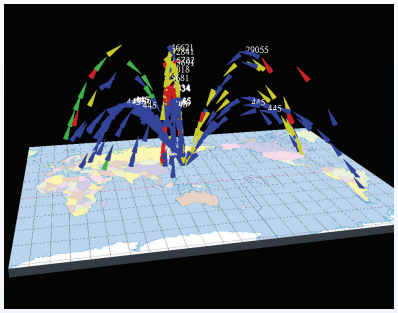


Fig.2: Atlas
This visualization engine identifies the country by the IP address of incoming packets, and displays the real-time status of how the packet is transmitted from the capital of the dispatching country to the capital of the destination country on the world map.

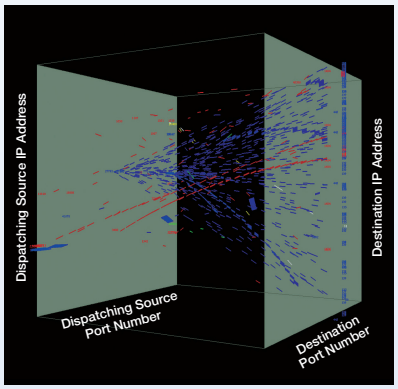


Fig.3: Cube
This is a visualization engine for displaying three dimensional animation of incoming packets observed. In this engine, two parallel faces of a cube are regarded as the dispatching source and the destination respectively, and the vertical axis represents the IP address and the horizontal axis represents the port number. By passing monitored packets from the dispatching source to the destination, statuses of scan and back scatter are visualized and understanding of the phenomenon is improved easier.

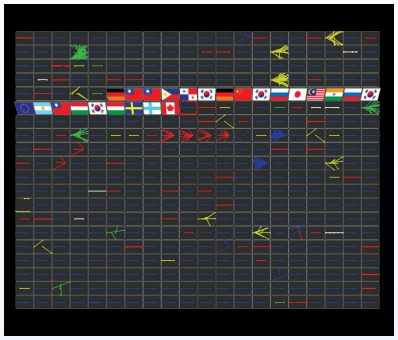
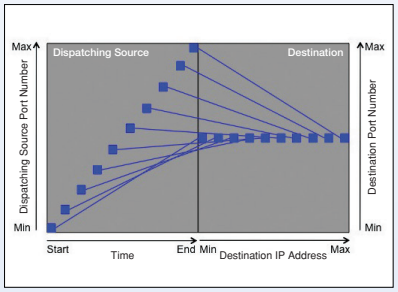


Fig.4: Tiles
This visualization engine analyses and visualizes behaviors of monitored packets by source hosts. Each of small tiles represents the behavior in each host. The engine continuously monitors these behaviors and updates as the latest analysis results as necessary. One side of a tile displays the flag of a dispatching country, and the other side of the tile displays a view using time, by dispatching the source/destination port number, and the destination IP address of packets transmitted by the destination host for 30 seconds. One packet is represented in one line. Furthermore, the engine analyses these behaviors, and notices the operator with the alert when it detects new behavior.



[Macro Analysis System]

This system monitors and analyzes in real-time what happens on Internet by watching the entire Internet. We set sensors with 120,000 or more IP address groups in total in the several base points for monitoring nationwide. These sensors are installed in the IP address space on Internet, called dark net, which is accessible but not used. Although transmitting packets to unused IP addresses does not occur in the general use of Internet, a great number of packets actually reach there. Most of these packets are transmitted for the purpose to infect malware via the network.

The visualization engines (Atlas, Cube and Tiles) (Figs. 2-4) display and allow us observe the monitored packets as real-time, intuitive, and easily understandable view of network attack statuses.

[Micro Analysis System]

This system analyses malware, the cause of network attacks. We use honey-pot, Web crawler, and other tools to collect malware. Automatic analysis of collected malware allows the analysis of up to about 2000 specimen per day. The micro analysis system uses two analysis engines, static and dynamic analysis engines, for this evaluation.

[Static Analysis Engine]

Disassembling execution codes of malware, this engine specifically analyzes functions and characteristics of malware at the assembler level. This engine extracts information including API list included in malware execution codes, and character strings of messages used for access.

[Dinamic Analysis Engine]

This engine executes malware on a real machine to analyze behaviors of API used by malware and network access. Since these behaviors begin new infection activities or network attacks if executed in a real network environment, we established an entirely isolated dummy network for this analysis.

The recent malware distinguishes the real network from the dummy network, and are unlikely to start its intrinsic infection activities or network attacks. We prepare a lot of dummy servers such as DNS and IRC which the malware uses for checking, to emulate the real Internet.

[Correlation Analysis System]

The primary characteristic of nicter is the Network and Malware Enchaining System. This system profiles scans monitored in the macro analysis system by respective characteristics, matches them with scan profiles extracted from the malware in the micro analysis system, and searches the malware with similar profile as candidate. Like this, the fusion of both macro and micro analysis results allows the identification of incidents currently occurring and the malware to be their cause, as well as leading to actions according to the identified malware.

Aiming at more refined incident countermeasures

This article introduces Network Incident analysis Center for Tactical Emergency Response (nicter) which aims at the early detection of security incidents, cause analysis, and derivation of measurements, by matching the network monitoring through the macro analysis system and malware analysis results from the micro analysis system.

In the future research and development, we will aim at providing more refined incident measures in real-time.

Measuring Security Level of Cryptographic Technologies

Missions of CRYPTREC and activities of Security Fundamentals Group

Profile

Hidema Tanaka
Senior Researcher
Security Fundamentals Group
Information Security Research Center

After completing a doctoral course of postgraduate school, worked for Tokyo University of Science as a research fellow. Joined Communications Research Laboratory (current NICT) in 2002. Has been engaged in researches including current cryptographic theory, information security, information theory and code theory. Doctor of Engineering.

Fundamental technology to ensure security

Accompanying the development of e-commerce, electronic authentication in e-government and electronic money on the information communication network, ensuring confidentiality and integrity (not being compromised) of information is essential for establishment of the safe and secure social infrastructure. In such network environment, the fundamental technology to ensure security is cryptography. Cryptography is applied as an elemental technology in many aspects of these environments and unconsciously used in our daily activities such as online shopping, ETC on expressways, document request to governments by using the Basic Resident Register card, Osaifu-ketai" (wallet-mobile), and electronic money.

Security evaluation of cryptography

Security Fundamentals Group of NICT is engaged in the research on analysis methods of cryptography and returns outcomes of the research to the society as guidelines for secure design methods and usage restrictions of cryptographic technologies. One of the specific examples of our social deployment is the operation and management of Cryptography Research and Evaluation Committees (CRYPTREC: http://www.cryptrec.go.jp), which refers to a project to evaluate cryptographic technologies, in collaboration with government ministries including Ministry of Internal Affairs and Communications. Especially, this project monitors ciphers listed on e-Government Recommended Ciphers List (hereinafter referred to as "the list"), and reports technical guidance required for aging degradation of security. These reports are reflected on "Standards for Information Security Measures for the Central Government Computer Systems (the 4th edition)."

Furthermore, we are forecasting the compromise (a status not completely critical but serious) of RSA, a public key encryption which is currently used in various applications. The security of RSA can be estimated by the computer resources required for prime-factor-decomposed computation (* See the supplementary reference.) of large composite numbers. Numbers of 1024 bits, the most commonly used composite numbers, will be factorized as early as by 2020 if the top performance of computers is assumed to be continuously increased by the current improvement ratio in the future (Fig.1). Based on this estimation, it becomes necessary for RSA to use larger composite numbers than 1024 bits in the near future. In response to the growing focus on the method using proprietary hardware, we developed the world's first proprietary hardware in the commissioning research by Collaborative Research Department of NICT (Research and Development concerning Technological Evaluation of Cryptography Based on the Difficulty of Prime-Factor-Decomposed Computation: Fujitsu Laboratories Ltd.)

As shown above, we should consider the daily degradation of cryptography strength by the synergetic effects of progress of algorism and advancement of technologies.

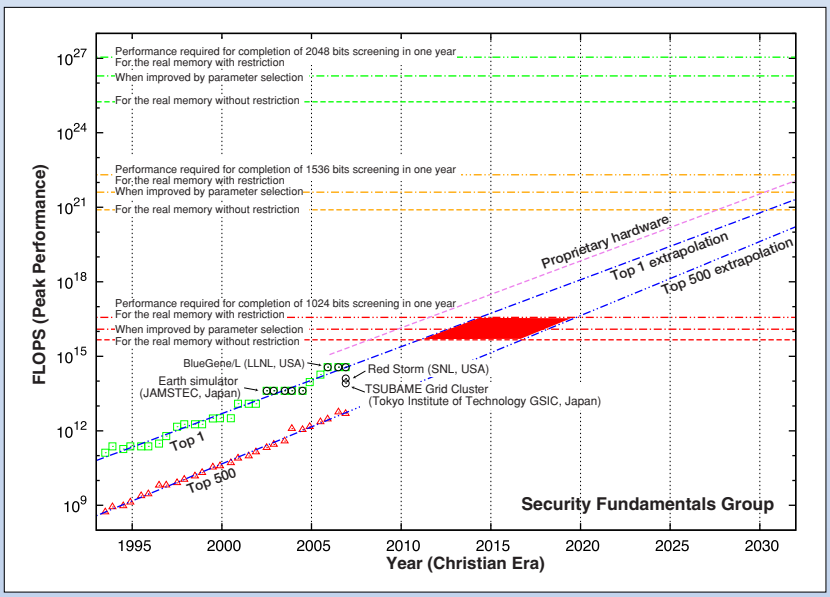


Fig.1: Prediction of Processing Performance Required for Completion of Screening in One Year

Expiration date of cryptographic technologies and migration issue

Cryptography has expiration date for secure use, which requires us to migrate to the next cryptographic technology.

Based on the evaluation results of CRYPTREC, public key encryption RSA 1024 and hash function SHA-1 currently used in e-government are scheduled to be transferred to RSA 2048 and SHA-256 by 2013 respectively (according to "Guidelines for Migration of Cryptography Algorism SHA-1 and RSA 1024 currently used in the Central Government Computer Systems" issued by National Information Security Center). The resultant systems required to be transferred are:

- Δ Authentication Infrastructure of the Central Government
- Δ Authentication Infrastructure of Local Governments
- Δ Electronic Signature and Authentication Services
- Δ Electronic Authentication System Based on Commercial Registration
- Δ Laws concerning Electronic Signature and Authentication Services

Migration of cryptography is a real problem which requires a huge amount of budget. Moreover, the daily operation should continue during the migration and the data after the migration should retain compatibility with the previous data. In the future, the feasibility and procurement cost as well as security will be considered as selection criteria.

(Note: RSA 2048 and SHA-256 are recommended cryptography for electronic government.)

Mission of CRYPTREC and contribution of Security Fundamentals Group

The list currently used was established in 2003. We have been reviewing this list since 2008 and plan to revise in 2013. The request when we started to decide the list in 2000 was "Recommendation of Secure Cryptography." Almost ten years has passed and the focus was changed to more practical perspective "Recommendation of Cryptography to Ensure Secure Systems," which means that the demands are shifted from availability of various cryptography options to clear up which cryptography can be practically procured.

In response to these needs, we have been reviewing from the structure and operation of the list since fiscal 2008. As part of this activity, we solicit the practical use of new cryptography in fiscal 2009, which requests the strong focus on practical application to meet the above demand. In addition to logical security evaluation, with implementation security (Resistance to side channel attacks: Resistance to attacks, which utilizes physical phenomenon generated during device operations, such as consumed electricity or electromagnetic wave radiation) newly included in the evaluation items, we also consider the security in practical aspects.

For establishing the security of our country

Since NICT is a public research institute, Security Fundamentals Group is requested to make advanced technical judgments on a neutral and impartial position. In order to establish the security of our country, we understand that it is our mission to use our abilities to the full and are committed to pursue research activities contributing to the support for technologies in our country.

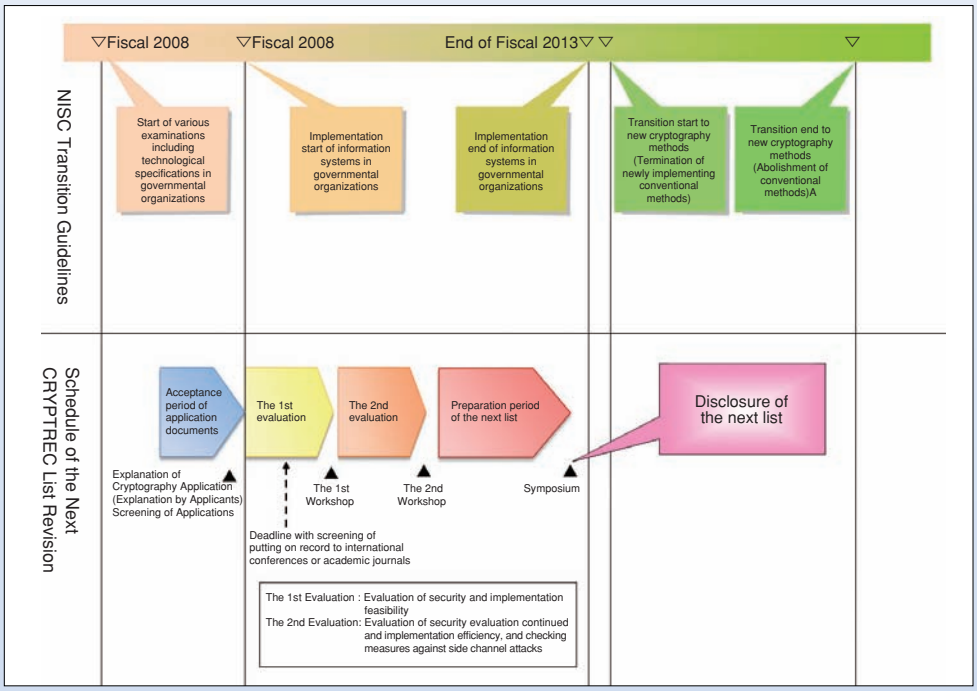


Fig.2: Schedule of CRYPTREC e-Government Recommended Ciphers List Revision and NISC (National Information Security Center) Transition Guidelines

●Supplementary Reference:
Cryptanalysis and prime-factor-decomposed computation

Generally, we imagine getting plain texts (original texts before encryption) by assuming secret information like key from cipher texts, with the term "decryption." However, with modern cryptography, we provide more favorable conditions to attackers to evaluate the security, including a condition to use plain texts and the corresponding encrypted sentences (known plain text attack) and a condition to gain the corresponding encrypted sentences to self-selected plain texts (selective plain text attack). These conditions may be seemed as unrealistic. With public key cryptography, in which the encrypted key is disclosed, however, attackers can freely generate pairs of plain texts and encrypted sentences, request a key recorded in an IC card, and use many other attack options.

Logically, they can always get a key if they try the brute force search, but we set a large size key that cannot be decrypted even by a computer with top performance to ensure security. In this approach, we develop more efficient decoding methods than round-robin, and evaluate the security by computing resources (computing volume and memory) required for execution of the strongest attack method.

RSA discloses the key used only for generating encrypted sentences (public key), and users secretly manage the decryption key (secret key). In this method, if the prime factor of a composite number contained in the public key is decomposed, the secret key is disclosed. Consequently, the encrypted sentences are decrypted or electronic signatures using public key encryption is forged. Based on this understanding, we need as large composite numbers of prime factors as not decomposed even by computers with the top performance. Even with the composite number of RSA 1024 is a number of as large as 1024 bits (10 raised to around 300th power), its security is gradually degrading according to the advancement of prime-factor-decomposition algorisms and progress of computation capabilities.

ICT Useful for Information Collection during Any Disaster

Profile

Osamu Takizawa

Group Leader
Disaster Management and Mitigation Group
Information Security Research Center

After completing a master course of postgraduate school, joined Radio Research Laboratory (current NICT) in 1987. Has been engaged in the research and development of emergency disaster management communications and contents security since 2000. Took the current position in 2006. Has doubled as Group Leader of Security Fundamentals Group since 2008. Doctor of Engineering. Disaster Prevention Manager (Bousaisi in Japanese)

Information collection is the primary step during any disaster

When any disaster occurs, we must collect information first of all. This article will show a part of NICT activities aiming at the utilization of ICT for information collection during any disaster.

Information collection by using mobile phone terminal

Being the most common ICT device today, which is highly likely that everyone carries anywhere at any time, mobile phone handsets are expected to be used during disasters. However, mobile phones may not be useful as a phone because communications become difficult during the disaster caused by congestion or out of order. From this perspective, establishment of network technologies not being interrupted during any disaster is important, but from another perspective, an approach to establish technologies to use mobile phones for information collection in other usage than as phone is likely to be more directly useful during disasters.

When local officials and other members investigate the field for checking the damage status during any disaster, they usually bring paper maps, cameras and other relevant items. However, these items do not so effectively work in such conditions, nor comprehensively catch the status with limited number of members during the time when people are forced to take actions to the damage. Based on this fact, NICT, in collaboration with National Research Institute of Fire and Disaster, is pursuing the development of applications that allow citizens to collaboratively investigate the damage status by utilizing camera and positioning functions of mobile phone handsets which everyone carries. The targeted capabilities are that collected damage status data can also be brought to the disaster measures office by accumulating the information in the memory of terminal even when communications are interrupted, and that positioning function autonomously operates only by GPS without using a base station. We have organized several demonstration experiments since last year, in which citizens of 20-60 years old actually operated the applications, to improve and achieve more easily handled applications.

Furthermore, in collaboration with Fire and Disaster Management Agency, National Research Institute of Police Science, and other relevant authorities, NICT participates in a joint project of the science and technology promotion subsidy entitled “RFID-based Positioning Systems for Enhancing Safety and Sense of Security ” (The representative research institute: Center for Spatial Information Science of Tokyo University). In this joint project, as a complementary positioning method in areas where GPS positioning is difficult like an underground street, NICT is pursuing the establishment of technologies used for disaster management and criminal prevention by installing Radio Frequency Identification tags (RFID) in walls or other relevant places, and receive the IDs by using portable terminals to understand the position of the user itself. As part of this activity, our institute is developing a method, using mobile phone terminals equipped with Bluetooth and RFID Reader, to understand the position of the user itself with the clue of address transmitted from Bluetooth devices installed in walls or other relevant places, and to write and leave messages on passive (without using electricity source) type RFID in the field equally installed in the walls as “Electronic Bulletin” (Fig. 1). We assume that this approach will be used for information exchange about the safety in the fields during large scale disasters, rapid safety inspection of damaged buildings, and other relevant applications. As of today, due to the restriction of readers to be integrated with mobile phone handsets, we use read-only RFID, and writing is virtually achieved by writing in the server on the network.

However, we believe that the realization of the function to directly read and write off-line to writable RFID, which we already realized using portable personal computers (see the NICT NEWS, November 2004), also with mobile phone terminals is indispensable during disasters when accesses to networks are not ensured, and we will continue the improvement of these technologies.

We will register the outcomes of these developments in application servers of mobile phone carriers to enable those who are interested to download, although

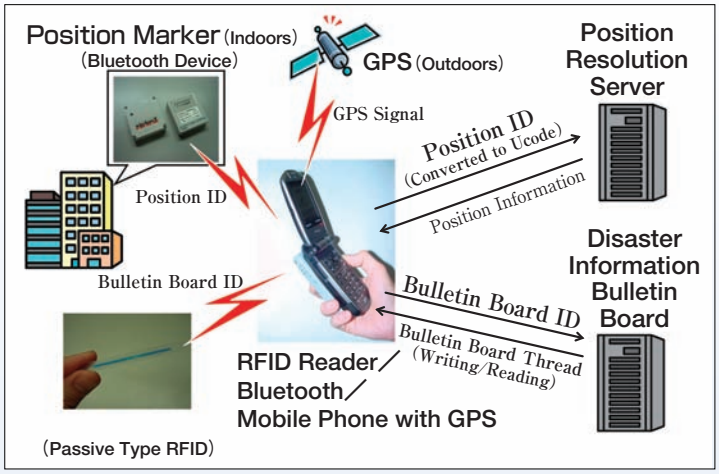


Fig.1: Concept of Positioning by Mobile Phone Terminal Equipped with Bluetooth and RFID Reader, and "Electronic Bulletin"

Last November, around the Nagareyama-Otakanomori station of Tsukuba Express and Tobu Railway in Chiba prefecture, organizations participated in the project jointly implemented field experiments, when the Geographical Survey Institute set a lot of benchmarks (equivalent to the 4th grade) with RFID. One of these benchmarks remains on the sidewalk in front of the station as a monument. Please find the benchmark with organization names including NICT carved if you have an opportunity to visit there.

available models may be restricted, and plan to broadly provide to the disaster management and criminal prevention volunteers as the beginning targets.

Information collection by rescue robots

Telerobots are expected as a method to explore in buildings where it is so dangerous that rescue workers or other emergency services can't enter during disasters and terrorism. NICT participates in "Strategic Project for Advanced Robot Component Technologies" promoted by New Energy and Industrial Technology Development Organization (NEDO), in which NICT is in charge of the research and development of communication technologies to transmit stable multiple images from multiple high speed mobile communication within closed space, measured data and action instruction data (The representative research institute: International Rescue System Institute). While wireless transmission is suitable for communication method of remotely piloted robots, this approach has many issues to stably send multiple images in closed space. On the other hand, the problem with wired communications is that the existence of cables becomes the restriction to actions in irregular terrain such as disaster site. Based on these conditions, as a compromise plan, we aim at the establishment of wired and wireless hybrid communication approach, which at first one robot (Fig.2) installs one communication cable with wireless access points positioned with an interval of several tens meters in a row deeply in the exploring space as central nerve; then using the cable as a life line, wireless controlled multiple robots make exploring activities around each access point. The project has worked together with active-duty rescue teams to make repeated demonstration experiments in underground streets in Sendai and Kobe cities to identify issues and improve the technology. Up to now, the technology achieved to the level to which we can remotely control the robots 700m away (approximately a distance of one station) in an underground street. According to the results of stage gate (refinement evaluation) conducted by NEDO at the end of last year, only the development team in which NICT participates was determined as "passed," and the continuation for two more years was authorized towards practical application. This result means, we believe, that the practical development concept of NICT assuming actual use, including wired and wireless hybrid communication approach is highly evaluated. With this project, we aim at actual deployment around 2015.

Fig.2: Communication Cable Laying Robot under Joint Development with International Rescue System Institute and Other Research Organizations

Aiming at the establishment of "usable disaster management and mitigation technologies"

As shown above, common characteristics in our research and development are the policy aiming at the accumulation of "immediately usable steady technologies" to leverage limited functions even if ordinary communication capabilities are not available, to manage to be used during disasters. Disaster management and mitigation is not an easy subject which can be realized by developing one top-down, advanced system with huge investment. During disasters, not an "advanced technologies like a glass sculpture" but a "surviving low technologies" is supported. The fact is that even with low technologies, since the steady innovations to achieve survival (raise survivability of technologies) have different difficulties from the research and development of advanced technologies, even organizations and manufacturers related to disaster management cannot launch. Consequently, public research institute in the ICT field like NICT have to address these problems in close collaboration with related parties of disaster management. Disaster Management and Mitigation Group should take the responsibilities for the efforts to establish "usable disaster management and mitigation technologies" as the only research group in NICT that is mainly focusing on the aspect of disaster management (including the period of our former organization).

Observation of Wind by Doppler Lidar

Analyzing Urban Scale Atmospheric Phenomenon to Help Improve Our Lives

Profile

Hironori Iwai

Researcher
Environment Sensing and Network Group
Applied Electromagnetic Research Center

Joined Communications Research Laboratory (current NICT) in 2001. Was engaged in the research on space weather forecasting. Currently is engaged in the research on Doppler Lidar.

Observing winds over urban areas to help resolve environmental problems

"We observe urban scale atmospheric phenomena, mainly wind, by a ground-based Doppler lidar," says Mr. Iwai, the researcher of Environment Sensing and Network Group in Applied Electromagnetic Research Center.

The Doppler lidar is a remote sensing instrument that measures movement speed of aerosols in the atmosphere, or wind speed, by transmitting laser beams into the atmosphere. Since the Doppler lidar does not have side lobes, it can observe the wind near the ground surface in urban areas crowded with buildings. The Doppler lidar can also observe small scale atmosphere phenomena in urban areas, so that it will contribute to the improvement of weather forecast accuracy as well as the resolution of environmental problems including air pollution and heat island effect in urban areas. Eye-safe near-infrared lasers which do not damage human eyes are used for the Doppler lidar.

Various outcomes from steady observations

Mr. Iwai is engaged in studies on methods for observing and analyzing wind by the Doppler lidar. He has carried out various field experiments and analyzed these observation results. In Yamagata Prefecture, he made observation to elucidate the generation mechanism of characteristic strong wind called "Kiyokawa Dashi," which damages agricultural products, and observed three-dimensional wind fields around the generation source. He also succeeded in the visualization of spatial distribution and flow of Kosa (Asian Dust) arriving in the Tokyo metropolitan area based on the observation results at the NICT headquarters (in Koganei).

In the observation at the Sendai airport by using two Doppler lidars, he found out that the wind from the sea generated the horizontal roll vortices. "By observing wind with two Doppler lidars, we could capture the three-dimensional wind structure in detail, which could not be achieved with one lidar," explains Mr. Iwai. The Doppler lidar is an expensive instrument and there are only several Doppler lidars in Japan. Besides, it is not easy to transport Doppler lidar. Due to these reasons, there are only several cases in the world regarding the observation to use multiple Doppler lidars.

"In the future, I would like to observe atmospheric/meteorological phenomena peculiar to urban areas, including building winds, torrential rainstorms, air pollution and the like via a network of Doppler lidars," talks Mr. Iwai, who studied on space plasma in his graduate school days, and was engaged in the research on space weather forecasting for four years at NICT. "I just began the research on meteorology after I moved here three years ago. But the work observing the wind to get data in the actual experimental sites is congenial to me," he also showed us an interesting aspect of meteorological study.

Toshiyuki Okuyama
Research Manager, Project Promotion Office,
Information Security Research Center

CRYPTREC Symposium 2009

— Towards the Revision of e-Government Recommended Ciphers List —

With regard to the project of Cryptography Research and Evaluation Committees (CRYPTREC) which has been managed by the Ministry of Internal Affairs and Communications (MIC) and the related ministries and government offices, the public application for a new cryptography will be advertised from the fiscal 2009 towards the revision of e-Government Recommended Ciphers List scheduled in the fiscal 2013. In order to broadly announce this public application, on February 18 (Wed.), NICT and Information-Technology Promotion Agency (IPA), Japan held the CRYPTREC Symposium 2009 at the Toranomon PASTRAL Hotel under joint sponsorship of MIC and the Ministry of Economy, Trade and Industry (METI).

In this symposium, NICT set up the program for lectures regarding the importance of e-Government Recommended Ciphers List and how to proceed with the revision of its ciphers list, and besides, the panel discussion regarding the future cryptographic technology research. It was very magnificent with more or less 230 participants from the related com-panies, universities, government offices, public organizations and so on.

A Scene of Conference Hall

NICT Information and Communications Security Symposium

— Reading the Future Information Security —

As an event related with "Information Security Day" on February 2, which has been specified in the Information Security Policy Council, on February 26, 2009, NICT hosted the symposium at the Toranomon PASTORAL Hotel under the sponsorship of Information Security Policy Council, Ministry of Internal Affairs and Communications, and related learned, scientific societies.

This symposium aimed at the opportunity prospecting future technologies of information communications security while deeply understanding the latest trend of information communications security through three lectures by experts of information and communications security, and three panel discussions under the following respective themes: "Reading the Current Status of Identity Management Technologies and Foreseeing its Future" in the first part; "Foreseeing the Future of Network Security Technologies" in the second part. Those panel discussions were performed actively and enthusiastically through many questions and comments given by not only panelists but also participants.

A Scene of Panel Discussion

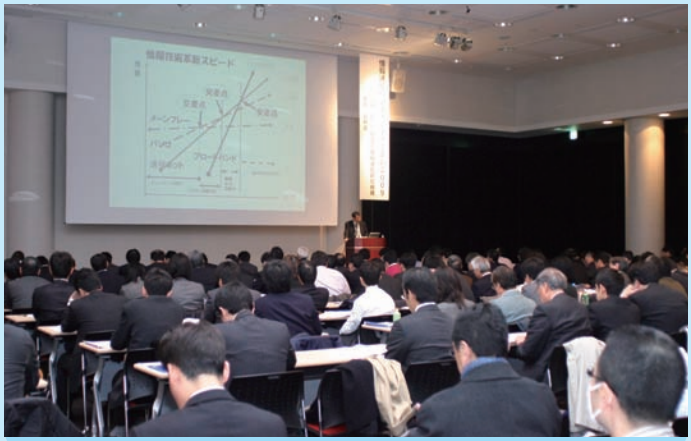
Event Report of Information and Communications Venture Forum 2009

Hiroshi Yoshino
Manager, New Business Support Group,
ICT Proactive Outreach Department

Every year, NICT holds "Information Communications Venture Forum" as the event for related parties of ICT venture businesses, aiming to promote the startup of ICT venture businesses and activate their management and deployment.

On February 20, 2009, NICT set up at the Bellsalle Iidabashi the program for a keynote speech by an expert of ICT and relay lectures by four younger managers of ICT ventures under the basic theme, "Prospects of ICT Venture Business — Investigating the Phases from Startup to Growth —" in this fiscal year.

After the lecture program, about 200 people participated in the event, and lecturers and participants actively had interaction one another by exchanging their opinions in the information exchange session on that day.



A Scene of Conference Hall (Bellesalle Iidabashi)

	Lecturer	Subject of Lecture
Key-note Speech	**Hiroshi Nakajima** President, MM Research Institute Executive Research Fellow /Professor, Center for Global Communications, International University of Japan	New Trends and Future Markets of Information and Communications
Relay Lecture	**Kengo Ito** President & CEO, MetaCast	Experience sharing changes social media: Social Lifestreaming Service — Semantic is a keyword in 2009!? —
	Takashi Uemura President, ALBERT	ICT Venture Aiming at Global Deployment with Unique Recommendation Technologies
	Taisei Tanaka President & CEO, Geisha Tokyo Entertainment	"In 20 years committed to exceed Nintendo, Apple and Disney:" very much talks the president of high-tech entertainment.
	Tadatoshi Senoo President, maneo	Social Lending : Web 2.0 Finance — Global Circumstances and Japan —

※ReferenceURL http://www.venture.nict.go.jp/ezp/index.php/venture/nict_2/node_20835/2009/node_25315

Information for Readers:

In the next issue, we will feature the Applied Electromagnetic Research Center which aims at safety and security of living environment through measurement technologies.

NICT NEWS No.379 , Apr 2009

Published by
Public Relations Office, Strategic Planning Department,
National Institute of Information and Communications Technology

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
URL: http://www.nict.go.jp/index.html

Editorial Cooperation: Japan Space Forum