NICT NEWS
独立行政法人
情報通信研究機構
National Institute of Information and Communications Technology
2014 MAR
3
No. 438

Cover image: "DAEDALUS: Darknet Monitoring-based Alert System and its Practical use in Society"

DAEDALUS: Darknet Monitoring-based Alert System and its Practical use in Society

Daisuke INOUE

Director of Cybersecurity Laboratory, Network Security Research Institute
Director of Cyber Tactics Laboratory, Cybersecurity Research Center

After completing a doctoral course in 2003, he joined Communications Research Laboratory (currently NICT). He has been engaged in research and development of network security focusing on Network Incident analysis Center for Tactical Emergency Response (NICTER) since 2006. Ph.D. (Engineering).

Introduction

The majority of conventional security technologies primarily involves "perimeter protection", which detects and defend against cyber attacks within network boundaries, where the internal network is connected to the Internet. However, malware*1 infections from mediums inside the organization, such as email attachments, USB memories, and BYO (bring your own) PCs, frequently cause security incidents that break perimeter protection. Thus, the importance of security measure that complements the traditional perimeter protection has been increasing.

The Direct Alert Environment for Darknet And Livenet Unified Security (DAEDALUS) provides the post-infection measure based on the presupposition that completely preventing malware infection is difficult when an incident occurs. This system makes it possible to detect malware infected host (especially, worm-type malware that has the self-propagation function) inside the organization in earlier stages, and send an alert to the organization.

The mechanism of DEADALUS

The DAEDALUS mechanism for detecting the attack and sending an alert is quite simple:

If packets are sent to the darknet from a particular organization, the system sends an alert to the organization.

Here, the darknet refers to an unused IP address space on the Internet. In usual communication, it is unlikely that a packet (the minimum unit in the Internet communication) arrives at an unused IP address space. However, when you observe communications on the darknet, you find that it receives a large number of packets. Most of these packets are brought from the worm-type malware infected hosts to explore the next targets. Such communications where these hosts spread the packets on the Internet is called scan. Just like the mailbox of a vacant apartment receives only useless direct mails, the most of the packets that reaches the darknet are the unauthorized communications caused by malware. In this case, the sender is considered to be

Mechanism of DAEDALUS (3 steps)
① Malware or attacker sends attack packets.
② NICTER collects and analyzes the darknet communication and detects the attack packets (or Dos Backscatter) from observation target organization.
③ Send the alert that includes the information of the attacking host to the observation target organization.

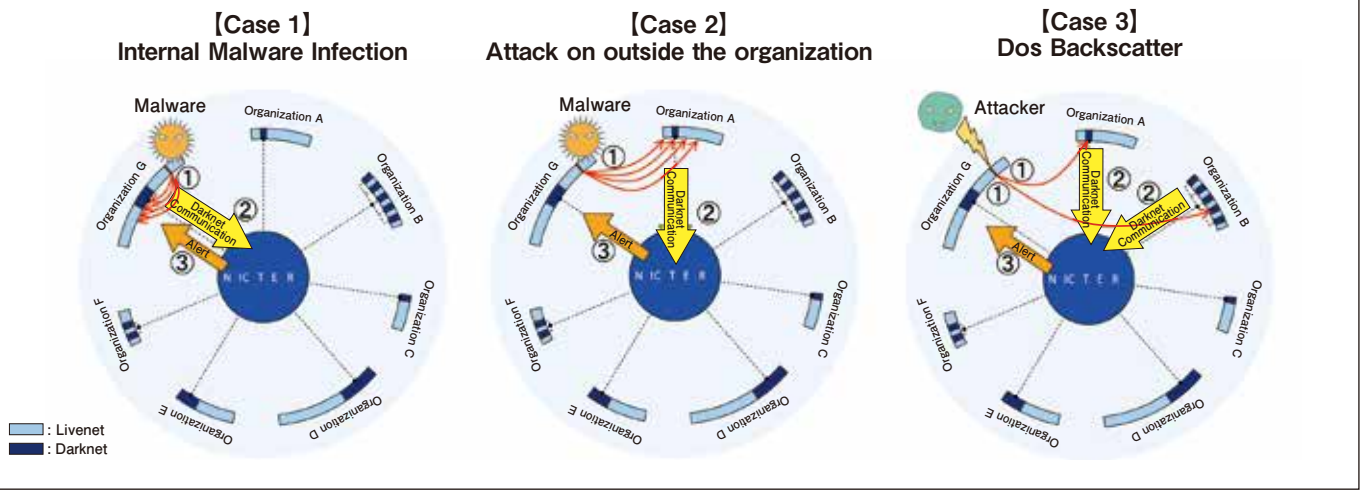


Figure 1 DAEDALUS attack detection case 1-3

- Case 1: Infection activities inside the organization by a malware infected host (Local Scan)
- Case 2: Infection activities outside of the organization by a malware infected host (Global Scan)
- Case 3: Bounce of a DoS attack to a particular organization by an external attacker (Backscatter*2)

*1 Malware
A generic term for software such as viruses, worms, trojan horses, spyware, and a bot, that perform harmful activities such as data destruction, information leakage, and infections to other computers. This term was coined as an abbreviation of "malicious software".

*2 Backscatter
A packet response (SYN-ACK) from the server that has received DoS attack (SYN-flood attack) from spoofed IP address. When the IP address is spoofed at random, the packet response comes to the darknet from the server that receives DoS attack, so it is possible to detect the occurrence of DoS attack.

Figure 2 Visualization screen of DAEDALUS-VIZ

Figure 3 Displaying the time of the new alert

Figure 4 Examples of local scan by malware

infected by malware. So, by sending an alert to the organization that uses the IP address, this system enables the rapid incident response as a trigger.

Attacks that can be detected by DAEDALUS can be divided into three cases as shown in Figure 1. It should be noted that NICTER in Figure 1, is an incident analysis system including the large-scale darknet monitoring network, which is the foundation of DAEDALUS, and it observes the approximate 210,000 (as of January 2014) of unused IP addresses in real time.

In order to observe the case 1, it requires to install observatory sensor for darknet in the internal networks. Cases 2 and 3 are externally observable by the large-scale darknet monitoring network of NICTER, so there is no need to install sensor.

Visualization engine of DAEDALUS

Figure 2 shows the screen of the visualization engine DAEDALUS-VIZ that provides the bird's-eye view of the alert status reported by DAEDALUS. The sphere at the center represents the Internet, and the orbiting rings around the sphere represent the networks of the organization that has the darknet observation sensor. The comet-shaped object flying between the rings and the sphere represents the communication to the darknet.

The part of the ring colored in light blue is the livenet (used IP address block) area, while dark blue part is the darknet area. The Chinese character (indicating "caution") on the outer periphery of the ring indicates the sender IP address that causes an alert inside the organization. DAEDALUS will automatically send emails to the organization at the same time as the alert is displayed on the DAEDALUS-VIZ.

Figure 3 shows the Chinese character (indicating "caution") displayed on the whole screen when a new alert is sent. Figure 4 shows the malware infection activity (yellow curve indicates the local scan by malware) in the organization.

Social deployment of DAEDALUS

NICT is promoting the social deployment of DAEDALUS in Japan and abroad.

In Japan, we carry out the installation of visualization engine and darknet observation sensor, and provide the alert for educational institutions. For enterprises, we have started to provide the commercial alert services*3 based on DAEDALUS. In addition, in cooperation with Local Authorities Systems Development Center (LASDEC), we have provided the alert (and alert response manual) for local governments since November 2013. As of January 2014, 110 of local governments have been registered on the list of organization that receive alert when an attack occurs (Figure 5).

Outside of Japan, we have begun providing DAEDALUS alert as a part of the technical cooperation project for security measurement (JASPER*4) of Ministry of Internal Affairs and Communications for the ASEAN countries.

Summary

Worm-type malware has caused many outbreaks since the early 2000s, and is still rampant on the Internet today. DAEDALUS provides a quick alert about the source of infection based on the result of observation by operating the large-scale darknet observation network. One of the characteristics of DAEDALUS is that its ability of detection improves as the number of organization that join the network observation increases. So, based on the win-win relationship where we provide the alert from DAEDALUS and install in cooperation organizations, we will continue to expand it to industry, academia and government in the future.

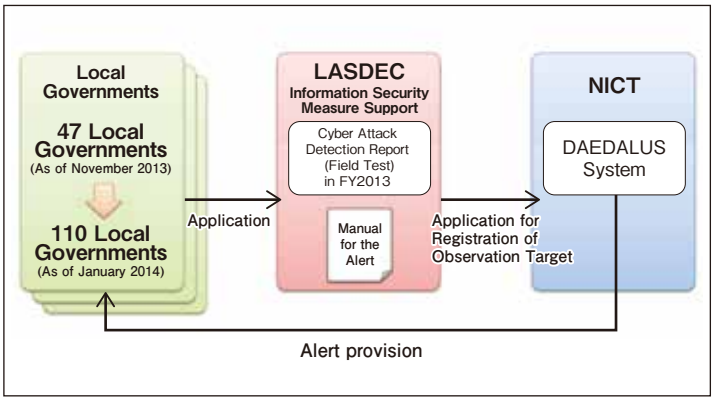


Figure 5 DAEDALUS alert provision to local governments

*3 Alert service
SiteVisor (http://sitevisor.us)

*4 JASPER
Japan ASEAN Security PartnERship

Radio Wave Shutter for WiFi White Space

—Shield frequency is controllable with low power consumption—

Kyoichi IIGUSA

Senior Researcher, Smart Wireless Laboratory, Wireless Network Research Institute

After completing his master's course in 1987, he joined Radio Research Laboratory, the Ministry of Posts and Telecommunications (currently NICT) in the same year.
Since then, he has been engaged in R&D related to antennas, such as near-field measurement, slot array antenna, ESPAR antenna, and wideband antenna. Ph.D. (Engineering).

Radio wave shutter

Radio waves are now used in various applications, not only in broadcasting and telephones, but also in data communications and power transmissions including mobile communications. While they are invisible to our eyes, they are flying about the space around us. Even in these radio wave environments, some frequency bands are not used (they are called "White Space"), depending on time or location. In terms of the effective use of the frequency resources, the research and development of the secondary use of the White Space are currently being promoted. In addition, if users can create White Space at their will, it is anticipated that the efficiency of frequency utilization will be further enhanced. In order to implement this technology, NICT has been conducting research and development of a radio wave shutter which electronically shields a specific frequency band.

The radio wave shutter creates White Space by shielding the radio waves of a specific frequency band. This enables shielding of indoor WiFi*1 while transmitting the signals for mobile phones, which improve the indoor WiFi environment while maintaining the necessary communication environment to the outside. Because the shutter enables us to confine radio waves in a certain space, it can be used in multiple ways, such as limiting the service area of wireless LAN, preventing the off-site interception of the wireless microphones in a concert hall, and protecting electric equipment in an intense electric field area.

The structure, principle, and features

As shown in Figure 2, the radio wave shutter is constructed with conductor wires printed in grid shape on a circuit board. Variable reactance, that are constructed with varactors*2, and high impedance are alternately connected to the conductor wires arranged in the longitudinal direction in 1/4 wavelength intervals of frequency that is to be controlled. By controlling variable reactance to the almost short-circuited state, the conductor wires between high impedance become approximate 1/2 wavelength in length, and shield the radio wave because current is strongly resonated on the wires. On the other hand, when variable reactance is set to the almost open-circuited state, radio waves will transmit because current hardly flows on the wires. By changing the reactance value of the varactors by DC voltage, the shield frequency (resonance frequency of conductor wires) of radio wave can be continuously controlled.

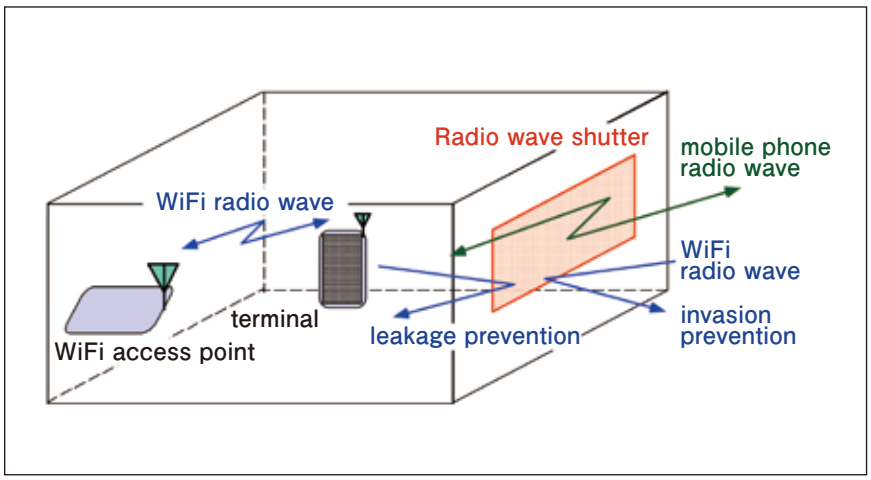


Figure 1 Usage example of a radio wave shutter for White Space

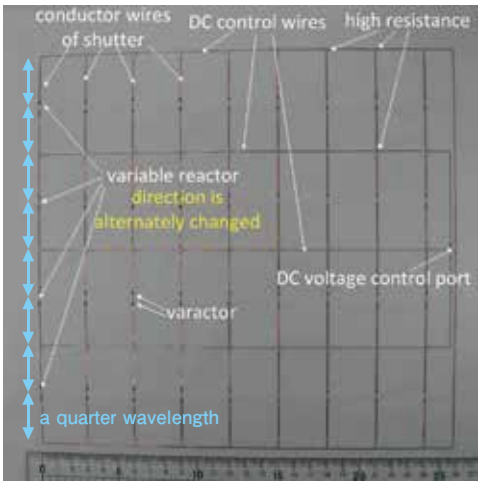


Figure 2 Radio wave shutter trial product

*1 WiFi
A widely used standard of wireless technology for connecting to the network.

*2 Varactor
Variable capacitance diode. It is a variable reactive element whose capacitance can be varied by controlling the terminal voltage.

Since the varactors are controlled by the reverse bias, DC current hardly flows to the varactors, and thus they require less power consumption. Moreover, by changing the direction of the bias of the varactors alternately, higher DC voltage is not required even when a larger radio wave shatter is to be realized. This is because only the voltage necessary for controlling one variable reactance can control the voltage for all varactors. The conductor wires in latitudinal direction are only for controlling DC voltage.

Design for lowering cost and control voltage

In order to operate a radio wave shutter effectively, the reactance value needs change drastically. Since the variable range of reactance of a varactor is limited, several varactors need to be connected in series in order to achieve a specific range of reactance, and this causes the issue of increasing the cost and control of voltage. Therefore, we enlarged the interval between longitudinal conductor wires to achieve a specification with a variable reactance consisting of two varactors. Since the increase of the interval between conductor wires weakens the effect of current, shield frequency band becomes narrow. So, it is possible to increase the change of transmittance even when the variation width of shield frequency is small. Also, the required number of varactors is reduced by enlarging the interval. This time, with setting the interval between longitudinal wires to be 30 mm, we designed a radio wave shutter so that the transmittance of perpendicular incident waves in the WiFi frequency band 2.401–2.495 GHz (bandwidth: 94 MHz, 22 MHz/ch) was switchable from the transmitting state (transmit more than half) to the shielding state (transmit less than one-tenth).

The transmission characteristic for perpendicular incident waves

Figure 3 shows the measurement results of the transmittance, when the radio wave of vertical polarization irradiated from the front of the trial radio wave shutter. It shows frequency characteristics when DC control voltage is changed from 0 V to 50 V in every 10 V step. The transmittance of radio wave around 2.5 GHz is –3 dB (50%) with control voltage set to 0 V (red line). With 40 V (blue line), however, the radio wave can be shielded to be less than –20 dB (less than 1%). Since cross polarized wave (in this case, horizontally polarized wave) in the frequency around 2.4–2.5 GHz is almost transmitted regardless of control voltage, it is possible to control the transmittance regardless of polarization by overlapping another radio wave shutter by rotating 90 degrees.

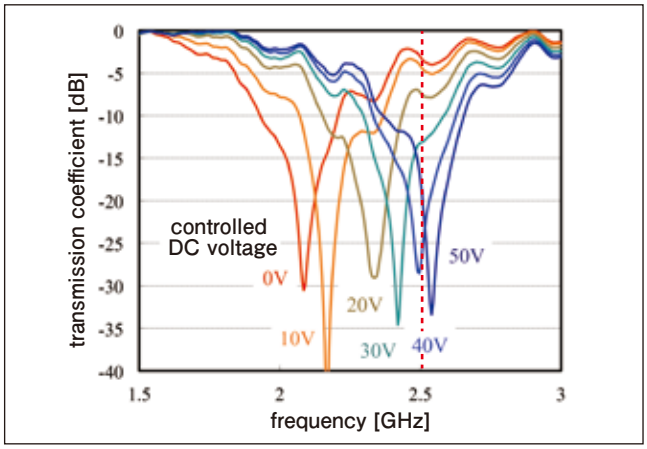


Figure 3 Result of transmittance of perpendicularly incident vertically polarized wave

Experiment of shielding WiFi communication

We were able to confirm that the transmittance of a perpendicular incident wave can be changed about 20 dB in the shield frequency by the radio wave shutter. However, it is difficult to completely shield the radio wave, and the shield frequency shifts when the incident angle of radio wave is tilted from the front direction to a slant direction. So we experimented to see if the shutter could shield the actual WiFi radio waves in the configuration shown in Figure 4. In the experiment, we placed the WiFi access point in the RF shield box by opening its lid, and setting two radio wave shutters, which are about 30 cm square, over the opening aperture of RF shield box and rotating one shutter by 90 degrees. We downloaded a large file from the PC server on the upper right to the PC on the left via the WiFi access point in the RF shield box. The transmitting power of the access point was fixed and the channel 2 (2406–2428 MHz) was used. When we changed the control voltage of the shutters from 0 V to about 32 V, we observed in the screen of the left PC (right side of the horizontal axis represents past time) that the download speed decreased and the download was subsequently suspended.

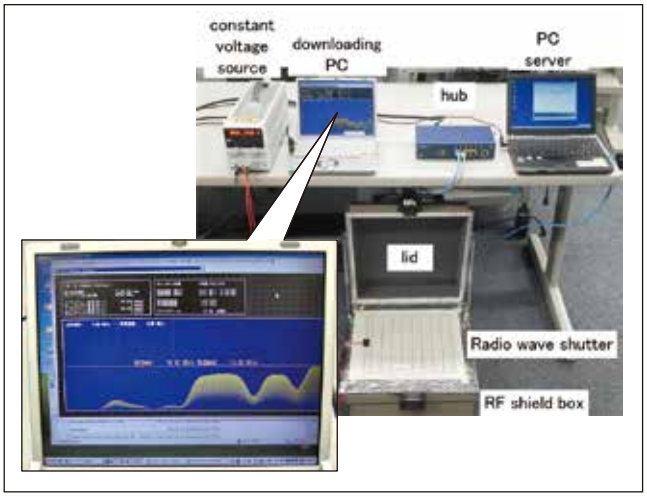


Figure 4 Experiment of shielding WiFi transmission

Future prospects

Variable directivity antennas and tunable antennas are expected to be realized by setting a radio wave shutter near an antenna and operating the shutter as a frequency-variable polarization-selective reflector, as shown in Figure 5. Therefore, we will research such antennas as applications of radio wave shutters.

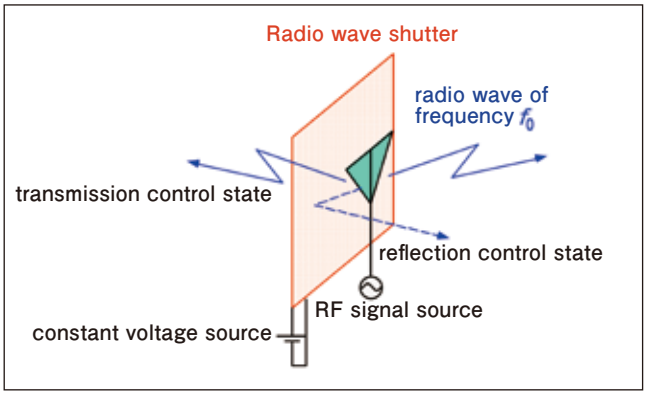


Figure 5 Application example as a polarization-selective reflector

"Connecting" Japan and the World

—International collaborative research promotion on New Generation Networks—

Nozomu NISHINAGA

Director of New Generation Networks Laboratory, Network Research Headquarters

After completing graduate school and working as Research Fellow and an assistant at Nagoya University, he joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (currently NICT) in 1999. He has been engaged in research and development of New Generation Networks. Ph.D.(Engineering).

The significance of international cooperation in research and development

NICT is promoting the research and development of New Generation Networks with the aim to realize a network infrastructure to solve various problems in the current network and provide safe and secure ICT services for the future. The New Generation Networks is expected to connect things, people, and information around the world on a greater scale than the one of the current network, and it is anticipated to enrich people's lives.

There are various network devices around us, such as cell phones, smartphones, and PCs. These devices have some essential technologies developed by "open innovations" method that is a way to develop huge and complex systems by having everyone utilize the respective R&D results freely in the world. Today, most of the networking technologies are too complex to research, develop and deploy by a single organization or one country. In addition, the network itself is meant to be used globally, say it is used for connecting the world. Therefore, it is very important to proceed the research and development that meets the required condition globally in cooperation with a lot of countries and organizations.

International conference for the promotion of international collaborative research

How do you promote international collaborative research? Figure 1 shows the current status of research and development of the New Generation Networks or Future Internet of the United States and Europe. In the United States, National Science Foundation (NSF) provides research funding to universities primarily, and in Europe, European Commission (EC) provides research funding to private sectors and universities for promoting the R&D activities. NICT has held international conferences on a regular basis to promote international collaborative research in cooperation with NSF and EC since around 2007, the year when we started the R&D of the New Generation Networks. The most important objectives of these conferences are to make specific and feasible international joint research proposals. The conferences are like "matchmaking party" for international collaborative research where researchers from various initiations discuss after presentations, and where they make collaborative research proposals at the end.

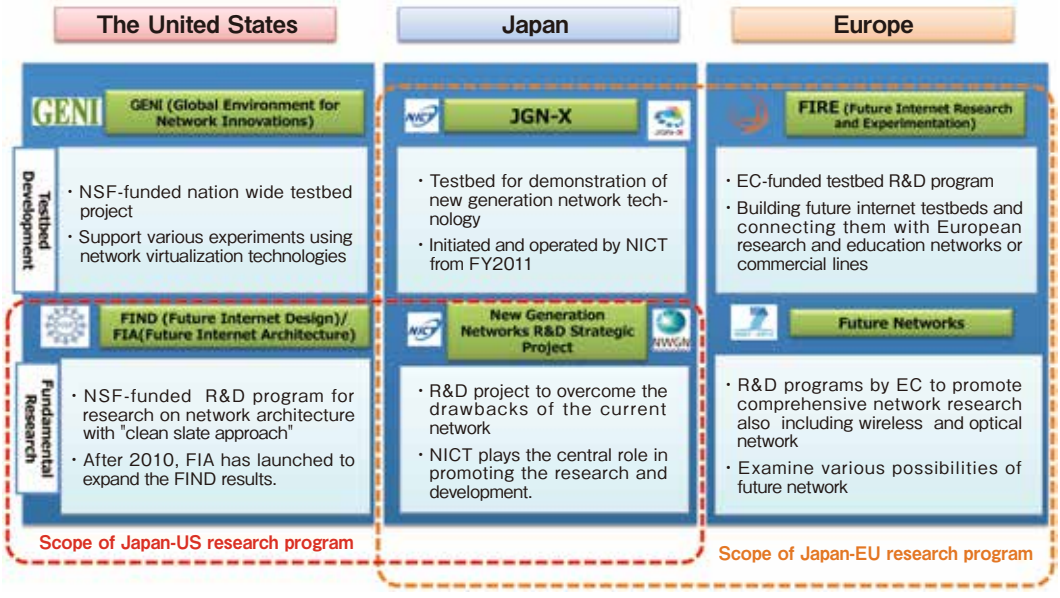


Figure 1 Current status of research and development in Japan, the United States, and Europe about the Next Generation Networks

Promoting international collaborative research by the International Joint Funding

In order to promote international collaborative research of the New Generation Networks in cooperation with the NSF and EC, NICT is offering grant programs for international collaborative research between Japan and the United States, or between Japan and Europe. By referring to the joint research proposals from the international conference we mentioned above, this joint program strategically appoints the joint research field for both Japan and the United States or Japan and Europe and jointly accepts applications from the public (Figure 2). For instance, Japanese research institution that wish to apply for the program, makes a proposal in cooperation with the recipient country, and submits it to NICT while the counterpart submits to NSF (for the United States) or EC (for Europe). After the proposal, NICT and NSF or EC jointly evaluate the proposal, and then decide to adopt it or not. Research by the international grant program has some strengths: 1. it enables to capitalize the strength of both research institutes, 2. it enables almost twice scale R&D funded by two parties (the partner country is to fund about the same amount as Japanese), 3. it makes easier to conduct international standardization of the research result.

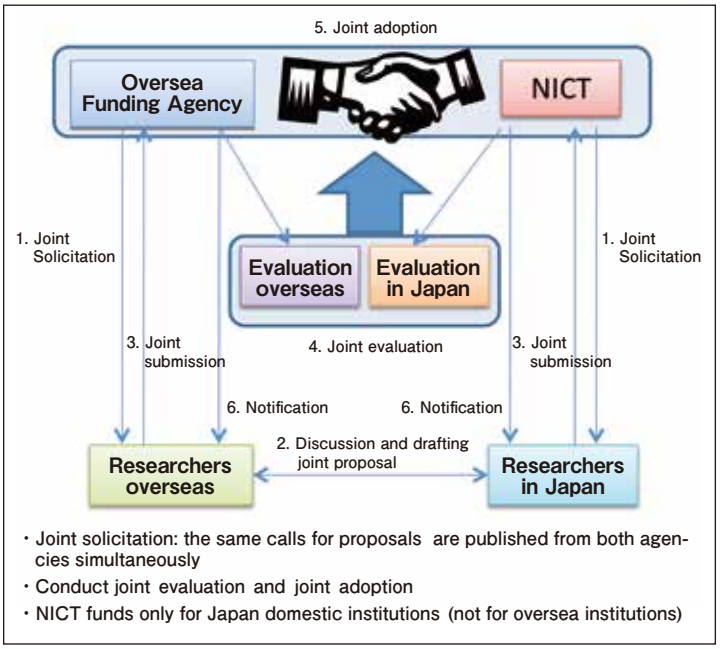


Figure 2 The research and development through joint grant program

Japan and U.S. collaborative research program

NICT and NSF have agreed to promote international collaborative research on the New Generation Networks through "the Japan-U.S. Policy Cooperation Dialogue on the Internet Economy" and so on.

The first Japan-U.S. joint research program was initiated in 2010. 7 joint research projects were adopted in research institutes from universities in the U.S., NICT, and universities in Japan over the architecture of the New Generation Networks. In the 3rd Japan-US workshop (Figure 3), researchers from both Japan and the U.S. discussed the fields for the future collaborative research. In May 2013, NICT and NSF agreed to have the next collaborative research grant program on R&D on super large scale information network infrastructure technology with reference to the workshop results and signed Memorandum of Understanding (MoU)[1]. 7 projects were adopted including 3 research projects NICT conducts by itself for the second Japan-U.S. joint research program[2]-[4].

Japan and EU collaborative research program

Through the Japan-EU ICT Policy Dialogue, NICT and EC have agreed to promote international collaborative research. NICT and EC have discussed over research collaboration with reference to more than 20 of the collaborative research proposals that have been proposed at the 3rd Japan-EU Symposium held in 2010 fall (Figure 4). As the first phase, we offer grants for research proposals about 3 themes in FY2012[5], and the international collaborative research is underway since April 2013[6]. In addition, for the second phase, from January to April 2014, we started accepting proposals on two research themes as follows[7].

1. Experimentation and development on federated Japan-EU testbeds
2. Access networks for densely located users

For the program of the second phase, we will conduct Japan-EU joint evaluation this summer, and research and development is set to start this fall.

International collaborations in the future

Research and development of the New Generation Networks will enter the third phase with a focus on demonstration and dissemination of the technologies. In this phase, it will become more important to have international cooperation for such as international standardization and market introduction. In the future, we will focus not only on R&D but also on international cooperation with application demonstration of the research results for promotion and dissemination to overseas.

Reference URL

[1] http://www.nict.go.jp/en/press/2013/05/30-1.html
[2] http://www.nict.go.jp/collabo/commission/20130710kobo.html
[3] http://www.nict.go.jp/press/2014/02/04-1.html
[4] http://www.nsf.gov/news/news_summ.jsp?cntn_id=130239
[5] http://www.nict.go.jp/press/2012/10/02-1.html
[6] http://www.nict.go.jp/press/2013/06/03-1.html
[7] http://www.nict.go.jp/collabo/commission/20140107kobo.html

([2] [3] [5] [6] [7]: Japanese version only)

Figure 3 Participants at the 3rd Japan-US Future Network Collaboration Workshop on Advanced Research Issues

Figure 4 Snapshot of the 3rd Japan-EU Symposium

Awards

Recipient ● Masataka HIGASHIWAKI / Director of Green ICT Device Advanced Development Center, Advanced ICT Research Institute

Co-recipients: Kohei SASAKI
(Tamura Corporation)
Akito KURAMATA
(Tamura Corporation)
Shigenobu YAMAKOSHI
(Tamura Corporation)
Takekazu MASUI
(KOHA Co.,Ltd.)

◎Award Date: July 23, 2013
◎Name of Award:
Special Award, 27th Advanced Technology with Originality Awards
◎Details:
In recognition of R&D of advanced and innovative gallium oxide power devices by industry/government cooperation
◎Awarding Organization: Fuji Sankei Business i.

◎Comment from the Recipient:

In award-winning "R&D of gallium oxide power devices", our achievement of pioneering a new semiconductor material was highly evaluated as a big step to the future application of the devices.

With this award, we would like to put further efforts on R&D to pave the way for its industrialization. Finally, I would like to thank all the people supporting this R&D.

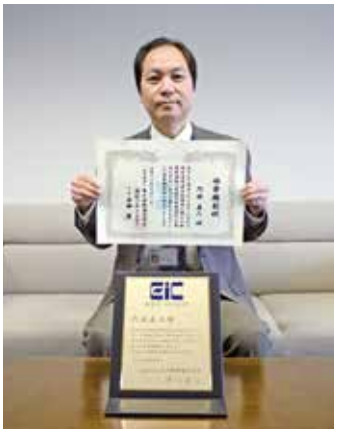
Recipient ● Naoto KADOWAKI / Senior Executive Director/Executive Director, Strategic Planning Department

◎Award Date: September 18, 2013
◎Name of Award: IEICE Fellow
◎Details:
For contribution to research and development of networking technology in broadband satellite communications network
◎Awarding Organization:
The Institute of Electronics, Information and Communication Engineers (IEICE)

◎Award Date: September 18, 2013
◎Name of Award:
IEICE Communications Society Outstanding Contribution Award
◎Details:
In recognition of contributions for managing the research committee as the chairperson of Technical Committee on Satellite Communications at IEICE.
◎Awarding Organization:
The Institute of Electronics, Information and Communication Engineers (IEICE)

◎Comment from the Recipient:

Accepting IEICE Fellow is a great honor. This award recognizes the outcome and contribution to R&D of networking technology in broadband satellite communications network including the development of WINDS. The IEICE Communications Society Outstanding Contribution Award evaluates our activities at the Technical Committee on Satellite Communications as a chairperson and vice-chairperson. I am extremely grateful for various seniors for giving us guidance and support, and for those involved in research and development together. I would like to continue my commitment for the development of satellite communication technology in Japan, and expansion of this field in the future.



Recipient ● Naoyuki SHINOHARA / Researcher, Security Fundamentals Laboratory, Network Security Research Institute

Co-recipients: Tsuyoshi TAKAGI
(Institute of Mathematics for Industry, Kyushu University)
Takeshi SHIMOYAMA
(FUJITSU LABORATORIES LTD.)
Takuya HAYASHI
(Institute of Mathematics for Industry, Kyushu University)

◎Award Date: October 18, 2013
◎Name of Award:
Docomo Mobile Science Award
Advanced Technology Award of Excellence
◎Details:
For contribution to mobile communication,"Pioneering research to apply the next-generation cryptography that can utilize anonymous data"
◎Awarding Organization:
Mobile Communication Fund

◎Comment from the Recipient:

Since the diversification of services and safety of cloud-based information services are expected by the use of a pairing-based cryptography, the cryptography has been attracting attention as the next generation cryptography. The pairing-based cryptography of 278 digits has been estimated to cost several hundreds of thousand years to break. But, using our method, we succeeded with the cryptanalysis of it in 148.2 days. This fact means that we have set a world record of cryptanalysis. Our achievement will be used to calculate the safe digit length of the cryptography, will lead to safe use of next-generation cryptography. We would like to express my appreciation to everyone involved and those who have supported our research.

From left, Takuya HAYASHI, Naoyuki SHINOHARA, Takeshi SHIMOYAMA, Tsuyoshi TAKAGI

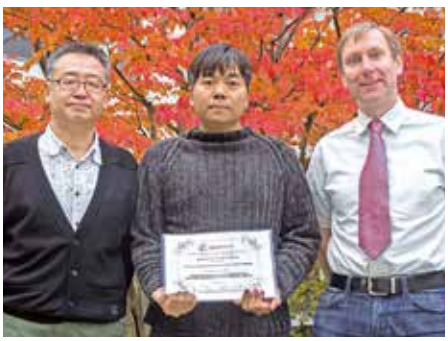
Recipients ● Ye Kyaw Thu / Researcher, Multilingual Translation Laboratory, Universal Communication Research Institute
Finch Andrew MICHAEL / Senior Researcher, Multilingual Translation Laboratory, Universal Communication Research Institute
Eiichiro SUMITA / Director of Multilingual Translation Laboratory, UniversalCommunication Research Institute

Co-recipients: Yoshinori SAGISAKA
(Waseda University)

◎Award Date: October 30, 2013
◎Name of Award:
SNLP2013 Special Award(Emerging)
◎Details:
In recognition of the useful segmentation method in research presentation titled "Unsupervised and Semi-supervised Myanmar Word Segmentation Approaches for Statistical Machine Translation" at SNLP2013
◎Awarding Organization:
SNLP2013 (The 10th Symposium on Natural Language Processing)

◎Comment from the Recipients:

Automatic word segmentation of languages in which data and tools are limited, is an important issue to be addressed in natural language processing. In the awarded paper, in order to solve this problem, we proposed a new word segmentation method using a dictionary and a Bayesian learning algorithm, and adapted the technique to Myanmar. We significantly improve the translation quality of an automatic translation system from Myanmer to multiple languages. In the future, we would like to extend the application to other languages and make further improvement to the technique.



From left, Eiichiro SUMITA, Ye Kyaw Thu, Finch Andrew MICHAEL

Report on "10th Forum of Japan-USA ICT R&D"

Eisaku YAMAJI,
Managing Director, International Affairs Department/
Director of North-America Center

Themed in Big Data, NICT hosted the 10th Forum of Japan-USA ICT R&D in Washington D.C., U.S.A, on January 24, 2014. Ten individuals from NICT headed by Masao SAKAUCHI, President of NICT, and twenty individuals from the U.S. government and research entities in the field of Big Data, such as Dr. George O. STRAWN, the Director of the Federal Networking and Information Technology Research and Development (NITRD), National Coordination Office (NCO) and Dr. Charles H. ROMINE, Director of the Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST), attended the forum, introduced R&D activities, and exchanged opinions with each other.

This forum's main function was to survey the current R&D trends in the U.S., but it also served as a great opportunity for us to learn about active R&D in the U.S., and for leading researchers in the U.S. to know about the current state of NICT's R&D. In addition, the field of Big Data is anticipated to cover a wide range of applications while privacy protection is required. The forum gave NICT a momentum to continue exchanging information closely with U.S. researchers in the future.

Furthermore, on the day before the forum (January 23), Dr. SAKAUCHI, President of NICT and other members from NICT visited National Science Foundation (NSF) and NIST, and exchanged opinions with Dr. Cora B. MARRETT, Acting Director of NSF, Dr. Willie E. MAY, Principal Deputy & Associate Director for Laboratory Programs, NIST, and Dr. Charles H. ROMINE. With the close cooperation, we have built a good relationship with these institutes so far, and we reaffirmed that we will continue to have further cooperation in the future.

Snapshot of the forum
(Greetings of Dr. SAKAUCHI, President of NICT, back of center)

The participants of the forum

Dr. Cora B. MARRETT, Acting Director, NSF (center),
Dr. Farnam JAHANIAN, Assistant Director, NSF (left),
Dr. SAKAUCHI, President of NICT (right)

Dr. Willie E. MAY, Principal Deputy & Associate Director
for Laboratory Programs, NIST (second from left),
Dr. Charles H. ROMINE, Director of ITL, NIST (fourth from left)

Report on Hosting "Disaster Crisis Management ICT Symposium 2014" and Report on the Exhibition of "The 18th Earthquake Countermeasure Technology Exhibition Yokohama"

NICT Applied Electromagnetic Research Institute and ICT Forum for Security and Safety (President: Dr. Fumio TAKAHATA) exhibited at The 18th Earthquake Countermeasure Technology Exhibition Yokohama on two days of February 6 and 7, 2014 at Pacifico Yokohama. Also, we held Disaster Crisis Management ICT Symposium 2014 —Communication and sensing technology for crisis management— at its Annex Hall on February 7. In the symposium, we had 2 keynote lectures in the morning and 4 lectures in the afternoon. From NICT, we had lectures on network security by Masashi ETO, Senior Researcher, and on sensing technology using laser by Kohei MIZUTANI, Chief Senior Researcher. About 160 people from disaster prevention personnel of local governments, agencies, universities, and disaster prevention equipment manufacturers took part in the symposium. Presentation slides are available on the following URL. http://ictfss.nict.go.jp/yokohama2014/index.html (Japanese version only)

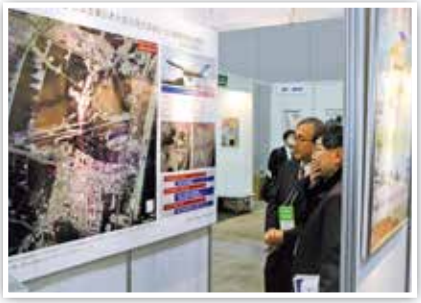
Lecture by Masashi ETO, Senior Researcher

Lecture by Kohei MIZUTANI, Chief Senior Researcher

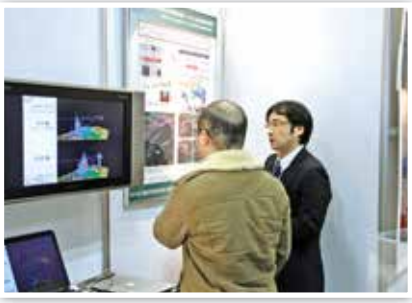
Snapshot of the symposium

In the exhibition, NICT showcased "Observation using the Polarimetric and Interferometric Airborne Synthetic Aperture Radar System (Pi-SAR2) —Significant time reduction for providing data by the on-board processing—", "Phased array meteorological radar", "Non-destructive inspection technology for buildings using an infrared 2D lock-in amplifier", "Radio relay system via small unmanned aircraft", " In-vehicle small mobile station for WINDS", and "Disaster-resilient wireless mesh network —NerveNet—" using exhibition panels and actual machines for demonstrations. In addition, we had the panel exhibition by the members of ICT Forum for Security and Safety, which showed the effort for counter-measures against disasters.

The number of visitors at the exhibition was 14,408 people, and there were many visitors at NICT booth. We perceived visitors' high interests in the earthquake and disaster measure technologies of NICT.



Polarimetric and Interferometric Airbone Synthetic Aperture Radar System (Pi-SAR2)



Phased array meteorological radar

Radio relay link system via small unmanned aircraft

In-vehicle small mobile station for WINDS

NerveNet

Panel exhibition at NICT booth

Report on "NICT Information and Communications Security Symposium 2014"

NICT held "NICT Information and Communications Security Symposium 2014" in KOKUYO HALL (Shinagawa, Tokyo) on February 13, 2014. It was the 8th of annual symposium held every year in February during "Information Security Awareness Month" set by the government. On the day, many people involved in information security from universities, private sectors, and government agencies joined the symposium.

The event consisted of three parts of lectures divided by themes. Following the lectures by guest speakers, we reported on the topics and the progress of R&D in Network Security Research Institute and Cybersecurity Research Center of NICT.

Due to growing concerns in network security, participants vigorously discussed over these lectures; asked questions about the correlation between the observation result of network traffics and a specific cyber attack, and requested disclosure of NICT's achievement of R&D publicly as a system. In addition, the survey taken at the event included opinions asking for stronger promotion for cutting-edge R&D, its further promotion to the public, and requests for continuation of invited lectures by top researchers from overseas in the future.

"We are working on network security as one of the most important issue at NICT. Not only that we achieve research results as an impartial research institute, we would like to stimulate further research for Japan's network security, and contribute to the society", said Makoto IMASE, Vice President, as a closing remark.

For the details of this symposium and lecture materials, please visit the following URL.

http://www2.nict.go.jp/nsri/plan/H26-symposium/ (Japanese version only)

Program

Part 1 Cryptographic Protocols that Provide Advanced Security Features and Safety Evaluations

Invited Lecture

"Research of Cryptographic Protocols for Advanced Security Technologies"
Dr. Hideki IMAI, Professor of Chuo University

Invited Lecture

"Efforts on Evaluation Technology Consortium for Cryptographic Protocols"
Dr. Satoru TEZUKA, Professor of Tokyo University of Technology

"Contribution to International Standardization and Safety Evaluation of Cryptographic Protocols"
Shin'ichiro MATSUO, Director of Security Architecture Laboratory, NICT

Part 2 The Forefront of Network Security Research

Invited lecture

"Taming the Malicious Web"
Dr. Christopher KRUEGEL, Professor of the University of California

"From Darknet to Livenet —the Forefront of Cyber Security Research—"
Daisuke INOUE, Director of Cybersecurity Laboratory, NICT
Director of Cyber Tactics Laboratory, NICT

Part 3 SSL/TLS and its Safety Evaluation for Cryptographic Protocols

Invited Lecture

"Vulnerability of RC4 and Attack on SSL/TLS"
Mr. Takanori ISOBE, Sony Corporation

"Safety of RSA Public Key in SSL Server Certificate"
Shiho MORIAI, Director of Security Fundamentals Laboratory, NICT

Snapshot of the symposium

Employment Information for FY2015 (Permanent Researcher)

National Institute of Information and Communications Technology (NICT) is an independent administrative institution. We would like to invite applicants regardless of age, gender, or nationality for excellent and enthusiastic researchers to promote the research and development on information and communications technology.

Start of employment ● April 1, 2015 (in principle, but negotiable)

Themes ● (1) Network Technologies, (2) Universal Communications Technologies, (3) Advanced ICT, (4) Applied Electromagnetic Technologies, (5) Other innovative research for Information and Communications

Persons to be recruited ● Permanent researcher, more than a dozen

Application deadline ● May 7, 2014 (no later than 17:00 JST)

For details, please visit the following URL and see the Recruitment Information for FY 2015.
http://www.nict.go.jp/employment/permanent/2014perm-kenkyu.html (Japanese version only)

Inquiry ● Tel: +81-42-327-7304 E-mail: jinjig@ml.nict.go.jp

Enjoy our NICT Exhibition Room!

Admission Free

NICT exhibits our latest research results. You can see and even touch them. Enjoy our interactive exhibition.
We are looking forward to your visit.

- Open time: 9:30–17:00 (reception closes at 16:30)
- Venue: NICT Headquarters (Koganei, Tokyo)
- Closed: on Saturdays, Sundays, national holidays, Year-end and New Year holidays
  URL http://www.nict.go.jp/about/exhibition/hq/ (Japanese version only)

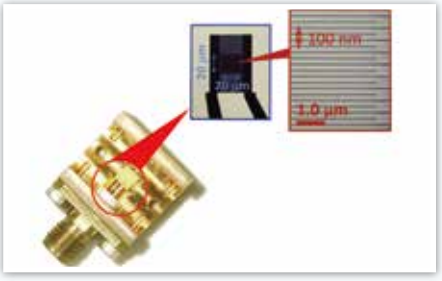
Guided tours for NICT headquarters are also offered every Wednesday.

- About the tour (reservation required)
  URL http://www.nict.go.jp/about/tour/ (Japanese version only)

Aroma shooter

19-core optical fiber only observable via microscope

Monitor exhibition of NICTER/DAEDALUS



Superconducting Single-Photon Detector (SSPD)

NICT NEWS No.438, MAR 2014
ISSN 2187-4034 (Print)
ISSN 2187-4050 (Online)

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

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/en/

〈Recycled Paper〉