Creating Security Technology that Everyone Can Understand, Select, and Use Correctly

Mitsuaki Akiyama
Senior Distinguished Researcher,
NTT Secure Platform Laboratories

Overview

People and businesses are becoming more dependent on cyberspace. Along with the benefits that come with such dependence, the risk of being exposed to threats is increasing; thus, a safe and secure information and communication technology environment is necessary. In 2018, Japan established a new strategy with the aim of building a *cybersecurity ecosystem*. We asked Mitsuaki Akiyama, a senior distinguished researcher at NTT Secure Platform Laboratories, what kind of research and development is required to maintain the safety and security of cyberspace.

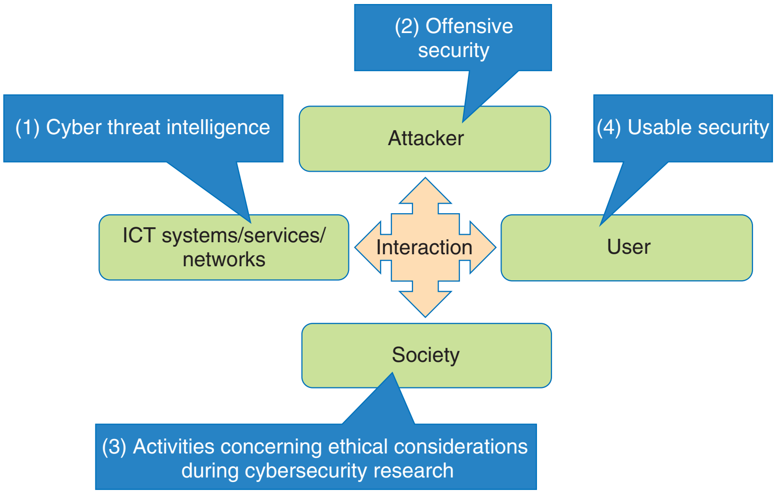
Keywords: cybersecurity, usable security, research ethics

We have obtained numerous results concerning the prevention of various cyberattacks

—Would you tell us about your current research?

The term “cyberattack” has been used frequently in various media outlets. The purpose of cyberattacks includes achieving self-display, making social and political claims, and carrying out intelligence activities. However, cyberattacks aimed at achieving economic gains directly involve many general users, and attackers focused on this thinking about how to conduct attacks efficiently and earn profit proportionate with costs.

We are researching cybersecurity, which is diverse, to protect the safety and security of users from such cyberattacks. We are conducting research on the basis of the following four themes (**Fig. 1**): (i) analyzing the characteristics of cyberattacks, accumulating information (i.e., intelligence concerning countermeasures against cyberattacks), and using that information to prevent similar attacks that may occur in the future; (ii) investigating *offensive security*, that is, stopping potential attacks by discovering and addressing potential security and privacy threats to systems and services from the attacker’s perspective; (iii) investigating activities related to the ethics of research on cybersecurity to provide the results of advanced research to society at large in an appropriate manner by applying, for example, experimental methods for detecting security and privacy threats and methods for disclosing discovered threats; and (iv) investigating *usable security* to design a system that can determine safer behavior based on the understanding of security and privacy awareness of users with regard to systems and services.


(2) Offensive security
(1) Cyber threat intelligence
Attacker
(4) Usable security
ICT systems/services/networks
Interaction
User
Society
(3) Activities concerning ethical considerations during cybersecurity research

ICT: information and communication technology

Fig. 1. Research targets on cybersecurity to protect safety and security of users.

—Have you conducted specific evaluations and obtained results?

Around 2007, when I joined NTT, cyberattacks using malware-infected devices were rampant. Engineers and researchers from various organizations gathered at ICT-ISAC (the Information and Communication Technology Information Sharing and Analysis Center) Japan to discuss the sharing of information and exchanging of ideas for countermeasures. In a demonstration experiment of cyberattack countermeasures led by the Ministry of Internal Affairs and Communications, ICT-ISAC participated alongside major Japanese Internet service providers and security vendors. The honeypots* we developed were used in that experiment, and the actual situation regarding large-scale malware infections and the effectiveness of measures for filtering malicious communications were verified. The results of the experiment helped push the publication of the guidelines for handling cyberattacks on telecommunications carriers and confidentiality of communications, which was jointly formulated by telecommunications-carrier-related associations such as the Telecommunications Carriers Association.

The ICT society continues to evolve and enrich people's lives, and new software, hardware, and protocols continue to be developed daily to support this. However, there is a huge number of these supporting components, and their combinations are complicated; consequently, security defects caused by design mistakes and bugs can be mixed into systems and services, and such problems are difficult to solve.

In such a situation, the attacking side has an overwhelming advantage, and the best the defending side can do to solve these problems is to develop security patches. To change this situation, we are developing an offensive security approach to discover potential defects in systems and services from the attacker's perspective and find potential defects ahead of attackers so that we can take action before the defect is exploited. We have been working for several years to discover threats to security and privacy brought to us by various web services and have already discovered some serious threats that could affect many systems and services around the world. By notifying major social networking services that might be affected by threats before they are exploited and by implementing countermeasures, we have protected hundreds of millions of users from security and privacy threats.

Addressing issues in new research areas while facing ethical challenges

—It sounds as if you have produced important results that are having a significant impact worldwide.

While research on cybersecurity may handle issues in new research areas, it also faces ethical issues that

* Honeypot: A technology that invites cyberattacks and reveals the source of various attacks by operating a decoy that pretends to be a vulnerable system or service.

can have a direct impact on society. For example, research activities and results—concerning the acceptable range of network scanning to find vulnerable devices in cyberspace, experiments with real systems to detect security flaws, and actions to be taken by the discoverer when a defect or vulnerability is found—have sometimes been miscommunicated to the general public. Consequently, many cases have been criticized by the public and have developed into legal battles; thus, impediments to advances in science and technology due to researchers being discouraged must be avoided. Therefore, researchers must consider how to be responsible rather than irresponsibly conducting experiments and publishing attack methods and vulnerabilities.

In biomedical science, ethical issues concerning clinical research have been discussed and addressed for over half a century. An assessment of ethical risk concerning research has been conducted on the basis of the Nuremberg Code and the Belmont Report. The Menlo Report, which expanded the ethical principles of the Belmont Report in the context of ICT and security research, was released in 2012. How to conduct daily research in accordance with these ethical principles is now being discussed, particularly in the Western research community, and it is becoming common to ask authors to describe their research ethics in papers presented at academic conferences. Despite these trends, few research organizations in Japan, which have accumulated sufficient knowledge of ICT and security research, have research-ethics review committees, and awareness of research ethics concerning cybersecurity has not become widespread.

—The topic of ethics is often being discussed in the field of biomedical sciences, but I didn't know it is also being discussed in the field of cybersecurity. How will the ethics concerning research on cybersecurity that has just begun in Japan be promoted and disseminated?

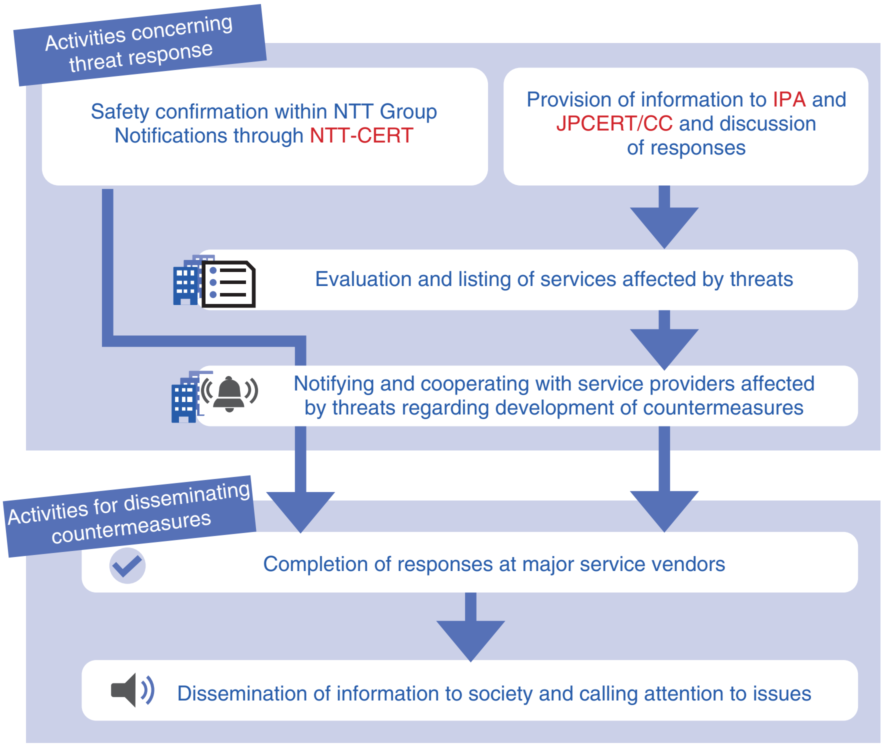
To disseminate the innovative and competitive security technology coming from Japan, I believe that ethical considerations are essential to ensure that research results are accepted by society. Accordingly, since 2016, we have been promoting educational activities concerning ethical research processes in research on cybersecurity at various academic organizations. Regarding research on the above-mentioned offensive security, we have been collaborating with stakeholders and other related parties to appropriately return research results to society. Such experiences are also disclosed to researchers through these activities as best practices (**Fig. 2**).

At the Computer Security Symposium (CSS), a research ethics consultation service—consisting of experts in cybersecurity research and legal systems—was set up to provide appropriate advice to researchers regarding their concerns about research ethics. A checklist summarizing common pitfalls learned from previous activities has been published, and researchers can use it to conduct self-assessments when they are conducting experiments or writing papers. I hope that these efforts will contribute to the creation of a research community for developing globally competitive security technologies.

Collaboration enables us to address serious challenges

—You are not only obtaining research results but also expanding your activities on how researchers work. What will you do in the future?

From the viewpoint of research that will be useful to society, I am currently focusing on usable security. As ICT and associated social systems become more sophisticated, security decisions and actions that users must take are becoming more complex. Although everyone should be able to enjoy the benefits of ICT equally, it is concerning that some users facing situations in which the required decisions and actions are complicated are unable to respond and will be left behind. For example, when a security alert is displayed on a user's browser, it is becoming increasingly difficult for the user to properly determine what the risk is and how he/she should act. Furthermore, social-engineering attacks—which are effective by taking advantage of users' cognitive vulnerabilities by prompting them to take erroneous actions through the displaying of fake warning screens—have also occurred. I believe that creating security technology that everyone can understand, select, and use correctly will make it possible to create a true ICT society that is inclusive of a wide variety of people. Usable security is a major theme for making this belief a reality. By understanding a user's usual recognition and behavior concerning security and privacy, thereby, quantifying security threats, we are aiming to (i) quantify the extent to which users are affected by security threats, prioritize those threats, and deal with the truly important threats, and (ii) design a system that can help users recognize and


Activities concerning threat response
Safety confirmation within NTT Group Notifications through NTT-CERT
Provision of information to IPA and JPCERT/CC and discussion of responses
Evaluation and listing of services affected by threats
Notifying and cooperating with service providers affected by threats regarding development of countermeasures
Activities for disseminating countermeasures
Completion of responses at major service vendors
Dissemination of information to society and calling attention to issues

IPA: Information-technology Promotion Agency, Japan
JPCERT/CC: Japan Computer Emergency Response Team Coordination Center
NTT-CERT: NTT Computer Security Incident Response and Readiness Coordination Team

Fig. 2. Activities concerning response to threats and countermeasure dissemination based on an ethical research process in cybersecurity research.

decide safer behavior.

While we promote activities related to research ethics, we will also tackle challenges in interdisciplinary fields with a team. In a sense, research ethics is an interdisciplinary field, but apart from that, cybersecurity research is conducted to solve problems that comprehensively combine various basic technologies in computer science such as software engineering and networks. We are also addressing challenges that cannot be addressed without incorporating a wide range of interdisciplinary technologies and knowledge, such as in social sciences, psychology, and human-computer interaction. It is extremely difficult for one person to master all fields, so I want to solve serious problems that cannot be solved by one person by working as part of a team in cooperation with experts in each field.

—How did you become a researcher?

Inspired by the movie “The Net” about cybersecurity, I wanted to be a scientist who was “cool” in the minds of kids, so I took the path of security research at university and graduate school. While I was a graduate student, I was able to study with the late Professor Suguru Yamaguchi, a distinguished security researcher. I was greatly influenced by the attitude of Professor Yamaguchi concerning the relationship between technology and society and the spread of the benefits of safe and secure technology. Even now, as a researcher, I still have the same desire to change the world for the better.

As a researcher, however, I want to discover something new and conduct research the result of which will have a lasting effect. Technological innovation is so fast nowadays that it is difficult to predict what will be possible 100 years from now; even so, I want to conduct research that will remain pertinent for the next 10 or 20 years.

So what kind of research will remain? I think the answer is research that pursues the true nature of things. For example, concerning the relationship between humans and computers, society should be human-centered and computers should exist for enriching human life. Therefore, I think that problems that arise between humans and computers will continue to exist. In terms of usable security, human cognition cannot keep up with the progress and complexity of technology, and that situation creates gaps at which attacks are aimed. I think that the need for research that tackles such problems is universal.

What's more, you can't continue this kind of research unless you think it's interesting. Research does not bear results immediately; it can only be done with persistence. However, discovering something during such trial-and-error research activities creates the exciting feeling that "I'm the only one who knows this now!"—and that feeling motivates us even more. When we discovered a threat that would greatly affect society through our research on offensive security, we notified the relevant person, who responded by redesigning the system in question. At that time, I realized that I could do some good.

Start with what you like! Confidence comes later with experience

—Do you have any advice for researchers?

When I'm listening to students, I hear many of them are interested in research, but not many are confident enough. Confidence comes later with experience, so if you have a theme that you want to explore, you should just start researching that theme. I think that the most important thing is to have the mindset that research is interesting and can be continued rather than having a particular talent for research. In my case, being told by my seniors that I was researching something interesting was the first stage in building my confidence. The next stage was when my paper was accepted and acknowledged in the research community. From this, I created an effective cycle by which I could decide what research to try next.

In the process of getting a paper accepted, you may have a tough time getting through peer review, but the feelings you have about that process change as you get older, and as you gain experience, you can often pass peer reviews by applying a little ingenuity to your writing. I think that these hardships and experiences also build confidence.

The other point is that meeting and connecting with people is important. I think that I owe what I am now to good friends and teachers. Cybersecurity research has a wide range of research areas, and experts from various fields come together to solve problems. To take up this challenge, researchers in each field must be respected, and international conferences present good opportunities to meet outstanding researchers. That is why I am actively participating in them.

In particular, meeting my mentor—the late Professor Yamaguchi—had a significant impact on me. Although I'm now a researcher, I'm still often amazed by the paths and signposts he left behind. Even if I don't reach his level, I hope to make similar paths for my subordinates to follow.

■ **Interviewee profile**
Mitsuaki Akiyama

Senior Distinguished Researcher, Cyber Security Project, NTT Secure Platform Laboratories.

He received an M.E. and Ph.D. in information science from Nara Institute of Science and Technology in 2007 and 2013. Since joining NTT in 2007, he has been researching and developing network security techniques, focusing on honeypots and malware analysis. He is also active in promoting research ethics in cybersecurity research.