I Would Like to See a World in Which All Engineers Have a Cybersecurity Background

Mitsuaki Akiyama
Senior Distinguished Researcher,
NTT Social Informatics Laboratories

Abstract

NTT laboratories have a long history of research and development (R&D) in the field of computer science, including the world's most-advanced cryptography and cybersecurity. Senior Distinguished Researcher Mitsuaki Akiyama is conducting R&D on cybersecurity by incorporating social science, such as social value, people's happiness, legal systems, and social acceptability, to transform and develop society. We asked him about the progress of his research and attitude as a researcher.

Keywords: socio-technical system, usable security, research ethics

Pursuing a *socio-technical system* that is based on relationships and interactions among technology, people, and society

—It has been three years since your last interview in 2019. How have your research activities been going since then?

Continuing from our last interview, I have been researching cybersecurity to protect the safety and security of users from cyber-attacks. I'm focusing on four key themes: (i) research on analyzing the characteristics of cyber-attacks, accumulating such information (i.e., intelligence for cyber-attack countermeasures), and using this information to prevent similar attacks in the future; (ii) research on *offensive security* to stop attacks before they happen by finding and dealing with potential security and privacy threats and flaws (such as bugs in systems and services) from the attacker's viewpoint; (iii) activities related to ethics in research on cybersecurity to ensure that the results of advanced research properly benefit society, including experimental methods for discovering security and privacy threats and methods for disclosing discovered threats; and (iv) research on *usable security* to design systems that prioritize security threats and help users recognize such threats and make safer decisions by quantifying these threats according to users' security and privacy awareness and behavior toward systems and services.

In July 2021, NTT laboratories were reorganized, and NTT Social Informatics Laboratories was established. Considering it necessary to proceed with research and development (R&D) in various fields in a more composite manner, NTT Social Informatics Laboratories is engaged in a variety of research projects. These include (i) well-being research for human happiness; (ii) innovation technology for

social systems through the fusion of information and communication technology (ICT) technology and social science; (iii) establishment of new technologies to eliminate threats such as cyber-attacks; (iv) establishment of technologies to realize innovations to create safe social systems through the analysis and prediction of social information; (v) creation of high-value-added social systems through data distribution and utilization that balances usability and security; (vi) new data protection technology that utilizes cryptography as well as physical properties; and (vii) creation of fundamental next-generation cryptography theories that will lead global expansion [1].

Cybersecurity has often been regarded as a cost factor. At NTT Social Informatics Laboratories, we are breaking away from this mindset. That is, we are engaged in R&D on cybersecurity technology that acts as a "prime mover" to drive and develop people and society by maintaining security and privacy. Accordingly, I'm taking advantage of the opportunity to pursue my research activities at this lab and increasing the weight of interdisciplinary aspects, such as human behavior and social aspects, in my research compared with the past. As people are forced to use new technologies without having sufficient knowledge of their security and privacy, new security and privacy threats are emerging. Under these circumstances, I believe there is an emerging need to establish a scientific foundation for cybersecurity and an approach to solving problems concerning cybersecurity from an interdisciplinary perspective.

In the industrial sector, for example, cybersecurity technology has been dominated by symptomatic and empirical measures and operations against daily cyber-attacks. Such reactive measures require an endless amount of operations, which results in increased personnel costs, slow response, and security fatigue and makes it difficult to maintain a reliable ICT system against increasingly sophisticated cyber-attacks. To create a fundamental solution that eliminates this problem, I believe it is important to create cybersecurity technologies that are transparent, reproducible, and verifiable through means such as theoretically sound mathematical and scientific methods, comprehensive theory of cybersecurity, principled system-design methods, modeling at various layers and scales for complex and dynamic systems, and creating indices to evaluate the effectiveness of cybersecurity technologies.

From the perspective of an interdisciplinary approach, I'm also pursuing a *socio-technical system* that is based on the relationships and interactions among technology, people, and society. Even if a technology is secure, it may not be secure if people use it incorrectly, and if it does not become widely used in society, people will not be able to fully benefit from it. Although many security technologies have been devised, many have never been fully used. There are many cases in which end-users are deceived by phishing scams or a technology was not properly used because the reasons for issues, such as the difficulty of implementing security-by-design in development projects, had not been clarified.

In view of these issues, I've been adopting an interdisciplinary approach that incorporates fields, such as social science and social psychology, in addition to computer science to clarify the root causes of cybersecurity problems from the viewpoints of humans and society and review ICT systems from their design phase. To achieve usable security, I'm aiming to solve security and privacy problems that depend on people's perceptions and decision-making so they cannot be solved simply by focusing on systems. Solving such problems involves the following process: (i) observing and analyzing human behavior, mental models, and decision-making processes regarding security and privacy, (ii) feeding the findings of the observation and analysis back to system design, implementation, and operation, and (iii) enabling people to make appropriate decisions on the basis of correct perceptions about security and privacy.

To make this process feasible, I believe it is essential to properly observe and analyze people's behavior and perceptions, and I am researching measures to prevent the spread of false information. False information includes *misinformation*, which is spread unintentionally, and *disinformation*, which is spread with the intent to cause harm or deceive. The spread of misinformation and disinformation through social media represents the next generation of cyber-attacks that threaten correct human cognition and judgment. It is not limited to individual problems such as falling victim to phishing or being deceived by hoaxes; it can have a major impact on democracy, as in the case of the 2016 US presidential election.

Our papers highlighting social issues were accepted by prestigious conferences

—You have achieved significant academic results through these research activities.

Our paper on offensive security was accepted at the

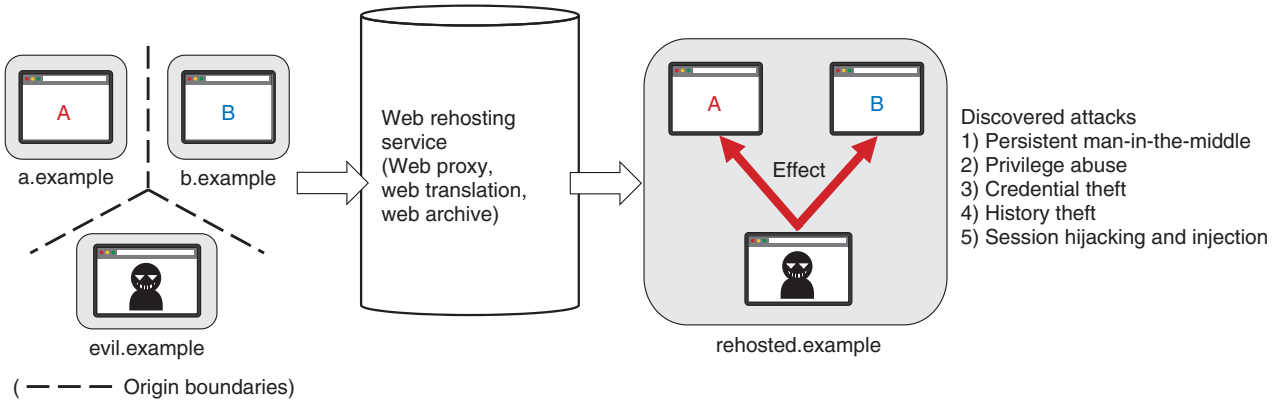

Fig. 1. Potential threats to web rehosting services.

27th Annual Network and Distributed System Security Symposium (NDSS 2020), one of the top cybersecurity conferences, and received the Distinguished Paper Award [2]. We named a service that rehosts web content on another web site a web rehosting service, developed multiple threat models for web rehosting services, and clarified, through verification, the conditions under which the threats are actually manifested (**Fig. 1**).

We discovered a critical phenomenon concerning web rehosting services; namely, the mechanisms underlying web security fail to work when web content from different origins (i.e., attributes defined by URL protocol, host, port pairs) are merged into the same origin. This discovery indicates that a variety of attacks are possible in web rehosting services, and appropriate design guidelines for web services to avoid such attacks can be provided.

This research has made it possible to detect threats before they become apparent and take countermeasures against them at the design phase. It is thus possible to avoid service operators having to redesign a service as a whole. Our goal is not to simply find vulnerabilities but to establish a more-versatile verification method and theoretical foundation for finding such security and privacy threats. With that goal in mind, we have identified many threats on the web, where various types of communication are currently aggregated, and established methods for verifying them. I hope to summarize our findings in about five years.

Regarding usable security, our research aimed at enabling secure software development focusing on developers and development projects was selected for presentation at the 37th Annual Computer Security Applications Conference (ACSAC 2021) [3]. This research was based on a large-scale online survey of professional software developers in Japan and the United States to identify organizational issues such as whether a decision-making authority exists and difficulties in decision-making (**Fig. 2**).

Our paper on explaining the principles of human deception and creating appropriate support technologies was accepted at the 17th Symposium on Usable Privacy and Security (SOUPS 2021) [4]. While previous research implicitly studied perceptions and behaviors of users when confronted with phishing emails in their native language, we focused on non-native English speakers, who make up the majority of the world's population, confronting English phishing emails. For the first time in a large-scale study, we clarified the relationship between language and handling phishing emails and proposed support techniques specific to non-native English speakers.

At European Symposium on Usable Security (EuroUSEC) 2021, our paper indicating problems in user-study methods regarding why people are deceived with respect to phishing emails received the Best Paper Award [5]. The study revealed for the first time that several methods used for screening participants in user studies are highly inconsistent because they exclude careless participants who are easily deceived by phishing emails, namely, those whose data are most needed. Another paper of ours, presenting research on countermeasures against the spread of false information in social media, was accepted at the 7th International Winter School and Conference on Network Science (NetSci-X 2022) [6], and some of the results of that research were exhibited and reported at the NTT R&D Forum.

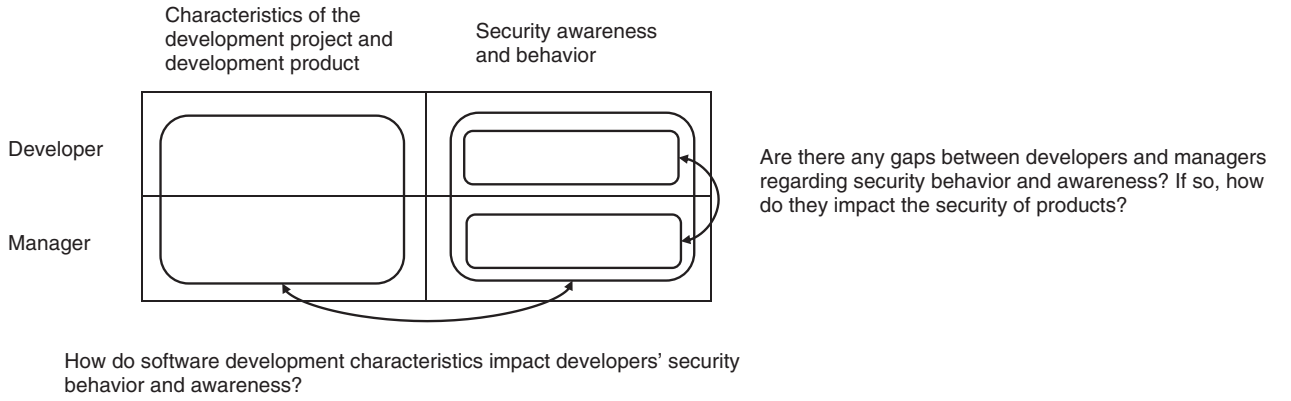

Fig. 2. Analysis of factors that hinder secure software development.

You become good at what you like doing

—What do you keep in mind and consciously implement when looking for research themes?

First, I try to be interested in new technologies and services while constantly updating my knowledge. Rather than thinking about a technology alone, I consider how such technology is used from the perspective of the people, organizations, and society involved with the technology as well as laws and ethics.

I also value having discussions with experts in fields different from mine. Since it is common to go beyond one's field of expertise when attempting to achieve something, it is essential to collaborate with researchers in other fields and adopt an interdisciplinary approach. In this sense, I think that NTT laboratories have abundant human resources.

I believe that the phrase "you become good at what you like doing" is an important attitude to have as a researcher. I don't think I have special research talents that are superior to those of others, but I do think I have a stronger interest in cybersecurity issues.

I have seen many people who have stopped doing research despite their very high technical ability or did not take a research job because they said they did not have the confidence to do research. However, research does not produce immediate results; in fact, it can take several years, maybe even 10 or 20 years, to produce a single result.

In such a situation, you may want to quit by thinking that you have no talent; however, if a research theme is something you are interested in, you may be able to continue to work on it with high motivation and interest, regardless of whether it produces results. If you can continue to work on it, the likelihood of achieving results will certainly increase.

For this reason, I first consider whether I really like the research theme I intend to work on. If I really like a research theme, I can only accept the results of my research, whether successful or not, and that those results will not change my liking of the research theme.

—How will you advance your research activities in the future?

R&D on cybersecurity had often considered individual threats in isolation and in a retrospective manner, so it has been difficult to solve fundamental problems. I'd like to see a world in which not only cybersecurity experts but also all engineers have a background in cybersecurity and take cybersecurity into account when manufacturing products. In other words, I want all engineers to share the mindset of a cybersecurity expert. I believe it is my job to help create cybersecurity technology that is available to everyone. In that case, the meaning of the term *cybersecurity expert* would change.

I'm also working on research ethics. In the cybersecurity-research community in Japan, I've been continuously raising awareness of cybersecurity-research ethics since around 2016, and the concept has spread to a certain level (**Photo 1**). In fact, a consultation service on research ethics has been available in Japan since 2018 at the Computer Security Symposium, one of the largest computer security symposiums in Japan, even before measures regarding research ethics were taken at the IEEE (Institute of Electrical and Electronics Engineers) Symposium on Security and

Photo 1. Panel discussion at a symposium in the Japanese cybersecurity community.

Privacy. The Computer Security Research Group of Information Processing Society of Japan has also released a checklist of research ethics in a form that can be used by various research groups.

In 2021, the conduct of a researcher at a US university became controversial. The researcher implemented patches with vulnerabilities to the Linux kernel to evaluate the code review process in the open-source software community and wrote a paper about it. In light of this, a panel discussion was held in the Japanese cybersecurity community to discuss the relationship between cybersecurity researchers and the development community. In this discussion, I argued that (i) experiments on people and their communities and organizations must be designed and conducted with full consideration of their impact on those people, communities, and organizations, (ii) no divisions should exist between the development community and research community, and (iii) it is important for researchers to work together as members of the development community.

It is important that cybersecurity researchers respect software developers and cooperate with them on better technology development on the basis of these three arguments, and I intend to continue to focus my efforts on raising awareness of cybersecurity-research ethics.

References

[1] Website of NTT R&D, NTT Social Informatics Laboratories, https://www.rd.ntt/e/sil/overview/index.html#introduction

[2] T. Watanabe, E. Shioji, M. Akiyama, and T. Mori, "Melting Pot of Origins: Compromising the Intermediary Web Services that Rehost Websites," Proc. of NDSS 2020, San Diego, USA, Feb. 2020.

[3] F. Kanei, A. A. Hasegawa, E. Shioji, and M. Akiyama, "A Cross-role and Bi-national Analysis on Security Efforts and Constraints of Software Development Projects," Proc. of ACSAC 2021, pp. 349–364, Austin, USA, Dec. 2021.

[4] A. A. Hasegawa, N. Yamashita, M. Akiyama, and T. Mori, "Why They Ignore English Emails: The Challenges of Non-native Speakers in Identifying Phishing Emails," Proc. of SOUPS 2021, Online, Aug. 2021.

[5] T. Matsuura, A. A. Hasegawa, M. Akiyama, and T. Mori, "Careless Participants Are Essential for Our Phishing Study: Understanding the Impact of Screening Methods," Proc. of EuroUSEC 2021, pp. 36–47, Online, Oct. 2021.

[6] S. Furutani, T. Shibahara, M. Akiyama, and M. Aida, "Competitive Information Spreading on Modular Networks," NetSci-X 2022, Porto, Portugal, Feb. 2022.

■ **Interviewee profile**

Mitsuaki Akiyama 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 engaged in research and development on cybersecurity. His research interests include cybersecurity measurement, offensive security, and usable security.