Cybersecurity Research Ethics and Related Activity in Japan

Mitsuaki Akiyama
Distinguished researcher
Secure Platform Laboratories,
Nippon Telegraph and Telephone Corporation

Katsunari Yoshioka
Associate Professor
Graduate School of Environment and
Information Sciences, Yokohama National University

1. Cybersecurity Research Ethics

The rapid development of the Internet has brought convenience and efficiency to our daily lives, but it has also brought increases in cyberattack occurrences and availability of sensitive information that can be used to identify individuals. ICT research, and cybersecurity research in particular, has also had major effects on our living environments, from both research results and the research processes themselves.

To conduct cybersecurity research, it is essential to observe actual incidents on the Internet. However, such measurement research can deal with a wide range of communications beyond just that of the attack being observed, so it involves various security risks related to privacy and other issues. To minimize such risks, appropriate planning and accountability for any potential risks must be achieved before proceeding.

Further, if a security hole (defect) in a particular piece of software is discovered in the process of such research, there is a risk that it will be exploited maliciously in an attack if it is brought to light before being dealt with adequately in affected systems and services.

Since the year 2000 as the Internet has spread, there has been ongoing ICT research on a large scale. However, since there have been no appropriate guidelines for ethical research, there is no doubt that some research has been done without adequate ethical review. As such, discussion of research ethics related to ICT and cybersecurity has been on the increase since 2010, particularly in the USA, new ethical principles have been established, and technical research papers are starting to be reviewed from the perspective of research ethics. Research ethics is unavoidable with any innovative research in cybersecurity, and has become an essential aspect of work for all researchers and technologists creating globally competitive technologies.

The importance of research ethics in cybersecurity has also become more widely recognized in Japan recently. Symposiums are being held, mainly by academic institutions, and organizations to develop and promote research ethics in cybersecurity have been established.

This article describes principles of cybersecurity research ethics, introduces global trends and recent cases, and discusses the current state and outlook for cybersecurity research ethics in Japan.

2. Principles of research ethics

No suitable guidelines related to research ethics were available for early ICT research, and in many cases, research was done without adequate ethical review. This includes handling of malware, counter attacks for cyberattacks, attacks on or publication of vulnerabilities, and collection of detailed vulnerability and attack information. As such, the approach taken in the Belmont Report, which was produced in 1979 to establish research ethics in the biomedical field, had to be interpreted in the context of ICT research. Then in 2012, the US Department of Homeland Security issued the Menlo Report, compiled mainly by researchers in the USA. This article introduces the research ethics principles in the Belmont Report and discusses differences between biomedical and ICT research, and then introduces new research ethics principles stipulated by the Menlo Report.

2.1 Belmont Report

The Belmont Report defines research ethics for the biomedical field, based on the following general principles.

- Respect for Persons. Participation in research is decided freely by each participant, based on informed consent (respecting their right to make decisions based on adequate explanation of the details).
- Beneficence. Maximizing the potential benefit and minimizing the potential harm resulting from the research. An assessment of risk, harm and benefit is done.
- Justice. Individuals must receive fair consideration for how they are treated. Also benefits of the research must be fairly distributed, and the burden also shared equally among research subjects.

2.2 Differences between biomedical and ICT research

The ethical principles cited in the Belmont Report are a basis for biomedical research, but they also suggest a basic code of conduct that can be applied broadly in other fields.

However, it must be noted that ICT research is now being done based on environmental conditions that could not have been imagined at the time the Belmont Report was created. Specifically, differences between biomedical and ICT research include the following.

- Scale
  The Belmont Report assumes biomedical research in which the researcher and subjects are able to interact face-to-face, dealing with tens or thousands of subjects, while ICT research is able to collect and analyze data from millions of people. In such cases it is not easy to obtain informed consent from each person.
- Speed
  Most biomedical research involves manual processes (conducting interviews in a laboratory, etc.), so if problems occur, research can be suspended before damage spreads. Conversely, ICT research has the potential to adversely affect millions of devices in an instant, so risks and damage must be assessed rapidly and accurately.
- Aggregation and interrelation of information
  In ICT research, information resources are interconnected through networks, and are strongly related. For example, smartphones store information including email addresses, lists of contacts of friends and associates, and SNS account information. Thus, they could leak personal information of not only the owner, but also others connected to the owner.
- Decentralization
  With ICT, various technologies are interdependent and communication content is located in various locations as text, audio, or video, and is controlled by various entities. As such, it can be difficult to identify from whom informed consent should be obtained.
- Non-transparency
  Biomedical research involves meeting with subjects, but ICT research is done involving many people indirectly, via ICT. Subjects are not met directly so it is difficult to anticipate who will be affected by the research and how.

Researchers in ICT are obliged to design and execute research plans ethically, with consideration for these sorts of condition.

2.3 Menlo Report

As the Internet developed, differences between biomedical and ICT research (Sec. 2.2) become clearer, and it became necessary to interpret the approach taken in the Belmont Report in the context of ICT research. As such the Menlo Report[1], modeled after the Belmont Report, was established in 2012. In addition to interpreting the three main principles in the context of ICT research, the Menlo Report adds the following new research ethics principle.

- Respect for Law and Public Interest. Research methods and results must maintain transparency and take responsibility for such behavior.

This ethical principle interprets the Beneficence principle from the Belmont Report in the context of ICT research and clarifies new issues that need to be addressed, such as opposition or ambiguity between laws of different regions, stakeholder-specific difficulties, and discrepancies between laws and public interest.

If a security hole is discovered in the research process, there is an obligation to practice Responsible disclosure, taking responsibility to identify the stakeholders that could be affected and disclose the information in a way that minimizes damage. Note that the Menlo Report is accompanied by a summary of discussion and responses based on example cases[2].

3. Global trends

Given the increase in concern for cybersecurity research ethics, new international academic conferences focusing on cybersecurity research ethics have been held between 2013 and 2015, including CREDS, CREDSII, and NS-Ethics[3][4][5]. Activities at these conferences deal with changing ICT environments and support better ethical research, including review of past research projects for which discussion of research ethics was inadequate, sharing of best practices, and ethical research design.

Since 2013, there has also been a steadily increase in mentions of research ethics in calls for papers for conferences, including the top cybersecurity conferences (IEEES&P, ACM CCS, USENIX Security, ISOC NDSS). Specifically, calls for papers are asking for “Clear descriptions of research ethics in papers that could stimulate discussion on research ethics. Such papers must also be approved by the research ethics committees of their own organizations.”

So how is ethical cybersecurity research actually being practiced around the world? In the results of a survey of research ethics descriptions in papers at a top international conference in the past several years (approximately 300 papers presented at USENIX Security 2012 to 2016), discussion and assertions on research ethics were classified mainly into the following categories.

- Obtaining consent/agreement
  User (subject) consent, service operator agreement, research ethics committee (IRB) consent.
- Legal/legitimate procedures, performance of anonymization, conformance to policies/guidelines, assertion of legality, no-alternate options, performance of responsible disclosure.
- Risk/Damage control. Minimizing risk, preventing new damage.

- Benefits, sharing best practices, public benefits.
- Research application that does not affect other persons.

In this way, the experience of earlier researchers with concrete methods can be used as reference case studies for researchers and technologists starting similar research in the future.

4. Research case studies

This section introduces cases of research by organizations in Japan that are particularly relevant to research ethics.

4.1 Sandbox detection

Yokoyama et al. from Yokohama National University has studied sandboxes, which are a tool used for analysis and detection of malware. They provide a run time environment for running a program being investigated, to study its behavior so it can be detected, and to analyze its functionality. They have been able to clarify typical characteristics of sandboxes and identify the potential to inhibit malware analysis and detection using a sandbox[6].

For this study, they first investigated the state of sandboxes actually in operation. To gather information about the features of the sandboxes being used by the services, they created data-gathering samples and submitted them to online malware analysis services that perform sandbox analysis. They used machine learning based on feature data to show that the sandboxes and ordinary user environments can be accurately discriminated, and reported that their discriminator is also effective for commercial sandbox products.

These test results and test samples were provided to the sandbox product vendors and malware analysis service providers beforehand, to contribute to improvement of these products and services. Also, the product names and particular internal information for these products and providers were anonymized in papers, and collected features were presented as statistical data, to minimize any effect on particular products or services. By publishing research results in this way, effort was made to maximize the benefits and minimize any damage caused.

4.2 Social account detection

Watanabe et al. from the NTT Secure Platform Laboratories has discovered a new type of privacy attack able to identify the account of any targeted user on a social Web service[7]. This attack uses the blocking functions that are provided as standard on social Web services maliciously, so it has the potential to affect social Web services widely around the world, and users are vulnerable to such an attack.

This research involved experiments on real services to verify the attack, and these tests were designed very carefully to minimize the risks and other negative effects. In particular, to avoid attacks on real users, experiments were conducted on accounts owned by the researchers, and were planned carefully to avoid any unnecessary increase in load on the service.

They also contacted the 12 service operators and major browser vendors being checked for the vulnerability beforehand, and shared information regarding how to reproduce the attack method and how to counter it. As a result, service operators and browser vendors each changed their specifications, so this research contributed to social Web services that are safer for users. These results were also presented at the international conference, IEEE Euro S&P 2018, raising awareness of the threat around the world and contributing to the public good.

5. Current and future state in Japan

Since 2016 in Japan, the sharing of knowledge regarding cybersecurity research ethics and serious discussion of ethical research practices has begun in a domestic research community called the “anti Malware engineering WorkShop (MWS)”[8].

Later, cybersecurity experts gathered under one roof and discussed awareness of issues and action plans for the future at the largest security technology symposia in Japan, the Symposium on Cryptography and Information Security (SCIS)[9], and a symposium held by the Japan Society for the Promotion of Science (JSPS). However, little research in Japan requires discussion of research ethics, so more research is needed for these initial steps and to push it further.

5.1 Emerging issues

- Sharing knowledge and practices
  Impact and benefits around the world varies by case, and cannot be determined in a uniform way. As such, researchers and technologists must accumulate more case studies. Responsible disclosure is particularly complex, from stakeholder estimates to practical procedures. In Japan, reports can be submitted to the “Information Security Early Warning Partnership” operated by IPA and JPCERT/CC, which provides a mechanism for performing responsible disclosure of vulnerabilities in products and software. On the other hand, there are cases that would not be considered vulnerabilities in software or products, but still require responsible disclosure (examples in Sec. 4). These must be handled mainly by the researchers themselves. It is difficult for a single organization to accumulate enough know-how for this, so a venue for discussion and knowledge sharing across organizations is needed.

- Research significance
  In research requiring discussion of research ethics, there is research value in the attack methods and vulnerabilities discovered, but also in the computer science and engineering techniques used to find them. Spreading these detection techniques throughout the world also provides global benefits such as enabling developers to check for and find them at the development stages. Clarifying common pitfalls and the basic ways to deal with them also has research value. Spreading and popularizing these issues and solutions throughout the world also has benefits for the future.
- University-industry collaboration
  Substantial solutions are only possible through collaboration between academia and industry. As such, discussion involving industry is necessary, since the consensus on issues, such as grace periods for implementing solutions and methods of responsible disclosure, could differ in different areas of industry. Researchers must also work to build trust relationships between academia and industry so that, for example, responsible disclosure, adequate information, grace periods, and work-arounds can be presented.

5.2 Future initiatives

Among the initiatives receiving wide recognition in Japan is the Cyber Security Research Ethics Working Group, established in February 2018 at the 192nd Committee on Cyber Security in a group of University-Industry Cooperative Research Committees from JSPS[10]. This working group is intended to promote activities supporting the understanding and practice of cybersecurity research ethics, with a neutral perspective spanning academia and industry.

Even looking globally, there are still very few research facilities that maintain a research ethics committee capable of making proper judgments regarding cybersecurity research ethics. In light of this, the Computer Security Symposium (CSS) in Japan is considering having a desk for consultation on cybersecurity research ethics. The desk would enable researchers who have questions on research ethics to discuss them before proceeding with their research.

6. Conclusion

The ethical principles stipulated in the Menlo Report are essential knowledge that researchers and technologists should have access to when conducting research in ICT and cybersecurity.

We anticipate that innovative activities promoting ethical research in cybersecurity in Japan will contribute to ongoing creation of advanced and competitive security technologies from Japan.

References

[1] Menlo Report: https://www.caida.org/publications/papers/2012/menlo report actual formatted/

[2] Applying Ethical Principles to Information and Communication Technology Research: http://www.caida.org/publications/papers/2013/menlo report companion actual formatted/menlo report companion actual formatted.pdf

[3] Cyber-security Research Ethics Dialog & Strategy Work-shop (CREDS 2013): http://www.caida.org/workshops/creds/1305/

[4] Cyber-security Research Ethics Dialog & Strategy Work-shop (CREDS II-The Sequel): http://www.caida.org/workshops/creds/1405/

[5] Workshop on Ethics in Networked Systems Research (NS-Ethics): https://conferences.sigcomm.org/sigcomm/2015/netethics.php

[6] Yokoyama et al., SandPrint:Fingerprinting malware sandboxes to provide intelligence for sandbox evasion, RAID 2016.

[7] Watanabe et al., User Blocking Considered Harmful? An Attacker-controllable Side Channel to Identify Social Accounts, IEEE EuroS&P 2018.

[8] anti-Malware engineering WorkShop (MWS): https://www.iwsec.org/mws/

[9] Symposium on Cryptography and Information Security (SCIS): https://www.iwsec.org/scis/2018/

[10] 192nd Committee on Cyber Security in the group of University-Industry Cooperative Research Committees: https://www.jsps.go.jp/english/e-soc/list/192.html