Mimicry in Cyberspace and Application to Malware Evasion Technology

1810048 Takahiro Kitazawa

With the development of information technology, important information such as document files, personal information, and passwords are managed on computers. By using the Internet, this information can be transmitted at high speed and long distances. However, there are cyber attacks that steal and sniff such information via the Internet. According to Information Security 10 Major Threats 2019 released by the Information-technology Promotion Agency, in 2019, targeted attacks, Business E-mail Compromise(BEC) and ransomware were the most common cyberattacks on organizations.

National center of Incident readiness and Strategy for Cybersecurity(NISC) has proposed to strengthen its ability to respond to "accident based society" in the Second Information Security Basic Plan(released on February 3, 2009). As of 2019, accident based security technology has IPS, cyber resilience, and cyber deception. Cyber deception relies on the attacker entering the network and uses deceptive mechanisms. The purpose of cyber deception is to increase the cost of once attack. This security technology increase the cost of attack and decrease the value of the target. At result, it can stop the attacks. There are two ways to achieve deceptive protection: obfuscation and mimicry. Previous works about mimicry further classified mimicry into protective and warning colors. Protective color is to conceal features that are a threat to attackers such as honeypots. Warning color is to perform protection by reproducing features in the object.

However, previous works about deception and mimicry in cyberspace have obscured their definitions. The detailed definition of mimicry could not be confirmed. In addition, only superficial information such as a name or an existing path in a process, file was defined regarding the characteristics necessary for performing mimicry.

Here I show, I define about deception and mimicry in cyberspace in detail to reveal it. In addition, I propose a mimicry construction flow for constructing the cyber deception using mimicry, and a mimicry element classification table that summarizes mimicry elements and mimicry conditions. Using the mimicry element classification table, I can construct clever mimicry. The level of mimicry of the constructed mimicry environment can be confirmed. As an example of using the mimicry construction flow and the mimicry element classification table, I applied it to malware avoidance technology. In this research, the malware avoidance environment can provide a consistent and independent mimicry environment for each malware process. This is different from the construction method of the previous research.

For applications in malware avoidance technology,I make simple program which provides the mimicry environment which ensured consistency and independence. In order to verify this program, I created a pseudo malware with only a pair analysis function and confirmed its operation.

I also carried out qualitative evaluation of the design method and implementation method of the previous research and this research.

In this paper, I defines deception and mimicry in cyberspace. I suggest construction procedure and mimicry element classification table were proposed. And, as an example of the application of this research, I made the the malware avoidance environment.

I think this paper has three future task. First, it is necessary to consider recognition type and protection type mimicry of four mimicry categories. I need to identify the factors, situations, and psychological impact that are needed to bring out the cognitive and protective effects. Second, I need to think about mimicking in other OS and content When the purpose of the OS and the contents are different, the mimicry element and the mimicry condition may change. Therefore, it is necessary to consider this. Third, I should implement high mimicry environment using the Mimetic DLL or server. I dealt with two simple pair analysis functions. However, I must support other pairing functions. Purpose of cyber deception using mimicry increases the cost of an attacker's action and induces the attacker to stop. But if I can provide more sophisticated mimicry, I think I can take advantage of the cat-and-mouse relationship between attackers and security engineer.