Abstract

The purpose of this research is to solve the problem of human error in the existing threat modeling field and the difficulty of implementation due to high introduction costs, by automatically estimating threat information from network design information. It is to support the implementation of modeling. First, we estimated potential threat information and mitigation measures from the threat database MITRE ATT&CK and network configuration information. In contrast to Rak et al.'s method, which is a research that automates existing threat modeling, we estimate threat information using MITRE ATT&CK, which is a more general threat database, to compare and analyze discovered threats. We compared the accuracy. As a result, we confirmed that our method had a vulnerability detection performance similar to that of existing methods. Regarding the input of design information for network systems, we were able to use fewer features compared to existing methods. This made it possible to reduce work costs during the preparation stage for handling the automation system. By using MITRE ATT&CK in the vulnerability database, we succeeded in adding mitigation, subtechniques, and tactics to techniques. This can be expected to make it easier to counter vulnerabilities using mitigation compared to using a threat list consisting only of techniques. Also, by knowing the tactics in advance, it became possible to predict the attacker's objectives. One of the future challenges for this research is that the threat database is only MITRE ATT&CK, so it is difficult to compare the results with other methods that use different vulnerability databases. Improvements can be expected by using a mapping technology called BRON. The second challenge for the future is that by simplifying the design information of the network system, a lot of unnecessary vulnerability information will be detected. In the current method, design information is input manually by humans. By automating this process, it may be possible to refine the input information and narrow down the detected threat information.