Towards Automated Malware Analysis for Understanding Characteristics in Malicious Capability Using Dynamic Analysis

氏　　名　　与那嶺 俊

研 究 室 名　　サイバーレジリエンス構成学研究室

主指導教員名　　門林 雄基

内容梗概（1 ページ目に収めること）

In this dissertation, we tackle with developing countermeasures against malware through automated malware analysis in order to gain an understanding of the malicious capability that the malware can accomplish. This research explores methods that can automatically characterize the malware behavior and is generalized to analyzing malware that can target various kinds of internet-connected devices like IoT. Against the threat landscape brought by the innovation and sophistication of malware, this research aims to provide perspectives to keep adapting functionalities for analyzing malware that can target various devices like IoT.

First, we propose an analysis method that automatically identifies the kind of malicious capability that the malware can perform. In order to identify a specific malicious capability in malicious activity, we consider system calls executed by malware to perform data input from file/socket as malicious actions that may initiate malicious behavior. This is based on the insight that most malicious behavior involves data input from a file that malware can target and a socket that malware has connected with C&C servers. Our proposal leverages data flow tracking using taint analysis and virtual machine introspection in order to analyze malicious activity executed in the system in detail. The experimental evaluation has shown the feasibility of our proposal to identify various kinds of malicious capabilities from malware's activity in an automated manner. Further, we have shown an advantage of our proposal that may work effectively for analyzing malware that uses multiple malware processes for evading dynamic analysis. Thus, this work also may provide a perspective that complements the traditional malware analysis method.

Second, we proposed a sandbox dedicated to extracting characteristics of the malicious behavior for analyzing IoT malware. Our proposed sandbox supports execution environments for binaries specific to architectures for IoT and aims to provide functionality for automating dynamic malware analysis for IoT malware. Besides, our proposal provides a feature that elicits the malicious behavior of IoT malware and facilitates dynamic analysis. This work demonstrates the feasibility of our proposal that can perform dynamic malware analysis automatically against a number of malware samples in a dataset. Further, this work combines methods for advanced dynamic malware analysis and verifies the benefits that can be brought by these efforts. The evaluation based on data analysis approaches has demonstrated an advantage that this approach could provide insights for understanding the malicious behavior of IoT malware in detail.