平成26年度 情報工学コース卒業研究報告要旨

高田 研究室	氏　　名	魏　靖軒
卒業研究題目	HAZOP-based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack	

Nowadays, ECUs(Electronic Control Units) are commonly integrated within modern automobiles. While these digital components have brought us various advancements both in efficiency and safety, they have also introduced us some new potential risks. Researchers have identified that the system is actually fragile if an attacker could locate a security flaw in the system. Although security analysis techniques such as Attack Tree and STRIDE have been published, a general, compatible, and effective technique for analyzing security vulnerabilities still remains uncertain in the industry.

This paper presents a security analysis method to conduct at the phase of system design, which is more easy and applicable to even non-experienced beginners of security analysis. During the analysis, threats should be eliminated as much as possible by implementing related countermeasures. HAZOP, hazard and operability studies, is a technique applying guidewords to each process of the chemical production, in order to infer deviations from the original design. And possible causes leading to the deviation as well as all possible consequences are also discussed to reduce risks of certain chemistry plant. Based on this fundamental idea from HAZOP, this paper refines a new security analysis method by changing the original guidewords into 8 actions extracted from the attack taxonomy of CERT. This HAZOP-based security analysis method uses these actions as the new guide words to examine a given software architecture and uncover the security vulnerabilities from the design.

To consider the causes and the consequences from certain deviation, this paper discusses about system local effects as well as the global effects that was generated by the deviation. On summarizing all the result entries into one overall table, this paper also issues a severity value to each of the result entry in order to argue about whether or not further precautions or even adjustments of architecture should be implemented during the system design. This paper conducts security analysis across 2 levels, an overall system service level using guidewords borrowed from SHARD, and a detailed objects messages level using the new guidewords extracted from the attack taxonomy by CERT. Diagrams also play significant role as they perfectly visualizes the system's design, making it possible to conduct the analysis explicitly. And this paper uses UML component diagram for the service level and UML sequence diagram for the messages level to assist analyzing the security concerns.

To demonstrate the applicability of the proposed method, this paper also describes a simple case study of Open Source Immobilizer Protocol Stack(here as OSIPS) developed by Atmel®. This paper analyzes security vulnerabilities inside the OSIPS from service level as well as messages level in order to generate a comprehensive and accurate analysis result.

At last, by comparing the final results to papers about security analysis on OSIPS, this paper discusses about the strengths and drawbacks of this security analysis method. And as future works, we plan to address problems found in this case study.