組込みシステム向け HAZOP ベースセキュリティ分析手法

魏　靖軒[†]，松原　豊[†]，高田　広章[†]

HAZOP-based Security Analysis for Embedded Systems

Jingxuan Wei, Yutaka Matsubara, Hiroaki Takada

ねらい　組込み業界において，今までシステム対する安全分析やセキュリティ分析の手法がたくさん提案されているが，セキュリティの脅威（第３者による意図的な攻撃）を網羅的に列挙する手法はまだ明確ではないということは現状である。そこで，我々は安全分析手法である HAZOP の考え方を移植して，HAZOP ベースなセキュリティ分析手法を提案して，この手法をいかに活用して組込みシステムの脆弱性が発見できるかについて研究で取り込んでいる。そして，Open Source Immobilizer Protocol Stack[1]を分析対象としてケーススダディを行って，手法の適切性や有用性を検証した。

キーワード　安全分析，セキュリティ分析，HAZOP，オープンソースイモビライザプロトコルスタック

Target: Nowadays, with the introduction of network connectivity both inside and outside modern vehicles, researchers have identified that the system is actually fragile if an attacker could locate any security vulnerabilities of the system. Although security analysis techniques prospered in the industry, still a general, exhaustive and effective one remains uncertain. Our research aims to transplant the safety analysis technique HAZOP into an appropriate security analysis technique. By conducting a case study of security analysis for Open Source Immobilizer Protocol Stack [1], we have been able to demonstrate the applicability as well as usability of the proposed technique and also realized that there are still unresolved issues which require further discussions.

Keywords: Safety Analysis, Security Analysis, HAZOP, Open Source Immobilizer Protocol Stack

１．想定する読者・聴衆

Our research caters to crowds who are involved within the work of designing embedded systems. Up until now, although security analysis techniques prospered in the industry, there is still not a general, exhaustive and effective technique for identifying security vulnerabilities within embedded systems. Therefore, it will be a privilege for us to be able to provide a probable solution to those who are engaged as system designers, in order to help them eliminate security vulnerabilities as much as possible during the architecture design phase of a safety-critical embedded system.

2．背景

Certain techniques, such as Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA), have been provided to the industry for conducting a comprehensive safety analysis. However, with the debut of network connections for embedded systems, highly digitalized modern machineries are exposed to information attacks via all kinds of unauthorized network connection, which enlightened the research and development of security analysis. When designing an embedded system (Flow showing in Figure 1),

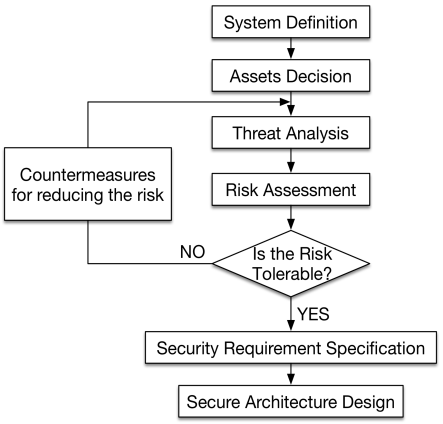

図 1　組込みシステムの設計フロー

Figure 1. Flow: Designing an embedded system

there is a practical engineering approach suggesting to firstly decide significant assets that require proper protection. [2] After determining which asset to protect, we set the asset as the analysis object to conduct a threat analysis. Threats detected are then evaluated by conducting a risk assessment in order to decide whether or not such risk is tolerable, and whether or not further countermeasures are required in order to eliminate such risk.

3．課題

[†]名古屋大学大学院情報科学科
E-mail: {jx_wei, yutaka, hiro}@ertl.jp

Now that, security problems have become a general concern when developing an embedded system, and certain techniques that assist system designers to perform a security analysis have also been introduced to the industry. Attack Tree, for example, can be used for representing attacks against a system. However, such analysis technique relies heavily on the related experience of the analyzer, and may not be a suitable choice for people, who are still not quite familiar with security concerns. Same issue happens to other security analysis techniques such as STPA-Sec and SafSec, which also mainly focuses on the security analysis of modularized avionics production. Therefore, the application of automobile embedded system software still remains unclear.

On the other hand, safety analysis technique HAZOP, takes up a whole new viewpoint neither from the reasons causing any system failure proposed in FMEA, nor the supposed consequences of any system faults proposed in FTA. Yet, it takes the execution flow as the analysis object during a simulation of the system's running. We believe that such approach will be proper not only for a safety analysis, but also required for an exhaustive security analysis.

4. 提案・実験

Since the original HAZOP guidewords are considered as not suitable for analyzing software functionalities, we firstly changed those guidewords into 8 actions (Shown in Table 1) extracted from the attack taxonomy of the taxonomy Computer Emergency Response Team (CERT) [3]. With the new guidewords, we examine the given system architecture and uncover the security vulnerabilities from the system design.

During the threat analysis, applying the guidewords to the given system architecture will help us to find out deviations (unexpected functionality, unwanted connection, etc.) of the system. To consider the causes and the consequences of certain deviation, we discuss about certain deviation's local effects (affecting system's normal functionality) as well as the global effects (keeping the user from using the system properly). On summarizing all the analysis result entries into one overall table, we also issue a severity value to each of the result entry in order to conduct a risk evaluation and argue about whether or not further precautions should be implemented during the system design.

In order to demonstrate the usability, we have also conducted a case study taking Open Source Immobilizer Protocol as the analysis object. Please refer to our paper [4] listed at 文献 section for more details of the case study.

表 1　新しいガイドワードの解釈

Table 1. Meaning of the new Guidewords

Guideword	Meaning
PROBE	Access a target in order to determine its characteristics
SCAN	Access a set of targets sequentially in order to identify which targets have a specific charateristic
FLOOD	Access a target repeatedly in order to overload the targets capacity
AUTHENT-ICATE	Present an identity of someone to a process and, if required, verify that identity, in order to access a target
SPOOF	Masquerade by assuming the appearance of a different entity in network communications
BYPASS	Avoid a process by using an alternative technique to access a target
MODIFY	Chage the content or characteristics of a target
READ	Obtain the content of data in a storage device, or other data medium

5. 効果

We are thrilled to see that, at the end of our case study, when comparing to the possible attacks reported in [7], in which the security issues include (not limited to) relay attack with genuine key fob, tracking, denial-of-service attacks, replay attack on authentication, spoofing attack on memory access protection, and hijacking communication sessions, we were able to find most of attacks. We think that our analysis results imply the effectiveness and applicability of our proposed technique for conducting security analysis.

6. まとめ(今後の課題・謝辞等)

Our research presented a HAZOP-based security analysis technique to perform an exhaustive security analysis during the system design. Although this HAZOP-based technique did succeed in locating some of the security flaws, still, a large amount of arguments and issues remain, in order to make this method become much better and more suitable to general purposes. As for the future works, we plan to address these issues with further discussion of this HAZOP-based security analysis technique.

7. 用語・文献

文　　献

[1] Atmel, "Open Source Immobilizer Protocol Stack", Available online:http://www.atmel.com/tools/opensourceimmobilizerprotocolstack.aspx, 2015.

[2] 松並勝, ソニーの電子お薬手帳システムに適用したセキュリティ設計分析手法, 12th WOCS[2], Jan, 2015

[3] R.R. Brooks, and others, "Automobile Security Concerns, Challenges and State of the Art of Automotive System Security", IEEE Vehicular Technology Magazine, June 2009.

[4] 魏靖軒, 松原豊, 高田広章, HAZOP-based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack, ECAI 2015, Jun, 2015