氏　　名	Ooi Sian En
学位の種類	博士（情報科学）
学位記番号	博情第 498 号
学位授与年月日	令和 5 年 3 月 24 日
論文題目	Automated Secure Design of Networked Systems
論文審査委員	BEURAN, Razvan Florin　JAIST　准教授
	丹 康雄　同　教授
	篠田 陽一　同　教授
	リム 勇仁　同　准教授
	黒田 貴之　日本電気株式会社　主任研究員

論文の内容の要旨

The trend of Digital Transformation (DX) to modernize the society introduces various ICT challenges. DX ICT often requires a high frequency of change and emphasises speed, flexibility and efficiency, which as a result, requires an agile system delivery method. Conventionally, systems are manually designed based on tacit and explicit knowledge of the system designer. While manual design may work for small or relatively simple systems, the tractability of a system is quickly lost for systems of systems, which are common in Society 5.0. The challenges are even greater when considering securing the system, especially when frequent changes require the reassessment of the system's security to ensure that those changes did not degrade the security of the intended system.

This research aims to improve the security of a system by introducing an automated verification of the security characteristics of a system into fundamental system design. An automated secure design framework, SecureWeaver, was proposed and implemented, which consists of contributions such as a knowledge base for secure design and security verification algorithms to verify the generated design. In addition, case studies on IoT applications, such as end-to-end communication and secure configuration implementation were carried out. The results of the case studies were also used as the motivating evaluations for SecureWeaver. A set of models for IT/NW and IoT system design were developed to evaluate SecureWeaver, which cover scenarios such as typical corporate network, IoT appliances, and also hardware-level system design in an automated and secure manner.

The evaluation showed that SecureWeaver is able to generate a system design that mitigates the security threats present in the input requirements via the automatic placement of security-based components in the system design. The performance characteristics of SecureWeaver also demonstrated that the security verification overhead compared to the total system design time is largest for simple scenarios, for which the actual design is very fast, still being just 0.58% in such a case. The expected impact of this dissertation is to decrease the human effort in system design via automatically designing secure systems by using the proposed framework. This formalized design approach will also add to the knowledge field in automatic system design.

Keywords: networked systems, secure system design, automated design, design space exploration, MITRE ATT&CK

論文審査の結果の要旨

The dissertation of Mr. Ooi Sian En deals with the important topic of how to automate the secure design of networked systems. Secure design is mandatory in the modern “security by design” approach that is needed to counter the increasing number of cybersecurity threats, and automating this design is mandatory to make sure that complex networked systems can be designed in an error-free and efficient manner.

Mr. Ooi outlined the need for an automated secure design methodology and implemented it as the automated secure design framework SecureWeaver. The implementation was based on the Weaver system designer developed by NEC Corp., adding to it secure design features via a secure design database and a security verification mechanism. The database leverages the MITRE ATT&CK framework that is widely used for threat analysis and uses it as foundation to create the corresponding design refinement rules, a threat mitigation knowledge base, as well as a secure protocol database. The verification mechanism is based on a set of security verification functions that ensure a given system design is secure in the sense that the necessary mitigations have been applied to eliminate the security threats.

In addition to developing the SecureWeaver framework, Mr. Ooi conducted several case studies to analyze the mechanisms needed to implement secure end-to-end communication and to improve overall security via the hardware security features of IoT systems, demonstrating the limitations of current approaches and emphasizing the need for the automated secure system design approach proposed in his dissertation.

The evaluation of the SecureWeaver framework demonstrated the feasibility and soundness of the methodology via three case studies in which all the verification functions were tested. Furthermore, the effect of introducing the security verification mechanism on system design performance was shown to be minimal, being up to 0.58% for the smallest scenarios and much lower than that for larger scenarios. In addition, the extension of the framework for the domain of IoT systems and end-to-end applications was evaluated and proved to function correctly as well. Lastly, the comparison with related works showed the advantages of the proposed approach in terms of capabilities, target domains, and threat mitigation mechanisms.

The work of Mr. Ooi has been presented in a top-level journal in the field of security (Elsevier Computers & Security, IF 5.105), as well as in three peer-reviewed international conference papers, which demonstrates both the validity of his results and his high-level English language skills.

Based on the above considerations, we conclude that this is an excellent dissertation, and we approve awarding the doctoral degree to Mr. Ooi Sian En.