Title	
Author(s)	OOI SIAN EN
Citation	
Issue Date	2023-03
Type	Thesis or Dissertation
Text version	ETD
URL	http://hdl.handle.net/10119/18424
Rights	
Description	Supervisor: BEURAN, Razvan Florin, ,

Automated Secure Design of Networked Systems

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.