Politecnico di Torino

ScuDo
Scuola di Dottorato - Doctoral School
WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation
Doctoral Program in Computer and Systems Engineering (36thcycle)

Vulnerability-Tolerant Architectures for IoT Devices

By

Vahid Eftekhari Moghadam

******

Supervisor(s):
Prof. Paolo Prinetto, Supervisor

Doctoral Examination Committee:
Prof. Tiziana Margaria, Referee, University of Limerick
Prof. Liviu Miclea, Referee, Universitatea Tehnică din Cluj-Napoca

Politecnico di Torino
2024

Declaration

I hereby declare that, the contents and organization of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.

Vahid Eftekhari Moghadam
2024

* This dissertation is presented in partial fulfillment of the requirements for **Ph.D. degree** in the Graduate School of Politecnico di Torino (ScuDo).

Vulnerability-Tolerant Architectures for IoT Devices

The widespread utilization of the Internet of Things (IoT) and its consequential societal impact necessitates a rigorous focus on data protection and information security. The heterogeneous nature and complex design of IoT infrastructure, spanning from big cloud servers to small edge computing devices, consistently expose these systems to a range of security and privacy concerns.

Embedded systems, positioned at the heart of IoT, constitute a foundational aspect of contemporary interconnected infrastructures, from industrial control mechanisms to everyday consumer gadgets. These systems, purposely engineered for precise functionalities, are often integrated into networks or interfaced with diverse devices, thereby enabling seamless data transmission and command execution. However, this increased interconnectedness also increases the risk of security vulnerabilities.

With the increasing amount of data volumes and functionalities within interconnected systems, there is a crucial need for scientific research into the methodologies for safeguarding the security and privacy of information, as well as the safety and reliability of operations. Despite considerable advancements in securing general-purpose devices, there remains a big open question concerning the protection of special-purpose embedded systems and their trustworthiness.

The emphasis on optimization often leads to the utilization of low-level languages like C and C++ in embedded systems. However, these languages are susceptible to memory-unsafe practices, resulting in common programming errors and vulnerabilities such as buffer overflows, memory corruption, and code injection. These vulnerabilities enable attackers to manipulate data and program execution, posing significant threats in the form of binary attacks.

Moreover, numerous solutions tailored for general-purpose domains are incompatible with embedded systems due to their unique characteristics. Consequently, this raises questions about the effectiveness of security testing for such devices.

Testing embedded software presents distinct challenges, mainly due to hardware reliance and limited physical access, particularly during early testing phases. The absence of standardization in embedded software systems further complicates security measures.

Another critical concern revolves around strengthening embedded communication protocols, which are essential pathways enabling inter-device data exchange. However, the inherent vulnerabilities of these protocols expose systems to numerous attack vectors, permitting unauthorized access, data manipulation, or communication disruption. Recognizing this threat, the National Institute of Standards and Technology (NIST) has issued comprehensive guidelines advocating robust security measures. These guidelines stress the importance of fortified design principles, including encryption, authentication mechanisms, and careful communication protocols, to bolster the resilience of embedded systems against malicious intrusions.

In this study, we aim to propose an architectural solution encompassing the security of IoT devices both in isolation and in networks, introducing a novel security-enhanced communication framework tailored explicitly for embedded systems. By abstracting the intricacies of specific communication protocols, this framework serves as a safeguarding mechanism against potential vulnerabilities, particularly within mission-critical or safety-critical domains. An illustrative implementation of this framework underscores its efficacy as a reference model for fortified communication in embedded systems.

Furthermore, addressing vulnerability discovery and tolerance in embedded IoT devices, we advocate for three main solutions: (i) security benchmarking tool tailored for embedded applications to enable comprehensive security analysis and resilience (ii) a holistic security framework for inter-device communication that tackles the specific challenges associated with device interactions within IoT systems (iii) an experimental secure design approach implementing Control-Flow Integrity (CFI) to maintain data and code integrity.