Microprocessors and Microsystems 41 (2016) 29–36

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Multi-dimensional analysis of embedded systems security

Haytham Elmiligi[a], Fayez Gebali[b], M. Watheq El-Kharashi[c,*]

[a] Computing Science Department, Thompson Rivers University, Kamloops, Canada
[b] Electrical and Computer Engineering Department, University of Victoria, Victoria, Canada
[c] Computer & Systems Engineering Department, Ain Shams University, Cairo 11517, Egypt

ARTICLE INFO

Keywords:
Common Criteria (CC)
Cryptographic Module Validation Program (CMVP)
Embedded systems security
FIPS 140-2
Reverse engineering
Side-channel attacks

ABSTRACT

The primary goals of this paper are to analyze the security of embedded systems at different levels of abstraction and to propose a new procedure to assess and improve the security of embedded systems during various product life cycle phases. To achieve these goals, this paper introduces new classification of embedded systems attacks using a novel multi-dimensional representation, explores the possible threats to embedded systems, and proposes a new procedure to evaluate and improve the security of embedded systems during various product development phases.

1. Introduction

Embedded systems are widely used in many fields, yet current work on embedded systems security considers only simple physical attacks against the hardware itself and straightforward software defenses. This has raised serious concerns regarding possible threats to military systems, financial infrastructures, and even household consumer appliances. In fact, security professionals concluded that the failure of military devices in different incidents was due to electronic warfare. In particular, Trojans were added to ICs used in suspected military equipments to shut them down at certain times [1]. Even at the regular consumer level, electronic devices, such as cell phones, are currently being integrated into enterprises, government agencies, and even in the military [2]. These devices hold valuable and sensitive contents and thus face the same risk of being attacked on a daily basis [2].

The problem with current straightforward software defenses in most systems is that hardware is the base physical layer in any embedded system and an attack on that layer can allow a full control over the software running above. This low-level control enables sophisticated attacks that can defeat regular software-based defenses [1].

Attacks on embedded systems can have different forms, such as theft of service, cloning, spoofing, and reverse engineering. In this paper, we categorize the possible attacks on embedded systems and visualize the different types of attacks using a multi-dimensional analysis. Based on our analysis, we introduce a new methodological security evaluation scheme to help designers better evaluate the security of their designs.

1.1. Main contributions

This paper presents two main contributions:

1. Creating a new classification of embedded systems attacks using a novel multi-dimensional representation. This new classification allows system designers to study the security of their embedded systems at 27 different scenarios.
2. Developing a new methodological security evaluation scheme to assess and improve the security of embedded systems during various product life cycle phases. This new scheme identifies the requirements of four security levels and is complementary to other methods, such as the Cryptographic Module Validation Program (CMVP) and Common Criteria (CC) [3,4].

This paper is organized as follows. Section 2 reviews existing security standards. Section 3 highlights related work. Section 4 introduces a new systematic classification of implementation-oriented attacks on embedded systems and presents three main perspectives that could be used to classify attacks on embedded systems. Section 5 discusses our proposed procedure to evaluate the security of embedded systems. A case study is presented in Section 6. Section 7 evaluates the proposed approach and compares it to related work. Finally, we draw our conclusion and suggest new ideas for future work in Section 8.

2. Review of existing security standards

Cryptographic Module Validation Program (CMVP) was established by the National Institute of Standards and Technology (NIST)

* Corresponding author.
E-mail address: watheq.elkharashi@eng.asu.edu.eg (M.W. El-Kharashi).

http://dx.doi.org/10.1016/j.micpro.2015.12.005
0141-9331/

and Communications Security Establishment Canada (CSEC) in 1995 [3]. CMVP validates commercial cryptographic modules to the Federal Information Processing Standard (FIPS) 140-2 and other cryptography-based standards. On the same context, Common Criteria (CC) lists seven Evaluation Assurance Levels (EALs) [4].

2.1. Review of CMVP and FIPS 140-2

In 2005, NIST and CSEC identified four security levels for cryptographic modules to protect sensitive information in computer and telecommunication systems [3]. The first security level requires minimal physical protection and no specific physical security mechanisms are required beyond the requirement for production-grade components [3]. The second security level adds the requirement for tamper-evident mechanisms, which includes the use of tamper-evident coatings or seals on removable covers of the module [3]. The third security level intends to have a high probability of detecting and responding to attempts at physical access, use, or modification of the cryptographic module [3]. The fourth security level provides the highest level of security defined in the FIPS 140-2 standard. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module. This includes protecting a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature [3].

2.2. Review of CC

CC is another security scheme that identifies seven Evaluation Assurance Levels (EVLs). EAL-1 provides a basic level of assurance just to make sure that the Target of Evaluation (TOE) is consistent with its specifications [4]. EAL-2 requires developer testing, a vulnerability analysis, and independent testing based upon more detailed TOE specifications. EAL-3 requires more complete test coverage of the security functionality to make sure that the TOE will not be tampered with during development. EAL-4 adds the requirement for more design description, the implementation representation for the entire TOE Security Functions (TSF), and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development. EAL-5 requires semiformal design descriptions, a more structured architecture, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development. EAL-6 requires more comprehensive analysis, a structured representation of the implementation, more architectural structure, more comprehensive independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential. EAL-7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs.

2.3. Limitations of CMVP/FIPS 140-2 and CC

Although CMVP and FIPS 140-2 provide an essential standard that helps protecting sensitive information in computer and telecommunication systems, they focus on the cryptographic modules and do not cover the complete system, including hardware modules. The cryptographic modules considered by the standard are assumed to be completely secured and inherently free from any malicious content. Furthermore, the existing standard does not provide security measures to assess and classify threats during various development phases, programmability levels, or integration levels.

On the same context, the US National Institute of Standards and Technology (NIST) has proposed using the CC and system-level protection profiles (SLPPs) to specify security requirements in large systems [4]. CC is widely used by software vendors, biometric system designers and smart-card application-developers. A substantial research and practical experiences exist for the CC, such as framework development [5], vulnerability awareness improvement [6], and structuring modular safety software certification by using CC concepts [7]. However, attempts to apply CC policies in the USA federal systems engineering environment faced three specific issues that made it difficult to implement CC. These issues, listed by Keblawi and Sullivanet in [8], are: (1) complex technology environments, (2) complex and inflexible standards, and (3) the lack of a clear relationship between the CC and the systems development approach.

Because of these issues, and many others, some independent consultants started to question the future of the CC. Hearn listed the following three specific key observations in [9], based on the 4th International CC Conference:

1. Little commercial interest is driving the CC market; most evaluations and certifications result from government regulations or purchases.
2. Buyers see certifications as a "tick in the box" for procurement and seldom read the security target or certification reports, or even use the evaluated configurations.
3. Sellers do not see CC as a product-improvement evaluation methodology.

After complying with the CC requirements, many users still wonder how this CC-evaluated product improves their IT systems security [9]. Specific for hardware systems, CC does not provide a clear implementation of the requirements. Furthermore, CC focuses on the development phase of the product and is missing the possible attacks during and after the production phase.

Therefore, in this paper, we develop a new multi-dimensional scheme to address these missing issues and provide a complementary vision to existing hardware security requirements in both CMVP and FIPS 140-2, as well as CC.

3. Related work

This section highlights related work in embedded systems security. The work published in this area can be classified into three categories: (1) modeling and analyzing hardware attacks and security requirements, (2) providing solutions for the security of embedded memories and supporting on-chip secure communications, and (3) managing security requirements in system-on-chip (SoC) and FPGA-based designs.

3.1. Modeling and analyzing hardware attacks and security requirements

Analyzing attacks and evaluating systems' security are becoming more challenging with the increasing complexity of integrated circuits (ICs) [10]. Companies tend to outsource several parts of their designs and integrate third-party IPs to achieve cost efficiency and fast time-to-market. Because of the lack of enforcing a common standard for hardware security in the IC industry, researchers made several attempts to standardize the security requirements for embedded systems. Rostami et al. presented a classification of several hardware threat models and discussed possible evaluation metrics for important hardware-based attacks [11]. Koppel et al. analyzed the Hardware Security Modules (HSM) high availability settings and discussed two possible flaws that could lead to security problems [12]. The authors also discussed possible solutions that could be applied by targeted organizations. At a higher level, Lee discussed two classes of hardware security: an architecture for hardware-enhanced security and a secure hardware platform [13].