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].

The author also presented the Secret-Protected (SP) architecture, which is a minimalist set of hardware features that can be added to processors in embedded systems to protect keys, encrypted information, programs, and data [13].

3.2. Providing solutions for the security of embedded memories and supporting on-chip secure communication

Memories are at the heart of any embedded system and the center of information storage. Protecting memories is one of the main goals for any system security requirement. Researches proposed several solutions to address memory issues. Venkataramani et al. developed MemTracker, a new hardware mechanism that can be configured by developers to perform several tasks related to memory access monitoring [14]. The main idea of MemTracker is associating memory words with few bits that represent several states [14]. Then, the system monitors the memory access and logs any event that can affect the current state. A programmable state transition table is used to switch to the next state after detecting the event [14]. At the silicon level, Tiwari et al. proposed a replacement to the classical memory elements, called NOVeA [15]. NOVeA uses a scalable embedded flash technology with an integrated on-chip SRAM array to facilitate password authentication [15]. A different approach proposed by Iyengar et al. is to utilize a physics-based model of the domain wall memory (DMW) to comprehend the process variations and use physically unclonable functions (PUFs) to secure the key generation process [16]. PUFs are preferred to be used, especially relay-PUF and memory-PUF designs, as they could provide a higher degree of resilience against reverse engineering [16–18].

At the micro-architecture level, researchers addressed covert timing channels through different approaches. In [19], Chen and Venkataramani presented CC-Hunter, which is a framework that allows users to detect the possible presence of covert timing channels. This is done by developing an algorithm to analyze conflict patterns used in covert transmission. With a focus on contention-based covert timing channels, the algorithm presented by Chen and Venkataramani was discussed in more details in [20]. The proposed work was evaluated using covert timing channels on wires, logic, and memories [19,20].

Another approach was taken by Liu and Lee [21,22]. They first introduced a new classification of cache side-channel attacks in [21]. This classification considers two main types: contention-based attacks and reuse-based attacks. Following that, they presented a new methodology to launch a successful side-channel attack against the last level cache in [22]. The attack utilized two techniques developed by the authors to enable a Prime + Probe attack [22]. The achievable bandwidth was 1.2 Mbps and they also demonstrated the attack on the sliding-window modular exponentiation implementation of ElGamal in the latest GnuPG version [22]. The authors extended their work to the smartphone technology and presented a new multi-sensor authentication mechanism to improve smartphone security in [23]. In [23], authors designed an adaptive system that continuously learns the user's behavior and creates a profile to identify users based on users' patterns [23].

3.3. Managing security requirements in SoC and FPGA-based designs

The emerging utilization of system-on-chip (SoC) and networks-on-chip (NoC) designs in current embedded systems comes with high risk of systems' failures due to hardware-based attacks. Researchers proposed different solutions to address the security issues in current emerging technologies. Kim et al. explored different methods to recover systems from hardware attacks by changing the configuration and mode of operations [24]. They proposed architectural features of SoC that can minimize the impact of hardware attacks and provide seamless system operation during and after function replacement [24]. Tiwari et al. presented a new approach for microkernel, processor, and I/O system with strict and provable information flow security [25]. Their main idea is constructing a configurable architectural skeleton that couples the microkernel with low level hardware implementation. This integration allows information flow properties of the entire construction to be captured and statically verified from the system level all the way down to the gate-level implementation [25]. Several work was done also to address security issues in NoC and FPGA applications. Wassel et al. introduced SurfNoC, an on-chip network that improves the security of on-chip communication [26]. Swierczynski et al. investigated a possible attack vector against cryptography. They demonstrated how attackers could modify an FPGA bitstream to break cryptographic algorithms and discussed possible solutions to countermeasure these attacks [27].

Although a lot of research has been done in this area, system designers need a new classification of embedded systems attacks that takes into consideration the whole system perspective. It is also clear that there is a great need for a standard methodological security evaluation scheme to assess and improve the security of embedded systems during various product life cycle phases. Our work in this paper addresses these two issues.

4. Classifications of attacks on embedded systems

Fig. 1 shows a multi-dimensional representation of embedded systems that could be used to visualize possible attacks from different perspectives. We developed this figure to help engineers better understand the possible threats to their applications at each integration level, taking into consideration the programmability level and the product life cycle phase. For each level of integration, designers must (1) explore all possible threats to the target design based on the other two dimensions and then (2) apply the required security measures to protect the target design against these threats.

There are many different ways to classify attacks on embedded systems [28]. In this paper, we present three main perspectives that could be used to classify attacks on embedded systems. These perspectives are: programmability level, integration level, and life cycle phase.

Other dimensions could also be added to the representation in Fig. 1, e.g., controllability and observability. However, we found the three dimensions, shown in Fig. 1, better represent embedded systems from the architectural and life cycle perspectives, whereas controllability and observability could not be used to visualize the possible security threats of embedded systems at the same level of abstraction. We selected the dimensions of our representation based on their significance to quantify the overall security of the different embedded systems, while being reasonably practical to be considered by designers and manufacturers.

4.1. Classification based on programmability level

4.1.1. Hardware (HW) attacks

Hardware (HW) attacks include hijacking, data monitoring, and denial-of-service attacks that prevent the system from functioning correctly after being triggered by a predetermined input sequence [29]. Hardware attacks also include physical attacks, such as reverse engineering of a chip or a printed circuit board (PCB) and using probes to monitor inter-component communications. Another type of hardware attacks is hardware Trojan, which is a malicious addition or modification to a hardware circuit to change its functionality [29].

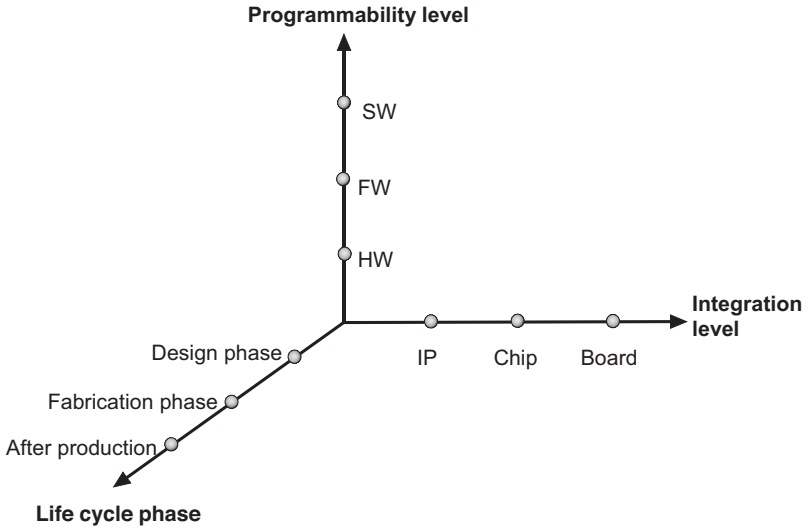

Fig. 1. A multi-dimensional representation of embedded systems.

Hardware-based side-channel attacks rely on monitoring the physical behavior of the system. This can be done by monitoring the voltage level, electromagnetic radiation, and data traffic between chips. It can also be done by adding a malicious circuit to facilitate the observation process [30].

4.1.2. Firmware (FW) attacks

Firmware attacks include attacks against the OS kernel, as demonstrated in [31]. While firmware in ROMs and EPROMs are not usually updated by the customer, EEPROMs or flash memories can be re-written from software. Embedded systems currently store the firmware code, in most cases, in flash memories to allow OS upgrades through any Internet connection. Although in-field updates ease system upgrades, they open the door to bypassing security features and could result in illegal privilege escalation.

4.1.3. Software (SW) attacks

Software attacks are usually designed to alter the behavior of the system, such as viruses, software Trojans, etc. Software attacks could also target the packet switching protocols and could result in a malicious behavior, e.g., packet replay, unknown destination, or deadlock. One of the common software attacks is the buffer overflow, which causes serious damages to application-specific embedded systems [32]. Some of the software attacks on microcontrollers aim at either exploiting vulnerabilities that are not malicious themselves or executing malicious code. On the other hand, software-based side-channel attacks rely on monitoring the logical behavior of the system. This can be done by monitoring the data traffic and extracting confidential information or by adding a malicious code to facilitate the observation process.

4.2. Classification based on integration level

4.2.1. Intellectual property (IP)-level attacks

There are three types of IPs: soft, firm, and hard IPs [29]. Each type of IPs is vulnerable to various attacks. A soft IP is subject to modifying the source code so that hackers can fully control the whole system later on. A firm IP is subject to connecting malicious IPs to its IO interfaces so that hackers can affect data integrity and cause silent data corruption. A hard IP is subject to cloning during and after the fabrication process. Attacks on IP cores also include adding Trojan circuits to try to do attacks at specific times or after specific sequence of events.

4.2.2. Chip-level attacks

Chip level attacks include chip cloning using advanced imaging techniques and fault attacks, which is the new class of attacks on secure microcontrollers [33]. Another type of attacks is changing the mode of operation based on the geographical location, time zone, time of the day, day of the year, etc. This includes remote shutting down, remote utilization, remote reconfiguration, etc. There are also other types of attacks related to programmable logic designs, e.g., those related to FPGA-based designs. These attacks include bitstream reverse engineering, radiation-induced faults, and illegal remote reconfiguration [34].

4.2.3. Board-level attacks

Board level attacks can be categorized into three main groups: invasive, semi-invasive, and non-invasive attacks [35]. Invasive attacks require physical access to the board to reverse engineer the design layout. Hackers use mechanical, chemical, and image processing techniques to copy and reproduce the PCB layout design layer-by-layer. Semi-invasive attacks work only for simple, double-sided PCBs, as hackers use photo scanners to scan the top and bottom layers, then convert the scanned image pixel-format into a vector-format that could be read by CAD tools. Non-invasive attacks can be either passive or active [29]. Passive attacks do not interact with the board and just monitor or observe the data traffic between different chips, whereas active attacks tend to play with the supply voltage and clock signals to disable the board protection or force a chip to do a wrong operation.

4.3. Classification based on life cycle phase

4.3.1. Design phase attacks

Attacks during the design phase are usually executed by an insider. Insider threats are among the most significant security breaches because the attacker can gain access to protected information, which could result in destruction or cloning of a design, fault generation, spoofing, adding a kill switch, or gaining illegal access to the target system at any time in the future [36]. One way to address these attacks is by using processor encryption to ensure that an insider cannot activate any Trojans inserted at the design phase [37].

4.3.2. Fabrication phase attacks

Attacks during the fabrication phase are usually related to market competition. During the fabrication phase, an attacker can try

to reverse engineer or copy a specific IP, a chip, or a aboard from the owner with a primary goal of gaining an advantage in the marketplace [38].

4.3.3. After-production attacks

After-production attacks happen when the design, whether it is an IP, a chip, or a board, is released to the market and it is already in the customer hands. Attacks, in this case, can be either a physical attack aiming at cloning the design, achieving privilege escalation, or extracting confidential information; or a remote attack through online updates to firmware and software applications [39].

5. A procedure to evaluate the security of embedded systems

As each axis in Fig. 1 is divided into 3 points, designers can study the security of their embedded systems at 27 different points.

5.1. Attack examples

To give concrete examples of different types of attacks that belong to the 27-point classification, we present the following three examples.

1. Example 1: *A SW attack that operates on a chip level during the design phase.* At early design phases of a SoC-based product that requires a SW-HW co-design, an insider developer can add a malicious SW that runs on a SW-HW Co-design framework to shut the system down, delete sensitive information, or store and transmit RAM contents when triggered by a unique external signal. This type of attacks is sometimes classified as a *Kill-Switch* and it is a SW attack that starts during the design phase and targets a chip level execution. One real case was presented by Adee in [1].
2. Example 2: *A FW attack that operates on an IP level during the fabrication phase.* With the current trend of IC design companies being fabless and outsourcing fabrication to various semiconductor manufacturing companies, IPs are becoming more vulnerable to reliability attacks. Reliability attacks are induced in the offshore fab house during the fabrication phase to modify the original firmware or chip design. Due to budget limitations, managers might consider one-time programmable (OTP) memories and ship their FW that works on a certain IP to the fab house to integrate the firmware programming in the fabrication process in order to save the cost. This can also introduce a great risk of man-in-the-middle attacks after the product is shipped to end users.
3. Example 3: *A HW attack that operates at the board level after-production.* One example is the PCB reverse engineering. Various techniques to attack PCBs have been reported, including using X-ray stereo imaging to separate the layers of two layered PCB [40]. Our classification helps system designers consider PCB protection methods at early phases of the design to eliminate after-production attacks.

These examples demonstrate the strength of our 3-D classification system and help explain how attacks could be mapped to each one of the 27 points.

5.2. Evaluation procedure

To improve a system's immunity to possible threats, the target system must be protected at all levels. To achieve this goal, the following evaluation procedure is suggested.

1. Using Fig. 1, create a list of 27 scenarios, representing all possible threats to the target system in each scenario. An example of the list of all 27 scenarios is presented and discussed in Section 6 to show how these 27 points should be evaluated.
2. For each the 27 possible scenarios, indicate whether the system is protected against the possible attacks or not and assign a severity level for each corresponding attack.
3. The security of the system is as strong as the weakest protected point.

To simplify this procedure, each one of the 27 scenarios can be assigned one of four security levels. The following subsection introduces these security levels.

5.3. Security levels

Since security requirements depend on the target system and application, we introduce, for the first time, four security levels for embedded systems. The proposed levels consider a layered approach of multiple security mechanisms to protect against a specific threat or to reduce a vulnerability. This proposal aims to apply security measures during product design and to treat security as an integral part of the overall system design.

5.3.1. Security level 1: basic security

Security level 1 is the basic acceptable level for any embedded system. It requires that designers use tamper-resistance mechanisms to make tampering of an IP, a chip, or a board very difficult. For example, encapsulating the entire PCB with resistant epoxy compound will help protect the circuitry. Designers can hide the PCB tracks in the inner layers and move the power polygons to the top and bottom layers, as opposed to exposing the tracks to the surface of the board. Another example is using an embedded component technology, such as buried resistors and capacitors in the internal PCB layers. At the chip level, designers can employ security measures to prevent attackers from reading stored data, such as using physical fuses on ROMs, boot-block protection in flash memories, and lock bits in microcontrollers.

5.3.2. Security level 2: intermediate security

Security level 2 requires applying all security measures in level 1 plus adding two more features. The first feature is detecting any internal malicious behaviors that prevent the system from functioning correctly. This includes access control by employing authentication techniques, IP profiling and monitoring during different modes of operation, testing all third-party design modules to make sure that no Trojans are hidden inside. The second feature is protecting the design against attacks during the fabrication phase, including hardware obfuscation, watermarking, secret key activation, custom-generated boot-loaders, and other techniques to prevent overproduction and reverse engineering during the fabrication phase.

5.3.3. Security level 3: high security

Security level 3 requires that designers apply all security measures in level 2 plus adding more features for tamper evidence, detection, and response. Tamper evidence and detection mechanisms allow a system to be aware of tampering and ensure that a visible evidence is left behind when tampering occurs. The detection can be done using microswitches, sensors, or other circuitry for hardware devices. For software modules, this can be done using firewalls and authentication methods. Once an attack is detected, tamper response varies according to the target system. For example, the system can respond by completely shutting down or disabling itself, or erasing all memory units to prevent an attacker from accessing secret data, etc. Actions in level 3 do not include any physical destruction of the system.

5.3.4. Security level 4: advanced security

Security level 4 prevent attackers from gaining access in any way, shape, or form to any part of the system. In addition to all security measures in level 3, level 4 allows physical destruction of a system using a small explosive charge to completely prevent any access to the system once an illegal attempt is detected.

These four presented security levels are based on the 27 scenarios presented in Fig. 1. To consider systems' security at early design phases, design tools should accommodate security-plugin-features to evaluate the probability of successful hacking for different implementations.

6. A case study

This section explains how to use the scheme proposed in Section 5 to evaluate the security of embedded systems. We study a simple control board and evaluate its security level based on the requirements discussed before.

6.1. System description

The target embedded system is a simple control board that has an embedded processor and several other peripherals mounted on a multi-layered PCB. A daughter-board is used for sensor interfaces. The packages of all chips are chosen to be surface mounted and all passive components are buried in the internal layers. Commercial chips are used and no IP/Chip design is done internally. All PCB tracks are placed in inner layers, the entire PCB is encapsulated with resistant epoxy compound, and all memory components are locked to prevent unauthorized read/write and shipped with the firmware to the assembly house. The system is designed to respond to any attempt to read the firmware by any module other than the processor by erasing all memory units to prevent an attacker from accessing secret data. Source code encryption and version control are enforced during the design phase to prevent insider attacks and system activation is required on the first power-up to prevent illegal overproduction. The PCB of the main board and the daughter-board are manufactured at two different houses.

6.2. Evaluation of the system security

To evaluate the security of this system, we first need to analyze all security measures implemented in the system based on our multi-dimensional representation of embedded systems in Fig. 1. Following that, we consider each one of the 27 points discussed in Section 5 and associate a security level to it, if applicable. Table 1 summarizes our findings for the target system. We can justify the security level associated with each one of the 27 points as follows.

- As stated in the system description of this case study, commercial chips are used and no IP/Chip design is done internally. Therefore, security requirements to protect the internal IPs are out of scope for this specific case. IP integration fields are marked **x** throughout the life cycle of the system. The same rule applies for chip hardware design at the design phase.
- According to the system description, the used chips did not have any associated software components and there is no common software/firmware at the board level. Therefore, chip software, board software, and board firmware components are out of scope for this specific case and all related fields are marked with **x**.
- At the design phase, source code encryption and version control are enforced during the design phase to prevent insider attacks. This satisfies the first requirement of the second security level for firmware chip design and board hardware design as tamper-resistance and detection mechanisms were enforced during the design phase. The second requirement is met by implementing system activation upon first power-up. Therefore, chip firmware and board hardware security levels are set to *level 2* for the design phase.
- In the fabrication phase, all memory components are locked to prevent unauthorized read/write and shipped with the firmware to the assembly house, which meets the requirements of the first security level to protect chip hardware and firmware designs during the fabrication phase. Consequently, two different facilities are used to manufacture the main and daughter boards, which again meets the requirements of the first security level for board hardware design. Therefore, chip hardware, chip firmware, and board hardware security levels are set to *level 1* for the fabrication phase.
- For the after production phase, the system is designed to respond to any attempt to read the firmware by any module other than the processor by erasing all memory units to prevent an attacker from accessing secret data, which addresses the requirements of the third security level by adding more features for tamper evidence, detection, and response. Therefore, chip firmware security level is set to *level 3* for the after production phase.
- As per the system description, all chips are chosen to be surface mounted and all passive components are buried in the internal layers. All PCB tracks are placed in inner layers, the entire PCB is encapsulated with resistant epoxy compound, and all memory components are locked. This satisfies the requirements of the first security level for chip and board hardware designs in the after production phase. Therefore, chip hardware and board hardware security levels are set to *level 1* for the after production phase.

Based on our findings, our overall evaluation of this specific system will be set as *level 1* because, as we mentioned before, the security of the system is as strong as the weakest protected case.

Table 1
Case study: evaluation of the security level of an embedded system example. "x" means that the security requirement to protect the system is out of scope for this specific case.

No.	Life cycle	Integration phase	Programmability level	Security level
1	Design phase	IP	HW	x
2			FW	x
3			SW	x
4		Chip	HW	x
5			FW	Level 2
6			SW	x
7		Board	HW	Level 2
8			FW	x
9			SW	x
10	Fabrication phase	IP	HW	x
11			FW	x
12			SW	x
13		Chip	HW	Level 1
14			FW	Level 1
15			SW	x
16		Board	HW	Level 1
17			FW	x
18			SW	x
19	After production	IP	HW	x
20			FW	x
21			SW	x
22		Chip	HW	Level 1
23			FW	Level 3
24			SW	x
25		Board	HW	Level 1
26			FW	x
27			SW	x

Table 2
Comparing our proposed classification methodology to CMVP/FIPS 140-2 and CC.

No.	Limitations in CMVP/FIPS 140-2 and CC	Proposed work
1	The cryptographic modules considered by the CMVP/FIPS 140-2 standard are assumed to be completely secured and inherently free from any malicious content	The proposed method does not assume any part of the design to be malicious-free or secured. All design modules are subject to security assessment
2	The CMVP/FIPS 140-2 standard does not provide security measures to classify and assess threats during various design processes	The proposed method categorizes threats based on a 27-point classification system
3	CC is complex and lacks flexibility [8]	The proposed method simplifies the execution of risk assessment by considering three different perspectives and giving designers the flexibility to customize the 27-point system to match the design specification of the target product
4	CC lacks a clear relationship with the system development approach [8]	The proposed method clearly relates the security assessment to three different system development perspectives, namely: development phases, programmability, and integration levels
5	Designers do not see CC as a product-improvement evaluation methodology	The proposed method gives designers an opportunity to evaluate and improve their system security by considering four security levels for each of the 27 different scenarios, which brings the total to 108 possible security measures/solutions that could be considered to meet the target security level that must be achieved
6	CC focuses on the development phase of the product and misses possible attacks during and after production [9]	The proposed methodology considers attacks during development, fabrication, and after production
7	CC does not provide a clear implementation of the security audits for HW requirements [9]	The proposed method evaluates HW systems at IP, chip, and board levels with clear connection to development phases at each integration level

7. Evaluation of proposed approach

Our proposed classification allows system designers and auditors to classify and evaluate security requirements of embedded systems from 27 different angles by introducing a new three dimensional analysis. This has never been done before and is missing in CMVP/FIPS 140-2 and CC. In this section, we evaluate the efficiency of the proposed work by comparing it to the main standards that are currently available in the industry. Table 2 shows how the limitations in CMVP/FIPS 140-2 and CC are covered by the methodology proposed in this paper.

8. Conclusion

This paper presented a completely new classification for embedded systems security. This new multi-dimensional classification can help engineers have a better understanding of the security level of their final product and, hence, protect their embedded systems designs at different life cycle phases.

We plan to extend this work on two directions. The first direction is to develop a reliable measurement method to quantify the level of the target security so that it can be represented as one number, based on our multi-dimensional diagram. The second direction is to apply our method on real case studies that currently use CMVP/FIPS 140-2 and CC to evaluate the accuracy of the proposed model compared to them.

References

[1] S. Adee, The hunt for the kill switch, IEEE Spect. 45 (5) (2008) 34–39.
[2] Q. Li, G. Clark, Mobile security: a look ahead, IEEE Secur. Priv. 11 (1) (2013) 78–81.
[3] The Cryptographic Module Validation Program (CMVP), 2014. Online: https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program (accessed January 2016).
[4] Common Criteria Portal, The common criteria for information technology security evaluation (CC), part 3: security assurance components, 2012. Online: http://www.commoncriteriaportal.org (accessed January 2016).
[5] K. Taguchi, N. Yoshioka, T. Tobita, H. Kaneko, Aligning security requirements and security assurance using the common criteria, in: Proceedings of the 2010 Fourth International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2010), Singapore, 2010, pp. 69–77.
[6] S. Ardi, N. Shahmehri, Introducing vulnerability awareness to common criteria's security targets, in: Proceedings of the Fourth International Conference on Software Engineering Advances (ICSEA 2009), Porto, Portugal, 2009, pp. 419–424.
[7] C. Preschern, K. Dietrich, Structuring modular safety software certification by using common criteria concepts, in: Proceedings of the 2012 38th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA), Izmir, Turkey, 2012, pp. 47–50.
[8] F. Keblawi, D. Sullivan, Applying the common criteria in systems engineering, IEEE Secur. Priv. 4 (2) (2006) 50–55.
[9] J. Hearn, Does the common criteria paradigm have a future? IEEE Secur. Priv. 2 (1) (2004) 64–65.
[10] S. Narasimhan, D. Dongdong, R.S. Chakraborty, S. Paul, F.G. Wolff, C.A. Papachristou, K. Roy, S. Bhunia, Hardware Trojan detection by multiple-parameter side-channel analysis, IEEE Trans. Comput. 62 (11) (2013) 2183–2195.
[11] M. Rostami, F. Koushanfar, R. Karri, A primer on hardware security: models, methods, and metrics, Proc. IEEE 102 (8) (2014) 1283–1295.
[12] B. Koppel, S. Neuhaus, Analysis of a hardware security module's high-availability setting, IEEE Secur. Priv. 11 (3) (2013) 77–80.
[13] R.B. Lee, Rethinking computers for cybersecurity, Computer 48 (4) (2015) 16–25.
[14] G. Venkataramani, B. Roemer, Y. Solihin, M. Prvulovic, MemTracker: efficient and programmable support for memory access monitoring and debugging, in: Proceedings of the 2007 IEEE 13th International Symposium on High Performance Computer Architecture (HPCA'07), Phoenix, AZ, USA, 2007, pp. 273–284.
[15] J. Raszka, V. Tiwari, A. Mittal, M. Han, A. Shubat, Embedded flash memory for security applications in a 0.13μ CMOS logic process, in: Proceedings of the 2004 IEEE International Solid-State Circuits Conference (ISSCC). Digest of Technical Papers, San Francisco, CA, USA, vol. 1, 2004, pp. 46–512.
[16] A.S. Iyengar, S. Ghosh, K. Ramclam, Domain wall magnets for embedded memory and hardware security, IEEE J. Emerg. Sel. Top. Circ. Syst. 5 (1) (2015) 40–50.
[17] H. Handschuh, Hardware-anchored security based on SRAM PUFs, Part 1, IEEE Secur. Priv. 10 (3) (2012) 80–83.

[18] J. Zhang, Y. Lin, Y. Lyu, G. Qu, A PUF-FSM binding scheme for FPGA IP protection and Pay-Per-Device licensing, IEEE Trans. Inf. Forensics Secur. 10 (6) (2015) 1137–1150.
[19] J. Chen, G. Venkataramani, CC-Hunter: uncovering covert timing channels on shared processor hardware, in: Proceedings of the 2014 47th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO), Cambridge, UK, 2014, pp. 216–228.
[20] J. Chen, G. Venkataramani, An algorithm for detecting contention-based covert timing channels on shared hardware, in: Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy (HASP'14), Minneapolis, MN, USA, 2014.
[21] F. Liu, R.B. Lee, Random fill cache architecture, in: Proceedings of the 2014 47th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO), Cambridge, UK, 2014, pp. 203–215.
[22] F. Liu, Y. Yarom, Q. Ge, G. Heiser, R.B. Lee, Last-level cache side-channel attacks are practical, in: Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2015, pp. 605–622.
[23] W.-H. Lee, R.B. Lee, Multi-sensor authentication to improve smartphone security, in: Proceedings of International Conference on Information Systems Security and Privacy (ICISSP 2015), Angers, France, 2015, pp. 203–215.
[24] L.-W. Kim, J.D. Villasenor, Dynamic function replacement for system-on-chip security in the presence of hardware-based attacks, IEEE Trans. Reliab. 63 (2) (2014) 661–675.
[25] M. Tiwari, J.K. Oberg, X. Li, J. Valamehr, T. Levin, B. Hardekopf, R. Kastner, F.T. Chong, T. Sherwood, Crafting a usable microkernel, processor, and I/O system with strict and provable information flow security, in: Proceedings of the 38th Annual International Symposium on Computer Architecture (ISCA), San Jose, CA, USA, 2011, pp. 189–199.
[26] H.M.G. Wassel, Y. Gao, J.K. Oberg, T. Huffmire, R. Kastner, F.T. Chong, T. Sherwood, Networks on chip with provable security properties, IEEE Micro 34 (3) (2014) 57–68.
[27] P. Swierczynski, M. Fyrbiak, P. Koppe, C. Paar, FPGA Trojans through detecting and weakening of cryptographic primitives, IEEE Trans. Computer-Aided Des. Integr. Circ. Syst. 34 (8) (2015) 1236–1249.
[28] P. Kocher, R. Lee, G. McGraw, A. Raghunathan, S. Ravi, Security as a new dimension in embedded system design, in: Proceedings of the 41st Design Automation Conference (DAC 2004), San Diego, CA, USA, 2004, pp. 753–760.
[29] M. Tehranipoor, C. Wang, Introduction to Hardware Security and Trust, Springer-Verlag, Berlin, Germany, 2012.
[30] K. Hu, H. Chandrikakutty, R. Tessier, T. Wolf, Scalable hardware monitors to protect network processors from data plane attacks, in: Proceedings of the First IEEE Conference on Communications and Network Security (IEEE CNS 2013), Washington D.C., USA, 2013, pp. 314–322.
[31] G. Hoglund, G. McGraw, Exploiting Software: How to Break Code, Addison-Wesley Professional, Reading, MA, USA, 2004.
[32] Z. Shao, Q. Zhuge, Y. He, E.H.-M. Sha, Defending embedded systems against buffer overflow via hardware/software, in: Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC'03), Las Vegas, NV, USA, 2003, pp. 352–361.
[33] S. Khaleghi, K.D. Zhao, W. Rao, IC piracy prevention via design withholding and entanglement, in: Proceedings of the 2015 20th Asia and South Pacific Design Automation Conference (ASP-DAC), Tokyo, Japan, 2015, pp. 821–826.
[34] A. Lesea, S. Drimer, J.J. Fabula, C. Carmichael, P. Alfke, The rosetta experiment: atmospheric soft error rate testing in differing technology FPGAs, IEEE Trans. Device Mater. Reliab. 5 (3) (2005) 317–328.
[35] S. Ghosh, A. Basak, S. Bhunia, How secure are printed circuit boards against Trojan attacks? IEEE Des. Test 32 (2) (2015) 7–16.
[36] A.K. Sood, S. Zeadally, R. Bansal, Exploiting trust: stealthy attacks through socioware and insider threats, IEEE Syst. J. PP (99) (2015).
[37] J. Rajendran, A. Kanuparthi, M. Zahran, S.K. Addepalli, G. Ormazabal, R. Karri, Securing processors against insider attacks: a circuit-microarchitecture co-design approach, IEEE Des. Test 30 (2) (2013) 35–44.
[38] N.G. Tsoutsos, M. Maniatakos, Fabrication attacks: zero-overhead malicious modifications enabling modern microprocessor privilege escalation, IEEE Trans. Emerg. Top. Comput. 2 (1) (2014) 81–93.
[39] S. Lamprier, N. Baskiotis, T. Ziadi, L.M. Hillah, CARE: a platform for reliable comparison and analysis of reverse-engineering techniques, in: Proceedings of the 2013 18th International Conference on Engineering of Complex Computer Systems (ICECCS), Singapore, 2013, pp. 252–255.
[40] H.G. Longbotham, P. Yan, H.N. Kothari, J. Zhou, Nondestructive reverse engineering of trace maps in multilayered PCBs, in: Proceedings of the IEEE International Automatic Testing Conference (AUTOTESTCON '95), Atlanta, GA, USA, 1995, pp. 390–397.

Haytham Elmiligi received his Ph.D. degree in Electrical and Computer Engineering from the University of Victoria, Victoria, BC, Canada, in 2011. He is currently affiliated with the integrated microsystems (IMS) research group at the University of Victoria and the Computing Science Department at Thompson Rivers University, Kamloops, Canada. Haytham is a senior member of IEEE and a book series co-editor with CRC Press. His research work strongly relies on combining advanced analytical models and optimization techniques to improve the overall performance of multi-core systems.

Fayez Gebali received his B.Sc. in Electrical Engineering (first class honors) from Cairo University, his B.Sc. in Mathematics (first class honors) from Ain Shams University, and his Ph.D. degree in Electrical Engineering from the University of British Columbia, where he was a holder of an NSERC postgraduate scholarship. He is a Professor and Chair of the Department of Electrical and Computer Engineering at the University of Victoria. His research interests include parallel algorithms, NoC, three-dimensional ICs, digital communications, and computer arithmetic.

M. Watheq El-Kharashi received the Ph.D. degree in Computer Engineering from the University of Victoria, Victoria, BC, Canada, in 2002, and the B.Sc. degree (first class honors) and the M.Sc. degree in Computer Engineering from Ain Shams University, Cairo, Egypt, in 1992 and 1996, respectively. He is a Professor in the Department of Computer and Systems Engineering, Ain Shams University, Cairo, Egypt and an Adjunct Professor in the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada. His general research interests are in advanced system architectures, especially networks-on-chip (NoC), systems-on-chip (SoC), and secure hardware. He published more than 125 papers in refereed international journals and conferences and authored two books and 7 book chapters.