International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Volume 12, Issue 01)
Publishing Month: May 2015
An Indexed and Referred Journal
ISSN: 2347-601X
www.ijemhs.com

A Review Paper in PCB Security

Mugtaba Abdalrazig Mohamed Alhassan[1] and Dr. Muawia Mohamed Ahamed Mahmoud[2]

[1]Faculty of Engineering, Al- Neelain University, Khartoum, Sudan
elexaple@hotmail.com

[2]Faculty of Engineering, Al- Neelain University, Khartoum, Sudan
muawia15858@hotmail.com

Abstract

This paper present and reveal how embedded devices can be exposed to many different attacks and shows some methods that has been followed to hack these devices. Also it's summarized the previous work in this field, and explains to researches the weak areas that need to a future work around.

Keywords: *Secure hardware, embedded systems, PCB security, hacker attacks.*

1. Introduction

There is no such a thing where people can live in a world without affected by a hacker's threats, and today almost every one cannot coexists without the assistance of the embedded devices.
So securing these devices is remains a big headache to the users, the government and the manufacturers.
These days the usual security techniques are not sufficient anymore to encounter the different threats. Because of the technology evolution is very fast, which creates a motive
Well documented papers regard this concern has been published, which will be a solid base for researchers helping to minimize these hackers' attacks.
The level of security required for an embedded device varies dramatically depending upon the function of the device. Rather than asking if the device is secure, the OEMs should be asking if the device is secure enough. A military communication satellite or nuclear power plant control system clearly needs a very different level of security than a water softener equipped with Internet connections for remote diagnostics and automated reordering of salt. [1]

2. Embedded Security Challenges [1]

a. Critical functionality: Embedded devices control transportation infrastructure, the utility grids, communication systems and many other capabilities modern society relies upon. Interruption of these capabilities by a cyber-attack could have catastrophic consequences.
b. Replication: Once designed and built, embedded devices are mass produced. There may be thousands to millions of identical devices. If a hacker is able to build a successful attack against one of these devices, the attack can be replicated across all devices.
c. Security assumptions: Many embedded engineers have long assumed that embedded devices are not targets for hackers. These assumptions are based on outdated assumptions including the belief in security by obscurity. As a result, security is often not considered a critical priority for embedded designs. Today's embedded design projects are often including security for the first time and do not have experience and previous security projects to build upon.
d. Not easily patched: Most embedded devices are not easily upgraded. Once they are deployed, they will run the software that was installed at the factory. Any remote software update capability needs to be designed into the device to allow security updates.
e. Long life cycle: The life cycle for embedded devices is typically much longer than for PCs or consumer devices. Devices may be in the field for 15 or even 20 years. Building a device today that will stand up to the security requirements of the next two decades is a tremendous challenge.
f. Proprietary/industry specific protocols: Embedded devices use specialized protocols that

International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Volume 12, Issue 01)
Publishing Month: May 2015
An Indexed and Referred Journal
ISSN: 2347-601X
www.ijemhs.com

are not recognized and protected by enterprise security tools. Enterprise firewalls and intrusion detection system are designed to protect against enterprise specific threats, not attacks against industrial protocols.

g. Deployed outside of enterprise security perimeter: Many embedded devices are mobile or are deployed in the field. As a result, these devices may be directly connected to the Internet with none of the protections found in a corporate environment.

3. Categories of attacks to embedded systems

In "Security Requirements for Embedded Devices" [2] explain what is really needed to overcome and encounter the hacker's attacks. And in Figure.1 it describes the different classification attacks to embedded systems

Attacks are classified into three main categories based on their functional objectives.

_ Privacy attacks: The objective of these attacks is to gain knowledge of sensitive information stored, communicated, or manipulated within an embedded system.

_ Integrity attacks: These attacks attempt to change data or code associated with an embedded system.

_ Availability attacks: These attacks disrupt the normal functioning of the system by misappropriating system resources so that they are unavailable for normal operation.

A second level of classification of attacks on embedded systems is based on the agents or means used to launch the attacks. These agents are typically grouped into three main categories as shown in Figure 1:

- Software attacks, which refer to attacks launched through software agents such as viruses, Trojan horses, worms, etc.
- Physical or Invasive attacks, which refer to attacks that require physical intrusion into the system at some level (chip, board, or system level).
- *Side-channel attacks*, which refer to attacks that are based on
- Observing properties of the system while it performs cryptographic operations, *e.g.*, execution time, power consumption, or behavior in the presence of faults.

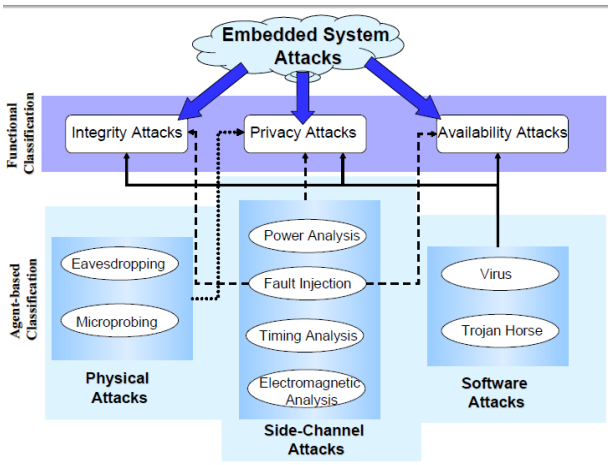

Fig. 1 Taxonomy of attacks on embedded systems [2]

In table 1 a comparison of attacks classification with the available resources, this revels to the companies that manufacture these embedded device to have knowledge about what kind is theirs enemy, so they can take their precaution in the developing phase and even later.

In Abraham, et al.'s *Transaction Security System* [8], attackers are classified into three groups (now essentially an industry-standard) depending on their expected abilities and strengths:

Class I (clever outsiders). They are often very intelligent but may have insufficient knowledge of the system. They may have access to only moderately sophisticated equipment. They often try to take advantage of an existing weakness in the system, rather than try to create one.

Class II (knowledgeable insiders). They have substantial specialized technical education and experience. They have varying degrees of understanding of parts of the system but potential access to most of it. They often have highly sophisticated tools and instruments for analysis.

Class III (funded organizations). They are able to assemble teams of specialists with related and complementary skills backed by great funding resources. They are capable of in-depth analysis

of the system, designing sophisticated attacks, and using the most advanced analysis tools. They may use Class II adversaries as part of the attack team.

Table 1. Comparison of Attack Classification with Available Resources [7]

Resource	Class I (Curious hardware hacker)	Class II (Academic)	Class III (Organized crime)	Class III (Government)
Time	Limited			
Budget ($)	< $1000	$10k - $100k	> $100k	Unknown
Creativity	Varies	High	Varies	Varies
Detectability	High	High	Low	Low
Target/Goal	Challenge/Prestige	Publicity	Money	Varies
Number	Many	Moderate	Few	Unknown
Organized?	No	No	Yes	Yes
Release information about attack?	Yes	Yes	Varies	No

4. Example of successful hacking

4.1 USB Hardware Token Devices

Fig. 2 Aladdin Knowledge Systems' eToken R1, top, and Rainbow Technologies' iKey 1000 and 2000, bottom. [6]

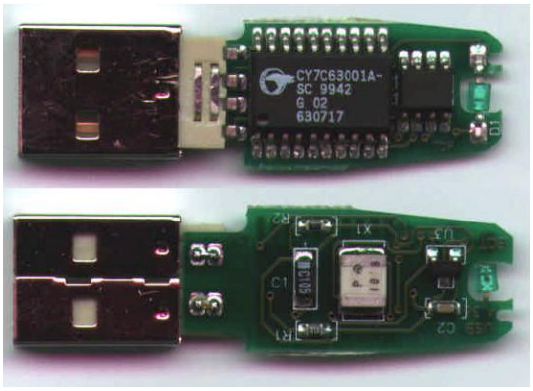

Figure3: eToken R1 PCB version 4.3a, top: front, bottom: back. [6]

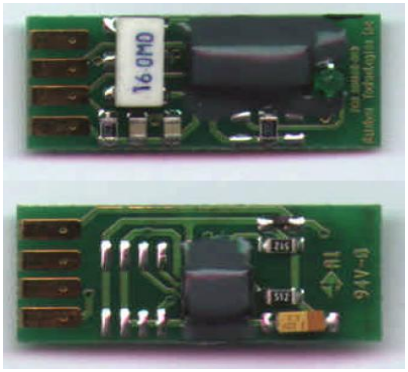

Figure 4: iKey 1000 PCB 106160-003, top: front, bottom: back. [6]

And the result is as shown in table 2.

Table 2. The investigation results [6]

Device	Difficulty To Penetrate Housing	Protection of Internal Circuitry
eToken R1	Moderate	None
iKey 1000	Easy	Moderate (Epoxy)
iKey 2000	Easy	Moderate (Chip-on-Board)

The security shall be kept in mind throw all of the processes of the design, example of that in software development is shown in fig 5.

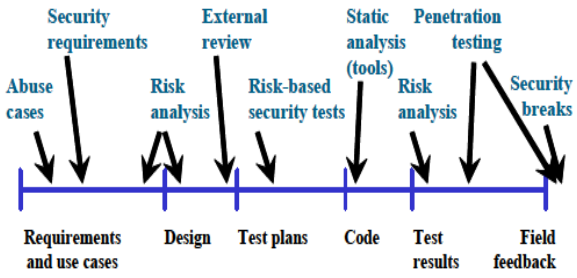

Figure 5: Software security best practices applied to various software artifacts in the Software Design Life Cycle (SDLC). [3]

4.2 Power analysis attacks

The power profile of cryptographic computations can be directly used to interpret the cryptographic key used. For example, (simple power analysis) SPA analysis can be used to break RSA implementations by revealing differences between the multiplication and squaring operations performed during modular exponentiation. In many cases, SPA attacks have also been used to augment or simplify brute-force attacks.

For example, it has been shown in [9] that the brute-force search space for one software DES implementation on an 8-bit processor with 7 bytes of key data can be reduced to 240 keys from 256 keys with the help of SPA.

DPA (differential power analysis) attacks use statistical techniques to determine secret keys from complex, noisy power consumption measurements. In fig 6 explain for a typical attack, an adversary repeatedly samples the target device's power consumption through each of several thousand cryptographic computations. These power traces are collected using high-speed analog-to-digital converters, such as those found in digital storage oscilloscopes.

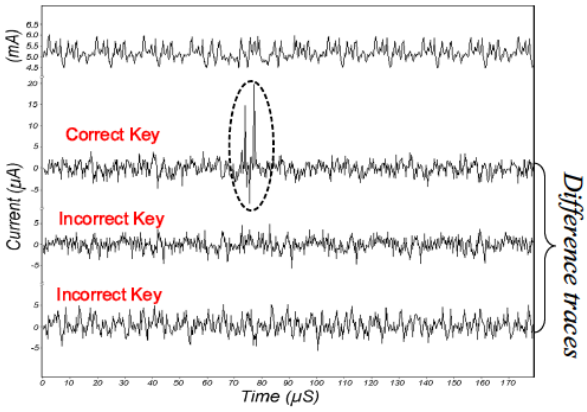

Figure 6: Power consumption traces generated during a DPA attack on a DES implementation [3]

5. Conclusions

It is important to the embedded devices' designers to keep in mind: a PCB component that is hard to access, with high encrypted software, will produce a better secure device that can stand exceedingly against the attackers.

References

[1] Alan Grau, Icon Labs, "Security Requirements for Embedded Devices – What is Really Needed? ", 2014.
[2] Srivaths , Anand and Srimat, "Tamper Resistance Mechanisms for Secure Embedded Systems", NEC Laboratories, America, Princeton, 2004.
[3] Paul Kocher and other, "Security as a New Dimension in Embedded System Design", NEC Laboratories America, Princeton.
[4] DAVID D.HWANG and others, "Securing Embedded Systems",University of California, 2006.
[5] Saar Drimer, Steven J. Murdoch, Ross Anderson, "Thinking inside the box: system-level failures of tamper proofing", 2008.
[6] Reykjavik University,USA, "Attacks on and Countermeasures for USB Hardware Token Devices".
[7] Joe Grand, "Practical Secure Hardware Design for Embedded Systems," Proceedings of the 2004 Embedded Systems Conference, San Francisco, California, March 29-April 1, 2004.
[8] D.G. Abraham, G.M. Dolan, G.P. Double, and J.V. Stevens, "Transaction Security System," IBM Systems Journal, vol. 30, no. 2, 1991, http://www.research.ibm.com/journalsj/302/ibmsj3002G.pdf.
[9] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," IEEE Trans. Comput., vol. 51, pp. 541–552, May 2002.