Real-World Attacks Toward Circuits & Systems Design, Targeting Safety Invasion

M. Katsaiti [I], A. Rigas [I], I. Tzemos [I]
[I] Computer Engineering & Informatics Department,
University of Patras,
GREECE

Nicolas Sklavos [I, II]
[II] KNOSSOSnet Research Group,
Computer Informatics & Engineering Department,
Technological Educational Institute of Western Greece,
GREECE

***Abstract*—As a result of the continuous need for the evolution of Internet of Things, microprocessors have prevailed over embedded systems; they provide engineers with various advantages concerning designing applications. Although, implementations need to be accompanied by high security levels, as microprocessors are excessively vulnerable to real-world attacks. This work examines modern applied attacks, toward circuits and systems design. Four different approaches are introduced and examined in detailed: side channels analysis via SimonsVoss approach, onetime password token with Yubikey method, optical fault injection methodology and finally FPGA approach on side channel attacks, are introduced. Comparisons results and benchmarks of the four approaches are presented in detail.**

Keywords—side-channel analysis; security; microprocessor; real-world attacks; code extraction; Internet of Things

I. INTRODUCTION

The Internet of Things (IoT), researchers visualize, refers to the correlation where each and every physical component becomes virtual, able to communicate with others through the invisible web of IoT. Microcontrollers (μCs) have undoubtedly become the big buzz of embedded systems, offering hardware design engineers, tons of benefits. From the privileged size and cost of them to the surprising adaptability to various implementations, they always manage to be the number one choice for the majority of applications. The massive use of μCs is increasingly leading to the implementation of the imagined IoT described above. However, their colossal application is simultaneously hazardous; there are different methods that pose threats toward the entire security of the system. All of them focus on a common goal, to disclose the embedded code and extract the secret cryptographic key; in other words, cause the invasion of the security protection. Research has proved μCs' structural design tends to be more susceptible to side-channel leakage, compared to an FPGA or an ASIC.

This work specifically deals with the existing, real-world applications that use different techniques and prove that safety can be circumvented. Dominating the field of digital locking systems, in Europe, SimonsVoss Technologies AG, offer a wide range of products, covering applications from simple apartments to embassies; all vulnerable to attacks. Next attempt is focused on penetrating Yubico's Yubikey 2, a μC-based onetime password (OTP) token. The latter, encoded in Advanced Encryption Standard (AES), is utilized in various cases where the username/password authentication method proves to be of limited use. Another implementation of μCs, used in daily basis, is Smart Cards; examples are SIM cards or PIN banking cards. Attackers aim to break down their security, something possible if they handle the situation carefully and with special equipment.

The structure of this work paper begins with building a background theory over IoT, in Section II. Security and microprocessors are studied in Sections III and IV correspondingly. The violation of a SimonsVoss locking system with the help of side-channel analysis method is presented in Section V. Moving forward to Section VI, the Yubikey method proves to be successful considering the circumvention of one-time password kind of security. In Section VII, fault injection efficiently attacks applications of Smart Cards. Another attack based on side-channel analysis, presented in Section VIII, is focused on FPGAs. In Sections IX and X, we attempt to compare and contrast these real-world attacks and jump to a conclusion about which method is more efficient. During the comparison, we take consideration of the total cost needed to breakdown the μC as well as the time spent to achieve the final goal. Additionally, we might take account of the power consumption or other technical characteristics in certain cases.

II. INTERNET OF THINGS (IOT)

In the new era of the Internet of Things (IoT), technological advancements aim to build the new, virtual world. The main idea behind the IoT, is the representation of every physical object as a sum of heterogeneous virtual ones. Entities are able to interact with others, using characteristics like location or address to identify one another, on a virtual level. Each component, represented by an avatar, achieves this communication via a universal network of interconnected objects [1]. As depicted in Figure 1, examples of IoT components can be considered electronic devices like computers, tablets, or smart phones, printers, cameras and various digital locking systems. Added to the paradigms above, the security system applied from houses to embassies is part of the IoT, all controlled by the human aspect. On this digital base, entities operate to produce or consume a great amount of services, aiming to a mutual target.

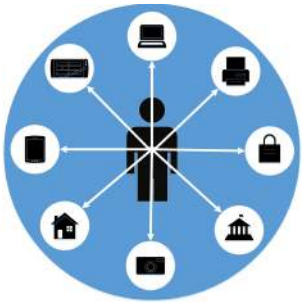

Fig. 1. *Aspects of the virtual ecosystem*

In the essence of "anywhere, anyhow, anytime", IoT deals with obstacles concerning the security throughout the entire lifecycle of the object. Researchers should rise to the challenge of deciding, whether existing methods are sufficient or new designs need to be developed. Security measures need to be implemented gradually, on a level-by-level base, and as a whole [2].

III. Security Aspects In The Era Of IoT

The steps leading toward the envisioned IoT have formed an entirely new field of research and expertise. The security issues that are concerned vary as safety can be circumvented on different levels [2]. Certain cases that are following will puzzle out the necessity of security in IoT [1]. Personalized services, included in the IoT, produce an amount of data that poses a threat if acquired. Another aspect of security deals with the ability IoT elements should have to recover from an attack to a prior unharmed state, e.g. fault tolerance [2].

There are enough techniques that make security collapse, but Side Channel Analysis (SCA) and Code Extraction are the ones that differ from others [3]. SCA is the product of an effort made by attackers to acquaint with the device, in the essence that unlimited physical access was mandatory. The aim of SCA is to get a sample side-channel signal, also known as trace, and process it with the help of the proper digital signal processing methods. The procedure resumes by analyzing with statistics so as to retrieve the secure key. The other approach leading to security breakdown is code extraction. Despite manufacturers' firmware and data protection mechanics, e.g., lock bit method, it is proved that with power glitching techniques attackers are capable of reproducing the embedded code, known as reverse engineering.

On the other hand, certain procedures exist to assure safety. Cryptography has a major role protecting the network infrastructure; a vastly used algorithm for this purpose is the Advanced Encryption Standard (AES). Additionally, in order to achieve end-to-end security, forward-looking adaptation on existing protocols needs to be implemented on devices lacking the essential resources, e.g. sensors [2]. One last scenario that empowers safety deals with identity principles and privacy assurance; these techniques allow users to bypass the device based on the "what I am + what I know" or "what I have + what I know" security forms [1].

IV. Microprocessors Design

Being established as one of the smallest individual computer systems, microprocessors have conquered the world of embedded systems and modern technology. The fields of their use vary from everyday applications such as household appliances, mobile devices to complex ones, such as, industrial. Due to the wide range of use combined with their low expense, microprocessors have gone viral and their necessity has become inevitable. As a promising tool for future applications, microprocessors need to be insusceptible to potential security risks. However, in various research works, it has been proven that security of a µC may be violated, either on a hardware level of the device or in the established communication channels [2], known threats towards the Internet Of Things (IoT).

Microcontrollers, mostly referred as µCs, are a single chip architecture with internal ROM and flash memory, core and various peripherals. Despite the fact that there is a great amount of different microcontrollers, many of their characteristics are in common. As a result, it is sufficient enough to familiarize with one, so as to be able to handle the rest.

ARM Cortex M0, is one widespread µC included in many embedded systems. It belongs on ARM Cortex M series, a family of µCs, consisting of cores aimed at very cost sensitive, deterministic, interrupt driven environments. Cortex M0 is both the smallest and the lowest power ARM 32-bit processor existing, developed for high power adequacy. Furthermore, it has been designed for ultra low power deep sleep. This processor supports ultra low-power standby implementation, which is very useful and important for battery-based applications. Cortex M0 is comprised of ARM core, a Bus Matrix, a configurable Debug and Debugger Interface. Also, it includes an interrupt controller (NVIC) and a very low gate count Wake-up Interrupt Controller (WIC). Processor accesses and debug accesses share the external interface to external AHB peripherals. Finally, Cortex M0 offers critical privileges to developers e.g. simple architecture, energy efficient operation, excellent code density [4].

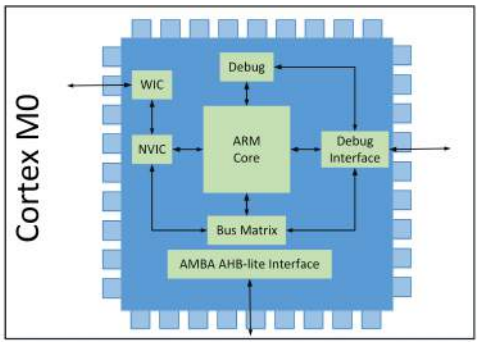

Fig. 2. *Inner Architecture of µC*

V. Side Channel Analysis Via SimonsVoss Approach

SimonsVoss's "Generation 2" digital locking system 3060, broad use, is the reason why, researchers have focused their efforts into evaluating its undisclosed, proprietary cryptographic protocol. With no knowledge over the inner design of the system, the reverse engineering method reveals, that every Printed Circuit Board (PCB) consists of a SimonsVoss-proprietary ASIC in charge of the radio-frequency transmission amplitude, a PIC16F886 µC executing

and storing the authentication protocol [5] and an Electrically Erasable Programmable Read-Only Memory (EEPROM), all playing their part on the authentication process. Side-Channel Analysis (SCA), the method used in this approach, can be characterized as a passive attack, taking into consideration that the procedure takes place in normal operating conditions. Before the use of SCA, certain steps need to be followed. As a first step, a firmware extraction effort is attempted on the EEPROM, holding the μC's firmware. Using an EEPROM Erasable Tool as a UV-C light source, it is possible to achieve an alteration to the fuse bits, so that the code readout protection is disabled without any harm to the remaining content (firmware), now able to be accessed. Having the code, a SimonsVoss's Authentication Protocol review reveals that it figures eleven steps and that a mutually shared key exists in both transponder and lock [6].

Key's structural design, determines its components and their derivation method. By default, the door's system key is divided into four same keys, each calculated by a two input XOR logic gate, with $K_{T,int}$ the internal EEPROM stored key and $K_{T,ext}$ the external one. The transponder's key (K_T) is identified with the help of the system key and aids the lock authentication process by producing the identifier I_T. Function K is the lock's tool that utilize the earlier mentioned system key and I_T to authenticate. Moving toward the extraction of the key, SCA, aims at the key derivation function K with the assumption that the system key, can be of aid, calculating every transponder's key, given its I_T. Device's Under Test (DUT) profiling method, is based on a trigger step to function K and an EM probe, close to the power supply pins, for power traces assessment. Experimental procedure, leads to the profiling of the DUT and the conclusion that, for a profiled DUT, only a few power traces, properly aligned and filtered, are needed to recover the key in a noninvasive manner, in contrast to the 1.000 recorded ones during the profiling step.

VI. Yubikey Method for Onetime Password Token

Problematic authentication methods aimed research to alternative, two-factor validation, security measures like Yubikey 2. Yubico treats customers in need of high security services with an OTP token generator, utilizing an open-source protocol based on AES standard. Yubikey's OTP token is formed by a total of 16-B, sum of different reference bytes, encrypted in AES's standards. Due to poor knowledge on a hardware level, limited to only promotional videos [7], certain procedures were invoked to determine the μC in use and an applicable, noise-efficient, power traces measurement method for the developed USB power and data lines adapter. As a result of a notable voltage drop, during DUT profiling, caused by the LED off function, specifically underlined admissions concerning the point of reference and the sample rate were made. During that method, the EM traces were also captured for a comparison, which concluded to the supremacy over the power traces eligible results. Having that in mind, EM traces were chosen over the power traces to recover the AES key with a reduced number of measurements and time consumption. As an example for 4.500 usable traces, 7.000 need to be acquired and with an approximate of 1.000 traces per 1.5h, 10.5 hours are needed, in contrast to 800 EM traces and 1 hour.

On an attempt to extract the AES encrypted key (Figure 3), a metric summarizing the ratio between the correlation of the correct key and the second best candidate can be used, leading to an hour need of physical access to hardware for an attack to be successful. A lot more efficient, when compared to the power traces use in this method (10.5 hours). Once the key is obtained, attacker is able to reproduce acceptable OTPs, with minor physical traces left on the DUT to point out that is compromised.

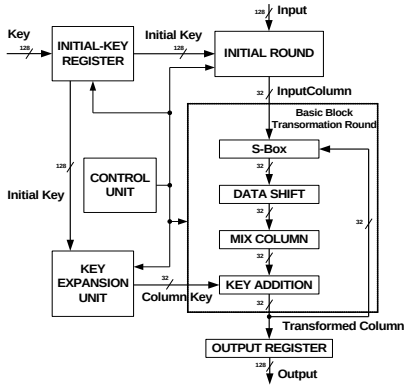

Fig. 3. *AES Full Architecture Design*

VII. Optical Fault Injection Methodology

Optical fault injection method is proven to be the most adequate one, to bypass security on smart cards. The fact leading to this conclusion, is the difficulty engineers face on developing efficient countermeasures to mitigate the security risks. As the procedure takes place outside the normal specifications of the card, it can be characterized as an active attack. In addition, based on the chip preparation required, it is true to claim that we are dealing with a semi-invasive attack. As a first step of the optical fault injection, an essential chip preparation is required. Access of the attacker needs to be established either on the front or the back side of the card. The front side of the card consists of metal layers and transistors protected by a thin, transparent or not, sheet of epoxy; in case it is transparent the attacker has direct access, otherwise the epoxy has to be discarded. On the other side of the card, it is necessary to extract the smart card contact pad so as to have access to the chip.

Once access is established, the procedure continues [8], [9]. The purpose of the attack is to cause a temporary fault while a specific process is executed. More detailed, a high-intensity diode laser is accurately targeting on a specific, extra sensitive area and is synchronized to the multiple instructions by a pattern based trigger. Experiments on smart cards with and without operation system prove that 1000 and 10000 continuous fault injections, correspondingly, are needed so as the perfect combination of time and location is known. The fault caused in the chip helps to circumvent security by e.g. guessing the correct passwords required in a SIM card.

VIII. FPGA Approach on Side-Channel Attacks

Side-channel attacks successful rates increase, force researchers to investigate and apply countermeasures, only to find themselves on a vicious cycle of new security risks

appearances. To this end, Edwards curves and coordinates for Elliptic Curve Cryptography (ECC) [10] claim, to be both side-channel security, as well as, operation wise efficient, is tested. A FPGA (Model XC2VP7-FG456-5), is used to develop an architecture resembling a standard elliptic curve processor, that is able to perform a point multiplication in Edwards coordinates [6]. On an algorithm level, to prevent Simple Power Analysis (SPA) and make Differential Power Analysis (DPA) tricky, a basic countermeasure is used to achieve random order execution in the Montgomery ladder. This step, aims at an enlarged number of measurements in order to achieve a successful attack. Furthermore, a simple setup is configured, consisting of a SASEBO-G side-channel evaluation board, an oscilloscope and a desktop PC for obtaining the measurements [11]. Finally, after pre-processing and filtering the measurements and samples acquired, it is possible to recognize the key bit. With that in mind, PCA's efficacy over the point multiplication in Edwards coordinates seems applicable, not only to a random order execution countermeasure but to others too.

IX. Comparisons Of The Examined Methods

Piecing together the above attack methodologies, it is feasible to jump to certain conclusions on three main axes; laboratory equipment needs, complexity of profiling and time consumption of the procedure (Figure 4). On the first axis, each method introduces, more than one, specific tools needed to achieve its goal. UV-C lights, EEPROM Erasable Tools, USB adapters, SASEBO boards, diode lasers and pattern based triggering generators aim to the exact measurements acquisition for an accurate profiling or the reverse engineering of the hardware in test. As a result, attacks in Sections VII and VIII can only be performed inside a laboratory environment, while Sections' V and VI attacks environment is irrelevant. Furthermore, on a complexity level during the profiling of a DUT, precision matters.

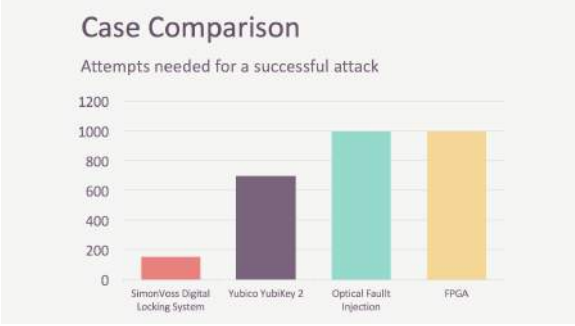

Fig. 4. *Examined Approaches Benchmark*

Code extraction methods, used in Sections V and VI, require specific safety bits to be altered, while the rest, containing the code, remain intact. On the same track, profiling countermeasures like the ones in Section VIII and noise problems encountered in Section VI, need to be overcome either by specific algorithmic methods for power traces collection or alternate measurements' setup.

Time consumption, the security attack's main field of concern, can be partially represented by the number of usable power traces. Profiling a DUTs' power traces, pose an ongoing matter of study, with approximation and down sampling being certain steps for limiting the gathered power traces; and as a result the time, needed for an attack. In Figure 5, a comparison over usable power traces, for every attack method, on a profiled DUT is presented with Section's V attack being the most efficient one and Section's VIII FPGA attack proving that a μC is more susceptible than a FPGA.

X. Conclusions & Future Work

The security of modern μCs is in doubt. It is presented that, even if engineers aim to mitigate the risks and augment proper countermeasures, an attack can still bypass the safety of a μC. Different attack cases are formerly presented in an effort to expose those kinds of threats. As a future work, we target to further research based on the implementation of innovational countermeasures. Security needs to be enforced, as μCs tend to conquer every dimension of our daily lives.

XI. Acknowledgment

This work is supported under the framework of EU COST IC 1204: TRUDEVICE (Trustworthy Manufacturing and Utilization of Secure Devices) Project.

References

[1] R. Roman, C. Alcaraz Tello, J. Lopez, N. Sklavos, "Key Management Systems for Sensor Networks in the Context of the Internet of Things", Computers & Electrical Engineering, Elsevier Science Press, Vol. 37, Number 2, pp. 147-159, 2011.

[2] N. Sklavos, G. Di Natale, "TRUDEVICE Project: Trustworthy Manufacturing and Utilization of Secure Devices", HiPEAC Computing Systems Week (CSW), Athens, Greece, 8-10 October 2014.

[3] D. Strobel, D. Oswald, B. Richter, F. Schellenberg, and C. Paar, "Microcontrollers as (in)Security Devices for Pervasive Computing Applications", Ruhr University Bochum, Germany. Article published in Proceedings of the IEEE, vol. 102, issue 8, pp. 1157 – 1173, June 2014.

[4] ARM, "CortexTM-M0 Revision: Technical Reference Manual", 2009.

[5] Microchip Technology Inc., ''PIC16F882/883/884/886/887 Data Sheet'', 2009.

[6] D. Oswald, D. Strobel, F. Schellenberg, T. Kasper, and C. Paar, ''When reverse-engineering meets side-channel analysis--Digital lockpicking in practice,'' Selected Areas in Cryptography. Berlin, Germany: Springer-Verlag, 2013, pp. 571–588.

[7] D. Oswald, B. Richter, and C. Paar, ''Side-channel attacks on the Yubikey 2 One-Time Password Generator'', Research in Attacks, Intrusions, Defenses, vol. 8145, S. J. Stolfo, A. Stavrou, and C. V. Wright, Eds. Berlin, Germany: Springer, 2013, pp. 204–222, LNCS.

[8] D. Strobel, D. Oswald, B. Richter, F. Schellenberg, and C. Paar, "Microcontrollers as (in)Security Devices for Pervasive Computing Applications", Ruhr University Bochum, Germany. Article published in Proceedings of the IEEE, vol. 102, issue 8, pp. 1157 – 1173, June 2014.

[9] Stefan Mangard, Elisabeth Oswald, Thomas Popp, "Power analysis attacks: revealing the secrets of smart cards", IRISA Laboratory, France. Book Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security), Springer-Verlag, 2007.

[10] J. Vliegen, N. Mentens, J. Genoe, A. Braeken, S. Kubera, A. Touhafiand I. Verbauwhede, "A Compact FPGA-based Architecture for Elliptic Curve Cryptography over Prime Fields", 21st IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP), IEEE, pp. 313–316, 2010.

[11] A. Bechtsoudis, N. Sklavos, "Side Channel Attacks Cryptanalysis Against Block Ciphers Based on FPGA Devices", proceedings of IEEE Computer Society Annual Symposium on VLSI (IEEE ISVLSI'10), Kefalonia, Greece, July 5-7, 2010.