Malware in IoT Software and Hardware

[I] Jelena Milosevic, [II] Nicolas Sklavos, [II] Konstantina Koutsikou

[I] Advanced Learning and Research Institute (ALaRI), Faculty of Informatics,
Universita della Svizzera italiana, Lugano, Switzerland

[II] SKYTALE Group,
Computer Engineering & Informatics Department,
University of Patras, Hellas

Abstract*— Internet of Things (IoT) devices have conquered the modern world, and they are increasingly gaining ground day by day. Together, with their widespread use also interests from attackers in abusing them are rising, causing increase of malicious software (malware). The goal of this wrok is to introduce a detailed study of currently existing malware threats in IoT devices, that have arisen during the past years for both system hardware and software. For these purposes, first a detailed overview of recent security incidents involving IoT devices from a software viewpoint, is introduced. Then we present the most widespread types of malware, such as rootkits, ransomware and bots among others. We point out hardware environment with different types of side-channel attacks. Finally, we present existing malware detection methods and outline expected future directions.

Keywords—malware; side-channel analysis; security; microprocessor; real-world attacks; malware detection; Internet of Things (IoT).

I. INTRODUCTION

IoT devices consist of all the cyber physical computing devices with internet connectivity, such as routers, web cameras, smartphones, point-of-sales terminals, building automation devices, medical equipment, smart TVs, medical devices, smart home devices, cars, etc. In particular, as regards the worldwide mobile phone market, around 1.4 billion smartphones were sold in 2015, according to the evaluations provided by the International Data Corporation (IDC) [1] [2]. In addition, 6.4 billion connected IoTs were reported in 2016, and an amount of 20.8 billion is estimated to be sold by 2020 [1].

On one side, the IoT devices offer extended features, along with the facilitation of a wide range of functions. But on the other their security level is still low with well-known weaknesses. In [3], an extended list of vulnerabilities has been reported per surface area, such as software and hardware weaknesses, encryption issues, data privacy matters. In [4] it has been stated that around 1 million new threats were released each day during 2014. Later research, in [5], showed that rootkits, ransomware, bots, viruses, worms and trojan horses rank as the most frequent malware [6].

Together with the threats posed to software, recent studies have shown that hardware threats are harmful and alarming as well. Technological experiments have proved the possibility of tampering backdoor A2, during the fabrication process [5]. Additionally, side-channel attacks can take place in the device's physical unclonable functions (PUFs) [7]. Attacks of this kind aim at retrieving the secret key, which is used for data encryption and decryption. These attacks, are focused primarily on the physical implementation of a system. In addition, they are derived in numerous classes, the most recognized of which include timing attacks, power monitoring attacks, electromagnetic attacks, differential fault analysis, etc.

This paper aims to provide a detailed study of the most common IoT security issues, and an outline of the most important findings reported, in recent years. Furthermore, it depicts a concise illustration of the most significant hardware attacks, focusing mainly on side-channel attacks, and more specifically in Differential Power Analysis (DPA) and Differential Fault Analysis (DFA). In conclusion, an analysis of different detection and protection methods is provided.

The structure of the paper is organized as follows: in Section II we describe current malware in IoT devices, from both software and hardware perspectives. Then, in Section III we explore the malware detection and protection methods in detail. In Section IV, we provide a summary of the current situation and the future directions, that should be given priority according to the current results. Finally, Section V concludes the paper.

II. MALWARE IN IOT DEVICES

In this section, we analyze different types of malware that can affect software applications and hardware devices. With respect to the software area, several studies and publications that carried out over the last years have shown that malware attacks, especially in Android based applications, have risen dramatically. As a result, a remarkable increase has been reported during 2015, reaching the highest volume over the first quarter (Q1) [1]. As shown, in Figure 1, the emergence of new malware in Android devices is significantly higher (G DATA-Mobile Malware Report 2016). During the second half of 2015 and the first half of 2016, a 98% increase was evident in smartphone infection rates [8]. In this context, a new malware

sample is detected every 9 seconds, according to security analysts [9].

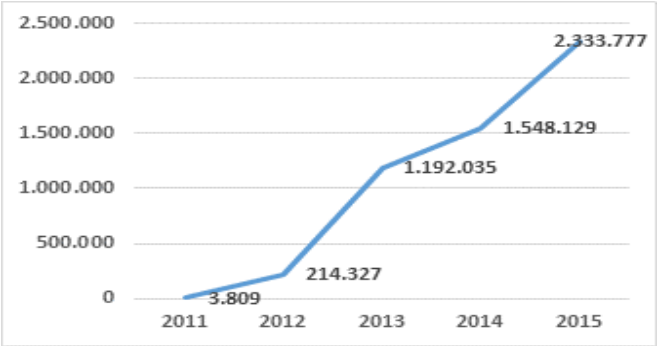

Figure 1: Android Malware Samples Evolution

On the hardware side, as studies have shown, fabrication-time attacks, can take place by tampering the chip during its fabrication and by taking advantage of analog circuits [6]. These changes can create favorable conditions for future attacks. On the other hand, research has also demonstrated that in the case of analog hacks, a cell can be added during the chip's fabrication, operating as an electric capacitor which is able to expose the system to an attacker [5]. Such attack is otherwise known as the "A2 analog attack".

a. Malware in Software

Malware is the most serious threat for IoT devices, which can either destroy the device or, in some cases, it can shift the system into a privileged state under the attacker's authority [10]. The most well-known malware [10] according to cyber-attack statistics are rootkits, ransomware, bots, financial malware, logic bombs, virus, worms and trojans. Rootkit is a malware type, that the attacker can progressively access, with the end goal of shifting the system, under his or her authority. Ransomware malware can lock the user's device or software, seeking monetary gain from the user to remove the current infection. As noted previously, "screen locker ransomware" is able to lock an Android-based smart TV. Designed as a self-propagating type of malware, bots are targeted to infect a device. These malware threats subsequently connect to a server, also known as a "bot master", which acts as a central control hub for compromised devices. Financial types of malware, try to collect banking account information from a device, or by means of fault banking sites. Logic bombs are code-blocks added by the attacker into a system. When these programmatic functions are triggered, they can harm the system, either by deleting data or by creating conditions that can destroy the entire system. Virus malware software is spread through a software program and can be harmful for a system. In order for a virus to be installed and replicated in a device, the user's action is needed (for instance, by triggering it via an executive program). Contrarily to viruses, worms can be spread without the user's interaction and can act independently, as a stand-alone entity. On the other hand, worms are disseminated via the network. Trojans consist of a type of malware that invades a system by stealing user identity and information [6]. Due to their stand-alone attribute, such malware can enable further attacks by opening a backdoor.

In a similar fashion, Grayware and Madware pose a considerable threat to security. Grayware, which among other viruses includes adware and dialers, cannot be considered as malicious, although they can still perform undesired actions, thereby negatively affecting the device's performance. Madware, on the other hand, uses targeted and aggressive advertising messages or pop-ups, to collect information from a user's device [10].

According to the findings in [8], three (3) of the most frequent threats pertaining to mobile phones are Uapush.A, Kasandra.B and SMSTracker. Uapush.A is a trojan which can steal data from a mobile device, by sending an SMS. Kasandra.B is another trojan, which resembles a security app. Kasandra.B can access sensitive data contained in a mobile phone like logs, credentials, history, etc. SMSTracker is an android app, that allows the attackers to monitor the traffic functions (SMS, phone calls, etc.) of a mobile device in their entirety. Similarly, it has been noted that a "screen locker ransomware" is able to lock an Android-based smart TV [8].

Finally, numerous IoT devices, including IP cameras, routers, DVRs, printers, etc., have been hacked by a malware named "Mirai". It attacks IoT devices, by scanning factory-default usernames and passwords [11].

b. Malware in Hardware

When talking about malware in hardware, attackers have found ways to act on the chip level, which is the integral part of a system. By using several methods, a device or a system, can be exposed. Minor modifications to a chip, might be the cause of numerous attacks. This paper, focuses predominately on the overview of the IOT software and hardware malware. However, it also tackles the issue of modern microprocessors, which consist of numerous microprograms and operations defining the device's operation [12].

The fundamentals of hardware configurations, are structured by implementing strong algorithms and cryptographic functions. An attacker can intervene in operations, involving cryptographic computation values to retrieve the authority, by implementing various techniques. One of the most practical methods to compromise device security, is by using side channel attacks [13]. These attacks have one common goal, to retrieve information from the leaking signals, during the device's operations. This information, coupled with the appropriate calculations, can lead to the retrieval of the secret key by the attacker. Side-channel attacks are divided into passive and active. Passive attacks are predominantly oriented towards information gathering. In this context, a passive side-channel attack presupposes the action of gathering useful information during the operation process. On the other hand, apart from the information gathering process, active attacks are more dynamic, whereby an attacker can retrieve the secret keys by injecting faults in a normal operation. More specifically, during the information-gathering process of a side-channel attack, special equipment is used consisting of probes, oscilloscope, bandwidth amplifier, analyzing software, etc.

The knowledge of the plaintext is not mandatory, during the differential power analysis, whereby power traces (T 1...m [1…k], k samples) are captured and the ciphertext is recorded

(C [1...m]), (Figure 2). By applying the selection function and computing the differential trace of the k sample, the attacker can gain favorable results. In this vein, the differential power analysis can be applied in many algorithms such as AES, DES, etc.

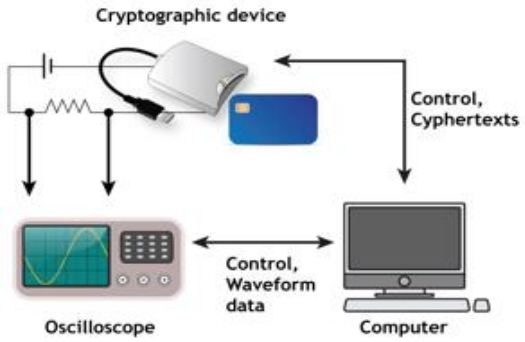

Figure 2: Differential Power Analysis

The differential fault attack, is an attempt to modify the computation of an algorithm, by generating faults or by taking advantage of existing faults. In fact, the same data are encrypted, and this operation is depicted in the results. Furthermore, the attacker can make correlations between the correct and the fault ciphertext to retrieve the key candidates. This process can be applied many times until the unique key is identified. This is the case for chip cards, which are prone to such attack. The embedded microprocessors are sensitive in high temperatures, or their power supply capacity is very specific. All these conditions can create an ideal setting for an attacker. As a result, physical weaknesses may generate the environment of such an attack.

In a situation, where a timing attack is performed, the attacker can discover the secret key, by estimating the processing time of a cryptographic operation. In such event, the attacker uses measurement instruments to compute the operation time. In particular, algorithms such as RSA, Diffie-Hellman and RC5, have been reported as vulnerable to such attacks.

As far as power monitoring attacks are concerned, an attacker can extract cryptographic keys and other information by monitoring the power consumption of cryptographic devices (integrated circuits, etc.). Power monitoring attacks are divided into simple and differential types, depending on the advanced power analysis level. Simple power analysis (SPA) is mostly focused on electrical activity, whereas differential power analysis (DPA) entails a more dynamic method. In addition to monitoring power traces or electrical power, an attacker can also retrieve values from cryptographic calculations.

Notwithstanding the foregoing, electromagnetic attacks are carried out by measuring the electromagnetic radiation emitted from a device. The attacker analyses and captures the results of a mined signal. The amount of radiation depends on the operation's identity, which enables the attacker to capture the performed operation and to find the encryption keys. The RSA algorithm, in particular, is prone to electromagnetic attacks.

Another frequent exploit is the differential fault analysis (DFA), which is known as the technique of fault injections in the device's cryptographic algorithms. In other words, it is an attempt to modify the computation of an algorithm. These modifications generate 'falsified' output ciphertext, allowing thus an attacker to retrieve the key candidates with differential cryptanalysis techniques. Consequently, the correct key can be retrieved with continuous fault injections. Symmetric block ciphers and public key algorithms, are specifically affected by the DFA.

In the previous years, Rowhammer attacks have also been detected in Android devices. According to researchers [14], an attacker can bypass the Android permission system to have full access of the device. As reported in experimental studies, disturbance errors that have been created in the row-level of a DRAM (Dynamic Random-Access Memory) can affect other memory rows as well [14].

Hardware trojan horses can also significantly impact a hardware device [6]. These, as dubbed, pertain to alterations in the electronic circuit of a chip during the fabrication phase [6]. When triggered, this malware can either create malfunction in the device or steal the secret key for the cryptographic application [15].

Buffer overflow and Cross-Site Request Forgery (CSRF) attacks have also been mentioned in recent years. For instance, the Belkin F9K1122 wireless range extender was affected by a CSRF, whereas the ZyXel NBG6716 wireless router underwent a buffer overflow attack [16].

III. Detection and Protection Methods

The continuous increase in malware associated with IoT devices has raised the need for stable and efficient detection and protection methods. In some cases, the numbers have shown that the current detection and protection methods are not efficient enough. Suffice to say that according to [17], 400,000 IoT devices have been found accessible on the internet, including IP cameras and other devices. This means that except for the insufficient detection/protection methods, one of the most severe threat, remains people's unawareness. The current malware detection methods fall into three (3) categories: Signature-Based Detection, Static Detection and Dynamic Detection [10].

As the most common method, Signature-Based Detection depends on antivirus/antimalware systems' signatures. The signature is interbred via an updated malware database, whereby the malware is detected if the results are verified. This method is considered inappropriate for devices with insufficient memory [10].

Static methods are based on the device's static characteristics and resources. The absence of dynamic tracking mechanisms, prevents the detection threats that appear at run-time [10]. Static methods are in most cases low-resource-consuming and lightweight [18]. Other experimental surveys have shown that through binary obfuscation techniques and by loading opaque constants into a register, a static detection tool cannot identify the transformed values. This experiment clearly

identifies the 3SAT problem, providing limits in static detection methods when an obscure malicious code runs in a program [19].

In contrast, dynamic detection methods can detect malicious functionalities by pinpointing abnormal activities, such as network behavior, power consumption, CPU load, calls, SMS, virtual memory, etc. They are considered as promising due to their ability to detect malware at run-time and their resistance to malware obfuscation [10]. Finally, the best protection from malware can be obtained, by using both static and dynamic approaches, and investigating potentially malicious applications behavior from both aspects.

IV. Current Situation & Future Directions

Taking into consideration the continuous increase in IoT devices and the multidimensional threats that have arisen over the past years, the current situation would be described as quite worrisome. According to the 2016 results, 68% of the worldwide population uses an Android device, while 87% of Android users had an outdated Android version. Furthermore, 1,723,265 new malware samples had been verified until the first half of 2016 [9].

In order to keep pace, with increased number of IoT devices also the detection solutions have to be improved and made more resistant to security threats that appear with time. However, having in mind the resource constrained environment of most of IoT devices, running complex malware detection and protection solutions on them is almost prohibited. This opens up new research challenges, on how to both effectively and efficiently protect these devices. One of the works that proposes both effective and efficient solution for runtime on-device mobile malware detection is presented in [18]. This work focuses and tests the detection performance of the proposed method, on the detection of malware on mobile devices, but the authors suggest its usage also for other resource-constrained devices of IoT. In the near future, we expect to see more works in this direction, which would focus on low-power, low-cost solutions for protection of IoT devices, against malware.

As aforementioned, an attack can start from the chip's fabrication level and the current functional testing techniques cannot ensure the security of the components. Hence, a lack of trust is reflected in the manufactured hardware [16]. Apart from developing more effective and accurate detection solutions for malicious software, new defenses are required related to the processor-level backdoors and the post fabrication testing methods. Moreover, further research should take place in the device's physical level, with a particular emphasis on the physical implementation of the cryptosystem. As such, the defenses should start from within.

V. Conclusions & Outlook

Malware and its exploits, whether referring to hardware or software levels, remain the Achilles' Heel in modern systems implementation. Since both the creation of malware and the attacker's intention cannot be eliminated, it is in the best interest of all parties concerned to invest in technology advances related to secure IT environments in order to minimize threats and take corrective action concerning malicious attacks. In this paper, we introduce a detailed of the currently existing software and hardware malicious threats, so as of existing detection methods. Additionally, we present a state of the art analysis of current situation of the IoT security, which is followed by envisioned research directions in both software and hardware.

Acknowledgment

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

References

1. Symantec, "ISTR, Internet Security Threat Report", Symantec, April 2016.
2. IDC, www.idc.com, 2016.
3. OWASP, www.owasp.org, 2016.
4. V. Harrison and J. Pagliery, "CNNMoney", CNNMoney (London), April 2015.
5. K. Yang, M. Hicks, Q. Dong, T. Austin and D. Sylvester, "A2: Analog Malicious Hardware", 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016.
6. G. Kalogeridou, N. Sklavos, A.W. Moore, O Koufopavlou, "On the Hardware Trojans Detection, using Mixed-Signal ICs", proceedings, workshop on Trustworthy Manufacturing and Utilization of Secure Devices, Conference DATE 2015, Grenoble, France, March 9-13, 2015.
7. N. Sklavos, "Securing Communication Devices via Physical Unclonable Functions (PUFs)", Information Security Solutions Europe (isse'13), Brussels, 22-23 October, Belgium, 2013, pp. 253-261, Springer, ISBN: 978-3-658-03370-5.
8. Nokia, "Nokia Threat Intelligence Report", 2016.
9. G DATA, "G DATA Mobile Malware Report", G DATA, 2016.
10. J. Milosevic, F. Regazzoni and M. Malek, "Malware Threats and Solutions for Trustworthy Mobile Systems Design", Hardware Security and Trust, Design and Deployment of Integrated Circuits in a Threatened Environment, Switzerland: Springer, 2017, pp. 149-157.
11. Available online: www.krebsonsecurity.com, 2016.
12. M. Katsaiti, A. Rigas, I. Tzemos, N. Sklavos, "Real-World Attacks Toward Circuits & Systems Design, Targeting Safety Invasion", proceedings of the International Conference on Modern Circuits and Systems Technologies (MOCAST'15), Thessaloniki, Greece, May 14-15, 2015.
13. 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.
14. Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. Lai and O. Mutlu, "Flipping Bits in MemoryWithout Accessing Them: An Experimental Study of DRAM Disturbance Errors", 2014.
15. S. S. Chandra, B. N. Biswal, S. K. Udgata and J. K. Mandal, Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014: Volume 2, Springer, 2014.
16. Available online: www.csoonline.com, 2016.
17. SENRIO, http://blog.senr.io/, 2016.
18. J. Milosevic, A. Ferrante and M. Malek, "MalAware: Effective and Efficient Run-time Mobile Malware Detector", IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, Lugano, Switzerland, 2016.
19. A. Moser, C. Kruegel and E. Kirda, "Limits of Static Analysis for Malware Detection", Technical University Vienna, Vienna, 2007.