УДК 47.03.07

SECURITY ISSUES IN TEST AND REPAIR INFRASTRUCTURE FOR SYSTEMS-ON-CHIP

Harutyunyan G. [*]**, Shoukourian S.** [**]**, Tshagharyan G.** [***]

[*]Yerevan State University
Armenia, Yerevan
h.gurgen@yahoo.com
[**]Yerevan State University
Armenia, Yerevan
samshouk@sci.am
[***]Yerevan State University
Armenia, Yerevan
grigor.tshagharyan@gmail.com

Abstract – The rapid development in the modern technology and its widespread utilization in number of applications brings in new challenges that should be addressed. Security is one of such challenges that has grown into a major concern over the years. Periodically new incidents of data and system breaches are reported. For this purpose, usually different side channels in the system are being exploited by the attackers to bypass the protection mechanisms. Especially vulnerable with this regard is the traditional test and debug infrastructure placed on the System on Chips (SOC) which provides an alternative path into the chip internal structure. The aim of this paper is to present a comprehensive overview of various security aspects of SOCs including the known threat models, classes of attackers as well as existing techniques for securing test access.

Keywords: security, test and repair, countermeasure, attack, system on chip.

Introduction

It is already commonly acknowledged fact that security is one of the critical challenges in 21st century. In the modern world the trends in nearly every semiconductor industry segment are towards electronization. Today electronics can be found everywhere and the end-use markets are manifold including traditional applications like military and aeronautics, and quickly spreading to highly progressing automotive, Internet of Things (IoT) and biomedical applications. The worldwide spread and utilization of personal computers, various handheld and mobile devices, highly computerized equipment make a room for the plenty of security risks and challenges that should be addressed by the community. There are number of evidences showing how even the smallest flaws in security mechanisms of any system can be maliciously utilized to completely break the system. Several of the accidents reported in [1]-[5] prove that even the worldwide known companies’ products and systems in various spheres are not guaranteed against vulnerabilities that eventually can be discovered and maliciously exploited.

To build a robust system, security aspects should be paid an immense attention at all stages of system design. Security should be built in right from the beginning of system design. The cost of detecting security holes and system vulnerabilities and then fixing them increases with each step of the design process, so it is of critical importance to do it as early as possible. From the security perspective it is important to pay attention to closing all the possible backdoors and side channels that attackers can use for bypassing the security. One of such channels should be considered also traditional test and debug access ports of SOCs and surrounding test infrastructure.

Testing aspects of SOCs were always paid high importance since insufficient testing may result into manufacturing defects being undetected and therefore considerable yield loss. Test and debug operations are usually realized by inserting specific Design for Testing (DFT) structures in the chip therefore increasing the observability over the chip. In the meantime, the risk of security threats increases simultaneously. Test structures can be maliciously used as a side channel for accessing the confidential information stored in the system, data theft, reverse engineering, counterfeiting as well as other scan-based attacks. Testability and security are basically contradicting terms since security's goal is exactly the opposite to testability, i.e., to limit the controllability and observability of the chip. In the next sections of the paper more details will be provided on various security aspects within SOCs and the known threat mechanisms with corresponding countermeasures.

IoT and Automotive: Two main security drivers

During the recent years the semiconductor industry has evolved significantly. The share of electronic and electrical systems and components in modern applications is constantly increasing at higher rates and the main contributors to this growth are IoT and automotive. IoT defines a variety of applications starting from simple sensors to more advanced systems that require leading-edge control techniques, rich graphic content and more. IoT is an extremely fragmented market and can be considered as anything from sensors to servers. IoT basically consists of several layers which are in constant communication with each other. The outer layer consists of smart "Things", i.e., so called edge devices with sensors and actuators which main function is to monitor and control. These devices are connected to the central processing unit, otherwise called "cloud", which analyzes the data and provides other relevant services. In between there can be one or many aggregation layers which may consist of hubs and gateways providing interface to collect and send the edge data to the cloud.

The automotive is yet another fast growing industry segment which drives the modern world. The tendency for greater safety and better driving experience is forcing automakers to continually integrate large amount of Electronic Control Units (ECU) like Advanced Driver Assistance Systems (ADAS) and In-Vehicle Infotainment (IVI) into their vehicles. Few examples of such systems are adaptive cruise control, parking assistance, automotive emergency braking, lane change assistance and so forth as this list continues growing. Furthermore, automakers are forced to adopt aggressive technology shrinking strategy to increase computing power and communication performance which poses additional security and safety challenges.

In both IoT and automotive not only the electronic devices and systems themselves are vulnerable to attacks but the connectivity between them and the cloud gives rise to even more threats including:

- Theft & replacement of credentials
- Rogue devices connected to the network
- Software and IP theft or tampering
- Cloning
- Snooping of sensitive data

There are number of reported accidents of security breaches that show how even the smallest security flaws can be discovered and used to break the system security. For instance, the unsecure cellular access (rogue access through Internet) was used to tamper the firmware in Jeep Cherokee and remotely stop it on the highway with the driver in it [3]. Another example is a security breach found on Tesla’s Linux operating system which allows to gain access to the instrument cluster [4]. Eventually this gave the hackers permissions to remotely unlock the door of the car, take over control of the dashboard computer screen, open the trunk or even fold in the wing mirrors while the vehicle was in motion.

No less important are data breaches which are just getting larger like the one with half a billion users accounts leaked from Yahoo servers [5]. The IBM research in [6] found that while many companies happily invest money in developing exciting new features for mobile application users, they are more conservative when it comes to spending money on cybersecurity within those applications. The fact is that this is characteristic for nearly every industry segment. In this connected era when up to billions of devices are connected to each other one weak spot is enough to compromise the security of the whole network. As IoT and automotive markets continue to grow, so does the attack surface and exploitable vulnerability volume. Lack of widely adopted security standards and big fragmentation hinders the interoperability therefore making the security one of the biggest challenges to face.

System Security Considerations and Classification of Threats

When considering security specifications for any SOC, several important aspects are necessary to be considered before moving on with the actual system design. This includes but not limited to understanding classes of potential attackers, identifying critical assets of the system, calculating the security budget and so forth. Consideration of these aspects may allow to obtain the material understanding of system’s security threats, needs and scales in advance and use this knowledge as a guideline for secure system design.

First, it is important to understand who can stand behind the possible attacks and benefit from breaking the system security. Usually three major classes of attackers are considered:

- Insiders: People working in the same organization who have potential access to the system and/or have substantial knowledge of the system internal structure.
- Outsiders: Spans over a large spectrum of people from curios individuals to professional intruders. They usually do not have a sophisticated awareness of system design, but use their technical knowledge and experience to identify the weaknesses of the system to break though.
- Funded organizations: Consist of the group of specialists with advanced technical skills, big budget, and specialized equipment. This class can include both crime and governmental organizations.

Another important aspect of SOC design is to evaluate assets of the system which need protection and align them with its security budget. This does not refer only to amount of money, but also spent time and efforts. Each security feature requires considerable time and efforts for development as well as for qualification and validation. The more complex is security feature, the more accurate analysis is needed for it to avoid further exploitable flaws. Moreover, security implies considerable overhead in terms of performance and area depending on implemented security features. If this overhead is not preserved in the reasonable range, then security may become a headache rather than a solution. So there is always a trade-off between value of the system and cost of security to consider when designing protection mechanisms.

Next challenge is defining the SOC operation modes that need protection. There are usually three different modes considered, which have their specifics and possible threat scenarios such as listed below:

- Manufacturing, test and silicon debug – malicious 3rd party individuals, tools or IPs trying to learn chip information
- Standalone chip – hacking for reverse engineering or counterfeiting
- In-field operation (mission mode) – accessing, modifying, or tampering sensitive data by switching to test mode

Finally, the most critical is to understand the threat environment at every stage of SOC development starting from its design up to the final test and deployment. There are 3 main categories of attacks to consider:

- Communication attacks
  - Sniffing of sensitive data (e.g., passwords, credentials, keys)
  - Remote attacks (exploiting system backdoors)
- Software attacks
  - Malware (viruses, worms, rootkits, spyware)
  - Exploit of buffer/stack overflows to access sensitive information

    - Taking advantage of weak implementation of protocols, cryptography, or passwords
- Physical (Hardware) attacks
    - Outside the package (using existing interfaces, JTAG/test ports, side channels)
    - Inside the package (decapsulation, probing, laser)

As software evolved from stand-alone applications to internet applications and controlled devices, the concerns of software products have shifted. While in the beginning it was quality only, with the internet, security became a key concern as well. The potential damage of malfunctioning software has increased dramatically. Crashing standalone software applications were generally annoying but tolerated as a "fact of life". This was also re-enforced by weak product liability regulations and broadly protective software license terms. Lack of software security previously also caused certain problems like financial damage directly (i.e., money loss) or indirectly (i.e., brand name) but as soon as devices are becoming controlled by software, the story changes dramatically. Health and human lives are suddenly put at stake and potential liability is unbounded.

Hardware in contrast to software was always considered as the main source of attacks. Physical or hardware attacks by their nature can be classified as

- noninvasive attacks - which do not damage the chip package, and
- invasive attacks - which require chip disassembling

Noninvasive attacks are especially dangerous since the compromised system might not even notice that the secret information has been stolen. Below are shortlisted the most common classes of attacks.

Brute-force attack – is the simplest form of the attack where the attacker uses an exhaustive search technique for breaking the system security. With the computer hardware speed increasing over the time, it becomes the matter of days or even hours to obtain the correct pass code if it is not long and complex enough.

Side-channel attack – aims to exploit peculiarities of physical implementation of the system and requires sufficient technical knowledge and usually also specialized equipment [7]. Virtually attackers can maliciously use any information about the system like timing, temperature, sound, electromagnetic radiation, power consumption and so forth.

Fault injection attack – can also be considered as a type of side channel attack. As the name suggests the idea is based on tampering the system via deliberately injecting faults. The aim is to affect the internal or external conditions in the system like supply voltage or temperature causing its malfunction (e.g., [8]).

Scan-based attack – another type of attack which started to gain popularity recently targeting the malicious use of chip's DFT infrastructure. Test scan chains and test interfaces can be exploited as a side channel for accessing the confidential information stored in the system, breaking cryptographic primitives and so forth (e.g., [9]).

Hardware Trojan attack – is realized in the form of malicious modifications of a hardware which can result in functional changes of the system [10]. This can be done either by the rogue employees (insiders) or by untrusted foundries during the chip design or fabrication process. Hardware Trojans may vary per their physical implementation, triggering conditions and severity of the caused damage.

Microprobing attack – is a more advanced type of a security threat. Unlike the previously discussed noninvasive types of attacks, microprobing attack is an invasive attack meaning that during this type of attack, attackers are capable of depackaging the chip and obtaining access to the chip internal structure [11]. However, these types of attacks require professional equipment and large budget as well as sufficient technical knowledge.

Common Approaches for Secure Testing

In most of the cases the test infrastructure of the system is constructed using scan architecture built upon known test interface standards developed by the IEEE working groups over the years. This includes both IEEE 1149.1 and IEEE 1500 as well as recently ratified IEEE 1687 (or IJTAG) standards. Nevertheless, all the described test interfaces are not inherently designed with built-in protection mechanisms which makes them the easy target for the intruders. Building secure test infrastructure is relatively new sphere and therefore there is still a plenty of work to be done. However, number of solutions are already proposed in the literature for securing test interfaces as well as scan network consisting of individual scan chains, most common of which are discussed below.

TAP (e.g., most frequently JTAG) is usually the test interface used at system level providing access to the internal test structure of the system. One of the light-weight solutions for protecting access to TAP may be permanently disabling the test infrastructure on the chip or disabling the switching between the mission and test modes after the manufacturing. However, this may not be acceptable solution for many applications which require in-field test and debug capabilities. Therefore, several alternative techniques have been proposed in the literature (mainly based on JTAG standard) which aim to protect the system from unauthorized access. For instance, a solution proposed in [12] suggests adding the capability to reset the system and perform an initialization process every time the chip switches from test mode to mission mode or vice versa.

However more sophisticated solution is based on challenge-response based authentication scheme which suggests that one of the parties presents the challenge while the other should provide a valid response in order to be authenticated. In the simplest case the password-based authentication mechanism is added to the JTAG which requires users to enter valid credentials to gain access to the system (e.g., [13]). A little bit more complex but more advanced approach is based on using the public-key or private-key cryptography for the user authentication (e.g., [14]). Even more sophisticated approach proposed in [15] suggests utilizing the concept of multi-level hierarchical permission system to control the individual users or user's groups access to the system.

There are also several techniques proposed which aim to protect individual scan chains from illegal access via locking mechanisms. Some of the them are "flipped scan tree" [16] and "Lock and Key Technique" [17]. In case if the test scan architecture on the chip is built on the base of IEEE 1687 there are secure solutions proposed as well. The central idea here is protecting reconfigurable scan networks (RSN) which are realized via the gateways called segment insertion bits (SIB) for dynamically configuring the test paths to the instruments. In [18] authors proposed inserting the separate authorization instrument while in [19] an alternative approach is proposed suggesting to replace the SIBs with so-called Locking SIBs (LSIB) requiring certain key value to be scanned into the network for unlocking. At last, similar key-based techniques were also proposed to be embedded into 1500 Standard Test Wrapper to protect the embedded cores from unauthorized access (e.g., in [20]).

Conclusions

With current tendencies in IoT and automotive markets, the share of electronic components in such applications is continually increasing bringing in new challenges. Among those security is highlighted as one of the most critical. This paper first focuses on considering different aspects of security including the system's security needs, possible attacker types, and the classification of well-known threat models. Among the latter, scan-based attacks are getting increasingly popular since the traditional test architecture provides enhanced observability and controllability over system therefore contradicting the idea of security. At last, the comprehensive overview of existing countermeasures against scan-based attacks is presented.

References

1. https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix, [Online].
2. https://www.usatoday.com/story/tech/2015/02/15/hackers-steal-billion-in-banking-breach/23464913, [Online].
3. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway, [Online].
4. https://electrek.co/2016/09/27/tesla-releases-more-details-on-the-chinese-hack-and-the-subsequent-fix, [Online].
5. https://www.usatoday.com/story/tech/2016/09/22/report-yahoo-may-confirm-massive-data-breach/90824934, [Online].
6. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03074BEEN, [Online].
7. B.-E. Hagai, “Introduction to side channel attacks”, Discretix, White Paper, 2010.
8. J.K.R. Sastry, J.S. Bhanu, and K. SubbaRao, “Attacking embedded systems through fault injection”, Emerging Trends and Applications in Computer Science (NCETACS), 2011, pp. 1-5.
9. S. S. Ali, O. Sinanoglu, S. M. Saeed, R. Karri, “New scan-based attack using only the test mode”, IEEE 21st International Conference on Very Large Scale Integration (VLSI-SoC), 2013, pp. 234-239.
10. S. Narasimhan, W. Yueh, X. Wang, S. Mukhopadhyay, S. Bhunia, “Improving IC security against Trojan attacks through integration of security monitors,” IEEE Design & Test of Computers, vol. 29, no. 5, pp. 37–46, Oct. 2012.
11. S. Skorobogatov, “Introduction to Hardware Security and Trust: Physical Attacks and Tamper Resistance”, Springer New York, 2012, pp. 143-173.
12. D. Hely, F. Bancel, M.-L. Flottes, B. Rouzeyre, “Test Control for Secure Scan Designs”, European Test Symposium (ETS), 2005, pp.190-195.
13. F. Novak and A. Biasizzo, “Security extension for IEEE std 1149.1”, Journal of Electronic Testing, vol. 22, no. 3, pp. 301–303, June 2006.
14. K. Rosenfeld, R. Karri, "Attacks and Defenses for JTAG", IEEE Design & Test of Computers, vol.27, no. 1, pp. 36-47, January-February 2010.
15. L. Pierce, S. Tragoudas, “Enhanced Secure Architecture for Joint Action Test Group Systems”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 21, no. 7, pp. 1342-1345, July 2013.
16. G. Sengar, D. Mukhopadhayay, D. R. Chowdhury, “An Efficient Approach to Develop Secure Scan Tree for Crypto-Hardware”, International Conference on Advanced Computing and Communications (ADCOM), 2007, pp. 21-26.
17. J. Lee., M. Tehranipoor, C. Patel, J. Plusquellic, “Securing Designs against Scan-Based Side-Channel Attacks”, IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 4, pp. 325-336, October-December 2007.
18. R. Baranowski, M. A. Kochte, H.-J. Wunderlich, “Fine-Grained Access Management in Reconfigurable Scan Networks”, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 6, pp. 937-946, June 2015.
19. J. Dworak, A. Crouch, J. C. Potter, A. Zygmontowicz, M. Thornton, “Don't forget to lock your SIB: hiding instruments using P1687”, International Test Conference (ITC), 2013, page 1-10.
20. G.-M. Chiu, J.C.-M. Li, “A Secure Test Wrapper Design Against Internal and Boundary Scan Attacks for Embedded Cores”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 20, no. 1, pp. 126 – 134, Jan. 2012.