ISSN 2672-1562
VOL. 6

The 6th International Conference
on Next Generation Computing 2020

ICNGC 2020

Dates December 17(THU) ~ 19(SAT), 2020

Venue Shilla Stay Haeundae, Busan, Korea

Organized by | 사단법인 한국차세대컴퓨팅학회 Korean Institute of Next Generation Computing

Sponsored by | IITP 정보통신기획평가원 TRACOM

Neutralizing Side-Channel Attacks Through Hardware Uniqueness Derivation

Hye-lim Jung
Department of Information Security
Sejong Unverysity
Seult, South Korea
Hyello13@gmail.com

Sung-Kyu Ahn
Department of Information Security
Sejong Unverysity
Seult, South Korea
yiimfn@gmail.com

Ki-Cheol Choi
Department of Information Security
Sejong Unverysity
Seult, South Korea
gichoel0295@gmail.com

Jae-Kyung Ju
Department of Information Security
Sejong Unverysity
Seult, South Korea
jj01020905906@gmail.com

Ki-Woong Park
Department of Information Security
Sejong University
Seoul, South Korea
woongbak@sejong.ac.kr
(Correspondence author)

***Abstract*—Side-channel attack techniques include attack techniques that analyze the circuit power of a device to obtain information, enabling it to steal the critical information and encryption keys of a terminal. Herein, we propose an internal trade mechanism that renders the attacker incapacitated when analyzing the power communicated between computing chips. This mechanism allows OTP(One Time Password) to be performed based on the unique information of only the corresponding chip using a hardware security chip through encrypted communication between chips. This mechanism applies OTP based on the unique information of this chip using a hardware security chip through encrypted communication between chips. The internal trade mechanism proposed herein cannot replay an attack even if an attacker probes the communication for analysis and can provide reliability for data received between chips.**

Keywords—Embedded system; Side-channel attack; Security communication

I. INTRODUCTION

The side-channel attack is an attack technique in which an attacker steals critical information by analyzing physically generated information, such as sound, power, and computation time [1,2]. As a side-channel attack technique, probing attack is a method of analyzing power by probing the current flowing through an electronic device circuit [3,4]. For example, in 2010, a case of successful cracking by microprobing the memory of the Infineon TPM(Trusted Platform Module) chip was reported [5]. In this case, an attacker can perform an attack to steal the encryption key by analyzing the power flow obtained through probing. When such a side-channel attack is performed on a device such as an IoT(Internet of Things) device as an attack target, the attacker can obtain internal critical commands, data, and encryption keys. Through this process, the attacker can leak information, damage the IoT device, or communicate malicious information to the server.

Herein, we propose an internal trade mechanism to protect the communication between chips from side-channel attacks. This mechanism can provide communication with the uniqueness and confidentiality of only such chips by generating an OTP(One Time Password) based on the challenge/response of a PUF(Physical Unclonable Function) chip. A PUF chip is a hardware security chip that can perform challenges/responses based on device-specific features and generate signature values [6,7]. [Figure 1] shows the replay attack and main attributes described earlier. A replay attack is an attack that causes an abnormal operation of the target chip by intercepting the transmitting and receiving data of the target chip. The application of the mechanism can neutralize the replay attack because the key used for communication will change even if the side-channel attack is performed as an attacker. Furthermore, it can prevent the leakage of important data or commands and provide reliability for falsified/modified data and commands.

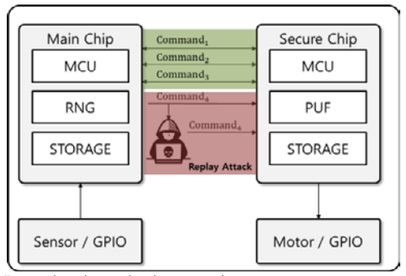

Fig. 1. Internal trade mechanism overview

This paper describes the benefits of related studies and the main contributions in Section 2. Section 3 describes the process related to the main contribution of this study in detail. Section 4 concludes this paper.

II. RELATED WORK

This section describes related studies [8,9] pertaining to the internal trade mechanism proposed herein as well as the advantages of the proposed mechanism. The first related study implemented a hardware authentication mechanism to secure nonvolatile memory vulnerable to side-channel attacks.

In that study, security tests were implemented to test IP blocks by applying a PUF-based authentication mechanism to reduce overhead. Furthermore, the authentication mechanism of NVM(Non-Volatile Memory) was implemented by applying the Hamming distance challenge to prevent replay attacks.

The second related study presented a solution to prevent external intrusion during communication by continuously changing the baud rate during the UART(Universal asynchronous receiver/transmitter) communication process, which is a chipset protocol. In that study, an automatic baud rate detection function was added to the transmit/receive chip to enable normal interchip communication during continuous baud rate changes.

The solution presented by the abovementioned study is suitable for long-distance communication, high-speed communication, and low-cost communication environments, i.e., characteristic of UART communication; however, it has a limited baud rate range. Therefore, if an attacker invests sufficient time to perform an attack, communication reliability may not be guaranteed. Herein, we propose a system that is secure against random attacks using PUF chips to solve the security limitations of interchip communication, which is restricted owing to physical limitations, and generates random encryption key values through the challenge–response mechanism.

III. INTERNAL TRADE MECHANISM

When communicating between chips inside an IoT-based hardware device, an attacker can leak data through a probing attack that analyzes the communication using an oscilloscope or a logic analyzer. To prevent such attacks, a method to protect data such as critical data or core commands inside IoT devices is required when they are exposed during internal data communication. Various IoT solutions have been investigated to solve this problem. However, another vulnerability targeting IoT devices such as replay attacks or side-channel attacks may occur. Herein, we propose an internal trade mechanism to defend against side-channel attacks, including probing and replay attacks. The mechanism proposed herein minimizes the leakage of important information or command data from devices. As this mechanism prevents forged/modified data or commands from being injected into the chipset inside the IoT device by an attacker, it can guarantee the communication reliability of the chips inside the IoT device.

The structure of the internal trade mechanism proposed herein can be categorized into the main chip, which performs the general role of the IoT device; and the secure chip, which performs the important operation. The main chip generally collects and analyzes data (IoT device sensor, GPIO input, etc.) and contains an MCU(Micro Controller Unit) and RNG(Random Number Generator) for general operations.

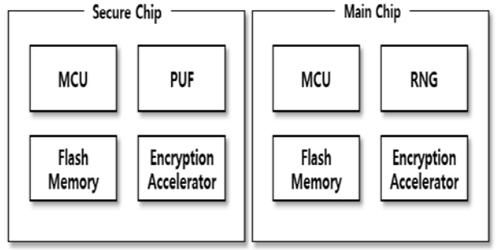

Fig. 2. Structure of internal trade mechanism model

Actions based on data collected from the main chip, such as GPIO output and data transmission, are performed by the secure chip. The secure chip has a chip set that provides PUF

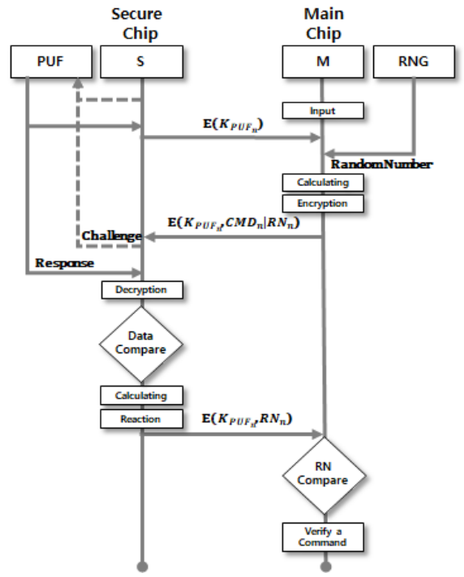

Fig. 3. Sequence diagram of internal trade mechanism

function internally.

IV. STRUCTURE OF INTERNAL TRADE MECHANISM

The structure of the internal trade mechanism proposed herein is composed of a main chip and a secure chip. When the device operates for the first time, the secure chip acquires a response by performing a random challenge to the PUF operating inside. The PUF's response is shared with the main chip through the elliptic-curve Diffie–Hellmann encryption.

A. Internal trade mechanism process

The main chip receives external inputs such as sensor input or GPIO(General-Purpose Input/Output) input, analyzes the input data, and generates a command to yield the appropriate output for the input. The command is merged with the RN(Random Number) generated from the RNG of the main chip and then encrypted using the PUF key received from the secure chip. The encrypted RN and command are transferred to the secure chip. The secure chip inputs the same challenge value as the previously created challenge value into the PUF to obtain the response value; subsequently, it uses this response value as a key to decrypt the encrypted command and the RN received from the main chip. The secure chip controls the operation of devices such as IoT sensors or motors based on the normally decoded commands. Furthermore, the secure chip encrypts the RN received from the main chip with the PUF value. If the decrypted data cannot be executed or is in an abnormal data format, then an abnormal operation or a replay attack by an attacker is assumed. The RN encrypted with the PUF key is delivered to the main chip. The main chip decrypts the received encrypted RN using its PUF response value and compares it with the RN used for command transmission. If the RN does not match, then an abnormal operation or command injection by an attacker is assumed.

V. Conclusion

During communication between chips inside an IoT hardware device, an attacker can detect data through a probing attack that analyzes the communication. To prevent such an attack, a method to protect sensitive data or data such as key commands are required during internal data communication. Herein, we proposed a countermeasure mechanism for side-channel attacks as an attack that can occur in IoT devices.

Acknowledgment

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grants funded by the Korean government (MSIT) (No. 2019-0-00426) and supported by National Research Foundation of Korea (NRF) grants funded by the Korean government (NRF-2020R1A2C4002737).

References

[1] Daniel Genkin, Itamar Pipman, Eran Tromer, Get your hands off my laptop: physical side-channel key-extraction attacks on PCs, proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2014, LNCS 8731, 242-260, Springer, 2014

[2] Rostami, Mohamad, Farinaz Koushanfar, and Ramesh Karri. "A primer on hardware security: Models, methods, and metrics." Proceedings of the IEEE 102.8 (2014): 1283-1295.

[3] Briais, S., Cioranesco, J. M., Danger, J. L., Guilley, S., Naccache, D., & Porteboeuf, T. (2012, September). Random active shield. IEEE Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 (pp. 103-113).

[4] Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., & Whelan, C. (2006). The sorcerer's apprentice guide to fault attacks. Proceedings of the IEEE, 94(2), 370-382.

[5] " Unhackable" Infineon Chip Physically Cracked, Fox Business, http://www.foxbusiness.com/personalfinance/2010/02/11/unhackable-infineon-chip-physicallycracked/ Feb. 2010.

[6] S. Kalanadhabhatta, D. Kumar, K. K. Anumandla, S. A. Reddy and A. Acharyya, "PUF-Based Secure Chaotic Random Number Generator Design Methodology," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 7, pp. 1740-1744, July 2020.

[7] DS28E50, DeepCover Secure SHA-3 Authenticator with ChipDNA PUF Protection, maxim integrated, https://datasheets.maximintegrated.com/en/ds/DS28E50.pdf

[8] Rajgure, Eshant G., and Ajay P. Thakare. "The Novel Technique For Channel Security using UART." 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE). IEEE, 2014.

[9] Das, Amitabh, et al. "PUF-based secure test wrapper design for cryptographic SoC testing." 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2012

Operational Fuzzy Control and Crisp Rules for a Creative 3D Assembly

Sanguk Noh
School of Computer Science and Information Engineering
The Catholic University of Korea
43 Jibong-ro, Wonmi-gu, Bucheon-si, Gyeonggi-do 420-743, Republic of Korea
sunoh@catholic.ac.kr

***Abstract*—This paper presents the testing and evaluation of a simulator for the operational control of a creative 3D assembly. We model the 3D assembly as a moving agent, which generates a sequence of actions according to graphical programming block scripts previously defined at any given domain. To guide or control the operation of the 3D assembly, we accumulate crisp if-then rules into the knowledge base, and we also provide a fuzzy control system which consists of a set of fuzzy variables, membership functions for fuzzy variables, and a set of rules specifying the relationship between fuzzy input and output variables. We develop an interpreter that generates standard XML scripts from graphical programming blocks, which can then be converted to a C# object. The simulator that we implement processes both crisp logical rules to determine an exact action at a discrete condition and fuzzy logical rules to control the fuzzy actions of the 3D assembly given continuous input values of a situation. We experiment with our simulator and a variety of graphical programming blocks to test and evaluate the operational control of the creative and movable 3D assembly in simulated settings. In the experiment, the assessment includes (1) the definition of three types of motion, control, and data blocks, (2) the generation of XML scripts, and (3) the execution of both crisp and fuzzy logical rules, respectively.**

Keywords—testing operational control; crisp and fuzzy logical rules; graphical programming blocks; creative 3D assembly

I. Introduction

In an interdisciplinary and applied educational environment pursued by our research project, students from elementary school to high school can build creative assemblies with 3D bricks in their own way, and they can also endow the autonomy to the assemblies to properly act in the given situation at hand. We provide the users with graphical programming blocks, which follow SNAP! [1], to define a set of possible actions. We need to translate the graphical programming blocks into the form of scripts, such as XML, which can then be interpreted in various programming applications. Whenever any condition in the scripts is satisfied with input value, the resulting action determined using either a crisp logical rule or a fuzzy logical rule should be executed for the operational control of a 3D assembly.

In this paper, we design and implement a simulator for the operational control of a creative 3D assembly. The simulator shows the creative 3D assembly's behavior that maps any given percept sequence to an action. We model the creative 3D assembly as a moving agent, which generates a sequence of actions according to the scripts previously defined at any given domain. To guide or control the operation of the creative 3D assembly, we accumulate crisp logical rules represented as if-then rules into the knowledge base [2], and construct various knowledge bases for a series of 3D assemblies in discrete settings. We also provide a fuzzy control system [3-8], which consists of a set of fuzzy variables, their membership functions, and a set of rules specifying the relationship between fuzzy input and output variables. Our fuzzy control system deals with vague linguistic adverbs such as 'near,' 'close to,' 'very,' 'slightly,' and so on, representing ambiguity in continuous input and output variables. Thus, our simulator processes both crisp logical rules and fuzzy logical rules for the operational control of creative 3D assembly.

The paper is organized as follows: in the following section, we design the overall architecture of our system, which defines a set of actions using graphical blocks, translates the programming blocks into the script in the format of XML, and decide actions given discrete and continuous input conditions using crisp and fuzzy logical rules. In Section III, we describe three kinds of programming blocks, which consist of variable blocks, motion blocks, and control blocks. We further implement our simulator and, in Section IV, experiment with the moving agent based upon graphical programming blocks to test the soundness of both logical rules. In the concluding section, we summarize the testing and evaluation of our simulator and discuss further research issues.

II. Implementation of Simulator

In our research project, we are focusing on the real world applications of creative and challenging problem solving. For this purpose, students utilize 3D bricks to build movable creative assemblies. Before the students are working on real assemblies, they plan to define a set of actions for the complete creative assembly, and try to test its operational correctness. In this paper, we provide students with a visual programming language to define the actions of the assemblies, and also a simulated testbed to verify their behaviors given a situation at hand. The overall flow of our system for the operational control of creative 3D assemblies is shown in Fig. 1.