Multiple PUF-based lightweight authentication method in the IoT

Seungyong Yoon, Byoungkoo Kim, and Yousung Kang
Cryptographic Engineering Research Section
Electronics and Telecommunications Research Institute
Daejeon, Republic of Korea
{syyoon, bkkim05, youskang}@etri.re.kr

2021 International Conference on Information and Communication Technology Convergence (ICTC) | 978-1-6654-2383-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICTC52510.2021.9620972

***Abstract*— This paper relates to lightweight authentication technology for Internet of Things (IoT) devices using Physical Unclonable Function (PUF). In particular, it relates to a lightweight authentication technique applicable to resource-constrained IoT devices with minimal user intervention using PUF in the IoT environment. The proposed scheme uses multiple PUFs to solve the security vulnerabilities and problems of the existing PUF-based authentication methods.**

Keywords—IoT; PUF; authentication

I. Introduction

PUF is a technology that utilizes inherent hardware characteristic information of each device, such as biometric information, for example, a human fingerprint or iris. It is a digital fingerprint technology that has different values even for devices made by the same process [1]. In other words, no matter how identical a device is made, its unique characteristics cannot be duplicated. Therefore, there is no circuit having the same output value to the same input value even if the circuit is produced by the same manufacturing process.

Recently, IoT services have been widely used in various fields such as smart home, automobile, healthcare, smart factory, and smart city. As new and diverse services are provided and spread in the IoT environment, security vulnerabilities and threats are also rapidly increasing. However, since most IoT devices cannot apply the security technology used in the existing PC or server as it is due to power and resource limitations, only a lightweight or minimal security function is applied, or no security function is loaded. There are too many restrictions to implement cryptographic methods and traditional security mechanisms in IoT devices. In addition, IoT devices are faced with challenges in that the device must be safely protected from various cyberattacks and the cost must be low.

PUF, a hardware-based security technology to solve the challenges facing IoT devices, is attracting attention. This is a robust and lightweight solution to secure IoT devices. Compared with classical cryptographic solutions, it has the greatest advantage of being applicable to IoT devices with limited computational resources. PUF technology can be applied to IoT devices to provide security functions such as product certification, firmware integrity verification, device authentication, and real-time key generation. In particular, PUF-based device authentication scheme provides a lightweight, cost-efficient, and ubiquitous application solution, and can perfectly perform secure authentication of the device without any encryption technique.

II. Traditional PUF-based Authentication

Because PUF technology has different response to the same challenge even if the circuit is produced by the same process, the CRPs (Challenge-Response Pairs) of each PUF are used as a means to authenticate. That is, in the manufacturing process step, the CRP database for device authentication is stored and built in the authentication server in advance, and by comparing it with the CRP generated through the PUF of the device, authentication for each device is performed [2]. Fig. 1 shows the overview of PUF-based device authentication.

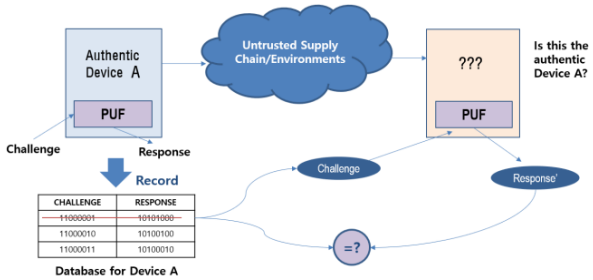

Fig. 1. Overview of PUF-based Authentication

When an authentication request is received from device A, a challenge randomly selected from the CRP database is delivered to the device. The device replies by generating a response to the received challenge through PUF, and the authentication server authenticates the device by matching the response to the challenge stored in database. At this time, the CRP used once is deleted to prevent a replay attack and is never reused. However, this existing PUF-based authentication method has many security threats and vulnerabilities. From the attacker's point of view, if the CRP is known, the attack can be successful by bypassing the PUF-based authentication method. These attacks are possible from three perspectives. Fig. 2 shows the possible attacks of hackers.

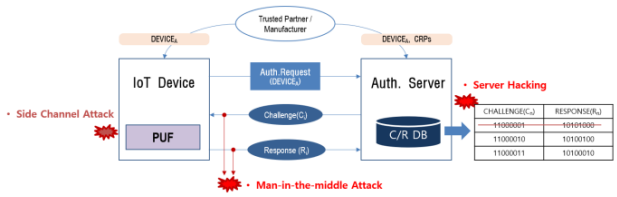

Fig. 2. Possible Attacks

First, a side channel attack is possible from the aspect of IoT devices. Since IoT devices are generally installed in physically accessible places, hackers can easily acquire the device and perform a side channel attack [3]. Second, a man-in-the-middle attack is possible from a communication channel perspective, and CRP prediction is possible by sniffing packets transmitted between the IoT device and the authentication server. With the evolution of artificial intelligence technology, a machine learning-based modeling attack that can predict CRP has emerged, and the existing PUF-based authentication method has been found to be very vulnerable to the attack [4]. Third, the authentication server can be attacked by hackers. If it is hacked, the CRP database for all managed devices is exposed, which is very vulnerable in security.

Researches to counter these attacks are being actively conducted. The response techniques studied so far can be summarized in three aspects.

First, researches to counter side-channel attack in IoT devices is being conducted in the direction of applying physical protection mechanisms or developing a new PUF architecture that is safe for side-channel attack [3]. Second, various methods are being studied for efforts to respond to machine learning-based modeling attack in terms of communication channel. PUF has been originally considered to be unpredictable because it has randomness. However, as the modeling attack succeeded due to the evolution of artificial intelligence technology, it was attempted to improve the robustness of the PUF architecture by increasing the non-linearity [4]. The easiest countermeasure to prevent modeling attack is to encrypt and transmit CRPs. When the attack became known, most of the early solutions took this approach. Such countermeasures cause a significant load on encryption and cannot be applied to resource-limited IoT devices. It also has fundamental flaws that defeat the original purpose of applying PUF to IoT devices. Therefore, recently, the focus is on hiding the direct relationship between PUF's challenge and response without any encryption technique. This is possible by using it in combination with an appropriate authentication protocol. The response generated by the device is post-processed and transmitted by omitting a significant part [5], or padding a sub-string [6], or using the challenge obfuscation technique [7]. After transmission, the receiver also uses challenge recovery techniques. However, these techniques also have disadvantages in that additional processing costs are incurred, the complexity of the authentication protocol increases according to the pre-processing/post-processing of the challenge/response, and the possibility of man-in-the-middle attack still exists. Third, as a countermeasure to prevent the threat of CRP exposure when the authentication server is hacked, the public key of each device is registered in the server, and encrypted transmission and authentication are performed through the private key. Even if the server is hacked, it prevents the exposure of CRP's information (private key). However, this technique also causes a serious load due to the use of heavyweight public key cryptography, cannot be applied to resource-limited IoT devices, and has fatal limitations contrary to the original purpose of applying PUF to IoT.

III. Proposed Multiple PUF-based Lightweight Authentication

A. Proposed Scheme

This paper provides a lightweight authentication method for IoT devices based on multiple PUFs. Unlike the existing PUF-based authentication method, PUF is installed to the authentication server and multiple PUFs are installed to the IoT device. There must be at least two PUFs installed to the device. The configuration of multiple PUFs may include two or more of the same type, or two or more of different types. Various types of PUFs such as Arbiter PUF, Ring Oscillator PUF, SRAM PUF, Resister-Capacitor PUF, and Flash PUF may be applied to the multiple PUFs. Since the PUF itself is very cheap, the cost increase due to the addition of such multiple PUFs is almost insignificant.

In this paper, in order to hide the direct relationship between challenge and response, CRP information of any PUF that is directly mapped is not transmitted or stored. Therefore, it fundamentally blocks CRP exposure threats in case of machine learning-based modeling attacks or server hacking, which are the biggest security threats of existing PUF-based authentication techniques. In addition, there is no need to apply CRP encryption, so no hash or encryption function is used. By providing this lightweight authentication method, it can be applied to any IoT device environment that lacks power and resources. Therefore, this paper provides a lightweight authentication solution to safely protect devices from various security threats faced by IoT devices, thereby further improving IoT security and safety.

The multiple PUF-based lightweight authentication method for IoT devices consists of an enrollment phase and an authentication phase. In the registration stage, unlike the existing PUF-based authentication method, the CRPs of the IoT device are not directly stored in the database of the authentication server. After the challenge-response generation step in the PUF of the authentication server, the challenge-response generation step in the multiple PUFs of the IoT device is performed. In this series of processes, the initial challenge (SC_0) and final response (CR_n) are stored in the CRP database. In order to secure the CRP database to be used in the subsequent authentication, the registration operation is completed by repeating the above-described series of processes. Fig. 3 shows the authentication phase. Device authentication is performed by comparing the CRP of the database stored at the time of registration with the received CRP. Fig. 4 shows in detail the authentication verification of the IoT device.

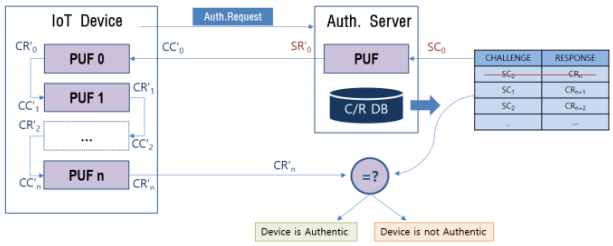

Fig. 3. Authentication Phase

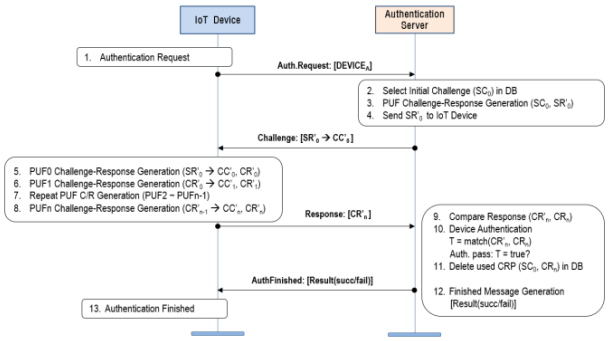

Fig. 4. Authentication Verification

B. *Security Analysis*

The proposed authentication method in this paper can effectively block various existing security threats and attacks.

- Protection against machine learning-based modeling attack: In order for the hacker to succeed in the attack, the minimum number of direct CRPs required for learning, N_{min}, must be obtained. N_{min} depends on the type of PUF and the learning strategy. Based on theoretical considerations (dimension of the feature space, Vapnik-Chervonenkis dimension), it is proposed in [4] that the minimal number of direct CRPs, N_{min}, that is necessary to model a N-stage delay-based arbiter PUF with a misclassification rate of e is given by: $N_{min} = O(N/e)$. The scheme proposed in this paper hides the direct relationship between challenge and response, so that even if a hacker overhears the communication channel between the IoT device and the authentication server, N_{min} can never be obtained. Therefore, it is safe against machine learning-based modeling attacks.
- Prevention of CRP exposure during server hacking: When an attacker hacks the authentication server, the CRP information stored in the database, (SC_i, CR_{n+i}), is exposed. This is not the direct CRP information (SC_i, SR_i) of the authentication server, nor the direct CRP information (CC_i, CR_i) of the IoT device. Therefore, the information acquired by the attacker through hacking cannot be used in the subsequent authentication process, so it is safe from the CRP exposure security threat.
- Protection against response guessing attack: If the length of the response is n, it has an n-*bit* security level. That is, the attacker must perform 2^n attempts to succeed in the attack, which is the same as the complexity of the brute force attack. Therefore, we can defend against guessing attack by setting an appropriate response length.
- Protection against replay attack: Since the CRP ((SC_i, CR_{n+i}) information in the database used once for device authentication is deleted and not used again, it is safe from replay attack.

IV. CONCLUSION

In this paper, a multiple PUF-based IoT lightweight authentication method with minimal user intervention is provided. The biggest problem of the existing PUF-based authentication method, the machine learning-based modeling attack and the threat of CRP exposure during server hacking, is solved by hiding the direct relationship between challenge and response. For this, the structure of multiple PUF is used. In addition, by providing a lightweight IoT device authentication method without any CRP encryption, it can be applied to any IoT device with severe resource constraints.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00230, Development on Autonomous Trust Enhancement Technology of IoT Device and Study on Adaptive IoT Security Open Architecture based on Global Standardization [TrusThingz Project]).

REFERENCES

[1] C. Herder, M. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial", Proceeding of the IEEE, Vol. 102, No. 8, pp. 1126-1141, August 2014.

[2] G. Suh, and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", In Proceedig of ACM/IEEE Design Automation Conference, pp. 9-14, June 2007.

[3] D. Merli, D. Schuster, F. Stumpf and G. Sigl, "Side-Channel Analysis of PUFs and Fuzzy Extractors," Trust and Trustworthy Computing, LNCS 6740, pp. 33-47, June 2011.

[4] U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling Attacks on Physical Unclonable Functions", In Proceeding of ACM CCS, pp. 237-249, October 2010.

[5] M. Yu, M. Hiller, J. Delvaux, R. Sowell, S. Devadas, and I. Verbauwhede, "A Lockdown Technique to Prevent Machine Learning on PUFs for Lightweight Authentication", IEEE Transactions on Multi-scale Computing Systems, Vol. 2, No.3, pp.146-159, July 2016.

[6] M. Rostami, M. Majzoobi, F. Koushanfar, D. Wallach and S. Devadas, "Robust and Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring matching", IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 1, pp. 37-49, March 2014.

[7] Y. Gao, G. Li, H. Ma, S. Al-Sarawi, O. Kavehei, D. Abbott, and D. Ranasinghe, "Obfuscated challenge-response: A secure lightweight authentication mechanism for puf-based pervasive devices", In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communication Workshops, pp. 1-6, March 2016.