PUF-based IoT Device Authentication Scheme on IoT Open Platform

Byoungkoo Kim, Seungyong Yoon and Yousung Kang
Cryptographic Engineering Research Section, Cyber Security Research Division
Electronics and Telecommunications Research Institute (ETRI)
Daejeon, Korea
{bkkim05, syyoon, 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/ICTC52510.2021.9620848

***Abstract*—Recently, it is predicted that interworking between heterogeneous devices will be accelerated due to the openness of the IoT (Internet of Things) platform, but various security threats are also expected to increase. However, most IoT open platforms remain at the level that utilizes existing security technologies. Therefore, a more secure security technology is required to prevent illegal copying and leakage of important data through stealing, theft, and hacking of IoT devices. In addition, a technique capable of ensuring interoperability with existing standard technologies is required. This paper proposes an IoT device authentication method based on PUF (Physical Unclonable Function) that operates on an IoT open platform. By utilizing PUF technology, the proposed method can effectively respond to the threat of exposure of the authentication key of the existing IoT open platform. Above all, the proposed method can contribute to compatibility and interoperability with existing technologies by providing a device authentication method that can be effectively applied to the OCF Iotivity standard specification, which is a representative IoT open platform.**

Keywords—IoT, Device Authentication, PUF, OCF Iotivity

I. INTRODUCTION

The development of Internet technology and the spread of smart devices are providing a convenient environment for people, which is becoming common as a technology called IoT. However, the development and demand of IoT technology is causing various problems such as personal information leakage due to attacks by hackers who abuse it. Recently, interworking between heterogeneous terminals, networks, and applications is accelerating due to the openness of the IoT platform, and it is predicted that additional security threats in technical and management aspects will occur. Accordingly, most IoT open platforms are trying to standardize security technology suitable for each component or utilize existing security technology. However, since the device authentication method provided in most IoT open platforms is a method of storing the key in memory, there is still a security threat due to the exposure of the authentication key. To solve this problem, a technology called PUF has emerged[1]. The PUF is a technology that allows each device to have unique identification information that cannot be copied. Therefore, if a PUF-based IoT device authentication method that can be operated on an IoT open platform is provided, it is possible to fundamentally block the exposure of the authentication key while ensuring compatibility and interoperability with existing standard technologies. In other words, this paper provides a PUF-based IoT device authentication method, but aims to provide an effective and safe device authentication method applicable to a global standard-based IoT open security platform.

This paper proposes a PUF-based device authentication scheme on IoT open platform. This paper is organized as follows: Section II briefly presents the current status of IoT open platform and PUF. Section III describes the proposed IoT device authentication scheme and explains how the proposed scheme authenticates the device on IoT open platform. Section IV presents the prototype platform to which the proposed scheme will be applied. Lastly, Section V presents the conclusion.

II. BACKGROUND

Currently, there are various issues necessary for the construction of the IoT ecosystem, and one of the biggest issues among them is to ensure interoperability between devices. Therefore, platform competition to take the lead in the IoT market is underway in various organizations, and there are IoT open platforms led by representative standardization organizations such as OCF and oneM2M. Table I below shows a brief description of them. Among them, OCF provides interoperability in the Internet of Things market through an open source project called Iotivity, and additionally provides a Iotivity-lite version for lightweight devices. In addition, the device authentication/authorization function of the IoT platform is provided in detail through a separate security specification[2].

TABLE I. IOT OPEN PLATFORMS

	Description
oneM2M	- Joint operation of global standards development organizations such as TTA, ETSI, ATIS/TIA, etc. - Basic authentication and access control functions - OCEAN Open Source: Mobius, &Cube
OCF	- A company-oriented standardization organization for the development of IoT standard platform technology - Standard specifications consist of Core, Resource Type Device, Bridging, Security, etc. - OCF Open Source : IoTivity, IoTivity-lite

However, since the device authentication method defined in the above security specification stores the key in the memory due to the nature of software security, there is a high possibility that a significant damage may occur due to key exposure. To solve this problem, a technology called PUF that can be generated and used only when necessary without the need to separately store the key in memory has emerged. Table II below briefly shows representative PUF technologies. Such PUF technology is a representative hardware-based key hiding technology, and is a technology that allows each device to have unique identification information that cannot be copied[3]. That is, it is a technology that allows devices made by the same process to have unique characteristics, and when used for device authentication in an appropriate manner, security stability can be greatly increased. Therefore, if the PUF technology

can be utilized for the authentication of the IoT device on the above IoT open platforms, compatibility with the existing standard technology can be guaranteed and the possibility of security threats caused by the exposure of the authentication key can be fundamentally blocked.

TABLE II. PUF TECHNOLOGIES

PUF Type	*Advantages*	*Disadvantages*
Arbiter PUF	Partially robust against machine learning attacks	Delay pass must be the same
RO-PUF	Easy to implement	Sensitive to environmental factors
SRAM PUF	Excellent statistical performance	Limited number of CRPs
PHY PUF	Real-time PUF value acquisition	Limited number of CRPs

III. PROPOSED IOT DEVICE AUTHENTICATION SCHEME

A. *Device Authentication on IoT Open Platform*

The proposed method provides a PUF-based IoT device authentication method on the OCF Iotivity standard, which is a representative IoT open platform.

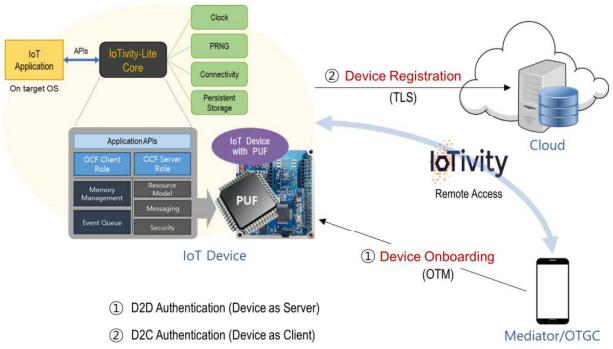

Fig. 1. IoT device authentication on OCF Iotivity

Fig. 1 briefly shows how the proposed method is applied on the OCF Iotivity. As shown in the figure, the IoT device is equipped with a PUF device and works with peripheral devices. The OCF Iotivity standard provides a cloud-based IoT device control method through a user device called Mediator/OTGC (Onboarding Tool & Generic Client), and provides Iotivity-lite version for lightweight devices. Here, the IoT device authentication is performed during the device onboarding and registration process. First, the device onboarding process is a procedure for acquiring ownership of an IoT device that a user wants to control through Mediator/OTGC, and the device authentication is performed through various types of OTM(Ownership Transfer Method). In the device-to-device(D2D) authentication procedure, the IoT device operates as a server that responds to the authentication request. Next, the device registration process is a procedure for registering the IoT device acquired through the onboarding process to the cloud, and generally performs a device authentication method through certificate-based TLS communication. In the device-to-cloud(D2C) authentication procedure, the IoT device operates as a client, the subject that requests registration. That is, the proposed method is applied to procedures ① and ② in the figure, and detailed descriptions are given below.

B. *D2D Authentication using PUF*

The OCF security specification provides a device onboarding process for acquiring ownership of an IoT device, which is performed through an OTM between devices. The techniques are performed in a similar way to TLS, and are divided into *Just Works OTM*, *Random PIN Based OTM*, and *Certificate based OTM*. The *Random PIN Based OTM* is a device authentication method based on PSK(Pre-Shared Key), and the *Certificate-based OTM* is a device authentication method based on a public key encryption system. The proposed method provides a device authentication method that effectively utilizes the PUF technology in the OTM.

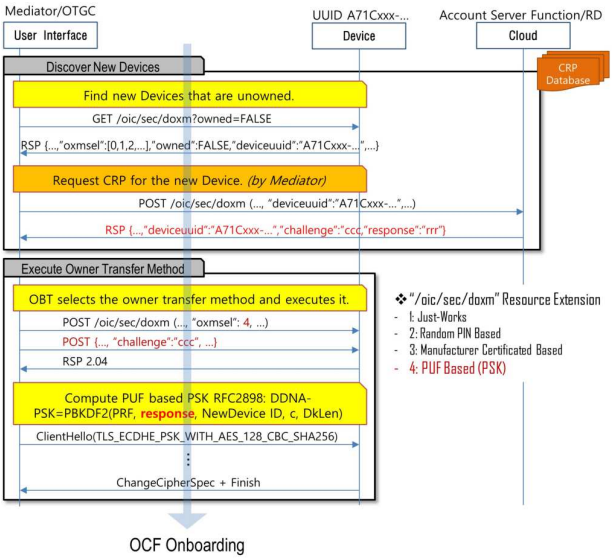

Fig. 2. PSK based device authentication using PUF

Fig. 2 briefly shows the PSK based device authentication method using PUF. This is similar to the *Random PIN Based OTM*, but the output value of the PUF is used for PSK generation. As an initial setting, the cloud stores the CRP (Challenge-Response Pair) information of the device in a CRP database. The detailed main procedure is as follows.

1) Mediator/OTGC receives one random CRP information corresponding to the device ID of the newly discovered device from the cloud.

2) Mediator/OTGC transmits only the challenge value among the CRP information to the new device.

3) Mediator/OTGC and the device perform device authentication by acquiring the same PSK from the response value corresponding to the challenge value. Here, the device obtains a response value directly from its PUF by inputting the challenge value.

Next, Fig. 3 briefly shows the certificate-based device authentication method using PUF. It is performed in the same way as the *Certificate based OTM*, but the PUF is used to generate the device's certificate. As an initial setting, the IoT device has a random challenge value, and generates its own certificate based on a response value of the PUF. Here, the public key is generated by using the response value as the private key. The detailed main procedure is as follows.

1) Mediator/OTGC receives the certificate from the newly discovered device.

2) The device uses its own challenge value as the input of its PUF to obtain a response value, and transmits the digital signature value using the response value as the private key to the Mediator/OTGC.

3) Mediator/OTGC verifies the digital signature value with the public key in the certificate received in *1)*.

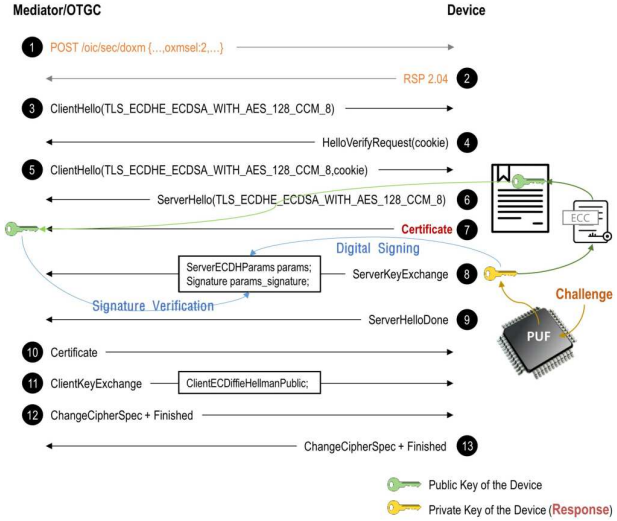

Fig. 3. Certificate based device authentication using PUF

C. *D2C Authentication using PUF*

The OCF security specification provides a device registration procedure to the cloud for cloud-based device control, and device authentication is performed through a general type of certificate-based TLS communication.

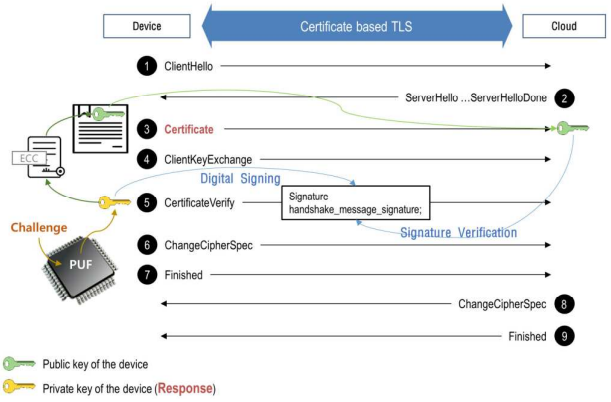

Fig. 4. D2C authentication using PUF

In the device registration procedure, D2C authentication using PUF is performed in a similar way to *Certificate based OTM* for performing device onboarding, but there is only the difference that it operates as a client, which is the subject that requests authentication over the general TLS protocol. That is, it is possible to perform device authentication using PUF without major modification.

IV. Implementation

The proposed IoT device authentication method was developed to solve the key exposure threat of existing IoT open platforms. To verify the proposed mechanism, we implemented a PUF based device authentication platform applicable to the OCF Iotivity standard.

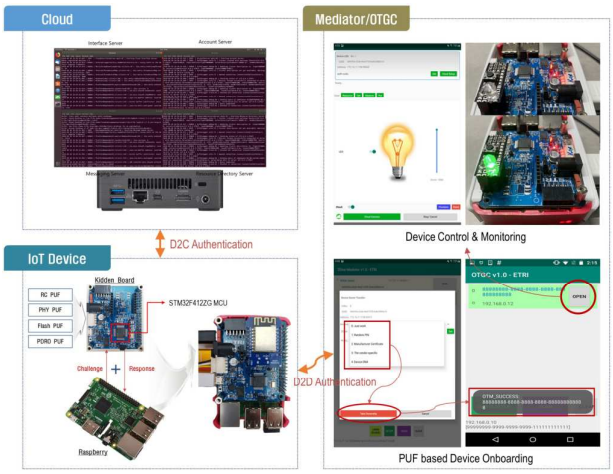

Fig. 5. Our prototype platform implementation

Fig. 5 shows the prototype platform implemented based on the Iotivity-lite 2.0.5 open source project, which is a lightweight implementation of the OCF standard. As shown in the figure, the device basically operates on a commercial Raspberry Pi 3 model B, and uses a self-made board called a *Kidden Board* as a peripheral device. The self-made device provides various PUF technologies. Next, the cloud used a general Linux server system based on Ubuntu. Finally, Mediator/OTGC is implemented as an Android app that can be used on smart devices and has a PUF-based device onboarding screen. In addition, in order to check the normal operation on the OCF standard specification, cloud-based device control and monitoring service functions using LED bulbs were tested.

V. Conclustions

In this paper, we proposed a PUF-based IoT device authentication method that operates on the OCF Iotivity standard, which is a representative IoT open platform. In the future, we plan to test the stability of the proposed method by actually installing and operating it in our prototype platform.

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] Byoungkoo Kim, Seungyong Yoon, Yousung Kang and Dooho Choi, “Secure IoT Device Authentication Scheme using Key Hiding Technology,” in Proc. of ICTC2020, pp.1821-1823, Oct. 21-23, 2020.

[2] Jaehong Jo, Jaehyun Cho, Rami Jung and Hanna Cha, “IoTivity-Lite: Comprehensive IoT Solution In A Constrained Memory Device,” in Proc. of ICTC2018, pp.1367-1369, Oct. 17-19, 2018.

[3] John Ross Wallrabenstein, “Practical and Secure IoT Device Authentication using Physical Unclonable Functions,” in Proc. of IEEE 4th Conference on FiCloud, pp.99-106, August 22-24, 2016.