Security enhancement scheme for mobile device using H/W cryptographic module

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

***Abstract*— This paper is about a mobile device security enhancement technology using a hardware cryptographic module. More specifically, it is a technology that provides an encryption function to access networks such as private networks and national defense networks that require a higher level of security. The hardware cryptographic module is a separate hardware device physically independent of the mobile device. It provides not only basic encryption functions such as data encryption, message authentication, and digital signature, but also security functions such as identification and key management, authentication, and secure storage in conjunction with the built-in Physical Unclonable Function (PUF).**

Keywords—Mobile Security; PUF; Cryptographic module

I. INTRODUCTION

As mobile technology has recently developed, various application services on the Internet can be easily used through a mobile device such as a smart phone. Financial services such as banking, stock trading, and mobile shopping/payment, as well as SNS services, web surfing, and email services, can be used anytime, anywhere. This is because mobile security technology develops together and supports safe handling of data. In addition to basic encryption solutions, mobile security technologies such as mobile vaccine, mobile device management (MDM), and app integrity verification are applied to mobile services to ensure data confidentiality, integrity, and access control.

In order to use application services on the Internet through general service apps, secure communication channels are established based on security protocols such as TLS/DTLS [1]. Most Android-based mobile devices perform encryption functions such as data encryption, message authentication, hash, and digital signature by utilizing software cryptographic modules provided by the platform or by OpenSSL [2].

However, in order to access networks with a very high level of security, such as private networks and national defense networks, existing mobile security technologies are insufficient. It is proposing to apply higher security requirements to mobile devices. In addition, since there is a possibility of leakage of important information when a mobile device is lost or stolen, a separate dedicated device is manufactured and used.

II. PROPOSED SCHEME

In this paper, we propose a mobile device security enhancement scheme using hardware cryptographic module technology to solve the above-mentioned problems. The hardware cryptographic module is a separate, detachable hardware device that fundamentally prevents the leakage of keys and important information, and provides a device authentication technique that enables safe use of mobile devices without external key injection or user intervention. In addition, it provides convenience and security by making it possible to run a general app for Internet access and a dedicated app for private network access at the same time with one mobile device without the need to manufacture a separate dedicated device. Therefore, the mobile device security enhancement technique using a hardware cryptographic module provides a security solution that can safely use various application services by accessing a network requiring a high level of security, such as a private network and a national defense network.

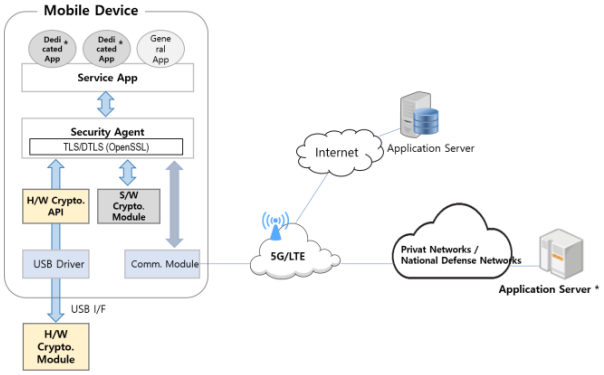

Fig. 1. Security enhancement scheme for mobile device

General apps utilize existing mobile security technologies and use application services on the Internet in conjunction with software cryptographic module. The dedicated apps are for using the application service of the private network/defense network, and are interlocked with the

hardware cryptographic module. Security Agent recognizes installation and detachment of hardware encryption module in real time, and connects or blocks access to private network/defense network. In addition, the security agent provides an encrypted communication channel using a security protocol such as TLS/DTLS to establish a secure channel with the application server.

The hardware cryptographic module is connected to the mobile device through the USB interface and provides a USB driver and hardware cryptographic API so that the security agent can use the cryptographic function. By means of the security agent, dedicated apps can use dedicated application services by accessing private networks/defense networks, and general apps can use general application services by accessing the Internet. Therefore, it provides the advantage of being able to use both dual services with one mobile device without manufacturing a separate dedicated device.

Fig. 2 shows the architecture of the hardware cryptographic module. The hardware cryptographic module consists of an I/O interface for USB communication with mobile devices, a Main Processor Unit (MPU) for data processing, a PUF for key generation and device authentication [3], a secure storage for safely storing data, a cryptographic engine and so on.

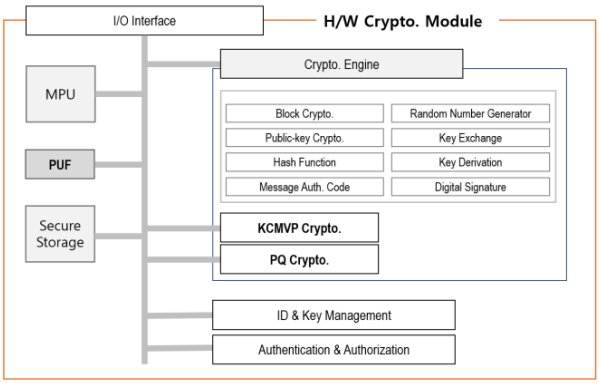

Fig. 2. Architecture of H/W cryptographic module

The I/O interface is responsible for communication with the mobile device. The I/O interface provides a USB interface (version 2.0 or 3.0) to ensure throughput of hundreds of Mbps or more. Since the latest commercial mobile devices basically provide a USB-C type standard interface, they communicate using it.

MPU is in charge of data processing for performing all encryption functions in the hardware cryptographic module.

PUF uses the unique characteristics of hardware and is not physically copied, so it is mainly used for key generation or device authentication [4][5]. PUF generates a unique output value, Response (R_0, R_1, ..., R_n), for Challenge (C_0, C_1, ..., C_n), which is an input value. In the hardware cryptographic module, an identifier or secret key is generated by using strong PUF having many Challenge-Response Pair (CRP). A specific challenge, for example C_0, is used as an identifier for the hardware cryptographic module, and the remaining C_1, C_2, ..., C_n can be used as a secret key.

Secure storage provides a function to encrypt and store keys or important information. All encryption keys have a hierarchical architecture based on the storage root key, so to access a specific encryption key, the parent key must be decrypted sequentially.

The identification/key management block manages the identifier and secret key of the hardware cryptographic module in conjunction with the PUF. That is, it performs management functions such as generation, renewal, and deletion of identification and secret keys.

The authentication/authorization block performs device authentication for the hardware cryptographic module in conjunction with the PUF, and grants access rights according to the authentication result.

The cryptographic engine consists of block crypto, public-key crypto, hash function, message authentication, random number generator, key establishment, key derivation, and digital signature block.

The KCMVP crypto block is intended to support Korea Cryptographic Module Validation Program [6], a system that verifies the safety and implementation suitability of cryptographic modules used to protect important information among data communicated in national/public networks. It supports domestic encryption algorithms such as ARIA, SEED, LEA, HIGHT, LSH, KCDSA, and EC-KCDSA.

PQC crypto block is for post quantum cryptography, which is being standardized by NIST in the United States [7]. It supports Lattice-based Crystals-Kyber, Crystals-Dilithium, Falcon algorithms, and Code-based Classic McEliece algorithm, and Hash-based SPHINCS+ algorithm.

In order to install and use the hardware cryptographic module on a mobile device, a device authentication process is required. Device authentication is performed based on TLS, a security protocol, using the PUF embedded in the hardware cryptographic module. The following two methods are available: Pre-Shared Key (PSK) based and Certificate-based authentication method using PUF.

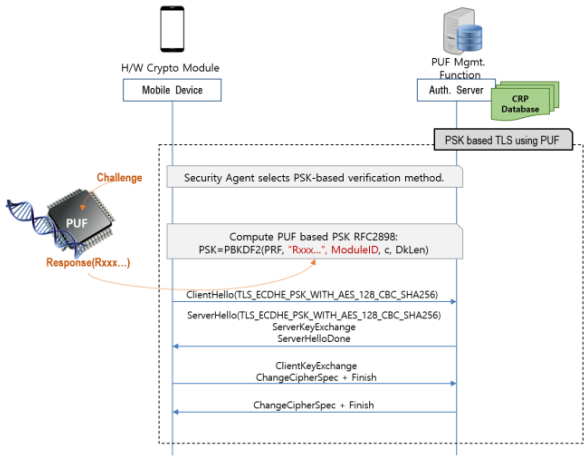

Fig. 3. PSK-based device authenticaiton

Fig. 3 shows a PSK-based authentication method using PUF. The hardware cryptographic module generates PSK according to RFC2898 [8], and uses the following function.

PSK = PBKDF2(PRF, "Rxxx…", ModuleID, c, DkLen)

At this time, ModuleID and Response (Rxxx...) created using PUF are passed as parameters.

A PSK-based authentication method using PUF is much simpler and less expensive than a certificate-based authentication method. It is mainly used in environments where it is difficult to generate and distribute certificates. When a device authentication request comes in from a mobile device with a CRP database built in advance in the authentication server, the authentication process is performed.

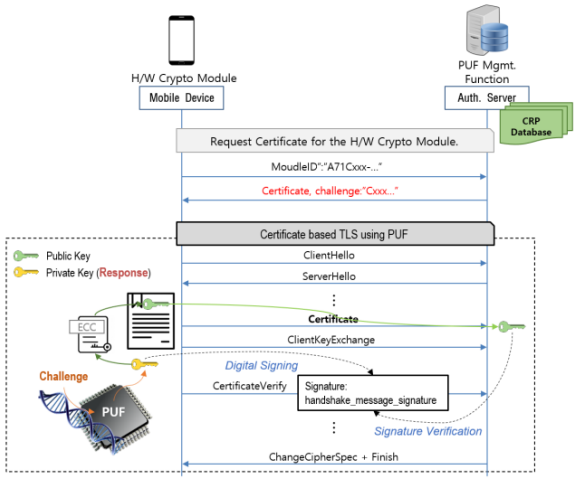

Fig. 4. Certificate-based device authentication

Fig. 4 shows a certificate-based authentication method using PUF. The private key of the certificate is not stored in a non-volatile memory such as Flash, but is generated by requesting the PUF in real time when necessary, and then device authentication is performed through digital signing and verification.

III. IMPLEMENTATION

We have implemented a TLS-based server system and mobile device security program to test the security enhancement functions of mobile device using hardware cryptographic module. The server system has implemented on Ubuntu 20.04 LTS, and the mobile device has implemented on Android 12 operating system. It supports both TLS version 1.2 and 1.3, and supports ECDHE and ECDSA algorithms for key exchange and digital signature, respectively. For data encryption, block ciphers such as ARIA, LEA, and SEED have implemented and functional tests have performed. Fig. 5 shows the screenshots of the server system and mobile device testing the TLS cipher suite "ECDHE-ECDSA-ARIA256-GCM-SHA384".

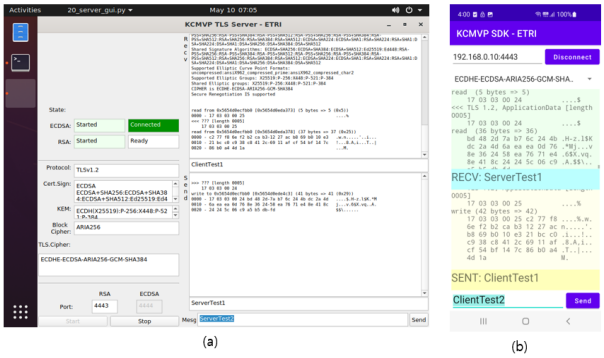

Fig. 5. Screenshots of test program: (a) Server system, (b) Mobile device

IV. CONCLUSION

In this paper, we presented a mobile device security enhancement method using a hardware cryptographic module. Mobile security technology using existing software cryptographic modules has security vulnerabilities, so there is a risk of leakage of important information when the device is lost or stolen.

The proposed technique fundamentally blocks the leakage of important information by utilizing a portable size hardware cryptographic module that can be detached/mounted on a mobile device. In addition, it is possible to solve the inconvenience of having to manufacture and use a separate dedicated device to access a network with a high security level, such as a private network/national defense network. It is possible to use application services by simultaneously running general and dedicated apps on a single mobile device, resulting in significant cost savings.

The hardware cryptographic module proposed in this paper has a built-in PUF, so it can perform identification and device authentication functions without external key injection or user intervention. In addition, by supporting KCMVP domestic cryptographic algorithm, it can be easily applied to domestic national/public institutions, and through PQC cryptographic algorithm support, it is possible to solve the problem of cryptographic security vulnerability due to the advent of the quantum age in the future.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.RS-2023-00225201, Development of Control Rights Protection Technology to Prevent Reverse Use of Military Unmanned Vehicles).

REFERENCES

[1] OpenSSL, Cryptography and SSL/TLS Toolkit, https://www.openssl.org/

[2] Panagiotopoulou Vasiliki, Cryptography in mobile devices security protocol, 6CS513, March 2015

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

[4] Lee, S.; Oh, M.; Kang, Y.; Choi, D. "RC PUF: A Low-Cost and an Easy-to-Design PUF for ResourceConstrained IoT Devices," In Proceedings of the 20th World Conference on Information Security Applications, Jeju, Korea, pp. 326–337, August 2019.

[5] 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.

[6] KCMVP, Korea Cryptographic Module Validation Program https://www.nis.go.kr:4016/AF/1_7_3_1.do

[7] PQC, Post-Quantum Cryptography, https://csrc.nist.gov/projects/post-quantum-cryptography

[8] RFC2898, PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000.