International Journal of Internet, Broadcasting and Communication Vol.5 No.1 18-22 (2013)
http://dx.doi.org/10.7236/IJIBC.2013.5.1.18

IJIBC 13-1-5

RFID-based Secure Communication for Smart Device in Future Home Network Environment

Nong-Jun Li[1], Kee-Hyun Choi[1], Kyung-Soo Jang[2], Dong-Ryeol Shin[1]

[1]*Department of Information and Communication Engineering, Sungkyunkwan University, Korea*
linongjun@skku.edu

[2]*Department of Video Broadcasting and Information, Kyungin Women's College, Korea*
ksjang@kic.ac.kr

Abstract

We introduce, in this paper, a novel approach of protection mechanism for data which are transmitted not only between the networked devices but also between the digital media devices. As the devices are getting more powerful and more storage capacity, they can process the encoded/encrypted data autonomously. However, all devices must know the secret key that used to encrypt data, and also use secure method to distribute that key. Moreover, there are no protection mechanisms supporting end-to-end copy protection which result in the fact that the data passed through various devices can be manipulated or captured. Therefore, we propose a RFID-based key distribution and protection mechanism to resolve these problems.

Keywords: *RFID, Smart Device, Future Home Network, Secure Communication*

1. Introduction

Since the personal computer (PC) was introduced to the general public, the device that people use it every day has evolved and has even becoming more powerful. The Devices that used in home and office provide their own dedicated function for people in the past time. Recently, however, multi-functional devices such as smart phone, smart TV can provide not only their dedicated service but also other services such as web browsing, interaction services, games and so on. From a perspective of the flow of data, output device is the last device that provides a certain result to people. In order to give an appropriate service to people, the data must be processed by devices on the flow. Multi-functional device, however, can provide results directly without preprocessing devices and even output devices. In the case of copyrighted digital content, people only need to send it to such devices as long as all the devices share the secret key used to encrypt the content. In order to share the key securely, the device can communicate each other without human intervention, and the data can be transmit through secure channel between devices. Unfortunately, traditional protection system such as DRM-based copy protection system and link protection system have vulnerabilities, and even some of them are compromised.

Thus, we propose a novel protection mechanism using RFID (Radio frequency identification) technology for providing automatic key distribution and data copy protection. In this paper, we assume that all devices are multi-functional device and RFID-enabled device so that the device could communicate with each other

Manuscript Received: Nov. 14, 2012 / Revised: Jan. 12, 2013 / Accepted: Feb. 8, 2013
Corresponding Author: ksjang@kic.ac.kr
Tel:+82-31-290-7232, Fax: +82-31-290-7232
Dept. of Video Broadcasting and Information, Kyungin Women's College, Korea

and share the secret key.

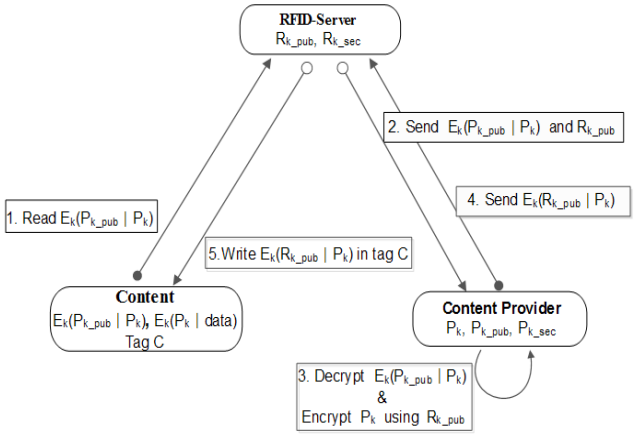

Fig 1. Device Initialization

The organization of this paper is as followed. In section II, we introduce the background of technical challenges. In section III, we discuss RFID-based protection and key distribution mechanisms. Finally, we conclude our paper in the in section IV.

2. Background

Radio frequency identification (RFID) is a popular kind of automatic identification technology, which automatically recognizes and counts the data in a tag via radio-frequency signal without manual intervention. It is a simple wireless system which contains only two main basic fundamentals like reader and tag. In our proposed system, we use RFID to detect, control and track digital contents, because RFID can give uniqueness to object, and it can be embedded into storable and streaming digital contents.

Digital rights management technology is used to protect the copyright of digital content (DC). The principle of operation is use encryption key to lock the digital content, and when consumer requires the DC, the authorization right is given from authority centre, because the decryption key is supplied to decrypt the locked DC. There are plenty of DRM technologies being used, but most of them cannot provide end-to-end protection. In 2007, Steve Jobs and Bill Gates expressed disappointment with the current situation of DRM technology. Even Jobs advocated laying off DRM

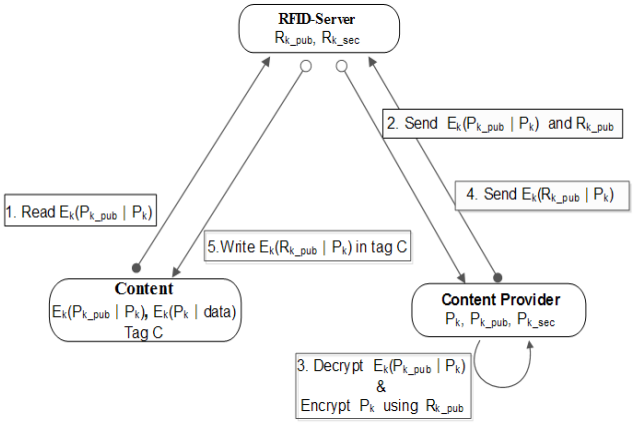

Fig 2. Content Identification

[1][2].

Based on the attacks that have been made on DRM systems, it is shown that attackers will probably try extracting keys or circumventing the encryption before attempting brute-force attacks on the encrypted content. These facts point out that the encryption methods used today are secure except the supporting architecture for distributing keys and storing method is still lack of security [3]. So in our proposed systems, we still use cryptography algorithm.

From the view of technical ways, we found that it is impossible to prevent copy action completely. So we propose device initialization, content identification and content protection system in this paper in order to protect the digital content from end to end [4][5].

3. Technical Issues

We assume that RFID tag or virtual tag can be tagged into CD/DVD disk and streaming digital content respectively. Additionally, RFID reader is embedded into RFID-Server and device which can identify the tag, and all devices have network function

3.1 Device Initialization with RFID-Server

In this system, the consumer's device can connect to RFID-Server using network function. In the same way, the RFID-Server can connect to the device manufacture which can verify the device information and generate security

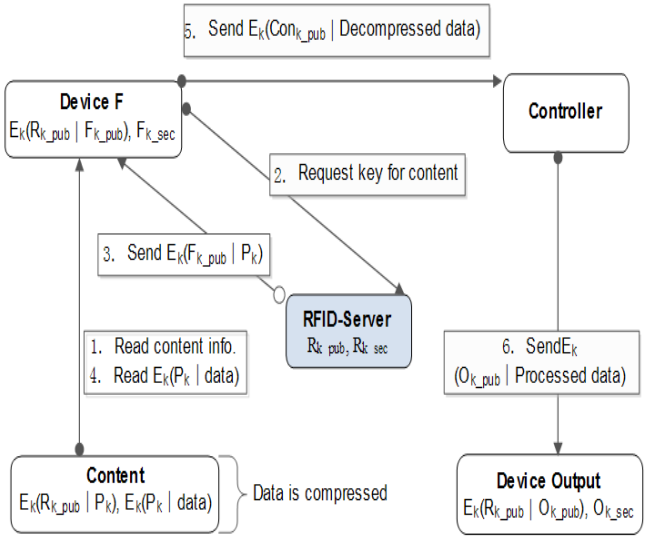

Fig 3. Lossy Compression Content Protection

keys. The auto-update function guarantees the standard of protection system can be renovated. This means when the security key is deciphered, it will be revoked, and the device can be notified immediately. For device manufacturer, it is more feasible to enhance its DRM technology until recently. Simultaneously, consumer does not need to buy new hardware for the sole purpose of preserving copy protection as shown in Fig. 1.

For end-to-end protection, we assume that consumer's device must be initialized before playing the digital content. This process is accomplished automatically without manual intervention. The RFID-Server has the obligation to identify the encrypted device information Ek(Pk | Info), and then send it with Rk_pub to device manufacturer. When the information is verified, the manufacturer generates security keys Dk_pub and Dk_sec which are encrypted by Rk_pub and Pk separately. The encrypted key Ek(Rk_pub | Dk_pub) is written in tag D, and Ek(Pk | Dk_sec) is saved in device. It must note that the RFID-Server also can generate

the keys. In such case, device manufacturer sends only Ek(Rk_pub ｜ Pk) in step 4.

3.2 Content Identification with RFID-Server

By the same token, content provider requires cooperation with RFID-Server to identify digital content. The reason is that the data is encrypted by Pk, and content provider can have a great vested interest in protecting Pk using automatic RFID-Server's encryption key Rk_pub in step 4 and 5. In rental agency, each product should be identified before leased out as shown in Fig. 2.

Firstly, RFID-Server reads the encryption key Ek(Pk_pub ｜ Pk) from the content, then transfers it and Rk_pub to content provider in step 2. Since encrypted key Pk is decrypted, it will be re-encrypted by Rk_pub. This system can block up piracy when the security key is divulged. Because of the content owns one unique identity in RFID tag, the RFID-Server will know when piratical content is displayed in RFID-based device.

3.3 Content Protection in Multi-function Device

Nowadays, multi-functional device is widely used for more entertaining in smart home environment. But all-in-one multi-function machine, like PC, gives lots of feasibility for piracy. It is shown that attackers normally extract keys or circumvent the encryption before attempting brute-force attacks on the encrypted content. It means that the encryption methods used today are secure except the supporting architecture for distributing keys and storing method is still lack of security[3]. Normally, most of piracy attack is accomplished in multi-functional device, like capturing the decrypted analog data. It is well known that there are two types of compression, like lossy and lossless compression. So we propose the two different content protection mechanisms inside of the multi-functional device as shown in Fig. 3.

When device F reads content information from the content, the Ethernet-enable device F can request key from RFID-Server. Then device F can read encrypted data Ek(Pk ｜ data) after receives the encrypted key Pk. For lossy compression, the controller obtains the decompressed data which is encrypted by Conk_pub. Before sending processed data from controller, it will be encrypted again by Ok_pub. For lossless compression, Ek(Pk ｜ data) is compressed firstly which is different with compressed data in lossy compression. In step 5, device F sends decompressed data Ek(Pk ｜ data) to controller, and other steps are same with lossy compression. Whereas we find that it takes a long time to encrypt/decrypt in controller and output device using Conk_pub and Ok_pub respectively. In practice, it is scarcely possible to implement these keys, so symmetric key (e.g. Pk) can be used instead of them.

4. Conclusion

This paper provides a brief discussion of the RFID-based protection system. Admittedly, media privacy is a problem that cannot be solved completely, because the high attack feasibility provided by multi-function device. For this reason, the proposed mechanisms using RFID technology and cryptography algorithm can offer more convenient and secure to provider and consumer. Device initialization and content identification mechanism can be updated automatically; therefore the encrypted process can prevent intentional stealing. The content protection in multi-function device can provide secure channel between controller and output, this process can reduce attack communication channel. In our proposed system, we are only interest of the encryption and decryption time of the hybrid cryptosystem for the purpose of verifying the feasibility, and thus the secure concern of the conventional cryptosystem is not discussed specifically here. In the future, we will verify our proposed system using simple simulation in which two device communicates based on our proposed protection mechanism. Moreover, we will study on more specific protection area such video/audio rental business.

References

[1] J. Karaganis (Ed.), "Media Piracy in Emerging Economies", New York, U.S: Social Science Research Council, 2011.

[2] "Steve Jobs Makes Case for Abolishing DRM (2007)", Available at: http://www.dailytech.com/Steve+Jobs+ Makes+Case+for+Abolishing+DRM/article6011.htm (Accessed: 10 September 2012).

[3] M. Persson and A. Nordfelth, "Cryptography and DRM", Uppsala, Sweden: Uppsala University, 2008.
[4] Kee-Hyun. Choi, Kyung-Soo Jang and Ho-Jin Shin, "RFID-ACP: RFID-based Digital Content Identification and Authentication Mechanism in Smart Home Environments", JDCTA 2011, pp. 129-141, 2011.
[5] Kee-Hyun. Choi, Kyung-Soo Jang and Ho-Jin Shin, "Content Self-Protection for Digital Products Using RFID-enable Agent Platform", International Journal of Engineering and Industries Volume 2, Number 2, June 2011