A Prototype System of the RFID Authentication Processing Framework

John Ayoade, Osamu Takizawa, Koji Nakao
ayoade@nict.go.jp, taki@nict.go.jp, ko-nakao@kddi.com

Security Advancement Group
National Institute of Information and Communications Technology, Tokyo, Japan

Keywords: RFID, Authentication Processing Framework, Tags, Readers

Abstract: In the RFID system, malicious readers could illegally access the tag without the knowledge of the users. This has raised a lot of growing concerns regarding the violation of users' privacy. Moreover, the growing concerns will continue unless researchers find a novel solution to this problem as soon as possible. We have proposed a basic concept of RFID Authentication Processing Framework for this purpose. In this paper, we are presenting the prototype system of our proposed solution which is called APF (Authentication Processing Framework). The APF system provides mutual authentication for both tags and readers. The mutual authentication in APF provides security for the information stored in the tags.

1 INTRODUCTION

In the RFID system, many proposals have been presented to deter the privacy and security problems however, those proposals have one disadvantage or the other and these had made them insufficient to completely address the problems. We agreed that a simple approach for dealing with the problem of privacy is to prevent readers from receiving data coming from tags [1]. However, as mentioned earlier all the propositions till date have one disadvantage or the other.

We will quickly describe some of the approaches and their adverse effects:

a. Kill Command Idea - The standard mode of operation proposed by the AutoID Center is indeed for tags to be killed upon purchase of the tagged product. With their proposed tag design, a tag can be killed by sending it a special "kill" command. However, there are many environments, in which simple measures like "kill command" are undesirable for privacy enforcement. For example, consumers may wish RFID tags to remain operative while in their possession [2].

b. Faraday Cage Approach - An RFID tag may be shielded from scrutiny using what is known as a Faraday Cage - a container made of metal mesh or foil which is impenetrable by radio signals (of certain frequencies). There have been reports that some thieves have been using foil-lined bags in retail shops to prevent shoplifting-detection mechanisms [2].

c. The Active Jamming Approach - An active jamming approach is a physical means of shielding tags from view. In this approach, the user could use a radio frequency device which actively sends radio signals so as to block the operation of any nearby RFID readers. However, this approach could be illegal for example if the broadcast power is too high it could disrupt all nearby RFID systems and not that alone it could be dangerous and cause problems in restricted areas like hospital and also in the train [3].

d. The Blocker tag Approach - The blocker tag is the tag that replies with simulated signals when queried by reader so that the reader can not trust the received signals. Like active jamming, it may affect the other legal tags [3].

All these approaches could have been great solutions to the privacy problem but the

disadvantages make them unacceptable. In this paper, we considered that good authentication procedure will be the best option to tackle this problem. The reason is that our proposed solution – APF provides solutions to the privacy problem and enhanced the security in RFID system.

2 THE PROPOSED CONCEPT OF THE AUTHENTICATION PROCESSING FRAMEWORK

In [4] we proposed a framework that will authenticate readers before they can access the information in the tags. The proposed procedure is called Authentication Processing Framework - APF. The main idea of this framework is that tags and readers will register with the APF database which will authenticate readers prior to when it will read the data in the tag. Implementing this kind of framework in the RFID system will alleviate the security and privacy concerns. Some examples of the areas where the APF system could be deployed will be described in the discussion part of this paper.

3 OVERVIEW OF THE APF SYSTEM

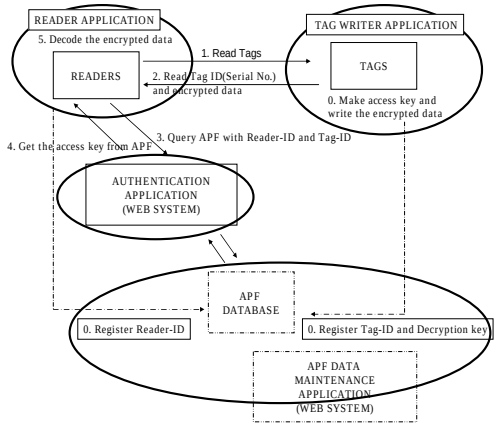


Figure 1 The Functional Diagram of the APF

The APF system was proposed to deter the data security problem in the RFID system.

APF is a framework that makes it compulsory for readers to authenticate themselves with the APF database before they can read the information in the registered tags.

Basically from figure 1, APF system comprises of four application segments:

i. The tag writer's Application: is the part of the APF system that encrypts the information in the tag and produces the decryption key which will be submitted along with its identification number to the APF database.

ii. The Reader's Application: is the part of the APF system that queries the tag and registers readers' identification number with the APF database. Also, this is the part of the system that gets the decryption key to decrypt the encrypted information after it has been authenticated by the APF database.

iii. The Authentication's Application: is the part of the system that integrates both the reader application and the APF database maintenance application.

iv. The Maintenance's Application: is the part of the system that maintains the APF database.

3.1 THE METHODOLOGY OF THE APF SYSTEM

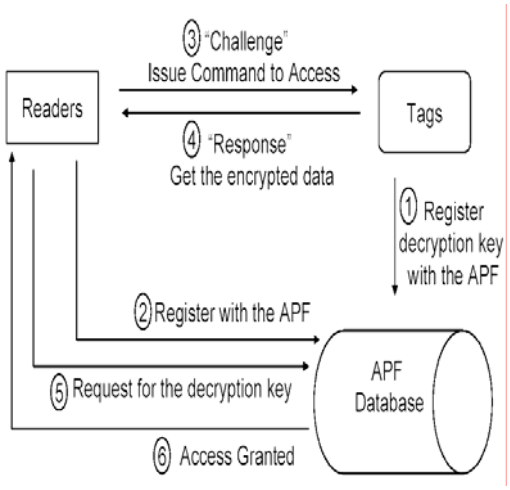


Figure 2 The Flowchart of the APF Framework

Figure 2 is the representation of the step by step of the APF system. Initially, the tags will register their identification numbers and the decryption keys with the APF database. Also, the readers will register their identification numbers with the APF database. Normally the readers will send "Challenge" command to

access tags. However, with the APF system protocol, tags will send "Response" command which will be the tag identification number and the encrypted data to the readers. The response message from the tag will instruct the reader to get the decryption key from the APF database in order to decrypt and read the data in the tag. Since, authentic readers would have registered with the APF database, only authentic readers would be given the decryption key to decrypt the encrypted data in the tags.

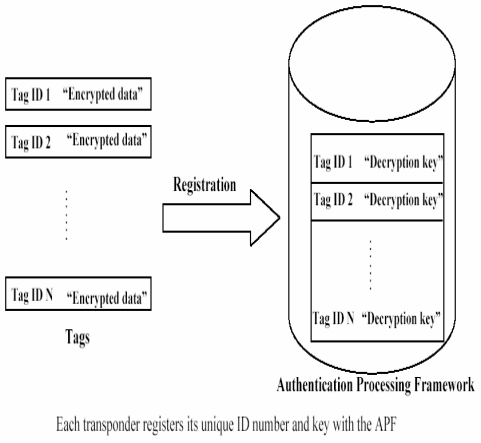
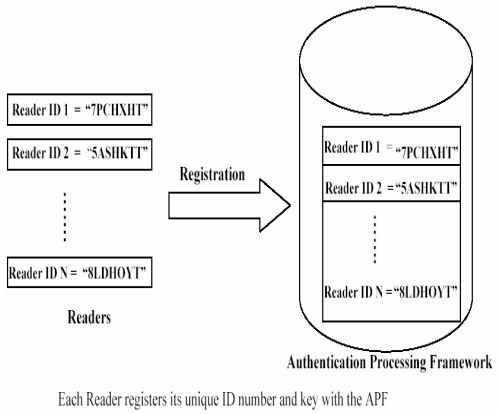


Figure 3 The Registration of Tags with the APF

In order to prevent illegal access to the information stored in the tags there should be a procedural access control to the information stored in the tags. From figure 3, as discussed earlier each tag will register its unique ID and the decryption key with the APF database. This is necessary for the protection of tag from unscrupulous readers that have ulterior intention. Once tag registers its unique identity and decryption key with the APF, it will be difficult for unregistered reader to have access to the data in the tag without possessing the decryption key to the tag. This means every registered reader will be authenticated prior to getting the decryption key to access stored data in the tag. In the next paragraph, we will discuss about how the authenticated reader would have access to the stored data in the tag.

Furthermore, every reader will register its identification number with the APF in order for it to be authenticated prior to the time the reader will request for the decryption key to access the data in the tag. In a nutshell, every reader will register its unique identification number with the APF and this will be confirmed by the APF before releasing the decryption key to the reader in order to read the encrypted data in the specific tag.



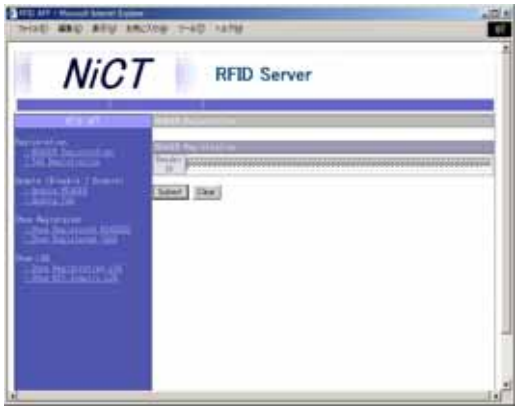
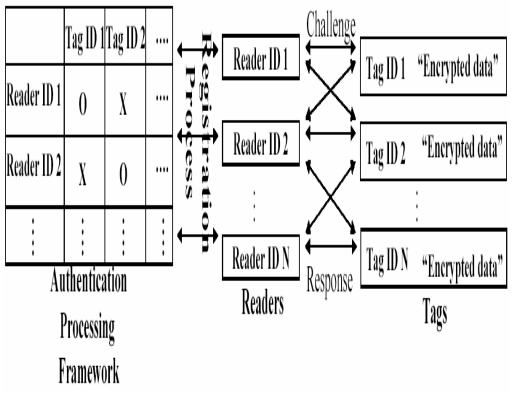
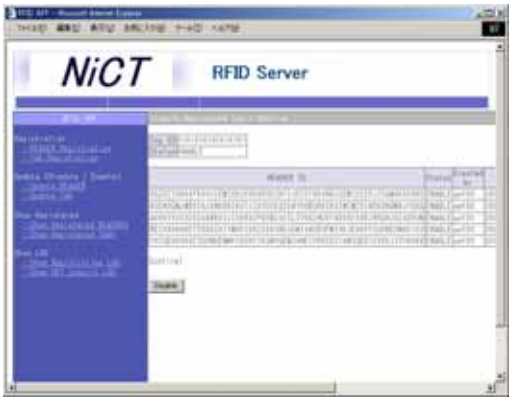


Figure 4 The Registration of Readers with the APF

From Figure 4 every reader registers its unique identification number with the APF. Since both readers and tags register their identification numbers with the APF, these serve as a mutual authentication and protect the information in the tags from malicious readers which is one of the concerns users have. This means that unauthorized access into the tag will be eradicated if APF systems is implemented and used. In the next paragraph, we will discuss about the registration and access control of readers to the APF.





O-means access granted X-means access denied

Figure 5 The Registration/Access Control of Readers to the APF/Tag

In the previous paragraphs, we discussed about the registration of the tags' unique ID and the decryption key with the APF. Also we discussed about the registration of readers with the APF prior to accessing the information in the tags. When the reader sends a "read" command to the tag, the tag will reply with its identification number and encrypted data, this means that the data is encrypted and the registered reader with the APF will be able to get the decryption key in order to decrypt the encrypted data. Once the key is received the data in the tag will be readable. In this framework, there are two important processes, the first one is that, mutual authentication was carried out by the APF because it authenticates the reader and the tag. Secondly, the privacy concern is guaranteed because the data stored in the tag is protected from malicious reader. Since, the information the reader got from the tag is encrypted and it can only be read after the decryption key to access the information is received from the APF.

4 DISCUSSION

The APF proposed prototype described in this paper has many applications. For example, it can be applied in the supply chain management and also in restricting access of certain areas to certain groups of people in the hospitals. This has been major concerns in many big hospitals [5]. If APF system is implemented in the above examples this kind of growing concerns will be eradicated. Take for example, in a hospital or supermarket where the RFID system is used, the APF system will guarantee total security from malicious readers because every authentic reader will register with the APF system prior to reading the tags and all tags that will be read by those readers will register with the APF. This means that there will be mutual authentication and the information in the tags will be secured.

In this prototype system, the encryption algorithm used is AES – Advanced Encryption Standard, this is because it is specifically designed to resist the most sophisticated cryptographic attacks, such as timing analysis and power analysis also, it has very low memory requirements so it is particularly suited for embedded applications such as smart cards[8].

Moreover, regarding the issue of scalability, the APF system will register only tags and readers that are necessary for a particular application. It will not register tags and readers that are not meant for that particular application. Furthermore, the traffic flows of

steps ⑤ and ⑥ in figure 2 will be encrypted by secure sockets layer in order to protect the information that will be decrypted by the authentic reader from being revealed to the malicious reader.

Furthermore, we will like to mention that in [7] they proposed an idea for the protection of the location security in which the server sends decrypted ID of the tag to the reader each time it accesses the tag however, in this paper our prototype system is for the protection of the content security and the APF database will have to authenticate readers and give the decryption key to only the authentic readers before authentic readers can decrypt the data in the tag.

5 CONCLUSION

The potential applications of RFID system may be identified virtually in every sector of industry, commerce and services where data is to be collected. However, RFID system has faced widespread resistance due to lack of privacy [6]. This calls for a prompt and concrete solution for the full realization of the RFID system potentials. We are convinced that the APF system will go a long way to defuse the fears and concerns that the consumers have regarding the present lack of privacy in the RFID system. Moreover, in the prototype system we put into consideration to employ Secure-HTTP and SSL protocols for the protection of the APF database however, we will further our research work on how the APF database will be protected from various malicious attacks.

REFERENCES

[1.] Gildas Avoine et al, RFID Traceability: A Multilayer Problem 2004 http://lasecwww.epfl.ch/~gavoine/download/rfid-multilayer-paper.pdf

[2.] Liu Dingzhe et al, Pretty-Simple Privacy Enhanced RFID and Its Application 2003

[3.] Juels Ari et al, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy 2003 http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf

[4.] Ayoade John, Security and Authentication in RFID The 8th World Multi-Conference on Systemics, Cybernetics and Informatics 2004 U.S.A

[5.] RFID in the Hospital 2004 Http://www.rfidgazette.org/2004/07/rfid_in_the_hos.html

[6.] Rakesh Kumar, Interaction of RFID Technology and Public Policy 2003 http://www.rfidprivacy.org/2003/papers/kumar-interaction.pdf

[7.] Ohkubo Miyako et al Forward-secure RFID Privacy Protection for Low-cost RFID SCIS 2004, Japan

[8.] Denis Crampton, TechWorld What is Encryption? 2004. Http://www.techworld.com/security/features/index.cfm?FeatureID=993