3-10 Finding Solution to the Illegal Access in RFID

AYOADE John Olurotimi, TAKIZAWA Osamu, and NAKAO Koji

In a system where many readers have access to read from and write to a tag, one can fear that ill-intentioned persons may try to modify the information contained in the tag which could lead to the denial of service, intrusion into the personal/private information in the tag and violation of privacy/confidential information.

In this paper, 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. Readers will register with the APF and get the access control key that will allow them to have access to read from and write to the tag. Implementing this kind of framework in the RFID system will alleviate the security and privacy concerns which are some of the major potential challenges and impediments to the RFID system's benefits.

Keywords
RFID, Authentication, Illegal Access, and APF

1 Introduction

RFID stands for Radio Frequency Identification. It is an automatic identification system which comprises of a reader, a tag, an antenna and a host system. Radio frequency Identification (RFID) is an enabling technology which allows the identification of anything that can be `tagged` with a special device known as a tag. This tag can then be read by a stationary or mobile `reader` which can identify those tags within its proximity via radio frequency. This technology is particularly useful for moveable equipment and transportation vehicles such as automobiles, railroad locomotives and rail cars, since the tag can be read by the reader while the vehicle is in motion[1].

1.1 Security in RFID

Security in RFID has received little attention so far because of several reasons:

- It has been so far mainly used in closed systems.
- Read Only tags have often been used.
- The RFID industry has focused its attention on increasing the performance (read range) and reducing the cost, and has paid little attention to the security requirement of the users.

The only exception is in the automotive applications (immobilizers).

The use of the term "security" has extremely broad application. For clarity, the following definitions are established with reference to security in RFID:

- Data Security – This refers to the allowance of access to the data stored in a tag as part of an RFID system. The author / owner of such information may require that only "authorized" recipients may be allowed to "know" the contents.
- Data Integrity – This refers to the assurance that data contained in a tag cannot, either intentionally or unintentionally, be changed or modified by "unauthorized" source. This includes modification that

may render the referenced data as unusable (corrupted).

- Data Validity – This property refers to the "authenticity" of data being retrieved from a tag as having originated by the claimed source. This is with particular reference to the issue of data duplication via counterfeit tags[2].

2 The problem description

Security functions are required to insure data integrity and authorized use. The concept here is that it may not be desirous to have just anyone read a tag. In the case of read/write functions, one may desire to control who writes to the tag. As data move from location to location as part of a tag, one may want to have a system where control codes and encryption techniques and options are available for ones use. Therefore, it is important to control who is going to have access to the data in a tag[1].

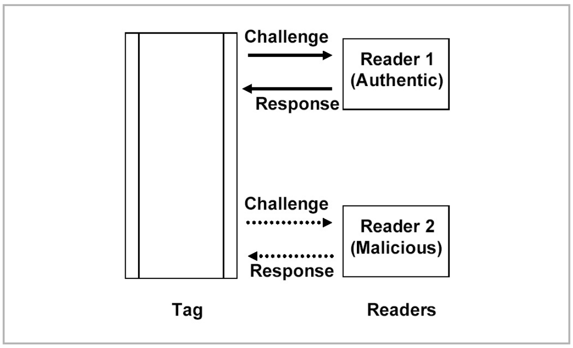


Fig. 1 A challenge/response commands between a tag and readers

Figure 1 shows readers sending challenge commands to the tag with the intention of reading the information stored in the tag. Also, the tag sends response commands to the readers, which could include the identification number of the tag and the information stored in it.

However, there is a tendency that any malicious reader could read the information stored in the tag without the knowledge of the owner of the tag.

Take for example, from fig.1, reader 1 is the authentic reader and reader 2 is the malicious reader. From this example we deduced that there are three problems that can be generated:

(a) Lack of Confidentiality: Reader 2 could gain access to the information in the tag without the knowledge of the owner of the tag and steal personal/private information in the tag once it has access to the tag and this will lead to the violation of privacy/confidentiality of the owner of the tag.

(b) Lack of Availability: Reader 2 could deny Reader 1 from accessing the information in the tag and this will lead to the denial of service for reader 1.

(c) Lack of Integrity: Reader 2 could modify the information in the tag.

However, out of the three problems listed above we are considering solving only the first problem that is, lack of confidentiality.

2.1 Previous work

Few works have been done regarding RFID security and authentication.

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[3].

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[3].

c. The Active Jamming Approach - An

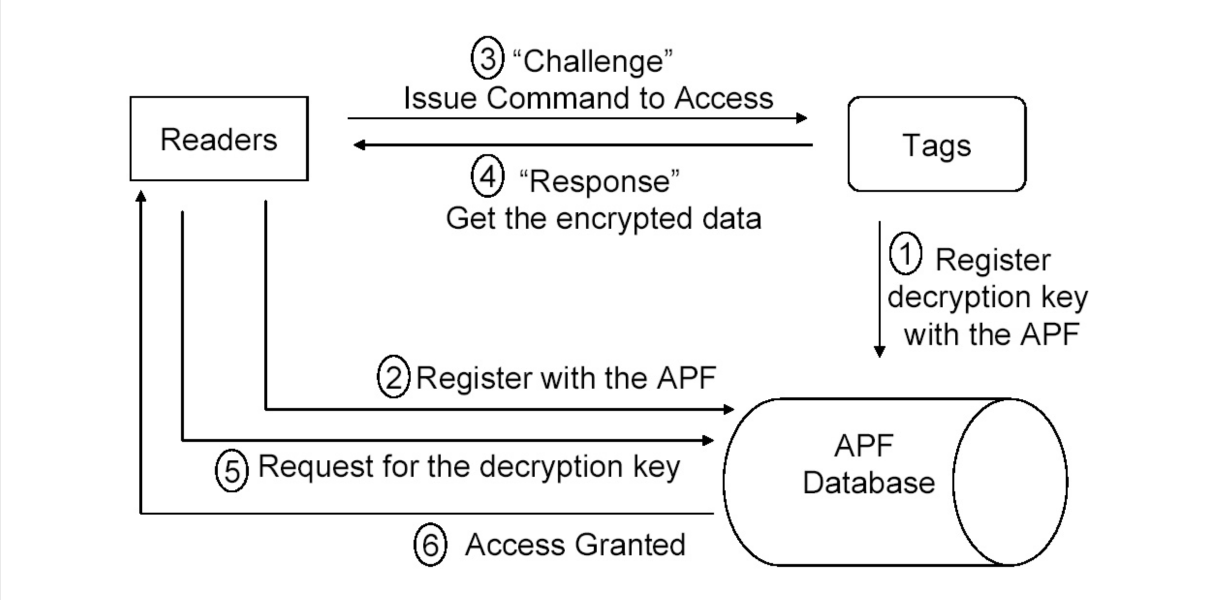


Fig.2 The Flowchart of the APF Framework

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[4].

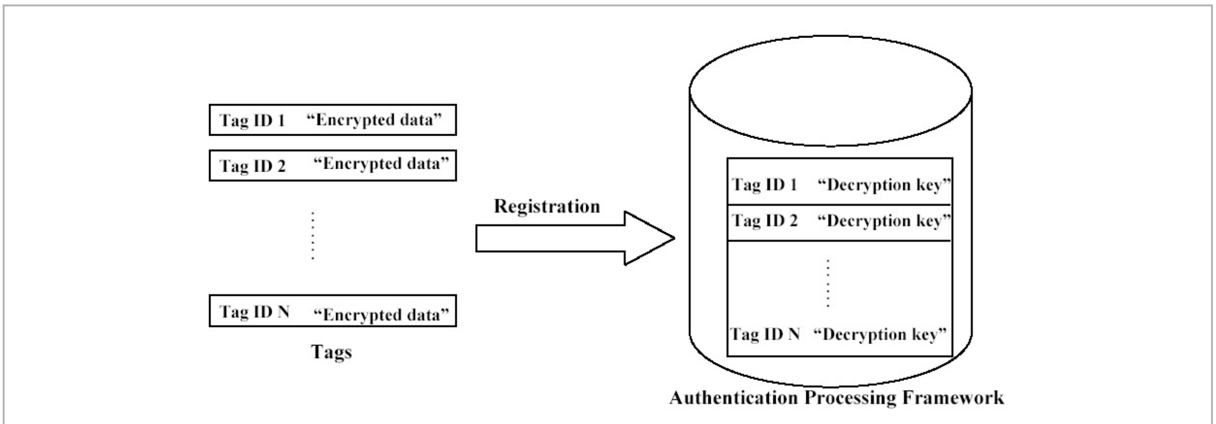
d. The Blocker tag Approach - The blocker tag is the tag that replies with simulated signals when queried by reader so that the reader can not trust the received signals. Like active jamming, it may affect the other legal tags[4].

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.

3 The proposed authentication processing framework

In this paper, we are proposing an APF (Authentication Processing Framework) which registers reader before it gains access to the information in the tag. Authenticating the reader prior to reading from and writing to the tag will protect the unauthorized access of malicious readers to the tag. This is the reason why we are proposing the Authentication Processing Framework (APF) as a procedure that could solve illegal access of malicious readers to the tag. In the next paragraph, we will explain the APF procedure and how the APF framework could overcome the problem of malicious reader's illegal access to the tag which could result into the violation of privacy.

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 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


Tag ID 1 "Encrypted data"
Tag ID 2 "Encrypted data"
Tag ID N "Encrypted data"
Tags
Registration
Tag ID 1 "Decryption key"
Tag ID 2 "Decryption key"
Tag ID N "Decryption key"
Authentication Processing Framework

Each transponder registers its unique ID number and key with the APF

Fig.3 *The Registration of Tags with the APF*

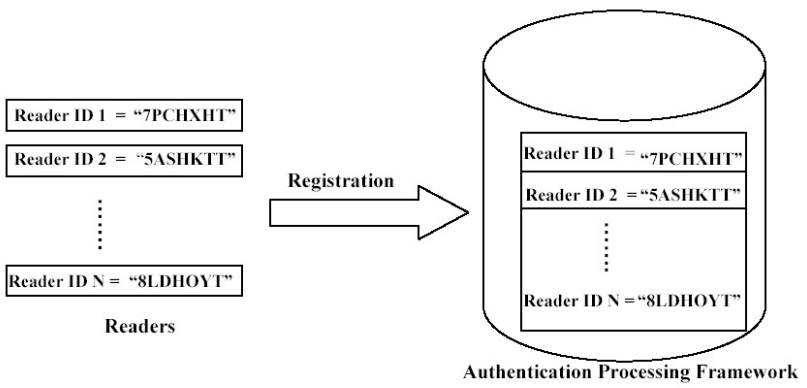
message from the tag will instruct the reader to get the decryption key from the APF database in order to decrypt and read the data in the tag. Since, authentic readers would have registered with the APF database, only authentic readers would be given the decryption key to decrypt the encrypted data in the tags.

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 fig.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 information in 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.

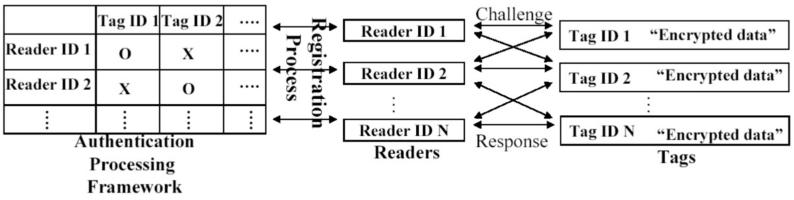
From Fig.4 every reader registers its unique identification number with the APF. Since both readers and tags register their identification numbers with the APF, these serve as a mutual authentication and protect the information in the tags from malicious readers which is one of the concerns users have. 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 and tags.

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



Each Reader registers its unique ID number and key with the APF

Fig.4 The Registration of Readers with the APF


Registration Process
Challenge
Response
Reader ID 1
Reader ID 2
Reader ID N
Readers
Tag ID 1 "Encrypted data"
Tag ID 2 "Encrypted data"
Tag ID N "Encrypted data"
Tags
Authentication Processing Framework

	Tag ID 1	Tag ID 2	....
Reader ID 1	O	X	....
Reader ID 2	X	O	....
⋮	⋮	⋮	⋮

O-means access granted X-means access denied

Fig.5 The Registration/Access Control of Readers to APF/Tags

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.

Also from fig.5, it shows that unregistered readers for a particular tag cannot have access to the information in the tag that it did not registered for. For example in fig.5, reader 2 did not register to have access to tag 1 and that means reader 2 cannot get the decryption key to access the information in the tag 1. However, reader 1 can get the decryption key to access tag 1 because it registered with the APF to access the information in it. Moreover, reader 1 cannot get the decryption key to access tag 2 because it did not register with the APF to access the information in tag 2. However, reader 2 can request for the decryption key to access the information in tag 2 since it registered with the APF to access tag 2.

4 Conclusion

Tags can be protected from illegal access by unscrupulous readers through the authentication procedures of the APF systems as we have described above, it is very imperative to protect the illegal access or unauthorized access in order to prevent the violation of privacy and confidential information stored in the tag. Moreover, the above framework is a mutual authentication which makes it a system that will be able to protect unauthorized readers from accessing information in the tag. We believe that the APF-Authentication Processing Framework will be a good procedure to achieve this.

References

1 J.D.Gerdeman, RFID Radio Frequency Identification Application 2000, Research Triangle Consultants, Inc., 1995.

2 Alain Berthon, “Securityi n RFID”, http://www.nepc.sanc.org.sg/html/techReport/N327.doc July 27th 2000

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

4 Juels Ari et al, The Blocker Tag, Selective Blocking of RFID Tags for Consumer Privacy 2003, http://www.rsasecurity.com/rsalabs/staff

***AYOADE John Olurotimi**, Ph.D.*

Expert Researcher, Security Advancement Group, Information and Network Systems Department

Information Security

***TAKIZAWA Osamu**, Ph.D.*

Senior Researcher, Security Advancement Group, Information and Network Systems Department

Contents Security, Telecommunication Technology for Disaster Relief

NAKAO Koji

Group Leader, Information and Network Systems Department

Information Security