CRYPTOGRAPHY AND AUTHENTICATION PROCESSING FRAMEWORK ON RFID ACTIVE TAGS FOR CARPET PRODUCTS

Shadi Oyarhossein
eCommerce senior speciallist of Iran Center for eCommerce Development (ICeCD) of Islamic Republic of Iran Ministry of Commerce
Shady_oyar@yahoo.com
Dr.S.Mohammadi
Associated professor, Industrial Engineering Department, K.N.Toosi University of Technology,Tehran, Iran ,

Abstract

The Carpet industry is one of the most important sectors of many third word countries such as Iran.
The object of this paper is to propose on idea called APF (Authentication Processing Framework) as one of the ways to deter the growing concerns (transponder) which could result in to the violation of information stored in the carpet tag. Tags are embedded on the upper part of carpet products such as a rug and high – value carpet. To determine whether a product is counterfeit, tag authentication on that carpet product can be performed and this will advise us whether the carpet product is genuine or faked .while similar industries such as apparel-industry uses "passive tags" to identify items ,this paper suggest to use "active tags" for having a better level of security & manageability. This will be followed by an efficient model for handling active tags and their relationship with the readers.
Keywords: RFID, APF, Cryptography, Active Tags, Carpet Products

1 Introduction

Radio Frequency Identification (RFID) technology has been used for over half a century, primarily by the military.[1] As technologies continue to advance forward in antenna technology, microchip fabrication and radio spread spectrum, RFID is rapidly pushed to the existing markets with diversified applications, such as automatic tariffs payment in public transport, animal identification and tracking, and automated manufacturing and logistic control. RFID technology is facilitate information sharing in decentralized business environments such as supply chain. Atypical RFID system will consist of a tag, a reader, an antenna and a host system. Most RFID tags are passive which means that they are battery-less and that they obtain power to operate from the reader. While some are battery powered tags which means they are active and do not need power from the reader to function. RFID tags are tiny computer chips connected to miniature antenna that can be affixed to physical objects (Berthon 2000).[1] In the most commonly touted applications of RFID, the microchip contains an Electronic Product Code (EPC) with sufficient capacity to provide unique identifiers for all items a radio signal, tags in the vicinity respond by transmitting their stored date to reader. With passive (battery-less) RFID tags, read-range can vary from less than an inch to 20-30 feet, While active (self-powered) tags can have a much longer read-range. On one hand, we will discuss the importance of RFID system and other hand, we will discuss about the security implications that the RFID systems have over consumers' privacy and security. Regarding RFID security, few issues are related to the date protection of the tags, message interception over the air channel, the eavesdropping within the interrogation zone of the RFID reader.

In general, there are two approaches to provide this data security on the RFID tag.[1] Data encryption is one of the approaches to be stored on the tags. In doing so , the data can be protected in chipper text format instead of in clear text format. The data retrieved by any unauthorized readers will show no interests to attackers, unless they are able to decrypt all the information. Authentication between the RFID reader and the tags is another approach. It means that normal information retrievals from the tags to the reader can be allowed to proceed, provided that authentication has been done before. Thus, both the reader and the tags identify they are the right parties to exchanges information. RFID system has many beneficial uses as it can be applied to many areas of our day to day

978-1-4244-4817-3/09/$25.00 ©2009 IEEE

activities. Since RFID tags responds automatically to any reader, that is, they transmit without the knowledge of and this property can be used to track a specific use or object over wide areas. While expectations are growing or the use of RFID systems in various fields, opposition to their use without the knowledge of the user is increasing furthermore if personal identify were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. For example Tags are embedded inside Carpet products can be performed and this will advise us whether the Carpet product is genuine or faked. In this APF, the tag security is targeted for active RFID tags because active tags can have a much longer read in compare of passive tags.

2 Related work on RFID privacy and authentication schemes

Industrial professionals, research, as well as standardization bodies are all looking for and expect an effective RFID system to make it as a promising pervasive computing that is possible to apply in commercial applications, particularly Carpet business. In Carpet business its size is too big for stored all information about, brand, design, electronic identify certificate and other important information in tag so it is necessary to use active tag because its don't have any limitation in resource and capability.

2.1 Active tag

An active tag is an RFID tag that incorporates a battery, and can communicate with a reader that is several tens of meters away (there are tags that can communicate at several hundred of meters)[7]. While passive tags can only respond to an electromagnetic wave signal emitted from a reader, active tags can also spontaneously transmit an ID .There are various types of transmission opportunities such as the very common periodic transmission type, or the unscheduled transmission type such as when there are changes in vibration or temperature or when a button is pushed. In many cases, the ID data comprise tens of bits. Generally, systems that employ active tags comprise the tags, a reader, and a server. The tag spontaneously transmits its ID. For example, if the tag is a periodic transmitting type, the tag transmits its ID once every several second. When the reader receives the ID, it notifies the server of the ID via the network, ad based on the ID the server executes the target service.

2.2 System Architecture

In order to resolve privacy, we adopt the basic architecture shown in figure 1.

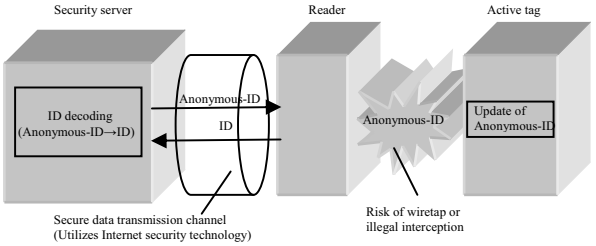

Figure 1. Basic architecture

At a transmission opportunity, the tag outputs a temporary ID called an anonymous-ID transmits a different random value each time. For this reason, if the Anonymous-ID are collected and analyzed by eavesdroppers, the Ids can only be recognized as unrelated random number sequences, and they cannot be determined to be from the same ID. Certainly, the frequency that the Anonymous-ID is updated can be changed to satisfy the privacy protection level.
The security server decrypts the Anonymous-ID into the original ID. The decoded results are obtained only by a reader that has the acquisition authorization for that ID. In this way, threats to content privacy and location privacy caused by readers with out authorization having unlimited access can be avoided. The reader authentications, its ID acquisition authorization, and secure communications between the reader and the server, take advantage of the existing Internet security technologies.

2.3 Anonymous-ID Generation Methods

This paper uses the three schemes described below as methods for generating Anonymous-ID for carpets.
2.3.1 Probabilistic encryption scheme
Inside the tag, a probabilistic public key encryption scheme[4] is implemented, and this scheme generates a different Anonymous-ID each time Probabilistic encryption is an encoding scheme in which a different text is generated each time and it is difficult to determine the degree of relatedness among the generated cipher text. More specifically, even if the same ID is encrypted , the first encryption results and the second encryption results are totally different and unlikable Since, in this scheme, information such as the secret key is not stored in the tag it is highly resistant to tampering . However, since the ID is stored as plain text, it is possible that the ID can be disclosed by tampering. Whether or not this type of self-disclosure can be linked to a threat to privacy depends on the circumstances.
In regard to these problems, a function called re-encryption is effective. In this re-encryption function, without decryption one cipher text is generated from

another cipher text by using only the public key. Regardless of the number of times re-encryption is performed, the plain text can be obtained by performing decoding once. If this re-encryption function is used, the encrypted ID can be stored inside the tag, and even the danger of disclosing the original ID due to tampering can be abated.

2.3.2 Common key encryption scheme

When public key encryption, which incurs a large calculation load, is used in the probabilistic encryption scheme[1,4,11], the battery life is curtailed in applications such as the active tag, which has limited calculation resources. To address this, we propose using a method that employs common key encryption, which has a far lower calculation load compared to that for public key encryption. Common key encryption itself does not provide properties such as probabilistic encoding and re-encryption. Common key encryption and random number generation are implemented in the tag, and the original ID and secret key are stored in the tag as well. When the ID and the random number are combined and encrypted by the secret key. Therefore, each time a different Anonymous-ID can be generated.

In comparison to the probabilistic encryption scheme, the common key encryption scheme has a small calculation load; however, since the secret key must be stored in the tag, it is extremely vulnerable to tampering. Since the secret key must be shared among multiple tags, when disclosing the secret key other tags can also be decrypted and privacy can no longer be protected. The reason that the secret key must be shared is described in the following. If the secret keys are individualized, the server must know which secret key to use for the decoding. In order to make that discrimination, additional information such as an ID key number must be included, and the fixed ad unique characteristic of this form would case new privacy violations.

2.3.3 Hash-chain scheme

In order to address the issues related to the probabilistic encryption scheme and common key encryption, we believe that applying the Hash-chain scheme[1,4,11]

Here after, a simple explanation of the function of the Hash-chain scheme is given using Figure 2. When the tag updates the ID, (1) local variable α is input into Hash function H and (2) α is updated. Next, (3) α is input into Hash function G, and (4) Hash value β is updated as the Anonymous-ID. At the next transmission opportunity, the tag transmits β. The corresponding relationships between the original ID and the initial value of α are safely managed in the server as secret information.

Based on the randomness of Hash function G, the Anonymous-IDs, β, generated each time are different and unlink able to one another. Since this process is one way, there is no way to retrieve the internal secret information, α, from β. The secret information inside the tag, α, is updated one-way each time α is read using Hash function H. For this reason, even if a third party knows α through tampering, the third party cannot know the retroactive values of α. As a result, previous values of the Anonymous-ID, β, cannot be investigated.

In this way, even if tampering of the secret information in the tag occurs, the previous information up to that point (cipher text, signature, etc.) is protected by the characteristic called forward security. The Hash-chain scheme provides this characteristic.

However, the main issue of this scheme is the limited scalability of resolving the IDs at the security server. Different from encryption, hash functions are one-way functions. For this reason, to resolve the original ID, the server must repeat its calculation until it obtains the identical match to the Anonymous-ID (β) received from the tag by retesting the same procedures that are performed by the tag for each of the initial values of α, which has a one-to-one correspondence to the original ID. As a result, as the number of IDs managed at the server increases the decoding processing time increases. However, if the server disk capacity is sufficiently large that the corresponding tables for all of the β values and IDs can be generated beforehand, the IDs can be resolved in a $\log_2$ (N. M) level of retrieval processing time, where N is the number of Ids and M is the envisioned maximum number of reads.

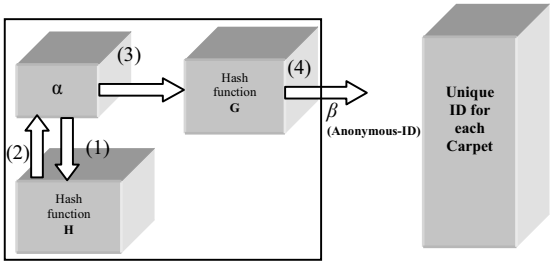

Figure. 2 Hash-chain scheme

3 The Proposed Model

Primarily Hash-chain scheme generate Anonymous-ID then each Anonymous-ID correspondence to the unique ID for carpet product. In this paper propose authentication framework for describe communication between tags and readers in Carpet Industrial, Furthermore use from special database for carpet products.

This is a framework that makes it compulsory for th readers to authenticate themselves with the APF database before they can access registered tags.

In order to prevent illegal access to the memory segment of tag there should be a procedural access control to the memory segment of the tag.

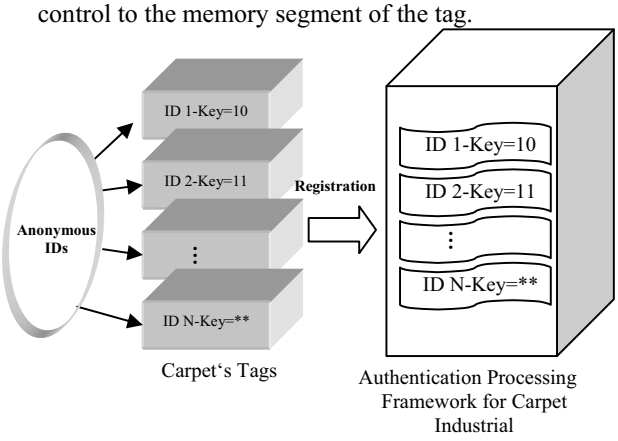

Figure 3. The registration of tag with the APF

From Figure 3, each tag memory segment will register its unique ID and the access key to the memory of the tag with the APF. This means both the unique access key and the data in the tag will be encrypted and the access key will be registered with the APF. This is necessary for the protection of tag from unscrupulous readers that have ulterior intention. Once tag registers its unique identity and access key with the APF, it will be difficult for any reader to have access to the memory segment of the tag without possessing the access key to the tag. We will discuss about how the authenticated reader would have access to the memory segment of the tag.

Furthermore, every reader will register itself with the APF in order for it to be authenticated prior to the time the reader will request for the 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 encrypted key to the reader in order to read the encrypted data in the specific tag.

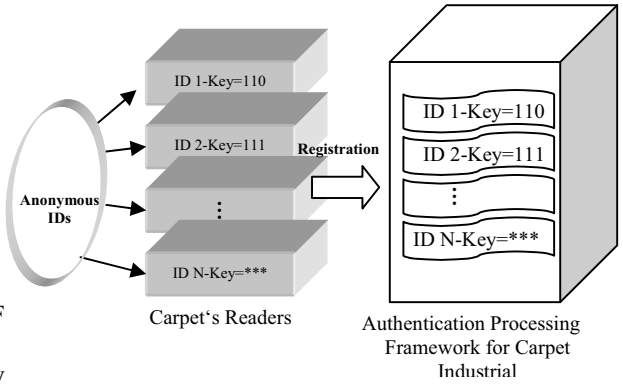

Figure 4. The registration of readers with the APF

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, this will serve as a mutual authentication and will protect tags from malicious readers which is one of the concerns users have for the full realization of the RFID systems. This means that unauthorized access into the tag will be eradicated if APF framework is implemented and used.

In the previous paragraphs we discussed about the registration of the tag memory segment’s unique identity and access key with the APF. Also we discussed about the registration of readers with the APF prior to accessing the tags. When the reader sends a read ‘‘command’’ to the tag, the tag will reply with its identification number and the encrypted data, this means that only registered reader with the APF will be able to get the decryption key to access the encrypted data. Once the key is received the data in the tag will be readable (Figure 5).

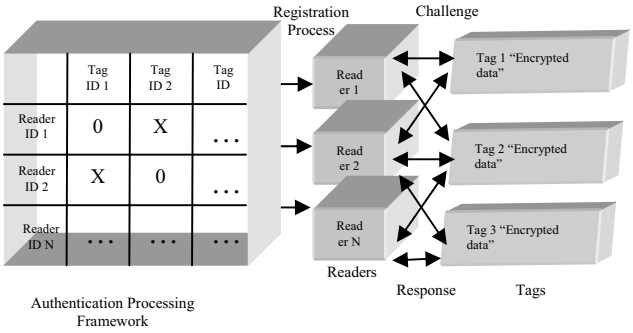

Figure 5. The registration of readers to the APF/tag

In this framework, there are two important processes, the first one is that, mutual authentication will be carried out by the APF because it authenticates the reader and the tag.

Secondly, the privacy concern will be guaranteed because the data stored in the tag are 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.

3.1. The flowchart of the APF framework

The flowchart of the APF framework is given in Figure 6.

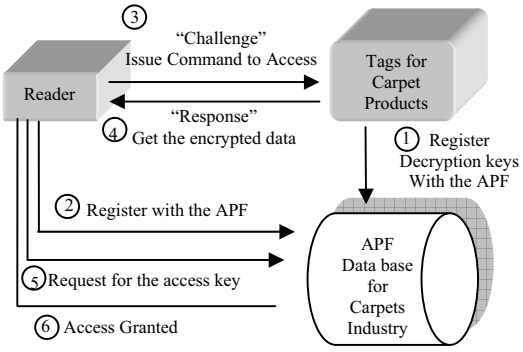

Figure 6. The flowchart of the APF framework

3.2. The importance of the APF

3.2.1 It prevents malicious readers from reading the information in the tags.
3.2.2 It permits consumers their wishes for RFID tags to remain operative while in their possession.
3.2.3 It also helps to authenticate both tags
and readers that is, it deploys mutual authentication.

4 Conclusions

This paper examined related works on RFID privacy and authentication schemes with the goal of reaching to an ideal model for secure sell of carpets. It has been recognized that the carpet industry suffers from an insecure market environment as well as undesirable relationship between active tags and the readers in the similar industries. Therefore, the related technologies such as authentication on RFID active tags have been discussed. The main contribution of this paper can be divided into three parts. In part one, the impotence of usage of Active tags instead of Passive tags are discussed and shown. For the first time, the paper suggests that RFID Active tags can be a suitable too to provide a secure market for carpet industry. Secondly, while the paper discussed and compared usage of the three different schemes suitable for provision of Anonymous-IDs for carpets, it introduces Hash-chain scheme as the more suitable method for creation of anonymous-IDs for carpets. At the end, an active tag prototype that enables ID encryption and restriction – less update control, implemented.

The APF provides assurance to the RFID users that the information stored in the tag is secured in the sense that only authenticated reader by the APF can have access to the tag. The reason for this is that, the information received by the reader from the tag is encrypted and this information can only be decrypted by getting the decryption key from the APF. Also, the reader that did not register with the APF previously, it gets the information from the tag.
At last, tag authentication on that carpet product can be performed and this will advise us whether the carpet product is genuine or faked.

References

[1]:Krik H.M.Wong,patrickC.LHui,Allan ck chan, Cryptography and authentication on RFID passive tags for apparel products,computers in Industry 57 (2006) 342-349, **,21 november2005** www.elsevier.com/locate/compind.
[2]: Jad S. Rasul , , Chip on paper technology utilizing anisotropically
conductive adhesive for smart label applications, Microelectronics Reliability 44(2004) 135-140, July 2003, www.elsevier.com/locate/microrel.
[3]: Selwyn Piramuthu, Protocols for RFID tag/reader authentication, Decision support systems 43 (2007) 897-914, 2 January 2007,www.elsevier.com/locate/dss.
[4]: karl Christian, maria elisabet Oswald, Side Channel Analysis of Stream Ciphers, Institute for Applied Information Processing Communication (IAIK),Graz university of Technology,2004.
[5]: Hung-Yu Chien a, Che-Hao Chen b, Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards,computer standards & Interfaces 27 (2007) 254-259, www.elsevier.com/locate/csi.
[6]: Rene Mayrhofer a Florian Ortner a Alois Ferscha a Manfred Hechinger , , Securing Passive Objects in Mobile Ad-Hoc
Peer-to-Peer Networks,electronic notes intheoretical computer science 85 (2003),www.elsevier.com/locate/entcs/volume85.html.
[7]: WOWGAO INC, Applications of Active Tags, Global Relcase Distribution,jan 08,2007,www.epcglobalinc.org/standards-technology/specifications.html.
[8]: Alex P.J. Hum, , Fabric area network ± a new wireless communications
Infrastructure to enable ubiquitous networking and sensing on
Intelligent clothing,computer network 35 (2001) 394-399, www.elsevier.com/locate/comnet.

[9]: Samuel Fosso Wamba_, Louis A. Lefebvre, Ygal Bendavid, ´ lisabeth Lefebvre, Exploring the impact of RFID technology and the EPC network
On mobile B2B eCommerce: A case study in the retail industry,production economics, 6 fabruray 2007,www.elsevier.com/locate/igpe.
[10]: Roger Smith , RFID: A Breif Technology Analysis,
RFIDconference,2004,www.rfidjournal.com/article/whitepaper/1-123.
[11]: miyako ohkubo,koutaro Suzuki and shingo kinoshita, Cryptography Approach to Privacy-Friendly Tags,RFIDconference,
Jan2005,www.rfidjournal.com/article/whitepaper/2-023.html
[12]: Eleonora Bottani_, Antonio Rizzi, , Economical assessment of the impact of RFID technology and EPC system on the fast-moving consumer goods supply chain, ,28 February 2006,www.elsevier.com/locate
[13]:Hung-Yu Chien, Che-Hao Chen b, " Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards", June 2006,computer standards &Interfaces,www.elsevier.com/locate/sce.