12

Smart RFID Security, Privacy and Authentication

Mouza A. Bani Shemaili, Chan Yeob Yeun and Mohamed Jamal Zemerly
Khalifa University for Science, Technology and Research
United Arab Emirates

1. Introduction

Radio-frequency identification (RFID) is an automatic identification method, used to transmit the identity such as serial number of objects or subjects (people) wirelessly, through radio waves. RFID technology is a new promising technology that will spread in the near future to enter most of our everyday activities.
An RFID system consists of three main components; a tag, a reader, and a server. There are three types of tags as follow:

1. **Passive tag**
   Passive tags need to be beamed by the reader to be activated. Passive tags are also smaller, less expensive than other kind of tags and used for a short range.
2. **Semi Passive tag**
   Semi passive tags have an on-board power source to run the tag chip circuit and draw the communication energy from the reader. Besides, semi passive tags have longer read range than the passive tags**.**
3. **Active tag**
   Active tags include miniature batteries used to power the tag, so RFID reader can read active tags at distances of one hundred feet or more. Also, active tags can be used as sensors and are more expensive than other kind of tags. Table 1 shows the advantages and disadvantages of the three types of RFID tags.

Tag Type	Advantages	Disadvantages
Passive	• Longer Life time • Lowest Cost • More Flexible	• Distance Limited
Semi Passive	• Longer range for Communication • Can be used as sensors	• Expensive due to the battery • Cannot determine if the battery is good or bad
Active		

Table 1. Comparison of various types of tags

Some smart tags have memories that can be written into and erased, while others have memories that can only be read, so the cost of the tag depends on the memory size that it contains.

As for the reader it consists of two parts. First part is an antenna which is used for communication with RFID tags wirelessly. Second part is an electronic module that is networked to the host computer through cables and relays messages between host and all tags within antenna's range. Also, the electronic module is responsible of some security functions such as encryption/decryption, and authentication. The last part is the server (a PC or a workstation) which is considered as the brain of an RFID system. The server is responsible of tracking movement and redirecting the objects through the system and verifying identity and granting authorization for the tags. The RFID system communication starts when the reader emits radio waves to query the tag, then the tag transmits its stored data to the reader which will relay the tag's data back to the server. The server is responsible of the following tasks:

1. Controls the system's data purchase.
2. Keeps inventory and alerts suppliers when new inventory is needed.
3. Tracks movement and redirects the objects through the system communication.
4. Verifies the identity of tags and grants authorizations for them. Figure 1 shows the RFID system communication.

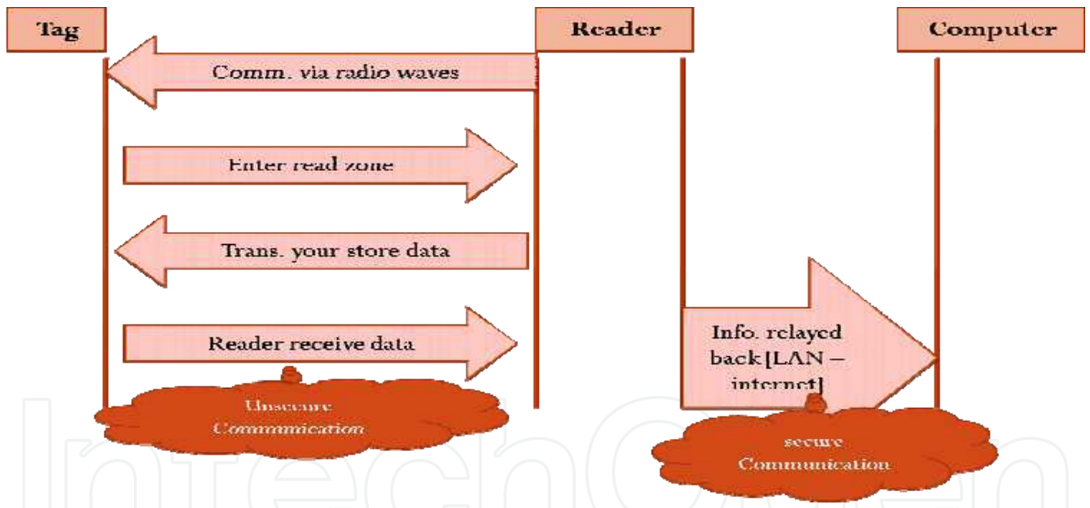


Fig. 1. RFID system communication

RFID technology is predicted to be a substitute for the second generation of the barcode technology since there are four main advantages for the RFID technology over barcode (Hunt ***et al.***, 2007) as follows:

1. RFID eliminates the need for direct line-of-sight reading that the barcode depends on.
2. RFID scanning can be done at greater distances than the barcode scanning.
3. RFID can scan multiple products simultaneously.
4. Since RFID can be used as a unique system identifier and can be used as a product pointer in the database, which can facilitate the tracking of all products history.

Most RFID applications today utilize the passive tags as they are so much cheaper to manufacture and operate over four ranges of frequency. Table 2 shows the comparison between the four different types. The antenna shape is also important to the tag's performance as the larger the antenna, the more energy it can collect.

Microwave 2.45GHz & 5.8GHz	Ultra-High Frequency (UHF) 868- 915 MHz	High Frequency (HF) 13.56 MHz	Low Frequency (LF) 125 KHz	Frequency Range
Longest	Medium	Short	Shortest	Typical Max Read Range
Fastest	Fast	Moderate	Slower	Data Rate
Worse	Poor	Moderate	Better	Ability to read near metal or wet surfaces

Table 2. Comparison between the four frequencies type

Recently, RFID technology can be considered as the niche development technology. However, they have limited power constraint (powerless for passive tags), limited communication range, and a small number of gates for logical operation. All of these limitations led to building RFID systems but without a security aspect. As a result RFID technology now faces some major security issues that may hinder its propagation if not handled properly. In this chapter we will focus on the passive RFID tags and its security development. The rest of this chapter is organized as follows. RFID application examples are pointed out in Section 2. The security challenges and the practical secure implementation of RFID in general and related work are summarized in Sections 3 and 4. The analysis of some of the privacy and authentication solutions are given in Section 5. We describe applications of Smart E-Travel based on RFID in Section 6. We conclude this chapter with future work in Section 7.

2. Application Areas

RFID technology is used anywhere that needs a unique identification system, hence the RFID system able to identify the objects or the subjects by means of the serial number. Thousands of companies worldwide have resorted to RFID systems to improve efficiency in production and to automate routine decision-making. Because, RFID tags can automate the computers to do the next steps, without human interference (Henrici, 2008).

Therefore, RFID applications are widespread nowadays; here we will introduce only some of them as follow:

- **Product tracking:** tracking goods in the supply chain and during the manufacturing process by using Electronic Product Code (EPC) which can provide a unique ID for any physical object.
- **Building access:** allows controlled access to buildings and networks.

- **Human implantation:** implanting RFID tag in the human body, so it can be used for information storage, including personal identification, medical history, medications, allergies, and contact information related to the person with the tag.
- **Hospital:** using RFID for patient identification and portable asset tracking.
- **Libraries:** list a lot of library items in their collections in a short time. To allow users to automatically check out and return library property. Besides speeding up checkouts, keeping collections in better order, RFID provides a better control on theft, non-returns, and misfiling of a library's assets.
- **Transportation:** using RFID in toll collection, ticketing, vehicles tracking, e-Passport, RFID baggage sorting system, and other transport applications. Figure 2 shows some examples of the RFID applications. In Section 6 we give a scenario that shows how RFID technology applies in the airport environment.

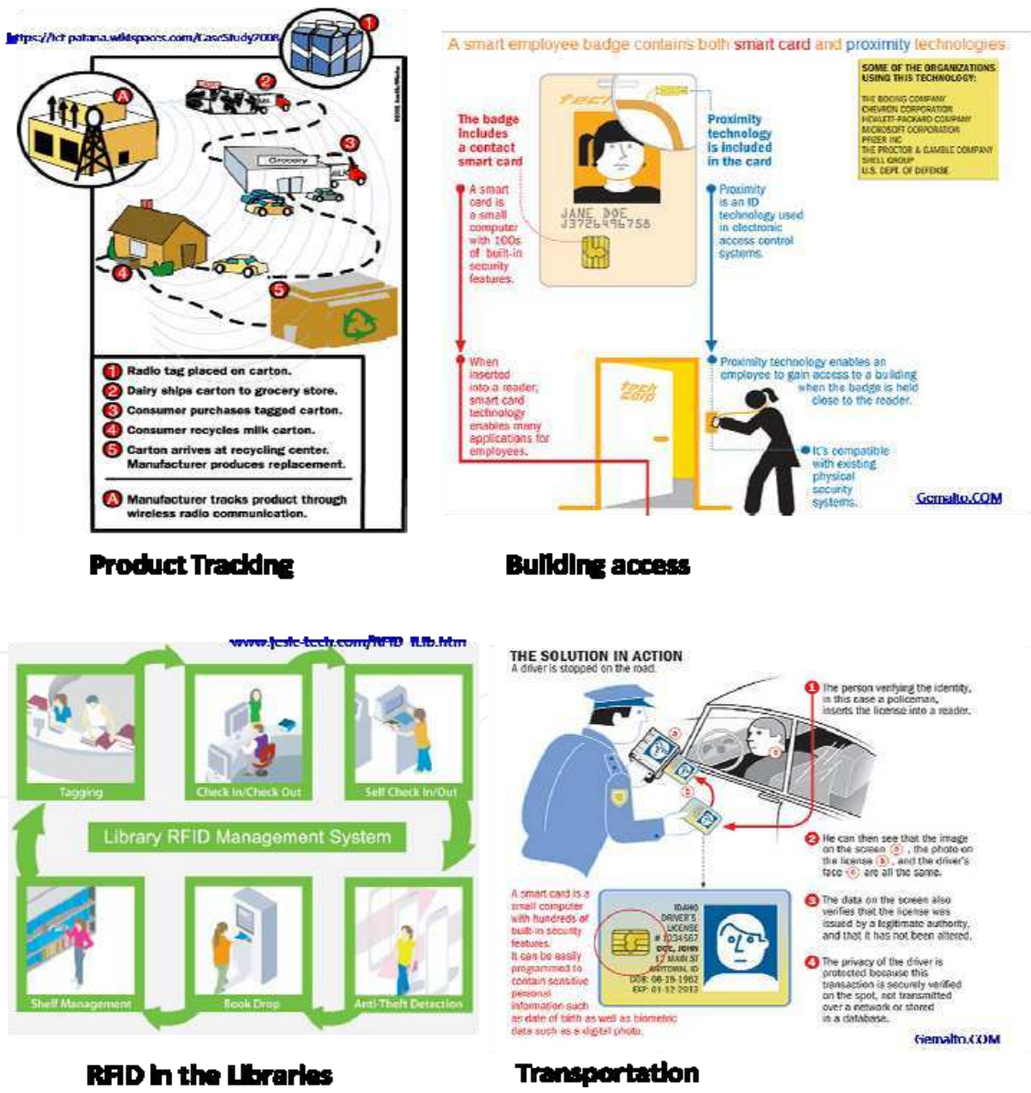


Fig. 2. Examples of RFID applications

3. Security Challenges and Threats

Although the use of RFID tags continues to increase according to a new report from In-Stat (Instat, 2009), which states that over 1 billion tags were produced last year, and by 2010, the number will rise to **33 billion.** However, the RFID technology faces some security threats. Threats are potential events that cause a system to respond in an unexpected way e.g. attacker attacks the system causing some damage to the RFID system (Henrici *et al.*, 2009). Threats to RFID system are categorized into seven threats that are listed below.

1. **Spoofing identity**. Occurs when an attacker successfully gains an unauthorized access to the RFID system. Any attacker with suitable equipment is able to clone any legitimate tag and communicate with a legitimate reader as a genuine tag where in fact it is a fake tag. Figure3 illustrates how adversary could clone RFID tag.

Fig. 3. Process of cloning RFID tag

2. **Tampering with data.** This deals with the tag integrity and occurs when an attacker modifies, adds, deletes, or reorders data in the RFID tag.
3. **Repudiation.** Occurs when a user denies an action that was performed during the execution of the RFID protocol.
4. **Privacy disclosure.** Occurs when information is exposed to an unauthorized user and that can cause some privacy violation. Actually, there have been issues which have arisen from by privacy advocates over the use of RFID tags to track people or their tagged stuff. Also, a tag emits data to any reader without alerting its owner. This can be made worse if the tag contains some personal data such as name, birthday, etc. related to the tag owner so the attacker will not only be able to track the tag owner but also he/she could create a profile that relates to that person. Figure 4 depicts one of the privacy disclosure issues in the RFID.
5. **Denial of service.** This deals with the availability of the tag data and occurs when an attacker denies service to valid users. In the RFID system it occurs when an attacker prevents the tag to update a value after a successful authentication in the RFID protocol.

6. **Elevation of privilege.** Occurs when an unprivileged user can gain a higher privilege in the RFID system than what they are authorized for.
7. **Man–in–the-Middle attack.** Occurs when the attacker creates a connection between the legitimate reader and tag and through this connection the attacker is able to catch the massages between the reader and the tags or even interrupt and modify these messages.

Researchers are currently seeking solutions to solve the security issues in RFID, so it can be proliferated without any shortcomings in the future. In the next section we divide the research work into two major areas.

Fig. 4. Security issues- profiling process

4. Practical secure implementation

In order to build RFID security algorithms, the designer first must understand the applications that RFID systems will be used in, so that he/she can design algorithms with suitable security approach. We can classify the practical security approach into three types (Karygiannies *et al.*, 2008) as follow:

1. **Randomization Approach**

   Random assignment schemes depend on the random number or pseudorandom rotation to create challenges in order to hide the real tag identifiers. We can divide Randomization approach into two types as follow:

   a- **Pseudorandom Rotation**

   Create a list of pseudorandom numbers that are stored in both of the tag and the reader memory. Such approach is like Juels (Juels, 2004) proposed, he

suggested the idea of Minimalist cryptography which consists of storing a short list of random pseudonyms in the tag so each time a tag is queried it emits the next pseudonym in the list until the end of the list. Then it starts from the beginning until it ends. This scheme can be implemented in an RFID tag by just adding several hundred bits of memory to the tag with enabling the read write feature. Using this mechanism helps to prevent the tracking of the tag by illegitimate reader.

Also, (Peris-Lopez *et al.*, 2006) proposed a lightweight mutual authentication protocol based on the idea of Minimalist and index-pseudonyms (IDSs). Each tag stored key is divided into four parts of 96 bits (K= K1||K2||K3||K4), X||Y denotes the concatenation of data items X and Y and they are updated after each successful authentication. This protocol consists of four steps. Tag Identification, Mutual Authentication, Pseudonym Index Updating, and Key Updating. Also, pseudorandom can be generated by implementing a hardware device in RFID tags that present some of the challenge response authentication protocol between tag and reader.

One of the algorithms that used hardware approach is (Lee & Hong, 2006) algorithm that used a pseudorandom pattern generator (PRNG) implementation using linear feedback shift registers with self-shrinking generator (SSG). This algorithm is used to authenticate the tag to the reader by exchanging a challenge-response using SSG.

b- **Random Number**

In the random number approach the tag identifies itself with random identifier that is not related to its serial number such as Meta-id. An example of this approach is **(**Lee & Verbauwhede, 2005) algorithm which is a lightweight authentication protocol that can be used for low cost RFID called Advanced Semi-Randomized Access Control (A-SRAC). First of all, a reader sends a query and a random number Rs to the tag. Then, the tag will generate a random number Rt and send it to the reader with the tag MetaID. After that, the reader relays this message back to the server through a secure channel.

The server looks up the key corresponding to the tag MetaID, then the server will check the uniqueness of the MetaID among other MetaIDs in the system. If that MetaID is not unique then the server will generate random number R2 till it reaches the new unique MetaID. Then, the server will send R2 and h(key||R2||R1) to the tag through the reader. The tag will check the correctness of the message if it is correct then, it will update the previous key with the new key.

2. Encryption Approach

Encrypt the data between the reader and the tags. The tags only store the cipher-text and are not responsible of any encrypt or decrypt operation. The encrypt/decrypt operation are done by reader or other enterprise subsystem components. We can divide the encryption approach into two parts as follow:

a- Secret Key Cryptosystem

This approach needs a shared secret key between reader and tag to encrypt the messages between the reader and the tag. The use of secret key cryptosystem approach can provide either one way or mutual authentication mechanism between the reader and the tag. The Randomized Hash Locks algorithm (Weis *et al.*, 2004) is a lightweight authentication algorithm that can be embedded into low cost RFID tags. Randomized Hash Locks is a scheme for mutual authentication between RFID reader and tag. A reader contains a list of the tags keys and each tag stores its own key. In the first step, a reader sends "Who are you?" message to the tag. Then, the tag will generate a random number R and sends it along with the hash value of the tag stored key. When the reader receives the tag message it will start to compute the hash value for every key in the list and compares it with the tag message. Finally, after finding the corresponding key from the comparison then the reader will send "You must be K" message, which K is the tag identifier, to the tag so the tag will make sure that the reader is a valid one.

Also, (Ilic *et al.*, 2008) proposed the Synchronization Approach as a solution to authentication issues in the RFID system. The scheme verifies and updates the synchronized secrets of tags. It states that each tag has a secret Kx shared in both of the reader and tag memory on every communication between reader and tag. After each communication the secret Kx will be updated between both of the reader and the tag, so it will increase by one and the secret will be Kx+1. Therfore, if a genuine tag identifier and the synchronized secret are copied to a fake tag, and by then the fake tag tries to interrogate with the reader, the reader will be able to detect de-synchronization. This approach is cost-effective and can be implemented in low cost RFID tags.

Moreover, (Song & Mitchell, 2008) proposed a protocol which consists of three exchanges between the reader and the tag. Each tag stores a hash value of string μ [t = h(μ)] unique to each tag. Also, each server stores [(μ,t)new,(μ,t)old, D] where (μ,t) new is the new values of the string μ and corresponding h(μ) = t, and (μ,t)old is the previous stored data, and D is the data of the tag such as price. After a successful authentication both the server and tag will update their values.

Furthermore, (Lu *et al., 2007)* suggested the Key-Updating scheme to solve the problem of keys compromised in tree approach scheme (Molnar *et al.*, 2005) which states that a temporary key is used to store the old key for each non-leaf node in the key tree. For each non-leaf node, a number of state bits are used in order to record the key-updating status of nodes in the sub-trees such as 1 bit for having been updated, otherwise it will have 0 bit. Based on this design, each non-leaf node will automatically perform key-updating when all its children nodes have updated their keys.

Another algorithm that is considered one of the most secure classic algorithms is the One Time Pad (OTP) (Stallings, 2002). Typically, the pad is generated in some random way and is shared between the senders and the receivers. Usually, the key will expire as soon as it has been used once. When a message is to be sent, the sender uses the secret key to encrypt each character, one at a time. The encryption algorithm is simply the XOR operation between the message and the key. Only the sender and receiver have the ability to encrypt and decrypt the message using the

shared secret pads. Once the one-time pad is used, it cannot be reused. If it is reused, someone who intercepts multiple messages can begin to compare them for similar coding for words that may possibly occur in both messages. This algorithm is simple and can be used to secure the unsecure RFID communication. However, OTP has some disadvantages such as having long messages requires long keys. Also, distributing the pad in a secure manner is difficult.

b- Public key Cryptosystem

This approach is similar to the secret key approach but uses two keys: public key and private key. The public key is used to convert from plaintext to ciphertext which will be stored in the tag memory. After that only the holder of the private key will be able to decrypt the ciphertext stored on the tag. The agency that holds the private key must be a trusted agency. An example that uses this approach with a trusted agency is the re-encryption approach that uses the European Central Bank as a trusted third party.

When the European Central Bank proposed using RFID in banknotes (Juels & Pappu, 2003) proposed a re-encryption scheme to solve the privacy issues in the RFID. Re-encryption is changing the appearance of the ciphertext without changing the plaintext. The re-encryption schemes may be done by shops, banks, or by consumers that hold the banknotes. An RFID banknote has a memory that has a serial number, a signature, a cipher text, and a random number which are used in the El-Gamal algorithm (El Gamal, 1985) that is used to re-encrypt the ciphertext and save it in the RFID tags. The drawback of this algorithm is that the re-encryption algorithm may not be done frequently enough.

Universal re-encryption suggested by (Golle *et al.*, 2004) is another algorithm that uses the Public key Cryptosystem. Universal re-encryption is a cryptographic technique that is similar to the El-Gamal cryptosystem except that it does not require a public key. In the universal re-encryption the input plaintext must be encrypted by the recipient public key before it enters the mix servers that consist of a chain of involved servers. Each server involved in the scheme re-encrypts the input ciphertext from the previous server until it reaches the last sever so the recipient should have the whole output ciphertext from the mixnet servers then decrypts them all using his/her private key until it has the match cipher that is encrypted under his/her public key.

This scheme can be used to enhance privacy in RFID tags so they can be re-encrypted under the agency that generates them. For example, a man walking home with his bag that has an RFID tag which can be re-encrypted by the stores related to that bag all along the way to the man's house. Universal re-encryption may be an efficient scheme but it has some limitations such as the recipient should decrypt all the output cipher text to have his/her plaintext.

Next section analyzes the previously mentioned algorithms; however most of the algorithms actually focus either on the authentication or privacy issues. Therefore, in the next section we divided the analysis of the algorithms into two parts: privacy solutions analysis, and authentication solutions analysis.

5. Analysis of the privacy and authentication solutions

We can evaluate the RFID privacy and authentication algorithms based on four categories as the following:

1. **Cost and Complexity:** which depend on the memory size of the RFID tags and the number of gates that may be needed for the algorithm, adding these to the tag can affect the tag cost. Since RFID tags are used in large scale, so the cost of the tag depends on how much of the resources the algorithm will use, so we need to reduce the size of the memory needed for the algorithm and the number of the gates. Therefore, in designing RFID algorithms there is a need to try to create a simple algorithm that needs a small amount of memory and gates. For example, for the SHA-1 algorithm about 4200 gates are required where lighter hash algorithm need about 1700 gates (Yu *et al.*, 2004) which makes this algorithm less complex than the SHA-1 algorithm.

2. **Performance:** we can measure the performance of the RFID algorithm by estimating the times of each message round trip, the time to retrieve the data from backend server, and to read and write the data to the tag. So the performance can be improved by reducing the size and the number of the messages in the algorithm. For example, public key algorithms are slower than secret key algorithms, so the public key algorithm must be used in case the message is so small, but if we have large amount of data then secret key algorithm will perform better.

3. **Availability:** the RFID system is used in critical businesses that the system must be available all the time such as using RFID in a supply chain. Therefore, the availability of the system must be guaranteed during the execution of the algorithm.

4. **Anonymity:** Tags must have anonymity to prevent the tracking problem. So, the tag response must appear as a random number and refreshed frequently so the attacker will not be able to trace.

This subsection uses the four categories that are mentioned above to evaluate the RFID security algorithms. Here is the analysis of each algorithm after dividing the algorithms into two parts as follow:

5.1 Privacy Solutions Analysis

1. **Minimalist:** (Juels, 2004) points out that needs more memory to store the list of pseudonyms and the communication cost per session will be a little bit costly. On the other hand, the performance of the protocol is good since the computation in the tag side will be limited to some string comparisons and XOR operation. Furthermore, Since Minimalist list use two exchange identifiers and refresh the pseudonyms after each successful authentication in the protocol it will help to prevent the denial of service attack and tracking problem so the algorithm can provide the availability and the anonymity features.

2. **Re-encryption scheme and universal re-encryption**: Since re-encryption and universal re-encryption schemes use public key cryptographic scheme then the cost of the algorithms will be costly since these schemes need more memory. The complexity of these algorithms increases with the number of logic gates. Moreover, these algorithms will need a lot of computation on the server side which will lead to slower response from the server side and will take time to write the cipher text on the tag chip so the performance of the algorithms will be affected. However, these algorithms can provide anonymity to the tag identifier by re-encryption scheme.

5.2 Authentication Solutions Analysis

1. **Peris-Lopez Algorithm**: Since this algorithm uses as a basis the Minimalist algorithm then the algorithm will face the same conditions, so the algorithm will be a little bit costly. Moreover, this algorithm does not need a lot of the computation power by either of the tag or the server side so it will perform very well. However, the algorithm faces Desynchronization attack (Li & Wang, 2007) so the availability of the system cannot be ensured all the time. Finally, the algorithm uses four keys to ensure the anonymity of the identifier.

2. **SSG Algorithm**: this is a low cost and simple algorithm that uses small size of memory with a small number of gates compared with other security algorithms. Moreover, the messages of this algorithm can transfer quickly between the tag and the server so the performance of the algorithm is good. But, the algorithm is vulnerable to Desynchronization attack so the availability of the data is an issue here. Finally, the algorithm is able to change the identifier after each successful authentication.

3. **A-SRAC**: the algorithm uses simple computation so it is not that costly or not a complex one. Moreover, the number of the sent messages and the size of the messages are small so the algorithm performance is good. Also, the server saves the old and the new data to prevent Denial of Service (DoS) attack. Also, the algorithm uses Meta- id to prevent the tracking of the tag.

4. **Randomized Hash Locks**: heavy weight solution if the key list is long and it could be costly. Besides, the algorithm is not resistance to DoS attacks. Yet, the algorithm is able to prevent tag trace identifier using hash algorithm.

5. **Synchronization Approach**: simple and does not need a lot of memory size so the algorithm is cheap with low complexity. However, the algorithm is vulnerable to Desynchronization attacks. Finally, the algorithm is able to provide anonymity since the identifier is different in each session.

6. **Song and Mitchell Algorithm**: this algorithm uses simple computation and little memory size so it is simple with low complexity. In addition, since the server stores the old and the new values of the tag identifiers then the algorithm can

provide better availability. However, the algorithm is vulnerable to face attacks that prevent the anonymity of the tag identifier.

7. **Lu *et al.* Algorithm:** this algorithm needs a lot of communication and comparison on server side so its performance is not that good. However, the algorithm is able to prevent DoS attacks and maintains the anonymity of the tag by using more than one key for each tag. Table 3 shows a summary of the algorithms with their evaluation.

In the next section we present an application of how to implement RFID in the airport considering the security aspects that were previously mentioned. Moreover, we think that the real problem in most of this technology implementation is that it is applied without considering the security threats. Therefore, the real challenge can be how to apply the RFID technology in a safeguard way.

Algorithm	Algorithm Solves		Cost Complexity	Performance	Availability	Anonymity
	Privacy	Authentication				
Minimalist	√		X	√	√	√
Peris-Lopez Algorithm		√	X	√	X	√
SSG Algorithm		√	√	√	X	√
A-SRAC		√	√	√	√	√
Randomized Hash Locks		√	X	X	X	√
Synchronization Approach		√	√	√	X	√
Song and Mitchell Algorithm		√	√	√	√	X
Lu *et al.* Algorithm		√	X	X	√	√
re-encryption scheme	√		X	X	N/A	√
universal re-encryption	√		X	X	N/A	√

Table 3. Summary of the proposed algorithms with their evaluation

6. Smart e-Travel Scenario

First of all, we aim to use e-passport with RFID chip in a secure manner. We will focus here on the authentication issues. In the beginning, each e-passport holder must authenticate himself to the e-passport issuer authority by providing his picture and fingerprint to adjust this data to each passport holder in a safe database. Then the E-passport tag will only contain the encrypted password of the matched tag holder data in the database. Now we can state the e-passport holder application in the airport as follow:

The passenger holds his e-passport (e-passport contains encrypted data that identifies the passenger) and enters the airport. At the check-in point, there is a reader that reads the encrypted data in the passenger e-passport then it will match this data to the data in the back end database. If there is a match then the passenger is considered as an authorized person in the airport environment, and can enjoy the facilities of the airport. After the authentication process the reader will ask for the mobile number of the passenger, the passenger mobile must be able to read RFID tags (Evans, 2005). Then some applications will be downloaded to the passenger mobile so now he/she can tour in the airport easily using this application. The application can read the tags in the airport and show the passenger the airport facilities such as airport bathroom, or coffee shops. Moreover, when the passenger luggage which contains an RFID tag to facilitate luggage tracking securely reaches the flight then, the passenger will be notified by sending an SMS message to his/her mobile to inform him/her about the place of the luggage.

Of course, this scenario needs security features, so that nobody except the airport authority can read the passenger personal data. Also, no unauthorized person can fool the airport reader and enters the airport as an authorized one.

7. Future Work

The scenario described in Section 6 requires a lightweight mutual authentication protocol that meets all the evaluation categories. Moreover, the proposed solution needs to have low cost and can easily be implemented. It is envisaged that the algorithm will be based on the Shrinking Generator (SG) mechanism. The idea of SG can be used to provide cryptographic services to secure the communication over unsecured channels and it is suitable to be implemented in RFID system.

In summary, the RFID systems are emerging technologies that will propagate in our daily life in the future. However, these technologies have some security concerns especially in the privacy and authentication issues. This chapter reviewed some of the proposed solutions to solve the privacy and authentication issues in the RFID. Also, this chapter analyzed the proposed solutions upon some evaluation categories. In the end, the chapter shows a senario of how to implement the RFID technology in the airport in security manner.

8. References

El Gamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms, *Proceedings of CRYPTO 84 on Advances in cryptology*, Santa Barbara, California, United States, Springer-Verlag New York, pp. 10-18.

Evans, M. (2005). Prototype Nokia 3220 NFC RFID phone could reshape society, Mobile Mentalism.com, http://mobilementalism.com/2005/12/12/prototype-nokia-3220-nfc-rfid-phone-could-reshape-society

Golle, P. ; Jakobsson, M., Juels, A. & Syverson, P. (2004). "Universal encryption for Mixnets", *Proceedings of CT-RSA 2004,* In T. Okamoto (Ed.), LNCS 2964, pp. 163–178.

Henrici D. (2008). *RFID Security and Privacy Concepts, Protocols*, and Architectures, Springer.

Henrici, D.; Kabzeva, A., & Mueller, P. (2009). RFID System Architecture Reconsidered, In: *Development and Implementation of RFID Technology*, Turcu, C. (Ed.), In-Tech.

Ilic, A.; Lehtonen, M., Michahelles, F. & Fleisch, E. (2008). Synchronized Secrets Approach for RFID- enabled Anti-Counterfeiting, *Proceedings of Demo at Internet of Things Conference 2008*, Zurich, Switzerland.

Instat (2009). RFID Tag Market to Approach $3 billion in 2009, http://www.instat.com/newmk.asp?ID=1206

Juels, A. (2004). Minimalist cryptography for low-cost RFID tags, *Proceedings of Int. Conference on Security in Communication Networks – SCN 2004*, LNCS 3352, Amalfi, Italy, Springer-Verlag, pp. 149-164.

Juels, A. & Pappu, R. (2003). Squealing Euros: Privacy-protection in RFID-enabled banknotes, *Proceedings of Financial Cryptography*, Gosier (Ed.), Guadeloupe, FWI, LNCS 2742, Springer-Verlag, pp.103-121.

Karygiannies, A.; Eydt, B., Phillips & Ted S. (2008). Practical Steps for Securing RFID Systems, In: *RFID Handbook Applications, Technology, Security, and Privacy*, Ahson, S. & Ilyas, M. (Ed.), Taylor & Francis Group.

Lee, H. & Hong, D. (2006), The tag authentication scheme using self-shrinking generator on RFID system, *World Academy of Science, Engineering and Technology* Vol. 18 , pp. 52–57.

Lee, K. & Verbauwhede, I. (2005). Secure and Low-cost RFID Authentication Protocols, *Proceedings of the 2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN)*.

Lu, L.; Han, J., Hu, L., Liu, Y. & Ni, L. (2007). Dynamic Key-Updating: Privacy-Preserving Authentication for RFID Systems, *Proceedings of Pervasive Computing and Communications*, pp. 13-22.

Li, T. & Wang, G. (2007). Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols, *Proceedings of the 22nd IFIP TC-11 Int'l Information Security Conference,* Vol. 232, Springer, pp. 109-120.

Molnar, D.; Soppera, A. & Wagner, D. (2006). A Scalable, Delegatable Pseudonym Protocol Enabling Owner-shipTransfer of RFID Tags, *Proceedings of SAC*, LNCS 3897, Springer-Verlag, pp. 276-290.

Peris-Lopez, P.; Hernandez-Castro, J., Estevez-Tapiador, J. & Ribagorda, A. (2006). EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags, *Proceedings of OTM Federated Conference and Workshop*: *IS Workshop*, pp. 352-361.

Hunt, V.; Puglia, A. & Puglia, M. (2007). *RFID: A Guide to Radio Frequency Identification*, Wiley-Interscience, April 10.

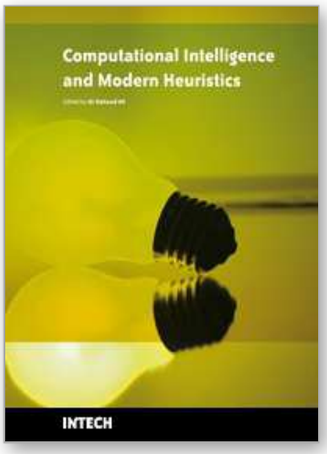
Song, B., & Mitchell, C.J. (2008). RFID authentication protocol for low-cost tags, *Proceedings of the First ACM Conference on Wireless Network Security 2008*, Gligor, V. D.; Hubaux, J. P. & Poovendran, R. (Ed.) , Alexandria, VA, USA, March 31 - April 02, 2008, pp.140-147.

Stallings, W. (2002), *Cryptography and Network Security,* Third Edition, Prentice Hall.

Weis, S.; Sarma, S., Rivest, R. L. & Engels, D. W. (2004). Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems, *Proceedings of Security in Pervasive Computing,* LNCS 2802, pp. 201-212.

Yu, M.; Zhou, T., Wang, J. & Ye, Y. (2004). An Efficient ASIC Implementation Of SHA-1 Engine For TPM, *Proceedings of IEEE Asia-Pacific Conference on Circuits and Systems,* pp. 873-876.

IntechOpen



Computational Intelligence and Modern Heuristics

Edited by Al-Dahoud Ali

ISBN 978-953-7619-28-2

Hard cover, 348 pages

Publisher InTech

Published online 01, February, 2010

Published in print edition February, 2010

The chapters of this book are collected mainly from the best selected papers that have been published in the 4th International conference on Information Technology ICIT 2009, that has been held in Al-Zaytoonah University, Jordan in the period 3-5/6/2009. The other chapters have been collected as related works to the topics of the book.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Mouza A. Bani Shemaili, Chan Yeob Yeun and Mohamed Jamal Zemerly (2010). Smart RFID Security, Privacy and Authentication, Computational Intelligence and Modern Heuristics, Al-Dahoud Ali (Ed.), ISBN: 978-953-7619-28-2, InTech, Available from: http://www.intechopen.com/books/computational-intelligence-and-modern-heuristics/smart-rfid-security-privacy-and-authentication

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen