

## Chapter 2

# RFID Security Threats and Basic Solutions

**Abstract** Radio Frequency Identification (RFID) technology is challenged by numerous security and privacy threats that render the widespread of such an advantageous technology. The security threats encountered in RFID systems is different from the security threats of traditional wireless systems. This chapter is devoted to survey the existing security threats and their primitive solutions that do not consider cryptography. We classify the existing security threats into those which target the physical RFID components such as the tag, the communication channel, and the overall system threats. We discuss the physical system security solutions and the basic authentication techniques that ensure the valid identity of the communicating parties.

Like many other technologies, RFID systems confront a new set of challenges in providing security and privacy for individuals or organizations against possible threats while they are accomplishing a great productivity gains. Since the communication between the tags and the reader is performed through an unsecure wireless channel, the transmitted data is vulnerable to attacks by unauthorized readers. However, the security threats encountered in RFID systems are different from the security threats of traditional wireless systems. In this chapter, we overview the existing security threats and their primitive solutions that do not consider cryptography. We classify the existing security threats into those which target the physical RFID components, the communication channel, and the overall system threats. Then, we present the physical system security solutions and the basic authentication techniques that ensure the valid identity of the communicating parties.

## 2.1 Security Attacks in RFID Systems

RFID security attacks can be categorized into two main categories: privacy violations and security violations. In privacy violations, the attacker tries to harvest information from the objects by eavesdropping to the communications between the object and the reader or by tracking them. In security violations, an adversary

counterfeits the behavior of a tag or a reader for making undesirable communications. Such security attacks may target the physical tag, the communication channel between the tag and the reader, or the application or the system which employs the RFID technology. Multilayer attacks also exist which affect more than one layer [10]. In what follows, we classify the existing security risks and threats according to their target into physical threats, channel threats and system threats. Of course, threats which RFID systems face today are not limited to those listed below. The characteristics of information security research is that you never know what kind of attack steps the attacker will take next. With the popularity of RFID systems, attacks targeting RFID systems will increase and become more complex.

### ***2.1.1 Physical RFID Threats***

Physical threats are those threats that use physical means to attack the RFID system to disable tags, modify their content, or to imitate them.

#### **2.1.1.1 Disabling Tags**

In these attacks, an attacker takes advantage of the wireless nature of RFID systems in order to disable tags temporarily or permanently [10]. To permanently disable a tag, the attacker may remove the tag from one item with high price and switch it with a tag of an item with low price. The other way is sending a kill command to erase the memory of the tag. Removing the antenna or giving a high energy wave to a tag will destroy the tag permanently. To disable the tag temporarily, the attacker can use a Faraday cage like an aluminum foil-lined bag in order to block electromagnetic waves from it. In other case, the attacker may prevent tags from communicating with readers by generating a signal in the same range as the reader which is called active jamming.

#### **2.1.1.2 Tag Modification**

Since most RFID tags use writable memory, an adversary can take advantage of this feature to modify or delete valuable data from the memory of the tag. This information might be critical such as the data about a patient's health which any inconsistency between the data stored on the RFID tag and the corresponding tagged object may result in serious problems. In some cases, the reader may not even notice this inconsistency during the communication and thinks that the content of the tag is unaltered.

### **2.1.1.3 Cloning Tags**

In these attacks, the adversary clones or imitates the tags after skimming the tag's information. Each RFID tag used for identification has a unique ID number. If the ID information is exposed by the attacker, the tag can easily be copied. Now that a lot of programmable read-write tags are put into use, cloning a tag is not challenging. This new tag can then act as the ordinary tag without being detected. Such cloned tags are used in counterfeiting and spoofing system-level attack.

### **2.1.1.4 Reverse Engineering and Physical Exploration**

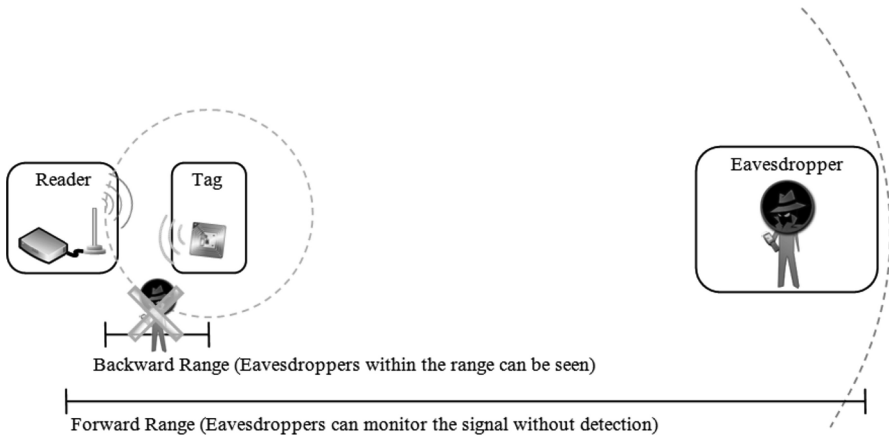
To maintain the tag cost low, most RFID tags are not equipped with a tamper-resistant mechanism for an estimated long period of time. An attacker with physical access to a tag can duplicate a tag with reverse engineering, and by means of physical probing, the attacker is capable of getting confidential information stored within tag. This is different from tag cloning which does not require physical exploration of the tag. However, they also are used in counterfeiting and spoofing system-level attack.

## ***2.1.2 RFID Channel Threats***

Channel threats refer to the attacks targeting the insecure channel between a reader and a tag. Since the RFID technology uses wireless means of communication between the reader and the tag, RFID systems may face eavesdropping, snooping, counterfeiting, playback, tracking threats, and other communication security issues that lead to privacy leaks.

### **2.1.2.1 Eavesdropping**

This threat addresses one of the main privacy concerns over the use of RFID technology. Eavesdropping happens when the channel is overheard secretly by an attacker to retrieve information from it [16]. Since RFID systems working in UHF covers more reading distance than other frequency bands, this threat is more likely to happen in it. Eavesdropping is a feasible threat and hard to be detected since it can be carried out at longer range on the communications between a tag and a valid reader while the adversary is passive and do not send out any signal (Fig. 2.1). This threat becomes serious when sensitive information is exchanged on the channel like data of a credit card without any encryption to protect them.



**Fig. 2.1** Eavesdropping attack adapted from [2]

### 2.1.2.2 Snooping

This attack is defined as the illegal reading of a device's identity and data. Snooping is similar to eavesdropping with the following difference. In eavesdropping, the attacker collects the information exchanged between a legitimate tag and legitimate reader. While snooping occurs when the data stored on the RFID tag is read without the owner's knowledge or agreement by an unauthorized reader interacting the tag. This attack happens because most of the tags transmit their stored data in their memory without requesting any kind of authentication.

### 2.1.2.3 Skimming

In this attack, the adversary observes the information exchanged between a legitimate tag and legitimate reader. Via the extracted data, the attacker attempts to make a cloned tag which imitates the original RFID tag. To perform this attack, the attacker does not need to have any physical access to the real tag. Skimming attack is precarious when documents like drivers' licenses or passports are authenticated through RFID system. In these situations, the attackers observe the interactions between the RFID tag embedded in the document with the reader to make a fake document.

### 2.1.2.4 Replay Attack

One of the most serious threats which RFID systems face is the replay attack. The replay attack is when a malicious node or device replays those key information which is eavesdropped through the communication between reader and tag, in order

to achieve deception. A typical application is when the illegal device playback the authentication between the reader and the tags, deceiving readers or tags to pass verification. Solutions to replay attacks include the use of stamp program, a one-time password and using the random number in authentication protocol, or updating the ID information dynamically. The researchers came up with a number of solutions to solve the problem of replay attacks such as David's Digital Library RFID protocol and distributed RFID interrogator [1].

### 2.1.2.5 Relay Attacks

A relay attack, also known as man-in-the-middle attack, is when an attacker places an illegal device between the reader and the tag such that it can intercept the information between the two nodes and then modify it or forwarded directly to the other end. The information transmitted through illegal devices will encounter some delay, and hence, these attack are called relay attacks.

A typical RFID relay attack system is described as follows: Suppose A is a legitimate reader, B is a legitimate label, and A' and B' are both illegal devices. A' and B' move close to the A and B, respectively, forwarding the communication information between A and B, making A believe that it communicate with B directly. The illegal device B' can be passed off as legitimate by palming off B. Meanwhile, the RFID system generally have limited communication distance, and hence, many security protocols are based on that the RFID readers and tags are in proximity are designed. However, in the relay attack, A' and B' can use other forms of communication, e.g., communication can be very far away, which destroys the premise that the reader and the tag are in proximity. An effective method to response to relay attacks is to use Distance Bounding Protocols. In 2005, Hancke et al. [6] proposed a distance limitation agreements using ultra-wide band radio, such that the readers and tags send bits of continuous authentication information to each other. By detecting the response time, the system ensures that the distance between readers and tags are closer. Later, Avoine and Reid et al. improved Hancke's agreement, achieving better results. Meanwhile, Fishkin et al. [4] found that the reader's signal to noise ratio is directly related to the distance between the reader and tag, which can be used for distance authentication.

### 2.1.2.6 Electromagnetic Interference

RFID channels can be the target of an adversary which aims at sabotaging the communication channel to prevent the tags from communicating with the reader. Such a communication channel threat can be either unintentional (passive interference) or intentional (active jamming).

- **Passive Interference:** Considering the fact that RFID systems operate in an inherently unstable and noisy environment, their communication is rendered

susceptible to possible interference and collisions from any source of radio interference such as noisy electronic generators and power switching supplies. This interference prevents accurate and efficient communication between the tags and the readers.

- **Active Jamming:** Although passive interference is usually unintentional, an attacker can take advantage of the fact that an RFID tag listens indiscriminately to all radio signals in its range. Thus, an adversary may cause electromagnetic jamming by creating a signal in the same range as the reader in order to prevent tags from communicating with readers.

### **2.1.3 System Threats**

System threats mainly refer to the attacks on the flaws existing in the authentication protocol and encryption algorithm. The following attacks are the main RFID system attacks

#### **2.1.3.1 Counterfeiting and Spoofing Attacks**

When the attackers get some information about the identity of RFID tags either by detecting the communication between readers and legitimate tags (skimming threats) or by physical exploration of the tags, the attacker can clone the tags. The RFID system will then be accessed using this information of identity to impersonate the legitimate labels or readers, which is called the counterfeiting or spoofing attacks. An attacker can fake labels, as well as readers. The effective means to prevent counterfeiting and spoofing attacks is to use efficient two-way authentication protocol to realize mutual authentication between tags and readers.

#### **2.1.3.2 Tracing and Tracking**

These threats violate the concept of location privacy. Illegal tracing and tracking occurs because RFID tags design requires the tag to always respond to the reader's query [16]. By sending queries and obtaining the same response from a tag at various locations it can be determined where the specific tag is currently and which locations it has visited. Since each RFID tag is affixed to a particular physical item with a unique ID number, this infers that the tag has visited those locations in which object. Encrypting the response can prevent having unauthorized access, since the adversary cannot obtain the tag contents without the secret key. However, since the tag always returns a constant response to the queries, the adversary can use this fact to perform illicit tracing and tracking.

### 2.1.3.3 Password Decoding

As currently most RFID systems use encryption technology to ensure the confidentiality and integrity of information delivery, attacking against the encryption algorithm is a common form of attack. Attackers can decode the encryption algorithms by conducting violent attacks, and decipher the intercepted cryptograph to get the plain-text. To respond to this attack, one need to design stronger encryption algorithms, or use longer keys to increase the difficulty of password cracking. Because of the constraint of the limited resources of RFID tags, traditional encryption or signature algorithms are difficult to be integrated into the tag. For this reason, many international scholars work on low-cost RFID encryption algorithm. For example, Yüksel proposed a low-cost 64-bit Hash function, only 1700 equivalent gates are required for the realization [18]. The Feldhofer, proposed a 128-bit Advanced Encryption Standard (AES) algorithm which requires only 3500 equivalent gates to be achieved [3], the algorithm is by far known the lowest cost AES program. The AES will be discussed in details in the next chapter.

### 2.1.3.4 Denial of Service (Dos) Attacks

RFID systems also may be subject to Denial of Service (DoS) attacks, which causes the system to not work properly. The attacker targets to block the reader from reading tags by using a blocker tag. Denial of service attacks are the threat to all modern communication systems. A set of mature anti-DoS solutions has developed for such threats. However, many of these solutions cannot be used in RFID systems due to the limited resources of RFID tags. For the RFID system to prevent denial of service attacks is still an area to be studied. Modern readers use anti-collision algorithms to support serving tags within their coverage areas. There are two main anti-collision algorithms; slotted ALOHA, or binary search tree. In the slotted ALOHA, the blocker tag sends an invalid packet at each time slot which will cause collision at all time slots. In binary search tree, the blocker tag will send both logic-1 and logic-0 at each bit in the serial number. Thus, the reader will be forced to search all of the possible combinations in the binary tree (i.e. if the time identifying a one serial number is 1 ms and the serial number length is 48-bit, the reader needs  $1 \text{ ms} \times 2^{48} \approx 8925 \text{ years}$  for searching all the binary tree!!).

## 2.2 RFID Security Measures and Defenses

To address the various aforementioned security threats, RFID devices had to employ various security measures designed to counter the different threats. In this section, we explore these various defense techniques employed by RFIDs [12]. Our main focus in this section is on such techniques that are applicable to simple (low cost and low power) RFIDs which have limited resources. This is because more powerful

RFIDs with more resources can employ cryptography to further increase the security of the system. Cryptography principles and how it is used in RFID system will be discussed in details in Chap. 3. In contrast, simple RFID tags are unable to perform typical cryptographic operations since such simple tags has a couple of thousand gates. These gates are mainly for basic operations and only very few gates are available for use to implement security functions. The lack of computational resources is counted as a temporary state of affairs, in the hope that Moore's Law will soon render inexpensive tags more computationally powerful. However, the cost factor is still a problem since RFID are used in vast numbers. Since RFID tags replace barcodes on individual items, they will contribute substantially to the cost of those items if the tag cost is high. Hence, this section discusses security and privacy defense mechanisms that employ simple measures such as tag-killing, tag-blocking, re-encryption and many others. We classify such techniques to those which address the privacy concerns and those which address the security concerns.

### ***2.2.1 Physical Solutions for RFID Privacy Protection***

To protect the privacy of RFID tags against possible attacks and threats, physical solutions that tackle the RFID itself are helpful. In this section, we introduce such defenses and investigate their pros and cons.

#### **2.2.1.1 Killing Tags**

In this method, the RFID tags are "killed" upon purchase of the tagged product by a customer. After killing the tag, it is no longer functional and cannot be re-activated anymore. This approach is performed by sending a special command including a short password [15]. For instance, in a supermarket, the tags of purchased goods would be killed at checkout for protecting the privacy of consumers. Therefore, none of the purchased items would contain alive RFID tags.

The advantage of this solution lies in the simplicity and effectiveness of the method. However, since in this method the tag cannot be reused, its lifetime is limited and it cannot be utilized for after-sale purposes while consumers may wish to keep them alive after buying them. For example, a smart fridge which keeps the expiration dates of groceries from their tags. Based on this information, it can also give a report of what is inside it and generate a list of shopping list. Other examples of RFID tag applications include theft-protection of belongings and wireless cash cards. In these applications, the RFID tag is required to be alive when the customer buys it and it cannot be killed.



### 2.2.1.2 Sleeping Tags

The “sleeping” mechanism is another type of physical solutions [2]. In this approach, the reader sends a “sleep” command including a password to the tag to make it temporarily inactive. This method is similar to the killing tag method with the difference that the sleeping tag can wake up and be activated as soon as it receives the command from the reader. Meanwhile, the tag can never be re-activated in the killing tag method.

The sleeping tag approach offers an advantage to the user to switch the state of the tag between active and inactive. The problem of using this method is the existence of the possibility that the password used for controlling the tags might be overheard by an eavesdropping attack.

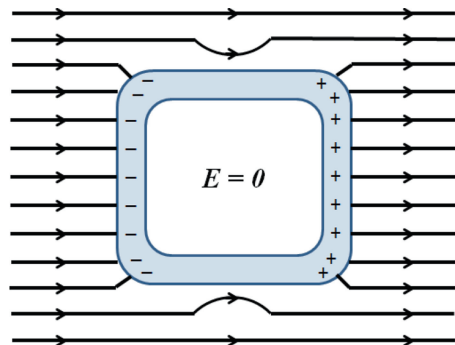
### 2.2.1.3 Faraday Cage

Faraday cage is an easy way of protecting an RFID tag that is inspired by the characteristics of electromagnetic fields and was introduced in [5]. A Faraday cage is an enclosure design made of conducting materials to exclude electromagnetic fields. Since any exterior radio signals cannot penetrate inside the cage, no reader can have access to the tag to read it as long as the RFID tag is inside such a cage.

Figure 2.2 shows how a Faraday cage shield enclosed tag from unwanted electromagnetic waves. The electromagnetic field pushes electrons of the cage toward the left. It leaves a negative charge on the left side and a positive charge on the right side of the cage. The result is that the electric field inside the cage is zero.

Faraday cages are extremely effective at providing consumer privacy against eavesdropping and tracking attacks. However, the main drawback of using this cage is its impracticality. The tag is protected from being read by unauthorized reader only when it is inside the cage. It might be practical for some items like smart cards, while using the cage is not convenient for a variety of objects like for tags injected under the skin or tags attached to a dress when it is being worn. The other problem

**Fig. 2.2** A Faraday cage in an electric field



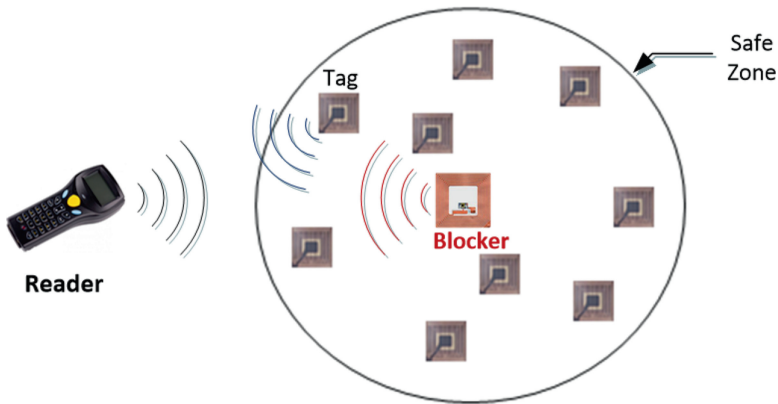
is preventing being read by the authorized readers unless the tag is outside the cage. Besides, using a Faraday cage for each tag imposes extra cost. These disadvantages put some limitations on using this approach which make this solution only suitable for some particular applications.

#### 2.2.1.4 Blocker Tags

A blocker tag is a physical solution for protecting privacy in RFID systems introduced in [9]. A blocker tag is similar to an RFID tag with the difference that it can block readers from reading the identification of those tags that exist in the blocker tag's range.

The operation of blocker tags is based on creating collision for a reader when it is attempting to identify tags in its field. To identify a tag from other tags, a reader sends a query asking its serial number. Since there is a possibility that multiple of tags exist in the reader's range and respond to this query at the same time, the probability of jamming to occur is high. Therefore, readers use some algorithms like tree walking to resolve this collision. In this algorithm, each time the reader asks that only those tags which serial number starts with a special number answer. If the reader still receives more than one response, it will continue by limiting the range of serial number until just one tag answers the query. The blocker tag uses this feature and by answering all queries that reader broadcast, it fabricate a fake collision (Fig. 2.3). Thus, the reader is tricked into believing that all tags in its field are in interrogation zone. This way, a blocker tags can establish a safe zone around the tags and all RFID tags that exist in this zone can impede reading their data at the presence of a blocker tag.

One of the practical and attractive applications for blocker tags is their use in supermarkets. Before purchasing the goods, their RFID tag can be read inside the



**Fig. 2.3** Blocker tags blocks reading by broadcasting signals for every reader's query

supermarket without any restrictions. When they are placed in the hands of the customer, a blocker tag might be added to the shopping bag to block all further communications. This blocker tag guarantee the customer's privacy against any threats until the items are removed from the shopping bag. Then, the tags of the purchased items can operate again like before.

The major advantage of this approach is keeping the functionality of tags. Unlike killing tags wherein the lifetime of the tags are limited by the purchasing time, this method allows the tags to be more useful by expanding their lifetime. However, a major drawback of this method is its limited safety. The attacker cannot have access to tags just in a defined range and beyond this range, tags are not protected from attacks. Besides, blocker tags are not applicable everywhere. For example, in supply chains, tags are required to be available all the time and they cannot be blocked from being read by readers while the blocker tags impeded all readers to have communications with tags even authorized readers.

### **2.2.1.5 Tag Relabeling**

It is an approach in which the unique identifier of the tag is relabeled with a new unique identifier. However, the old identifier remains on the tag for further use. There are various works done based on this idea such as [17] which proposed the idea of rewriting a new random number on the RFID tags on each checkout. The authors used such a technique to present a solution for clandestine scanning of library books. Alternatively, the authors of [7] suggest two approaches for RFID tag privacy. The first tag-labeling privacy solution is based on masking the permanent ID of the tag under a private ID that is given by the users. In the other approach, the tag's permanent ID is split into two parts: a partial ID sequence that is assigned to an object, and the rest of the ID is given by user-assignable RFID tags. According to these approaches, the users have the control over the ID's uniqueness either locally or globally. Hence, the users can enable the tag's private or public ID in the different stages of the life cycle of the object.

### **2.2.1.6 Minimalist Cryptography**

"Minimalist cryptography" in RFID tags achieves the goals of cryptography under the special resource constraints imposed by RFID tags. A "minimalist" system in which the main idea is to apply pseudonyms to help enforcing privacy in RFID tags was first proposed in [8]. In a nutshell, a tag may carry multiple, random-looking names. Each time it is queried, the tag releases a different name. In principal, only a valid verifier can tell when two different names belong to the same tag. Of course, an adversary could query a tag multiple times to harvest all names so as to defeat the scheme. This approach involves some special enhancements to help preventing such adversary. First, tags release their names only at a certain (suitably slow) prescribed rate. Second, pseudonyms can be refreshed by authorized readers. The minimalist

scheme can offer some resistance to corporate espionage, like clandestine scanning of product stocks in retail environments. A new security model for EPC G2 tags which is based on minimalist cryptography was proposed in [13]. Such a model provides a solution against spoofing, replay, denial-of-service, traffic analysis and tracking.

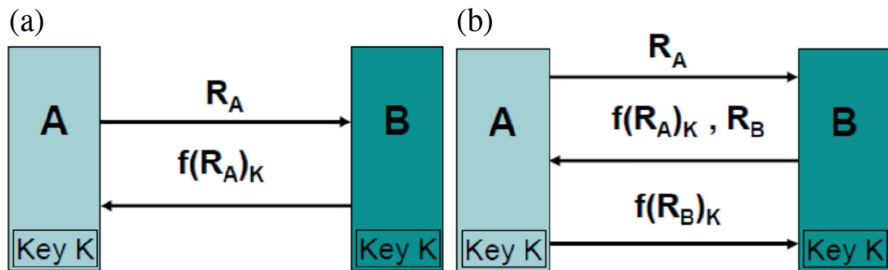
### 2.2.1.7 Proxy Privacy Devices

Generally RFID readers and tags cannot have the ability to provide consumer privacy protection. One way to overcome this challenge is to rely on the reader for privacy protection. However, relying on the reader for privacy is risky due to the fact that the reader is public. Alternatively, privacy-enforcing devices can be added to RFID systems. Along with this approach, researchers have proposed several systems such the *RFID Guardian* proposed in [14]. The *RFID Guardian* is a platform that offers centralized RFID security and privacy management for individual people. It is integrated with four separate security policies, i.e. auditing, efficient key management, access controls and act as mediator between the RFID readers and the RFID tags as an RFID firewall.

## 2.2.2 Authentication

Authentication is a process through which an object proves its claimed identity to other communication party with providing some evidence such as what it knows, what it has, or what it is. This process is applicable through only software solutions and it is not possible by physical solutions. In RFID systems, authentication is required in two phases. First, before beginning any communication, both the tag and the reader should verify their identity to make sure that they are contacting with the wished partner. The second phase is when data is exchanged between the two parties to ensure that the exchanged data is intact.

When a tag passes through the electromagnetic field of a reader, it becomes activated and can detect the reader's signal. To reply to the reader, the tag needs to know if the reader is the legitimate one or not. Otherwise, an unauthorized reader can obtain information from tags which are currently in its field by eavesdropping and keep a tracking of their current locations. Also, an unauthorized reader can have access to the tag's memory to read or even manipulate its data. Therefore, to prevent these threats, a process is required to authenticate the reader to the tag. On the other hand, the reader is required to find out if the tag contacting with is reliable or not. This way, the reader can make sure that it is not communicating with a counterfeit tag. This process is called authenticating tag to the reader. Mutual authentication permits the two parties to authenticate each other's identity. This happens when both tag to reader authentication and reader to tag authentication



**Fig. 2.4** Challenge-response technique in symmetric authentication. (a) Unilateral authentication. (b) Mutual authentication [11]

are performed. Conducting mutual authentication between RFID tags and readers should be performed before exchanging any key and data. This way, all of the former mentioned security problems in the last sections can be solved.

Implementing unilateral and mutual authentication at the beginning of the communication has been the focus of many researches. The authors of [11] presented three authentication methods. The first method, password authentication, provides a weak level of security. Customized and zero-knowledge authentication is another technique based on mathematical problems, the implementation of which imposes high cost. Challenge-response is a high secure scheme which is being of interest recently. This scheme is categorized into two groups: symmetric and asymmetric. Asymmetric techniques are time consuming and their implementation cost is high. On the contrary, symmetric methods need key exchange and management since they use one shared secret key (Fig. 2.4).

During communication, providing authentication is required since there is a possibility that attackers send the message on behalf of each party or manipulate the message such that they replace their desired message with the real one. This service can be implemented by keyed hash function or Message Authentication Codes (MAC). Using MACs bring the benefit that the integrity of the message can be guaranteed. Authentication is essential when the possibility of existing attackers are high like battle fields or the condition of environment is harsh and may affect the accuracy of the messages. Also, performing this service is vital in applications in which the value of data is important such as health care applications.

## 2.3 Concluding Remarks

Considering the limitations and drawbacks of the physical solutions discussed in this chapter for providing security and privacy in RFID applications, these solutions are suitable for particular applications and cannot be applicable for all applications. Other solutions are required that does not suffer any limitation on the life-span of tags such as in killing method or block authorized readers like faraday cage.

Such solutions also should not be restricted to a special zone like blocker tags. The suggested solution is using cryptographic algorithm to encrypt messages exchanged between the tags and the reader. In this solution, an adversary cannot have access to the information by overhearing if it does not have the secret key. This solution also brings benefits like providing integrity and authentication which are not possible in physical solutions. However, this solution needs to be compatible with tags which are very resource limited. In the next chapter, a survey of lightweight cryptosystems developed for RFID systems will be presented.

## References

1. Chauhan, M., Sharma, E.: A survey on RFID technology. *Int. J. Res.* **1**(10), 1316–1322 (2014)
2. Chen, Y., Tsai, M.: The Study on Secure RFID Authentication and Access Control. InTech (2011)
3. Feldhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong authentication for RFID systems using the AES algorithm. In: *Cryptographic Hardware and Embedded Systems-CHES*, vol. 3, pp. 357–370. Springer, Berlin (2004)
4. Fishkin, K.P., Roy, S., Jiang, B.: Some methods for privacy in RFID communication. In: *Security in Ad-hoc and Sensor Networks*, pp. 42–53. Springer, Berlin (2005)
5. Garfinkel, S., Rosenberg, B.: *RFID: Applications, Security, and Privacy*. Addison-Wesley, Reading, MA (2006)
6. Hancke, G.P., Kuhn, M.G.: An RFID distance bounding protocol. In: *Proceedings of IEEE 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks [SecureComm 2005]* (2005)
7. Inoue, S., Yasuura, H.: RFID privacy using user-controllable uniqueness. In: *Proceedings of RFID Privacy Workshop* (2003)
8. Juels, A.: Minimalist cryptography for low-cost RFID tags. In: *Proceedings of 4th International Conference on Security Communication Networks. Lecture Notes in Computer Science*, vol. 3352, pp. 149–164. Springer, Berlin (2004)
9. Juels, A., Rivest, R.L., Szyldo, M.: The blocker tag: Selective blocking of RFID tags for consumer privacy. In: *Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS '03* (2003)
10. Mitrokotsa, A., Rieback, M., Tanenbaum, A.: Classifying RFID attacks and defenses. *Inf. Syst. Front.* **12**(5), 491–505 (2010)
11. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: *Handbook of Applied Cryptography*. CRC Press, Boca Raton (1997). Available online at <http://www.cacr.math.uwaterloo.ca/hac>
12. Pateriya, R.K., Sharma, S.: The evolution of RFID security and privacy: a research survey. In: *IEEE International Conference on Communication Systems and Network Technologies [CSNT]* (2011)
13. Qingling, C., Yiju, Z., Yonghua, W.: A minimalist mutual authentication protocol for RFID system & BAN logic analysis. In: *Proceedings of ISECS International Colloquium on Computing, Communication, Control, and Management* (2008)
14. Rieback, M., Crispo, B., Tanenbaum, A.: RFID guardian: a battery-powered mobile device for RFID privacy management. In: *Proceedings of Australasian Conference on Information Security and Privacy. Lecture Notes in Computer Science*, vol. 3574, pp. 184–194. Springer, New York (2005)
15. Sarma, S., Weis, S., Engels, D.: RFID systems and security and privacy implications. In: *Cryptographic Hardware and Embedded Systems - CHES 2002. Lecture Notes in Computer Science*, vol. 2523, pp. 454–469. Springer, Berlin (2003)

16. Weis, S., Sarma, S., Rivest, R., Engels, D.: Security and privacy aspects of low-cost radio frequency identification systems. In: *Security in Pervasive Computing. Lecture Notes in Computer Science*, vol. 2802, pp. 201–212. Springer, Berlin (2004)
17. Wu, D.L., Ng, W.W.Y., Yeung, D.S., Ding, H.L.: A brief survey on current RFID applications. In: *International Conference on Machine Learning and Cybernetics* (2009)
18. Yüksel, K.: Universal hashing for ultra-low-power cryptographic hardware applications. Ph.D. thesis, Worcester Polytechnic Institute (2004)

RFID Security

A Lightweight Paradigm

Khattab, A.; Jeddi, Z.; Amini, E.; Bayoumi, M.

2017, XXII, 171 p. 80 illus., 61 illus. in color., Hardcover

ISBN: 978-3-319-47544-8