
2 Attacking RFID Systems

*Pedro Peris-Lopez, Julio Cesar Hernandez-Castro,
Juan M. Estevez-Tapiador, and Arturo Ribagorda*

CONTENTS

2.1	Introduction.....	30
2.1.1	Background.....	30
2.1.2	Attack Objectives	30
2.1.3	Security Needs	31
2.2	Main Security Concerns	32
2.2.1	Privacy	32
2.2.2	Tracking	33
2.3	Tags and Readers.....	34
2.3.1	Operating Frequencies and Reading Distances	34
2.3.2	Eavesdropping.....	35
2.3.3	Authentication.....	36
2.3.4	Skimming.....	37
2.3.5	Cloning and Physical Attacks	38
2.3.6	Replay and Relay Attacks	40
2.3.7	Hiding	41
2.3.8	Deactivating	41
2.3.9	Cryptographic Vulnerabilities	42
2.4	Back-End Database	43
2.4.1	Tag Counterfeiting and Duplication.....	43
2.4.2	EPC Network: ONS Attacks.....	44
2.4.3	Virus Attacks	45
	References	46

A great number of hackers end up working in the security departments of IT and telecommunications companies. In other words, the best way of making a system secure is knowing how it can be attacked. Radio-frequency identification (RFID) is no different from any other technology, so the possible attacks on it should be studied in depth. The extent of an attack can vary considerably; some attacks focus on a particular part of the system (e.g., the tag) whereas others target the whole system. Although there are references to such attacks in a number of publications, a rigorous study has not been made of the subject until now. We examine, in this chapter, the main threats to RFID security. First, we look at data and location privacy. Although these are the risks most often referred to in the literature, there are other equally important problems to consider too. RFID systems are made up of three main components (tag, reader, and back-end database), so we have grouped the threats according to the unit involved in the attack. First, we examine those related to tags and readers such as eavesdropping, cloning, replay, and relay attacks. Then we look at the threats to the back-end

database (e.g., object name service [ONS] attack, virus). By the end of this chapter (and with the opportunity to consult the extensive bibliography for further details), we hope the reader will have acquired a basic understanding of the principal security risks in RFID.

2.1 INTRODUCTION

2.1.1 BACKGROUND

Press stories about radio-frequency identification (RFID) often give inaccurate descriptions of the possibilities that exist for abuse of this technology. They predict a world where all our possessions will have a unique identification tag: clothes, books, electronic items, medicines, etc. For example, an attacker outside your house equipped with a commercial reader would be able to draw up an inventory of all your possessions, and particular information such as your health and lifestyle could also be revealed. Also, it is said that this technology allows “Big Brother” to know when you are in public places (office, cinemas, stores, pubs, etc.), tracking all your movements and compromising your privacy in terms of your whereabouts (location).

RFID technology is a pervasive technology, perhaps one of the most pervasive in history. While security concerns about the possibility of abuse of this pervasive technology are legitimate, misinformation, and hysteria should be avoided. One should be aware that ways of collecting, storing, and analyzing vast amounts of information about consumers and citizens existed before the appearance of RFID technology. For example, we usually pay with credit cards, give our names and address for merchandizing, use cookies while surfing the Internet, etc.

In this chapter we give an overview of the risks and threats related to RFID technology, helping the reader to become better acquainted with this technology. Although the privacy issues are the main focus in literature [1–12], there are other risks that should be considered when a RFID system is designed.

2.1.2 ATTACK OBJECTIVES

The objectives of each attack can be very different. It is important to identify the potential targets to understand all the possible attacks. The target can be the complete system (i.e., disrupt the whole of a business system) or only a section of the entire system (i.e., a particular item).

A great number of information systems focus solely on protecting the transmitted data. However, when designing RFID systems, additional objectives, such as tracking or data manipulation should be considered. Imagine the following example in a store: an attacker modifies the tag content of an item reducing its price from 100 € to 9.90 €. This leads to a loss of 90 percent for the store. In this scenario, the data may be transmitted in secure form and the database has not been manipulated. However, fraud is carried out because part of the system has been manipulated. Therefore, to make a system secure, all of its components should be considered. Neglecting one component, whatever the security level of the remaining components, could compromise the security of the whole system.

The objectives of the attacks are very different. As we see in the above example, the attack may be perpetrated to steal or reduce the price of a single item, while other attacks could aim to prevent all sales at a store. An attacker may introduce corrupt information in the database to render it inoperative. Some attacks, such as the faraday cage or active jamming, are inherent in the wireless technology employed. Other attacks are focused on eliminating physical access control, and ignore the data. Other attacks even involve fraudulent border crossings, identity stealing from legitimate e-passports, etc.

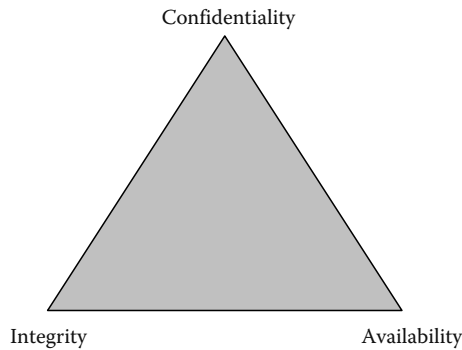


FIGURE 2.1 Three pillars of security: the CIA triad.

2.1.3 SECURITY NEEDS

As any other mission-critical system, it is important to minimize the threats to the confidentiality, integrity, and availability (CIA) of data and computing resources. These three factors are often referred to as “The Big Three.” Figure 2.1 illustrates the balance between these three factors.

However, not all systems need the same security level. For example, not all systems need 99.999 percent availability or require that its users be authenticated via retinal scans. Because of this, it is necessary to analyze and evaluate each system (sensitivity of the data, potential loss from incidents, criticality of the mission, etc.) to determine the CIA requirements. To give another example, the security requirements of tags used in e-passports should not equal those employed in the supply chain (i.e., tag compliant to EPC Class-1 Generation-2).

Confidentiality: The information is accessible only to those authorized for access. Privacy information, such as the static identifiers transmitted by tags, fits into the confidentiality dimension. Both users and companies consider this issue of utmost importance. Furthermore, RFID technology allows the tracking of items. From a user perspective, tracking should be avoided. However, companies may control the movements of materials in the supply chains, increasing the productivity of their processes.

Integrity: The assurance that the messages transmitted between two parties are not modified in transit. Additionally, some systems provide the authenticity of messages. The receipt is able to prove that a message was originated by the purported sender and is not a forgery (nonrepudiation). An example of this kind of attack is the spoofing attack.

Availability: System availability is whether (or how often) a system is available for use by its intended users. This factor will determine the performance and the scalability level of the system. Denial-of-service (DoS) attacks are usual threats for availability (i.e., active jamming of the radio channel or preventing the normal operation of vicinity tags by using some kind of blocker tag).

Each time a new technology is implanted, contingency plans for various points of failure should be designed. We recommend periodical security audits to review the security policies, procedures, and IT infrastructures. As has been frequently mentioned, RFID technology may be a replacement for bar-code technology. Nevertheless, new risk scenarios should be considered with its implantation. For example, consider the repercussions of a bar-code reader failing or an RFID reading going down. When a bar-code reader fails, an operator can manually enter the codes into the terminal and the system works, albeit with relatively slowness. On the other hand, if the RFID reader is processing high volumes of items and these items are moving at high speed, the consequences will be much worse. Security needs should therefore be considered a priority.

2.2 MAIN SECURITY CONCERNS

2.2.1 PRIVACY

No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks [13].

Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of individuals, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals [14].

Privacy has no definite boundaries and its meaning is not the same for different people. In general terms, it is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves.

The invasion of privacy by governments, corporations, or individuals is controlled by a country's laws, constitutions, or privacy laws. For example, taxation processes normally require detailed private information about earnings. The EU Directive 95/46/EC [14] on the protection of individuals with regard to the processing of personal data and the free movement of this, limits and regulates the collection of personal information. Additionally, Article 8 of the European Convention of Human Rights identifies the right to have private and family life respected. Within this framework, monitoring the use of e-mails, Internet, or phones in the workplace, without notifying employees or obtaining their consent can result in legal action.

RFID technology is a pervasive technology, and seems destined to become more and more so. As Weiser already predicted in 1991, one of the main problems that ubiquitous computing has to solve is privacy [15]. Leakage of information is a problem that occurs when data sent by tags reveals sensitive information about the labeled items. Products labeled with insecure tags reveal their memory contents when queried by readers. Usually, readers are not authenticated and tags answer in a transparent and indiscriminate way.

As an example of the threat this could pose, consider the pharmaceutical sector where tagged medication is planned for the immediate future. Imagine that when you leave the chemist's with a given drug—say an antidepressive or AIDS treatment, an attacker standing by the door equipped with a reader could find out what kind of medication you have just bought. In a similar scenario, thieves equipped with tag readers could search people, selecting those with multiple tagged bank bills to rob, and they would know how much they would earn with each robbery.

Advanced applications, where personal information is stored in the tags, have appeared recently. E-passports are a good example of this sort of application. As part of its U.S.-VISIT program, the U.S. government mandated the adoption of e-passports by the 27 nations in its Visa-Waiver Program. A combination of RFID technology and biometric technology is employed [7,16,17]. The RFID tags store the same information that is printed on its first page (name, date of birth, passport number, etc.) as well as biometric information (facial image). In phase-2 of the European e-passport project [18], the biometric data from two fingerprints, which is very sensitive information, will also be stored.

Several organizations like CASPIAN [19] and FOEBUD [20] are strongly against the massive deployment of RFID technology. They believe that RFID technology will lead to a significant loss of citizens' privacy. Some of CASPIAN's activities include successful boycott campaigns against important companies like Benetton [21,22], Tesco [23], and Gillette [24], to name but a few. Additionally, a book titled "*SPYCHIPS: How Major Corporations and Government Plan to Track your Every Move with RFID*" and published in 2005 [25], has contributed to promoting suspicion about RFID technology.

Another example of objection to RFID technology is the case of California State Senator Joe Simitian (Senate Bill 682), who planned to restrict the use of identification systems based on RFID technology: "The act would prohibit identity documents created, mandated, or issued by various

public entities from containing a contactless integrated circuit or other device that can broadcast personal information or enable personal information to be scanned remotely” [26]. Due to significant industry opposition, Bill 682 was stalled in the Assembly Appropriations Committee and an important missed deadline resulted in the expiry of the Bill. Legislative maneuvering allowed the resurrection of the case by means of Bill 768 [27]. This bill was finally vetoed by California Governor Arnold Schwarzenegger. In particular, Bill 768 proposed to

1. Criminalize the “skimming” of personal data from RFID-enable identification documents.
2. Implement specific provisions to ensure the security of data contained in such identification documents.
3. Impose a three-year moratorium on the use of RFID technology in certain types of government-issued identification documents.

In 2002, Garfinkel proposed a set of rights that should be upheld by any system that uses RFID technology [28]. Consumers should have:

1. Right to know whether products contain RFID tags.
2. Right to have RFID tags removed or deactivated when they purchase products.
3. Right to use RFID-enabled services without RFID tags.
4. Right to access an RFID tag’s stored data.
5. Right to know when, where and why the tags are being read.

These rights are not necessarily considered as the basis for a new law, but as a framework for voluntary guidelines that companies wishing to deploy this technology may adopt publicly.

2.2.2 TRACKING

Location information is a set of data describing an individual’s location over a period of time [29]. The resolution of the system (time and localization) depends on the technology used to collect data.

Indeed, location privacy can be viewed as a particular type of privacy information [30]. A secondary effect of wireless communication is that information can be made public and collected. In a mobile phone context, the regions are divided up into cells. Each time a phone enters a new cell, the mobile is registered. Mobile phone operators record handset location information and supply it to third parties (i.e., police, the company that subscribed the localization service, etc.). Other techniques such as triangulation can be used to increase the precision of the system. The new localization services (i.e., third-generation mobile phones) allow an accuracy of a few meters by means of the incorporation of a global positioning system (GPS) receiver. In data network context, Wireless 802.11 Ethernet cards obtain connectivity by registering with access points which could be used to locate a network device.

RFID technology is not a high-tech bugging device. It does not possess GPS functionality or the ability to communicate with satellites. RFID tags do not have the storage and transmission capability for large quantities of information. An RFID system is normally composed of three components: tags, readers, and a back-end database. Readers are connected, using a secure channel, to the database. When a database is present in the system, tags might only transmit an identifier. This identifier is used as a index-search in the database to obtain all the information associated with the tag. Therefore, only people with access to the database can obtain the information about the labeled item.

Most of the time, tags provide the same identifier. Although an attacker cannot obtain the information about the tagged item, an association between the tag and its holder can easily be established. Even where individual tags only contain product codes rather than a unique serial number, tracking is still possible using an assembly of tags (constellations) [31]. To clarify the potential risks of tracking, some examples are given:

Wall-Mart: It is an American public corporation, currently one of the world's largest. It has concentrated on streamlining the supply chain, which is why it encourages all its suppliers to incorporate RFID technology in their supply chains. The substitution of bar codes by RFID tags allows an increase in the reading-rate of the pallets as they move along the conveyor belt. RFID readers can automatically scan these as they enter or leave the warehouse, saving time and improving product flow. Right now, RFID technology is used at pallet level. Individual packaging is the next logical step.

Individual product packaging: Imagine that your Tag Heuer bifocals possess a tag, and this tag stores a 96 bit static identifier, allowing an attacker to establish a link between the identifier and you. On association, an attacker could know when you passed through a given place, for example when you enter or leave your home, when you arrive at or leave your office, etc. Even worse, the attacker could locate several readers in your favorite mall. He could collect data over a long time (data, time, shop, etc.) acquiring a consumer profile of you. Finally, he could send you personalized advertising information depending on your shopping habits.

E-passports: Since October 2006, the United States required the adoption of e-passports by all the countries in its Visa-Waiver Program. The International Civil Aviation Organization (ICAO) standard specifies one mandatory cryptographic feature (passive authentication) and two optional cryptographic features (basic access control and active authentication). Passive authentication only demonstrates that tag content is authentic but it does not prove that the data container is secure. Basic authentication ensures that tag content can only be read by an authorized reader. Additionally, a session key is established, encrypting all the information exchanged between the tag and the reader. Active authentication is an anticloning feature, but it does not prevent unauthorized readings. Independent of the security mechanism used, tracking is possible. The electronic chip required by the ICAO must conform to ISO/IEC 14443 A/B already adopted in other applications [32,33]. The collision avoidance in ISO 14443 uses unique identifiers that allow readers to distinguish one tag from another [17]. However, this identifier will allow an attacker to unequivocally identify an e-passports's holder. One simple countermeasure is to generate a new random identifier each time the tag is read.

As has been shown, RFID technology is not the only one that permits the tracking of people (i.e., video surveillance, mobile phone, Wireless 802.11 Ethernet cards, GPS, etc.). Nevertheless, the equipment used to track people holding RFID tags is not very expensive. If we return to the example of tracking in a mall, we will understand one of the principal differences between RFID and other localization technologies. The great majority of malls have a video surveillance system. You can be filmed in all the supermarket sections in which you buy an item. Then, the information obtained by the system (images) has to be processed to obtain your consumer profile. However, if RFID technology was employed, data could be automatically collected without the need for subsequent data processing as in video systems.

2.3 TAGS AND READERS

2.3.1 OPERATING FREQUENCIES AND READING DISTANCES

RFID tags operate in four primary frequency bands [34]:

1. Low frequency (LF) (120–140 kHz)
2. High frequency (HF) (13.56 MHz)
3. Ultrahigh frequency (UHF) (860–960 MHz)
4. Super high frequency/microwave (μ W) (2.45 GHz and above)

The characteristics of different frequencies are summarized in Table 2.1.

TABLE 2.1
Tag Frequencies and Reading Distances

Frequency Band	Frequency	Distance	Energy Transfer
Low (LF)	125 kHz	1–90 cm, typically around 45 cm	Inductive coupling
High (HF)	13.56 MHz	1–75 cm, typically under 40 cm	Inductive coupling
Ultrahigh (UHF)	865–868 MHz (Europe) 902–928 MHz (United States) 433 MHz (active tags)	Up to 9 m	Electromagnetic coupling
Microwave (μ W)	2.45 GHz 5.8 GHz	Typically 0.3–0.9 m	Electromagnetic coupling

LF tags: These tags operate at 120–140 kHz. They are generally passive and use near-field inductive coupling. So they are suited for applications reading small amounts of data at relatively slow speeds and at short distances. Their read range varies from 1 to 90 cm, typically below 45 cm. LF tags do not support simultaneous tag reads. LF tags are relatively costly because they require a longer, more expensive copper antenna. They penetrate materials such as water, tissue, wood, and aluminum. Their common applications are in animal identification, automobile security, electronic article surveillance, commerce, and other areas.

HF tags: These tags operate at 13.56 MHz. They are typically passive and typically use inductive coupling. HF tags penetrate materials well, such as water, tissue, wood, aluminum, etc. Their data rates are higher than LF tags and their cost is lower due to the simple antenna design. Their read ranges varies from 1 to 75 cm, typically under 40 cm. HF tags are used in smart shelf, smart cards, libraries, baggage handling, and other applications.

UHF tags: UHF active and passive tags can operate at different frequencies. UHF active tags operate at 433 MHz, and UHF passive tags usually operate at 860–960 MHz. Generally, passive UHF tags are not very effective around metals and water. They perform well at distances greater than 90 cm. UHF passive tags usually reach about 9 m. UHF tags have good non-line-of-sight communication, a high data rate, and can store relatively large amounts of data.

Super high frequency/microwaves tags: These tags operate at frequencies of 2.45 GHz and above (also 5.8 GHz) and can be either active or passive. Their characteristics are similar to those of UHF tags. However, they have faster read rates and are less effective around metals and liquids than tags of lower frequencies. These tags can be smaller in size compared to LF, HF, and UHF tags and are used for electronic toll collection as well as for the tracking of shipping containers, trains, commercial vehicles, parking, etc. The read range varies from 0.3 to 0.9 m for passive tags and is very dependent on design. Active systems also use microwave frequency.

2.3.2 EAVESDROPPING

RFID technology operates through radio, so communication can be surreptitiously overheard. In Ref. [35], the possible distances at which an attacker can listen to the messages exchanged between a tag and a reader are categorized (see Figure 2.2).

Forward channel eavesdropping range: In the reader-to-tag channel (forward channel) the reader broadcasts a strong signal, allowing its monitoring from a long distance.

Backward channel eavesdropping range: The signal transmitted in the tag-to-reader (backward channel) is relatively weak, and may only be monitored in close proximity to the tag.

Operating range: The read ranges shown in Section 2.3.1 are the operating read range using sales-standard readers.

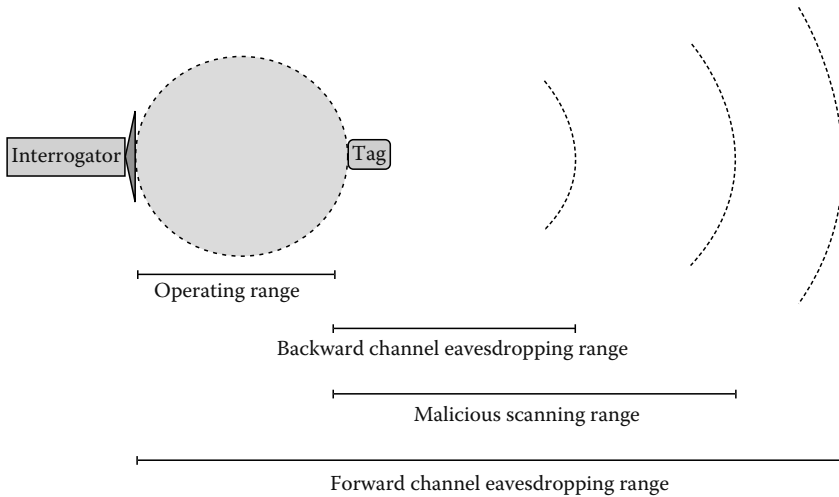


FIGURE 2.2 Eavesdropping range classification. (From Ranasinghe, D.C. and Cole, P.H., *Confronting security and privacy threats in modern RFID systems*. In *Proceedings of ACSSC 06*, 2006, pp. 2058–2064. With permission.)

Malicious scanning range: An adversary may build his own reader-archiving longer read ranges, especially if regulations about radio devices are not respected. A conversation between a reader and a tag can be eavesdropped over a greater distance than is possible with direct communication. For example, tags compliant to ISO 14443 have a reading distance of around 10 cm (using standard equipment). However, Kfir et al. showed that this distance can be increased to 55 cm employing a loop antenna and signal processing [36].

Eavesdropping is particular problematic for two reasons:

1. Feasibility: it can be accomplished from long distances.
2. Detection difficulty: it is purely passive and does not imply power signal emission.

Eavesdropping attacks are a serious threat mainly when sensitive information is transmitted on the channel. To give an example, we consider the use of RFID technology in payments cards (RFID credit cards) [37]. In an eavesdropping attack, information exchanged between the credit card reader and the RFID credit card is captured. Heydt-Banjamin et al. showed how this attack can be carried out [38]. An antenna was located next to an off-the-shelf RFID credit card reader. The radio signal picked up by the antenna was processed to translate it into human readable form. In particular, the following pieces of data were captured: cardholder name, complete credit card number, credit card expiry date, credit card type, and finally information about software version and supported communications protocols. As the above example shows, eavesdropping attacks should therefore be considered and treated seriously.

2.3.3 AUTHENTICATION

Entity authentication allows the verification of the identity of one entity by another. The authenticity of the claimed entity can only be ascertained for the instant of the authentication exchange. A secure means of communication should be used to provide authenticity of the subsequent data exchanged. To prevent replay attacks, a time-variant parameter, such as a time stamp, a sequence number, or a challenge may be used. The messages exchanged between entities are called tokens. At least one token

has to be exchanged for unilateral authentication and at least two tokens for mutual authentication. An additional token may be needed if a challenge has to be sent to initiate the protocol.

In RFID context, the first proposals found in literature are based on unilateral authentication [39–41]. However, the necessity of mutual authentication has been confirmed in many publications [42–45]. In ISO/IEC 9784, the different mechanisms for entity authentication are described [46]:

- Part 1: General model
- Part 2: Entity authentication using symmetric techniques
- Part 3: Entity authentication using a public key algorithm
- Part 4: Entity authentication using a cryptographic check function

Use of a cryptographic check function seems to be the most precise solution for RFID. Due to the fact that standard cryptographic primitives exceed the capabilities of a great number of tags, the design of lightweight primitives is imperative, at least for low-cost RFID tags.

The two entities (claimant/verifier) share a secret authentication key. An entity corroborates its identity by demonstrating knowledge of the shared key. This is accomplished by using a secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. This value can be recalculated by the verifier and compared with the received value. The following mechanisms, as shown in Figure 2.3, are possible.

2.3.4 SKIMMING

Takashimaya, one of the largest retailers in Japan, now sells antiskimming cards called “Sherry” at their department stores. Consumers can just put the cards in their wallets to prevent their RFID-chipped train passes, etc. from skimming attacks.

The antiskimming card functions by creating a reverse electromagnetic field like Taiyo’s technology [47].

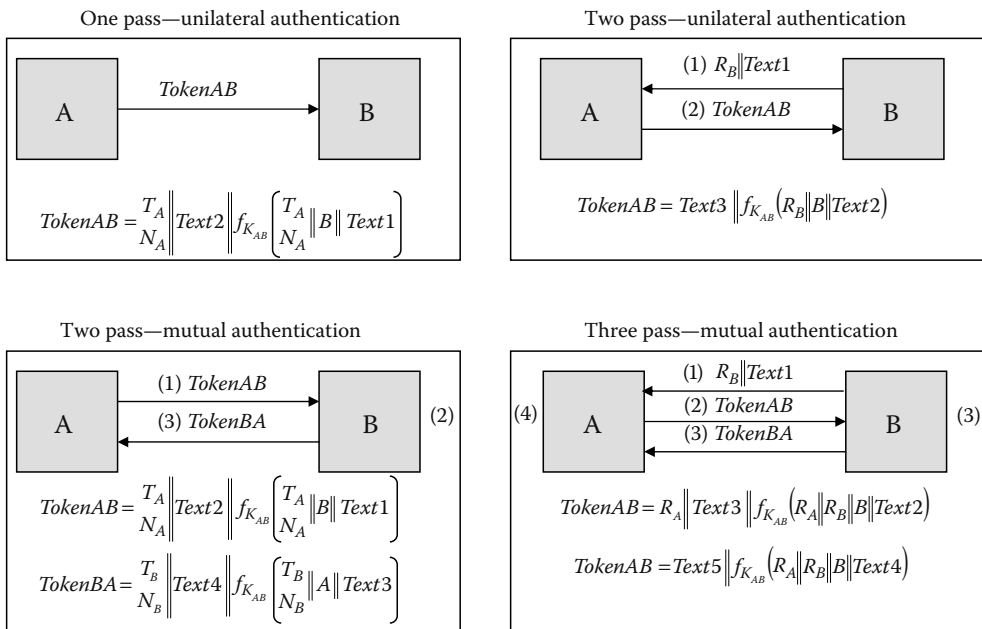


FIGURE 2.3 Entity authentication mechanisms.

Eavesdropping is the opportunistic interception of information exchanged between a legitimate tag and legitimate reader. However, skimming occurs when the data stored on the RFID tag is read without the owner's knowledge or consent. An unauthorized reader interacts with the tag to obtain the data. This attack can be carried out because most of the tags broadcast their memory content without requiring authentication.

One interesting project is the Adam Laurie's RFIDIOT project [48]. Specifically, RFIDIOT is an open source library for exploring RFID devices. Several experiments with readers operating at 13.56 MHz and 125/134.2 kHz are shown. The number of standards supported by the library is around 50. Some examples of the attacks carried out are the following:

Nonauthentication example: In 2004, Verichip received approval to develop a human-implant RFID microchip [49]. About twice the length of a grain of rice, the device is typically implanted above the triceps of an individual's right arm. Once scanned at the proper frequency, the Verichip answers with a unique 16 digit number which can correlate the user to the information stored on a database. The type of tag used by Verichip appears to be an EM4x05. This kind of tag can be read simply with the program "readlfx.py," obtaining the following information: card ID, tag type, application identifier, country code, and national ID.

Password authentication example: Since 2003, the Oyster card has been used on Transport for London and National Rail services. The Oyster card is a contactless smart card, with a claimed proximity range of about 8 cm, and based on Philips's MIFARE® standard [50]. A code for attacking this kind of card is included. The sample program "bruteforce.py" can be run against it, and it will try to log in the sector 0 by choosing random numbers as the key.

Nowadays, the security of e-passports have aroused a great interest [16,17,51,52]. Skimming is problematic because e-passports possess sensitive data. The mandatory passive authentication mechanism demands the use of digital signatures. A reader will be able to verify that the data came from the correct passport-issuing authority. However, digital signatures do not link data to a specific passport. Additionally, if only passive authentication is supported, an attacker equipped with a reader could obtain sensitive information such as your name, birthday, or even your facial photograph. This is possible because readers are not authenticated—in other words, the tag answers indiscriminately. Certain projects exist which give the code needed to read e-passports: RFIDIOT (Adam Laurie) [48], OpenMRTD (Harald Welte) [53], and JMRTD (SoS group, ICIS, Radbound University) [54].

2.3.5 CLONING AND PHYSICAL ATTACKS

Symmetric-key cryptography can be used to avoid tag cloning attacks. Specifically, a challenge-response like the following can be employed. First, the tag is singulated from many by means of a collision-avoidance protocol like the binary tree walking protocol. The tag (T_i) shares the key (K_i) with the reader. Afterward, the following messages are exchanged:

1. The reader generates a fresh random number (R) and transmits it to the tag.
2. The tag computes $H = g(K_i, R)$ and sends back to the reader.
3. The reader computes $H' = g(K_i', R)$ and checks its equality with H .

The g function can be implemented by a hash function or, alternatively, by an encryption function. Note that if the g function is well constructed and appropriately deployed, it is infeasible for an attacker to simulate the tag. Because standard cryptographic primitives (hash functions, message authentication codes, block/stream ciphers, etc.) are extravagant solutions for low-cost RFID tags on account of their demand for circuit size, power consumption, and memory size [55], the design of new lightweight primitives is pressing.

For some kinds of tags, resources are not so restricted. However, their cost is much higher than low-cost RFID tags (i.e., tags used in supply chain). An example of these sort of tags are e-passports. The active authentication method is an anticloning feature. The mechanism relies on public cryptography. It works by having e-passports prove possession of a private key:

1. The tag generates an 8 bytes nonce and sends it to the tag.
2. The tag digitally signs this value using its private key and transmits it to the reader.
3. The reader can verify the correctness of the response with the public key supposedly associated with the passport.

Tamper-resistant microprocessors are used to store and process private and sensitive information, such as private keys or electronic money. The attacker should not be able to retrieve or modify this information. To achieve this objective, chips are designed so that the information is not accessible using external means and can only be accessed by the embedded software, which should contain the appropriate security measures.

Making simple electronic devices secure against tampering is very difficult, as a great number of attacks are possible, including [56]:

- Mechanical machining
- Laser machining
- Energy attacks
- Temperature imprinting
- Probe attacks
- Active or injector probes
- Energy probes
- Manual material removal
- Clock glitching
- Electronic beam read/write
- Imaging technology
- Water machining
- Shaped charge technology
- Radiation imprinting
- High-voltage imprinting
- Passive probes
- Pico probes
- Matching methods
- High or low voltage
- Circuit disruption
- IR laser read/write
-
-

As sensitive information such as cryptographic keys are stored on the chips, tamper-resistant devices may be designed to erase this information when penetration of their security encapsulation or out-of-specification environmental parameters is detected. Some devices are even able to erase all their information after their power supply has been interrupted.

In the RFID context, we have to distinguish between low-cost RFID tags and tags used in applications without severe price restrictions. Low-cost RFID tags are very constrained resources (storing, computing, and energy consumption). These kinds of tags are usually nonresistant to physical attacks. An example of these kinds of tags are tags compliant with the EPC Class-1 Generation-2 specification [57]. High-cost tags, sometimes called contactless chips or smart cards, are not so restrictive

regarding resources. However, price increases from 0.05 € to several euros. For example, the chips used in e-passports have an EAL 5+ security level, the highest security level for chips [58]. Therefore, an attacker will not be able to acquire the private key used in private authentication to avoid cloning attacks. The plusID tag, manufactured by Bradcom, is another example of tamper-resistant tags [59]. Initially, its security level was 2 (tamper evidence) according to Federal Information Processing Standards (FIPS), but it was finally increased to level 3 (tamper resistant).

2.3.6 REPLAY AND RELAY ATTACKS

A replay attack copies a stream of messages between two parties and replays it to one or more of two parties. A generalized definition of a replay attack could be the following: an attack on a security protocol using replay of messages from a different context into the intended (or original and expected) context, thereby fooling the honest participant(s) into thinking they have successfully completed the protocol run [60]. An exhaustive classification of replay attacks can be found in Ref. [61].

Common techniques to avoid replay attacks are incremental sequence number, clock synchronization, or a nonce. In Ref. [62], a set of design principles for avoiding replays attacks in cryptographic protocols is presented. In a RFID context, clock synchronization is not feasible because passive RFID tags cannot make use of clocks, as these kind of tags do not have an on-board power source. Incremental sequence such as session token may be a straightforward solution if tracking is not considered a threat. Therefore, the use of nonce is the most suitable option for RFID tags.

A number of factors combine to make relay attacks on RFID technology is possible. Tags are read over a distance and activated automatically when close to a reader. Therefore, an attacker could communicate with a tag without the knowledge of its owner.

Two devices, as shown in Figure 2.4, are involved in the relay attack: the ghost and the leech [36]. The ghost is a device which fakes a card to the reader, and the leech is a device which fakes a reader to the card. A fast communication channel between the legitimate reader and the victim card is created by the ghost and the leech:

1. Legitimate reader sends a message (A) to the ghost.
2. Ghost receives it and forwards this message (A) to the leech through the fast communication channel (minimum delay).
3. Leech fakes the real reader, and sends the message (A) to the legitimate tag.
4. Legitimate tag computes a new message (B) and transmits it to the leech.

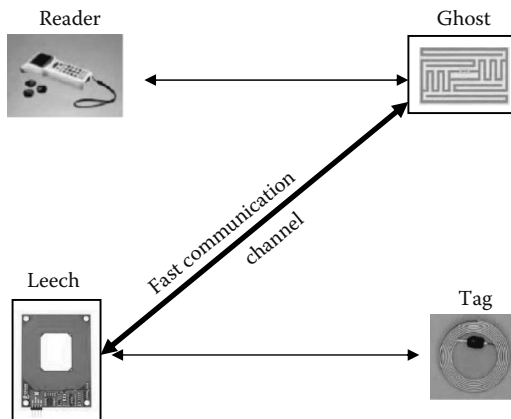


FIGURE 2.4 Relay attacks.

5. Leech receives it and forwards this message (B) to the ghost through the fast communication channel.
6. Ghost forwards this message (B) to the real reader.

This sort of attack dispels the assumption that readers and tags should be very close to communicate. Additionally, even if communications are encrypted, the attack is feasible because messages are only relayed through a fast communication channel, without requiring knowledge of its content. In Ref. [63], a practical relay attack against ISO 14443 compliant tags is described.

2.3.7 HIDING

RFID technology uses electromagnetic radio waves. Labeled items can be therefore protected by insulating them from any kind of electromagnetic radiation:

Faraday cage: A faraday cage or shield is a container made of conducting material, or a mesh of such material. This blocks out radio signals of certain frequencies. There are currently a number of companies that sell this type of solution [64,65].

Passive jamming: Each time a reader wants to interact with a single tag, the tag will have to be singulated from a population of tags. A collision-avoidance protocol such as Aloha or binary tree walking protocol may be employed. To conceal the presence of a particular tag, this could simulate the full spectrum of possible tags in the singulation phase, hiding its presence. This concept was first introduced by Juels et al. as the “Blocker tag” [66]. In 2004, a variant of the blocker concept, named “soft blocking,” was introduced [67]. This involves software (or firmware) modules that offer a different balance of characteristics from ordinary blockers.

Active jamming: Another way of achieving isolation from electromagnetic waves is disturbing the radio channel known as active jamming of RF signals. This disturbance may be effected with a device that actively broadcasts radio signals, so as to completely disrupt the radio channel, thus preventing the normal operation of RFID readers. However, in most cases, government regulations on radio emissions (power and bandwidth) are violated [68].

2.3.8 DEACTIVATING

Some methods exist for deactivating tags and rendering them unreadable. The most common method consists of generating a high-power RF field that induces sufficient current to burn out a weak section of the antenna. The connection between the chip and the antenna is cut off, rendering it useless. This method is usually chosen to address privacy concerns and to deactivate tags that are used to label individual items or prevent thefts in stores.

The benefits of using RFID technology in a store are clear. However, the deactivation of tags may be malicious. The necessary technology can be available to anyone. The usual range of a “kill” signal is only a few centimeters. However, designing and building a high-gain antenna with a high-power transmitter is easy. Using batteries, it could probably fit into a backpack. Then an attacker entering a store could kill all the tags, causing widespread retail chaos. A practical implementation of this sort of attack is the RFID-Zapper project [69,70].

Karjoth et al. proposed the use of physical RFID structures that permit a consumer to disable a tag by mechanically altering the tag [71]. In “clipped tags,” the consumer can physically separate the body (chip) from the head (antenna) in an intuitive way. Such separation provides visual confirmation that the tag has been deactivated. Then the tag can be reactivated by means of physical contact. The reactivation requires deliberate actions on the part of its owner. Indeed, reactivation cannot be carried out without the owner’s knowledge unless the item was stolen.

To avoid wanton deactivation of tags, the use of kill passwords has been proposed. Tags compliant to the EPC Class-1 Generation-2 implement this feature [57]. When an electronic product code (EPC)

tag receives the “kill” command, it renders itself permanently inoperative. However, to protect tags from malicious deactivation, the kill command is PIN protected. One of the main problems linked to solutions based on password is its management. Employing the same password for all tags could be a naive solution. Nevertheless, if a tag is compromised, all the tags would be at risk. Another straightforward solution is that each tag has a different password with the associated management and scalability problems.

The potential benefits of RFID technology usage are reduced if tags are permanently deactivated. Instead of killing tags, they could be put to sleep, rendering them only temporarily inoperative. As with the killing process, sleeping/waking up tags will not offer real protection if anyone is able to accomplish these operations. So some form of access control, such a PINs, will be needed. To sleep/wake up a tag, a PIN has to be transmitted.

2.3.9 CRYPTOGRAPHIC VULNERABILITIES

In nineteenth century, Kerckhoffs sets out the principles to the public known of cryptography systems [72]:

1. The system must be practically, if not mathematically, indecipherable.
2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
3. Its key must be communicable and retainable without the help of written notes, and changeable or able to be modified at the will of the correspondents.
4. It must be applicable to telegraphic correspondence.
5. It must be portable, and its usage and function must not require the concurrence of several people.
6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

RFID tags are very constrained devices, with restrictions in power consumption, storage, and circuitry. Due to these severe limitations, some commercial RFID tags support weak cryptographic primitives, and thus vulnerable authentication protocols. Additionally, some of these cryptographic primitives are proprietary. The use of proprietary solutions is not really inadequate if algorithms are published to be analyzed by the research community. However, time has shown, the security of an algorithm cannot reside in “obscurity.” A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that the flaws are unknown, and that attackers are unlikely to find them [72].

Texas Instruments manufacture a low-frequency tag, named digital signature transponder (DST). The DST executes a challenge–response protocol. The reader and the DST share a secret key K_i . The reader sends a challenge R to the DST. The DST computes an encryption function of the challenge $C = e_{K_i}(R)$ and sends this value to the reader. The reader computes $C' = e_{K_i'}(R)$ and compares this value with the received value. The challenge is 40 bits in length, and the output of the encryption function is 24 bits in length. The length of the K_i is only 40 bits. It is a very short length. The National Institute of Standards and Technology [73] and the ECRYPT EU Network of Excellence on cryptography [74] recommended in 2005 a key length of 80 bits for a minimal level of general-purpose protection, and 112 bits for the following ten years.

The most common uses of DST are the following:

1. DST is employed as a theft-deterrent (immobilizer keys) in automobiles, such as Ford and Toyota vehicles.
2. DST serves as a wireless payment device (speedpass), which can be used by more than seven million individuals in around 10,000 Exxon and Mobile gas stations.

Texas Instruments has not published details of the encryption algorithm, basing itself on security through algorithm obscurity. A team of researchers at Johns Hopkins University and RSA Laboratories discovered security vulnerabilities in the DST [75]. In particular, a successful reverse engineering of the DST encryption algorithm was accomplished. First, a rough schematic of the cipher was obtained from a published Texas Instruments presentation. With the reverse engineering of the cipher, they showed that a 40 bit key length was inadequate, the cipher being not only vulnerable to brute-force attacks as known by cryptographers. The attack can be divided into three phases:

Reverse engineering: They were equipped with a DST reader and some blank DST tags. With the reader and the blank tags, the output of the encryption function, with any key and challenge, could be obtained. Using specific key/challenge pairs and centering on the schematic of the encryption, operational details of the algorithm were derived.

Key cracking: After determining the encryption algorithm, a programmed hardware “key cracker” was implemented to recover the unique cryptographic key of the DST. The cracker operated by brute force (full space of 2^{40}). Given two input–output, in about 30 minutes the secret key was recovered.

Simulation: They programmed a hardware device with the key recovered from the DST. This device could impersonate the original DST.

The research on the DST exemplifies Kerckhoffs principles. Another significant example is the proprietary CRYPTO1 encryption algorithm used in Philips Mifare cards, which has been recently reverse engineered [76]. We recommend the publication of any algorithms. Open algorithms can be analyzed and refined by the scientific community, bolstering confidence in their security.

2.4 BACK-END DATABASE

2.4.1 TAG COUNTERFEITING AND DUPLICATION

Because the incorporation of RFID technology in sensitive applications such as passports [77] or pharmaceutical pedigrees [78], the possibility of creating counterfeiting tags has unleashed some concerns.

Here are some arguments that may dissuade users from alarmist attitudes [79]:

1. Usually, each tag has a unique identifier (ID) that allows its unequivocal identification. To counterfeit a tag, one would have to modify the identity of an item, which generally implies tag manipulation. The tag (ID) implementation may vary in each manufacturer as well as in each product. The major manufacturers first program the tag and then lock it. So resistance to using attacks lies in the lock. In most cases, it is not possible to unlock the tag without using invasive techniques. These techniques are not commonly available to the general industry.
2. RFID tags are generally sold preprogrammed with their identifiers, this being one of the phases of the normal production process. The ID format usually accords with a standard. The nonavailability of blank tags will therefore reduce the possibility of counterfeiting.
3. Another alternative is the design of blank tags. However, even with the equipment necessary for IC fabrication, designing these kind of chips is not an easy task.

Despite the difficulty of counterfeiting tags, on some occasions tags are duplicated. It is a similar problem to that of credit card fraud where a card is duplicated and possibly used in multiple places at the same time. As duplicate tags cannot be operatively distinguished, the back-end database should detect rare conditions. An example of a rare condition is the following: a tag cannot be in the toll

gate on the Madrid–Barcelona motorway and 15 minutes later in the toll gate of Valencia–Barcelona motorway. The design of back-end database should be considered case by case [80].

2.4.2 EPC NETWORK: ONS ATTACKS

The EPCglobal network is made up of three key elements, as displayed in Figure 2.5:

1. EPC information services (EPC-IS)
2. EPC discovery services
3. Object name service

When an RFID tag is manufactured with an EPC, the EPC is registered within the ONS. The RFID tag is attached to a product, and the EPC becomes a part of that product as it moves through the supply chain. The particular product information is added to the manufacturer’s EPC-IS, and the knowledge that this data exists within the manufacturer’s EPC-IS is passed to the EPC discovery service.

The ONS is a distributed but authoritative directory service that routes request for information about EPCs. Existing or new network resources can be employed to route the requests. The ONS is similar to domain name service (DNS) both technologically and functionally. When a query is sent to the ONS including the EPC code, one or more localizations (uniform resource locator or URL) where information about items reside, are returned. The ONS service is divided in two layers. First, the Root ONS, which is the authoritative directory of manufacturers whose products may have information on the EPC Network. Second, the Local ONS, which is the directory of products for that particular manufacturer.

As the ONS can be considered a subset of the DNS, the same security risks are applicable. In 2004, a threat analysis of the domain name system was published as RFC 3833 [81]. Some of the principal threats identified are the following:

1. Packet interception: manipulating Internet Protocol (IP) packets carrying DNS information.
2. Query prediction: manipulating the query/answer schemes of the DNS protocol.
3. Cache poisoning: injecting manipulated information into DNS caches.
4. Betrayal by trusted server: attacker controlling DNS servers in use.
5. DoS: DNS is vulnerable to DoS as happens in any other network service. Additionally, the DNS itself might be used to attack third parties.

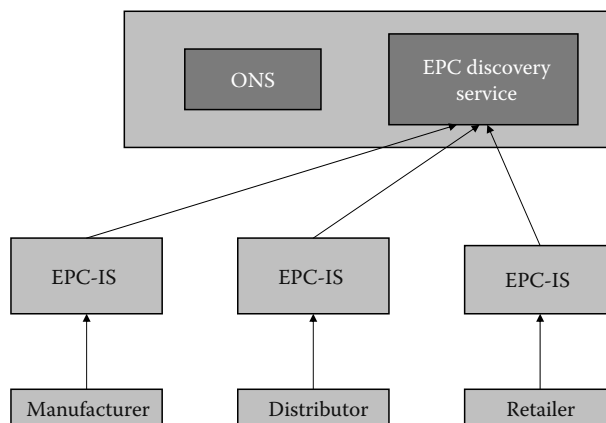


FIGURE 2.5 EPCglobal network.

However, there are some risks that are particular to the ONS service [82]:

1. **Privacy:** There are many situations where the EPC of an RFID tag can be considered highly sensitive information. Sensitive information can be obtained even knowing just part of the EPC. For example, knowing only the class of the identifier, you can find out the kind of object. To obtain the information associated with a tag, the EPC-IS has to be located. Even if the connections to the EPC-IS are secured (i.e., Secure Sockets Layer [SSL]/Transport Layer Security [TLS] protocol), the initial ONS look-up process is not authenticated nor encrypted in the first place. Therefore, sensitive information passes in clear on the channel (middleware-networks-DNS server).
2. **Integrity:** The correctness and the completeness of the information should be guaranteed. An attacker controlling intermediate DNS servers or launching a successful man-in-the-middle attack could forge the list of URLs (i.e., a fraudulent server). To prevent this attack, an authentication mechanism should be used for the EPC-IS.
3. **Availability:** If the adoption of the EPC network is widespread, there will be a great number of companies dependent on network services. ONS will become a service highly exposed to attacks. These could include distribute denial-of-service (DDoS) attacks that reduce the functioning of the server or its network connection by issuing countless and intense queries, or targeted exploits that shut down the server software or its operating system.

2.4.3 VIRUS ATTACKS

The RFID tag memory contains a unique identifier, but additional data may be stored. The data size varies from a few bytes to several kilobytes. The memory where this additional information is stored is rewritable. The information sent by the tags is implicitly trusted, which implies some security threats [80,83]:

1. **Buffer overflow:** It is one of the most frequent sources of security vulnerabilities in software. Programming languages, such as C or C++, are not memory safe. In other words, the length of the inputs are not checked. An attacker could introduce an input that is deliberately longer, writing out of the buffer. As program control data is often located in memory areas adjacent to data buffers, the buffer overflow may lead the program to execute an arbitrary code. As a great number of tags have severe storage limitations, resource-rich tag simulating devices could be utilized [84].
2. **Code insertion:** An attacker might inject malicious code into an application, using any script language (i.e., common gateway interface, Java, Perl, etc.). RFID tags with data written in a script language could perform an attack of this kind. Imagine that the tags used for tracking baggage in the airport contain the airport destination in its data field. Each time a tag is read, the back-end system fires the query, “select * from location_table where airport = <tag data>.” Imagine that an attacker stores in one piece of baggage “MAD;shutdown.” When this data is read, the database will be shutdown and the baggage system will crashed.
3. **Structure Query Language (SQL) injection:** It is a type of code insertion attack, executing SQL codes in the database that were not intended. The main objectives of these attacks are the following: enumerate the database structure, retrieve authorized data, make unauthorized modifications or deletions, etc. RFID tags could contain data for a SQL injection attack. Storage limitation is not a problem, as it is possible to do a lot of harm with a very small amount of SQL. For example, the SQL “drop table <tablename>” will delete a specified database table.

Summarizing, an RFID tag is an unsecured and untrusted database. So the information obtained from such devices should be analyzed until there is sufficient evidence that the data is accurate. However, this is not a new concept, as in all information systems the input data should be examined to ensure that it will not cause problems.

REFERENCES

- [1] L. Bolotnyy and G. Robins. Physically unclonable function-based security and privacy in RFID systems. In *Proceedings of PerCom'07*, pp. 211–220. IEEE Computer Society Press, Washington, DC, 2007.
- [2] J. Cichon, M. Klonowski, and M. Kutylowski. Privacy protection in dynamic systems based on RFID tags. In *Proceedings of PerSec'07*, pp. 235–240. IEEE Computer Society Press, Washington, DC, 2007.
- [3] T. Heydt-Benjamin, H.-J. Chae, B. Defend, and K. Fu. Privacy for public transportation. In *Proceedings of PET'06, LNCS*, 4258, pp. 1–19. Springer-Verlag, Cambridge, U.K., 2006.
- [4] T. Hjørth. Supporting privacy in RFID systems. Master thesis, Technical University of Denmark, Lyngby, Denmark, 2004.
- [5] A. Juels and R. Pappu. Squealing euros: Privacy protection in RFID-enabled banknotes. In *Proceedings of FC'03, LNCS*, 2742, pp. 103–121. Springer-Verlag, Guadeloupe, French West Indies, 2003.
- [6] S. Kinoshita, M. Ohkubo, F. Hoshino, G. Morohashi, O. Shionoiri, and A. Kanai. Privacy enhanced active RFID tag. In *Proceedings of ECHISE'05*, Munich, Germany, 2005.
- [7] E. Kosta, M. Meints, M. Hensen, and M. Gasson. An analysis of security and privacy issues relating to RFID enabled e-passports. In *Proceedings of Sec'07, IFIP*, 232, pp. 467–472. Springer, Sandton, South Africa, 2007.
- [8] D. Ranasinghe, D. Engels, and P. Cole. Security and privacy: Modest proposals for low-cost RFID systems. In *Proceedings of Auto-ID Labs Research Workshop*, Zurich, Switzerland, 2004.
- [9] M. Rieback, B. Crispo, and A. Tanenbaum. Uniting legislation with RFID privacy-enhancing technologies. In *Security and Protection of Information*, Brno, Czech Republic, 2005.
- [10] M. Rieback, G. Gaydadjev, B. Crispo, R. Hofman, and A. Tanenbaum. A platform for RFID security and privacy administration. In *Proceedings of LISA'06*, Washington, DC, 2006.
- [11] S.E. Sarma, S.A. Weis, and D.W. Engels. RFID systems and security and privacy implications. In *Proceedings of CHES'02, LNCS*, 2523, pp. 454–470. Springer-Verlag, Redwood City, CA, 2002.
- [12] S. Spiekermann and H. Ziekow. RFID: A 7-point plan to ensure privacy. In *Proceedings of ECIS'05*, Regensburg, Germany, 2005.
- [13] Universal declaration of human rights, Article 12, 1948.
- [14] EU Directive 95/46/EC—Data Protection Directive. Official Journal of the European Communities, November 23, 1995.
- [15] M. Weiser. The computer for the 21st century. *Scientific American*, 265(3):94–104, September 1991.
- [16] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. Wichers Schreur. Crossing borders: Security and privacy issues of the European e-passport. In *Proceedings of IWSEC'06, LNCS*, 4266, pp. 152–167. Springer-Verlag, Kyoto, Japan, 2006.
- [17] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In *Proceedings of SecureComm'05*. IEEE Computer Society, Athens, Greece, 2005.
- [18] Advanced security mechanisms for machine readable travel documents—extended access control (EAC) version. 1.0.1. Technical guideline TR-03110, Federal Office of Information Security, Bonn, Germany, 2006.
- [19] CASPIAN. <http://www.nocards.org/>, October 1, 2005.
- [20] FoeBuD. <http://www.foebud.org/rfid>, October 5, 2005.
- [21] Boycott Benetton. <http://www.boycottbenetton.com/>, April 9, 2003.
- [22] *RFID Journal*. Behind the benetton brouhaha. <http://www.rfidjournal.com>, April 14, 2003.
- [23] Boycott Tesco. <http://www.boycotttesco.com/>, January 26, 2005.
- [24] Boycott Guillette. <http://www.boycottguillette.com/>, September 2, 2003.
- [25] K. Albrecht and L. McIntyre. *SPYCHIPS: How Major Corporations and Government Plan to Track your Every Move with RFID*. Nelson Communications, Inc., Nashville, TN, 2005.
- [26] California Senate Bill 682. <http://www.epic.org/privacy/rfid/>, February 22, 2005.
- [27] What's in California's proposed RFID Bill? <http://www.rfidproductsnew.com>, January 20, 2006.

- [28] S. Garfinkel. Bill of Rights. <http://www.technologyreview.com>, October 2002.
- [29] G. Danezis, S. Lewis, and R. Anderson. How much is location privacy worth. In *Proceedings of Workshop of Economics of IS'05*, Cambridge, MA, 2005.
- [30] A. Beresfor and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1):1536–1268, 2003.
- [31] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *Proceedings of SPC'03, LNCS*, 2802, pp. 454–469. Springer-Verlag, 2003.
- [32] Identification cards—contactless integrated circuits cards—proximity cards. <http://www.wg8.de/sdi.html>, 2001.
- [33] Machine readable travel documents, Doc. 9303. <http://www.mrtd.icao.int>, July 8, 2006.
- [34] M. Brown, E. Zeisel, and R. Sabella. *RFID+Exam Cram*. Que Publishing, Indianapolis, IN, 2006.
- [35] D.C. Ranasinghe and P.H. Cole. Confronting security and privacy threats in modern RFID systems. In *Proceedings of ACSSC 06*, pp. 2058–2064, Pacific Grove, CA, 2006.
- [36] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In *Proceedings of SecureComm'05*. IEEE Computer Society, Athens, Greece, 2005.
- [37] J. Atkinson. Contactless credit card consumer report. <http://www.findercard.com>, April 3, 2006.
- [38] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, and T. Ohare. Vulnerabilities in first-generation RFID-enabled credit cards. In *Proceedings of FC'07, LNCS*. Springer-Verlag, Lowlands, Scarborough, Trinidad/Tobago, 2007.
- [39] M. Feldhofer. A proposal for an authentication protocol in a security layer for RFID smart tags. In *Proceedings of MELECON'04*, vol. 2. IEEE Computer Society, Dubrovnik, Croatia, 2004.
- [40] I. Vajda and L. Buttyán. Lightweight authentication protocols for low-cost RFID tags. In *Proceedings of UBIComp'03*, Seattle, WA, 2003.
- [41] M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic approach to “privacy-friendly” tags. In *Proceedings of RFID Privacy Workshop*, MIT, Cambridge, MA, 2003.
- [42] P. Peris-Lopez, J.C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. In *Proceedings of UIC'06, LNCS*, 4519, pp. 912–923. Springer-Verlag, Wuhan and Three Gorges, China, 2006.
- [43] H.Y. Chien and C.H. Chen. Mutual authentication protocol for RFID conforming to EPC class-1 generation-2 standards. *Computer Standards and Interfaces*, 29(2):254–259, 2007.
- [44] A. Juels. Minimalist cryptography for low-cost RFID tags. In *Proceedings of SCN'04, LNCS*, 3352, pp. 149–164. Springer-Verlag, Amalfi, Italy, 2004.
- [45] D. Molnar and D. Wagner. Privacy and security in library RFID: Issues, practices, and architectures. In *Proceedings of ACM CCS'04*, pp. 210–219. ACM Press, Washington, DC, 2004.
- [46] ISO/IEC 9798 Information Technology—Security techniques—Entity authentication. <http://www.iso.org>, 1995.
- [47] Anti-skimming in Japan. <http://www.future.iff.org/index.html>, August 10, 2005.
- [48] A. Laurie. RFIDIoT project. <http://www.rfidiot.org>, August 5, 2007.
- [49] Verichip corporation. <http://www.verichipcorp.com>, August 15, 2007.
- [50] Easing traveling in London’s congested public transport network. <http://www.mifare.net/showcases/london.asp>, August 10, 2007.
- [51] M. Halváč, Martin, and T. Rosa. A note on the relay attacks on e-passports: The case of Czech e-passports. In *Cryptology ePrint Archive, Report 2007/244*, IACR, 2007.
- [52] D. Carluccio, K. Lemke, and C. Paar. Electromagnetic side channel analysis of a contactless smart card: First results. In *Handout of Workshop on RFID Security*, Graz, Austria, 2006.
- [53] H. Welte. OpenMRTD project. <http://www.openmrt.org>, August 7, 2007.
- [54] SoSGroup, ICIS, and Radbound University. JMRTD project. <http://www.jmrt.sourceforge.net/>, August 9, 2007.
- [55] A. Juels. RFID security and privacy: A research survey. Manuscript, 2005.
- [56] S.H. Weingart. Physical security devices for computer subsystems: A survey of attacks and defenses. In *Proceedings of CHES'00, LNCS*, 1965, pp. 302–317. Springer-Verlag, Worcester, MA, 2000.
- [57] Class-1 Generation-2 UHF air interface protocol standard version 1.0.9: “Gen-2”. <http://www.epcglobalinc.org/standards/>, 2005.
- [58] C. Lee, D. Houdeau, and R. Bergmann. Evolution of the e-passport. <http://www.homelandsecurityasia.com>, September 3, 2007.

- [59] C. Swedberg. Broadcom introduces secure RFID chip. *RFID Journal*. <http://www.rfidjournal.com>, June 29, 2006.
- [60] S. Malladi, S. Alves-Foss, and R. Heckendorn. On preventing replay attacks on security protocols. In *Proceedings of SM'02*, pp. 77–83, CSREA Press, Las Vegas, NV, 2003.
- [61] P. Syverson. A taxonomy of replay attacks. In *Proceedings of CSF'94*, pp. 187–191. IEEE Computer Society, Franconia, NH, 1994.
- [62] T. Aura. Strategies against replay attacks. In *Proceedings of CSF'97*. IEEE Computer Society, Rockport, MA, 1997.
- [63] G. Hancke. Practical attacks on proximity identification systems (short paper). In *Proceedings of SP'06*. IEEE Computer Society, Oakland, CA, 2000.
- [64] mCloak for RFID tags. <http://www.mobilecloak.com/rfidtag/rfid.tag.html>, September 10, 2005.
- [65] Envelope to help you do it with your security, privacy, and discretion intact. <http://www.emvelope.com>, August 13, 2007.
- [66] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *ACM CCS'03*, pp. 103–111. ACM Press, Washington, DC, 2003.
- [67] A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap. In *WPES'04*, pp. 1–7. ACM Press, Washington, DC, 2004.
- [68] RSA Laboratories. Faq on RFID and RFID privacy. <http://www.rsa.com/rsalabs/node.asp?id=2120>, October 4, 2007.
- [69] J. Collins. RFID-Zapper shoots to kill. *RFID Journal*, January 23, 2006.
- [70] MiniMe and Mahajivana. RFID-Zapper project. [http://www.events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper\(EN\)_77f3.html](http://www.events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html), 2006.
- [71] G. Karjoth and P.A. Moskowitz. Disabling RFID tags with visible confirmation: Clipped tags are silenced. In *Proceedings of WPES'05*. ACM Press, Alexandria, VA, 2005.
- [72] A. Kerckhoffs. La cryptographie militaire. *Journal des Sciences*, 9:161–191, 1983.
- [73] Recommendation for key management. Technical Report Special Publication 800-57 Draft, National Institute of Technology, 2005.
- [74] Year report on algorithms and key sizes. Technical Report IST-2002-507932, ECRYPT, 2006.
- [75] S. Bono, M. Greem, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled device. In *Proceedings of SSYM'05*. Usenix Association, Alexandria, VA, 2005.
- [76] N. Karten and H. Plotz. Mifare little security, despite obscurity. <http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html>, 2007.
- [77] P. Prince. United States sets date for e-passports. *RFID Journal*, October 25, 2005.
- [78] E. Wasserman. Purdue Pharma to run pedigree pilot. *RFID Journal*, May 31, 2005.
- [79] M. Guillory. Analysis: Counterfeit tags. <http://www.aimglobal.org>, June 30, 2005.
- [80] F. Thornton, B. Haines, A. Das, H. Bhargava, A. Campbell, and J. Kleinschmidt. *RFID Security*. Syngress Publishing, 2006.
- [81] D. Atkins and R. Austein. Threat analysis of the domain name system (DNS). In *Request for Comments—RFC 3833*, Berkeley, CA, 2004.
- [82] B. Fabian, G. Oliver, and S. Spiekermann. Security analysis of the object name service for RFID. In *Proceedings of SecPerU'05*. IEEE Computer Society, Santorini Island, Greece, 2005.
- [83] M. Rieback, C. Bruno, and A. Tanenbaum. Is your car infected with a computer virus? In *Proceedings of PerCom'06*. IEEE Computer Society, Pisa, Italy, 2006.
- [84] B. Jamali, P.H. Cole, and D. Engels. In *Networked RFID Systems and Lightweight Cryptography, chapter RFID Tag Vulnerabilities in RFID Systems*, pp. 147–155. Springer, 2007.