Security and privacy concerns about the RFID layer of EPC Gen2 networks

Joaquin Garcia-Alfaro, Jordi Herrera-Joancomarti, Joan Melia-Segui

Security and Privacy Concerns about the RFID layer of EPC Gen2 Networks

Joaquin Garcia-Alfaro[1,2], Jordi Herrera-Joancomartí[1,3], and Joan Melià-Seguí[1,4]

[1] Internet Interdisciplinary Institute, Universitat Oberta de Catalunya,
Roc Boronat 117, 08018 Barcelona
[2] Télécom SudParis, CNRS UMR 5157 (SAMOVAR), 91011 Evry, France
joaquin.garcia-alfaro@acm.org
[3] Universitat Autonoma de Barcelona, Edifici Q, 08193, Bellaterra
jordi.herrera@uab.cat
[4] Universitat Pompeu Fabra, Tanger 122-140, 08018 Barcelona
joan.melia@upf.edu

Abstract. RFID systems are composed by tags (also known as electronic labels) storing an identification sequence which can be wirelessly retrieved by an interrogator, and transmitted to the network through middleware and database information systems. In the case of the EPC Gen2 technology, RFID tags are not provided with on-board batteries. They are passively powered through the radio frequency waves of the interrogators. Tags are also assumed to be of low-cost nature, meaning that they shall be available at a very reduced price (predicted for under 10 US dollar cents in the literature). The passive and low-cost nature of EPC Gen2 tags imposes several challenges in terms of power consumption and integration of defense countermeasures. Like many other pervasive technologies, EPC Gen2 might yield to security and privacy violations if not handled properly. In this chapter, we provide an in-depth presentation of the RFID layer of the EPC Gen2 standard. We also provide security and privacy threats that can affect such a layer, and survey some representative countermeasures that could be used to handle the reported threats. Some of the reported efforts were conducted within the scope of the ARES project.

Keywords: RFID, EPC Gen2, Security, Privacy, Threats, Countermeasures.

1 Introduction

Radio Frequency Identification (RFID) technology is an automatic identification method for retrieving digital information without physical contact or line-of-sight, that is revolutionizing the manner in which objects and people can be identified by computers [1]. Tagging objects or even people with smart labels (the so called RFID tags) emitting identifying information in form of binary modulated signal, is the way computers can actually understand the presence of objects. RFID technology is the closest approach to the ubiquitous computing [2] or the future *Internet of Things*. RFID labels are frequently referred as the next generation barcodes. Although the utility is the same (the identification of an object), RFID offers two main advantages over conventional barcode systems. On the one hand, optical barcodes only indicates the generic product, whereas

an RFID tag can identify the item (being able to distinguish different objects from the same product). On the other hand, there is no need of line-of-sight. Thus, while optical barcodes must be identified one by one, RFID tags can be read much faster, without human intervention and in large quantities [1, 3].

The unassisted wireless identification makes the RFID very attractive in areas like product traceability, inventorying or personal identification, but it also creates setbacks. Like the rest of wireless information technologies, RFID information transferred between sender and receiver is not completely secure. The air interface is much more insecure than the wired one, because the only presence of an attacker in the communication area gives him the opportunity to obtain information in a malicious way. The scarce available energy on tags, and the limited computational capabilities of tags are also determinant for security in RFID. In addition, RFID is very related with personal identification. Imagine, for instance, a medical application in wich the patient is using RFID tagged drugs. With some trivial techniques [3, 4], it will not be difficult to link patients and drugs by simply eavesdropping the exchange of messages at the RFID layer. Privacy issues must, therefore, be considered.

In this chapter, we describe those aformentioned threats and survey current countermeasures to handle them. We focus our interest on a particular RFID technology, namely the Electronic Product Code Class 1 Generation 2 (EPC Gen2) [5] standard. EPC Gen2 is a low-cost passive RFID technology for UHF, designed by EPCglobal [6] and developed in the MIT Auto-ID labs. This technology is being widespread in the retail industry [7], and also other sectors [8], thanks to the reduced price of their tags. EPC Gen2 was designed giving priority to reduce the price by means of a very simple performance [3]. Indeed, the price is the main reason for the industry to adopt or to refuse a technology. It is not a coincidence that the EPC technology appearance coincided with the explosion of RFID adoption in the retail industry [9], because tag price should not increase the product cost [3]. It can be said that a small area chip (thus a few logical gates) and no battery on-board (thus using radio frequency waves to energize the tag) will be a cheap tag. But that also means that there is almost no place for additional capabilities in the chip like security mechanisms. In fact, security measures implemented on those devices are scarce and are basically reduced to the use of pseudorandom number generators and short passwords [1].

Chapter Organization: Section 2 introduces the EPC Gen2 technology characteristics. Section 3 presents our classification of threats. Section 4 surveys recent conuntermeasures to handle the threats. Section 5 closes the chapter.

2 The EPC Gen2 Standard

The EPC technology is based on the use of RFID. This technology is intended to be the successor of the nowadays ubiquitous barcodes. Designed in the Massachusetts Institute of Technology Auto-ID Labs, and developed by the EPCGlobal consortium [6], the EPC technology represents the key component of an architecture known as EPCglobal Network [5]. The main components of the RFID system are the electronic labels or tags, the readers and the Information Systems (IS) e.g. middleware, databases and servers.

The main goal of this architecture is the object-in-motion automatic identification in the supply chain and factory production.

The EPC Gen2 tags are passive devices powered by the electronic field generated by the reader, due to the absence of on-board batteries. A summary of their properties is provided in Table 1. EPC Gen2 tags work worldwide on the ultra high frequency (UHF) band between 860 and 960 MHz, depending on the RF regulations for each continent. The communication range between tags and readers depends on the electric field, thus, it may vary depending on the power supply and antenna design, but also on the kind of surface where the tag is placed. RFID tags are intended to be deployed widely so they must be cheap. EPC Gen2 Tags are composed by two main elements, the *Integrated Circuit* (IC) and the *antenna*.

Table 1. EPC Gen2 tags main properties

Identification	96 bit
Communication range	$\sim$ 5 m
Tag power consumption	$\sim$ 10 μW
Frequency (Europe)	865-868 MHz (UHF)
Tags Tx ratio	40 - 640 kbps
Tags Rx ratio	26.7 - 128 kbps
Identifications per second	$\sim$ 200

The IC is based on a state machine model that processes and stores the RFID information. The antenna is intended to receive and transmit RFID signals, and also to energize the IC. In a low-cost RFID system, like EPC Gen2, the tags are very simple and resource limited, allowing to reduce their cost under the 10 cents of US dollar [10]. This reduction on the tag cost is proportional to the size of the silicon IC. The typical measure of space in silicon ICs is the *gate equivalent* (GE) that is equivalent to a boolean *two-input NAND gate*. The estimations on available GE for EPC Gen2 implementations are around 10,000 GE [11, 12].

The EPC Gen2 system communication model is common to other low-cost RFID systems where the reader (or radio-frequency interrogator) talks first. EPC Gen2 tags are passive and power dependent from the reader to respond the queries. The communication between tag and reader in the EPC Gen2 system is organized in three stages. In the *Selection* and *Inventorying* stages, the reader initiates the communication sending identification queries. The available tags in the communication range respond with a 16-bit provisional identifier extracted from the on-board pseudorandom number generator. When the reader acknowledges the provisional identifier, each single tag sends an identification sequence. The EPC Gen2 standard defines the identification sequence with 96 bits [5], but other identification sizes can be used depending on the tag manufacturer. If the reader manages to access or modify the tag memory content at this point, the *Access* stage is started. In the remainder of this section we introduce the main properties of the EPC Gen2 technology assumed in this chapter.

2.1 Tag Memory Details

An EPC Gen2 tag memory is logically divided into four banks (cf. Table 2):

- **Reserved**: This memory block shall contain the 32-bit access and kill passwords. If these passwords are not specified, a logic *zero* is stored on that memory area. Tags with a *non zero* access password have to receive that value before transitioning to a secure state.
- **EPC**: This block contains the Protocol Control (PC) bits and the 96-bit identification code (denoted as EPC) that identifies the tag. This memory block also contain a CRC-16 (defined in ISO/IEC 13,239) checksum of the PC and EPC codes.
- **TID**: This area of memory shall contain an 8-bit ISO/IEC 15,693 class identifier. Moreover, sufficient information to identify the custom commands and optional features supported by the tag is also specified in this memory block.
- **User**: This memory block is not mandatory thus, the block size is not specified in the standard. Instead, the User memory is factory-configured depending on the manufacturer.

Table 2. EPC Gen2 tag's memory logic map

User:	Optional
TID:	TID [15:0] TID [31:16]
EPC:	XPC_W1 [15:0] EPC [15:0] ⋮ EPC [95:79] PC [15:0] CRC [15:0]
Reserved:	Access Password [15:0] Access Password [31:16] Kill Password [15:0] Kill Password [31:16]

2.2 Communication Protocol and Processes

EPC Gen2 tags do not have a power source. Instead, tags are passively powered following a very basic protocol. Tags can only respond after a message is sent by the reader. Regarding the physical layer, the reader powers up the tag by transmitting a radio frequency (RF) continuous wave to the tag, and the tag backscatters a signal to the reader using the modulation of the reflection coefficient of its antenna. RFID passive tags are powered through the electromagnetic waves received from the interrogator.

Only a small fraction of the power emitted by the interrogator is received by the RFID tag antenna, inducing a voltage to the RFID tag IC. The European Telecommunications Standards Institute (ETSI) regulates the RF spectrum for the European region. It allows for the RFID UHF communication a maximum transmission power of 2 W from EPC Gen2 readers. According to the *Friis transmission equation* (cf. Equation 1) [13], the signal power received by an RFID tag IC depends on the power signal from the reader, the gain of the antennas of both tag and reader and the inverse of the free-space path loss (FSPL) equation.

$$P_{RX,tag} = P_{TX,reader} G_{reader} G_{tag} \left(\frac{\lambda}{4\pi d} \right)^2 \tag{1}$$

The FSPL for the UHF frequency, which in Equation 1 is represented by its wavelength (λ), decline quadratically (order of magnitude) with the distance (d) to the interrogator antenna. The communication distance d for the RFID tags depends on the factors included in Equation 1 and it is usually considered of about five meters, i.e., the maximum distance where the signal power is sufficient to activate the tag IC. Figure 1 shows the approximated tag received power curve depending on the distance between reader and tag. This distance is considered in ideal conditions but, on real RF environments, there are mitigation factors reducing such distance. Signal reflection, absorbing materials or inadequate antenna orientation are possible factors for reducing the communication distance. The communication is half-duplex. Simultaneous transmission and reception is not allowed.

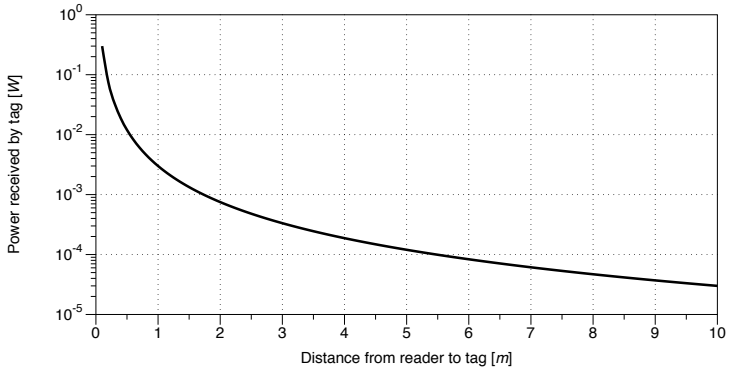

Fig. 1. At five meters, an EPC Gen2 tag receives around 100 μW from the reader

The communication between reader and tags in the EPC Gen2 protocol is organized in reader stages and tag states. Next, the three reader stages are described (cf. Figure 2):

– **Select**: In this stage, the reader selects a subset of the tag population in the communication range for inventory and access using one or more *Select* commands.

– **Inventory**: The process by which a reader identifies tags. An inventory round is initialized by the reader sending *Query* commands. One or more tags may reply, thus, the tags use an anti-collision protocol to avoid collisions [5]. After *selection* the tag loads a random slot counter between *zero* and $2^Q - 1$ (with $0 \leq Q \leq 15$, automatically adjusted or user-defined) decreasing one unit for each *Query* command reception. When the counter reaches the value *zero*, the tag initiates the reply. If the reader detects a single tag reply, it requests the identification from the tag. Figure 3 shows an example of a reader inventorying a single tag.
– **Access**: The process by which a reader modifies or reads individual tags' memory areas. This stage can only be initiated after a successful inventory process.

The following paragraphs describe each of the possible tag states (cf. Figure 4):

– **Ready**: After being energized, a tag enters in the *ready* state. The tag shall remain in this *ready* state until it receives a *Query* command. Tag loads a Q-bit number from its pseudorandom number generator, and transitions to the *arbitrate* state if the number is *non-zero*, or to the *reply* state if the number is *zero*.
– **Arbitrate**: A tag in an *arbitrate* state shall decrement its slot counter every time it receives a *QueryRep*, transitioning to the *reply* state and backscattering a 16-bit identifier (hereinafter denoted as RN16) when its slot counter reaches *zero*.
– **Reply**: A tag shall backscatter a RN16, once entering in the *reply* state.
– **Acknowledged**: If a tag in the *reply* state receives a valid acknowledge (*Ack*), it shall transition to the *acknowledge* state, backscattering its PC, EPC, and CRC-16. Otherwise, the tag returns to the *arbitrate* state.
– **Open**: After receiving a *Req_RN* command, a tag in the *acknowledge* state whose access password is *non-zero* shall transition to the *open* state. The tag backscatters a new RN16 that both reader and tag shall use in subsequent messages. Tags in an *open* state can execute all access commands except *Lock* and may transition to any state except *acknowledge*.

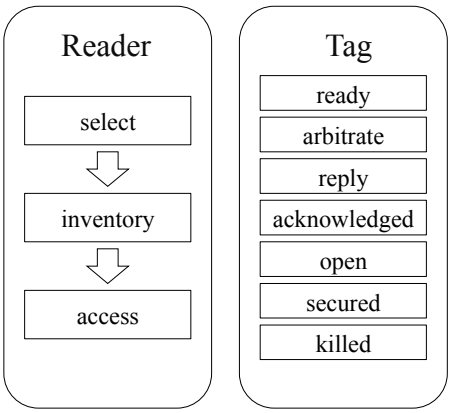

Fig. 2. Reader stages and tag states for the EPC Gen2 protocol

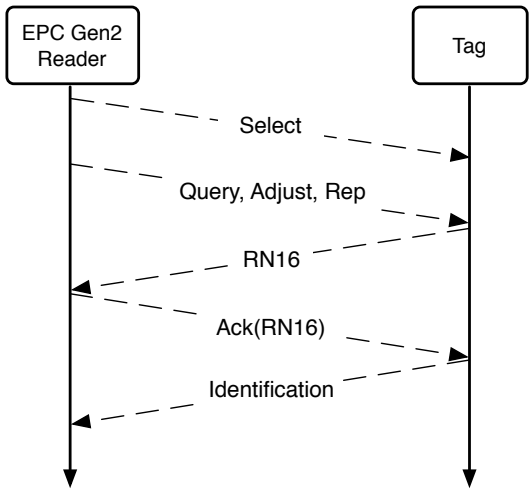

Fig. 3. Example of *Select* and *Inventory* process

- **Secured**: A tag in the *acknowledge* state, and holding an access password with *zero* value, shall transition to the *secured* state, upon receiving a *Req_RN* command. The tag backscatters a new RN16 that both reader and tag shall use in future messages. A tag in the *open* state, with an access password different to the *zero* value, shall transition to a *secured* state, after receiving a valid access command. It should include the same *handle* that was previously backscattered when the tag transitioned from the *acknowledge* state to the *open* state. Tags in the *secured* state can execute all access commands and may transition to any state except the *open* or *acknowledge* state.
- **Killed**: Once a *kill* password is received by a tag in either the *open* state or the *secured* state, it shall enter the *killed* state. *Kill* permanently disables a tag. A tag shall notify the reader that the killed operation was successful, and shall not respond to any further interrogation thereafter.

3 Classification of Threats

As many other communication systems, the RFID level of the EPC Gen2 standard can be affected by threats concerning the security of the information managed by the system, and the privacy of users holding tagged objects. For this reason, it is important to determine the nature of these threats and identify the possible adversaries, to be able to analyze the security measures to adopt and under which circumstances shall be implemented. Threats targetting the security and privacy of the transmitted information in an EPC Gen2 system, are specified by the tagged object intrinsic value, or the derived value from the correlation of the tag identification with the user being identified [14].

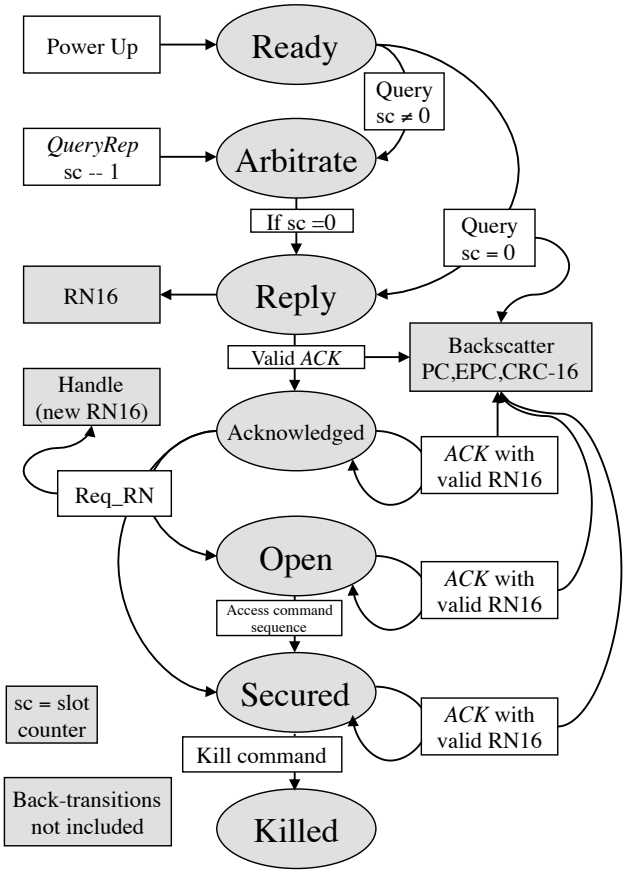

Fig. 4. EPC Gen2 tag state diagram extracted from [5]

3.1 Adversary Model and General Definitions

Prior to listing the threats, we provide some necessary definitions, such as communication parameters and expected adversary powers. We also define the abilities and goals for both parties. We start by listing the set of entities assumed in our system scenarios, and their main parameters.

- *Authorized reader*: A reader registered in the system, being able to access the tag restricted memory contents. We assume that an authorized reader can read and write in the tags.
- *Legitimate tag*: A tag registered in the information systems (IS), previously identified by an authorized reader.
- *Non authorized reader*: A reader not registered in the IS, but having access to the EPC Gen2 communication range.
- *Illegitimate tag*: Fraudulent tag accessing the EPC Gen2 system communication range. For example, a cloned tag is an illegitimate tag identification copied from a legitimate tag.

We define now some of the channel properties. We recall that in any EPC Gen2 setup, the identification tags are energized from the output power of the reader through radio-frequency waves. The communication channels are defined next, paying attention at possible security issues:

- *Reader-tag channel*: Communication from reader to tag. To achieve the maximum communication distance of ten meters, transmission from reader is performed at a higher power (2 - 4W) compared with the tag transmission ($\approx 10^{-4}$W). Because of this, the reader-tag channel can be eavesdropped from hundreds of meters from the transmission point [3]. The EPC Gen2 communications protocol solves this issue giving the option to encrypt the information sent from reader to tag with a one-time-pad cover coding technique.
- *Tag-reader channel*: Communication from tag to reader. Since the tag performance is powered by the reader backscattered power signal, the on-board computation resources are scarce. In fact, the tag-reader channel is mainly used, besides the tag identification, for reader commands acknowledgment and the transmission of the pseudorandom number generated nonces used to encrypt the reader-tag communication. In this sense, the weak tag-reader channel is used to exchange the ciphering keystream between reader and tag. Hence, all the information transmitted by the tag is in plaintext.

We have seen in Section 2 that the EPC Gen2 standard defines three basic stages for the communication between readers and tags: select, inventory and access, and a number of possible tag states for each communication stage. Select and inventory stages are related to the tag identification process, which is the basic functionality of the system. If the tag memory content has to be modified, then the Access Stage is necessary. The two basic interaction models between tag and reader are described next.

- *Identification*: To identify a tag, an EPC Gen2 reader uses two different stages. First the reader selects all the available tags in the communication vicinity in the stage

known as Selection. To perform the identification of individual tags, the reader starts the Inventorying processes sending query commands to the selected tags (legitimate or illegitimate, due to the absence of authentication processes at this stage). The tags respond sequentially by using an anti-collision technique, sending its identifier in plaintext. At this point, the identification process is finished.
- *Access*: Once the tag has been identified, a reader (authorized or non authorized) activates the process to access the tag memory content to read or write in it. Access queries to an EPC Gen2 tag memory are: read, lock, blockwrite, blockerase and block permalock. Access queries with the one-time-pad encryption mechanism are: write, kill and access [5].

We move now to define some of the parameters related to the adversary entities. For the EPC Gen2 system adversary model, a larger distance between tags and readers than the tag-reader communication range is assumed (unless the contrary is specified). The reason to prioritize the threats over the tag-reader channel is due to the chance of eavesdropping the information of the reader-tag channel from hundreds of meters away by using a compatible EPC Gen2 equipment. The following list of related definitions are based on [15].

- *Attack*: Attempt to gain unauthorized access to a service, resource, or information; or the attempt to compromise the integrity, availability, or confidentiality. Note that success is not necessary.
- *Attacker, intruder or adversary*: Originator of an attack.
- *Vulnerability*: Weakness in the system security design, implementation, configuration or limitations that could be exploited.
- *Threat*: Any circumstance or event (such as the existence of an attacker and vulnerabilities) with the potential to adversely impact a system through a security breach.
- *Risk*: Probability that an attacker will exploit a particular vulnerability, causing harm to a system asset.
- *Passive adversary*: Is the entity trying to exploit a vulnerability inside the system to execute the threat [16]. It is limited to eavesdrop information in the communication range without leaving presence evidences in the system.
- *Active adversary*: Like the passive adversary, but able to transmit and receive information in the communication range. In the case of being placed in the tag-reader communication range, an active adversary is able to modify the tag memory content.

We move now to provide some basic weaknesses related to the wireless communication channel, and the lack of security measures for the information exchange between readers and tags. Although the reader-tag communication can be encrypted, the encryption keys are sent as plaintext data over the tag-reader channel. This fact leads to a vulnerability being susceptible to be attacked by an adversary.

For example, the use of pseudorandom number generators with poor statistical properties, or a certain degree of predictability, may suppose a serious risk in the communication confidentiality. A non authorized reader may access the reader-tag channel of authorized readers and legitimate tags, and analyze the generated pseudorandom

sequences predictability in an Access Stage. If the adversary is able to decrypt the pseudorandom generation mechanism, a simple bitwise XOR operation between the eavesdropped and the predicted sequences will be enough to reveal the message. In that way, a non authorized reader in the reader-tag channel range may get access to the tag reserved memory areas, e.g., the kill and access passwords.

The next step in order to analyze the security of EPC Gen2 systems is to classify the main threats an adversary can take advantage. These threats are the consequence of the three basic vulnerabilities that can be pointed out when analyzing an EPC Gen2 system:

- The EPC Gen2 communication channel is weakly protected.
- Any EPC Gen2 compatible reader can obtain information from the tags in the communication channel.
- The tag design is optimized to reduce its cost. The tag capacity is very reduced and lacks of reliable authentication and security mechanisms.

The remainder of this section describes some important threats to the EPC Gen2 system security, with the corresponding vulnerability to be exploited by an adversary. The threats are grouped with regard to the targeted properties. First, we present some threats targeting confidentiality and privacy properties. Second, threats targeting integrity properties. Finally, threats tageting availability. A more detailed and methodological analysis of the threats is available in [16].

3.2 Eavesdropping, Rogue Scanning and Privacy Threats

In any passive RFID system, the reader provides a strong power signal to energize the tags. In the EPC Gen2 technology, this fact has a major relevance, since the tags may reply from larger distances. Illegitimate collection of traffic might be slightly protected by reducing the transmission power or by sheltering the area. It is, although, theoretically possible to conduct eavesdropping attacks. Two main types of eavesdropping are possible: (1) forward eavesdropping and (2) backward eavesdropping. Forward eavesdropping often refers to the passive collection of queries and commands sent from readers to tags, e.g., collection of queries and acknowledgments (cf. Steps 1 and 3) depicted in Figure 5. Backward eavesdropping refers to the passive collection of responses sent from tags to readers, e.g., collection of control sequences and identifiers (cf. Steps 2 and 4) depicted in Figure 5. Most authors consider that the range for backward eavesdropping could be only of a few meters [17], and probably irrelevant for a real eavesdropping attack. However, the distance at which an attacker can eavesdrop the signal of an EPC reader can be much longer. In ideal conditions, for example, readers configured to transmit at maximum output power, the signal could be received from tens of kilometers away. Analysis attacks inferring sensitive information from forward eavesdropping, for example, analysis of the pseudorandom sequences generated by the tags, are hence possible. See, for instance, results published in [18, 19], about practical eavesdropping of control data from EPC Gen2 queries with programmable toolkits, and the analysis of the obtained sequences to derive statistical artifacts of the tag components (e.g., their pseudorandom number generators).

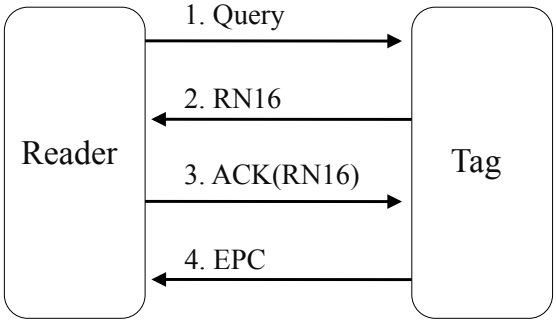

Fig. 5. Inventory protocol of an EPC Gen2 tag

Moreover, we have already observed in previous sections that any compatible Gen2 reader can access the EPC tags, and request their information. These operations are not properly authenticated. Therefore, it is also possible the unauthorized presence of readers in the reader-tag channel with the goal of performing fraudulent scanning of tags, i.e., performing rogue scanning attacks [17]. Although the distance at which an attacker can perform a rogue scanning is considerably shorter than the distance for eavesdropping the reader queries, the use of special hardware (e.g., highly sensitive receivers and high gain antennas) could enable rogue scanning attacks at larger distances. This clearly affects to the confidentiality of the transmitted data, which becomes highly vulnerable. Indeed, the rogue scanning threat is specially relevant because the identification code of an EPC Gen2 may reveal sensible information such as the brand, model or product cost of the tagged object. Also the production or distribution strategies from a company can be obtained. In that way the adversary may obtain an economic benefit from selling this information for industrial espionage reasons [20].

Observe that the lack of a strong authentication process in the EPC Gen2 technology has serious consequences to the privacy of tagged object bearers. The unauthorized interrogations of EPC Gen2 tags shall give attackers unique opportunities for the collection of personal information (and without the consent of the bearer). This can also lead location tracking or surveillance of the object bearers. An attacker can distinguish any given tag by just taking into account the EPC number. Therefore, when the tags are used to identify people or wearable objects (like clothes), threats to the privacy shall be considered and properly handled [4].

3.3 Tampering, Spoofing and Counterfeiting Concerns

EPC Gen2 tags are required to be writable [21]. To protect the tags from unauthorized activation of the writing process, tags implement an on-board access control routine, based on the use of 32-bit passwords. Other integrity actions, such as the self-destruction routine of EPC Gen2 tags, are also protected by 32-bit passwords. Via the

access control routine, it is possible to permanently lock or disable this harmful operation. In fact, tags are often locked by default in most of today's EPC applications, and must be unlocked by legitimate readers. Forward eavesdropping can be used by passive adversaries in order to deriving and unlocking such process [18]. Other techniques to retrieve the passwords have also been reported in the literature. For example, in [22] the authors present a mechanism to retrieve passwords by simply analyzing the radio signals sent from readers to tags. Although the proof-of-concept implementation of this technique is only available for Gen1 tags [21], the authors state that Gen2 tags are equally vulnerable.

The aforementioned attacks enabled by retrieving the passwords, that protect the writing of EPC Gen2 tags, can also be used to obtain the legitimate tag identification. This information can be reproduced on illegitimate tags, for example by means of skimming attacks [23]. If the *tag-reader* communication channel can be reached, a non authorized reader may perform active attacks like replay or scanning to obtain the information directly from the tags. Similarly, and once bypassed the password-driven routines, an EPC Gen2 authorized reader is not able to distinguish an illegitimate tag from a legitimate one. This vulnerability of the EPC Gen2 system represents a threat known as counterfeiting, since the memory of a tag can be easily modified or reproduced in the tag memory of a falsified product, what would turn into a tag cloning operation. At the same time, in a personal access system based on the EPC Gen2 technology, the identity of a person can be impersonated cloning its tag to an illegitimate one, receiving the access privileges from the impersonated person. In the context of a pharmaceutical supply chain, corrupting data in the memory of EPC tags can also be dangerous: the supply of medicines with wrong information, or delivered to the wrong patients, can lead to situations where a sick person could take the wrong drugs.

3.4 Denial of Service and related Availability Concerns

The aim of denial of service (DoS) threats is to restrict or reduce the availability of an information system. Regarding an EPC Gen2 system, a DoS implies leaving inoperative the communication channel (either reader-to-tag or tag-to-reader channels) by making non-viable the exchange of information.

A DoS can be done in different ways. For example, taking as a reference the model introduced in Section 2, a radio-frequency transmitter generating noise (jamming attack) between the 865 and 868 MHz frequencies in the reader-tag channel, fills all the EPC Gen2 wireless channels avoiding authorized readers to identify the tags placed in the communication area. Even with a non-authorized reader in the reader-tag channel constantly performing identification queries, that will considerably reduce the reading efficiency of the authorized readers, delaying the system's inventorying process. In additon, the aforementioned attacks to the integrity of the tags (cf. Section 3.3), i.e., enabled by retrieving the tag passwords, can be used to destroy the data stored on-board of the tags, or simply to the destroy the tag itsefl [24]. Tag information can also be destroyed by devices that send strong electromagnetic pulses. Devices, such as the RFID-zapper [25], have been presented in the literature with such purpose. Similar effects can be obtained via de-synchronization of flawed RFID protocols [3]. Such techniques aim at misusing to the logic of the high-level protocols, rather than the on-board security

primitives. Most cases show the lack of formality during the verification phase of new security techniques for low-cost RFID technologies, and can benefit from the use of formal verification [26].

4 Sample Countermeasures to Handle the Threats

EPC Gen2 security tools included in the standard [5] are basically an access password to protect certain areas of the tag memory, and pseudorandom nonces to cipher specific access commands. Additionally, low-cost RFID security related literature, brings security improvement solutions by modifying the communication protocols or the chip capabilities of the EPC Gen2 standard. In the sequel, we survey some of these solutions. First, we outline a summary of some representative research efforts conducted during the ARES project to handle those issues reported in Section 3. Then, we conclude with some other countermeasures proposed in the literature that we consider relevant as future directions for research.

4.1 Efforts Conducted within the Scope of the ARES Project

During the ARES project, several improvements to the security of EPC Gen2 tag primitives and protocols were proposed. We survey some of the contribution in this section. We classify the contributions in three main lines (lightweight authentication, security primitives improvement on tags, and secure RFID protocols), according to the types of threats they intend to address.

Lightweight Authentication: In a first phase, some efforts were made to handle the lack of authentication behind the eavesdroping and rogue scanning threats, while minimizing the execution of on-tag cryptographic operations. Algorithmic solutions based on secret-sharing schemes, such as those presented in [27–29] were studied and extended. The main idea is to assume that distributed secrets have been used to encrypt the EPC identifiers of a series of RFID tags. The necessary cryptographic material is split in multiple shares and distributed among multiple tags. In order to obtain the identifier of an RFID tag, a reader must collect a minimum number of shares distributed among some other RFID tags. Authentication is therefore achieved though the dispersion of secrets. The dispersion helps to improve the authentication process between readers and tags, as tags move through a supply chain. Assuming that a given number of shares is necessary for readers to obtain, e.g., the EPCs assigned to a pallet, a situation where the number of shares obtained by readers is not sufficient to reach the threshold protects the tags from unauthorized scanning (i.e., unauthorized readers that cannot obtain the sufficient number of shares cannot obtain the EPCs either). The approach can be implemented on EPC Gen2 tags without requiring any change to the current tag specification. An important problem is that privacy concerns, such as location tracking, are not addressed in the solutions reported in [27–29]. Indeed, the shares used in those approaches are static and can be misused to identify object bearers. This limitation is addressed in [30]. The extended solution relies on the use of a proactive

anonymous threshold secret sharing scheme. It allows the exchange of blinded information and anonymous self-renewal of shares with secret preservation between asynchronous shareholders, with the aim of mitigating eavesdropping, rogue scanning, and tracking threats. Readers aiming at obtaining an appropriate share to unlock a tag are provided with a different new identifier per query. The solution provides the necessary guarantees to avoid linkability attacks.

Security Primitives Improvement on Tags: In a second phase, a series of contributions to reinforce security primitives on-board of EPC Gen2 tags were presented. Such contributions aim at addressing situations in which EPC Gen2 primitives, such as pseudorandom number generators and password-protected operations, are misused to put in place integrity and availability threats (e.g., tampering, spoofing, DoS and other similar threats). The key idea is the following. If an adversary, eavesdropping previous communications from a legitimate reader, discovers flawed generation of EPC Gen2 control sequences (i.e., pseudorandom number sequences generated by the on-board generators of the tags), then he can analyze the sequences to retrieve, e.g., passwords. Assume, for instance, the protocol description depicted in Figure 6. It presents a simplified description of the protocol steps for requesting and accessing the writing process that modifies the memory of a Gen2 tag. We assume that a select operation has been completed, in order to single out a specific tag from the population of tags. It is also assumed that an inventory query has been completed and that the reader has a valid 16-bit identifier (denoted as RN16 in Figure 5, Steps 2 and 3) to communicate and request further operations from the tag. Using this random sequence (cf. Figure 6, Step 5), the reader requests a new descriptor (denoted as Handle in the following steps). This descriptor is a new random sequence of 16 bits that is used by the reader and tag. Indeed, any command requested by the reader must include this random sequence as a parameter in the command. All the acknowledgments sent by the tag to the reader must also include this random sequence.

Once the reader obtains the Handle descriptor in Step 6, it acknowledges by sending it back to the tag as a parameter of its query (cf. Step 7). To request the execution of the writing process, the reader needs first to be granted access by supplying the 32-bit password that protects the writing routine. This password is actually composed of two 16-bit sequences, denoted in Figure 6 as $\text{PIN}_{31:16}$ and $\text{PIN}_{15:0}$. To protect the communication of the password, the reader obtains in Steps 8 and 12, two random sequences of 16 bits, denoted in as RN16' and RN16". These two random sequences RN16' and RN16" are used by the reader to blind the communication of the password toward the tag. In Step 9, the reader blinds the first 16 bits of the password by applying an XOR operation (denoted by the symbol $\oplus$ in Figure 6) with the sequence RN16'. It sends the result to the tag, which acknowledges the reception in Step 10. Similarly, the reader blinds the remaining 16 bits of the password by applying an XOR operation with the sequence RN16", and sends the result to the tag in Step 13. The tag acknowledges the reception in Step 14 by sending a new Handle to the reader. By using the latter, the reader requests the writing operation in Step 15, which is executed and acknowledged

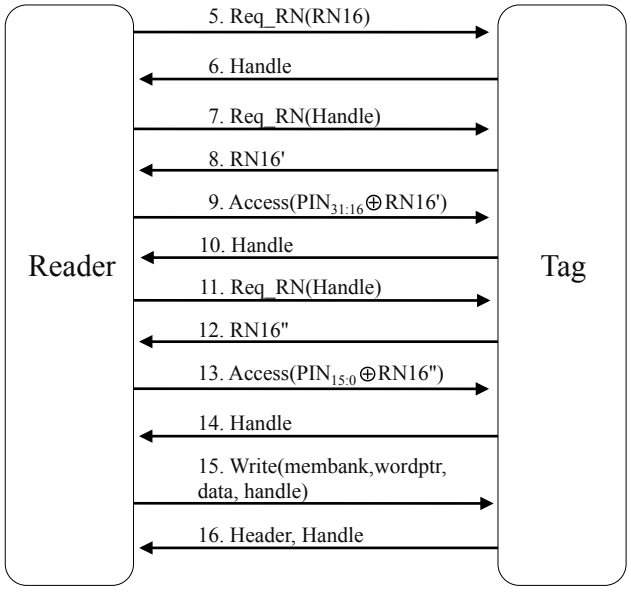

Fig. 6. Writing protocol of an EPC Gen2 tag

by the tag in Step 16. Notice that an attacker can find the 32-bit password that protects the writing routine. It suffices to intercept sequences RN16' and RN16", in Steps 8 and 12, and to apply the XOR operation to the contents of Steps 9 and 13.

In [31, 32], it was reported a flawed 16-bit pseudorandom number generator design presenting the aforementioned vulnerability. The design, based on linear feedback shift registers (LFSR) for the generation of EPC Gen2 pseudorandom sequences was presented in [33, 34]. It was demonstrated that the proposal is not appropriate for security purposes, since it does not correctly handle the inherent linearity of LFSRs. A new scheme to handle the discovered vulnerability was presented in [35, 36]. The new pseudorandom number generator design, named J3Gen, still based on the use of LFSRs, relies on a multiple-polynomial tap architecture fed by a physical source of randomness. It achieves a reduced computational complexity and low-power consumption as required by the EPC Gen2 standard. It is intended for security, addressing the one-time-pad cipher unpredictability principle. J3Gen is configurable for other purposes and scenarios besides EPC Gen2 RFID technologies through two main parameters: LFSR size and number of polynomials. Its hardware complexity was studied, as well as its randomness requirements, via a statistical analysis and the power consumption through an evaluation based on CMOS parameters and SPICE language simulation.

Secure RFID Protocols: In a third phase, it was finally tackled the problem of flawed designs on protocols that aim at establishing some security properties on RFID environments. Security RFID protocols reported in the literature are often error-prone. A great number of protocols surveyed in [3] were reported insecure shortly after their publication. These cases show the lack of formality during the verification phase of new security techniques for low-cost RFID technologies. In [37], we deepened on this problem and illustrated how a sample protocol for the EPC Gen2 RFID technology shall be formally specified with regard to its security requirements. We defined a sample key establishment protocol, and formally verified its conformity to security properties such as authenticity and secrecy. The verification process was conducted by using the AVISPA/AVANTSSAR model checker frameworks [38, 39]. The goal was to illustrate the appropriate way of ensuring the achievement of security requirements when specifying a security protocol for the EPC technology, e.g., confidentiality properties, integrity properties, and availability properties. The proposed protocol was formally proven to achieve secure data exchange between tags and readers, based on a key generation model adapted to Gen2 RFID tags. Similar techniques could also be used to verify, as well, reader and tag primitives. Verification frameworks able to quantify weaknesses of security protocols with regard to dictionary and guessing attacks might also help to enhance the validity of new security primitives. Some existing work in the literature on formal verification methods, such as [40–42], seem to head in this direction.

4.2 Complementary Research Directions

We conclude this section with a quick overview of complementary countermeasures that we consider relevant as future directions for research.

The first direction relies on pursuing measures based on identifier relabeling [3, 43, 44]. In a nutshell, these measures take advantage of the writable nature of EPC Gen2 tags, in order to avoid the *eavesdropping* and *spoofing* threats. Both relabeling and indetifier (hereinafter denoted as ID) encryption respond to the same idea: to link in a secured database the real tag ID and a pseudo ID that can be a simple pseudonym or an encryption of the valid ID. Once the pseudonym is computed, it is written in the tag ID memory. Both pseudonym and real ID are stored in a secured database to be accessible by the system. This measure does not solve a possible counterfeiting attack to, e.g., an end-user EPC Gen2 application or any other context where tags cannot be rewritten. *DoS* is not solved by this measure, either, since tags loose their performance properties.

It could also be interesting to study physical protection of tags. Solutions such as the shielding of tags (e.g., by using a metallic bag) is proposed in [45] to avoid the activation of the tag response. Also printing on tagged objects the identifier codified in, e.g. a barcode as proposed in [46], can be understood as a backup of the legitimate identifiers, avoiding possible *spoofing* or *counterfeiting* threats, as well as *DoS*. Physical solutions could be an appropriate complement to the use of message authentication codes (MAC). The goal is to improve the integrity of the information stored in the tag. For instance, assuming a 96-bit identifier, we can use 50 bits to manage the tag ID in an EPC Gen2 application chain, and the remaining 46 bits can still be used to protect the main ID content, so to detect possible *counterfeiting* threats. The use of a *hash* function

with a key k (only known by a given trusted party) can be a useful option to obtain the authentication code. This way, the final ID (96 bits) would be the result of concatenating the original ID, with the result of applying a *hash* function with key k to the *XOR* sum of k and ID_{50bits}:

$$ID_{96bits} = ID_{50bits} | H_k(ID_{50bits} \oplus k)_{46bits}$$

The operation can be done by the readers or backend servers of an EPC Gen2 application, and the result stored in the tag ID memory. Naturally, *brute force attacks* can eventually reveal the stored key. However, using an appropriate diversity of keys can improve the data integrity of most practical systems.

Some research efforts are also necessary in the field of trust, e.g., efforts with regard to trust properties of the system setups. Following the Trusted Tag Relation defined in [47], a tag is validated by an authorized party by scanning the tagged element (e.g., by reading a tagged letter with a hand-held RFID reader connected to a back-end system). Once scanned, a status flag is marked as *valid*. The following operations in the chain of Gen2 elements would simply trust on the information provided by the scanned tag only if the step-before has been validated. This measure helps to identify more easily *counterfeiting* actions. However, it is not suitable for *eavesdropping* or *spoofing* actions because the tag is not modified in all the process. It does not handle either the *DoS* threat, since readers would probably stop working correctly. Some improvements on the Trusted Tag Relation method have been presented in [48] and [49], based on a probabilistic identification protocol using collaborative readers.

5 Conclusion

EPC Gen2 systems represent one of the most pervasive technologies in the ICT field. The main feature of the EPC Gen2 technology is the tag reduced price (predicted to be under 10 US dollar cents) which means a compromise between cost and functionality. If moreover the communication between tags and readers is made in a potentially insecure channel, and that any compatible reader can access the communication between tags and readers in its communication range, the EPC Gen2 system communication has the risk of attacks on the security of the communications and the privacy of those individuals holding tagged object.

This chapter has surveyed the main characteristics of the EPC Gen2 technology and presented some of the threats and concerns reported in the related literature. It has also outlined a summary of some representative research efforts conducted during the ARES project to handle those reported theats. Particular emphasis has been made on the uniqueness of the EPC Gen2 system communications model, that only provides very basic measures for protecting the content transmitted in the reader-tag channel. The main results of this research were presented in [20, 30–32, 16, 12, 35–37, 18, 19, 50–56]. Finally, some other interesting countermeasures proposed in the literature have also been outlined. Measures such as ID relabeling or encryption can be applied in some cases due to the uniqueness of the EPC Gen2 characteristics and related applications, e.g., medical applications, to protect privacy properties.

References

1. L. Buttyan and J. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2007, available at http://secowinet.epfl.ch/.
2. D. C. Ranasinghe and P. H. Cole, *Networked RFID Systems and Lightweight Cryptography, Chapter 3*. Springer, Nov. 2008, ch. Networked RFID Systems, pp. 45–58.
3. A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 2, pp. 381–394, Feb. 2006.
4. S. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security & Privacy IEEE*, vol. 3, no. 3, pp. 34–43, jun. 2005.
5. *EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID , Specification for RFID Air Interface, Protocol for Communications at 860 MHz – 960 MHz, Version 2.0.0 Ratified*, EPCglobal, 2013.
6. EPCglobal, "The EPCglobal Website," [On-line], Last Access 2014, available at: http://www.epcglobalinc.org/.
7. Motorola, "RFID technology and EPC in retail," Whithe Papers, [On-line], Last Access 2014. [Online]. Available: http://www.motorola.com/rfid/
8. M. Potdar, E. Chang, and V. Potdar, "Applications of RFID in pharmaceutical industry," *Industrial Technology (ICIT), IEEE International Conference on*, pp. 2860–2865, Dec. 2006.
9. RFID Journal, "Wal-Mart Opts for EPC Class 1 V2," Tech. Rep., [On-line], Last Access 2014, Available at http://www.rfidjournal.com/article/articleprint/641/1/1/.
10. S. Sarma, "Toward the 5 cents tag," Auto-ID Lab, Tech. Rep., Nov. 2001, Withe Paper.
11. D. C. Ranasinghe and P. H. Cole, *Networked RFID Systems and Lightweight Cryptography, Chapter 8*. Springer, Nov. 2008, ch. An Evaluation Framework, pp. 157–167.
12. J. Melià-Seguí, "Lightweight PRNG for low-cost passive RFID security improvement," Ph.D. dissertation, Universitat Oberta de Catalunya, 2011.
13. D. Pozar, *Microwave Engineering*, 2nd ed. Wiley, 1998.
14. G. Avoine, "Adversarial model for radio frequency identification," Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC, Tech. Rep., 2005.
15. Committee on National Security Systems (CNSS), "National information assurance glossary," NSTISSI, Tech. Rep. 4009, May 2003.
16. J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Auerbach Publications, Taylor & Francis Group, October 2010, ch. Chapter 3, Handling Security Threats to the RFID System of EPC Networks, pp. 45–64.
17. D. C. Ranasinghe, *Networked RFID Systems and Lightweight Cryptography, Chapter 18*. Springer, Nov. 2007, ch. Lightweight Cryptography for Low Cost RFID, pp. 311–344.
18. J. Garcia-Alfaro, J. Herrera-Joancomarti, and J. Melia-Segui, "Practical Eavesdropping of Control Data From EPC Gen2 Queries With a Programmable RFID Toolkit," *Hakin9*, vol. 6, no. 9, pp. 14–19, September 2011.
19. J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomarti, "On the Similarity of Commercial EPC Gen2 Pseudorandom Number Generators," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 2, pp. 151–154, February 2014.
20. J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "Analysis of threats to the security of EPC networks," *Sixth Annual Communication Networks and Services Research (CNSR) Conference, Hlifax, Nova Scotia, Canada*, may. 2008.
21. EPCglobal, "The EPCglobal architecture framework," Tech. Rep., 2007. [Online]. Available: http://www.epcglobalinc.org/standards/
22. Y. Oren, "Remote power analysis of RFID tags," Cryptology ePrint Archive, Report 2007/330, IACR, 2007.

23. G. P. Hancke, "Practical eavesdropping and skimming attacks on high-frequency rfid tokens," *Journal of Computer Security*, vol. 19, no. 2, pp. 259–288, 2011.
24. D. Han, T. Takagi, H. Kim, and K. Chung, "New Security Problem in RFID Systems Tag Killing," in *Computational Science and its Applications (ICCSA 2006)*, ser. Lecture Notes in Computer Science, vol. 3982. Springer, 2006, pp. 375–384.
25. J. Collins, "RFID-Zapper shoots to kill" in *RFID Journal* (2006), [On-line], Last Access 2014, Available at http://www.rfidjournal.com/articles/view?2098.
26. R. M. Keller, "Formal verification of parallel programs," *Communications of the ACM*, vol. 19, no. 7, pp. 371–384, 1976.
27. M. Langheinrich and R. Marti, "Practical minimalist cryptography for RFID privacy," *Systems Journal, IEEE*, vol. 1, no. 2, pp. 115–128, 2007.
28. ——, "RFID privacy using spatially distributed shared secrets," in *Ubiquitous Computing Systems*. Springer, 2007, pp. 1–16.
29. A. Juels, R. Pappu, and B. Parno, "Unidirectional key distribution across time and space with applications to rfid security," in *SS'08: Proceedings of the 17th conference on Security symposium*. Berkeley, CA, USA: USENIX Association, 2008, pp. 75–90.
30. J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "Proactive Threshold Cryptosystem for EPC Tags," *Ad Hoc & Sensor Wireless Networks*, vol. 12, no. 3-4, pp. 187–208, 2011.
31. J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomarti, "Analysis and Improvement of a Pseudorandom Number Generator for EPC Gen2 Tags," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, R. S. et al., Ed. Springer, 2010, vol. 6054, pp. 34–46.
32. J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomartí, "A Practical Implementation Attack on Weak Pseudorandom Number Generator Designs for EPC Gen2 Tags," *Wireless Personal Communications*, vol. 59, pp. 27–42, July 2011, dOI: 10.1007/s11277-010-0187-1.
33. W. Che, H.Deng, X. Tan, and J. Wang, *Networked RFID Systems and Lightweight Cryptography, Chapter 16*. Springer, Nov. 2008, ch. A Random Number Generator for Application in RFID Tags, pp. 279–287.
34. W. Chen, W. Che, N. Yan, X. Tan, and H. Min, "Ultra-Low Power Truly Random Number Generator for RFID Tag," *Wireless Personal Communications,*, vol. 59, no. 1, pp. 85–94, 2011, DOI: 10.1007/s11277-010-0191-5.
35. J. Melià-Seguí, J. Garcia-Alfaro, and J. Herrera-Joancomartí, "Multiple-polynomial LFSR based pseudorandom number generator for EPC Gen2 RFID tags," in *IECON - 37th Annual Conference on IEEE Industrial Electronics Society*, Nov. 2011, pp. 3820 – 3825.
36. ——, "J3Gen: A PRNG for low-cost passive RFID," *Sensors,*, vol. 13, no. 3, pp. 3816–383, 2013, DOI: 10.3390/s130303816.
37. W. Tounsi, N. Cuppens-Boulahia, J. Garcia-Alfaro, Y. Chevalier, and F. Cuppens, "KED-GEN2: A key establishment and derivation protocol for EPC Gen2 RFID systems," *Journal of Network and Computer Applications*, vol. 39, no. 1, pp. 152–166, 2014.
38. A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. Drielsma, P. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, O. V. Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigano, and L. Vigneron, "The AVISPA tool for the automated validation of internet security protocols and applications," in *17th International Conference on Computer Aided Verification (CAV'05)*. Springer, 2005, pp. 135–165.
39. A. Armando, W. Arsac, T. Avanesov, M. Barletta, A. Calvi, A. Cappai, R. Carbone, Y. Chevalier, L. Compagna, J. Cuellar, G. Erzse, S. Frau, M. Minea, S. Mödersheim, D. Oheimb, G. Pellegrino, S. Ponta, M. Rocchetto, M. Rusinowitch, M. Torabi D., M. Turuani, and L. Vigano, "The AVANTSSAR platform for the automated validation of trust and security of service-oriented architectures," in *18th international conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2012)*. Springer, 2012, pp. 267–282.

40. S. Delaune, "Intruder Deduction Problem in Presence of Guessing Attacks," in *Proceedings of the Workshop on Security Protocols Verification (SPV'03)*, Marseille, France, 2003, pp. 26–30.
41. B. Groza and M. Minea, "A calculus to detect guessing attacks," in *Information Security*. Springer, 2009, pp. 59–67.
42. ——, "Formal modelling and automatic detection of resource exhaustion attacks," in *6th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2011)*. ACM, 2011, pp. 326–333.
43. H. Wong, C. Hui, and C. Chan, "Cryptography and authentication on RFID passive tags for apparel products," *Computers in Industry*, vol. 57, no. 4, pp. 342–349, may. 2006.
44. S. Weis, S. Sarma, and D. Engels, "RFID systems and security and privacy implications," in *Cryptographic Hardware and Embedded Systems – CHES 2002*, ser. LNCS, vol. 2523. Springer-Verlag, aug. 2002, pp. 454–469.
45. P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions," in *11th IFIP International Conference on Personal Wireless Communications*, ser. LNCS, vol. 4217. Springer-Verlag, sep. 2006, pp. 159–170.
46. A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," in *Financial Cryptography – FC'03*, ser. Lecture Notes in Computer Science, R. N. Wright, Ed., vol. 2742, IFCA. Le Gosier, Guadeloupe, French West Indies: Springer, January 2003, pp. 103–121.
47. A. Solanas, J. Domingo-Ferrer, A. Martínez-Ballesté, and V. Daza, "A distributed architecture for scalable private RFID tag identification," *Computer Networks, Elsevier*, vol. 51, no. 9, jan. 2007.
48. R. Trujillo-Rasua and A. Solanas, "Efficient probabilistic communication protocol for the private identification of RFID tags by means of collaborative readers," *Computer Networks*, vol. 55, no. 15, pp. 3211 – 3223, 2011.
49. R. Trujillo-Rasua, A. Solanas, P. A. Pérez-Martínez, and J. Domingo-Ferrer, "Predictive protocol for the scalable identification of RFID tags through collaborative readers," *Computers in Industry*, vol. 63, no. 6, pp. 557 – 573, 2012, Special Issue on Secure Collaboration in Design and Supply Chain Management.
50. J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomarti, "Análisis de Seguridad y Privacidad para Sistemas EPC-RFID en el Sector Postal," in *XI Reunión Española sobre Criptología y Seguridad de la Información, Salamanca - Spain*. Universidad de Salamanca, Sep. 2008.
51. ——, "Clasificación de las Amenazas a la Seguridad en Sistemas RFID-EPC Gen2," in *XII Reunión Española sobre Criptología y Seguridad de la Información, Tarragona - Spain*. Universitat de Tarragona, September 2010.
52. J. Melia-Segui, J. Herrera-Joancomarti, and J. Garcia-Alfaro, "Security and Privacy of Postal RFID Systems," Jan. 2009, RFIDSec Asia, Taipei, Taiwan (ROC).
53. J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomarti, "Clasificación de las Amenazas a la Seguridad en Sistemas RFID - EPC Gen2," in *XII Reunión Española sobre Criptología y Seguridad de la Información, Tarragona - Spain*. Universitat Rovira i Virgili, Sep. 2010.
54. ——, "RFID EPC-Gen2 for postal applications: A security and privacy survey," in *IEEE International Conference on RFID-Technology and Applications (RFID-TA) Guangzhou - China*. IEEE, Jun. 2010, pp. 118–123, 10.1109/RFID-TA.2010.5529872.
55. J. Garcia-Alfaro, J. Herrera-Joancomarti, and J. Melia-Segui, "A Multiple-Polynomial LFSR based Pseudorandom Number Generator Design for EPC Gen2 Systems," Jun. 2010, MITACS Workshop on Network Security & Cryptography, Toronto (Canada).
56. J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "Les composants RFID, sont-ils vulnerables ?" *Techniques de l'ingenieur*, no. 4-5, July/September 2009.