Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 6, 194-202(2017)

www.astesj.com

Special issue on Advancement in Engineering Technology

ASTESJ

ISSN: 2415-6698

Review on security issues in RFID systems

Mohamed El Beqqal*, Mostafa Azizi

University Mohamed first, ESTO, 60000, Morocco

ARTICLEINFO

Article history:
Received: 11 November, 2017
Accepted: 01 December, 2017
Online: 14 December, 2017

Keywords:
RFID System
Classification
Security
Privacy
Countermeasures

ABSTRACT

Radio frequency Identification (RFID) is currently considered as one of the most used technologies for an automatic identification of objects or people. Based on a combination of tags and readers, RFID technology has widely been applied in various areas including supply chain, production and traffic control systems. However, despite of its numerous advantages, the technology brings out many challenges and concerns still not being attracting more and more researchers especially the security and privacy issues. In this paper, we review some of the recent research works using RFID solutions and dealing with security and privacy issues, we define our specific parameters and requirements allowing us to classify for each work which part of the RFID system is being secured, the solutions and the techniques used besides the conformity to RFID standards. Finally, we present briefly a solution that consists of combining RFID with smartcard based biometric to enhance security especially in access control scenarios. Hence the result of our study aims to give a clear vision of available solutions and techniques used to prevent and secure the RFID system from specific threats and attacks.

1. Introduction

This paper is an extension of work originally presented in Wireless Technologies, Embedded and Intelligent Systems (WITS) [1]. It concerns the security in Radio Frequency Identification (RFID) systems. The implementation of this technology in many industrial fields has recently attracted a lot of attention. Due to its important role of identifying people as well as objects, and data tracking, RFID is becoming more and more popular as an important topic of research. In particular, with the emergence of the Internet of things (IoT) paradigm that refers to a kind of networks that links physical objects to the internet to exchange data [2] and where RFID plays a key role. Besides, RFID is considered to be the next generation of barcode technology which is the case in many countries [2]. The use of RFID technology in several domains including supply chain, healthcare, transportation, education and many other fields have significant advantages including the flexible way of deployment with low cost, the possibility of integration and cooperation with Wireless Sensor Network nodes [2]. However, despite its numerous advantages, RFID technology still brings out many challenges including technical problems, customer privacy issues, coexistence of heterogeneous RFID standards [3] and more importantly security and privacy concerns. In fact, an RFID system consists of tags that store the data, readers interacting with the tags and transmitting information to backend servers and finally a network canal that manages this communication [4]. This architecture multiplies the sources of security problems and threats.

Several types of attacks can target the RFID system depending on each part is more vulnerable to the attacker. For example, the modification of the data, Cloning technique, and impersonation can be applied at level tags, whereas the reverse engineering, Eavesdropping Side Channel Attacks can affect the communication between backend servers, readers and tags [5].

In the research field, many of solutions and techniques assuring security and privacy come with processing and cryptographic algorithms such as Elliptic Curve Cryptographic (ECC) technique or mutual authentication mode between all RFID system parts. Most of these techniques remain far from being implemented in practice due to the limited resources of storing in tags and the low capacity of processing and executing complex operations. Furthermore, RFID customers require some guaranties that data contained in tags or exchanged remain private and highly protected against tracking and customer identity reconnaissance. A guarantee must be provided to customers aiming to adopt RFID in their own goals by ensuring that their private data stored in the tags will remain private and protected against spying and tracking

*Corresponding Author: Mohamed El Beqqal, elbeqqal.mohamed@gmail.com

This work presents a clear vision about the concerns of security and privacy in an RFID system. Precisely we compare recent works dealing with security and privacy in an RFID system according to which layer the author is aiming to secure. To achieve this goal, we define some parameters and requirements such as CAI (Confidentiality, Availability and Integrity) based on the information suggested in [6]. We present for each work the category and the technique of solution used to deal with a typical defined attack. In addition, we verify for each work the application of RFID standards. Finally, we propose a device added scheme solution that we have used to enhance security in the access control scenario.

This paper is organized in 5 sections. The Section 2 summarizes the basics components of an RFID system, some examples of applications and a summarized review on most challenges and research directions where we concentrate on the problem of security. The section 3 presents our comparative study based on our parameters defining this study. The section 4 illustrates the smart card based biometrics solution to enhance RFID security and finally section 5 concludes this paper.

2. Background on RFID technology

In this part, we present the components of a typical RFID system, besides the related security challenges.

2.1. RFID Basics

An RFID system consists of 6 main components as shown in Figure 1:

- Tag: A tag is the data carrier and normally contains the ID number, and unique EPC code programmed into the tag.
- Reader & antenna: A reader captures the data provided by the tag when tags come in range of the area covered by the reader using its antenna.
- Middleware: The middleware can be a software as well as hardware dedicated to process data captured by the Reader, then dispatch this information to backend servers.
- Backend servers: The backend servers are the last station to make use of the data collected from RFID components. The information collected can be stored in database or sent to other systems for reporting and further analysis.
- Network infrastructure: Stands for the link between all RFID components which represents the main sources of RFID security and privacy threats.

2.2. Application domains

Animal tracking

RFID tagging systems are considered as powerful tools for animal identification management and tracking. Their benefits go beyond controlling the spread of diseases and ensuring quality-assured and safe food for consumers.
As an example of the application of RFID technology for animal tracking, an approach enabling an effective localization and tracking of small-sized laboratory animals was suggested in [7]

Logistics

The implementation of RFID technologies in logistics environments is increasingly attracting. The investment in this technology has shown that RFID is highly promising for identifying an object uniquely and providing the capability for "complete traceability" [8]. Moreover, it has been recognized as an effective solution to eliminate or reduce inventory inaccuracies [9].

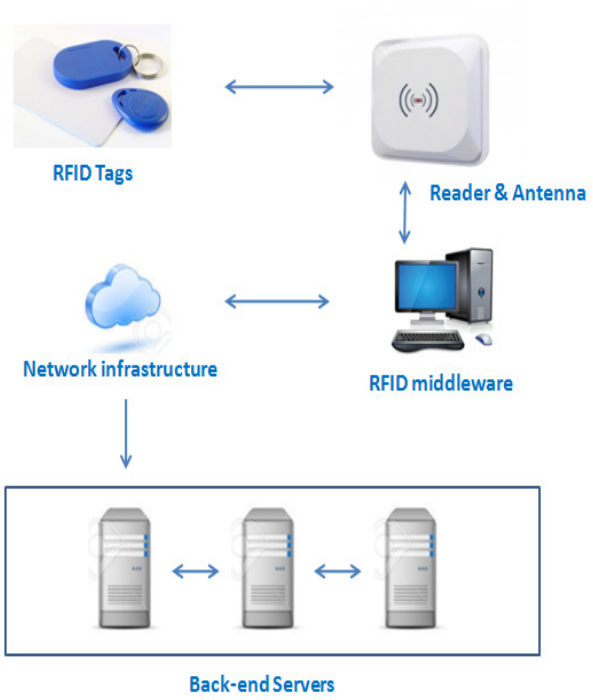

Figure 1. RFID system components

Intelligent transportation

The transport domain has widely benefited from the RFID adaptation due the ease of deployment of intelligence into each vehicle with a low cost approach [11].A vehicle emission inspection and notification system aiming to help daily monitoring of engine emissions through RFID devices was proposed in [12]. Also, a wireless system based on RFID technology was used to manage taxi fleets at the airports, train stations, bus terminals and all the taxis in cities [13]. RFID is also used in tolls collection as shown in Figure 2.

Healthcare

The use of RFID technology in the healthcare domain is making the patient's quality of care better. In fact, besides the collecting of information related to the patient as his presence inside a room and his health but also environment parameters can be detected such as temperature, humidity, and the presence of toxic gas [14].

In the same context, several efforts and research works have been made in this area. Exemplary, authors in [15] suggest a passive RFID platform for monitoring people during the night which deploys a long-range UHF RFID reader, wearable tags

integrated into clothes, and ambient tags dispersed in the environment, as well as a software engine for real-time processing and with warning modules [15].

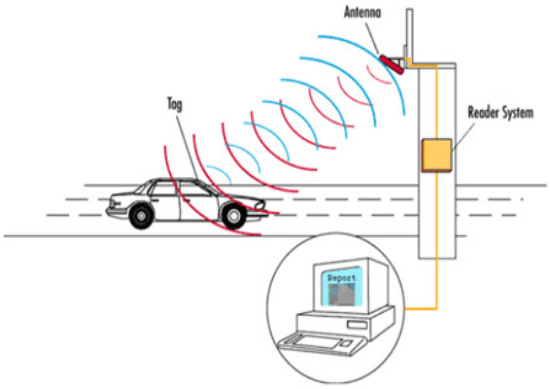

Figure 2. A toll collection using RFID [13]

2.3. RFID major issues

We address in this section some of the prominent issues related to RFID technologies and that still remain challenging topics of interest for a vast number of researchers.

Several works tried to study and gather the issues related the RFID to provide a baseline for researchers to understand the different sources as well as measures that can ensure the safety of sensitive data but more importantly to satisfy customers' needs and requirements in terms of efficiency, security and privacy. Among the most RFID challenges, we found technical problems, customer privacy issues and appliance to RFID standards [3]. In our work, we will focus on the last two problems which were taken into account in our comparative study (Section 3).

Technical problems

Among the biggest challenges during the implementation of an RFID system is studying the physical characteristics and capabilities of its components. In fact, the limited resource of storing information inside the tag, the low data processing and execution of complex operations can be a serious problem of performance and lack of mandatory features. In addition, due to the star architecture of the system, the reader can be the point of crush of the whole system, this problem occurs when a large number of items with RFID tags are energized by an RFID reader at the same time which leads to a confusion at the level of the reader and prevent it from tag scanning. A similar problem occurs when the coverage area of one RFID reader overlaps with another reader which leads to a signal interference and multiple reads of the same tag.

Standardization problems

Several efforts were dedicated to solve the problem of lacking of common RFID standards but the issue is still remaining in the industrial field. In fact, different standards coexist in parallel with divergent interests among which there is ISO 11784 that is utilized in the tracking of RFID cattle, the ISO 11785 for interface protocol, ISO 14443 for application of smart cards in payments and ISO 15693 that is applied to vicinity cards. The development of the electronic product codes (EPC) has been conceived to fill this need.

Obviously, the fact each of the existing standards is associated to a specific part of the RFID system make it different to deploy and protect data within an RFID system where tags standards can not comply with the communication standards for instance. Thus, it is of upmost importance to take into account the compliance to standards when implementing any RFID-based solution.

Security and privacy

Among the advantages of the deployment of RFID system is rendering the identification task automatically also gaining on performance and the ease of execution. All these benefits are not very useful is security and privacy are not guaranteed. For this reason, while designing an RFID system, many parameters should be taken into account to ensure a primary level of security, In fact, the data inside the tag, exchanged with the reader or dispatched to the back-end servers must be confidential, available and unchangeable (CIA characteristics). However, ensuring a full secure system which means keeping the whole system safe and operational, it remains a difficult task due to the several sources of attacks and threats that can coexist in parallel in some scenarios.

Table 1. RFID Typical attacks

Typical attack	The attack principle
Eavesdropping	This attack consists of listening to the network and sometimes recording for example all exchanges between tags and reader. The main goal of this attack is collecting data and taking advantage of the information gathered.
Denial of service	The denial of service consists of rendering equipment unavailable in the RFID system. An example of using this attack is spamming a reader with specific tags frequency requests which will make the reader out of service.
Cloning	The cloning attack is mainly to reproduce RFID tags. Using reverse engineering techniques to extract all the cart properties, precisely, the secrets keys, the tag can be modified and duplicated.
Tracking	The tracking attack consists of associating a tag to a person without his will and track his presence and movement as long as the attacker's reader is in range with the tag

During our research, many papers mentioned in their solutions some typical attacks that can take place in RFID systems, in the Table 1 below, we list some of most known attacks.

Many countermeasures and capabilities are proposed in literature to ensure security of the RFID system such as Pseudo-random based solution, Anonymous-ID scheme, symmetric and asymmetric cryptographic algorithms and others hashing based schemes [2].

Apart from the security aspect, the privacy is considered as a critical issue aiming to protect personal information. The expansion of the technology in several domains is not passing

without risks regarding the privacy the person since his identity information are associated to RFID chips that can be tracked and identified without his knowledge. As explained in table1 and due to the small size if RFID tags, they can be nested in personnel objects and clothes without being detected. The person movement and information are tracked and analyzed each time he come in range of the compatible reader area.

Some countermeasures and solutions were developed to protect personal data and reduce tracking capabilities. The table below illustrates the main techniques proposed in the literature studied for our classification.

Table 2. Some main countermeasures for privacy

Protection method	***How this technique improves privacy protection***
Delegation Tree	The principle of this method is delegating the control of reading tags depending on which privacy policy is assigned to each reader and tag. These specifications can be stored in database for example.
Protocol added *S*chemes	The technique consists of integrating a new coding scheme inside RFID tags and readers in order to create a specific protocol of communication; in this way, external readers cannot access to the network tags.
Tag killing	The tag killing method consists of destroying the content of tag after this one is no longer need to be used. The retailer can use the kill command after entering the right pin code. This technique can be used by the sellers after their products leave the store.
XOR encryption and PRNG	The XOR encryption and PRNG method is based on using a randomized protocol at each communication. This technique is powerful in the way to counter listening attacks such as Eavesdropping which will make the communication with tag a difficult task.
Blocker Tag	The Blocker tag technique aim to create an inductive field by the tag which will block communication between the tag and suspicious readers. Many occurrences of ID tag will be generated in order to hide the real one for the reader.

3. The comparative study

In this section, we will present the goal of our study besides the parameters defined for classification used to compare the selected academic works.

3.1. Motivation and design goal

Several levels of security can be applied to a typical RFID system, besides the nature of its architecture leads us to classify the solutions depending on each part of the system the attacks can take place. Furthermore, we refer to [6] to consider the three security main classes to classify the security threats in the reviewed works: Confidentiality, availability and integrity (CAI).

As defined in [6], the RFID system can be presented as three main layers: *1) RFID Edge Hardware Layer, 2) Communication Layer and 3) Backend Layer.* The possible threats and attacks related to each layer are mentioned based on CAI properties. In our work, besides classifying the attacks related to RFID security, we present also the solutions and techniques used to counter these problems. In [5], most of protection techniques can belong to specific categories as presented in Figure 3:

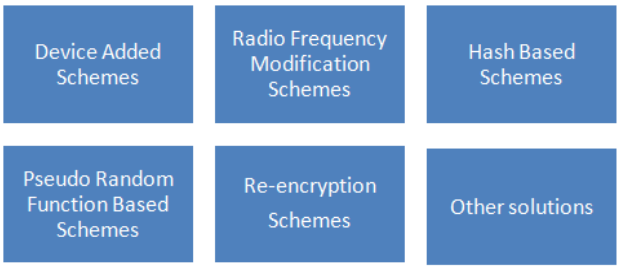

Figure 3. RFID security classes

In our study, we focus on recent works dealing with security and privacy, and we classify them according to the layers previously (attacks and solutions). In addition, we take into consideration other security requirements and parameters rather than CAI (untraceability, non-repudiation, forward secrecy, anonymity …).

Furthermore, we present the type of solutions and techniques dedicated for each layer and the attacks that can be related. At the end, we verify for each studied work the use and conformity to RFID standards. In this way, the following parameters are taken into account in our comparative study:

- *Privacy-focus / Security-focus*: Indicates whether the solution proposed take into account the security or consider privacy as the main concern.
- *Problem description and classification*: this parameter indicated which part of the system the problem can belong to. For this, we refer to the classification explained above.
- *Parameters of Security/Privacy considered:* Here we extract the security/privacy parameters considered by each author. Some papers focus on traditional security goals (confidentiality, integrity and availability) while other solutions take into account additional properties such as authorization, authentication, or forward secrecy.

Clearly, there are other properties to consider when authors focus in privacy as a main concern. These parameters include identity protection, anonymity and untraceability and. It is worth noting that these parameters are whether clearly cited in the paper or deducted.

- *Solution category*: As argued before, we have six mains classes of RFID solutions. For each of the twelve works studied we specify the class solution.
- *Techniques used:* For each class of solutions, we mention the techniques that have been exploited to ensure security and

privacy. Precisely, this includes cryptographic-based and no cryptographic-based methods.

- *Compliance to RFID standards?* Compliance to standards is considered as a primordial issue that need be highly highlighted. In this goal, for each studied work, we check the compliance to RFID or communication standards or if at least this issue is mentioned or an attention has been paid to by authors.
- *Examples of security attacks/ Threats considered:* this parameter indicates the security/ privacy attacks cited and treated in each paper. In the table below, the attack is defined for each part of the system it can occur and the solutions proposed to secure the system form this type of threats.

The objective of our comparative study as shown in Table 3, is not only presenting and classifying the security solutions and techniques regarding each of the recent studied paper but also making visible for researches and companies aiming to adopt an RFID system what are threats and attacks that should be taken into accounts while designing their systems.

As described before, the classification-based layer level helped us to locate the scope of each solution. Furthermore, during the study of the twelve works, we found that additional security / privacy parameters are considered rather than the traditional ones (CAI) in order to identify the several security/privacy threats. For Example, scalability is a primordial while aiming to enhance the system dimensions; some papers such as [24] consider scalability as a first topic while designing their solution. In fact, as mentioned in [22], this parameter remains among the real constraints of the majority of security solutions. Many techniques can be deployed to achieve scalability such as Checks handoff technique. As described in [24], this method was deployed to design a secure protocol supporting IoT.

Concerning techniques used, mutual authentication has taken more focus by authors as indicated in the works [20,16, 24] since, this security method is not only used in server's part but also between the reader and tags.

Concerning the security/privacy focus, many works try to ensure customer's privacy in their secured developed solutions and protocols. For instance, in [17, 20] intractability and an anonymous communication are taking into account to protect users' privacy. Thus, we noticed from the works presented in Table 3 that most of the solutions do not only focus on security or on privacy individually but these two concepts should be both take into consideration.

The second conclusion, we have subtracted from the Table 3 was that several works does not focus only on a single part of the system but they try to cover the whole layers (physical layer, communication layer, Back-end layer) that we have described in the section before.

For instance, authors in [18], propose two algorithms implemented by the Back-End server and a two-party protocol between the Back-End Server and a tag. In this way, two security methods were suggested in [20], the first contribution covers the backend layer by proposing two authentication (mutual and collaborative) schemes for both fixed and mobile readers, and the second contribution consisted at defining a secure channel between the reader and server in the communication layer. The main idea that we try to highlight is to not only paying attention to the data stored into tag or only securing communication between tags and reader but all the whole trajectory of data from data collecting to data storing in backend server.

As presented in Table 3, very few works we have studied focus on the device added schemes solution category. As an example, authors in [19] propose a solution that consist of changing the physical architecture of the RFID reader by dividing it into two different devices, an RF activator and a trusted shield device (TSD) playing an intermediary role between tags and reader for a secure communication [16].

In this way, the authors in [22] used the Physically Unclonable Functions (PUF) to secure data at level of tags (PUF is a security technology that seeks to introduce physical variation into individual devices taking part in cryptographic protocols [26]).

It is of upmost importance to tackle the issue of the RFID standardization. Indeed, and as illustrated in our comparative study, some works take into consideration the conformity of their solutions to RFID standards [12, 18, 19, 20, 20, 23, 24]. Intuitively, before designing any secure RFID solution it is crucial to verify whether this solution respects RFID standards or not.

Table 3: A comparative study of some security/privacysolutions in RFID systems

Characteristics / **Proposed Solution**	**Privacy-focus / Security -focus**	**Problem description and classification (Layer)**	**Parameters of Security/Privacy considererd**	**Solution category**	**Techniques used**	**Compliance to RFID standards?**	**Examples of security attacks/ Threat considered**
RFID-Tate: Efficient Security and Privacy Protection for Active RFID over IEEE 802.15.4 [16]	Both	Communication: A protocol for mutually authenticated (tag, reader) communication is suggested.	-Confidentiality -Availability - Authentication	Re-encryption	-Identity-based Encryption (IBE)	Yes : communication is performed over the standard IEEE 802.15.4f	- Cloning attacks. - Tag emulating, - Collision attack. - Spoofing - Replay attack -Sybil attack
A Secure Supply-Chain RFID System that Respects Your Privacy [17]	Both	Commiucation :p-Authors suggest a protocol between the reader and an individual tag	- Confidentiality - Integrity	Re-encryption	Public Key cryptography	Yes: (EPC tags standards)	-Reverse engineering

Secure Tag Search in RFID Systems Using Mobile Readers [18]	Both	Back-End: This paper suggests a search tag protocol; target backeEned Servers	- Confidentiality - Integrity - Anonymity - authorization	Pseudo-random based solution	XOR and 128bit PRNG operations	Yes : (EPC C1G2 compliance)	-Desynchronization, DoS attacks. -Side Channel Attacks: - Eavesdropping
Scalable RFID Security Framework and Protocol Supporting Internet of Things [24]	Security-Focus	Communication: A secure communication protocol and a framework supporting IoT	-Authentication. - Scalability - Confidentiality -Identity pretection -Adaptability	Other	Checks handoff (SCH) technique	Yes: EPCglobal standard	-Malware (Example SQLIA)
A New Security and Privacy Framework for RFID In Cloud Computing [25]	Both	Backend: A security and privacy model for RFID technology integrated to the Cloud computing (Servers) Was suggested.	- Confidentiality - Authentication	Re-encryption	Symmetric-key Cryptography	Not mentioned	No specified attacks was mentionned.
A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol [2]	Both	Both : Back-End: Two algorithms implemeted by the Back-End server are defined. Communication: A two-party protocol between the Back-End Server and a tag is proposed.	-Confidentiality - Availability - Forward security. -Anonymity Authorization, Authentication	Re-encryption	Public Key cryptography Elliptic curve cryptosystem	Mentioned but not applied	-Tag cloning attack. - Eavesdropping. - Replay attack. - Tag masquerade attack. -Denial-of-Service - Location tracking attack. - Server spoofing attack.
A Novel Coding Scheme for Secure Communications in Distributed RFID Systems [19]	Privacy-Focus	Physical Layer	Confidentiality - Integrity Anonymity	Device added scheme	- Reader changes architecture (New) Random Flipping and Random Jamming (RFRJ)	Only mentioned	- Random guessing attack. - Correlation attack. - Ghost-and-leech attack. - Eavesdropping.
A minimum disclosure approach to authentication and privacy in RFID systems [20]	Both	Both BackEnd: Two authentication (mutual and collaborative) schemes for both fixed and mobile reader are suggested. Communication: The channel between the reader and server is protected against attacks.	- Confidentiality - Untraceability Anonymity, Authentication, Forward secrecy	Pseudo-random based solution	Redundancy check (CRC) Pseudo random number generator (PRNG)	Yes (Conforme to EPC Class-1 Gen-2 spec-Ifications).	- Replay attack - Tag impersonation - Desynchronisation attacks.
Secure ownership transfer for multi-tag multi-owner passive RFID environment with individual-owner-privacy [12]	Both	Communication: Authors suggests multi-owner, multi-tag transfer protocol that achieves privacy-among-owners.	Confidentiality - Forward Untraceability Anonymity, Forward secrecy	Pseudo-random based solution	XOR and 128-bit pseudo-random number generators (PRNG)	Yes: complies EPC Global Class-1Gen-2 (C1G2)	-Tracking attacks - Replay Attacks - Denial of Service - Tag/Reader/Server Impersonation.
A Robust Grouping Proof Protocol for RFID EPC C1G2 Tags [21]	Security-focus	Communication: A grouping proof protocol ensuring a high level of security between tags and readers.	-Inegrity -Anonymity -Forward secrecy -Confidentiality	Pseudo-random based solution	(XOR) encryption and 128-bit pseudorandom number generators,	Yes: Complies EPC Global Class-1Gen-2 (C1G2)	-Replay Attacks -Denial of Service (DoS) Reader/Tag/Server impersonation Attack. -Active Attacks
Providing destructive privacy and scalability in RFID systems using PUFs [22]	Privacy-Focus	Communication: A private authentication protocol allowing a reader/tag communication.	- Confidentiality - Integrity - Authentication - Forward secrecy	Other	Physically Unclonable Functions (PUFs)	Not mentioned	- Compromising attack - Side-channel attacks
Computational Cost Analysis on Securing RFID Protocols Conforming to EPC Class-1 Generation-2 Standard [23]	Security-Focus	Both : A mutual authentication protocol seeking to achieve higher security level was proposed	-Confidentiality -Authentication - Forwad secrecy	Pseudo-random based solution	Pseudo-random number generators (PRNG)	Yes : Conform to EPC Class-1 Generation-2 standard (ISO 18000-6).	- DoS attacks - Reply attacks

4. RFID combining solution

4.1. Motivation

The comparative study presented in section 3, has shown many robust solutions and techniques that may counter several attacks, most of the techniques are based on cryptographic schemes and deal with direct attacks on physical layer of the RFID system components such as the tag and reader, whereas other techniques focus on the communication between readers and tags or reader and the backend servers to prevent the system from network attacks such as eavesdropping, man-in-the middle or desynchronization attacks.

Aiming to apply the RFID in the campus environment, we found that some scenarios are not totally secured. So, we propose to combine the RFID technology with other technologies to enhance security in the whole system.

4.2. Smart card based biometrics solution design

The RFID technology can be applied in many areas inside the university campus as shown below, in our work we focus on access control to exams rooms and sensitive areas like laboratories.

- Exams room
- Campus
- Research laboratories
- Library
- Staff offices
- Computer room

For instance, if we take the example of accessing to laboratories, the identity check must be verified before allowing the person access to the area. Based on the solutions proposed in Table 3, a cryptographic technique can be deployed in the inside the tag and the reader to secure the tag reading. However, the two main problems in our case are indicated in Figure 4.

For this reason, our method consists of enhancing the RFID technology by using smart card based biometrics solution. In fact, the RFID technology is seen as the fast-automatic technique of identification, whereas, the smart card check can support complex operations of cryptographic check as indicated in [27]. In addition, the biometric fingerprint will help us to check the true identity of the person aiming to access to the secured area. In Figure 5, we present the proposed system combining RFID with the smart card-based biometrics verification.

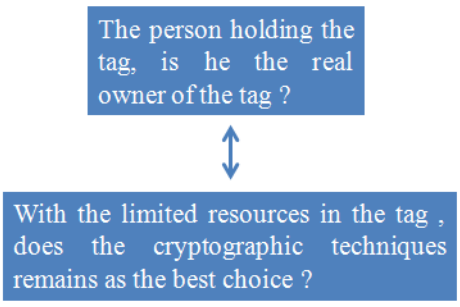

Figure 4. Access control issues in RFID system

As detailed in [27]. The step one consists of reading the RFID tag when it comes in range with the RFID reader. After that, in the step 2, the person's tag is sent to the local database to check if it belongs to the person's tags allowing him access the secure area. Once validated, the person inserts his smartcard and puts his fingerprint for validation. In this case, a first match-on-card is established comparing the user fingerprint with the other one stored in the smartcard. If the check is performed successfully, the fingerprint is sent to the database to verify that no changes were made on the couple (fingerprint, Tag ID). Finally, the door is opened if all the conditions are satisfied.

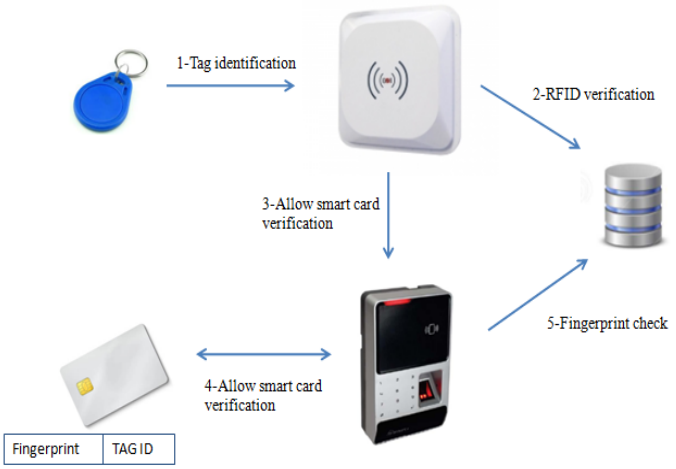

Figure 5. Components of the proposed system

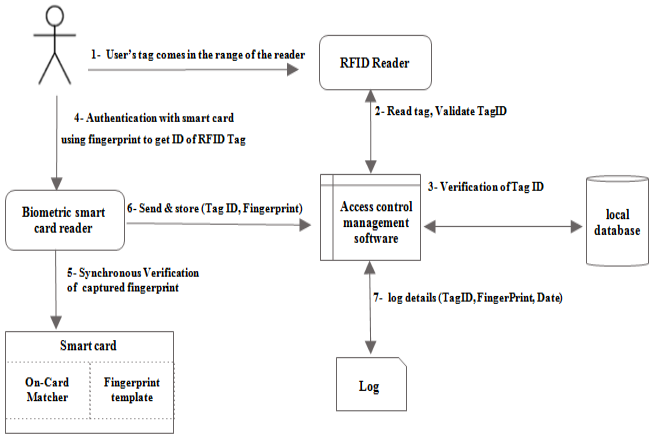

Figure 6. Flowchart of the access control system in sensitive areas [27]

In the proposed solution, we have chosen to combine smart card biometrics solutions with RFID in order to respect the limited resources and capabilities inside the tag for performing complex operations. Furthermore, even if the smart card is falsified or the person ask for authentication with a borrowed RFID tag, the verification explained above based multi-level of security will deny his access to the secured room. The flowchart in Figure 6 summarizes the sequence of actions during the authentication process. The system presented above meets the need presented in Figure 4 which are not guaranteed in the solutions presented in section 3.

5. Conclusion

In this paper, we have presented some recent works aiming to ensure security and Privacy in RFID systems. In particular, we tried to classify these solutions in order to provide a clear understanding of the different threats and risks related to security and privacy.

To achieve this goal, we compared some solutions according to the traditional security and privacy objectives. Also, we mentioned that additional parameters such as scalability and efficiency should be taken into account besides the traditional security and privacy objectives.

In addition, we proposed a combined solution using RFID and smartcard based biometrics to ensure performance and cover some security gaps detected while designing our RFID system. As future work, we plan to develop our device added scheme solution, by studying more the technical possibilities of its implementation inside the campus.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This research is performed inside the MATSI Lab., ESTO, University Mohammed First, Oujda (Morocco).

References

[1] M. El Beqqal and M. Azizi, "Classification of major security attacks against RFID systems," in 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), 2017. https://doi.org/10.1109/WITS.2017.7934622

[2] Yi-Pin Liao, Chih-Ming Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol", Journal of Ad Hoc Networks, Volume 18, July 2014, Pages 133–146,2013. https://doi.org/10.1007/978-3-642-35473-1_1

[3] AL-Kassab, J., W.C. Rumsch. 2008. Challenges for RFID cross-industry standardization in the light of diverging industry requirements. IEEE Systems Journal 2(2) 170-177. https://doi.org/10.1109/JSYST.2008.921291

[4] F. Kamoun," RFID System Management:State-of-the Art and Open Research Issues", IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 6, NO. 3, SEPTEMBER 2009 . https://doi.org/10.1109/TNSM.2009.03.090305

[5] K. Sabaragamu Koralalage, J. Cheng, "A Comparative Study of RFID Solutions for Security and Privacy: POP vs. Previous Solutions", International Conference on Information Security and Assurance, 2008. https://doi.org/10.1109/ISA.2008.89

[6] A. Mitrokotsa, M. Beye and P. Peris-Lopez, "Classification of RFID Threats based on Security Principles", GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES, 2009

[7] L. Catarinucci, R. Colella, L. Mainetti, L. Patrono, S. Pieretti, Ilaria Sergi, and L. Tarricone, "Smart RFID Antenna System for Indoor Tracking and Behavior Analysis of Small Animalsin Colony Cages", IEEE SENSORS JOURNAL, VOL. 14, NO. 4, APRIL 2014. https://doi.org/10.1109/JSEN.2013.2293594

[8] M. Alamgir Hossain, "Development of an integrated model for RFID extension", BUSINESS PROCESS MANAGEMENT JOURNAL· AUGUST 2014. https://doi.org/10.1108/BPMJ-04-2013-0055

[9] T. Fan, Feng Tao, S. Deng, S. Li, "Impact of RFID technology on supply chain decisions with inventory inaccuracies", Int. J. Production Economics, 2014. https://doi.org/10.1016/j.ijpe.2014.10.004

[10] Oh-Keun Ha Yong-Seok Song Kyung-Yong Chung Kang-Dae Lee · Dongjoo Park, "Relation model describing the effects of introducing RFID in the supply chain: evidence from the food and beverage industry in South Korea",Journal of Pers Ubiquit Comput, 2014. https://doi.org/10.1007/s00779-013-0675-x

[11] Lei Xie, Yafeng Yin, Athanasios V. Vasilakos,Sanglu Lu, "Managing RFID Data: Challenges, Opportunities and Solutions", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 3, THIRD QUARTER 2014. https://doi.org/10.1109/SURV.2014.022614.00143

[12] Sundaresan, S. Doss, R., Wanlei Zhou, "Secure ownership transfer in multi-tag/multi-owner passive RFID systems", IEEE Global Communications Conference (GLOBECOM), 2013. https://doi.org/10.1109/GLOCOM.2013.6831513

[13] S. Samadi, "Applications and Opportunities for Radio FrequencyIdentification (RFID) Technology in Intelligent Transportation Systems: A Case Study", International Journal of Information and Electronics Engineering, Vol. 3, No. 3, May 2013. https://doi.org/10.7763/IJIEE.2013.V3.330

[14] Sara A, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "RFID Technology for IoT-Based Personal Healthcare in Smart Spaces", IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 2, APRIL 2014. https://doi.org/10.1109/JIOT.2014.2313981

[15] C. Occhiuzz, Carmen Valleseb, S.Amendolab, S. Manzarib," NIGHT-Care: a passive RFID system for remote monitoring and control of overnight living environment", 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014). https://doi.org/10.1016/j.procs.2014.05.414

[16] Sadikin, M.F., Kyas, M., "RFID-tate: Efficient security and privacy protection for active RFID over IEEE 802.15.4, The 5th International Conference on Information, Intelligence, Systems and Applications, IISA 2014.in press. https://doi.org/10.1109/IISA.2014.6878787

[17] Arbit, A., Oren, Y. ; Wool, A, "A Secure Supply-Chain RFID System that Respects Your Privacy", Journal of Pervasive Computing, IEEE (Volume:13 , Issue: 2), 2014. https://doi.org/10.1109/MPRV.2014.22

[18] Sundaresan, S., Doss, R. ; Piramuthu, S. ; Wanlei Zhou, 'Secure Tag Search in RFID Systems Using Mobile Readers', Journal of Dependable and Secure Computing, IEEE Transactions on (Volume:12 , Issue: 2), 2014, in press. https://doi.org/10.1109/TDSC.2014.2302305

[19] Sakai, K, Sun, Min-Te ; Ku, Wei-Shinn ; Lai, T.H., "A Novel Coding Scheme for Secure Communications in Distributed RFID Systems",Computers, IEEE Transactions on (Volume:PP , Issue: 99), 2015, in press. https://doi.org/10.1109/TC.2015.2423671

[20] Robin Doss, , Wanlei Zhou, Saravanan Sundaresan, Shui Yu, Longxiang Gao , 'A minimum disclosure approach to authentication and privacy in RFID systems", journal of Computer Networks, Volume 56, Issue 15, Pages 3401–3416 pp. 544 - 549 , 2012. https://doi.org/10.1016/j.comnet.2012.06.018

[21] Sundaresan, S, Doss, R. ; Piramuthu, S. ; Wanlei Zhou," A Robust Grouping Proof Protocol for RFID EPC C1G2 Tags", Information Forensics and Security, IEEE Transactions on (Volume:9 , Issue: 6), 2014. https://doi.org/10.1109/TIFS.2014.2316338

[22] Mete Akgün, M. Ufuk Çağlayanb, "Providing destructive privacy and scalability in RFID systems using PUFs", Journal of Ad Hoc Networks, Volume 32, Pages 32–42, 2015, in press. https://doi.org/10.1016/j.adhoc.2015.02.001

[23] Avoine, G. Bingol, M.A. ; Carpent, X. ; Yalcin, S.B.O., "Privacy-Friendly Authentication in RFID Systems: On Sublinear Protocols Based on Symmetric-Key Cryptography". obile Computing, IEEE Transactions on (Volume:12 , Issue: 10), 2013. https://doi.org/10.1109/TMC.2012.174

[24] BR Ray, J Abawajy, M CHowdhury, "Scalable RFID security framework and protocol supporting Internet of Things", Computer Networks, vol. 67, pp. 89-103, 2014. https://doi.org/10.1016/j.comnet.2014.03.023

[25] Plos, T. Hutter, M. ; Feldhofer, M. ; Stiglic, M., "Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography", Very Large Scale Integration (VLSI) Systems, IEEE Transactions on (Volume:21 , Issue: 11), 2013. https://doi.org/10.1109/TVLSI.2012.2227849

[26] D. Moriyama1, S. Matsuo1 and M.Yung, "PUF-Based RFID Authentication Secure and Private under Memory Leakage", IACR Cryptology ePrint Archive , 2013. https://doi.org/10.1016/j.adhoc.2015.02.001

[27] M. El Beqqal, M. A. Kasmi, and M. Azizi, "Access control system in campus combining RFID and biometric based smart card technologies," Adv. Intell. Syst. Comput., vol. 520, pp. 559–569, 2017. https://doi.org/10.1007/978-3-319-46568-5_56