Security on RFID technology

Nabil Kannouf*, Youssef Douzi, Mohamed Benabdellah, Abdelmalek Azizi
ACSA Laboratory, Faculty of Sciences
Mohammed First University, Oujda, Morocco
{Nabil.kannouf, douzi.ysf21}@gmail.com, {med_benabdellah, abdelmalekazizi}@yahoo.fr

***Abstract*—RFID (Radio Frequency Identification) systems are emerging as one of the most pervasive computing technologies in history due to their low cost and their broad applicability. Latest technologies have brought costs down and standards are being developed. Actually, RFID is mostly used as a medium for numerous tasks including managing supply chains, tracking livestock, preventing counterfeiting, controlling building access, and supporting automated checkout. The use of RFID is limited by security concerns and delays in standardization. This paper presents some research done on RFID, the RFID applications and RFID data security.**

Keywords— RFID; RFID Technology; Security on RFID

I. INTRODUCTION

For several years, Radio Frequency IDentification (RFID) devices are gaining a prominent place in several domains such as logistics, library, health care and other. In Roy want article [15], "Radio Frequency Identification Technology (RFID) has moved from obscurity into main stream applications that help speed the handling of manufactured goods and materials". Actually, BarCode is still the important rule in supply chain industries and department stores. Although, RFID is replacing barcode technology and benefit from the great advantage of being independent of line sight problems and scanning the object from distance. Furthermore, RFID systems can identify many different tags set in the same area. RFID tags have a many capacity of 16 to 64 Kbytes which is great than barcodes (1 to 100byte) [11] and can stores many data such as identification data, manufacturer name and product specifications. RFID was the need for traceability, which is define the ability to a trace the history, used and located the articles or activities and other.

By the 1930's in World War I, the problem is how to identify the foe and friend. The major question is: which side was the aircraft? If was exactly this inability to identify aircraft that enabled the mistaken of incoming japans aircraft to an unrelated US bomber flight so ensured surprise at Pearl Hardor in 1941. The problem of identifying as well as detecting potentially hostile aircraft challenged all combatants during World War II [4]. In 1940, RFID idea begins to sprout with Harry Stockman works [7] and D.B. Harris works [1]. Their articles are considered the foundation of RFID and describe the principals that are still used to days. Recently in 2003, EAN international, auto-ID, UCC (Uniform code council) and other industries are created the EPC standard (EPCGlobal version 1.0) integrating RFID and internet technologies to implement the objects traceability networks [16]. By 2010, it was clear that the UHF tags are particularly suitable for tracking garments, and wide use of RFID for this purpose began create the mass market envisioned by the MIT team years before [4].

The paper is organized as follows; RFID technology in section 2, section 3 discusses RFID applications, and section 4 discusses attacks and security of RFID systems. Conclusion is listed in section 5.

II. RFID TECHNOLOGY

A. Tags

Different types of RFID tags exist, a device without integrated circuit, hold in the printed electronics [18] tags, the Surface Acoustic Wave [14] tags and the Thin Film Transistors Circuit (TFTC) [10] tags. Also, a semiconductor device (excluding integrated circuit), this device in constructed by diode capacity. Likewise, a devices to built circuit, still account the largest part of the RFID market. In last type, tag is broadly classified as active, semi-passive or passive. An active tag requires a power source and is either connected to a powered device or to a battery and is often limited by the lifetime of its source because is used to send and processing an integral data. Being dependent on a power source puts limitations on active RFID tags. Cost, size, lifetime make them impractical for regular use. Also, a semi-passive tag requires a power source and it used for processing an integral data. On the other side, passive RFID is interest because the fact they are independent of power source and maintenance "Fig.1,".

B. Distance and frequency

Among the first important characteristics of the specifications of an RFID application, the distance is used prominently, and its division (related to the physical elements or processes used games). Also the power characteristics of the tags influence the frequency and potential applications of an RFID system, as the table below shows "TABLE I,"

C. Operating principle of tags

There are several types of operation and possible communication transponders, are the following:

- Read only: it is only possible to read the transponder. Tags have a single identifier that is written once when a tag is manufactured.
- Reading and writes multiple: the goal is reuse of the transponder and /or updates their information.
- Reading and / or writing protected: data protection "secret" read or written can be done in software (passwords) or hardware (especially timing, etc.) and applied for all or part of the memory.
- Secure and encrypted reading and / or writing: securing wishes to partner authentication (base station – transponder) may communicate together by changing or rotating codes for example. The encryption of data

978-1-4673-8149-9/15/$31.00 ©2015 IEEE

exchanged between the base station and the transponder serves to counter eavesdropping and hackers.

Fig. 1. Comparison between passive and active transponders. [11]

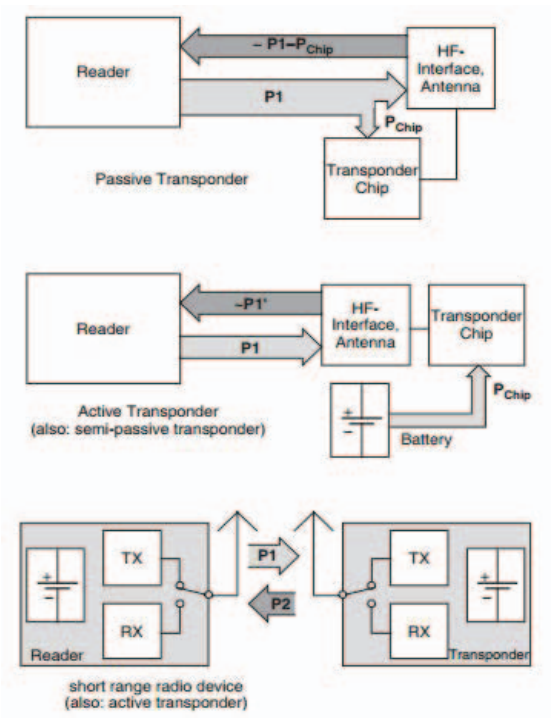

TABLE I. RFID DISTANCES AND FREQUENCIES. [3]

	Frequency	Distance	Example Application
Low Frequency (LF)	125-134 KHz	Few cm	Vehicle Immobilizer
High Frequency (HF)	13.56 MHz	1 m	Building Access Smart cards
Ultra-high Frequency (UHF)	860-930 MHz	~3 m	Supply Chain an logistics
Microwave	2.45 GHz	10 m	Traffic toll collections

D. Antenna and power transfer

For transponders, there are many types of differentiated by their shapes, materials, their earnings and manufacturing technologies. They are always special for transponder type (according to be characteristics of the integrated circuit or other), application and frequency of use. From a form point of view, we can mention the antennas in one dimension (round flat square, eight, etc.) or two-dimensional (cylindrical, etc.) as the examples presented in "Fig.2," Their materials also depend on the manufacturing technology. Examples include copper antennas made directly on the printed circuit boards, including copper wound; Sliver conductive inks or printed directly on paper or plastic support, etc.

The energy transfer between the base station (reader) and the transponder depends on many parameters including:

- The type of coupling: inductive or radiative,
- The distance between the transmitting and receiving antennas,
- The various dispersed power levels, re-radiated and reflected by the tag,
- The different gains of the transmitting and antennas, the coupling coefficient, the absorption of materials in the environment, etc.

Fig. 2. Examples of RFID transponders antennas

E. Communication

Passive tags do not have a power source. Instead of this, tags are powered by the reader and can only respond after receiving a message from the reader. The communication is half-duplex, simultaneous transmission and reception are not allowed. The communication between tag and reader in the EPC Gen2 system [20] is organized in three stages: Selection, Inventory and Access stages. In the Selection and Inventory stages, the reader initiates the communication sending identification queries. If the reader manages to access or modify the tag memory content, the Access stage is started. Starting from this point, an important security drawback is encountered, as the required password for the access is not sufficiently secure. The communication in the EPC Gen2 protocol is organized as follows:

- Select: The reader selects a part of the tag population in the communication neighborhood for inventory and access using one or more Select commands.
- Inventory: It is the process by which a reader identifies tags. A detailed description of the inventory operation is as follows:
    1. A reader sends a request message Query to tag. The query initiates an inventory round and decides about tags will participate in the round.
    2. The available tags in the communication range puck a 16-bit random value using the implemented Pseudo-Random Number Generator (PRNG) [19] on board, and shall load this value into a slot counter, decreasing one unit for each Query command reception. When the slot counter reaches zero, the tag backscatters a random value (named RN16) to the reader.
    3. If the reader detects a single tag reply, it requests the identification from the tag by acknowledging the tag with an ACK containing the same RN16.
    4. The tag compares the RN16 in the ACK with the RN16 it sent before. If they are equal, the tag backscatters it EPC (Electronic Product Code), PC (Protocol-Control), and CRC-16.
- Access: After acknowledging a tag, a reader may choose to access it. In this stage, a reader modifies and read individual tags memory areas. A reader can access to a tag as follows:
    1. The reader sends a ReqRN (Request Random Number), containing the previous RN16, to the acknowledged tag.
    2. The tag compares random number RN16 in the ReqRN with RN16 in the tag. If it is right, the tag generates and stores a new RN16, denoted as handle. Then backscatters it to reader.
    3. The Read, Write, and Kill commands are sent with 16-bit words (i.e., either data or half-password) form reader to tag. These commands use a one-time-pad key to hide the word being transmitted.

III. RFID APPLICATIONS

A. Object tag mainly

Objects tag mainly, is in two forma: logistic traceability (tracking) and product traceability (tracing). The first form concerned the quantitative of products. It focuses on the geographical location of the logistic units. The second form designating the qualitative of products. The manufacturer uses a particular look for the causes of quality problems. The products traceability focuses on characteristics of consumer units. Both are developed to satisfy the need of industrial traceability, supply chain very intensive amount of transponders.

Object tag mainly, allows industrial production of goods, monitoring and maintenance of manufacturing processes. It can be used in archiving systems (for example Magellan company [17] specialized in documents archives), wealth management (Agrihouse company [6] sells irrigation needs of the detection system), equipment management (for instance Air-conditioning capture, temperature capture, etc.), automobile, aviation, automation and process control and consumer goods (meals, cakes, etc.).

B. Tag with direct reference or potential to individuals

It has many forms. An access control and animals traceability represented by several types: label and tickets (football game tickets, transport passes and concert an tickets for the Beijing Olympic Games [5], etc.) access control systems, animals traceability (tag store medical and vaccination information, etc.) and individual traceability. Also the fidelity cards, membership and payment contain a few types: fidelity card, membership card (for example SpeedPass), contactless bank card and payment and advertising through mobile phone. In health, many applications types existed: Assistance to disabled (for example TellLate), hospitals management (instrument, traceability of blood donation, etc.), implants (patient identification, locate patients, etc.) [8], medical surveillance and intelligent implants (used for glucose measure, temperature, etc.) manufactured by VeriChip. As will, sport leisure and domotic business has like types: sports applications (for example radar of golf balls), rental systems (skis, ice skates, etc.), intelligent games (for example MINDSTRORMS robots) and domotic tag (like Domo Tag). Finally, public services offered a lot of types: maintenance of public services (for example water meters in Meylan France) ETC system, banknotes, ID cards, and passports and social security cards.

C. Applications outside class

The applications of RFID mentioned above do not constitute an exhaustive list. Among the many that could be added, some applications have indistinct boundaries and can't readily enter a mold, a category. Here are some recent examples: protection per self-destruction for example Virtuity Britannic company presents a self-destruction technology, based on WIFI and RFID Tags. Also, localization for instance a Loc8tor retrieves up to 180 meters away which is attached or

fastened to the transponders provided. Finally, Monitoring barmen e.g. the Capton beverage tracking solution is comprised of a set of wireless pour spouts linked to powerful cloud-based software that analyzes liquor usage and provides meaningful business intelligence.

D. Future applications

RFID technology likes to be combined with other technologies and domains. Such as smart products, smart appliances, RFID-enabled mobile phones and recycling plastics. The future application organized as follows:

- "Smart" products: Clothing applications, CDs, etc. tagged for store returns.
- "Smart" appliances: Refrigerators that automatically create shopping lists. Also, closets that tell you what clothes you have available, and search the Web for advice on current styles, etc. And, one such application is VistaCrafts RFIQin "Fig. 3," available in Japan, which comes with 24 recipe cards. The pan reads the card you show and "tells" the cook top what it do to perfectly monitor each cooking step and perfectly reproduce the most difficult recipes. Each pan handle is embedded with an RFID chip that uses a proprietary signal to communicate with coordinated chips in the cook top and special recipe cards that monitor each cooking step for a particular dish.
- RFID-enabled mobile phones (e.g., Nokia): scan movie poster to learn show times Scan consumer product to get prince quotes
- Recycling plastics that sort themselves.

Fig. 3. VistaCrafts RFIQin Source [13]

IV. ATTACKS AND SECURITY OF RFID SYSTEMS

A. Attacks

The attacks that are based on the way the RFID systems are communicating and the way that are transferred between the entities of an RFID network (tags, readers). In this section we describe attacks that affect the tags, reader and network protocol. We also provide possible ways to counter these attacks.

1) Attacks on the Tags

- Cloning. Even the most important and characteristic feature of RFID systems, their unique identifier, is susceptible to attacks. Although in theory you cannot ask an RFID manufacturer to create a clone of an RFID tag [12], in practice it has proven that the task of replicating RFID tags does not requite a lot of money or expertise considering the wide availability of writable and reprogrammable tags. An ominous example is the demonstration by a German researcher of vulnerability of German passports [2] to cloning.
- Spoofing. Spoofing is effectively a variant of cloning that does not physically replicate an RFID tag. In this type of attacks an adversary impersonates a valid RFID tag to gain its privileges. This impersonation requires full access to the same communication channels as the original tag. This includes knowledge of the protocols and secrets used in any authentication that is going to a take place.

2) Reader Attacks

- Impersonation. Considering the fact that in many cases RFID communication is unauthenticated, adversaries may easily counterfeit the identify of a legitimate reader in order to elicit sensitive information or modality data on RFID tags.
- Eavesdropping. The wireless nature of RFID makes eavesdropping one of the most serious and widely deployed threats. In eavesdropping an unauthorized individual uses an antenna in order to record communications between legitimate RFID tags and readers this type of attacks can be performed in both directions: tag to reader and reader to tag. Since readers transmit information at much higher power then tags, the former are susceptible to this type of attacks at much greater distances and consequently to greater degree. The information recorded can be used to perform more sophisticated attacks later. The feasibility of this attack depends on many factors, such as the distance of the attacker from the legitimate RFID devices.

3) Network Protocol Attacks

RFID systems are often connected with back-end databases and networking devices on the enterprise backbone. Nevertheless, these devices are susceptible to the sane vulnerability of general purpose networking devices. Flaws in the operating system and network protocols used can be used by malicious attacks in order to launch attacks and compromise the back-end infrastructure.

B. Security

Through appropriate data collection it is possible to detect cloned RFID tags. Alternatively, cloning attacks can be mitigated via challenge response authentication protocols. These should also support robust anti-brute force mechanisms. Nevertheless, the inherent resource constraints that RFID tags present lead to weak authentication protocols that are inefficient against determined attackers. Juels [9] has demonstrated some techniques for strengthening the resistance of RPC tags against cloning attacks, using PIN based access to achieve challenge response authentication. Public awareness of the security implication related to cloning attacks should be

the key policy to defend against. However, this is not always the case. For instance, none of the countries that issue e-passports have anti-cloning mechanisms [12] as suggested by the ICAO 9303 standard [2]. In order to defend against passive eavesdropping attacks encryption mechanisms could be used to encrypt the RFID communication. Spoofing and impersonation could be combated by using authentication protocol or a second form of authentication such as one-time passwords, PINs or biometrics. Network protocol attacks could be countered by hardening all components that support RFID communication, using secure operating systems, disabling insecure and unused network protocols and configuring the protocols used with the least possible privileges.

V. CONCLUSION

RFID is a technology with the potential to improve the way we live our lives and the way we conduct business. However, for this potential to be realized the challenges listed above, particularly those relating to security and privacy will have to be thoroughly addressed. A lot of research on RFID tags is ongoing including on embedding these with other devices, especially mobile devices. RFID manufacturers and users are looking for proper standardization and regulation of RFID. As prices fall further and technological improvements continue to occur, RFID technology is expected to become economically and technically more viable impact our daily lives as more application are developed.

We are interested to problem of security concern the RFID tags. Actually, our work focuses on RFID security and we are currently working on an algorithm about securing communication between tags and reader. Then, we will be interested in developing a private control of EPCGlobal network and products traceability.

After reading some research work being done on RFID security procedures, we are working on an encryption approach to securing some procedures used in RFID.

References

[1] A. R. Koelle, S. W. Depp, and R. W. Freyman, “Short-range radio-telemetry for electronic identification, using modulated RF backscatter”, Proceedings of the IEEE, Vol. 63, No 8, August 1975, pp. 1260-1261

[2] Aikaterini Mitrikotsa, Melanie R. Rienack and Andrew S.Tanenbaum, “Classification of RFID Attacks”, Gen, 2010, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.143. 9601& rep=rep1&type=pdf

[3] Charles Mutigwe and Farha Aghdasi, “Research Trends in RFID Technology”, Interim: Interdisciplinary Journal, 2007 – reference.sabinet.co.za, Vol. 6, pp. 68-82.

[4] Daniel M. Dobkin,, “The RF in RFID Passive UHF RFID in Practice, Chapter 2 – Histtory and Practice of RFID”, Elsevier 2008, pp. 7-49.

[5] Frédéric Lentient, “Etat de l’art et application RFID”, CUEFA Gronoble university 2008.

[6] Hans-Dieter Seelig, J. Stoner II Richard, Alexader Hoehn, William Walter Adams, III, ”Phytometric intelligence sensors”,2010, Agrihouse, Inc., The Regents Of The University of Colorado.

[7] Harry Stockmann,” Communication by Means of Reflected Power”, Proceeding of the IRE (institute of Radio Engineers), October 1948, pp. 1196-1204.

[8] Hervé Aubert, “RFID technology for human implant devices”, C.R Physique 12, 2011, pp. 675-683.

[9] Juels,A., “Stengthening EPC Tags Against Cloning”, In: Proc. Of ACM WorkShop on Wireless Security (WiSe’05). ACM Press(2005), pp. 67-76.

[10] Klaik, H., Gundlach, D.J. ; Jackson, T.N. , “Fast organic thin-film transistor cirsuits”, Electron device Letters, IEEE 1999, Vol. 20, Issue:6, pp. 289-291

[11] Klaus Finkenzeller,”RFID Handbook”, 3rd edition, John Ley & Sons, Wiley, 2010.

[12] Laurie, A., “Practical Attacks Against RFID”, In: Network Security, Vol. 2007, No9, pp. 4-7

[13] Nadita Srivastava, “RFID Introduction, Present and future application and security Implications”, 2006, http://cryptography.gmu.edu/~jkaps/download.php?docid=483

[14] Reindl, L.Shrena, I.; Kenshil, Peter, R., “Wireless measurement of temperature using surface acoustic waves sensors”, Proceedings of the 2003 IEEE International 2003, pp. 935-941.

[15] Roy Want, “An Introduction to RFID Technology”, IEEECS and IEEE ComSoc, Vol. 5, No. 1, Santa Clara, 2006, PP. 25-33.

[16] Somark Innovations (Juin 2007) Somark Innovations Announces Successful Live Animal Tests of Biocompatible Chipless RFID Ink in Cattle and Laboratory Rats. http://www.nonaiswa.org/wordpress/wp-content/uploads/2007/03/somarkbiocompatiblechiplessrfidink.pdf.

[17] Stuart Colin Littlechild, Michael John Stanton, “Radio frequency identification transponder”, 2007, Magellan Tchnology Oty Limited.

[18] Vivek Subramanian, Paul C. Chang, Josephine B. Lee, Amanda R. Muraphy, David R. Redinger, Stevern K. Volkman, “ Progress Toward development of All-Printed RFID Tags: Materials, Processes, and Devices”, Proceeding of the IEEE 2005, Vol. 93, No 7, pp. 1330-1338.

[19] Wiem Tounsi,”Security and Privacy Controls in RFID Systems Applied to EPCGlobal Networks”, Telecom Bretagne, University of Rennes 1, 2014.

[20] Wiem Tounsi, Nora Cuppens-Boulahia, Joaquin Garcia-Alfaro, Yannick Chevalier, Frédéric Cuppens, “KEDGEN2: A key establishment and derivation protocol for EPC Gen2 RFID systems”, Journal of Network and Computer Applications, 2014, Vol. 39, pp. 152-166.