ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

Radio Frequency Identification (RFID) security issues and possible solutions

Mohsen Khosravi, Ahmad Sharifi, Dr. Asadullah Shah

Abstract— ***Radio-frequency identification (RFID) has become popular for automated identification and tracking of objects, goods and people. As the applications of RFID are expanding every day, new security issues also will be appeared. This paper speaks about fundamentals of RFID systems and security issues which can be raised in each one of the RFID architecture parts, as a wireless communication technology. This paper emphasize on the requirement of security in each special type of RFID systems applications, different kind of treats which can influence the security and safety of the RFID applicants and the last improvements of existing security and privacy methods and protocols.***

Index Terms— **Reader, RFID, Security, Tag.**

I. INTRODUCTION

Radio-frequency identification (RFID) is an automatic identification and data capturing technology, which can be used in different fields in order to identify and track goods and people. The history of RFID returns to around 70 years back in Second World War which RFID was used to identify enemy aircraft. However, today's RFID applications are somehow different with its initial applications. Undoubtedly new applications of RFID have made a revolution in inventory and automation processes; RFID can be seen everywhere from supply chain inventory to animal identification, from health care management to RFID enable passports or in a supermarket like a barcode for goods.

A. RFID Fundamental

RFID system has at least a tag and a reader. A tag consists of a microchip, capacitors and an antenna coil. A tag communicates with an RFID reader through radio signals. RFID reader is used in order to do the tag inquiries and grasp the needed information from the tag. The reader sends out some radio waves to interrogate the tag. [1] These radio waves are emitted by reader's antenna then RFID tag replies the radio waves while in the other side the reader is connected to a backend database which processes the information's sent by the tag. RFID tag's microchip saves the information that are important like product code, id number or any information which must be retrieved by the reader. RFID tags are two general types: passive and active.

- Passive tags: this type of tags does not need battery to work. They generate power from a signal of an outer reader. The passive tags reflect the radio frequency signal transmitted to them from a reader then add information by modulating the reflected signal, and obtain power from the signal of an external reader. The most known application of passive tags is to replace the customary barcode technology (with some important advantages in compare to barcode) and has much lighter weight and chipper price in compare with active tag, and also virtually its effective lifetime is infinite .nevertheless on the other side, read ranges of passive tags is very limited. [2]
- Active tags: are battery-powered tags (usually on-board battery) and so having more transmission range and stronger signal in compare with the passive tags. That is why the readers can touch them from longer distance. [3]The onboard power supply increases the size and price of the active tags so active tags are larger and more expensive than the passive tags, thus large items tracked over long distance are the best operational platform for active tags. In comparison of two tags, it is obvious that passive tags are very inexpensive. Today each piece of passive tags is around 20 cents which seems a reasonable price to integrate into common materials and products, although technology is trying to make them chipper. Furthermore, passive tags size can also be quite small. By the new technology findings, about the tags antenna the size of new passive tags limits to about the size of a quarter. [2]

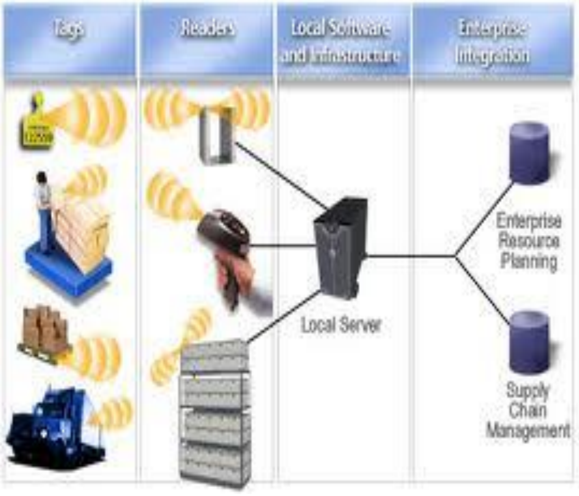


Fig 1- RFID Components [10]

II. RFID SECURITY ISSUES

Although the contactless nature of RFID and its fast speed in affording the information grants a big superiority over known machine-readable identification method's, some types of vulnerabilities are there in RFID systems which make them permeable to a wide range of attacks. Generally, RFID security issue and possible attacks can be divided in three major categories:

- Attacks which affect RFID edge hardware part
- Attacks which affect the communication part
- Attacks which affect the data support part

B. RFID Edge hardware

It consists of RFID physical and touchable devices. In RFID systems two major physical devices are available “tag and reader”. Tampering vulnerability can be seen in these devices due to common security weakness in these devices. [3].

C. Communication part

Information swapping is the major duty of the communication part. Most of the attacks in this part, are pointed to radio link. If the attacker can listen in, it can be ease to modify or jam the signal. The third part of RFID system is data support part, which connects the RFID reader to database and is vulnerable for different types of attacks. In each one of three parts of an RFID system attackers try to break one of this three security properties:

- Confidentiality
- integrity
- Availability

Confidentiality guaranties that unauthorized hands cannot access the important information or services. Integrity ensures that information or services are not touched, altered or modified by unauthorized hands. Availability guaranties that information and/or services should be always attainable to all rightful hands. [4]According to the three general security properties in RFID systems, possible attacks can be divided in six general types:

- spoofing identity
- tempering with data
- Repudiation
- information exposure
- denial of service
- looming of privilege

[5] Spoofing occurs when an attacker successfully puts on as an authorized user of a system and so, for example can perform an inventory of a store without any authorization through the scanning the EPC tags. When the attacker modifies, adds, deletes, or reorders the data, tempering attack occurs. For example modification of the tag on the passport while, modifies EPC number on tags in the shopping mall, kills or erases a tag in supply chain. Repudiation occurs when a user denies an action and no proof exist to prove that the action was performed, for example a retailer denies receiving a certain pallet, case or item or in other example the owner of the EPC number denies having information about the item to which the tag is attacked. Information exposure happens when the information is manifested to an unauthorized user i.e., a smart bomb placed at a street corner detonates in the time that a specific person with an RFID-enable passport discovered. Denial of service occurs when the system denies service to a valid user and for performing this attack, a tag can be killed, blocked to shoplifter can take the stolen item out of the shop or removed and maybe physically destroyed. Looming of privilege occurs when an unprivileged user or attacker gains higher privilege in the system than what they are empowered for example attacker can write or add malicious data in to the system as an administrator. [6]

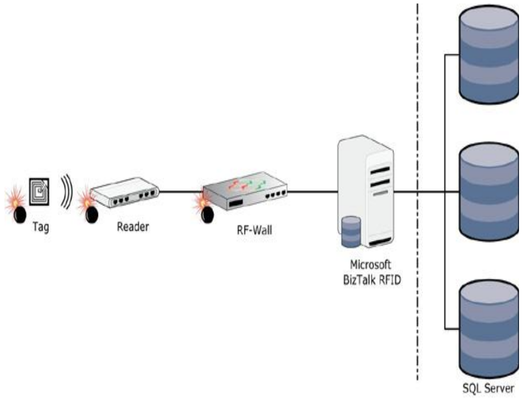


Fig 2- Communication

III. Possible Solutions

In the previous section, shows several types of attack are possible to occur in RFID systems. In this section, the most known security solutions proposed ever will be explained. [7]

- Killing the tag:

The first and easiest solution, when a tag is in the treat is to kill the tag. Each tag has a unique password, which has programed in the production time. Once the right password entered, the tag will be deactivated evermore.

- The solid cage method:

In this method, tag will be isolated from any electromagnetic waves. This can be gained by using a container made of metal mesh or foil that is impermeable by radio signals.

- Blocking a tag:

If more than one tags respond an inquiry sent by a reader, it figures out a collision, this method is used in the protocols like ALOHA and tree-walking protocols. [3]

- Classic cryptographic methods:

Cryptography algorithms and methods examples are rewritable memory, symmetric key encryption and public key encryption, which are used to keep the system secure. [7]

- Using hash function:

One of the most proposed methods for preserving the RFID system security is to use the hash function schemes like hash lock scheme, randomized hash lock scheme and hash chain scheme. [8]In addition to the named methods for maintaining RFID systems security and privacy some types of protocols like PRF private authentication scheme, tree-based private authentication, delegation tree, human protocols are proposed. [9]

IV. Conclusion

Although, today the RFID technology can be seen everywhere with different types of applications, but there are drawbacks and security issues yet that technology has not find perfect solutions for them this security issues make the society unwilling to accept the RFID systems with open arms in the case of sensitive applications like banking card. So if security and privacy problems be solved completely then the technology can guaranty the safety of the applicants curtail information which will lead to raise of the users satisfactory and of course more RFID universalization.

REFERENCES

[1] Knospe, H. and H. Pohl, RFID security. Information Security Technical Report, 2004. **9**(4): p. 39-50.

[2] LIU, L.M.N.a.Y., LANDMARKING: Indoor location Sensing Using Active RFID. Kluwer Academic Publisher. manufactured in nwtherlands, 2004. **10**: p. 10.

[3] Weinstein, R., RFID: a technical overview and its application to the enterprise. IT professional, 2005. **7**(3): p. 27-33.

[4] Mitrokotsa, A., M. Beye, and P. Peris-Lopez, Classification of RFID Threats based on Security Principles.

[5] Thompson, T., D.R., N. Chaudhry, and C.W. Thompson. RFID security threat model. in Conf. on Applied Research in Information Technology. 2006.

[6] Duc, D.N., et al. Open issues in RFID security. in Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for. 2009. IEEE.

[7] Pedro Peris-Lopez, J.C.H.-C., Juan M. Estevez-Tapiador, and Arturo Ribagorda, RFID SYSTEMS: A Survey on Security Thereats and Proposed Solutions. p. cuenca nad l. orozco-barbosa (Eds): PWC 2006, LNCS 4217, pp. 159-170, 2006

[8] Li, Y.Z., et al. Security and privacy on authentication protocol for low-cost RFID. in Computational Intelligence and Security, 2006 International Conference on. 2006. IEEE.

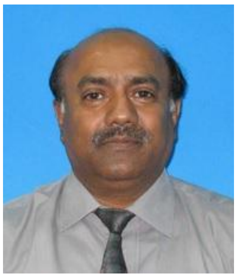
[9] IFIP international federation for information processing 2006, 2006: p. 159-170.

[10] www.digitivity.com

AUTHOR'S PROFILE

Mohsen Khosravi. He is PhD student in the Information Technology department of Information and Communication Technology (KICT) of International Islamic University Malaysia (IIUM). He has received his master of Information Technology from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India. His bachelor is software engineering from Azad university of Lahijan, Iran. His fields of interests are ADHOC, WSN and RFID that he works on it specially.

Ahmad Sharifi. He has received M.Tech in Computer Networks and Information Security from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India. In addition, he has received his bachelor in Electronic engineering from industrial university of Shahroud, Iran. Ahmad has professional experiences on technical engineering on ISP and network designs for many years. In addition, he is involving with teaching in universities. He interests in Cryptography, WSN, ADHOC, MATLAB, OPNET and other related issues. His personal website is www.ahmadsharifi.com. Furthermore, he cooperates with RIPE NCC www.ripe.net via www.sharifisp.com that is Internet Service Provider.



PROF. DR. ASADULAH SHAH.
He is Professor at Department of Computer Science, Kulliyyah of Information and Communication Technology, IIU Malaysia. Dr. Shah has a total of 24 years teaching and research experience. He has 60 research publications in International and national journals and conference proceedings. Dr. Shah has done his undergraduate degree in Electronics, Master's degree in Computer Technology from the University of Sindh, and PhD in Multimedia Communication, from the University of Surrey, England, UK. His areas of interest are multimedia compression techniques, research methodologies, speech packetization and statistical multiplexing. He has been teaching courses in the fields of electronics, computers, telecommunications and management sciences.