# "RFID Security Issues & Challenges"

Gurudatt Kulkarni,
*Rupali Shelke,*
*Lecturer in Marathwada Mitra Mandal's Polytechnic, Pune*

Ramesh Sutar
*Lecturer in Marathwada Mitra Mandal's Polytechnic, Pune*

Sangita Mohite,
*Lecturer in Dr. D.Y. Patil Polytechnic, Kolhapur*

*Abstract*:**-The deployment and use of Radio Frequency Identification (RFID) technology is growing rapidly across many different industries. Developers apply the technology not only in traditional applications such as asset or inventory tracking, but also in security services such as electronic passports and RFID-embedded credit cards. Within less than a decade, a large number of research papers dealing with security issues of RFID technology have appeared. In this paper we want to provide some thoughts on security issues concerning RFID systems and to highlight some of the areas that have to be considered regarding this topic. To deal with security and RFID means to deal not only with security aspects of RFID systems but also with security aspects of anything or anyone affected by RFID systems. The widespread dissemination of identification technology and storage devices certainly has side effects and can lead to new threats in other areas and applications.**

***Keywords:-RFID; Security; Privacy; Eavesdropping***

## I. INTRODUCTION

The significance of radio frequency identification (RFID) security is increasing explosively, leading to a research trend. The current most severe RFID security issues are privacy and authentication security. The renewable identity (ID) approach with a central database is the current dominating approach to achieve user privacy and authentication security. RFID (Radio-Frequency IDentification) is a technology for automated IDentification of objects and people. Human beings are skillful at identifying objects under a variety of challenge circumstances. A bleary-eyed person can easily pick out a cup of coffee on a cluttered breakfast table in the morning, for example. Computer vision, though, performs such tasks poorly. RFID may be viewed as a means of explicitly labeling objects to facilitate their "perception" by computing devices. RFID is expected to completely replace the bar code systems in near future. For commercial markets, RFID systems should overcome not only the restriction of cheap RFID tags but also operational and security problems such as scalability, the tracking problem and the cloning problem. In many cases, the security part is simplified in order to minimize a tags price. The technology has much potential to make life more comfortable and to provide huge savings due to increased productivity. But on the other hand, there are various requirements regarding security and privacy protection that need to be addressed properly. With the use of Internet many vulnerabilities and threats to the system security and the privacy of the users are inherited. This can be a malicious agent faking an innocent PML request over an ONS service or a disgruntled employee adding incorrect product information in the database, causing confusion and damaging the systems integrity. RFID tags may pose security and privacy risks to both organizations and individuals.[1,3]

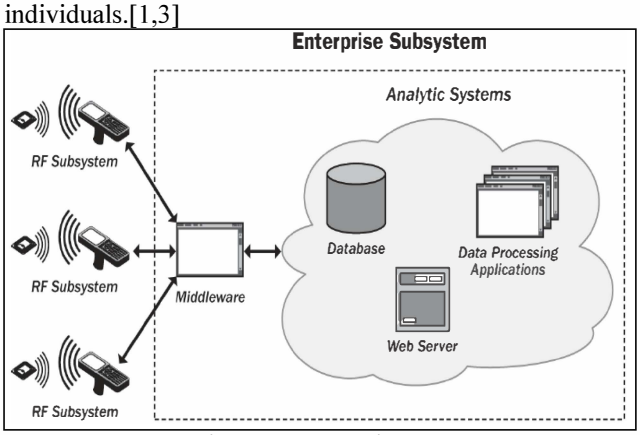


Figure 1.0 RFID Basic System

## II. SECURITY AND PRIVACY ISSUES

RFID systems, similar to other wireless technology, display a number of security and privacy risks to users; both the consumers and the manufactures. The following sections take a closer look at the security and privacy threats reacted by the use of RFID systems. It is important to note that privacy is a multi dimensional issue involving many areas such as policies, security and law enforcement agencies. Perfect Secrecy is only a mathematical concept; in reality, there will always be a human element that is difficult to quantify into any mathematical formulation. Thus, it is practically impossible to have a perfectly secure system. Once this is understood then it is possible to move onto addressing security and privacy issues shadowing RFID. It is important to understand the factors contributing to low RFID costs and the limitations placed on these low cost labels before considering the subject of security and privacy. Public acceptance of a RFID-based 'Internet of Things' depends on strong technical and operational, security and privacy solutions being in place. The security issues surrounding RFID and the challenges of providing security services, to meet the cost and interoperability requirements of the business process, with a resource limited device have been written about extensively in academic, government and industry publications. In this section we discuss only briefly the high-level system security aspects, which include some of the main challenges for the deployment of user-oriented RFID applications. [2,3]

*A. Jamming*

Jamming means a deliberate attempt to disturb the air interface between reader and tag and thereby attacking the integrity or the availability of the communication. This could be achieved by powerful transmitters at a large distance, but also through more passive means such as shielding. As the air interface is not very robust, even simple passive measures can be very effective. jamming, which paralyses the communication of an RFID system by generating a radio noise at the same frequency as that used by the system.

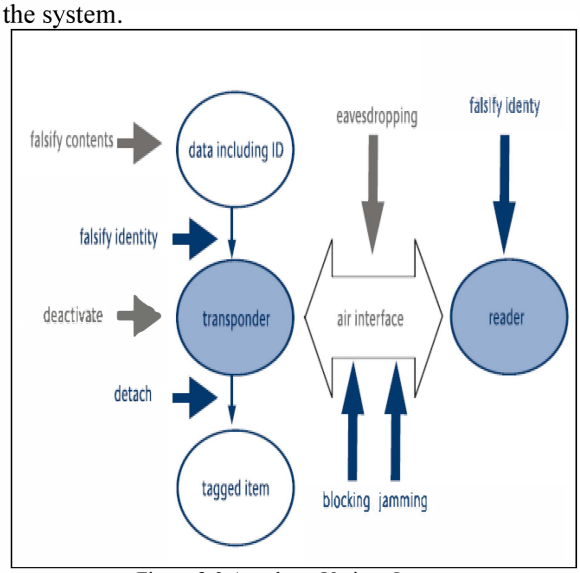


Figure 2.0 Attacks at Various Layers

*B. Eavesdropping*

Since an RFID tag is a wireless device that emits data, usually a unique identifier, when interrogated by an RFID reader, there exists a risk that the communication between tag and reader can be eavesdropped. Eavesdropping occurs when an attacker intercepts data with a compliant reader—one for the correct tag family and frequency—while a tag is being read by an authorized RFID reader. Since most RFID systems use clear text communication, due to tag memory capacity or cost, eavesdropping is a simple but efficient means for the attacker to obtain information on the collected tag data. The information picked up during the attack can have serious implications it can be used in subsequent attacks against the RFID system. The communication between reader and transponder via the air interface is monitored by intercepting and decoding the radio signals. This is one of the most specific threats to RFID systems. The eavesdropped information could for example be used to collect privacy sensitive information about a person. It could also be used to perform a replay attack, i.e. the attacker records all communicated messages and later on can either simulate this tag towards the reader, or simulate this reader towards the tag.

*C. Replay attack*

In the case of replay attack, the attacker abuses another person's identity by repeating the same authentication sequence as the one provided by an authorized person. A replay attack may be led by a clone of the legitimate tag or by re-sending the eavesdropped signal from a PC equipped with an appropriate card and antenna. In order to perform a replay attack, an attacker has to obtain some information which is sent by the tag during normal communication. The first line of defense is therefore to counter eavesdropping and unauthorized tag reading. A specific countermeasure against replay attack is authentication of the tag e.g. with a challenge response protocol. If the protocol is well designed, the key necessary for calculation

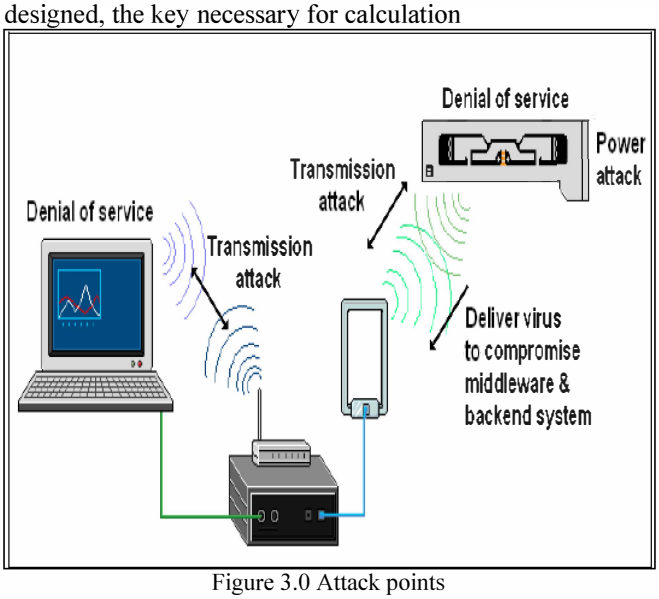


Figure 3.0 Attack points

*D. Deactivation*

This type of attack renders the transponder useless through the unauthorized application of delete commands or kill commands, or through physical destruction. Depending on the type of deactivation, the reader can either no longer detect the identity of the tag, or it cannot even detect the presence of the tag in the reading range.

*A. Detaching the tag*

A transponder is separated physically from the tagged item and may subsequently be associated with a different item, in the same way that price tags are "switched". Since RFID systems are completely dependent on the unambiguous identification of the tagged items by the transponders, this type of attack poses a fundamental security problem, even though it may appear trivial at first sight. [5,7]

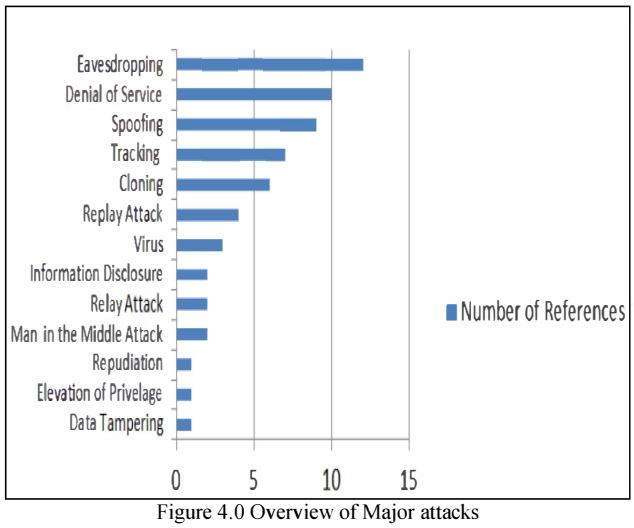


Figure 4.0 Overview of Major attacks

*B. Spoofing*

Spoofing is defined as duplicating tag data and transmitting it to a reader. Data acquired from a tag, by whatever means, is transmitted to a reader to mimic a legitimate source. For example, for an electronic seal, a threat that defines Spoofing is where the e-seal information is transmitted to the reader from some alternative source that is not the original e-seal. If the security protocol used in the RFID channel is revealed, attackers can write blank RFID tags with the same formatted data that has been collected. For instance, dishonest persons could replace the RFID tag on an item to get a cheaper price when checking out from a supermarket. Spoofing is defined as duplicating tag data and transmitting it to a reader. Data acquired from a tag, by whatever means, is transmitted to a reader to mimic a legitimate source. For example, for an electronic seal, a threat that defines spoofing is where the e-seal information is transmitted to the reader from some alternative source that is not the original e-seal. [9]

*A. Man-in-the-middle attack*

Depending on the system configuration, a man-in-the-middle (MITM) attack is possible while the data is in transit from one component to another. An attacker can interrupt the communication path and manipulate the information back and forth between RFID components. This is a real-time threat. The attack reveals the information before the intended device receives it and can change the information en route (Welch & Lathrop, 2003). Even if it received some invalid data, the system being attacked might assume the problem was caused by network errors and would not recognize that an attack occurred. An RFID system is particularly vulnerable to MITM attacks because the tags are small in size and low in price, all of which means that there is generally a lack of sophisticated protection circuitry. [4,7]

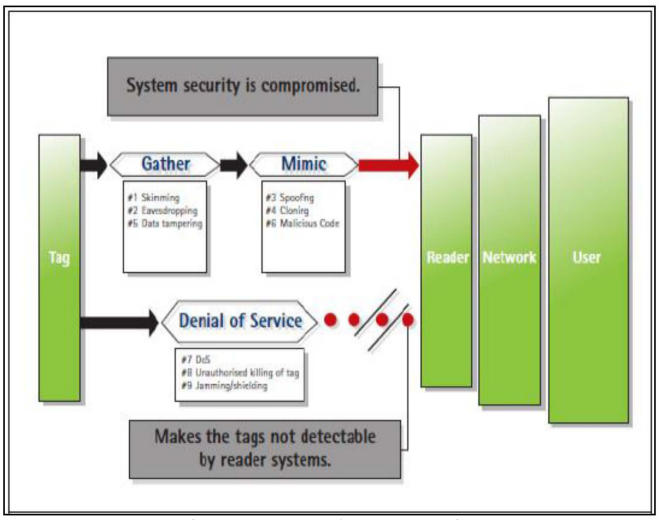


Figure 5.0 RFID Threat Categories

*B. Cloning*

Tag cloning is a process that first captures the data from a legitimate tag and then creates an unauthorized copy of the captured sample on a new chip. Researchers from Johns Hopkins University and RSA Labs published experimental results of cloning a cryptographically protected Texas Instruments digital signature transponder (DST) that was used to buy gasoline and activate a car's ignition. Cloning is a threat frequently categorized together with spoofing. However spoofing and cloning are not the same. Although both threats copy data from a legitimate tag, spoofing emulates the transmission of tag data while cloning means that the copied data is transferred onto a new tag owned by the attacker. Just as spoofing, the communication between legit RFID tags and readers will have to be read and stored, but a tag could also be stolen and then physically read. The data for the cloned tags are then altered to suit to the needs of the desired attack and copied onto an empty tag. The cloned tag is then inserted into a RFID system to perform the planned attack.

## III. CONCLUSION

It is possible that RFID tags revolutionize society. While bringing to fruition their convenience, we must understand their risks also. Implementing ubiquitous network connectivity in society will demand a close examination of personal privacy from both the technical and social aspects. Safety is one of the most important issues of communication systems, especially for wireless communication systems which use insecure wireless channel to communicate with each other. InRFID systems, data transmission between tags and readers or sometimes even data transmission between readers and back-end database uses the wireless channel. It is clear that RFID looks like a better candidate for various applications like, smart appliances, shopping, medication compliance, passports, libraries; toll- payment transponders etc. than the well establish barcode system. But due to its cost and resource constraint limitations, it does not have a sufficient security and privacy support. Presently, many researcher and scientist work to implement lightweight low

cost security and privacy protocol to increase the applicability.

REFERENCES


1. ”Specification of RFID Air Interface”, http://www.epcglobaline.org.
2. Bereford and F. Stajano, (2003), “Location Privacy in Pervasive Computing”, IEEE Pervasive Computing, Vol. 2, No. 1, pp 46-55.
3. Q. Z. Sheng , X. Li and S. Zeadally "Enabling next-generation RFID applications: Solutions and challenges", Computer, vol.41, no. 9, pp.21 -28 2008
4. Adriana Alxandru, Eleonora Tudora, Ovidiu Bica "Use of RFID Technology for Identification, Traceability, Monitoring and Checking of Product Authenticity" World Academy of Sciences, Engineering and Technology, Issue 71, November 2010, pp. 765-769.
5. Tieyan Li "Employing Lightweight Primitives on Low-cost RFID Tags for Authentication", IEEE VTC 2008 Fall.
6. Mitrokotsa, M.R. Rieback and A.S. Tanenbaum. Classifying RFID Attacks and Defences. Information Systems Frontiers, Springer, July 2009.
7. Juels. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, pp381-394, February 2006.
8. Divyan M. Konidala, Daeyoung Kim, Chan Yeob Yeun, Byoungcheon Lee "Security Framework for RFID-based Applications in Smart Home Environment" Journal of Information Processing Systems, Volume 7, March 2011, pp. 111-120
9. Garfinkel, S. & Rosenberg, B. (2005). RFID: Applications, Security, and Privacy, Addison-Wesley Professional, ISBN:0321290968, Boston, MA.