Various Attacks and their Countermeasure on all layers of RFID System

Gursewak Singh, Rajveer Kaur, Himanshu Sharma

Abstract— RFID (radio frequency identification) system is one of the most widely used technologies due to its broad applicability and low cost. RFID systems have various advantages but still it is prone to various attacks which try to degrade the performance of the system. As RFID system is a low cost system so security become much more challenging, because as we know the usual security mechanisms are infeasible to use on low cost tags due to their resource constrains so in this paper we present some countermeasure to prevent the attacks. The main goal of this paper is to easily define individually layers attacks and their procedure to prevent them.

Index Terms—RFID, countermeasures, tags, reader, attacks, layers.

I. INTRODUCTION

RFID (Radio frequency identification) is a technology that uses radio waves to offer automatic identification of objects and people. A RFID system consist of tag or transponder which is small RFID chip coupled to a microprocessor which wirelessly communicate with an RFID reader. In RFID the data is stored and retrieved remotely by using radio waves. RFID network is widespread in large areas and so the attacker take it as the new area to steal the information because it is easy for them to attack a wireless network then the wired network. As compared to traditional barcode identification technology, RFID are more preferable and efficient they do not need to focus the light of sight to access data, such as they have ability to communicate with multiple tags with readers that have a larger read range. RFID technology has the potential to provide automated data acquisition and analysis system, enable visibility of the environment in which the tracking is not possible, provide better asset utilization and in this way optimize and improving the operational efficiency of the system. Due to the multitudinous advantages, RFID is deployed in various applications, such as inventory tracking, warehouse management, homeland security, healthcare monitoring, and supply chain management.[1]

However, with the increasing popularity of RFID, Security and privacy issues are concentrated in a number of serious challenges to RFID applications. RFID tags are of two types active tag- it has a battery and send its ID periodically. Passive tag- it does not have battery, it uses the energy send by the reader as its source energy.

Almost all real time applications used RFID tags. RFID tags have some layers and each layer is prone to some attacks. The RFID system is permeable to a broad range of attacks ranging from a passive to active interface.

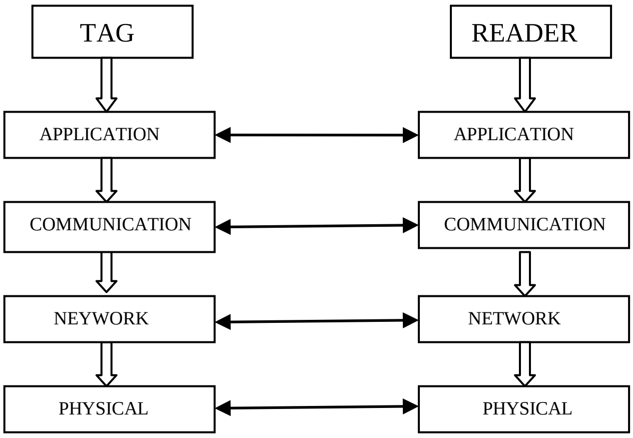

Fig 1. RFID layers communication

In this paper we will structure the most generic RFID attacks into RFID layers which are related but not identical to ISO layers [1, 6, and 7]. The layers of RFID communication is shown in figure1. This paper is classified as follows: part 2 discusses the physical layer attack and part 3 discusses the network layer attacks and part 4 covers the application layer attacks and part 5 discusses the strategic and multilayer attacks and part 6 covers the countermeasures for all layers and part 7concludes the paper.

II. ATTACKS ON RFID LAYERS

A. Physical Layer

The physical layer in RFID is having physical interface and the RFID devices. As the communication takes place over the wireless network, the attacker can attack the wireless nature of the RFID communication and can attack because of poor physical security over the network and of insufficient resilience against physical manipulation. The attacks that come under physical layer are, temporarily disabling tag, permanently disabling tag and relay attacks, these three further have categories.

Manuscript received on March, 2013.

Gursewak Singh, computer science and engineering department, Lovely professional university, phagwara, India.
Rajveer Kaur computer science and engineering department, Lovely professional university, phagwara, India.
Himanshu Sharma, computer science and engineering department, Lovely professional university, phagwara, India.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

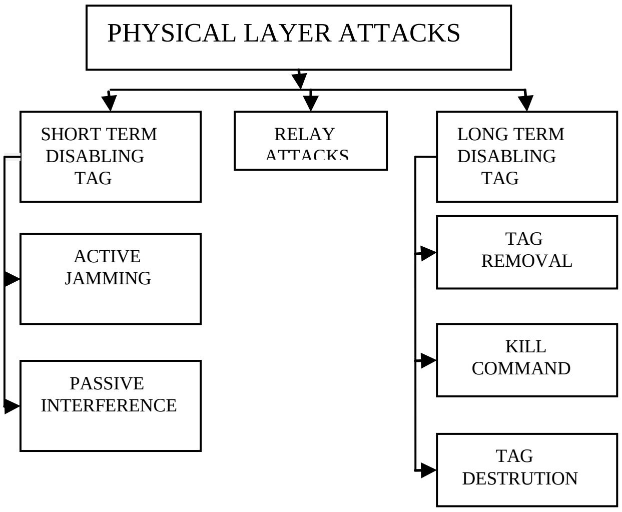

Fig 2. Physical layer attacks

1.1 Short term disabling tag

In Short term disabling tag, the attacker can use an aluminum foil lined bag, so that he can shield it from electromagnetic waves and can steal any product without disturbing. The attacker can also temporarily disabled the tag by covered it with ice or with some other ways. Short term disabling tags can be either passive or active

- Active jamming

In this the attacker cause electromagnetic jamming by sending the same radio signal as the reader was expecting or waiting for, in order to prevent the original tags from communicating with reader.

- Passive Interference

As the RFID network operates in a noisy and unstable environment, so there is interference and collision occur from any radio source. This type of interference prevents secure and efficient communication.

1.2 Relay attacks

In relay attacks, the attacker act as man in the middle, he placed his tag and the reader. The device can be able to modify the radio signal between device in between the reader and tag and can read all the information. The attacker can fooled the tag and reader by sending his radio signal, as the reader and tag thought they are exchanging information with each other, but in reality they both exchange information with the attacker. To use this attack more easily, the attacker can use two different devices, one for the reader and one for the tag.

1.3 Long term disabling tag

In this type, the attacker adopts all possible ways to permanently destroying the tag or permanently degrading the operation of RFID tag.

- Kill command

There is a scheme known as Auto-ID centre and EPC global, they created KILL command. According to which we can permanently destroy the RFID tag. as each RFID tag has a unique password, which is given by the manufacturer when he build the tag and attacker can use it for permanently disabling tag.[2]

- Tag removal

In tag removal the tag can be removed from one item and can be placed on another item due to poor physical security of RFID tag. For example, in a mall the attacker can remove the tag from expensive item and can placed on cheaper one and can buy the thing with less charge.

- Tag destruction

Sometimes the attacker intentionally destroys the tag just to annoy people or to create noise. The RFID tags can be affected by environmental conditions also, for example too high or too low temperature or by rough handling.

B. Network-transport layer

This layer has all the attacks in which the attacker attacks the communication between the RFID tag and reader and the data transferred between them. From the name we can make guess that what type of attacks will be there, that will attack on the transfer of data.

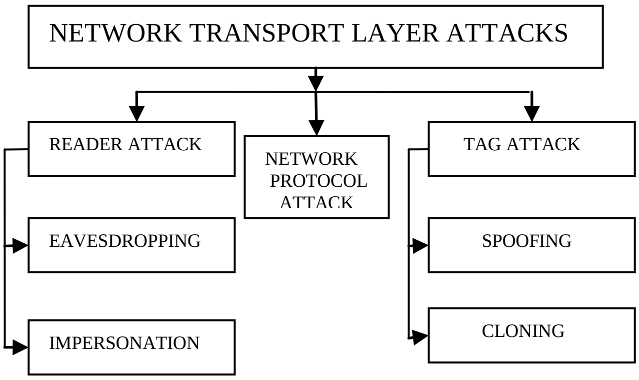

Fig 3. Network transport layer attacks

2.1 Reader attacks

- Eavesdropping

Eavesdropping is the most widely used attack, in this the attacker placed an antenna to record the communication between the tag and reader, it records data from both sides i.e. from reader to tag and from tag to reader. The reader to tag is more prone to eavesdropping as they transmit information at higher distance and to a greater degree.

- Impersonation

In some cases, RFID communication is not secured as they not use any authentication protocol for secured communication, so it is easy for the attacker to attack the data

2.2 Network protocol attacks

In network protocol attacks, the attacker takes advantages of the poor protocol and operating system to attack the back end database.

2.3 Tag attacks

- Spoofing

It is the variant of cloning, but in this the attacker directly attacks the valid RFID tag, access the data. For direct attack, the attacker needs full access to the original communication channel, so he needs the knowledge of the protocols used and the authentication procedure.

- Cloning

Cloning, the attacker makes the copy of the original tag to access the information between the reader and the tag by replacing the clone with the original tag.

C. Application layer

This layer includes the attacks on application and on the interaction between user and RFID tags. The attacker can do unauthorized tag reading, modification of tag data etc.

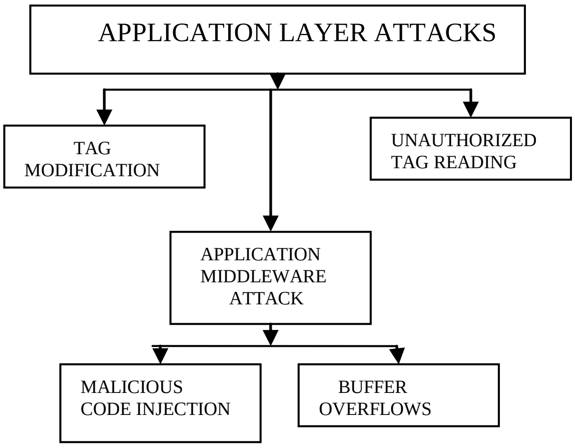

Fig 4. Application layer attacks

3.1 Tag modification

Tag modification cause the attacker to modify the important data inside the tag and send that data to the reader. As most of the RFID tags use writeable memory, so the attacker takes advantages of this.

The attacker modify the data and send to the reader as the correct data.

3.2 Application middleware attacks

- Malicious code injection

In this the attacker uses the memory space of RFID tags to keep the infective viruses. The attacker uses the RFID tags to infect other sources of the RFID network like reader and connecting networks [9]. As middleware use scripting language like PHP, XML, JavaScript etc, an attacker can add malicious code to affect the middleware systems. The code injection cause the unauthorized data reading or back end data base and even can modify the stored data to affect the middleware layer.

- Buffer overflows

Buffer overflows cause the data or code to exceed beyond the fixed length of buffer. The RFID tags are used by the attacker to use buffer overflow on the back end RFID middleware [9]. The attacker keeps on sending the same data repetitively to overflow the buffer at the back end. Buffer overflow is considered as the one of the most dangerous threat. buffer overflow is the major threat among the hardest security problems in software.

3.3 Unauthorized tag reading

The attacker takes help of same protocol for unauthorized tag reading. The attacker can easily read the tag without any interruption in the working of reader and tag and they are unaware about this. in this the attacker read the content of the tag by some unauthorized external reader or duplicate from the system, he may follow the same reading protocol, so the risk depend upon the external elements of the system.

D. Static and Multilayer Attacks

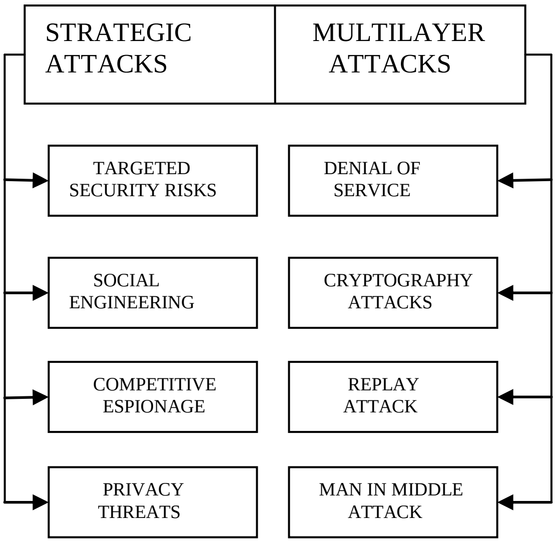

Fig 5. Strategic and Multi layer attacks

4.1 Static Layer Attacks

Static layer attacks also focused on the companies and Business Applications. In static layers the attacker taking the benefit of the negligent design of infrastructure and applications. Peculiarly in this layer included Targeted security risks, social engineering and competitive espionage and privacy threats. We describe these Risks and their effects.

- Targeted Security Risks

Targets Security Risks are the one type of static attacks. These are threats that target a class of malware destined for a specific organization or industry. These threats are design to capture sensitive information. It may include the attacks is delivered via a port attacks, phishing message, SMTP email etc.

- Social Engineering

In Social engineering the attacker use the social engineering skills to understanding the RFID system and unauthorized access to restricted information. Social engineering is used for hacking or cracking the RFID system in this the attacker uses his confidence trick to manipulate people into disclosure confidential information. It is similar to a simple fraud. Typically it is a trickery fraud for the purpose of information gathering and access RFID system.

- Competitive Espionage

Competitive Espionage is a type of static layer attack. This attack is mostly occurring in business and industry applications. The simple example of competitive espionage attack when your business discovers success then it will be attacked. In this attack the attacker has ability to exploit the track and detect tagged items and may gather the critical and secret information in order to sabotage their rivals. And this information includes the product schedule and marketing information of any industry.

- Privacy Threats

In the RFID system, the RFID tag responds to any reader either it is authorized or unauthorized without sending any identification about that to their owner.

Due to this the attacker can easily detect the information about the tag. Privacy threats arise mainly from the fact that objects can be tagged to the outside world has brought with tags functioning, if they are not disabled or removed in the security zone and these objects can be tagged actively eavesdropped violate your privacy. It does not look like other attacks (ex DOS) it affect people privacy. This attack generally affects the action, association and location and transactions of the RFID system.

4.2 Multilayer Attack

Many attacks in RFID system target more than one layer. Those attacks are considered in multilayer attacks. It includes denial of service, crypto attacks, replay attacks, man in middle attacks. We describe these attacks and their affects.

- Denial of Service

Denial of service attacks are easy to complete and are difficult to defend. Denial of service attack is affects many real time applications like supply chain, warehouse etc. In this the attacker kills the tag. The attack causes a tag to assume a state from its normal operating. The tag become temporarily or permanently incapacitated. For instance the tag reader state can be desynchronized or tag readings can be hinted by signal jamming. A significant fraction of tag population will severely affect RFID system survivability.

- Cryptography Attacks

The important information is stored in RFID tags and the encryption and decryption technique are used to protect this data. These techniques provide the confidentiality and integrity. For this different types of cryptography algorithm are applied on the RFID system. In this attack the attacker break these algorithms and try to get the data which is store in a tag. Brute force attack is mostly use in cryptography to break the encrypted algorithms.

- Replay Attack

In RFID system the tag and reader are share their information using different protocols. In this the attacker recorded the past transactions of the tag and intercepts the communication between the tag and reader. It takes the data from tag and modified it and sent to the reader and again receives the reader response and sent to the tag. Even if the information is encrypted, the attacker replays the login information to fool the RFID system and gains access.

- Man in Middle Attack

Man in middle attack intercepts the communication between the RFID tag and RFID reader. In this a malicious entity intercept between an RFID reader and tag by falsely claiming to be authentic reader and or the tag.

III. COUNTERMEASURES FOR ALL LAYERS

A. Physical layer

To prevent physical layer attacks like permanently disabling tag, we have to increase the physical security with guards, locked doors, cameras and gates etc. so some attacks can be controlled by use of aluminum foil lined bags [8]. Tag removal can be controlled by using strong glue or by embedding tag in product. Radio waves interruption can be controlled by opaque walls. With effective or secured passwords usage, the KILL command can be prevented. The relay attacks can be controlled by encrypting the RFID communication or by using passwords.

B. Network-transport layer

The cloning can be prevented by using challenge response authentication protocol and by appropriate data collection. With the help of encrypting RFID communication mechanism, we can defend eavesdropping. Authentication protocols can also prevent spoofing and impersonation, we can also use passwords and PIN codes. To prevent network protocols from being attacked by attackers, we can use secure operating system. We have to replace the insecure protocols with the secure one to prevent the attacks.

C. Application layer

We have to control the accessing of RFID tags to prevent unauthorized tag reading and tag modification. There was an approach in which they use aluminum lined based wallet to protect RFID payment cards and e-passports. However the use of encryption, hash functions, mutual authentication etc can protect the application layer from attackers. We have to perform regular code review to defend buffer overflow and malicious code injection; regular security checks can also prevent the attacks.

D. Strategic Layer

To control the threats or to increase the security we have to kill the targeted tag or to temporarily stop using them and to block unauthorized readers. Various encryption techniques can help in controlling attacks. It is the duty of the organization that is using RFID system to maintain privacy and to follow some policies to control threats [10]. All the employees in the organization should have knowledge about the policies and have to maintain the same. Regular training to the employees about the policies should be there.

E. Multilayer

As we know that the covert channels attacks are not easy to detect and to prevent because the owner and user of the RFID tags don not know that there tags have been attacked by the attackers by covert channel attack. Clearing the unused memory can help in some cases. Denial of service and man in middle attacks are severe attacks in both networks wired and wireless network. Cryptography attacks can be controlled by using strong and secure cryptography algorithms and by using a key with sufficient length. The use of timestamps, challenges response cryptography and one time password can prevent the replay RFID attacks.

IV. CONCLUSION

In this paper we identified various layers attacks and also defined their countermeasure. Also we defined how we can prevent some attacks with safe handling. We can get a more coherent view of the threats and the techniques how to overcome them. We layer wise defined the attacks and the possible ways to counter them. Physical layer have more attacks than other layers so we have to make the physical environment more secure. Some attacks need more research like denial of service and man in middle attack.

REFERENCES

1. G. P Rotter, “A Framework for assessing RFID system security and privacy risks.”IEEE pervasive computing, vol. 7, no 2, pp,70-77, 200
2. Center, A.I:900MHz class 0 radio frequencies (RF) Identification Tag Specification. In: Draft, www.epcglobalinc.org/standards.org/standards/specs/900_Mhz_class_0_RFIDtag_specification.pdf,(2003).
3. Shepard, RFID: Radio Frequency Identification. NewYork:Mc-Graw-Hill, 2005
4. A. Juels, “RFID security and privacy: A research survey,” IEEE J. Sel.Areas Commun., vol. 24, no. 2, pp. 381–394, Feb. 2006.
5. J. Ayoade, “Roadmap to solving security and privacy concerns in RFIDsystems,” Comput. Law Security Rep., vol. 23, pp. 555–561, Sep. 2007.
6. Garfinkel, S., Juels, A., Pappu, R.: RFID Privacy: An Overview of Problems and ProposedSolutions. In: IEEE Security & Privacy, Vol. 3. (2005) 34–43
7. Karygiannis, A., Phillips, T., Tsibertzopoulos, A.: RFID Security: A Taxonomy of Risk. In:Proc. of China’Com ’06. (2006) 1-8.
8. Karygiannis, T., Eydt, B., Barber, G., Bunn, L., Phillips, T.: Guidelines for Securing Radio Frequency Identification (RFID) Systems. In: NIST Special Publication 800-98, National Institute of Standards and Tecnology (2007)
9. Rieback, M.R., Bruno, B., Tanenbaum, A.S. Is Your Cat Infected with a Computer Virus?In: Proc. of the 4th IEEE Int’l Conf. on Pervasive Computing and Communications. (2006).
10. Juels, A., Rivest, R.,Szydlo,M.: The Blocker Tag: Selective Blocking of RFID Tags for ConsumerPrivacy. In: Proc. of the 10th ACM Conf. on Computer and Communication Security.(2003) 103–111

AUTHORS PROFILE

Gursewak Singh, Received the B.Tech degree in computer science engineering from Punjab technical university, India, in 2011. He is currently doing M.Tech degree in computer science and engineering at lovely professional university, India. His research interest includes RFID (radio frequency identification), Security analysis of RFID system and Cryptography algorithms for RFID, key redistribution schemes and Security schemes in wireless sensor networks.

Rajveer Kaur, Received the B.Tech degree in computer science engineering from Punjab technical university, India, in 2010. She is currently doing M.Tech degree in computer science and engineering at lovely professional university, India. Her research interest includes wireless sensor networks, Mathematical modeling and security of RFID (radio frequency identification) system and network security protocol design.

Himashu Sharma, Received the M.tech degree in computer science and engineering from lovely professional university in 2011, India. She is an associate professor with the Department of computer science and engineering at Lovely professional university, India. Her research interest is in wireless sensor networks and security, RFID security and multimedia processing. She is an author/coauthor of more than six research papers in referred international journals/conference.