Survey on Enhancing Security for RFID Smart Cards

Shilpa S. Badhiye[1]Prof.Rupali S. Khule[2]
[1] student, Electronics and telecommunication Department, MCOERC, Maharashtra, India
[2] Professor, Electronics and telecommunication Department, MCOERC, Maharashtra, India

ABSTRACT

Unauthorized money transaction is a very big problem. The main aim of the proposed system is to build a system that defends against unauthorized transaction in RFID. Although a variety of security solutions exist, many of them do not meet the constraints and requirements in terms of efficiency, security, and usability. In an attempt to address these drawbacks, the proposed system is used to overcome this. In the proposed system on the server side a secure transaction verification scheme is designed which decides whether to approve payment or block the card. Many researchers proposed different techniques for unauthorized transaction but all of them required some auxiliary devices to carry with users. In the proposed work there is an interrogation session between reader and user with addition of extra security for secure transaction and according to the behavior of the transaction theft can be determined.

Keyword: - *RFID, unauthorized transaction, security*

---

1. INTRODUCTION

RFID is a technology which uses radio frequency to identify objects or peoples. A typical RFID system consists of tags, readers, and back-end servers. Tag consists of small microchip with an antenna attached to it. It contains identification number that store information about their corresponding subject and these information is usually sensitive. The tag will broadcast its identification number to any nearby reader and these causes threat to consumer privacy. RFID tags are sensitive to ghost and leech relay attacks. In this type of an attack, an enemy called a ghost transfers the information secretly read from a legitimate RFID device to a leech which combine secretly to plan and prepare a harmful action[1]. The leech can then transmit the forwarded information to a corresponding reader and viceversa, thus a ghost and leech pair can succeed in attack without actually possessing the device, which distrubs the security. Therefore there is a need to work on security and privacy of RFID card. This sensitive information can be used in order to track the owner of the tag or to clone the tag. RFID cards are more durable but in RFID the credit card number and expiry date are not encrypted which presents a security problem. Due to this unauthorized reading it results in fraud. Different authors proposed different solutions for this unauthorized reading like use of blocker tag, Faradays cage, motion detection, vibrate to unlock and distance bounding protocol. All of these required some auxiliary devices to carry with users and it also affects the original usage model. In the proposed system we build a system which gives location validation and transaction verification. By using this technique we enhance the security in RFID credit card.

2. RFID SYSTEM

The smartcard consists of a sheet of plastic with an integrated circuit, normally a specialized microcontroller, mounted on the reverse of a group of eight contact pads. Current smart cards use only five contact pads i.e. ground, power, reset, clock are inputs supplied by the card reader, Smartcards are designed to operate at clock frequencies between 1and 5MHz. otherwise of 1/372 of that frequency.

2.1 RFID Tag

A tag typically consists of an electronic microchip and chip antenna designed to allow communications with a reader. Tags are of three types. Active tags, passive tags and semi-passive tags. In a passive system the tag is powered by coupling with the reader field by using electromagnetic induction called near field communication. An active tag may be totally or partially powered by its own battery supply. Tags may be designed to be read-only or to read and accept writes. Tags are typically having its unique identification number for the specific application. The transponder or 'tag' consists of a microchip and an antenna. Microchip is mounted on IC and an antenna is attached to it. A microchip is programmed with unique identification code and then is mounted with an IC on a wafer that holds assembly in place is shown in fig.1. Antenna is soldered onto IC. Mounting and soldering of antenna to the IC is done by robotic machines. RFID tag data capacity typically ranges from a few bits to few kilobytes according to the tag selected.

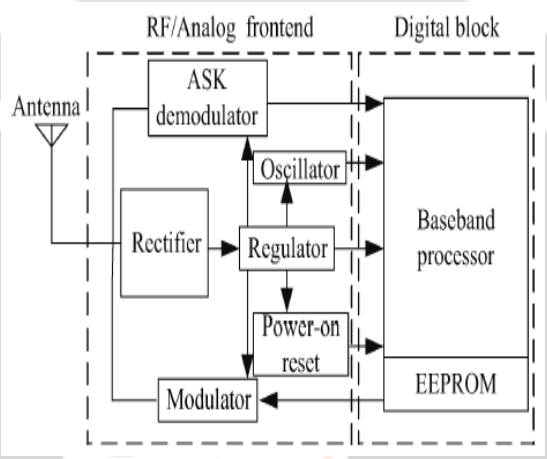

Fig -1: Block diagram of tag

One of the advantage of tag embedded RFID is the card not consists of any CVV number or card number on it, and it not require any mechanical contact to read data from it.

2.2 RFID Reader

Radio Frequency Identification (RFID) is a term used for non contacting technologies that use radio waves to automatically identify people or objects.

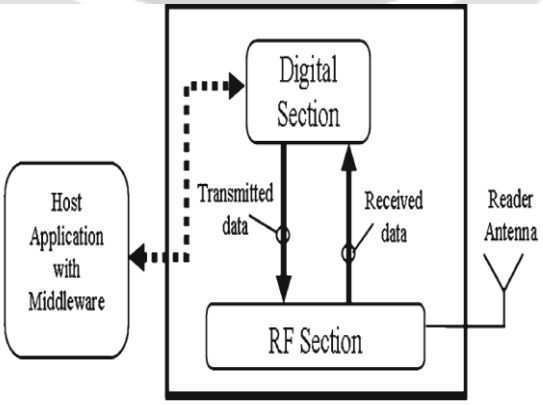

Fig -2: Block Diagram of RFID Reader

The digital section of the RFID reader performs digital signal processing over the received data from the RFID transponder. This section usually consists of a microprocessor, a memory block, a few analogue-to-digital converters (ADCs) and a communication block for the software application as shown in fig. 2.

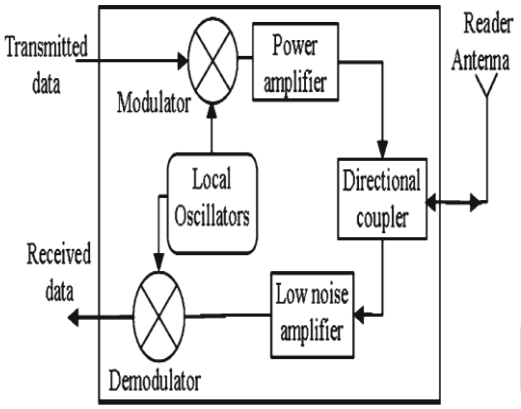

Fig -3: Block Diagram of RF Section of RFID Reader

The reader's RF section is used for RF signal transmission and reception and consists of two separate signal paths to correspond with the two directional data flows. The local oscillator generates the RF carrier signal, a modulator modulates the signal, the modulated signal is amplified by the power amplifier, and the amplified signal is transmitted through the antenna. A directional coupler separates the system's transmitted signal and the received weak back-scattered signal from the tag. The weak back-scattered signal is amplified using low noise amplifiers (LNA) before the signal is decoded in the demodulator as shown in fig 3.Different demodulation techniques are used when decoding the data received from the transponder. Most RF sections are protected from EM interference using metal cages. The radio waves returned from the RFID tag into a form that can be passed on to Controllers, which can make use of it. RFID tags and readers have to be tuned to the same frequency in order to communicate. RFID systems use many different frequencies, but the most common and widely used & required for the proposed work is 125 KHz. i.e. Low frequency. The TTL RS-232 Interface cannot be connected directly to a PC COM port Therefore the signal must be converted to RS 232 level for PC connection.

3. LITERATURE SURVEY

3.1 Hardware Based Selective unlocking

Hardware-based selective unlocking schemes have been proposed previously. These include blocker Tag, RFID Enhancer Proxy, RFID Guardian, and Vibrate-to-Unlock.

3.1.1 Blocker Tag

In blocker Tag, [3] a special RFID tag, called "blocker," is used to interrupt the flow of identification process used by the reader to identify tags that are closer to it. The use of selective blocking by blocker tags used as a way of protecting consumers from unwanted scanning of RFID tags attached to items they may be carrying or wearing. When blocker tag carried by a consumer, it blocks RFID readers or a blocker tag can block selectively by simulating only selected subsets of ID codes, such as those by a particular manufacturer, or those in a designated privacy zone. The operation of a basic blocker tag is quite simple. It simulates the full set of 2k possible RFID-tag serial numbers. Whenever the reader queries tags the blocker tag simultaneously broadcasts both a '0' bit and a '1' bit. This forced collision drives the reader to recur on all nodes, causing the reader to explore the entire tree. If the reader had enough time, memory, and processing power to complete the tree-walking algorithm in these circumstances, it

would output the entire set of all 2k possible tag serial numbers. In practice, therefore, the reader may be expected to stall after reaching only a few hundred leaves in the tree. The net effect is that the full blocker tag "blocks" the reading of all tags. The blocker tag can be refined so as to simulate and therefore effectively block just a subset of tags we call such a blocker a partial blocker tag or a selective blocker tag. For example, a selective blocker might reply to the reader only during execution of the tree-walking in the left subtree of the root. This selective-blocking feature would have the effect of obstructing only the reading of tags that bear a'0' prefix in their serial numbers. Tags that begin with a'1' bit could be read without interference. In this manner, the selective blocker tag can target a particular zone for protection. Indeed, a selective blocker tag may be easily and inexpensively created so as to block reading of all tags with an arbitrary prefix or small set of prefixes. (More generally, a selective blocker tag may be designed to simulate and thus block the reading of serial numbers satisfying any of a number of simple conditions) In fig.4 each tag has a three-bit serial number, corresponding to a leaf in this depth-three binary tree. The tree-walking singulation protocol corresponds to a depth-first search of this tree, restricted to the leaves/ID in use and their ancestors.

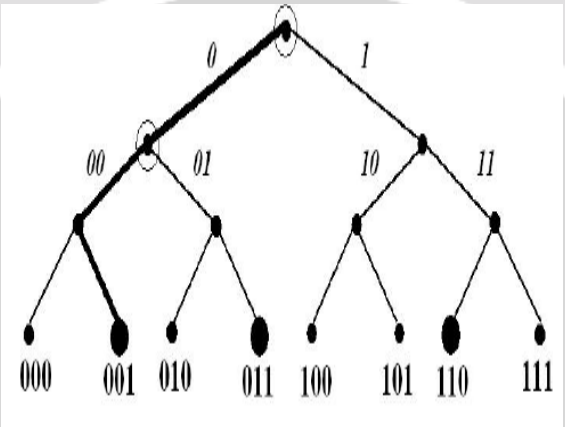

Fig -: 4 Tree-walking Algorithm

Limitations of blocker tags are as follows

(1) If a tag temporarily exits the broadcast range of a blocker, it is subject to complete compromise.

(2) Blocker tags can only be effective as a universal standard implemented on both tags and readers.

3.1.2 RFID Enhancer Proxy

RFID enhancer proxy (REP) [4] assumes the identities of tags and simulates them by proxy. By merit of its greater computing power, the REP can enforce more sophisticated privacy policies than those available in tags. It can also provide more flexible and reliable communications in RFID systems.REP helps to prevent malicious attack, even when tags do not have access-control features [4]. A REP must perform four different operations:

1. Tag acquisition

When the owner of a REP and RFID tag wishes the REP to simulate the tag, the REP must acquire all of the necessary tag information and place the tag in a state permitting the REP to act as its proxy. Acquisition of a tag by a REP involves transfer of the complete set of tag data or tags that simply broadcast identifiers and other public information. The REP need merely (better than what is specified or no more) scan the tag. Where it becomes more complicated is when a tag has associated secrets, particularly PINs required to implement secure tag operations such as writing and "killing."

2. Tag relabeling (or re-encryption)

The REP changes the identifiers on tags in its control so as to prevent close observations of these tags. Relabeling introduces various integrity problems, particularly the need to prevent adversarial re-writing of tags. Example is swapping the identifiers on two medications with differing dosages. It involves random input from the tag in the creation of pseudonyms, works even when tags do not have access-control features.

3. Tag simulation

Once the REP has acquired a tag, it can, simulate it as desired in the presence of an RFID reader, has the benefit of making tag reading more reliable. The REP, as a higher-powered device can transmit information to a reader more reliably than a tag. A REP, by contrast, can achieve a wholly personalized set of privacy policies. Additionally, a REP can enforce these policies in the presence of any reader even a malicious one. A REP may make decisions about whether to release information based on its geographical location. For example, a REP might release information about a pallet's RFID tags only when the pallet arrives at its destination. There is a variety of channels by which the REP might determine whether or not it is present at its destination.

4. Tag release

When the owner of a REP wishes it no longer to simulate a tag, the REP must release its control and it must restore the tag's original identity.

3.1.3 RFID Guardian

A RFID Guardian [5] is a compact, portable, electronic device which people can carry with them. The RFID Guardian looks for, records, and displays all RFID tags and scans in the vicinity, manages RFID keys, authenticates nearby RFID readers, and blocks attempted accesses to the user's RFID tags from unauthorized readers. In this way, people can find out what RFID activity is occurring around them and take corrective action if need be. The RFID Guardian is a platform that offers centralized RFID security and privacy management for individual people. The idea is that consumer who wants to enjoy the benefits of RFID-tagging, while still protecting their privacy, can carry a battery-powered mobile device that monitors and regulates their RFID usage. The RFID guardian is meant for personal use; it manages the RFID tags within physical proximity of a person (as opposed to managing RFID tags owned by the persons, who are left at home). For this reason, the operating range of the RFID Guardian must extend at least from the head to toe of the user; a radius of 1-2 meters should be sufficient. This full-body coverage requires the RFID Guardian to be portable. It should be PDA-sized, or better yet, could be integrated into a handheld computer or cell phone. The RFID Guardian could then occupy a vacant shirt pocket, handbag, or belt loop, and thus remain close to the person that it is supposed to protect. The RFID Guardian is also battery powered. This is necessary to perform resource-intensive security protocols, such as authentication and access control, which would not be possible if the RFID Guardian was implemented on a passive device, like an RFID tag. The RFID Guardian also performs 2-way RFID communications. It acts like an RFID reader, querying tags and decoding the tag responses. But far more interestingly, the RFID Guardian can also emulate an RFID tag, allowing it to perform direct in-band communications with other RFID readers. As we will see later, this tag emulation capability allows the RFID Guardian to perform security protocols directly with RFID readers. The heart of the RFID Guardian is that it integrates four previously separate security properties into a single device:

- Auditing
- Key management
- Access control

- Authentication

Limitations of RFID guardian:

Anyone who compromises the Guardian has total control over the RFID tags, whether it is lost or taken over by a hostile entity. This can be improved by using PIN codes to lock the device, and synchronizing the information on the RFID Guardian with trusted location (e.g. home-based) RFID systems.

3.1.4Vibrate-to-Unlock

Vibrate to unlock mechanism [6] allows users to control when and where their RFID tags can be accessed. In this technique a user unlocks his/her RFID tags by authenticating to these tags through a vibrating phone. However, such an auxiliary device may not be available at the time of accessing RFID tags, and users may not be willing to always carry these devices.

3.2 Cryptographic protocols

Cryptographic reader-to-tag authentication protocols could also be used to defend against unauthorized reading. However, due to their computational complexity and high-bandwidth requirements, many of these protocols are still unworkable even on high-end tags. However, these protocols usually require shared key(s) between tags and readers, which is not an option in some applications. However it requires secure association between tags and readers.

3.2.1 Distance Bounding Protocols

A distance bounding protocol [2] is a cryptographic challenge response authentication protocol. Hence, it requires shared key(s) between tags and readers as other cryptographic protocols. Besides authentication, a distance bounding protocol allows the verifier to measure an upper bound of its distance from the prover. (Normal "non-distance-bounding" cryptographic authentication protocols are completely ineffective in defending against relay attacks.) Using this protocol, a valid RFID reader can verify whether the valid tag is within a close proximity thereby detecting ghost-and leech and reader-and-ghost relay attacks. The upper bound calculated by an RF distance bounding Protocol, however, is very sensitive to processing delay (the time used to generate the response) at the prover side. This is because a slight delay (of the orders of a few nanoseconds) may result in a significant error in distance bounding. Because of this strict delay requirement, even XOR or comparison-based distance bounding protocols are not suitable for RF distance bounding since simply signal conversion and modulation can lead to significant delays. By eliminating the necessity for signal conversion and modulation, a very recent protocol, based on signal reflection and channel selection, achieves a processing time of less than 1ns at the prover side. However, it requires specialized hardware at the prover side due to the need for channel selection. This renders existing protocols currently in feasible for even high-end RFID tags.

3.2.2 Context-aware selective unlocking

Secret Handshakes is an interesting selective unlocking method that is based on context awareness [7]. Since an RFID tag or contactless card should only engage in communications when the user actually desires this action i.e., when the context is correct secret Handshakes. Conceptually, a secret handshake is a series of time-constrained physical actions or gestures which an individual must perform with the RFID tag or contactless card (or wallet, if the tag or card is in the wallet) in order to "unlock" the card and permit it to communicate with a card reader. Some example secret handshakes include:

• Key Twist – User makes key turning motion with the card.

• Hip Twist – User keeps card in his/her pocket and twists hip to bring pocket with reading range of the reader.

• Circle – User moves card in a circular manner, parallel with the surface of the reader.

• Double Circle – User makes two consecutive circles with the card.

• Triangle – User moves card in a triangular pattern parallel with the surface of the reader.

• 1-left-1-right – User waves card side to side (once left, once right) in front of the card reader.

• 1-right-1-left – User waves card side to side (once right, once left) in front of the card reader.

• 1.5-wave – User waves card side to side (once right, once left, once right) in front of the card reader.

3.2.3 Context Detection on the Card or Reader

Processing of the accelerometer readings can either be performed directly on the RFID tag or contactless card or can be encrypted and sent to the reader for processing. Specifically, signal processing on the card uses limited resources. To unlock an accelerometer-equipped RFID tag using Secret Handshakes, a user must move or shake the tag (or its container) in a particular pattern. For example, the user might be required to move the tag parallel with the surface of the RFID reader's antenna in a circular manner. A number of unlocking patterns were studied and shown to exhibit low error rates. A central drawback to Secret Handshakes is that a specialized movement pattern is required for the tag to be unlocked. This requires subtle changes to the existing RFID usage model. While a standard, insecure RFID setup only requires users to bring their RFID tags within range of a reader, the Secret Handshakes approach requires that users consciously move the tag in a certain pattern. This clearly undermines the usability of this approach. Motion detection[8] has been proposed as another selective unlocking scheme. A tag would respond only when it is in motion instead of doing so promiscuously. In other words, if the device is still, it remains silent. Although motion detection does not require any changes to the traditional usage model and raises the bar required for a few common attacks to succeed, it is not capable of discerning whether the device is in motion due to a particular gesture or because its owner is in motion. Hence, the false unlocking rate of this approach is high.

4. EXISTING SYSTEM

Europay, Mastercard, and Visa (EMV) is a global standard for debit and credit card payments. Payment systems based on EMV have been introduced across the world, known by a variety of different names such as "Chip and PIN". Mastercards Pay Pass is another EMV compatible "contactless" payment protocol. The proposed system consists of three entities of interest as RFID-enabled payment card, the merchant, and the issuer bank, which issues the card. The payment card stores card details such as the credit card number, name of the owner, and expiration date. It also stores a symmetric key shared with its issuer bank [9].The point-of-sale (PoS) terminal at the merchant side is equipped with an RFID reader. A transaction starts with the merchant issuing a challenge to the payment card. The card calculates a cryptographic response based on the challenge and other information using the key shared with the issuer bank. It then transfers the response to the merchant terminal through the RFID communication interface. The response is next forwarded by the terminal to the issuer bank, which verifies the response and approves the transaction, if authentication is successful.

5. CONCLUSION

This paper gave detail description of existing systems with their advantages and limitations. Many of them required some auxiliary devices to carry with user and some of them affects the original model of RFID. All these methods individually enhance the security in RFID but still there is scope for enhancing security and privacy. Solutions designed for RFID systems need to satisfy the requirements of the RFID applications in terms of not only efficiency and security, but also usability.

REFERENCES

[1]Di Ma,NiteshSaxena, Tuo Xiang, and Yan Zhu, "Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing," IEEE transactions on dependable and secure computing, vol. 10, no. 2, pp. 57-69, march/April 2013.
[2] S. Drimer and S.J. Murdoch, "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks," Proc. 16th USENIX Security Symp, Aug. 2007.
[3] A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," Proc. ACM Conf. Computer and Comm. Security (CCS), 2003.
[4] A.Juels, P.F. Syverson, and D.V. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility," Proc. Fifth Int'l Conf. Privacy Enhancing Technologies, 2005.
[5] M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management," Proc. Australasian Conf. Information Security and Privacy (ACISP), 2005.
[6] N. Saxena, B. Uddin, J. Voris, and N. Asokan, "Vibrate-to-Unlock: Mobile Phone Assisted User Authentication to Multiple Personal RFID Tags," Proc. IEEE Int'l Conf. Pervasive Computing and Comm. (PerCom), 2011.
[7] A. Czeskis, K. Koscher, J. Smith, and T. Kohno., "RFIDs and Secret Handshakes: Defending against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications," Proc. ACM Conf. Computer and Comm. Security, 2008.
[8] N. Saxena and J. Voris, "Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model," Proc. Workshop RFID Security (RFIDSec), June 2010.
[9] S. Drimer and S.J. Murdoch, "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks," Proc. 16th USENIX Security Symp., Aug. 2007.