ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Location Aware Selective Unlocking for Enhancing RFID Security

Sagar Dakhore, Padma Lohiya

Dept. of E &TC, D.Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India

Abstract: In this paper, a new approach for providing security as well as privacy is proposed. The un-authorized reading and relay attacks on RFID system is avoid by using location sensing mechanism. For example, location sensing mechanism used for location specific application such as on the door of ATM cash transfer van for providing security because the location of the van is fixed. So after reaching the pre-specified location the RFID card is active and then it accepts the fingerprints of the registered person, in this way a stronger cross layer security is provided. The location awareness is used by both tags and back-end servers for defending against unauthorized reading and relay attacks onRFID systems.

KEYWORDS:RFID, location sensing, secure verification safer card, Java development kit.

1 INTRODUCTION

RFID (Radio Frequency Identification) is a method of identifying unique items using radio waves. Typical RFID systems are made up of three components: readers (interrogators), antennas and tags (transponders) that carry the data on a microchip. RFID technology is used today in many applications, including security and access control, transportation and supply chain tracking. It is a technology that works well for collecting multiple pieces of data on items for tracking and counting purposes in a cooperative environment. The ability of allowing computerized identification of objects make Radio Frequency IDentification (RFID) systems increasingly ubiquitous in both public and private domains. The use of NFC-equipped mobile devices as payment tokens (such as Google Wallet) is upcoming the next generation payment system and the latest buzz in the financial industry[1]. RFID is becoming more popular day by day, one important reason for this is the effort of large organizations, to deploy RFID as a tool for automated oversight of their supply chains.

A typical RFID system consists of tags, readers and backend servers. Tags are miniaturized wireless radio devices that store information about their related subject. Such information is sensitive and personally identified. Readers broadcast the queries to tags in the radio transmission ranges for information contained in tags and tags reply with information. The queried information is sent to the server (which may coexist with the reader) for further processing and the processing result is used to performing proper actions (such as updating inventory, opening gate, charging toll and approving the payment). Due to the weaknesses of underlying wireless radio communication, RFID systems have wide variety of security and privacy threats. A large number of these threats are due to the tag's promiscuous response to any reader requests. This renders sensitive tag information easily subject to unauthorized reading. Information gain from a RFID tag can be used to track the owner of the tag[2] but these information consist of different types of relay attacks, Such as ``Ghost \& leech"[3] and ``Reader \& Ghost"[4] attacks. To addressing this attacks secure verification scheme is required.

The location information is utilize to defend against unauthorized reading and relay attacks in certain applications such as mobile payment scheme, context aware selective unlocking etc. It is noticed that in some time, tags only need to communicate with readers at some specific locations. Hence, location or location specific information can serve as a good way to establish a legitimate usage context. The location information is used to design selective unlocking mechanisms so that tags can selectively respond to reader interrogations. That is, rather than responding promiscuously to queries from any readers, a tag utilize the location information and then only communicate.

II.LITRATURE SURVEY

There are many researches in RFID security and location specific applications such as Web-based student attendance system, E-Passport, Distance bounding protocols, Context-aware selective unlocking, Secret handshakes and description of these researches are given as follows:

Web-based student attendance system. This describes the development of a student attendance system [5] based on Radio Frequency Identification (RFID) technology. The existing conventional attendance system requires students to manually sign the attendance sheet every time they attend a class. As common as it seems, such system lacks of automation, where a number of problems may arise. This include the time unnecessarily consumed by the students to find and sign their name on the attendance sheet, some student's may mistakenly or purposely sign another student's name and the attendance sheet may got lost. Having a system that can automatically capture student's attendance by flashing their student card at the RFID reader can really save all the mentioned troubles. This is the main motive of the system and in addition having an online system accessible anywhere and anytime can greatly help the lecturers to keep track of their students' attendance. Looking at a bigger picture, deploying the system throughout the academic faculty will benefit the academic management as students' attendance to classes is one of the key factor in improving the quality of teaching and monitoring their students' performance. Besides, this system provides valuable online facilities for easy record maintenance offered not only to lecturers but also to related academic management staffs especially for the purpose of students' progress monitoring.

E-Passport:- In E-passport [6] RFID's are embedded inside a chip which is holding the information of authentication. The implementation of E-passport using mobile devices to authenticate and access information stored by using context aware information to get access to user data or user's passport stored in a secure server related to the person is proposed. This help in eradicating costs involved in putting information on a RFID which user needs to carry, which may compromise the data on the chip due to various issues. So in order to avoid the compromise of data and making the system more secure and flexible enough, this work has been taken up. In the proposed work the authentication and authorization along with role assigned to the person holding the E-passport is made which in turn leads to dynamic context awareness. This aspect typically enhances security and privacy of data.

Distance bounding protocols:-Distance bounding protocols [7] have been used to thwart relay attacks [8], [9]. A distance bounding protocol 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. 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 [10], [11]. The upper bound calculated by an RF distance bounding protocol, but it 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.

Context-aware selective unlocking:-It shows that contextual information can be used to design selective unlocking mechanisms so that tags can selectively respond to reader interrogations [12]. That is, rather than responding promiscuously to queries from any readers, a tag can utilize “context recognitions" and will only communicate when it makes sense to do so, thus raising the bar even for sophisticated adversaries. For example, an office building access card can remain locked unless it is aware that it is near the entrance of the building.

Secret Handshakes: A recent approach, called ``Secret Handshakes" [13] relates closely to our proposed work. In order to authenticate to an accelerometer-equipped RFID device (such as a WISP) using Secret Handshakes, a user must move or shake his or her device in a particular pattern. For example, a user might be required to move his or her tag parallel with the surface of an RFID reader's antenna in a circular manner. A number of these kinds of patterns were studied and shown to exhibit low error rates].

III. PROPOSED DESIGN

Block diagram of proposed design is shown in fig.1. Proposed design is used for the location specific application. The GPS coordinates of the particular location is saved in the EEPROM of the AVR microcontroller, so only that location the RFID card is activated. For example, the proposed design is used on the door of the Van use for the ATM cash transfer and RFID card (secure card) is used to open the door of the Van. Hence, the location of the ATM in particular region where the Van is going is saved in the server. If the location is matched then only it accept the fingerprint of the registered person and RFID (secure card) card is activated otherwise, viceversa. In this way we can provide the security to the Van from the robbery. No one can activate RFID card other than the prespecified location. MAX-232 IC is used for converting TTL logic to CMOS and ULN 2003 is used to drive the relay board.

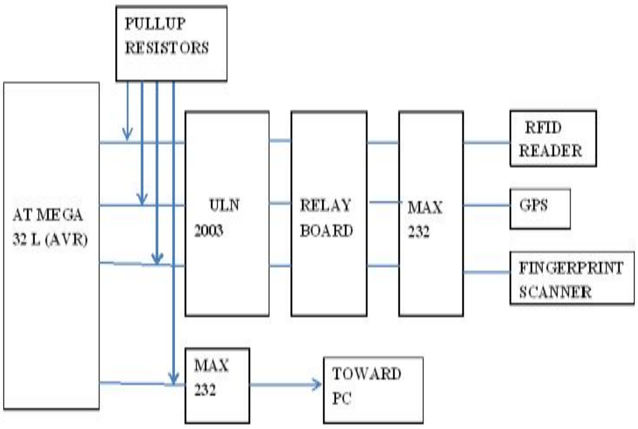


Fig 1: Block Diagram

IV.DESIGN IMPLEMENTATION

A) Hardware Design

1.AVR(AT MEGA 32L)

The Atmel AVR (ATmega32) is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega32 achieves throughputs approaching 1 MIPS per MHz allowing the system designer to optimize power consumption versus processing speed.AVR provides 32Kbytes of In-System Programmable FlashProgram memory with Read-While-Write capabilities, 1024bytes EEPROM, 2Kbyte SRAM, 32general purpose I/O lines, 32 general purpose working registers.
As compare to 8051 microcontroller, AVR take a fixed number of cycles to execute an instruction \& their instructions are also fixed size. AVR are pipe lined processor resulting in faster execution. 8051 has 8 eight bit registers \& has 4 banks, only one of which is usable at any time while AVR have 32 eight bit registers.

2.GPS Smart Antenna.(LOCOSYS)

The LS20031 GPS receiver is a complete GPS smart antenna receiver, that includes an embedded antenna and GPS receiver circuits. This low-cost unit outputs an large amount of position information 5 times a second. The receiver is based on the proven technology found in LOCOSYS 66 channel GPS SMD type receivers that use MediaTek chip solution. The GPS smart antenna will track up to 66 satellites at a time while providing fast time-to-first-fix, one-second navigation update and low power consumption.

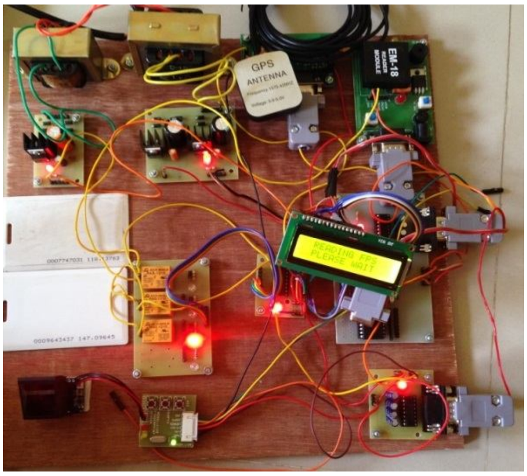


Fig.2 Hardware Design

3.RFID Reader

It is a low frequency (125Khz) RFID reader with serial output with a range of 8-12cm. It is a compact units with built in antenna and can be directly connected to the PC using RS232 protocol. It operate on 5 v supply .

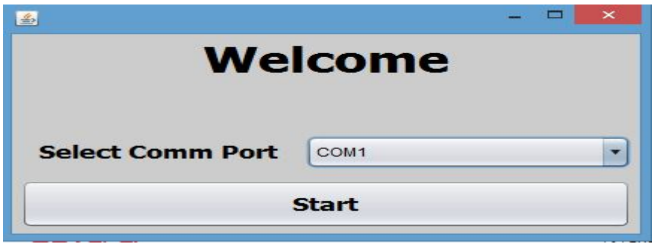
4. Fingerprint Scanner.(ZFM-20)

ZFM-20 Series are separate fingerprint identification module. Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching. When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library.

B) Software Design

The programming on the server side is done in Java to save the GPS as well as Fingerprint coordinates. **Java** is a general purpose computerprogramming language that is concurrent, class-based, object-oriented and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that compiled Java code can run on all platforms that support Java without the need for recompilation.

The RFID reader module is shown in fig.3. In ``welcome window" first COM port is selected. In second window RFID card is scan, RFID card number is displayed in first block and status of card, whether card is accepted or rejected is displayed in second block. RFID card number must matched to pre-specified RFID card number.


Welcome

Select Comm Port COM1

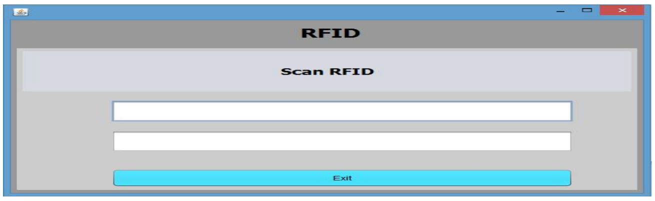


Fig: 3RFID Reader Module in Netbeans

Flowchart of RFID Reader Module in Netbean are given below :-

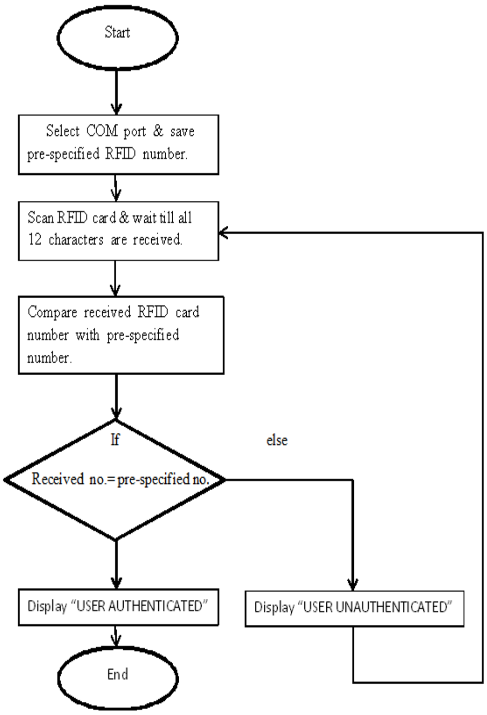

Start
Select COM port & save pre-specified RFID number.
Scan RFID card & wait till all 12 characters are received.
Compare received RFID card number with pre-specified number.
If
Received no.= pre-specified no.
else
Display "USER AUTHENTICATED"
Display "USER UNAUTHENTICATED"
End

Fig. 4. Flowchart of RFID Reader Module.

V. CONCLUSION& FUTURE WORK

A new approach to defend against unauthorized reading and relay attacks in RFID applications is proposed, whereby location can be used as a valid context. Location aware selective unlocking mechanisms and a location aware transaction verification mechanism is design. For collecting this information, GPS infrastructure is used. To demonstrate the feasibility of our location-aware defence mechanisms, a low-cost GPS receiver with a RFID tag is integrated. By using the location aware selective unlocking mechanism and secure verification, the relay attacks avoided with stronger security.

In future we can use the SHA-3 algorithm to avoid the collision effects due to the fingerprint.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

REFERENCES

[1] R. Clauberg, “RFID and Sensor Networks”, Proceding RFID Workshop, St. Gallen, Switzerland, Sept. 2004.

[2] A. Juels, “RFID Security and Privacy: A Research Survey”, IEEE Journal Selected Areas in Communication, Vol. 24, pp. 381-394,Feb. 2006.

[3] Z. Kfir and A. Wool, “Picking Virtual Pockets Using Relay Attacks
on Contactless Smartcard”, Proceding for Symposium on Security and Privacy for Emerging Areas in Communication Networks, Vol.2, pp.47- 58. Aug. 2005.

[4] S. Drimer and S. Murdoch, “Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks”, Proceding 16th USENIX Security Symposium, Vol. 12, pp.34-46, Aug. 2007.

[5] M. Kassim & H. Mazlan, “Web-based Student Attendance System using RFID Technology”, IEEE Journal, Vol. 2, pp. 213-218, April 2012.

[6] R.Sivasubramaniam, “Location-Aware E-passport: Enhancing Security and Privacy”, International Journal of Applied Engineering Research, Vol. 9, pp. 4693-4697, March 2014.

[7] G. Hancke, M. Kuhn, “An RFID Distance Bounding Protocol”, Procedings of IEEE Conference, Vol. 3, pp. 6773, September 2005.

[8] Nitesh Saxena and Jonathan Voris, “Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model”, IEEE Conference, Vol. 4, pp.23-43, March 2010.

[9] A. Francillon, B. Danev, and S. Capkun, “Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars”, Proceding 18th Internationl conference on Network and Distributed System Security, Vol. 21, pp. 247-255, June 2011.

[10] Di Ma, Nitesh Saxena, Tuo Xiang and Yan Zhu, “Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via LocationSensing”, IEEE Transaction, Vol. 10, pp. 57-70, MARCH/APRIL 2013.

[11] N. Saxena, B. Uddin, J. Voris, and N. Asokan, “Vibrate-to-Unlock:Mobile Phone Assisted User Authentication to Multiple Personal RFIDTags”, Proceding IEEE International Conference on Pervasive Computingand Communication(PerCom), Vol. 3, pp. 136-143, June 2011.

[12] T.Halvei, Haoyu Li, “Context-Aware Defenses to RFID UnauthorizedReading and Relay Attacks”, IEEE Transaction, Vol. 1, pp. 307-319, Dec.2013.

[13] A. Juels, P.F. Syverson, and D.V. Bailey, “High-Power Proxies forEnhancing RFID Privacy and Utility”, Proceding Fifth InternationalConference on Privacy Enhancing Technologies, Vol. 3, pp.235-243, Oct.2005.

[14] L. Zhang and Z. Wang, “Integration of RFID into Wireless SensorNetworks: Architectures, Opportunities and Challenging Problems”, ProcedingGrid Computer Workshops, Volume 2, pp. 433-469, sept 2006.

[15] C. Aumuller, P. Bier and J. Seifert, “Fault attacks on RSA with CRT: Concrete results and practical countermeasures”, Workshop on Cryptographic Hardware and Embedded Systems, pp. 1315, March 2002.

[16] D. Naccache and D. MRaihi, “Cryptographic smart cards, IEEE transctionvol. 16, pp. 1424, Aug. 1996.