International Journal of Research in Advent Technology (E-ISSN: 2321-9637) Special Issue
1st International Conference on Advent Trends in Engineering, Science and Technology
"ICATEST 2015", 08 March 2015

Location Aware Selective Unlocking & Secure Verification Safer Card for Enhancing RFID Security using SHA.

Sagar Dakhore[1], Mrs. Padma Lohiya[2].

PG Student, Dept. of E &TC, D.Y. Patil College of Engineering, Akurdi, Pune[1], Sagardakhore555@gmail.com
Professor, Dept.of E &TC, D.Y. Patil College of Engineering, Akurdi, Pune[2]

Abstract - In This Paper, we report a new approach for providing security as well as privacy to the corporate user. With the help of locations sensing mechanism by using GPS we can avoid the un- authorized reading & relay attacks on RFID system. For example, location sensing mechanism with RFID card is used for location specific application such as ATM cash transfer van for open the door of van. So after reaching the pre-specified location (ATM) the RFID card is active & then it accepts the fingerprint of the registered person only. In this way we get a stronger cross layer security. SHA algorithm is used to avoid the collision (due to fraud fingerprint) effect on server side.

Keywords: **RFID, Location Aware Selective unlocking, Java Development kit (JDK), Secure Hash Algorithm.**

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[13]. 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[14]. In both the popular press and academic circles, RFID has seen a swirl of attention in the past few years. One important reason for this is the effort of large organizations, such as Wal-Mart, Procter and Gamble and the U.S. Department of Defence , to deploy RFID as a tool for automated oversight of their supply chains. Thanks to a combination of dropping tag costs and vigorous RFID standardization, we are on the brink of an explosion in RFID use.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 gleaned from a RFID tag can be used to track the owner of the tag[8]. Promiscuous responses also different types of relay attacks. Such as "Ghost & leech"[11] and "Reader & Ghost"[12] attacks.

To addressing this problem we requires secure verification such as validation the tag is intended authorizing the intended payment amount. We utilizing the location information to defend against unauthorized reading and relay attacks in certain applications. It is noticed that in quite some

applications, under normal circumstances, tags only need to communicate with readers at some specific locations. Hence, location or location specific information can serve as a good means to establish a legitimate usage context. The location information can be 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 can utilize location information and will only communicate when it makes sense to do so, thus, raising the bar even for sophisticated adversaries without affecting the RFID usage model.

2. PRIOR WORK

Web-based student attendance system,[4] This describes the development of a student attendance system 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 students may mistakenly or purposely signed 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,[1] In E-passport identification process reading RFID are used. In this work 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 would 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,[9] These protocols have been used to thwart relay attacks [7], [5]. 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 [7], [5]. 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,[3] It show that contextual information can be 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 can utilize ''context recognition'' 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 (fixed) entrance of the building.

Secret Handshakes: A recent approach, called "Secret Handshakes" [7] relates closely to our proposal. 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 [7].

3 PROPOSED WORK

3.1 Hardware Design

We use the AVR microcontroller i.e. AT Mega 32 as shwn in the fig 1.This model can be use for the location specific application. The GPS coordinates of the particular location is saved in the EEPROM of the microcontroller, so only that location the RFID card is activated. For example, suppose we can use this model on the door of the Van use for the ATM cash transfer & 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 the it accept the fingerprint of the registered person & RFID (secure card) card is activated otherwise, vice-versa . In this way we can provide the security to the Van from the robbery. No one can activate RFID card other than the pre-specified location.

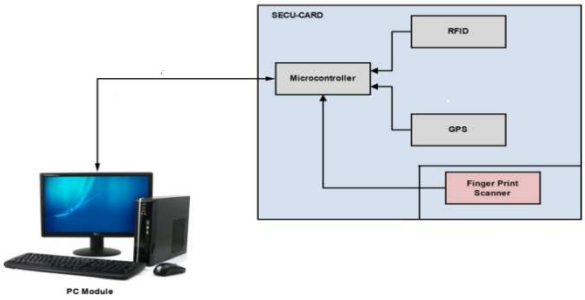

Fig.1 Proposed work Design

3.2 Software Design

The programming on the server side is done in Java to save the GPS as well as Fingerprint coordinates. If the GPS coordinates of the EEPROM of the microcontroller & server is matched then it only released the data after verifying the fingerprint coordinates. But, fingerprint can be produced by fraud manner i.e. the two different message produces the same digit in the server this terms as the collision effect. To avoid such type of effect we use the advanced SHA-3 algorithm.

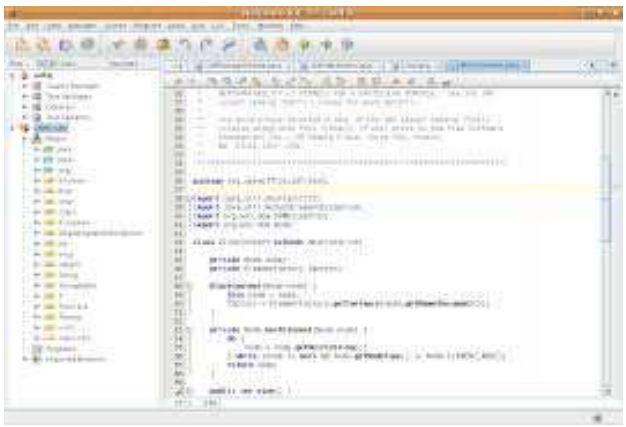

Fig: 2 Java Program in Netbeans

3.3 SHA ALGORITHM

SHA (Secure Hash Algorithm) process:-

Padding

○ Pad the message with a single one followed by zeroes until the final block has 448 bits.
○ Append the size of the original message as an unsigned 64 bit integer.

 Initialize the 5 hash blocks (h0,h1,h2,h3,h4) to the specific constants defined in the SHA1 standard.
 Hash (for each 512bit Block)
○ Allocate an 80 word array for the message schedule
■ Set the first 16 words to be the 512bit block split into 16 words.
■ The rest of the words are generated using the following algorithm
 word[i3]
XOR word[i8]
XOR word[i14]
XOR word[i16]
Then rotated 1 bit to the left.
○ Loop 80 times doing the following. (Shown in Image1)
■ Calculate SHAfunction() and the constant K (these are based on the
current round number.
■ e=d
■ d=c
■ c=b (rotated left 30)
■ b=a
■ a = a (rotated left 5) + SHA function () + e + k + word[i]
○ Add a,b,c,d and e to the hash output.
 Output the concatenation (h0,h1,h2,h3,h4) which is the message digest.

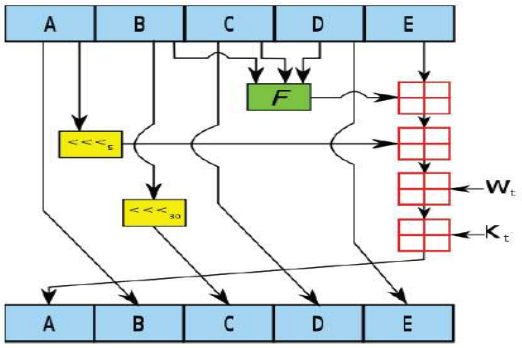

Fig: 3 Image1: 80 round interloop

4. CONCLUSION

In this paper, we reported a new approach to defend against unauthorized reading and relay attacks in some RFID applications whereby location can be used as a valid context. It argued the feasibility of our approach in terms of both technical and economical aspects. Using location information, we designed location aware selective unlocking mechanisms and a location aware transaction verification mechanism. For collecting this information, we made use of the GPS infrastructure. To demonstrate the feasibility of our location-aware defence mechanisms, it integrated a low-cost GPS receiver with a RFID tag (the Intel's WISP) and conducted relevant experiments to acquire location information from GPS readings. By using the secure hash algorithm we can provide the stronger security & avoid the collision attacks.

REFERENCES

[1] Raguramajayan , Sivasubramaniam , "Location-Aware E-passport: Enhancing Security and Privacy" International Journal of Applied Engineering Research ,Volume 9,pp. 4693-4697, Number 18, 2014.

[2] Di Ma, Member, Nitesh Saxena, Tuo Xiang, and Yan Zhu , " Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing" IEEE Transaction, VOL. 10, NO. 2, MARCH/APRIL 2013.

[3] T.Halvei , Haoyu Li, "Context-Aware Defenses to RFID Unauthorized Reading and Relay Attacks" IEEE TRANSACTIONS VOLUME 1, NO. 2, DECEMBER 2013.

[4] Murizah Kassim, Hasbullah Mazlan, "Web-based Student Attendance System using RFID Technology", IEEE, page no.213-218, 2012.

[5] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," Proc. 18th Ann. Network and Distributed System Security Symp. (NDSS), 2011.

[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] Nitesh Saxena and Jonathan Voris, "Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model" 2010.

[8] A. Juels, "RFID Security and Privacy: A Research Survey," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 381-394, Feb. 2006.

[9] Gerhard P. Hancke, Markus G. Kuhn, "An RFID Distance Bounding Protocol", Proceedings of IEEE, pp. 67–73. September 2005.

[10] 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.

[11] Z. Kfir and A. Wool, "Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard," Proc. Security and Privacy for Emerging Areas in Comm. Networks (Securecomm), 2005.

[12] S. Drimer and S.J. Murdoch, "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks," Proc. 16th USENIX Security Symp., Aug. 2007.

[16] Washington State Dept. of Licensing, "Enhanced DriverLicense/IDCard,"http://www.dol.wa.gov/about/news/priorities/edl.html, 2013.

[17] M. Calamia, "Mobile Payments to Surge to $670 Billion http://www.mobiledia.com/news/96900.html, July 2011.

[18] RFID Progress at Wal-Mart in IDTechEx Website. [Online]. Available: http://www.idtechex.com/research/articles/rfid_progress_at_wal_mart_00000161.asp

[19] R. Clauberg, ''RFID and Sensor Networks,'' in Proc. RFID Workshop, St. Gallen, Switzerland, Sept. 2004.

[20] L. Zhang and Z. Wang, ''Integration of RFID into Wireless Sensor Networks: Architectures, Opportunities and Challenging Problems,'' in Proc. Grid Coop. Comput. Workshops, 2006, pp. 433-469.