ISSN 2395-1621

Location Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing

[#1]Gaurav Thakur, [#2]Ninad Rajguru, [#3]Pranav Yermalkar, [#4]Dhananjay Korde,
[#5]Prof. Adhinath.M.Wade

[1]gaurav.thakur0810@gmail.com
[2]ninadrajguru22@gmail.com
[3]praan94@gmail.com
[4]dhananjaykorde@gmail.com

[#1234]Student, Department of Computer Engineering
[#5]Prof, Department of Computer Engineering

SKNCOE, Pune, India -411041.

ABSTRACT

In our paper, we report on a new approach for improving security and privacy in certain RFID applications where Location related or location information (i.e. speed) can serve as a legitimate access context. Following are Examples of these applications that include toll cards, access cards, credit cards, and other payment tokens. We have shown that location knowledge can be used by back –end servers And by both tags for protecting against unauthorized readings and retransmit attacks on a RFID systems. On the tag side, we design a location-aware selective unlocking mechanism using which tags can selectively respond to reader interrogations rather than doing so judgmentally. On the server side, we design a location-aware secure transaction verification scheme that allows a bank server to decide whether to approve or deny a payment transaction and detect a specific type of relay attack involving malicious readers. The premise of our work is a current technological advancement that can enable RFID tags with low-cost location (GPS) sensing capabilities. Dissimilar prior research on this subject, our protection does not depend on auxiliary devices or require any explicit user conditions.

Keywords: **MPS (Mobile Payment System), relay attack, GPS, RFID, Context Recognition.**

ARTICLE INFO

Article History

Received: 14th May 2016

Received in revised form :

14th May 2016

Accepted: 16th May 2016

Published online :

22st May 2016

I. INTRODUCTION

Less price, small size, and the ability of allowing recognition of objects make RFID systems increasingly omnipresent in the public and private domains. Prominent RFID applications supply chain management e-passports , credit cards , licenses , toll collection or car key, building, parking or public transport(access cards), and medical implants . Near Field Communication, is another upcoming RFID technology that allows smart phones, to have RFID tag and reader functionality.

Radio Frequency identification system consists of readers, tags, back-end servers. RFID Tags are miniaturized wireless radio devices that store information. Such information is sensitive. Readers transmit queries to tags in their radio transmission ranges for data contained in tags and the tags reply with required data. The queried data is then sent to the server for further processing. Data gained from a RFID tag can be used to track the owner of the tag.

The types of relay attacks are not specific here . One of the type of attacks is referred to as “ghostand- leech”. In this type of attack, an oppeser, called a “leech”, relays the information sneakily read from a legitimate RFID tag to a colluder entity known as a “ghost”. The ghost can then relay the received information to a same legitimate reader and vice versa in the other side. By This way a leech pair and a ghost can succeed in personating a legitimate RFID tag without actually possessing the device. A more danger form of relay attacks, usually against payment cards, is called “reader-and-ghost”; it involves a malicious reader and an unsuspecting owner trying to make a transaction . In this type of attack, the unauthorized reader, doing the role of a leech and colluder with the ghost, this can fool the owner of the card to approve a transaction which he did not intend to make (e.g., paying for a expensive gift purchase made by the adversary while the owner only intending to pay for food). We have note that addressing this type of problem requires a secure type of transaction verification, i.e., validation that the tag is

indeed authorizing the intended payment amount.

The feasibility of executing relay attacks has been demonstrated on many RFID (or related) deployments, including the Chip-and-PIN credit card system , RFID-assisted voting system, and keyless entry and start car key system . As the RFID applictions are used everywhere, there is a need for the development of security primitives and protocols to defeat unauthorized reading and relay attacks. However,to provide security and privacy services for RFID systems it presents a unique and formidable set of challenges. The inbuilt difficulty stems partially from the constraints of RFID tags in terms of computation, memory and power, and partially from the unusual usability requirements imposed by RFID applica- tions (originally geared for automation). Consequently, the solutions designed for the RFID systems need to satisfy the various requirements of the RFID applications in terms of only efficiency and security, and usability.

II. LITERATURE SURVEY

Overview In 2013 Di Ma, Nitesh Saxena GPS module. In this test module, we have chosen the 66-channel LS20031 GPS receiver module from LOCOSYS Technologies in our experiments [2].This module comes with an embedded ceramic patch antenna and GPS receiver circuits, which are designed for a broad spectrum OEM applications and outputs the data in more than six different NMEAGPS sentences to a TTL- level serial port. It provides us with a variable update rate of 1 to 5Hz. It also includes a LED indicator to indicate GPS x or no x. In our experiments.

The LS20031 (GPS module) communicates via TTL level serial communication (UART), which is interfaced to the A channel communication port (used for UART, SPI, and I2C) on the WISP as shown in the block diagram above. The Rx communication on the LS20031 is only used for sending commands to congure it. Since we have limited RAM, i.e., only 512 bytes on the WISP controller, we have to store location in the location list, we test whether it falls within the square region centered at a valid location. The size of the square space depends on how much error tolerance we can accord. We conduct various experiments to and out the accuracies of location recognition based on different error tolerances. Since the values obtained from the GPS are in degrees, we map the degree error onto meters for easier understanding. We also have to consider the problem of different latitudes. Since the radii vary as we move across different latitudes, the error tolerance also varies. We found that for about 10 degrees of variation in latitude, the error tolerance varies by less than 1 meter, which is reasonably small and is feasible for most of the applications Existing System We report on our work on utilizing location information to defend against unauthorized reading and tracked by road authorities via video cameras as is the practice nowadays. Similarly, a credit card can be tracked by its issuing bank whenever a transaction is made.

Hence, the objective of our privacy protection is to prevent privacy leakage due to unauthorized parties. We also note that, in some applications, the proposed approaches may not provide absolute security. However, they still significantly raise the bar even for sophisticated adversaries without affecting the RFID usage model. For example, the selective unlocking mechanism for toll cards, based solely on speed detection, will leave the card vulnerable in other situations where the car is undergoing the same speed designated at the toll booths. However, it still protects the car from being read by an adversary while traveling at other speeds or when stationary. In addition, although the proposed techniques can work in a standalone fashion, they can also be used in conjunction with other security mechanisms, such as cryptographic protocols, to provide stronger cross-layer security protection. Present system Only security of password Location not important for transaction No ways to authenticate the legitimate user or actual user Anyone and from anywhere can perform transaction if password is known. Proposed system Triple layer security i.e. RFID,GPS location and fingerprint scanning GPS location authentication Fingerprint authentication Actual user SKNCOE, Department of Computer Engineering 2015-16 17 can only use the system.

III. WORKING MODEL

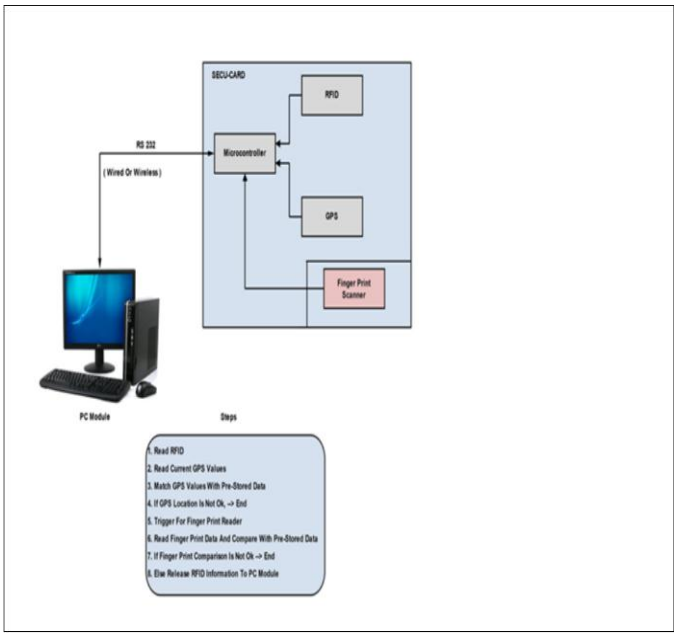

Fig 1. System Architecture

Component Diagram:

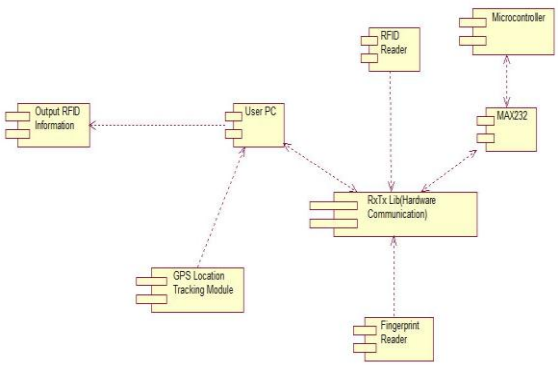

Fig 2. Component diagram

Mathematical Model

Let s = u, r, L, Fp, Rread, Fscanner, Tag, F

u < -u1, u2, u3,.., finite set of users

ri - r1, r2, r3,..., finite set of RFID

Li - L1, L2, L3, ..., GPS Location of the card

Fpi - Fp1, Fp2, Fp3,.. finite set of fingerprints

Rread < - RFID reader

Fscanner < - fingerprint scanner

Tag < - Tag1, Tag2,...Tagi ....unique tag associated with RFID

F < - F1, F2, F3,..., Finite set of function

Read RFID(Rread, Ri) //read the RFID tag

Read GPS Location(GPS)
//read GPS Location of the tag

Input fingerprint (Fscanner) // i/p fingerprint of user

Authenticate (FPi, FPdbi)
// compare the fingerprint with db

Swim Lane Diagram

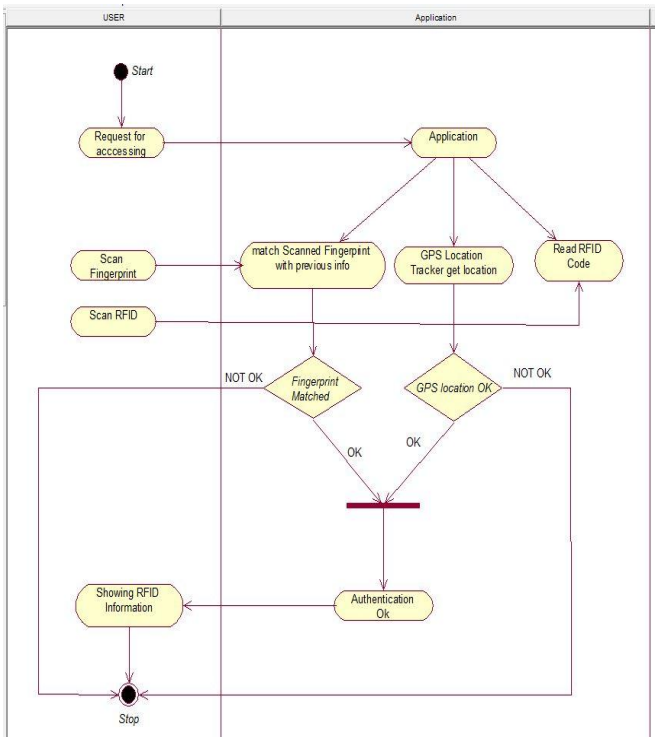

Fig 3. Swim Lane Diagram

IV. 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. We argued the feasibility of our approach in terms of both technical and economic aspects.

Using location and derived speed 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 defense mechanisms, we integrated a low-cost GPS receiver with a RFID tag (the Intels WISP) and conducted relevant Experiments to acquire location and speed information from GPS readings. Our results show that it is possible to measure location and speed with high accuracies even on a constrained GPS-enabled platform, and that our location aware defenses are quite useful in significantly raising the bar against the reader-and-leech attacks.

As an immediate avenue for further work, we intend to further optimize and ne-tune our location detection algorithms for better efficiency on resource constrained RFID platforms and improved tolerance to errors whenever applicable. Additionally, we are exploring the use of ambient sensors to determine proximity based on location-specific sensor information for the second security primitive secure transaction verification. We will also evaluate the promising of proposed techniques by means of usability studies.

REFERENCES

[1] J. Bringer, H. Chabanne, and E. Dottax, HB++: A Lightweight Authentication Protocol Secure against Some Attacks, Proc. Second Intl Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006.

[2] S. Brands and D. Chaum, Distance-Bounding Protocols, Proc. Intl Conf. Theory and Applications of Cryptographic Techniques Advances in Cryptology (EUROCRYPT), 2013.

[3] RFID Toll Collection Systems,http://www. securitysa.com/news.aspx?pklnewsid-25591,2007.

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

[5] G. Cropsey, Designing a Distance and Speed Algorithm Using the Global Positioning System, http://www.egr.msu.edu/classes/ece480/capstone/spring08/group10/documents/ApplicationApplication, Mar.2008.

[6] M. Kuhn, An Asymmetric Security Mechanism for Navigation Signals, Proc. Sixth Information Hiding Workshop, 2004.

[7] A. Czeskis, K. Koscher, J. Smith, and T. Kohno., RFIDs and Secret Handshakes: Defending against Ghost-and-Leech Attacks and Un-authorized Reads with Context-Aware Communications, Proc. ACM Conf. Computer and Comm. Security, 2008.

[8] Goldiron, Numerex Unveils Hybrid Tag Includes Active RFID, GPS, Satellite and Sensors, http://goldiron.wordpress.com/2009/02/25/numerex-unveils-hybrid-tag-includes-active-rd- gpssatellite-and-sensors/, Feb. 2009.

