LOCATION-AWARE AND SAFER CARDS

Dr. J. Narendra Babu[1], Dr. M Kezia Joseph[2], Dr N. Rajesha[3], Dr. B. Jayachandran[4], Dr.Nikhil Raj[5]
[1,2,3,4,5]Professor, Dept. of ECE,MRCE, Hyderabad

Abstract:

In this paper, we report on a new approach for improving security and privacy in certain RFID applications whereby location or location-related information (such as speed) can serve as a legitimate access context. Examples of these applications include access cards, toll cards, credit cards, and other payment tokens. We show that location awareness can be used by both tags and back-end servers for defending against unauthorized reading and relay attacks on 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 promiscuously. 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. Unlike prior research on this subject, our defenses do not rely on auxiliary devices or require any explicit user involvement.

Keywords- Context Recognition,RFID, Mobile Payment System, Relay Attacks, Location Sensing.

I. INTRODUCTION

Low cost, small size and the ability of allowing computerized identification of objects make Radio Frequency Identification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications supply chain management (inventory control), e-passports, credit cards, driver's licenses, vehicle systems (toll collection or car key), access cards (building, parking or public transport), and medical implants. NFC, or Near Field Communication, is yet another upcoming RFID technology that allows devices, such as smart phones, to have both RFID tag and reader functionality. In particular, the use of NFC- equipped mobile devices as payment tokens (such as Google Wallet) is considered to be the next generation payment system and the latest buzz in the financial industry.

A typical RFID system consists of tags, readers, and/or

back-end servers. Tags are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personally identifiable. For example, a US e-passport stores the name, nationality, date of birth, digital photograph, and (optionally) fingerprint of its owner. Readers broadcast queries to tags in their radio transmission ranges for information contained in tags and tags

reply with such information. The queried information is then sent to the server (which may coexist with the reader) for further processing and the processing result is used to perform proper actions (such as updating inventory, opening gate, charging toll or approving payment).

Due to the inherent weaknesses of underlying wireless radio communication, RFID systems are plagued with a 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 (might simply be a plain identifier) gleaned from a RFID tag can be used to track the owner of the tag, or be utilized to clone the tag so that an adversary can impersonate the tag's owner.

Promiscuous responses also incite different types of relay attacks. One class of these attacks is referred to as "ghostand- leech". In this attack, an adversary, called a "leech," relays the information surreptitiously read from a legitimate RFID tag to a colluding entity known as a "ghost." The ghost can then relay the received information to a corresponding legitimate reader and vice versa in the other direction. This way a ghost and leech pair can succeed in impersonating a legitimate RFID tag without actually possessing the device.

A more severe form of relay attacks, usually against payment cards, is called "reader-and-ghost"; it involves a malicious reader and an unsuspecting owner intending to make a transaction in this attack, the malicious reader, serving the role of a leech and colluding with the ghost, can fool the owner of the card into approving a transaction which she did not intend to make (e.g., paying for a diamond purchase made by the adversary while the owner only intending to pay for food). We note that addressing this problem requires secure 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. With the increasingly ubiquitous deployment of RFID applications, there is a pressing need for the development of security primitives and protocols to defeat unauthorized reading and relay attacks. However, providing security and privacy services for RFID systems presents a unique and formidable set of challenges. The inherent 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 applications (originally geared for automation). Consequently, solutions designed for RFID systems need to satisfy the requirements of the underlying RFID applications in terms of not only efficiency and security, but also usability.

In this paper, we report on our work on utilizing location information to defend against unauthorized reading and relay attacks in certain applications. We notice that in quite some applications, under normal circumstances, tags only need to communicate with readers at some specific locations or while undergoing a certain speed. For example, an access card to an office building needs to only respond to reader queries when it is near the entrance of the building; a credit card should only work in authorized retail stores; toll cards usually only communicate with toll readers in certain fixed locations (toll booths) or when the car travels at a certain speed.

Hence, location or location-specific information can serve as a good means to establish a legitimate usage context specifically; we present two location-aware defense mechanisms for enhanced RFID security and privacy. First, we show that 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, and thus, raising the bar even for sophisticated adversaries without affecting the RFID usage model. For example, an office building access card can remain locked unless it is aware that it is near the (fixed) entrance of the building. Similarly, a toll card can remain locked unless the car is at the toll booth and/or it is traveling at a speed range regulated by law.

II. BACKGROUND AND PRIOR WORK

All of these approaches, however, require the users to carry an auxiliary device. In Blocker Tag, a special RFID tag, called "Blocker," is used to disrupt the identification process used by the reader to identify tags in proximity. RFID Enhancer Proxy and RFID Guardian are special RFID-enabled devices that could be implemented in a PDA or cellphone. They are assumed to come with greater computation

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI:10.21276/ijcesr.2017.4.12.16

capability and, thus, can perform more sophisticated interactions with readers, on behalf of tags, for various security purposes. In Vibrate-to- Unlock, a user unlocks his/ her RFID tags by authenticating to these tags through a vibrating phone. However, such an auxiliary device (required by above schemes) may not be available at the time of accessing RFID tags, and users may not be willing to always carry these devices.

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. There has been a growing interest in the research community to design lightweight cryptographic mechanisms. However, these protocols usually require shared key(s) between tags and readers, which is not an option in some applications.

Distance bounding protocols. These protocols have been used to thwart relay attacks. 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. (We stress that 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 infeasible for even high-end RFID tags.

Context -aware selective unlocking: "Secret Handshakes"

is a recently proposed interesting selective unlocking method that is based on context awareness. 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, however, 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.

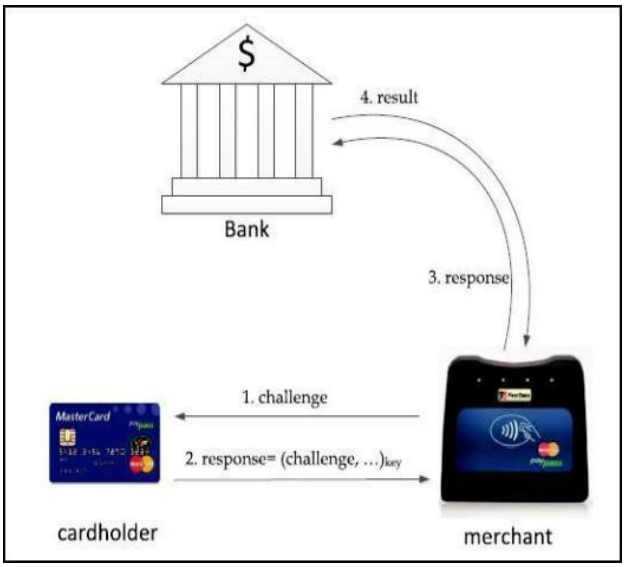


Fig. 1: Online Authorization in a Mobile Payment System.

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI:10.21276/ijcesr.2017.4.12.16

A. Advervrsarial models

Our proposed techniques are meant to defend against unauthorized reading, ghost-and-leech, and reader-and ghost attacks. Adversary models used in the three attack contexts are slightly different. In the following description, we call the tag (reader) under attack as valid tag (reader) and call the tag (reader) controlled by the adversary as malicious tag (reader).

In unauthorized reading, the adversary has direct control over a malicious reader. The malicious reader can be in the communication range of the victim tag without being detected or noticed and, thus, can surreptitiously interrogate the tag. The goal of the adversary is to obtain tag specific information and (later) use such information to compromise user privacy (through inventory checking), clone the tag (and thus impersonate the user), or track the user.

In ghost-and-leech attack, besides the malicious reader (the leech), the adversary has further control over a malicious tag (the ghost), which communicates with a valid reader. The adversary's goal is to use the malicious tag to impersonate the valid tag by letting the malicious tag respond to interrogations from the valid reader with information surreptitiously read from the valid tag by the malicious reader. In reader-and-ghost attack, originally called the "mafia fraud" attack, the adversary controls a malicious reader and tag pair, just like in the ghost- and-leech attack. However, the malicious reader controlled by the reader and- ghost adversary is a legitimate reader or believed by the valid tag as a legitimate reader. Hence, the valid tag (or its owner) is aware of and agree with communications with the malicious reader. That is, the interrogation from the malicious reader to the valid tag is not surreptitious as in unauthorized reading and ghost-and-leech attacks. The goal of the adversary is still to impersonate the valid tag.

In all the attack contexts, we assume the adversary does not have direct access to the valid tag, so tampering or corrupting the tag physically is not possible or can be easily detected. The adversary is also unable to tamper the tag remotely through injected malicious code. We further assume that the adversary is able to spoof the GPS signal around the victim tag but not around the victim reader. This is because the reader is usually installed in a controlled place (toll booth, office building gate, or retail store) and, thus, GPS spoofing around the victim reader can be easily detected. We do not consider loss or theft of tags.

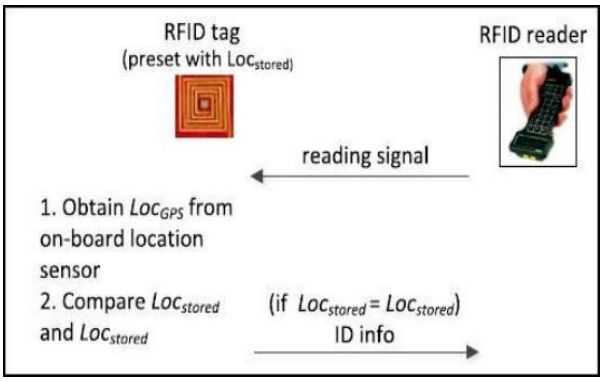


Fig. 2: Location-aware selective unlocking where Locstored is legitimate location (or speed) info stored on the tag side and LocGPS is the location info obtained from on-board GPS upon a reader request.

B. Location-Aware selective unlocking

In this section, we present our location-aware selective unlocking mechanism. It can be used to protect against unauthorized reading and ghost-and-leech attacks. Using location-aware selective unlocking, a tag is unlocked only when it is in an appropriate (prespecified) location. This mechanism is suitable for applications where reader location is fixed and well known in advance. One example application is RFID-based building access system. An access card to an office building needs to only respond to reader queries when it is near the entrance of the building.

A prerequisite in a location-aware selective unlocking scheme is that a tag needs to store a list of legitimate locations Locstored beforehand (as depicted in Fig. 2. Upon each interrogation from a reader, the tag obtains its current location information LocGPS from its on-board GPS sensor, and compares it with the list of legitimate locations and decides whether to switch to the unlocked state or not. Due to limited on-board storage (e.g., the WISP has an 8 KB of flash memory) of tags, the list of legitimate locations must be short. Otherwise, testing whether the current location is within the legitimate list may cause unbearable delay and affect the

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI:10.21276/ijcesr.2017.4.12.16

performance of the underlying access system. Moreover, the list of legitimate locations should not change frequently because otherwise users will have to do extra work to securely update the.

List on their tags. Thus, selective unlocking based on pure location information is more suitable for applications where tags only need to talk with one or a few readers, such as building access cards. It may not be suitable for credit card applications, as there is a long list of legitimate retailer stores, and store closing and new store opening occur on a frequent basis.

C. Location-Aware transaction verification

A highly difficult problem arises in situations when the reader, with which the tag (or its user) engages in a transaction, itself is malicious. For example, in the context of an RFID credit card, a malicious reader can fool the user into approving for a transaction whose cost is much more than what she intended to pay. That is, the reader terminal would still display the actual (intended) amount to the user, while the tag will be sent a request for a higher amount. More seriously, such a malicious reader can also collude with a ghost and then succeed in purchasing an item much costlier than what the user intended to buy. As discussed in Section 1, addressing this reader-and-ghost relay attack requires transaction verification, i.e., validation that the tag is indeed authorizing the intended payment amount. Note that selective unlocking is ineffective for this purpose because the tag will anyway be unlocked in the presence of a valid (payment) context.

In this paper, we set out to explore the design of location- aware automated mechanisms for protecting against reader- and-ghost attacks. We note that under such attacks, the valid tag and the valid reader would usually not be in close proximity. This is in contrast to normal circumstances whereby the two entities would be at the same location, physically near to each other. Thus, a difference between the locations of the tag and the reader would imply the presence of such attacks. In other words, both the valid tag (credit card) and valid reader may transmit their locations to a centralized authority (issuer bank). This authority can then compare the information received from both entities and reject the transaction if the two mismatch Measure their location information. Location information generated by both card and reader are then forwarded to the bank. The bank server decides whether to approve the transaction after comparing the location data received from the two ends. Fig.3 illustrates the process of location-based proximity verification inside the current mobile payment infrastructure. The user-side card generates its location information loccard while the merchant- side reader generates its version of location information locmerchant. loccard is protected (e.g., via MAC) with the key shared with the issuer bank before it is sent to the merchant's terminal, which then forwards its own location information locmerchant along with the card credentials to the bank for transaction verification and authorization. Since the integrity of loccard is protected by the shared key between the card and bank, a malicious

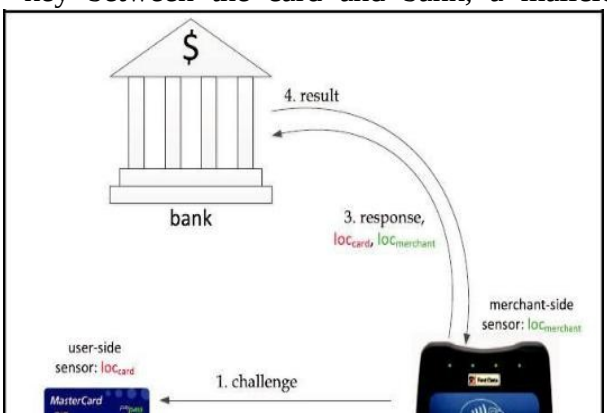
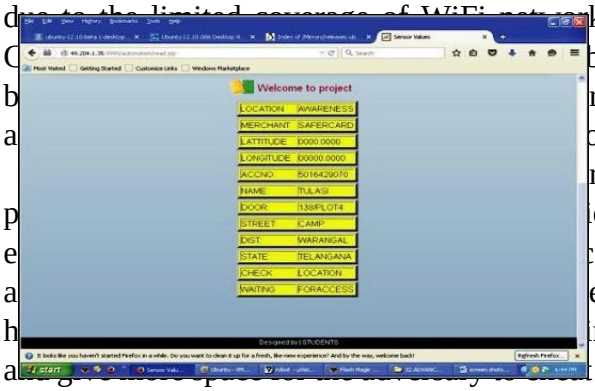


Fig. 3: Online Authorization in a Mobile Payment System Enhanced With Our Proximity Detection Approach.

III. DESIGN AND IMPLEMENTATION

GPS is generally used as the main source of location information and the major enabler for location-based services. It has world-wide availability and an accuracy of a few meters in location estimation—adequate enough for most civilian applications. However, the accuracy of GPS deteriorates inside buildings and in arrow urban canyons. Unlike GPS, WiFi positioning can provide good positioning results (with an accuracy of a few meters just like that of GPS) even indoors. However, it is prone to signal interferences and may not be always available

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI:10.21276/ijcesr.2017.4.12.16



proximity in server transaction verification. For this reason, the cellular network positioning technology is believed not a good candidate to use to get location information for security purpose.

A GPS receiver derives its location by timing the signals sent by GPS satellites high above the Earth. The receiver uses the messages it receives from the satellites to determine the travel time of each message and computes the distance to respective satellite. These distances along with the satellites' own locations are used with the possible aid of trilateration, to compute the position of the receiver. Storing list of valid locations. Since we have limited RAM, i.e., only 512 bytes on the WISP controller, we have to store this valid location list on an external memory for the purpose of our selective unlocking mechanism (note that the transaction verification mechanism does not require the tag to store anything). Location sensing and computation. For location sensing, we dynamically obtain the location data from the GPS continuously at the rate of 1 Hz, and compare it with the list of valid locations stored on the tag within a time span

IV. EXPERIMENTS AND RESULTS

Location tests, in this experiment, we used location information as a selective control to lock/unlock the tag. We took the reading of five locations around the campus and stored them as valid locations where the tag should be in an unlocked state.

Speed tests, we make use of the instantaneous speed of the GPS receiver in our experiments. We found the instantaneous speed from the GPS receiver matches the reading of odometer in the car. The kit designed was shown in below figure.

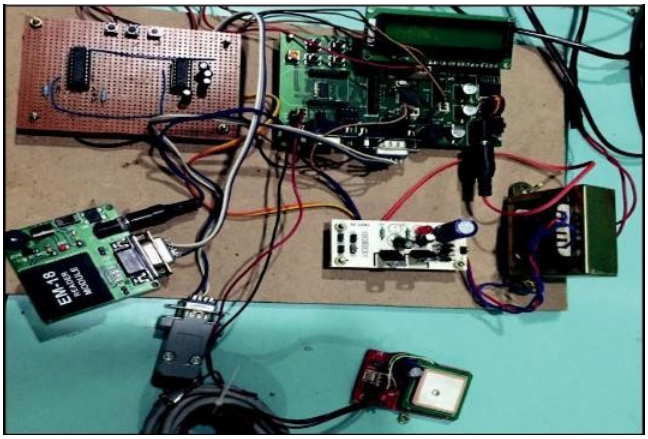


Fig. 4: Overall System

Fig. 5: Output of the System

V. 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 economical 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 Intel's 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.

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI:10.21276/ijcesr.2017.4.12.16

VI. REFERENCES

[1] G. Cropsey, "Designing a Distance and Speed Algorithm Using the Global Positioning System," [Online] Available: http://www.egr.msu.edu/classes/ece480/capstone/spring08/ group10/documents/ApplicationApplication%20Note-%20 Gabe.pdf, Mar. 2008.

[2] A. Czeskis, K. Koscher, J. Smith, 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.

[3] GM-101 Cost Effective GPS Module with Ttl Rs-232 Interface, [Online] Available: http://www.alibaba.com/ productgs/435104168/GM_101_Cost_Effective_GPS_ Module.html, 2011.

[4] GPS Glossory, [Online] Available: http://www.gsmarena. com/ glossaryphp3?term=gps, 2011.