International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Design of Location-Aware Selective Unlocking Mechanism via RFID and GPS

Bakyalakshmi. P
M.E ECE III Year
SCSVMV University,
Kanchipuram, India

Omkumar. S
Assistant Professor/ECE
SCSVMV University,
Kanchipuram, India

***Abstract*— A new approach has been proposed for enhancing 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. A 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, a location-aware selective unlocking mechanism has been designed using which tags can selectively respond to reader interrogations rather than doing so promiscuously. On the server side, a location-aware secure transaction verification scheme has been designed 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 the 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 defences do not rely on auxiliary devices or require any explicit user involvement.**

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 smartphones, 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 "ghost and-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.

Although a variety of security solutions exist, many of them do not meet the constraints and requirements of the underlying RFID applications in terms of (one or more of) efficiency, security, and usability.

In an attempt to address these drawbacks, this paper proposes a general research direction—one that utilizes sensing technologies—to address unauthorized reading and relay attacks in RFID systems without necessitating any changes to the traditional RFID usage model, i.e., without incorporating any explicit user involvement beyond what is practiced today. The premise of the proposed work is based on a current technological advancement that enables many RFID tags with low-cost sensing capabilities. Various types of sensors have been incorporated with many RFID tags. Intel's Wireless Identification and Sensing Platform (WISP) is a representative example of a sensor-enabled tag, which extends RFID beyond simple identification to in-depth sensing. This new generation of RFID devices can facilitate numerous promising applications for ubiquitous sensing and computation. They also suggest new ways of providing security and privacy services by leveraging the unique properties of the physical environment or physical status of the tag (or its owner). In this paper, we specifically focus on the design of context aware security primitives and protocols by utilizing sensing technologies so as to provide improved protection against unauthorized reading and relay attacks.

The physical environment offers a rich set of attributes that are unique in space, time, and to individual objects. These attributes—such as temperature, sound, light, location, speed, acceleration, or magnetic field—reflect either the current condition of a tag's surrounding environment or the condition of the tag (or its owner) itself. A sensor-enabled RFID tag can acquire useful contextual information about its environment (or its owner, or the tag itself), and this information can be utilized for improved RFID security and privacy without undermining usability.

II. Related Work

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.

III. Location Aware Defenses

Our proposed techniques are meant to defend against unauthorized reading, ghost-and-leech, and reader-and-leech attacks. Adversary models used in the three attack contexts are die rent slightly. In the following, 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 surreptitiously interrogate the tag. The goal of the adversary is to obtain tag specie in- formation and (later) use such information to peek 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 ghost), the adversary has further control over a malicious tag (the leech) which communicates with a valid reader. The ad- versary'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-leech attack, the adversary controls a mali- cious reader and tag pair, just like in the ghost-and-leech attack. However, the malicious reader controlled by the reader-and-leech 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, interrogations 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 attack contexts, we assume the adversary does not have direct access to the 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, once building gate, or retailer store) and thus GPS spoons around the victim reader can be easily detected. We do not consider loss or theft of tags.

A. *Location – Aware Selective Unlocking*

Using location-aware selective unlocking, a tag is unlocked only when it is in an appropriate (pre-specie) location. This mechanism is suitable for applications where reader location is _axed and well-known in advance. One example application is RFID-based building access system. An access card to an once building needs to only respond to reader queries when it is near the entrance of the building.

A pre-requisite in a location-aware selective unlocking scheme is that a tag needs to store a list of legitimate locations be- forehand. Upon each interrogation from a reader, the tag obtains its current location information 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 a 8KB of ash memory) and passive nature 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 act the 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.

Selective unlocking based on pure location information presents similar problems for toll systems as for the credit card sys- tems because toll cards will need to store a long list of toll booth locations2. We notice that vehicles mounted with RFID toll tags are usually required to travel at a certain speed when they approach a toll booth. For example, three out of eight toll lanes on the Port Authority's New Jersey- Staten Island Outer Bridge Crossing permit 25 mph speeds for E-Z Pass drivers; the Tappan Zee Bridge toll plaza and New Rochelle plaza, NY has 20mph roll-through speed; Dal- las North Toll way has roll-through lanes allowing speeds up to 30 mph. Hence, \speed" can be used as a valid context to design selective unlocking mechanisms for toll cards. That is, a toll card remains in a locked state except when the vehicle is travelling at a designated speed near a toll booth (such as 25-35 mph in the Dallas North Toll Way case). GPS sensors can be used to estimate speed either directly from the instantaneous Doppler-speed or directly from positional data differences and the corresponding time differences. For better protection against attacks, the speed and location can also be used together as a valid context for unlocking of toll cards. Here, the adversary will only be able to unlock the tag if both the valid location and speed criteria are satisfied.

B. 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, it- self 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 leech and then succeed in purchasing an item much costlier than what the user intended to buy. Addressing this reader-and-leech relay attack requires trans- action 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.

A display-equipped RFID tag can easily enable transaction verification for detecting reader-and-leech attacks. This, however, necessitates conscious user involvement because the amount displayed on the tag needs to be validated by the user and any user mistakes in this task may result in an attack. Distance bounding protocols have also been suggested as a countermeasure to the reader-and-leech attacks. However, these protocols are currently infeasible (as also reviewed in Section 5.1).

In this paper, we set out to explore the design of location-aware automated mechanisms for protecting against reader-and-leech attacks. We note that under such attacks, the valid tag and the valid reader would usually not be in close 2In some countries, toll-collection companies have set up roaming arrangements with each other. This permits the same vehicle to use another operator's toll system, thus reducing set-up costs and allowing even broader use of these systems. proximity (e.g., the tag is at a restaurant, while the reader is at a jewellery shop). 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. We note that such a solution can be deployed, with minor changes on the side of the issue bank, under the current payment infrastructure, where cards share individual keys with their issuer banks, and all communication takes place over secure channels.

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 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 passive 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 and passive GPS-enabled platform, and that our location-aware defenses are quite effective.

ACKNOWLEDGMENT

We would like to thank our University SCSVMV, my HOD, Dr. M. Sivanandham, my guide, Mr. S. Omkumar and other staff members for their continuous support and for their helpful comments on the earlier drafts of this paper.

REFERENCES

[1] A. Juels, "RFID Security and Privacy: A Research Survey," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 381-394, Feb. 2006.
[2] 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.
[3] A. Sample, D. Yeager, and J.R. Smith, "A Capacitive Touch Interface for Passive RFID Tags," Proc. IEEE Int'l Conf. RFID, 2009.
[4] A. Sample, D. Yeager, P. Powledge, and J. Smith, "Design of a Passively-Powered Programmable Sensing Platform for UHF RFID Systems," Proc. IEEE Int'l Conf. RFID, 2007.
[5] D. Schon, H. Lemelson, and W. Effelsberg, "Situation-Aware Choice of the Most Accurate Positioning System," Proc. IEEE Int'l Conf. Pervasive Computing Comm. Workshops (PerCom '12), 2012.
[6] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques Advances in Cryptology (EUROCRYPT), 1993.

[7] J. Bringer, H. Chabanne, and E. Dottax, "HB++: A Lightweight Authentication Protocol Secure against Some Attacks," Proc. Second Int'l Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006.
[8] R. Nithyanand, G. Tsudik, and E. Uzun, "Readers Behaving Badly: Reader Revocation in PKI-Based RFID Systems," Proc. European Symp. Research in Computer Security (ESORICS), 2010.
[9] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," Proc. IEEE Military Comm. Conf. (MILCOM), pp. 1-7, Nov. 2008.
[10] M. Buckner, R. Crutcher, M.R. Moore, and S.F. Smith, "GPS and Sensor-Enabled RFID Tags," http://www.ornl.gov/webworks/ cppr/y2001/pres/118169.pdf, 2013.
[11] M. Buettner, R. Prasad, M. Philipose, and D. Wetherall, "Recognizing Daily Activities with RFID-Based Sensors," Proc. Int'l Conf. Ubiquitous Computing (UbiComp), 2009.
[12] M. Calamia, "Mobile Payments to Surge to $670 Billion by 2015," http://www.mobiledia.com/news/96900.html, July 2011.
[13] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-Passports," Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (Securecomm), 2005.
[14] 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.
[15] 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.
[16] B. Hanlon, B. Ledvina, M. Psiaki, P.M. Kitner., and T.E. Humphreys, "Assessing the GPS Spoofing Threat," GPS World, http://www.gpsworld.com/defense/security-surveillance/ assessing-spoofin g-threat-3171?page_id=1, Jan. 2009.
[17] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, and T. O'Hare, "Vulnerabilities in First-Generation RFID-Enabled Credit Cards," Proc. Int'l Conf. Financial Cryptography and Data Security, 2007.
[18] J. Holleman, D. Yeager, R. Prasad, J. Smith, and B. Otis, "NeuralWISP: An Energy-Harvesting Wireless Neural Interface with 1-m Range," Proc. Biomedical Circuits and Systems Conf.
[19] J.R. Smith, P.S. Powledge, S. Roy, and A. Mamishev, "A Wirelessly-Powered Platform for Sensing and Computation," Proc. Eighth Int'l Conf. Ubiquitous Computing (UbiComp), 2006.
[20] sparkfun, "32 Channel San Jose Navigation GPS 5Hz Receiver with Antenna," http://www.sparkfun.com/products/8266, 2011.
[21] N.O. Tippenhauer, C. Popper, K.B. Rasmussen, and S. Capkun, "On the Requirements for Successful GPS Spoofing Attacks," Proc. ACM Conf. Computer and Comm. Security (CCS '11), Oct. 2011.
[22] D. Wagner, "Privacy in Pervasive Computing: What Can Technologists Do?" Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. (SecureComm '05), 2005.
[23] J.S. Warner and R.G. Johnston, "Think GPS Cargo Tracking = High Security?" technical report, Los Alamos Nat'l Laboratory, 2003.