www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 10078-10088

Context-Aware Approach for enhancing security and privacy of RFID

Lect. Nisha R. Wartha[1], Prof. Vaishali Londhe[2]

[1]Lecturer in Information Technology Department
Government Polytechnic, Thane,
nisha.wartha@gmail.com

[2]HOD of Computer Engineering Department
YadavraoTasgaonkar Institute of Engineering and Technology
vaishali.londhe@tasgaonkartech.com

Abstract: RFID systems have increasingly impact on both public and private domains. However, due to the inherent weaknesses of underlying wireless radio communications, RFID systems are plagued with security and privacy threats. Approach for enhancing security and privacy in certain RFID applications location-related information can serve as a legitimate access context. Examples of these applications include access cards, credit cards, and other payment tokens. To defend against unauthorized reading and relay attacks, such context information can be leveraged in two ways. First, contextual information can be used to design context-aware selective unlocking mechanisms so that tags can selectively respond to reader interrogations and thus minimize unauthorized reading and "ghost-and-leech" relay attacks. Second, contextual information can be used as a basis for context-aware secure transaction verification 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.

Keywords: RFID, relay attacks, context recognition, security and privacy, unauthorized reading.

1. INTRODUCTION

Radio Frequency Identification (RFID) is a wireless communication technology for automated identification of object and people. An RFID tag is a small microchip designed for wireless data transmission. RFID enables identification from a distance without requiring a line of sight.A typicalRFID system usually consists of tags, readers and/or back-end servers. Tags, also called transponders, are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personal identifiable. For example, a US e-passport stores the name, nationality, date of birth, digital photograph, and (optionally) fingerprint of its owner [11]. Other 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. Readers, also known as interrogators, broadcasts queries to tags in their radio transmission ranges for information contained in tags and tags reply with such information. The queried information is thensent to the server (which may co-exist 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).

Figure. 1.1: RFID system components.

Due to the inherent weaknesses of underlying wireless radio communication, RFID systems are plagued with a wide variety of security and privacy threats [12]. 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 [13]. 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 [12]. Promiscuous response also incites different types of relay attacks. One class of these attacks is referred to as "ghost-and-leech" [14]. In this attack, an adversary, called a "ghost,"

relays the information surreptitiously read from a legitimate RFID tag to a colluding entity known as a "leech." The leech 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-leech"; it involves a malicious reader using which the owner intends to make a transaction [15] . In this attack, the malicious reader, serving the role of a ghost and colluding with the leech, 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 deployments, including the Chip-and-PIN credit card system [15], RFID-assisted voting system [16], and keyless entry and start car key system [6].

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 tags 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 efficiency, usability and security.

PRIOR 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(mightsimplybea 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.

1) Hardware-Based Selective Unlocking

These include: Blocker Tag [19], RFID Enhancer Proxy [20] RFID Guardian [29], and Vibrate-to-Unlock [34]. All of these approaches, however, require the users to carry an auxiliary device (a blocker tag in [19], a mobile phone in [34], and a PDA like special-purpose RFID-enabled device in [20], [29]). Such an auxiliary device may not be available at the time of accessing RFID tags, and users may not be willing to always carry these devices. A Faraday cage can also be used to prevent an RFID tag from responding promiscuously by shielding its transmission. However, a special-purpose cage (a foil envelope or a wallet) would be needed and the tag would need to be removed from the cage in order to be read.

2) 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 were still unworkable even on high-end tags as of 2006 [18]. There has been a growing interest in the research com-munity to design lightweight cryptographic mechanisms (e.g., [10], [21]). However, these protocols usually require shared key(s) between tags and readers, which is not an option in some applications.

3) Distance Bounding Protocols

These protocols have been used to stop relay attacks [8]. A distance bounding protocol is a cryptographic challenge-response authentication protocol which allows the verifier to measure an upper-bound of its distance from the prover [3]. (We stress that traditional ``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 [8]. The upper-bound calculated by an RF distance bounding protocol, how-ever, is very sensitive to response time delay, as even a light delay (a few nanoseconds) may result in a significant error in distance bounding. Therefore, even XOR- or comparison-based distance bounding protocols [3] are not suitable for RF distance bounding since simply signal conversion and modulation can lead to significant delays. A recent protocol eliminated the need for signal modulation and instead utilized signal reflection and channel selection, achieving a processing time of less than 1 *ns* at the prover side [28]. However, the protocol requires specialized hardware at the prover side for channel selection. This renders existing protocols currently infeasible for even high-end RFID tags.

2. LITERATURE SERVEY

In "Context-Aware Defenses to RFID Unauthorized Reading and Relay Attacks" Tzipora Halevi, Haoyu Li proposes the use of cyber-physical interfaces, on-board tag sensors, to (automatically) acquire useful contextual information about the tag's environment (or its owner, or the tag itself). First, such context recognition is leveraged for the purpose of selective tag unlocking the tag will respond selectively to reader interrogations. In particular, novel mechanisms based on an owner's posture recognition are presented. Second, context recognition is used as a basis for transaction verification in order to provide protection against a severe form of relay attacks involving malicious RFID readers.A new mechanism is developed that can determine the proximity between a valid tag and a valid reader by correlating certain (specifically audio) sensor data extracted from the two devices. The evaluation of the proposed mechanisms demonstrates their feasibility in significantly raising the bar against RFID attacks.

Mr. A. Bharath Kumar and O. Anushareports in "Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing" on a new approach 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. They 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.The premise of their 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.

In "An Enhanced Digital Campus Security System Using RFID, GPS, GSM" A.Ashok Kumar,

P.Swapnadesigned and implemented a Digital Campus Security System (DCST) base on the RFID, GPS and GSM network. DCST reads the RFID tags and sends information to lpc2148.processor gives alerts through GSM network. If any invalid RFID (Thief) information comes into mobile they get the real-time tracking for valuables. Where the thief arrives anyone access control node, it would be blocked. User can also manage its own valuables such as lending and recovery operation through the web manager centre.

Di Ma and Nitesh Saxena proposes a novel research direction in "A Context-Aware Approach to Defend Against Unauthorized Reading and Relay Attacks in RFID Systems", that utilizes sensing technologies, to tackle the problems of unauthorized reading and relay attacks with a goal of reconciling the requirements of efficiency, security, and usability. The premise of the proposed work is based on a current technological advancement that enables many RFID tags with low-cost sensing capabilities.

Zhaoshun Wang, Hongsong Chen, Xiaoli Huang investigate the possible privacy and security threats to RFID systems, and consider whether previously proposed RFID protocols address these threats. We have reviewed the privacy, security, and performance requirements for RFID protocols. At the same time, we compare the security mechanism for RFID security. It is very useful to design and issue the RFID related protocol and standard .This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context in "Research for Threats and Security in Rfid Information System".

.

3. PRPOSED SYSTEM

In an attempt to address the drawbacks of prior research, this paper proposes a novel research direction, one that utilizes sensing technologies, to address unauthorized reading and relay attacks in RFID systems. 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 to 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 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, 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). Such contextual information can be leveraged in two ways:

- First, contextual information can be used to design context-aware 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 leverage upon "context recognition" 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, i.e., without imposing additional user burden. For example, an office building access card, equipped with a location sensor, can remain locked unless it is near the (fixed) entrance of the building. The following selective unlocking mechanisms will be explored as (i) magnetic-field triggered proximity sensing, (ii) posture recognition, and (iii) location sensing and location classification.
- Second, contextual information can be used as a basis for context-aware secure transaction verification to defend against special relay attacks involving malicious readers. For example, a bank server will deny a $2000 transaction when it detects the tag (RFID credit card) is currently located in a restaurant where a normal transaction is usually less than $200. The following two context-aware secure transaction verification schemes will be explored as: (i) numeric digit-based speech recognition, and (ii) location sensing and location classification.

The design of context recognition for RFID tags poses several challenges. First, the resource constraints of RFID tags hamper the complexity of the algorithms that can be used to judge what activity a tag is currently undergoing. Another obstacle is the lack of ways in which users can interact with their tags. RFID tags, being geared for automation, were designed to be astransparent as possible to their users, and as such lack any input or output interfaces such as buttons and displays. Moreover, many users are typically not in direct contact with their tags because they prefer to keep them inside other objects, such as wallets or purses [36]. For example, it is a common practice to swipe one's wallet containing the tag against the reader rather than taking the tag out from the wallet and directly swiping the tag. We note the proposed approach may not provide absolute security due to the possibility of errors associated with context recognition; however, it raises the bar even for sophisticated adversaries without affecting the RFID usage model. In addition, although the proposed techniques can work in a stand-alone fashion, they can also be used with other security mechanisms, such as cryptographic-based schemes, to provide stronger cross-layer security protection according to different security needs in various applications. Moreover, many of the proposed ideas and techniques will be applicable in the realm of other wireless (or wired) devices equipped with sensors. Because sensors serve as a bridge between the physical and the digital world, the proposed sensing-centric mechanisms will be instrumental towards providing dependability, security and privacy for complex Cyber-Physical Systems.

4.METHDOLOGY

CONTEXT-AWARE SELECTIVE UNLOCKING

The traditional selective unlocking techniques require special-purpose hardware and/or explicit user involvement, both greatly decrease the usability and acceptability of such solutions. To remedy this, we propose selective unlocking schemes based on context recognition, focusing not only on security and privacy, but also on usability. Below first review two recent works on selective unlocking based on context

recognition and discuss their merits and demerits. Next outline possible selective unlocking mechanisms based on conventional sensors such as accelerometer, magnetometer (compass), and location sensors. For each mechanism, discussed associated design challenges and also suggest specific application(s) that could benefit from it.

4.1. Previous Recent Work

"Secret Handshakes" is a recently proposed interesting selective unlocking method that is based on context inference [36]. In order to unlock an accelerometer-equipped RFID tag [32, 39] using Secret Handshakes, a user must move or shake the tag (or its container) in a particular pattern. A number of unlocking patterns were studied and shown to exhibit low error rates [36]. A central drawback to Secret Handshakes, however, is that a unique movement pattern is required for each tag to be unlocked. This requires subtle changes to the expected RFID usage modelwhile a standard, insecure RFID setup only requires users to bring their RFID tags within range of a reader.

.

Figure 4.1: Example of secret handshake/activation scheme. Both images show the alpha (α) motion per-formed with the card in front of the reader. In the left image, numbers indicate sequence of card positions across reader with time. In the right image, arrows show how the card moves across the reader with time.

Figure 4.2: Example secret handshake/activation scheme. In this image demonstrates the 1.5-wave gesture.

Keeping in mind the goal of not incorporating any usage model changes, "Motion Detection" [40] has been proposed by us as another selective unlocking scheme. In Motion Detection, a tag would respond only when it is in motion, instead of doing so promiscuously. In other words, if the device is still, it remains silent. This approach hinges on the straightforward observation that accessing a personal mobile RFID tag fundamentally involves moving it in some manner (e.g., swiping an access card in front of the reader). Although Motion Detection does not require any changes to the traditional usage model and raise the bar required for some common attacks to succeed, it is not capable of discerning whether the device in motion is due to a particular gesture or because its owner is in motion. Hence, the false unlocking rate of this approach is high, meaning there is a high chance that a tag gets unlocked when it actually should have been locked. In the following, we outline several new context-aware selective unlocking mechanisms which (1) have both low false locking and false unlocking rates, and (2) do not necessitate any change to the current usage model.

4.2. Selective Unlocking based on Proximity Sensing

Using this mechanism, a tag gets unlocked whenever it detects it is near a reader. The requirement for tag and reader being near is common in most RFID applications. For example, while making a payment, a user typically needs to bring his/her contactless credit card (or its container) closer to the reader for transaction processing. This requirement can therefore serve as an effective means to establish a valid context. One possible way of proximity sensing is through scalar magnetometers that measure the total strength of the magnetic field they are subjected to. More specifically, a magnet would be attached to the reader, and when the tag is brought close to the reader, the tag's on-board magnetometer would sense the magnetic field and the tag would get unlocked if the strength of the magnetic field is above some pre-defined threshold. If an adversary intends to unlock a tag, it cansimply be in very close proximity of the tag, just like a valid reader. However, being near, increases the chances of the challenger being detected. To remain secret, the challenger is therefore forced to generate a stronger magnetic field from an undetectable distance. Our preliminary investigation shows this attack does not seem feasible.

We also note that iron and steel can cause shielding effects on magnetic fields. Other materials such as wood, Plexiglas, Styrofoam, brass, copper, aluminum, leather or paper have almost no effect on shielding magnetic fields. This means that a magnetometer can work even when encased in many objects, such as wallets, purses or backpacks. This suggests that a magnetometer-equipped tag would not need to be removed from its container while accessing the tag.

4.3. Selective Unlocking based on Posture Recognition

"Secret Handshakes" described is based on gesture recognition. To unlock an accelerometer-enabled tag, a user has to move the tag in a special pattern - gesture. Hence "Secret Handshakes" is obtrusive and requires explicit user involvement, which is not convenient in a frequent use and reduces the usability of such approach. This motivates the need for study posture recognition to achieve non-obtrusive selective unlocking that does not require user involvement. We liberally use "posture" to denote activities performed by users without special intention but can serve as a valid context in certain applications. One class of such applications involves implanted medical devices (IMDs). Under legitimate IMD access, we can assume that the patient is lying down on his or her back. Thus, access to the IMD will be granted only when the patient's body is such a pre-defined unique posture. This will prevent an attacker from controlling the IMD in many common scenarios, such as while standing just behind the patient in public. Since posture formations are human activities performed by users unconsciously, posture recognition can provide a finer-grained non-obtrusive unlocking mechanism without purposeful or conscious user involvement.

Posture recognition is similar to gesture recognition to a certain extent. Similar to the gesture recognition Schemes

(like the Secret Handshakes scheme [36] we discussed previously), in a posture recognition scheme, user movement can be recorded by motion sensors such as accelerometers and the captured motion data is then compared with a reference posture template which has been recorded by performing the corresponding movement in a reference coordinate system. A match between the captured data and the reference template implies that the user has exhibited a certain posture transition defined by the reference template. However, there is one primary difference between gesture recognition and posture transition recognition, i.e., device tilt. In (hand) gesture recognition systems, users are assumed to be aware of their hand activities. So gestures are performed in a more-or-less controlled way without tilting the tag so that the effect of tilt can be greatly minimized or ignored. However, in posture transition recognition, as we do not require any explicit user involvement, the tag, placed inside a human body in the form of an IMD or into the pockets in the form of a car key, can be tilted due to the movement of human body or the device positioning itself. The reference template is usually collected in a reference coordinatesystem. However, once a device is tilted, movement data collected from the device is no longer in the reference coordinate system and the corresponding posture will not be detected correctly. It is therefore critical to detect the tag's orientation in order to rotate the data vector back to the reference coordinate system for correct recognition.In order to optimize our algorithms (due to RFID resource constraints), we classify postures into two primary types: posture and posture transition. Posture means a static bodily position that a user can maintain for certain duration, such as lying, sitting, standing and walking. Posture transition subsumes different human movements, such as ``stand-to-sit," ``sit-to-stand," ``sit-to-lie," ``lie-to-sit," and so on. Posture transitions capture the dynamics of human movement and usually only last for a short duration.

We analyze the features of these two posture types and realize that most of the postures and some of the posture transitions can be simply detected by measuring direction changes or status changes in sagittal and transverse planes. In case of posture recognition, consider, for example, an IMD such as a pacemaker implanted into the patient's chest area equipped with a 3-axes accelerometer. As the IMD is fixed to the human body, it remains static relative to the body system but has different orientations in the earth coordinate system (magnetic north and gravity) due to human body movement. Thus, we can detect such movements by simply monitoring its relative orientation change in the earth coordinate system. For example, when the patient is in the ``sitting" position, the Z axis of the accelerometer points to the sky and the X-Y plane is parallel to the earth surface. When the patient lies down, the Z axis now should be parallel to the earth surface while one of the X or Y axis should point to the sky. Thus, by simply monitoring the change of directions of axes, we can tell whether a patient is lying or not. We note that mobile devices also commonly use such detection techniques based on accelerometer axis direction change to perform screen rotation functions. Similarly, the work of tracks direction changes of magnetometer axes during walking.

Current systems for full orientation estimation, such as the one in Apple iPad2, usually use a set of sensor modalities – typically including gyroscopes, accelerometers and magnetometers – to estimate device orientation. Gyroscopes are used to determine accurately angular changes while the other sensors are used to compensate the integration drift of the gyroscopes and keep this estimate drift free. However, a typical gyroscope requires about 5 10 times more power than magnetometer and accelerometer together. Moreover, its comparably larger form factor also makes gyroscope not commonly available in a tiny single package MEMS chip. Considering the resource constrained RFID platforms, it might be necessary to restrict from using gyroscopes, and instead focus on using accelerometers and/or magnetometers for device orientation and posture estimation. As integrated accelerometers and magnetometers are commercially available in tiny packages, an RFID tag with such sensors can be flat and less obtrusive for the user, which makes them very attractive to be used in IMDs or smart car keys. There exist several attempts to use either accelerometers or magnetometers; however, it has been shown that neither of the two sensors is good enough alone to estimate full orientation. On the other hand, orientation estimation schemes that useboth accelerometers and magnetometers show very promising results.

4.4. Selective Unlocking based on Location Sensing and Location Classification

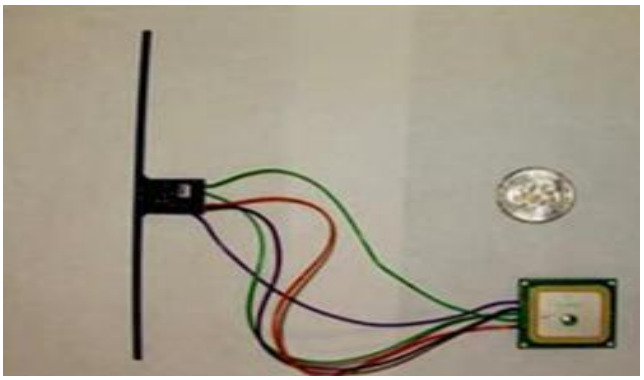

Figure 4.3. Location-aware selective unlocking where Locking is legitimate location (or speed) info stored on the tag side and Loc_{GPS} is the location info obtained from on-board GPS upon a reader request.

We notice in quite some applications, (under normal circumstances,) tags only communicate to readers at some specific locations. 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 (which may be located all over the world); toll cards usually only communicate with toll readers in certain fixed locations and when the car travels at certain speed. Hence, location can serve as a good means to establish a valid context. That is, a tag is unlocked only when it is in an appropriate (pre-specified) location. It is suitable for applications where reader location is fixed and well-known in advance.

Location information can be easily obtained through GPS sensors. A new tag from Numerex and Savi Technology has been equipped with GPS sensors and has the ability to conduct satellite communications. Researchers in Oak Ridge National Laboratory also worked with RFID system suppliers in developing new tags by combining GPS and environmental sensors. These tags are designed to track goods anywhere within a global supply chain. A prerequisite in a location-aware

selective unlocking scheme is that a tag needs to store a list of legitimate locations beforehand. Upon each interrogation from a reader, the tag gets 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 (WISP has a 8KB of flash memory) and passive nature of tags, the list of legitimate locations should be kept short. Otherwise, testing whether the current location is within the legitimate list may cause unbearable delay and affect the performance of the underlying access system. Moreover, the list of legitimate locations should not change a lot since otherwise users have to do extra work to securely update the list on their tags. So selective unlocking based on pure location information is more suitable to be used in 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, store closing and new store opening happen on a frequent basis.

Selective unlocking based on pure location information presents similar problems when it is applied to RFID toll systems since a toll card needs to store a long list of toll booth locations. We notice 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-ZPass drivers; the Tappan Zee Bridge toll plaza and New Rochelle plaza, NY has 20mph roll-through speed; Dallas 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 traveling 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.

One disadvantage with the GPS-based approach is the reliance on the GPS infrastructure. Thus, selective unlocking would require the constant accessibility of this infrastructure. Another disadvantage is potential delay due to initialization process of GPS receivers. A GPS receiver can have either a cold start or hot start. The hot start occurs when the GPS device remembers its last calculated position and the satellites in view, the almanac (i.e., the information about all the satellites in the constellation) used, the UTC Time, and makes an attempt to lock onto the same satellites and calculate a new position based upon the previous information. This is the quickest GPS lock but it only works if the receiver is generally in the same location as it was when the GPS was last turned off. The cold start is when the GPS device dumps all the information, attempts to locate satellites and then calculates a GPS lock. This takes longer time because there is no known or pre-existing information. The GPS module we are currently experimenting with can normally acquire a fix from a cold start in 35 seconds, and acquire a hot-start fix in less than 2 seconds. For applications which have extremely low delay tolerance, a storage capacitor can be added to the tag in order to help the GPS receiver keep running to avoid cold start [37]. Another disadvantage of the GPS-based approach is that multiple entities may share the same location information, which might not be desirable in some cases. For example, the stores at the same place, but on different levels of a shopping mall, can share the same altitude and latitude information. This motivates the need to design a "localized" approach to location sensing,that does not require any additional infrastructure besides the RFID. One idea is to make use of (multiple) environmental sensors (such as microphone, thermometer, or magnetometer, and perhaps odor and gas sensors) as a means to derive the location-specific information. The intuition is that the "localized data" gathered by these sensors is unique per location (or type of location, such as an office or a hospital), and thus one can build a classifier that can associate this data with a particular location. To justify this, we can consider the example of an access card application. The noise, temperature and odor levels, for instance, and their variations within a certain timeframe, at the office entrance, and at a nearby cafeteria or outside the office building are likely to be quite different. Thus, a classifier can be "trained" to acquire unique features from sensor data gathered at the office entrance building. On every read request (malicious or otherwise), the card will "test" the classifier on current sensor data and get unlocked only on a positive classification instance. Another example is that of an implanted medical tag [38], which will only get unlocked when the classifier detects it to be inside a hospital or a doctor's office, which may possess some unique sensor extracted features.

There exists some prior research which demonstrates the potential for sensor-based location classification. Other prior work also considers wireless radio receivers to address a similar problem. A number of challenges need to be addressed in order to realize the RFID location classification approach, however. First, distinct features of environmental data (a "location fingerprint") need to be identified, that remains constant across time, but can be used to uniquely identify a given location (or a location type). Second, a simplistic classifier needs to be developed that can be accommodated within the constraints of an RFID tag; traditional machine learning classifiers may not be feasible due to their high computational requirements. Third, the classifier needs to be robust enough to be used in practice, with low classification errors. The location estimation based approach may not be as fine-grained as the GPS approach. However, we view it as a much simpler alternative, and believe that it can be employed to provide improved security in the face of many common attacks.

CONTEXT-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 he/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. Perhaps more seriously, such a malicious reader can also collude with a leech and can succeed in purchasing an item much costlier than what the user intended to buy [15]. As addressing this problem requires secure 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 A display-equipped RFID tag can easily enable secure transaction verification. This, however, necessitates user involvement because (1) the tag must be taken out of one's wallet or purse, and (2) the amount displayed on the tag needs to be validated by the user. Distance bounding protocols have also been suggested as a

countermeasure to the reader-and-leech attacks [15]. However, these protocols are currently infeasible. One possible approach is for the user to indicate to the tag the intended amount of transaction (instead of the tag displaying this to the user, which requires direct access to the tag). Use of touch sensors [31] or on-board buttons is not feasible for this purpose as they would also require direct tag access; buttons will also hamper tag's form factor. Secret Handshakes [36] could be extended though. The user could create numeric patterns depicting the amount by moving her accelerometer-enabled tag (or wallet containing the tag). For example, user can create a '5' and then two '0's up in the air to indicate a transaction worth $500. This method, however, has the same shortcomings as Secret Handshakes – it requires explicit user involvement and has usability implications. Another, potentially more user-friendly, solution is to have the user speak-out the amount of transaction (e.g., digit-by-digit), which the tag can record using an on-board microphone and decode. This method requires some form of numeric speech (digit) recognition.

In order to provide improved resilience, specifically, to reader-and-leech attacks, location sensing could be used. Note that under such attacks, the valid tag and the valid reader would usually not be in close proximity (e.g., the tag is at a restaurant, while the reader is at a jewelery shop [15]). This is unlike 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 that of the reader would imply the presence of such attacks. Specifically, the tag (credit card) detects its current location and sends this location information encrypted with the key that it pre-shares with its issuing bank; the bank will then compare the tag's location with that of the (jewelry) merchant 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 issuer bank, under the current payment infrastructure, where cards share individual keys with their issuer banks (as discussed in [15]).GPS-enabled tags could be used for determining the tag's location. Similarly, the location classification approach described in previous section can also be employed; here the classifier will be executed by the bank's server – not by the tag locally as in selective unlocking – to "test" for tag's location against reader's location. We note that this solution will raise the bar against reader-aided relay attacks because it forces the attacker to be in the same location as the tag's owner in order to be successful.

5. APPLICATION

Initially, the deployment of RFID technology was confined to some simple applications like inventory and antitheft. However, it has been deployed in more sophisticated areas today, such as in electronic IDs and passports. Even though RFID is a technology that can be applied in numerous business scenarios its prime functionality is the identification of objects. With this background the following sections describe the most important application areas of RFID. A sample of applications is shown here:

5.1 Access and Route Control

Convenient RFID tags can replace magnetic cards and chip cards for access control or bank accounts. Users only have to position their card near a reader. Consequently high standards for security mechanisms are required in order to avoid fraud. For most applications the familiar plastic card format is used but housing the chip in watches or key fobs is also an option. Typical frequencies are in the 13,56 MHz area. Reader's support ranges of up to one meter. Apart from identification writing and updating tags is also possible. Access control systems can increase efficiency whenever a great number of people have to pass the same access point as it is the case in large companies and holiday resorts. Recently greater airlines have started using RFID for baggage routing to reduce errors. Another popular application area of RFID is the packet routing within companies. Usually only simple tags with a uniqueidentifier are required. Tracking information is stored in a central database, which is up dated whenever the packet passes a control point. This way customer can query the state of their
order via Internet.

5.2 Document Verification

Current pilot projects deal with the use of RFID in identity cards and travel documents. The tag is used to implement anti-forgery mechanisms and in further consequence provide extended verification capabilities. These mechanisms include the saving of biometric data, such as face and fingerprints, on the tag. There is a tendency towards cross-linking different identification features thus creating a multi-biometry platform to compensate for weaknesses of individual technical methods.

5.3 Asset Management

Particularly airports and vehicle factories, where the asset management comes in as amajor cost factor, can benefit from RFID. Firstly shrinkage and theft can be eliminated; secondly many processes can be optimized. Therefore RFID brings significant competitive advantage by:

1. *Avoidance of delays.*
Search actions for parts, tools, or documents are eliminated.
2. *Avoidance of human errors.*
The right parts and tools can be identified, and no toolsget misplaced or lost. This results in higher quality and security.
3. *Automation of documentation.*
Actions, tool use, and completeness checks are documented automatically.
4. *Efficient use of resources.*
The use of mechanics, parts, and tools is planned andmonitored.

5.4 Supply Chain

The supply chain is a multi-stage process, which involves everything from the supplying of prime materials, used to develop pro ducts, to the pro ducts delivery to customers via warehouses and distribution centers. Supply chains exist in service, manufacturing and retail organizations. Although, the complexity of the chain changes greatly from one industry branch to another, its management can be seen as the organization of the flows of these materials, as they move through the various processes. The efficiency of the supply chain has a direct impact on the profitability of a company. Therefore any major company striving for competitive edge needs to invest in infrastructures to control inventory, track products and manage associated finance. By increasing transparency in the supply chain, RFID allows the optimization of logistic process. The primary goal is the discovery of inefficiencies in the value chain within and between the companies thus rationalizing the material, information and financial flows. RFID enables the fine grained tracking of lot sizes down to one, over the entire logistic network, thus facilitating the detection and the locating of losses and shrinkage, the result of misplaced orders, theft and inefficient

stock management.

5.5Animal Tracking

This application of RFID technology is used for either tracking wild animals in scientific studies, or tracking pets when they are lost.

5.6 Contact-less Payments

Blue-chip companies such as American Express, ExxonMobil, and MasterCard use RFID technology on their products for contact-less payment.

5.7 Hospitals and healthcare

Adoption of RFID in the medical industry has been widespread and very effective. Hospitals are among the first users to combine both active and passive RFID. Many successful deployments in the healthcare industry have been cited where active technology tracks high-value, or frequently moved items, where passive technology tracks smaller, lower cost items that only need room-level identification.For example, medical facility rooms can collect data from transmissions of RFID badges worn by patients and employees, as well as from tags assigned to facility assets, such as mobile medical devices.

5.8 **Libraries**

Libraries have used RFID to replace the barcodes on library items. The tag can contain identifying information or may just be a key into a database. An RFID system may replace or supplement bar codes and may offer another method of inventory management and self-service checkout by patrons. It can also act as a security device, taking the place of the more traditional electromagnetic security strip.Since RFID tags can be read through an item, there is no need to open a book cover or DVD case to scan an item, and a stack of books can be read simultaneously. Book tags can be read while books are in motion on a conveyor belt, which reduces staff time. This can all be done by the borrowers themselves, reducing the need for library staff assistance.

6. SECURITY ANALYSIS

There are two main issues in RFID systems which are highlighted in this paper: privacy issues and security issues. These issues, although interrelated, are different. RFID tags and associated sensors are utterly dependent on reader transmissions for energy. A malicious entity that gains control of an RFID reader could thus trivially perform a denial-of-service (DoS) attack by simply refusing to supply enough power for the sensor to operate. Rather than a DoS attacker, in our evaluation, we consider a more clever opponent that may attempt to manipulate onboard tag sensors by subtly adjusting reader parameters. One such attribute is the rate at which a reader issues requests to tags. If an RFID protocol requires that a tag samples its sensor data each time it wakes up, an attacker could manipulate the rate at which samples are taken by changing the frequency at which a reader issues queries. This may have undesirable consequences from a security perspective. Sensor readings taken at different periods may contain more or less entropy, for instance. Along the same lines, an adversary could modify the signal strength of a RFID reader's transmissions in order to change the amount of power that is made available to tags. Since some tag hardware requires more power to operate than others, this could potentially alter the behavior of sensing hardware. A sensor may not operate correctly, and its output may be less accurate or more predictable when it is supplied with less power than its designers intended. With respect to RFID, we define these issues as follows:

1. **Privacy**: the ability of the RFID system to keep the meaning of the information transmitted between the tag and the reader secure from non-intended recipients.
2. **Security**: the ability of the RFID system to keep the information transmitted between the tag and the reader secure from non-intended recipients.

6.1 PRIVACY ISSUES

The major concern which thwarts widespread deployment of RFIDs is the possibility of privacy violation. This issue seems to be very difficult to tackle because it originates from the basic functions of RFID tags. As mentioned, each RFID tag contains a unique ID which identifies it through an RF wireless interrogation. This results in high risk of identification or tracking of bearers by illegitimate entities unless sufficient protection is used.

In general, violation of privacy has two forms: information leakage and location tracking. Information leakage includes obtaining the information from the tag to identify its owner, his preferences or physical condition. For example, if a person carries a bottle of medications with attached RFID tag, obtaining the information of the RFID tag may point to his disease. As RFID tags can be attached to almost every item we use in everyday life, obtaining their information can reveal a vast amount of data about a person's life style and therefore violates his/her privacy. This kind of information might be interesting for variety of entities e.g. marketers can obtain and use these leaked information to link buyers to specific items and make personal profiles in order to give them specialized sale offers. On the other hand, even if the tag responses do not leak information about the product it has been attached to, static responses of the tags during interrogations helps with tracking the owners.

6.2 SECURITY ISSUES

The security issues can exist in all RFID systems' components. In this subsection, we briefly explore some of the security issues related to the tags, readers and the communication between them.

6.2.1. SECURITY ISSUES OF THE TAG

Some of the security issues for the tags are:

- **Falsification of ID:** In this security issue, an attacker first obtains/steals the ID or other sensitive data of a tag and uses it to impersonate the tag and deceive the readers in further interrogations. This can be achieved by using an emulator tag or copying the obtained information on another tag (cloning or counterfeiting).

- **Unauthorized deactivation:** Each RFID tag based on EPC C1G2 has a mechanism for deactivation using kill command. Unauthorized usage of this command can render the tag unusable in further interrogations and deactivate the tag permanently.

- **Physical destruction:** Tags can be physically destroyed in different ways, for example by using strong electromagnetic fields (e.g. a microwave oven) or by some chemical substances. In the case of active tags, they could also be rendered unusable by removing their battery.

- **Detaching the tag:** A tag can be separated from the tagged item. The detached tag may even subsequently be attached to a different item. This type of attack poses a fundamental security problem because RFID systems are completely dependent on the unambiguous identification of the tags.

- **Falsification of Contents:** If the tags contain some extra data except from ID and security information, the data can be falsified by unauthorized write access to the tag while the ID (serial number) and any other security information (e.g. keys) remain unchanged. In this way, the readers continue to recognize the identity of the tags correctly while their contents have been changed.

6.2.2. SECURITY ISSUESOF THE READER

Readers are also susceptible to falsifying ID attack. In a secure RFID system, the reader must prove its authorization to the tag. If an attacker wants to read the data with his own reader, this reader must fake the identity of an authorized reader. If an attacker accomplishes to falsify the reader's ID, he/she will be able not only to have access to the tag's information but also to the back-end system.

6.2.3. SECURITYISSUESOFTHECOMMUNICATIONS

The communications between the components of RFID systems also suffer from security issues. Nevertheless, the level of vulnerability significantly differs from communication between the tag and the reader to communication between the reader and back-end system. While the latter is considered robust and almost secure due to application of standard security measures such as SSL or TLS, the former is the most vulnerable part of the whole system. Some of the security issues in the communication between the tag and the reader are listed below.

- **Eavesdropping:** The communication between reader and tags via the air interface can be monitored by intercepting and decoding the radio signals. This is one of the most specific threats to RFID systems. The eavesdropped information could for example be used to collect sensitive information about a person. It could also be used to perform a replay attack.

- **Replay Attack:** The attacker can obtain and save all the exchanged messages between a tag and a reader and either simulates the tag or the reader towards one another.

- **Jamming:** The air interface between reader and tag can be disturbed in order to attack the integrity or the availability (Dos attack) of the communication. This could be achieved by powerful transmitters at a large distance, but also through more passive means such as shielding.

- **Man-in-the-middle:** A man-in-the-middle attack is a form of attack in which the adversary provokes or manipulates the communication between the reader and the tag, where manipulating the communication means relay, withhold, or insert messages.

- **Relay attack:** A relay attack is similar to the well known man-in-the-middle attack. A device is placed in between the reader and the tag such that all communication between reader and tag goes through this device, while both tag and reader think they communicate directly to each other. In the case of payment systems, the attacker is able to charge someone else's payment device (e.g. a smart card with an RFID tag) to buy something for herself.

6.3. SOLUTIONS

Proposed solutions to security and privacy issues in RFID systems include defensive measures that could be taken in two levels: technical and management levels. To have a concrete solution for RFID system, it requires having a holistic perspective to the problem and adopting a combination of measures in both levels. In the management level, it is required to:

- Have an up-to-date risk assessment of the whole system to be aware of the possible threats and vulnerabilities in the system.

- Establish policies for the security of the data to tackle the risks. Incorporate security solutions that are transparent.
- Realize that security is an ongoing process.

There are quite a few related works in this layer in the literature such as well as some guidelines and recommendations. One of the first and best known proposals in this context is "RFID Bill of Rights" which proposes five privacy addressed articles for RFID systems: (1) The right to know whether products contain RFID tags, (2) the right to have tags removed or deactivate upon purchase of these products, (3) the right to use RFID-enabled services without RFID tags (i.e. right to opt out without penalty), (4) the right to access an RFID tag's stored data along with the possibility to correct and amend that data, and finally (5) the right to know when, where, and why the tags are being read.In addition, there are plenty of proposals in the technical level which can be categorized in four following groups:

- **Tag Killing Command or Permanent Deactivation:**

Using the kill command in RFID tags in an authorized manner (e.g. after shopping the tagged item) makes the tag permanently deactivated and thus renders any subsequent unauthorized reading impossible. It should be noted that although killing tags effectively enforces consumer privacy, it eliminates all of the post-purchase benefits of RFID for the customer.

- **A Faraday Cage or Jamming Approach:**

  Faraday Cage is a metal or foil-lined container that is impenetrable to radio frequency waves. By putting RFID tags inside a Faraday Cage, they can be made protected from reading by isolating them from any kind of electromagnetic waves. The reading of RFID tags may also be jammed by devices that emit powerful and disruptive radio signals. But usually such jamming devices violate government regulations on radio emissions.

- **Use of Blocker Tags:**

  A blocker tag is a special RFID tag that prevents unwanted scanning of tags.

- **Cryptography:**

  To achieve privacy in RFID systems, a typical solution can be the adoption of cryptographic techniques. Never the-less, this cannot be achieved through conventional cryptography due to special limitations of passive low-cost RFID tags. In the following section, we will discuss the paradigm shift which took place in cryptography to fulfill these limitations and led to coin the term lightweight cryptography in the literature.

7. CONCLUSION

This Seminar presented novel defenses to unauthorized reading and relay attacks against RFID systems without necessitating any changes to the traditional RFID usage model. More specifically, we proposed the use of on-board tag sensors to acquire useful contextual information about the tag's environment. First, such context recognition was leveraged for the purpose of selective tag unlocking. In particular, selective unlocking mechanisms based on owner's posture recognition were presented. Second, context recognition was used as a basis for transaction verification in order to provide protection against relay attacks involving malicious RFID readers. More precisely, a transaction verification mechanism was developed that can determine the proximity between a valid tag and a valid reader by correlating audio sensor data extracted from the two devices.

Evaluation of all the proposed mechanisms demonstrate their feasibility in effectively and significantly raising the bar against many lingering RFID attacks without negatively affecting the currently employed usage model of the underlying RFID applications.

REFERENCES

1. TziporaHalevi, Haoyu Li, Di Ma, NiteshSaxena, Jonathan Voris, And Tuo Xiang, "Context-Aware Defenses to RFID Unauthorized Reading and Relay Attacks", 2168-6750, 2013, IEEE**.**
2. Mr.A.Bharath Kumar and O.Anusha "Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing",International Conference on Computer & Communication Technologies 2K14 March 28-29, 2014|Hyderabad, INDIA.
3. S. Brands and D. Chaum, ``Distance-bounding protocols," in *Proc. Int.Conf. Theory Appl. Cryptograph. Tech. Adv. Cryptol. EUROCRYPT*, 1993, 344 359.
4. U. Blanke and B. Schiele, ``Towards human motion capturing using gyroscopeless orientation estimation," in *Proc. 14th ISWC*, Oct. 2010, 20 35.
5. Bakyalakshmi. P, Omkumar. S,"Design of Location-Aware Selective Unlocking Mechanism via RFID and GPS",International Journal of Engineering Research & Technology (IJERT) ,IJERTIJERT,ISSN: 2278-0181,Vol. 3 Issue 3, March – 2014..
6. Francillon A, Danev B, Capkun S. Relay attacks on passive keyless entry and start systems in modern cars. 18th Annual Network and Distributed System Security Symp11. Juels A, Molnar D, Wagner D. Security and privacy issues in E-passports. Security and Privacy for Emerging Areas in Communications Networks (Securecomm), 2005.
7. S. Brands and D. Chaum, ``Distance-bounding protocols," in *Proc. Int.Conf. Theory Appl. Cryptograph. Tech. Adv. Cryptol. EUROCRYPT*, 1993,344 359.
8. A. Francillon, B. Danev, and S. Capkun, ``Relay attacks on passive keyless entry and start systems in modern cars," in *Proc. 18th Annu. NDSS*, Feb. 2011, pp. 1 15.
9. A. Czeskis, K. Koscher, J. Smith, and T. Kohno, ``RFIDs and secret handshakes: Defending against Ghost-and-Leech attacks and unauthorized reads with context-aware communications," in *Proc. ACM Conf. Comput.Commun. Security*, 2008, pp. 479 490.
10. H. Gilbert, M. Robshaw, and Y. Seurin, ``HB#: Increasing the security and efciency of HB_C," in Proc. Adv. Cryptol. Int. Conf. Theory Appl. Cryptograph. Tech., 2008, pp. 361 378.
11. A. Devices. (2013). *ADMP401: Omnidirectional Microphonewith Bottom Port and Analog Output* [Online]. Available: http://www.analog.com/en/audiovideo-products/imems-microphone/admp401/products/product.html
12. Juels A. RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications February 2006; **24**(2):381–394.
13. Heydt-Benjamin TS, Bailey DV, Fu K, JuelsA,O'Hare T. Vulnerabilities in first-generation RFIDenabled credit cards. Financial Cryptography, 2007osium (NDSS), 2011.
14. S. Drimer and S. J. Murdoch, ``Keep your enemies close: Distance bound-ing against smartcard relay attacks," in *Proc. 16th USENIX Security Symp.*, Aug. 2007, pp. 87 102.
15. Drimer S, Murdoch SJ. Keep your enemies close:Distance bounding against smartcard relay attacks. *16th USENIX Security Symposium*, 2007
16. 16. Oren Y, Wool A. Relay attacks on RFID-based electronic voting systems. Cryptology ePrint Archive, Report 2009/422. Available online at http://eprint.iacr.org/2009/422 2009.

17. A. Fleury, N. Noury, and N. Vuillerme, ``A fast algorithm to track changes of direction of a person using magnetometers," in *Proc. IEEE Conf. EMBS*, Jan. 2007, pp. 2311 2314.
18. A. Juels, ``RFID security and privacy: A research survey," *IEEE J. Sel.AreasCommun.*, vol. 24, no. 2, pp. 381 394, Feb. 2006.
19. A. Juels, R. L. Rivest, and M. Szydlo, ``The blocker tag: Selective blocking of RFID tags for consumer privacy," in *Proc. ACM CCS*, 2003, pp. 103 111.
20. A. Juels, P. F. Syverson, and D. V. Bailey, ``High-power proxies for enhancing RFID privacy and utility," in *Proc. 5th Int. Conf. Privacy Enhancing*, 2005, pp. 210 226.
21. A. Juels and S. Weis, ``Authenticating pervasive devices with human protocols," in *Proc. Int. Cryptol. Conf.*, 2005, pp. 293 308.
22. A. Francillon, B. Danev, and S. Capkun, ``Relay attacks on passive keyless entry and start systems in modern cars," in *Proc. 18th Annu. NDSS*, Feb. 2011, pp. 1 15.
23. D. Giansanti, V. Macellari, and G. Maccioni, ``Is it feasible to recon-struct body segment 3D position and orientation using accelerometer-ric data," *IEEE Trans. Biomed. Eng.*, vol. 50, no. 5, pp. 25 35, Apr. 2003.
24. H. Gilbert, M. Robshaw, and Y. Seurin, ``HB#: Increasing the security and efciency of HB_C," in *Proc. Adv. Cryptol. Int. Conf. Theory Appl.*
25. T. Halevi, D. Ma, N. Saxena, and T. Xiang, ``Secure proximity detection for NFC devices based on ambient sensor data," in *Proc. ESORICS*, 2012,379 396.
26. G. P. Hancke and M. G. Kuhn, ``An RFID distance bounding protocol," in *Proc. 1st Int. Conf. Security Privacy Emerging Areas Commun. Netw.*, Sep. 2005, pp. 67 73.
27. T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O'Hare, ``Vulnerabilities in rst-generation RFID-enabled credit cards," in *Proc.Financial Cryptograph.*, 2007, pp. 2 14.
28. K. B. Rasmussen and S. *f*apkun, ``Realization of RF distance bounding," in *Proc. USENIX Security Symp.*, 2010, pp. 389 402.
29. M. R. Rieback, B. Crispo, and A. S. Tanenbaum, ``RFID guardian: A battery-powered mobile device for RFID privacy management," in *Proc.ACISP*, 2005, pp. 184 194.
30. B. Huyghe and J. Doutreloigne, ``3D orientation tracking based on unscented Kalmanltering of accelerometer and magnetometer data," in *Proc. IEEE Sensors Appl. Symp.*, Feb. 2009, pp. 148 152.
31. A. Juels, ``RFID security and privacy: A research survey," *IEEE J. Sel.AreasCommun.*, vol. 24, no. 2, pp. 381 394, Feb. 2006.
32. Sample A, Yeager D, Powledge P, Smith J. Design of a passively-powered, programmable sensing platform for UHF RFID systems. IEEE International Conference on RFID, 2007
33. A.Ashok Kumar, P.Swapna," An Enhanced Digital Campus Security System Using RFID, GPS, GSM" , International Journal of Research in Computer and Communication Technology, Vol 3, Issue 7, July – 2014.
34. N. Saxena, B. Uddin, J. Voris, and N. Asokan, ``Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun.*, Mar. 2011, 181 188.
35. Isik MT, Akan OB. Wireless passive sensor net-works. IEEE Communication Magazine August 2009;47(8):92–99.
36. Czeskis A, Koscher K, Smith J, Kohno T. RFIDs and secret handshakes: Defending against Ghostand-Leech attacks and unauthorized reads with context-aware communications. *ACM Conference on Computer and Communications Security*, 2008.
37. Yeager D, Prasad R, Wetherall D, Powledge P, Smith J. Wirelessly-Charged UHF Tags for Sensor Data Collection. IEEE International Conference on RFID,2008.
38. 42. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. *IEEE Symposium on Security and Privacy*, 2008
39. 47.Smith JR, Sample AP, Powledge PS, Roy S, Mamishev A. A wirelessly-powered platform for sensing and computation. *Proceedings of Ubicomp 2006*, 2006.
40. 48. Saxena N, Voris J. Still and silent: Motion detection for enhanced rfid security and privacy without changing the usage model. Workshop on RFID Security (RFIDSec), 2010.