Sensing-Enabled Defenses to RFID Unauthorized Reading and Relay Attacks without Changing the Usage Model

Tzipora Halevi[1], Sein Lin[1], Di Ma[2], Anudath K Prasad[2], Nitesh Saxena[3], Jonathan Voris[1], Tuo Xiang[2]

[1] *Polytechnic Institute of New York University*
[2] *University of Michigan-Dearborn*
[3] *University of Alabama, Birmingham*

***Abstract*—Many RFID tags store valuable information privy to their users that can easily be subject to unauthorized reading, leading to owner tracking or impersonation. RFID tags are also susceptible to different forms of relay attacks. This paper presents novel sensing-enabled defenses to unauthorized reading and relay attacks against RFID systems without necessitating any changes to the traditional RFID usage model.**

More specifically, the paper proposes the use of 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, i.e., only when it is deemed safe to do so. In particular, a novel selective unlocking mechanism based on owner's posture recognition is 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 transaction verification mechanism is developed that can determine the proximity (or a lack thereof) between a valid tag and a valid reader by correlating certain (specifically audio) sensor data extracted from the two devices. Our evaluation of the proposed mechanisms demonstrate their feasibility in significantly raising the bar against RFID attacks.

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. 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 [12]. 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 for further processing.

Due to the inherent weaknesses of underlying wireless radio communication, RFID systems are plagued with a wide variety of security and privacy threats [11]. 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* [9]. Information (such as an identifier) gleaned from a RFID tag can be used to track the owner of the tag, or to clone the tag so that an adversary can impersonate the tag's owner [11].

Promiscuous responses also incite different types of *relay attacks*. These include the "ghost-and-leech" attack [14], whereby an attacker (ghost) relays the information surreptitiously read from a legitimate RFID tag to a colluding entity (leech) which relays it to a legitimate reader. 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 a "reader-and-leech" attack. In this attack, a malicious reader colludes with the leach [5][1], and can make purchases using a victim's RFID tag. We note that addressing the reader-and-leech attack requires *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 [5], [7].

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 not only *efficiency* and *security*, but also *usability*.

A. Sensing-Enabled Automated Defenses

This paper proposes the use of sensing technologies towards addressing unauthorized reading and relay attacks without necessitating any changes to the traditional RFID usage model, i.e., without incorporating any explicit user involvement beyond what is practiced today.

[1] In contrast to the ghost-and-leech attack, the owner in the reader-and-leech attack is aware of the interrogation from the (malicious) reader.

The premise of our work is 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 [20], [10], [22]. Intel's Wireless Identification and Sensing Platform (WISP) [21], [24] 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).

B. Our Contributions

In this paper, we show that contextual information can be leveraged in two broad ways towards providing enhanced protection against RFID unauthorized reading and relay attacks, and put forth the following contributions.

- **Selective Unlocking Using Posture Recognition:** We show that contextual information can be used to design selective unlocking mechanisms so that tags can selectively respond to reader interrogations. That is, rather than responding promiscuously to queries from any readers, a tag can utilize "context recognition" and will only communicate when it makes sense to do so, thus raising the bar even for sophisticated adversaries.

We propose a concrete mechanism for such a context aware selective unlocking geared for many different RFID applications. Our approach is based on owner's *posture recognition*, and is well-suited for many applications where a specific posture of the owner of the RFID tag may serve as a valid context. These include implanted medical devices and smart car keys used as part of the Passive Keyless Entry and Start (PKES) systems [7]. We present the design, implementation, and evaluation of such a posture recognition/translation mechanism based on a combination of accelerometer and magnetometer readings. Our results indicate the mechanism to be fairly accurate even under severe resource constraints.

- **Transaction Verification Using Sensor Data Correlation:** We show that contextual information can be used as a basis for transaction verification in order to defend against the reader-and-leech attacks, a specialized form of relay attacks involving malicious readers. Specifically, we develop a new transaction verification mechanism that can determine the proximity (or lack thereof) between a valid tag and a valid reader by *correlating certain sensor data* extracted from the two devices. This is based on the assumption that certain ambient information, extracted by the tag and reader at the same time (transaction time), will be highly correlated if the two devices are in close physical proximity. In particular, we demonstrate that *audio sensors* (microphones) can be effectively used for such transaction verification. We present several techniques that can be used for determining similarity between two short audio signals extracted by the valid tag and valid reader, and show that these techniques are quite useful in significantly raising the bar against the reader-and-leech attacks.

C. Cost for Sensing-Enabled Tags

The cost of an RFID tag is dependent on several factors such as the capabilities of the tag (computation, memory), the packaging of the tag (e.g., encased in plastic or embedded in a label), and the volume of tags produced. The current cost of WISP tags – equipped with a thermometer and an accelerometer – assembled from discrete components is roughly $25 but it is expected that this number will be reduced closer to $1 once the WISPs are mass manufactured [3].

Integrating a magnetometer and a microphone with an RFID tag (as required by our approaches) is also quite feasible economically. We note that usually cost of sensing hardware varies greatly not only between different types of sensors but also between various models of the same kind. Magnetometers, for example, can be as costly as several hundred dollars or as inexpensive as a few cents when purchased in bulk Microphones are typically quite inexpensive [6]. These cost estimates are certainly acceptable for high-end tags and do not affect their business model.

II. Prior Work

Hardware-based Selective Unlocking: Hardware-based selective unlocking usually requires the users to carry an auxiliary device (such as a blocker tag in [13] or a mobile phone in [17]). 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. The requirement for a special-purpose cage (a foil envelope or a wallet) may decrease the usability of such solutions. Moreover, a crumpled sleeve is shown to be ineffective for shielding purposes [15].

Distance Bounding Protocols: These protocols have been suggested to thwart relay attacks [5], [7]. 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 . (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-leech relay attacks [5], [7]. The upper-bound calculated by an RF distance bounding protocol, however, is very sensitive to response time delay, as even a light delay (a few nanoseconds) may result in a significant error in distance bounding. A recent distance bounding scheme achieves a

processing time of less than 1 ns at the prover side [18]. 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.
Context-Aware Selective Unlocking: "Secret Handshakes" is a recently proposed interesting selective unlocking method that is based on context awareness [4]. In order to unlock an *accelerometer-equipped* RFID tag [21] 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 [4]. A central drawback to Secret Handshakes, however, is that a specialized movement pattern is required for the tag to be unlocked. This clearly requires subtle changes to the existing RFID usage model.

Motion Detection" [23] is another selective unlocking scheme. Here a tag would respond only when it is in motion instead of doing so promiscuously. Although Motion Detection raises the bar required for a few common attacks to succeed, it is not capable of discerning whether the device is in motion due to a particular gesture or because its owner is in motion, which results in a high false positive rate.

III. Selective Unlocking Using Posture Recognition

In certain RFID applications, a specific posture of the tag owner may serve as a valid context. One class of such applications involve *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 predefined unique posture. Yet another class of applications that can benefit from posture based contexts involve the *Passive Keyless Entry and Start* (PKES) system [7]. In such applications, a driver needs to move into the car and sit down on the driver's seat before the engine can be started automatically (while the key resides in the driver's pockets). Thus, getting into the car and sitting on the driver seat can be considered necessary posture sequences that need to be performed to unlock the car key. Such unlocking mechanisms prevent an attacker from launching attacks in many common scenarios, for example, controlling the IMD while standing just behind the patient in public, or, starting the car engine when the driver is sitting in a restaurant.

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. In the subsequent sections, we first point out the differences between two primary activity types: posture and posture transition. We then concentrate on posture transition recognition.

A. Posture Classifications

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 posture status that a user can maintain for a 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.

In contrast, posture transition recognition is similar to gesture recognition to a certain extent. Similar to the gesture recognition schemes, such as Secret Handshake [4], in posture transition recognition, user movement is recorded by motion sensors such as accelerometers. 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, we do not require any explicit user involvement. Thus the tag can be tilted due to the movement of the human body. The reference template is usually collected in a reference coordinate system. 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 the following subsections, we will focus on posture transition recognition in the presence of device tilt. From here on, we use posture and posture transition interchangeably.

B. Design Considerations

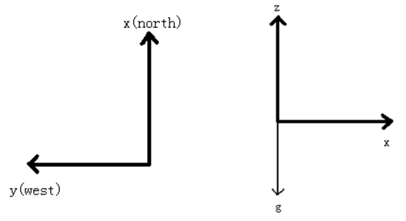
Choice of Sensors: Current systems for full orientation estimation, such as the one in Apple iPad2, typically use a set of sensor modalities – including gyroscopes, accelerometers and magnetometers – to estimate device orientation. Gyroscopes are used to accurately determine angular changes while the other sensors are used to compensate for the gyroscopes' integration drift. However, a typical gyroscope is larger and requires about 5 to 10 times more power than magnetometer and accelerometer together. Therefore, gyroscopes are not commonly available in a tiny single package MEMS-chip. Considering the resource constrains imposed by RFID platforms, we avoid using gyroscopes and instead focus on accelerometers and 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.

Device Orientation: A number of schemes have been proposed to estimate device orientation via the calculation of Euler angles using readings from both accelerometers and magnetometers. After investigating multiple schemes in the literature on human movement detection, we chose to adopt the scheme proposed in [2] for posture recognition. Unlike other schemes, which can be applied to detect generic types of movements (not only human movements), the scheme proposed in [2] is specifically designed to track certain human movements, e.g., rising from a chair or walking. So, it is well suited to planar movements which are classically performed by humans and relevant for our RFID applications. Many classical human movements are usually constrained to one or two degrees of freedom (DOFs). For example, during walking, we are interested in rotations in the sagittal plane and azimuth direction of the walking motion. This means that we can give up one DOF and still correctly catch the features of a specific posture. By giving up one DOF, the amount of computation needed for orientation estimation can be greatly reduced.

C. System Design

Our posture recognition system makes use of the strategies explored in the two gesture recognition systems [4], [16] and extends them to deal with device tilt due to certain human movements. Because our system is free of orientation limitations, there is no need for the user to hold the device in a certain fixed way during the movement. We achieve our goal by utilizing a 3-axis magnetometer and a 3-axis accelerometer combination. The magnetometer data is used to estimate device orientation in motion to mitigate the effect of motion disturbance since magnetometer reading is insensitive to acceleration. With the orientation information, the accelerometer data is "shifted" back to the reference coordinate system, and is then compared with the template(s) stored on the tag to recognize a certain posture.

Orientation Estimation: In this paper, all coordinate systems used are right-handed Cartesian coordinate systems. The earth-fixed reference coordinate system I is defined as follows (see Figure 1). The z axis points to the sky and is perpendicular to the ground. The x axis is parallel to the ground and points to the magnetic north. The y axis follows the right-hand rule, is also parallel to the ground and orthogonal to z and x. Each sensor, 3-axis magnetometer and 3-axis accelerometer, has its own body coordinate system B.



(a) Horizontal plane (b) North meridian plane

Figure 1. The Earth Reference Coordinate System

Let $\vec{v}_{acc} = (a_x, a_y, a_z)$ denote the values of the 3 axes from the accelerometer and $\vec{v}_{mag} = (m_x, m_y, m_z)$ denote the values of the 3 axes from the magnetometer. Let $\vec{I} = (x, y, z)$ be the unit vector in the earth reference coordinate system. In the general case, there exists a unique rotation matrix R that gives the relative orientation between the sensor coordinate system B and the reference system I. The rotation matrix R can be decomposed as a sequence of three elementary rotations, i.e., rotation around the Z axis or *yaw* angle (ψ), followed by a rotation around the Y axis or *pitch* angle (θ), and finally a rotation around the X axis or *roll* angle (φ). This transformation is shown as:

$$R(\psi, \theta, \varphi) = R(\psi)R(\theta)R(\varphi)$$

By adapting the approach proposed in [2], without losing the capability to catch the features of movements, we assume a *null* roll angle ($\varphi = 0$) and a null acceleration along the a_y axis. Now we can simply represent the rotation matrix as $R(\psi, \theta) = R(\psi)R(\theta)$. By minimizing a cost function:

$$J = ||\frac{\vec{v}_{mag}}{|\vec{v}_{mag}|} - R\vec{I}||^2 \tag{1}$$

we can recover the two Euler angles ψ and θ. From these angles, we can compute the acceleration in horizontal and vertical direction in the reference coordinate system as follows ($g = 9.81m/s^2$):

$$a_h = -a_x \cos\theta \cos\psi - a_z \sin\theta \tag{2}$$

$$a_v = a_x \sin\theta - a_z \cos\theta + g \tag{3}$$

System Components: Based on the orientation calculation algorithm presented above, posture recognition can be accomplished in the following steps:

1. **Template Creation:** Posture templates in the reference coordinate system are created and stored on the tag before posture recognition is performed. Each template defines a specific type of posture. We will also convert the template data into vertical and horizontal direction acceleration. A vector in the template is denoted as $\vec{T_i} = (T_{hi}, T_{vi})$.

2. **Data Collection:** While a user performs the movement

corresponding to a particular posture, accelerometer and magnetometer data are collected for a certain short period depending on the number of data points needed to accurately identify a movement. During data collection, the device/tag is either fixed on the shoulder/chest or casually placed inside the pocket.

3. **Orientation Estimation:** Once a series of temporal magnetometer data is captured, it is used to estimate the orientation of the tag and to transform the acceleration vector back to reference coordinate system as adjusted acceleration data. That is, the data is used to calculate the two Euler angles ψ and θ by minimizing the cost function J (as defined in formula 1).

4. **Posture Recognition:** Similar to the Secret Handshake scheme, we use cross-correlation to measure the similarity between two time series. The cross-correlation C of the adjusted acceleration data (a_h, a_v) against a template T is calculated as follows:

$$C = \sum_{i=1}^{n} (a_{hi} T_{hi} + a_{vi} T_{vi}) \tag{4}$$

A match will be confirmed when C exceeds a certain cross-correlation threshold. The estimation of C will be described in Section V.

IV. Transaction Verification Using Sensor Data Correlation

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 a transaction whose cost is much more than what she intended to pay. A malicious reader can also collude with a leech for the attack. Addressing such a relay attack requires validation that the tag is indeed authorizing the intended payment amount (selective unlocking is ineffective for this purpose as the tag is already unlocked).

In this paper, we set out to explore the design of sensor-enabled 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 proximity (e.g., the tag is at a restaurant, while the reader is at a jewelery shop [5]). 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, or some location-specific information, 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 issuer bank, under the current payment infrastructure, where cards share individual keys with their issuer banks (as discussed in Section 2.1 of [5]), and all communication takes place over secure channels.

The main question this raises is: what location-specific information could be used in the context of the RFID system? In this paper, our overarching idea is to derive such location-specific information by means of traditional ambient sensors that can be easily integrated with RFID tags. This is based on the assumption that certain ambient information, extracted by the tag and reader at the same time (the time of transaction), will be highly correlated if the two devices are in close physical proximity. Therefore, if two sensors, one attached to the tag and the other to the reader, report mismatching ambient information, this will indicate that the tag and reader are (most likely) not at the same location or close to each other.

A. *Correlation Using Audio*

We explore the use of audio sensors (microphones) for accomplishing the aforementioned approach to transaction verification. This choice is motivated by the intuition that the audio data captured at two different locations at a given time may be different to some extent. Specifically, we suggest that both the tag and the reader each be equipped with a microphone. Whenever a transaction is initiated, a short-term data acquired by these microphones on the two devices will be transmitted to the bank server. The server will then perform correlation analysis over the two audio signals and determine the outcome of the transaction based on the degree of correlation between the signals. As an example, under a normal scenario, when both the valid tag and valid reader are at the restaurant, the data captured by their respective microphones is likely to be highly correlated, in which case the transaction will be accepted. In contrast, under an attack, when the valid tag is at the restaurant but the valid reader is at a jewelery store, the audio data is not likely to be correlated, in which case the transaction will be rejected. In the following section, we present techniques that can be used for such correlation analysis over audio signals. Our goal is to design methods that can result in low False Rejection Rates (probability of rejecting a transaction under normal scenario) and low False Acceptance Rates (probability of approving a transaction under an attack).

B. *Similarity Detection Techniques*

We first need to determine if the audio recordings captured from the same location have higher similarity than recordings taken at different locations. To this end, we investigate a few methods to detect such similarity including: time-based methods, frequency-based methods as well as a combined time-frequency method.

Time-Based Similarity Detection: To detect the similarity between the time-based signals X_i and X_j, we propose using two methods: *correlation* and *difference*. The signals will first be normalized according to their energy (so that each signal has a total energy equal to 1). Then, in the first method, the correlation between each two signals will be calculated and the maximum correlation will be used. Therefore, the correlation based similarity between two signals X_i and X_j can be measured by:

$$S_c(i,j) = \max(Cross\text{-}Corr(X_i, X_j)) \tag{5}$$

In the second method, the distance between each bit of the signals is calculated and the overall Euclidean norm of the distance is used as below:

$$D(i,j) = \|X_i - X_j\| \text{ and } S_d(i,j) = 1 - D(i,j) \tag{6}$$

Our tests (Section V-B) show that the time-based correlation provides better results compared to the difference between the signals.

Frequency-Based Similarity Detection: In the frequency-based detection approach, we use Fast Fourier Transform (FFT) to create the frequency coefficients for each recorded signal. We then use both the correlation and the difference between the FFT coefficients in order to evaluate the similarity between different segments taken at the same place (in consecutive time periods) vs. recordings taken at different locations.

Time-Frequency Based Similarity Detection: This novel method combines both the time and frequency based measurements to create a point in 2-D space. In this technique, the overall time-frequency similarity measure is calculated by:

$$S(i,j) = \sqrt{(S_{c,time}(i,j))^2 + (S_{d,frequency}(i,j))^2} \tag{7}$$

This implies that the similarity measurement will be higher for closer signals.

V. Experiments and Results

To evaluate the effectiveness and performance of the proposed posture based selective unlocking technique, we built proof-of-concept prototypes on the Intel WISP tags (version 4.1) and extended the WISP with magnetic sensing capability.

A. Posture Recognition Experiments

We report on our implementation and evaluation of the posture recognition based selective unlocking scheme.

We have implemented a prototype of posture recognition on the WISP to evaluate the effectiveness of the proposed scheme in terms of successful recognition rate. In our current realization of the orientation estimation module, however, to find the (ψ, θ) pair that minimizes the cost function J in Equation 1, we need to go through, in an exhaustive way, a list of 360×360 possible candidate values. Moreover, the WISP platform has limited mathematical function support. We thus had to use software implementation of the $\sin$ and $\cos$ functions in order to rotate data vectors back to the Earth reference coordinate system. Although we tried to minimize computation cost via implementation optimizations, the aforementioned factors still make *posture recognition with orientation estimation* a bit slow on WISP tags. So, our evaluation with the WISP prototype does not use this module currently. We expect that implementation of posture recognition techniques with orientation estimation will be better-suited for more powerful tags with more resources, such as the smart keys used in modern cars which provides the user with various functionalities such as starting the car automatically while the driver sits down in the car. An NFC enabled smartphone can also be thought of as a powerful sensing-enabled RFID device.

While we were looking for a more efficient orientation estimation design for use with WISP tags, we also implemented a prototype on a desktop PC. Our PC-based prototype implementation serves the purpose of evaluating the effectiveness of posture recognition with orientation estimation on a more powerful RFID platform. Our design is modular and so the orientation estimation module can be ported to more powerful tags when they become available on the market.

We manually created posture templates by affixing a WISP on the front trouser pocket area of a test subject and recorded accelerometer data while the subject performed certain movements. We created templates for 4 postures: "sit-to-std" (moving from sitting posture to standing posture), "std-to-sit" , "sit-to-lie" and "std-to-car-sit". The std-to-car-sit posture simulates the smart key setting when a driver gets into the car, i.e., she stands before a car, then moves into the car, and sits down on the driver's seat. Normally, posture movement is slower than gesture movement. Thus, variations in the acceleration components do not change much during a posture movement. Therefore fewer data points are needed for successful posture recognition in comparison to gesture recognition. In our experiments, we collected 30 data points for each posture. Our experimental results show that this number is sufficient for accurate posture recognition.

To determine which cross-correlation detection thresholds to use, we collected 40 traces of accelerometer data for each posture. Each trace is then used as a template, which is compared with all the other traces to calculate a serial of C values (Equation 4). The smallest C value is chosen as the threshold value. This threshold value is stored with the corresponding template and a matched posture needs to yield a C value larger than this threshold.

We conducted the following experiment with the WISP prototype – *posture recognition without orientation estimation*. In this experiment, posture data is collected when the WISP is fixed in the position similar to the one we used while collecting the template data. This simulates the case of an implanted device which would usually remain in the same fixed position inside the body. For our second experiment, we tilted the WISP in different ways in the sagittal plane and then affixed it to the trouser pocket area. This is to simulate other (external) RFID devices that can be tilted inside the pocket or purse. We conducted this second type of experiments with orientation estimation using our PC prototype.

We requested a single participant to generate templates and test samples for our experiments. For each posture, we conducted 60 tests (each test yielded 30 data points) and calculated the success rate based on these 60 test results.

The results of our first experiment show that it takes only around 220 ms to recognize a posture on the WISP. Our overall results for the two posture recognition experiments are summarized in the two confusion matrices depicted in Table I. Table I(Left) represents the results for the WISP implementation without orientation estimation functionality executed on samples where the device was not tilted (simulating medical implants, for example); Table I (Right) represents the results for the PC implementation with orientation estimation module executed on samples where the device was tilted.

First comparing the successful posture recognition rates in Table I(Left) with that of gesture recognition schemes, such as Secret Handshakes [4] and uWave [16], we find that we achieve slightly lower recognition rates, although still high enough for practical purposes. This might be because of the tilt effect of human movement, as postures can not be performed in as controlled of a way as gestures. (Note that we could not completely prevent the effect of tilt while collecting our samples, unlike the case of a real fixed medical implant). The posture recognition rates in Table I(Right), on the contrary, are comparable to that of gesture recognition schemes. This confirms the effectiveness of the orientation estimation module for posture recognition in scenarios where device tilt occurs.

B. Sensor Data Correlation Experiments

In this section, we present our evaluation of the techniques for transaction verification based on audio data correlation.

1) Data Collection: Since the RFID reader is not mobile, we used two mobile phones for audio data collections from different locations. We developed a program that captures audio from the phone's built-in microphone. The program was designed to record up to 30 seconds of continuous audio data. The phones were synchronized by means of a wireless signal and recorded the samples at the same time. We recorded a few audio samples with both microphones at different locations.

To simulate a normal usage scenario (i.e., when no attacks occur), the phones were separated by a distance of 3-12 inches. In this case, we tried to detect the probability that two recordings taken at the same general location (but a few inches apart and with a different sensor) can be distinguished from recordings taken at different locations. For this purpose, we recorded 20 1-sec segments from two phones simultaneously at 5 different locations,.

To simulate attack scenarios, we recorded audio at 7 different locations, including a few retail stores and fast food restaurants.

2) Performance of Similarity Detection Techniques: We test the performance of various techniques, outlined in Section IV. Specifically, in every test group, we use 5 pairs of 1-sec recording segments. The two samples in each pair were taken by two different sensors at the same location simultaneously (each pair was recorded at a separate location). For each sample, we calculated the probability that the recording, identified as the most similar to it was indeed the recording taken at the same location with the other phone.

We ran the test for 20 separate groups of recordings. The summary of results obtained by using different techniques can be found in Table II. Our tests demonstrated that the result corresponding to time-frequency classification is superior to all other methods, with a successful detection rate of 53%.

Table II
Performance of Similarity Detection Techniques

Method	Detection Rate
Time-Based Cross-Correlation	38.29%
Time-Based Distance	13.57%
Freq-Based Cross-Correlation	38.57%
Frequency-Based Distance	50.00%
Time-Frequency	52.85%

3) False Accept Rate (FAR) vs. False Reject Rate (FRR): We next tried to determine the probabilities of incorrectly approving the transaction with an unauthorized tag and rejecting the transaction with an authorized tag. FAR is the sum of false positives, which occur when the audio signal captured by a valid reader matches the audio signal captured by a tag, even when the two devices are at different locations. FRR, on the other hand, is the sum of false negatives, and denotes the probability that the transaction is rejected even when the valid tag and valid reader are in close physical proximity.

We compare the similarity measurement for each recorded signal with the one taken by the second microphone at the same location as well as with all the recordings taken at different locations. We use the similarity matrix as our feature and train the classifier to learn the similarity threshold for each couple of samples. We use the *SimpleLogistics classifier* from the WEKA package to classify the samples. We run a 10-fold classification, which partitions the data into 10 partitions, trains the classifier over 9 of the partitions (which act as the training set) and classify the remaining samples (the testing set). This is repeated for each partition and training set in the dataset.

Using this classifier, we found that our FAR is equal to 0% while the FRR is equal to 6.87%. This indicates the highest level of security while only lowering the usability by

	sit-std	**std-sit**	**sit-lie**	**std-car-sit**
sit-std	91.67%	3.33%	3.33%	1.67%
std-sit	1.66%	88.34%	6.67%	3.33%
sit-lie	3.33%	1.66%	93.34%	1.67%
std-car-sit	3.33%	3.33%	1.67%	91.67%

	sit-std	**std-sit**	**sit-lie**	**std-car-sit**
sit-std	96.66%	1.67%	1.67%	0.00%
std-sit	1.67%	93.33%	3.33%	1.67%
sit-lie	1.67%	3.33%	95.00%	0.00%
std-car-sit	0.00%	1.67%	5.00%	93.33%

Table I
CONFUSION MATRICES FOR POSTURE RECOGNITION: (LEFT) WITHOUT ORIENTATION ESTIMATION AND DEVICE TILT (WISP IMPLEMENTATION); (RIGHT) WITH ORIENTATION ESTIMATION AND DEVICE TILT (PC IMPLEMENTATION)

a small amount (a small percent of the valid users will need to run the authentication a second time). We also calculated the Accuracy and the Precision. For our Data, we received Accuracy of 99.23% and Precision of 100%.

VI. CONCLUSIONS

We presented novel sensing-enabled defenses to unauthorized reading and relay attacks against RFID systems without necessitating any changes to the traditional RFID usage model. First, selective unlocking mechanisms based on owner's posture recognition was presented. Second, 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.

Our 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. As an immediate avenue for future work, we intend to further optimize and fine-tune our algorithms for better efficiency on resource-constrained RFID platforms and improved tolerance to errors whenever applicable. We also plan on working with other sensors (besides magnetometer, accelerometer and microphones), and combinations thereof, so as to further improve the security of our approaches.

REFERENCES

[1] Ulf Blanke and Bernt Schiele TU Darmstadt. Towards human motion capturing using gyroscopeless orientation estimation. In *14th International Symposium on Wearable Computers (ISWC'10)*, Oct. 2010.

[2] Stephane Bonnet and Rodolphe Heliot. A magnetometer-based approach for studying human movements. *IEEE Tran. on Biomedical Engineering*, 54(7), Jul. 2007.

[3] M. Buettner, R. Prasad, M. Philipose, and D. Wetherall. Recognizing Daily Activities with RFID-Based Sensors. In *International Conference on Ubiquitous Computing (UbiComp)*, 2009.

[4] 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 *ACM Conference on Computer and Communications Security*, 2008.

[5] S. Drimer and S. J. Murdoch. Keep your enemies close:Distance bounding against smartcard relay attacks. In *16th USENIX Security Symposium*, August 2007.

[6] Sparkfun Electronics. Low-Power Low-Cost Microphones. newblock Available online at http://www.sparkfun.com/search/results?term=microphone\&what=products.

[7] Aurelien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *18th Annual Network and Distributed System Security Symposium (NDSS)*, 2011.

[8] Gerhard P. Hancke and Markus G. Kuhn. An RFID distance bounding protocol. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 2005.

[9] Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare. Vulnerabilities in first-generation RFID-enabled credit cards. In *Financial Cryptography*, 2007.

[10] J. Holleman, D. Yeager, R. Prasad, J. Smith, and B. Otis. NeuralWISP: An energy-harvesting wireless neural interface with 1-m range. In *Biomedical Circuits and Systems Conference (BioCAS)*, 2008.

[11] A. Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, February 2006.

[12] Ari Juels, David Molnar, and David Wagner. Security and privacy issues in E-passports. In *Security and Privacy for Emerging Areas in Communications Networks (Securecomm)*, 2005.

[13] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *ACM Conference on Computer and Communications Security (CCS)*, 2003.

[14] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard. In *Security and Privacy for Emerging Areas in Communications Networks (Securecomm)*, 2005.

[15] Karl Koscher, Ari Juels, Vjekoslav Brajkovic, and Tadayoshi Kohno. EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond. In *ACM Conference on Computer and Communications Security*, 2009.

[16] Jiayang Liu, Zhen Wang, Lin Zhong, Jehan Wickramasuriya, and Venu Vasudevan. uWave: Accelerometer-based personalized gesture recognition and its applications. *Pervasive and Mobile Computing*, 5(6):657–575, December 2009.

[17] N. Saxena and B. Uddin and J. Voris and N. Asokan. Vibrate-to-Unlock: Mobile Phone Assisted User Authentication to Multiple Personal RFID Tags. In *Pervasive Computing and Communications (PerCom)*, 2011.

[18] Kasper Bonne Rasmussen and Srdjan Čapkun. Realization of RF distance bounding. In *Proceedings of the USENIX Security Symposium*, 2010.

[19] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. RFID guardian: A battery-powered mobile device for RFID privacy management. In *Australasian Conference on Information Security and Privacy (ACISP)*, 2005.

[20] Antti Ruhanen and et. al. Sensor-enabled RFID tag handbook. http://www.bridge-project.eu/data/File/BRIDGE_WP01_RFID_tag_handbook.pdf, January 2008.

[21] A. Sample, D. Yeager, P. Powledge, and J. Smith. Design of a passively-powered, programmable sensing platform for UHF RFID systems. In *IEEE International Conference on RFID*, 2007.

[22] A.P. Sample, D. Yeager, and Smith J. A capacitive touch interface for passive RFID tags. In *IEEE International Conference on RFID*, 2009.

[23] Nitesh Saxena and Jonathan Voris. Still and silent: Motion detection for enhanced rfid security and privacy without changing the usage model. In *Workshop on RFID Security (RFIDSec)*, June 2010.

[24] Joshua R. Smith, Pauline S. Powledge, Sumit Roy, and A. Mamishev. A wirelessly-powered platform for sensing and computation. In *8th International Conference on Ubiquitous Computing (Ubicomp)*, 2006.