# Context-Aware Defenses to RFID Unauthorized Reading and Relay Attacks

Tzipora Halevi, Haoyu Li, Di Ma, Nitesh Saxena,
Jonathan Voris, and Tuo Xiang

**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.

Specifically, the paper 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 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. Our evaluation of the proposed mechanisms demonstrate their feasibility in significantly raising the bar against RFID attacks.

**Index Terms**—RFID; relay attacks; context recognition; sensors

## 1 Introduction

The low cost, small size, and the ability of allowing computerized identification of objects make Radio Frequency IDentification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications include: supply chain (or inventory) management, e-passports, credit cards, driver's licenses, vehicle systems (toll collection or automobile key), access cards (building or parking, public transport), and medical implants.

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 [22]. 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 [18]. 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* [14]. Information (such as an identifier) gleaned from an 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 [18].

Promiscuous responses also incite different types of *relay attacks*. These include the "ghost-and-leech" attack [23], whereby an attacker (leech) relays the information surreptitiously read from a legitimate RFID tag to a colluding entity (ghost) 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-ghost" attack. In this attack, a malicious reader colludes with the ghost [6][1], and can make purchases using a victim's RFID tag. We note that addressing the reader-and-ghost 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, including the Chip-and-PIN credit card system [6], and keyless entry and start car key system [8].

### 1.1 Sensing-Enabled Automated Defenses

Although a variety of security solutions exist, many of them do not fully meet the requirements of the underlying

*This submission is a combination and consolidation of a concise contribution at Percom 2012 conference [11] and a paper at the ESORICS 2012 conference [12].*

*T. Halevi (thalev01@students.poly.edu) is with Polytechnic Institute of New York University*

*H. Li (haoyul@umd.umich.edu), D. Ma (dmadma@umd.umich.edu), and T. Xiang (txiang@umd.umich.edu) are with the University of Michigan-Dearborn*

*N. Saxena (saxena@cis.uab.edu) is with the University of Alabama at Birmingham*

*J. Voris (jvoris@cs.columbia.edu) is with Columbia University*

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

RFID applications in terms of (one or more of): efficiency, security and usability. We discuss prior work in Section 2.

In an attempt to address this situation, this paper proposes the use of sensing technologies for preventing 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.

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 [30], [15], [32]. Intel's Wireless Identification and Sensing Platform (WISP) [31], [36] 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).

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 therefore acquire useful *contextual information*, and this information can be utilized for enhanced RFID security and privacy.

### 1.2 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.

**Context-aware Selective Unlocking:** 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. For example, an office building access card can remain locked unless it is aware that it is near the (fixed) entrance of the building.

We propose a 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 [8]. For example, in the latter application, a car engine starts automatically when the driver sits down on the car seat while the key resides in the driver's pocket; a valid context for the key to get unlocked is an "upright seating posture". 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-ghost attacks, a specialized form of relay attacks involving malicious readers. For example, a bank server can deny a $2000 transaction (jewelery purchase) when it detects the valid tag (RFID credit card) is currently located in a restaurant where a normal transaction is usually less than $200, and can prevent the attack presented in [6].

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.

### 1.3 Scope of Our Work

Errors are inherent to any context recognition approaches. Our approaches are no different in this regard in that they yield non-zero, although quite low, false positive and false negative rates. Thus, the proposed approaches can not guarantee absolute security and usability. However, our techniques significantly raise the bar even for sophisticated adversaries without affecting the RFID usage model. Moreover, although the proposed techniques can work in a standalone fashion, they can also be used in conjunction with other security mechanisms, such as cryptographic protocols, to provide stronger cross-layer security protection. In addition, many of our proposed ideas and techniques will be broadly applicable in the realm of other devices equipped with sensors.

While we have designed and optimized our context detection approaches to minimize error rates, we are aware that false negatives may sporadically occur in which users are unable to gain access to a resource using their RFID hardware. In these situations it is important to have fallback contingencies through which users can still perform their required task. Most applications of our context recognition proposal can use a physical token or mechanism, such as a button, as fallback mechanism. For example, if a false negative occurs while a legitimate user is attempting to unlock their vehicle using a contactless system, the individual will be prevented from starting the car's engine. In this scenario, users could fall back to utilizing a physical key to activate the car.

### 1.4 Paper Outline

The rest of the paper is organized as follows. We review related works in Section 2. We present, in Section 3, our selective unlocking mechanisms based on posture recognition. Next, we present our secure transaction verification

based on signal correlation in Section 4. Finally, we report on our experimentation and associated results in Section 5. Section 6 provides concluding remarks.

## 2 Prior Work

**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.

**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 community to design lightweight cryptographic mechanisms (e.g., [21], [10]). However, these protocols usually require shared key(s) between tags and readers, which is not an option in some applications.

**Distance Bounding Protocols:** These protocols have been used to thwart relay attacks [6], [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 [6], [8]. 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. Therefore, even XOR- or comparison-based distance bounding protocols [3], [13] 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.

**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 [31], [36] using Secret Handshakes, a user must move or shake the tag (or its container) in a particular pattern. For example, the user might be required to move the tag parallel with the surface of the RFID reader's antenna in a circular manner. A number of unlocking patterns were studied and shown to exhibit low error rates [4]. A central drawback to Secret Handshakes, however, is that a specialized movement pattern is required for the tag to be unlocked. While a standard, insecure RFID setup only requires users to bring their RFID tags within range of a reader, the Secret Handshakes approach requires that users consciously move the tag in a certain pattern. This clearly requires subtle changes to the existing RFID usage model.

"Motion Detection" [35] is another selective unlocking scheme. Here 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. 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. The use of location (and speed) information derived from the GPS sensors for RFID security problems tacked in our paper has been explored in recent work [26], [27].

## 3 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 in 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. Yet another class of applications that can benefit from posture based contexts involve the *Passive Keyless Entry and Start* (PKES) system [8]. 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. In turn, this will "unlock" the car's engine, allowing its driver to ignite it and drive the vehicle. Note that posture is not used to unlock the vehicle's door in this scenario; the driver will gain entry to the vehicle via an existing mechanism. The posture recognition system is instead applied to prevent unauthorized individuals from turning on the car's engine. Such an unlocking mechanism will prevent an adversary from launching attacks in scenarios whereby the driver is not entering the car and then sitting on the car seat.

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.

There may be some situations where the assumptions regarding the usage specifics of a scenario differ. For example, in areas with colder climates, some people choose to start their car remotely to allow the vehicle's engine and interior to warm up before entering it. Our scheme is adaptable to situations such as these as each user's posture template will reflect the particulars of their usage habits. Of course, additional hardware may be required to accommodate less common usage scenarios, i.e., a longer transmission range would be required to detect the context of a user who starts his or her vehicle from a distance.

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.

### 3.1 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 bodily position 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. 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 [24]. Similarly, the work of [7] tracks direction changes of magnetometer axes during walking.

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.

### 3.2 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 [1]. Therefore, gyroscopes are not commonly available in a tiny single package MEMS-chip. In addition, it has been shown that neither accelerometers or magnetometers are good enough *alone* to estimate full orientation [9], [33]. On the other hand, orientation estimation schemes that use both accelerometers and magnetometers show very promising results [38], [17]. 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 [2], [17], [1]. However, many of them suffered from a common problem, called motion disturbance, which leads to inaccurate orientation estimation when the device is in motion. The scheme proposed in [17] uses an unscented Kalman filter to effectively reduce the influence of motion disturbance on the sensor signals. However, it has higher computational complexity due to the addition of a signal processing module. Considering the limited computation and memory resources of the RFID platform, it is clear that we have to simplify the algorithms as much as possible without losing efficiency and accuracy.

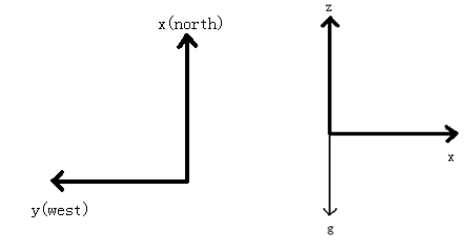
After investigating multiple schemes in the literature on human movement detection, we chose to adopt the scheme proposed in [2] for posture recognition. Unlike other schemes, which can be applied to detect generic types of movements (not only human movements), the scheme proposed in [2] is specifically 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.

### 3.3 System Design

Our posture recognition system makes use of the strategies explored in the two gesture recognition systems [4], [25] 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

Fig. 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 ($\psi$), followed by a rotation around the Y axis or *pitch* angle ($\theta$), and finally a rotation around the X axis or *roll* angle ($\varphi$). 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:

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

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

$$a_h = -a_x \cos\theta \cos\psi - a_z \sin\theta \quad (2)$$

$$a_v = a_x \sin\theta - a_z \cos\theta + g \quad (3)$$

**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. It serves as a reference to be later compared with real-time user movement data: a match indicates the recognition of a particular posture defined by the posture template. 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. Posture changes are relatively slow in comparison with hand gestures. Thus, variations in the acceleration components do not vary a lot during a posture transition. Hence, under normal circumstances, fewer data points are needed in posture recognition than in gesture recognition. 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 $\psi$ and $\theta$ 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:

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

A match will be confirmed when $C$ exceeds a certain cross-correlation threshold. The estimation of the cross-correlation threshold will be described in Section 5.

### 3.4 Enrollment

A posture detection system must include an enrollment mechanism in order to be practical. In a real-world system, users would first participate in a brief one time enrollment period during which their posture transition template would be created with respect to the location (e.g., pocket/wallet) of their sensing enabled RFID hardware. If a user wanted to store the RFID tag in a new location, he or she would have to perform an enrollment renewal to avoid the tag's new frame of reference from introducing errors into the unlocking process. Note that the unlocking process does not imply that any particular hardware response must take

place, but rather that the response may only take place once the hardware is unlocked. Using the car entry example, sitting in the driver's seat does not necessarily automatically start the vehicle's engine, but rather the vehicle's engine can be started at any time when the driver's RFID tag has indicated/detected that he or she is sitting in the vehicle.

# 4 Proximity Detection Techniques

## 4.1 Correlation Using Audio

We explore the use of audio sensors (microphones) for accomplishing the aforementioned approach to proximity detection. This choice is motivated by the intuition that the audio data captured at two different locations at a given time is different to some extent.

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 had 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:

$$S_c(i,j) = \max(Cross\text{-}Corr(X_i, X_j)) \text{ and } D_c(i,j) = 1 - S_c(i,j) \quad (5)$$

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:

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

**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:

$$D(i,j) = \sqrt{(D_{c,time}(i,j))^2 + (D_{d,frequency}(i,j))^2} \text{ and } S(i,j) = 1 - D(i,j) \quad (7)$$

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

Using audio data to perform proximity detection requires recording local sounds, which raises some privacy questions. Fortunately, after an audio sample has been used to determine the proximity of two pieces of hardware, there is no more need for the audio sample. It can thus be discarded from both of the devices performing the security operation, ensuring that this potentially sensitive data will not be the target of attack. A malicious device could potentially be programmed to retain the sound data after the correlation process. However, in the absence of our solution, an adversary could accomplish the same effect by placing a minuscule microphone near one of the devices or compromising other nearby microphone equipped hardware.

## 4.2 Correlation Using Ambient Light

We also explore the use of light sensors for the purpose of proximity detection. This choice is inspired by an observation that different types of places may have different lighting conditions. For example, fast food restaurants usually use bright lights to attract customers and to signify a place bustling with activity and very fast service, while fine dinning restaurants typically use low-intensity of light to create an intimate and leisurely atmosphere. As lighting conditions are location dependent, the ambient light can be used as the contextual information to determine the proximity between two devices (or a lack thereof).

Unlike ambient audio which can be heavily affected by surrounding human/non-human activity, indoor ambient light (without natural light) is intuitively quite steady over time as the lighting infrastructure usually remains untapped – this intuition is later validated through the experiments as illustrated in Section 5.3. Hence, in this case, we use a simple strategy that involves just comparing the mean value of the illuminance data to determine whether ambient light readings captured from the same location have higher similarity than recordings taken at different locations.

Let $L_i$ and $L_j$ be the mean value of illuminance data captured in a short time interval by two devices at location $i$ and $j$. The difference of mean value is calculated as:

$$D(i,j) = |L_i - L_j| \quad (8)$$

As long as $D(i,j)$ is below a threshold, we consider the two readings to be similar enough and believe that they are captured from the same location. Otherwise, the two readings are believed to be captured from different locations. We will discuss how to establish the threshold via experiments in Section 5.3.

Light sensors can be attached on both tag and reader in order to collect short-term data and transfer to the bank server for further processing and Instead of compare the patterns of the signal like what we do with audio data, we compare just the mean value of the illuminance data since unlike the audio signal is heavily affected by the around happening, the illuminance is intuitively considered steady through time for certain location and different for different location. The two figures below prove our intuition. Curves

in Figure 2 represent the data we collected from 4 different places (Fast-food restaurant, supermarket, fine dinner restaurant and shopping mall), the curves are steady and well and parallel separated which means the mean value can be used to distinguish these places. The boxes in Figure 3 show the mean value of the data we collected from various locations and give us a more direct view how the mean values of illuminance differ from locations.

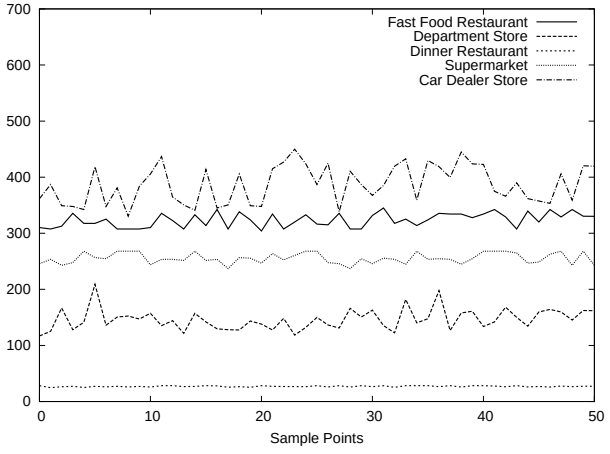



Fig. 2. Illuminance Data over Time at Different Locations

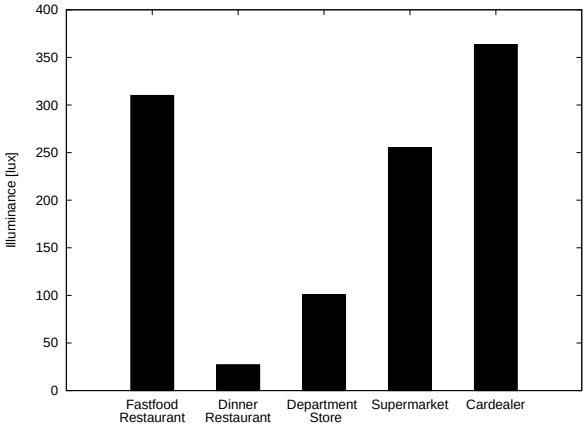



Fig. 3. Mean Illuminance at Different Locations

## 5 Experiments and Results

To evaluate the effectiveness and performance of the proposed posture based selective unlocking technique , we build proof-of-concept prototypes on the WISP tags. WISPs are passively-powered RFID tags that are compliant with the Electronic Product Code (EPC) protocol. Specifically, we utilized the 4.1 version of the WISP hardware, which partially implements Class 1 Generation 2 of the EPC standard. These tags possess an onboard Texas Instruments MSP430F2132 microcontroller and sensors such as the ADXL330 three-axis $\pm 3g$ accelerometer [37]. The 16-bit MCU features an 8 MHz clock rate, 8 kilobytes of flash memory, and 512 bytes of RAM. WISP is chosen as our test platform because: (1) it is the only existing programmable UHF RFID device, and (2) it has an extensible hardware architecture which allows for integration of new sensors.

To evaluate our sensor data correlation approach , we develop a proof-of-concept prototype on mobile phones, which allows us to collect data from different locations, and demonstrate the feasibility of our transaction verification approach. This experimental scenario is also directly applicable to the Near Field Communication (NFC) phone usage.

### 5.1 Interfacing Additional Sensors with the WISP

As mentioned above, the WISP already possesses an accelerometer which will be used as part of our posture recognition mechanism. In addition, we needed to integrate a magnetometer with the WISP.

To this end, we decided to use HMC1053 [16], a 3-axis magnetometer from Honeywell. The Honeywell HMC1053 is specifically designed for low-field magnetic sensing and can measure the direction as well as the magnitude of magnetic field ranging from 120 micro-gauss to 6 gauss. Each of its magnetoresistive sensors is configured as a 4-element wheatstone bridge to convert magnetic fields to differential output voltages. There are 3 such magnetoresistive sensor bridges connected orthogonally to obtain the magnetic field intensity in 3 axes. HMC1053 has ultra low power requirements which can be satisfactorily sustained by the WISP as these tags work ideally at 1.8 V.

As a proof-of-concept, in support of our transaction verification scheme, we also integrated a microphone with the WISP. Specifically, we integrated ADMP401 – an omnidirectional microphone manufactured by the Analog Devices [5] – with the WISP. This ideally suits the power requirement of the WISP as it has a very low current consumption of less than 250 $\mu$A and has a supply voltage range of 1.5 to 3.3V. Moreover, this microphone is quite thin and will not affect the form factor of a typical RFID card.

### 5.2 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 $(\psi, \theta)$ pair that minimizes the cost function $J$ in Equation 1, we need to go through, in an exhaustive way, a list of $360 \times 360$ 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 1. Table 1(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 1 (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 1(Left) with that of gesture recognition schemes, such as Secret Handshakes [4] and uWave [25], 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 1(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.

Our experiments also show that when a device can be tilted but no orientation estimation is used to correct the data, the posture recognition algorithms are not successful. This is because without orientation estimation, the readings of the accelerometer can not reflect the external force due to tilt. The same external force may produce different accelerations along the three axes of the accelerometer if it is tilted differently; likewise, the different forces may also produce the same accelerometer readings. Thus, without orientation estimation, a given posture can be confused with any of the other postures.

Overall, the results of our posture recognition experiments were mixed. On the positive side, we were able to efficiently estimate posture with a computational RFID tag; the 220 ms recognition rate that we achieved is fast enough to be used in applications with very low delay tolerances, such as access tokens. Furthermore, when taking orientation into account, the accuracy of our proposed posture recognition scheme was comparable to alternatives with more demanding usage models, such as gesture recognition. Unfortunately, we found orientation estimate to be too computationally expensive for current processor equipped tags such as the WISP. Moreover, a study with additional participants would help establish the applicability of our scheme to a broader population.

### 5.3 Audio Data Experiments

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

| | 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 1
Confusion Matrices for Posture Recognition: (Left) without orientation estimation and device tilt (WISP implementation); (Right) with orientation estimation and device tilt (PC implementation)

#### *5.3.1 Data Collection*

The goal of sensor data correlation is to detect whether the valid tag and valid reader are at the same or different locations. Therefore, we needed to collect the sensor data when the two devices are located in close physical proximity as well as when they are at two different locations. Since capturing this data at different locations is not feasible while using an RFID tag (since our RFID reader was not mobile), we decided to instead work with two mobile phones, simulating a valid RFID tag and a valid RFID reader.

To enable recording of background sounds using the phones, we developed a program that captures audio from the phone's built-in microphone and installed it on two mobile phones. The program was designed to record up to 30 seconds of continuous audio data. The audio-capturing programs were launched on both phones and activated at about the same time to record the samples (the phones were synchronized by means of a wireless signal). We recorded, with the microphones, a few audio samples at different locations. We needed to determine if it was possible to distinguish between recordings taken at the same location versus 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 collected data at 5 different locations, recording 20 1-sec segments from two sensors simultaneously (located a few inches apart).

To simulate attack scenarios, we recorded audio at 7 different locations, including a few retail stores and fast food restaurants. Specifically, we recorded surrounding noise at: McDonald's, Wendy's, Target, and our university cafeteria and library.

All recorded audio files were then converted from the 3GPP format to the WAV format to be fed into our matlab algorithms for signal correlation (discussed in Section 4.1). Conversion from 3GPP to WAV, unlike the inverse, is considered lossless, since there is no compression used in WAV format. Thus, no important information was lost during this conversion.

#### *5.3.2 Performance of Similarity Detection Techniques:*

We test the performance of various techniques, outlined in Section 4, to identify which one can most accurately detect the similarity between recordings taken at the same location. 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 all the techniques, we calculated the probability that the recording, identified as the most similar one to a given recording, was the recording taken at the same location.

We ran the test for the dataset collected previously. Our results showed that the time-based "correlation" (Equation 5) gave better result ($38\%$ detection rate) compared to the "distance" (Equation 6) between the signals (which resulted in detection rate of $14\%$). Also, our tests showed that frequency-coefficients based distance yielded better results ($50\%$ detection rate) compared to time-based methods and to frequency-based cross-correlation methods (which resulted in $39\%$ detection rate). Finally, our tests also demonstrated that the result corresponding to time-frequency classification is superior to all other methods, with a successful detection rate of $53\%$. In the rest of our analysis, therefore, we use the time-frequency based technique.

#### *5.3.3 Performance of Audio-based Proximity Detection:*

We next used the test dataset to determine the performance of our time-frequency detection on data taken under normal usage as well as attack scenario. We calculated the time-frequency distance measure between each two different samples. We found the square distance $D(i,j)^2$ (Section 4.1) and used it as our data features. For each pair of locations, we calculate the mean of the square distance. We generated a confusion matrix for our dataset as shown in Table 2.

To distinguish between recordings taken at the same approximate location we compare the time-frequency square distance between each recorded signal and the one taken by the second microphone at the same location as well as with all the recordings taken at different locations. We construct the similarity matrix $s$ using the similarity measurements and use it as our feature data. We use the input data to train the classifier to find 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

TABLE 2
Confusion Matrix of Square Time-Frequency Distance

| | Concert Hall | Library | McDonalds | Library (2) | Cafe |
|---|---|---|---|---|---|
| **Concert Hall** | 0.4678 | 1.7889 | 1.8645 | 1.7556 | 1.8412 |
| **Library** | 1.7889 | 0.8539 | 1.7878 | 1.6753 | 1.7545 |
| **McDonalds** | 1.8645 | 1.7878 | 0.6018 | 1.7962 | 1.7241 |
| **Library (2)** | 1.7556 | 1.6753 | 1.7962 | 0.8213 | 1.8140 |
| **Cafe** | 1.8412 | 1.7545 | 1.7241 | 1.8140 | 0.5289 |

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.

We note that the classifier arrived at a simple classification formula: if $y = 11.49 \times Corr - 8.69 < 0$, then both samples will be considered to be taken at the same place. Otherwise, they will be considered to be taken at different locations. This is a simple calculation (one multiplication and one addition) and will take the server a negligible amount of time to validate whether both samples were captured at the same location.

Using the classifier results, we find the detection rate for each pair of locations in which the samples were taken (where one sample is captured in each location). The detection rate is calculated over all the pairs of samples which were taken at the two locations, by dividing the number of pairs of samples that were correctly classified by the number of total pairs of samples (taken at those locations). The result of the correct recognition rates can be found in Table 3. As can be seen from the table, our audio signal based correlation technique yields 100% detection rate.

#### 5.3.4 False Accept Rate vs. False Reject Rate:

We next determined the probabilities of incorrectly approving the transaction with an unauthorized phone and rejecting the transaction with an authorized phone, by calculating the False Accept Rate (FAR) vs. the False Reject Rate (FRR). 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 phone, 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 phone and valid reader are in close physical proximity.

Using the classifier results, since our detection rates are 100%, our FAR and FRR are both clearly equal to 0%. This indicates that our audio-based proximity detection technique is very robust.

## 6 Conclusions

We 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.

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.

## References


[1] U. Blanke and B. Schiele, "Towards human motion capturing using gyroscopeless orientation estimation," in *14th International Symposium on Wearable Computers (ISWC'10)*, Oct. 2010.

[2] S. Bonnet and R. Heliot, "A magnetometer-based approach for studying human movements," *IEEE Tran. on Biomedical Engineering*, vol. 54, no. 7, Jul. 2007.

[3] S. Brands and D. Chaum, "Distance-bounding protocols," in *Advances in Cryptology - EUROCRYPT, International Conference on the Theory and Applications of Cryptographic Techniques*, 1993.

[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] A. Devices, "ADMP401: Omnidirectional Microphone with Bottom Port and Analog Output ," Available online at http://www.analog.com/en/audiovideo-products/imems-microphone/admp401/products/product.html.

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

[7] A. Fleury, N. Noury, and N. Vuillerme, "A fast algorithm to track changes of direction of a person using magnetometers," in *IEEE Conf. in Engineering in Medicine and Biology Society (EMBS)*, 2007.

[8] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *18th Annual Network and Distributed System Security Symposium (NDSS)*, 2011.

[9] D. Giansanti, V. Macellari, and G. Maccioni, "Is it feasible to reconstruct body segment 3-d position and orientation using accelerometric data," *IEEE Trans. Biomed. Eng*, vol. 50, p. 2003, 2003.

[10] H. Gilbert, M. Robshaw, and Y. Seurin, "HB#: Increasing the security and efficiency of hb+," in *Advances in Cryptology - EUROCRYPT, International Conference on the Theory and Applications of Cryptographic Techniques*, 2008.

[11] T. Halevi, S. Lin, D. Ma, A. K. Prasad, N. Saxena, J. Voris, and T. Xiang, "Sensing-enabled defenses to rfid unauthorized reading and relay attacks without changing the usage model (concise contribution)," in *International Conference on Pervasive Computing and Communications (PerCom)*, 2012.

[12] T. Halevi, D. Ma, N. Saxena, and T. Xiang, "Secure proximity detection for nfc devices based on ambient sensor data," in *ESORICS*, 2012, pp. 379–396.

TABLE 3
Experimental result of "positives" using WEKA SimpleLogistics classifier

| | Concert Hall | Library | McDonalds | Library (2) | Cafe |
|---|---|---|---|---|---|
| **Concert Hall** | 100% | 100% | 100% | 100% | 100% |
| **Library** | N/A | 100% | 100% | 100% | 100% |
| **McDonalds** | N/A | N/A | 100% | 100% | 100% |
| **Library (2)** | N/A | N/A | N/A | 100% | 100% |
| **Cafe** | N/A | N/A | N/A | N/A | 100% |


[13] G. P. Hancke and M. 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.

[14] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O'Hare, "Vulnerabilities in first-generation RFID-enabled credit cards," in *Financial Cryptography*, 2007.

[15] 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.

[16] Honeywell, "HMC1053 3-axis magnetic sensor," Available online at http://www.honeywell-sensor.com.cn/prodinfo/sensor_magnetic/datasheet/HMC1053.pdf.

[17] B. Huyghe and J. Doutreloigne, "3D orientation tracking based on unscented Kalman filtering of accelerometer and magnetometer data," in *IEEE Sensors Application Symposium*, Feb 2009.

[18] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, February 2006.

[19] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *ACM Conference on Computer and Communications Security (CCS)*, 2003.

[20] A. Juels, P. F. Syverson, and D. V. Bailey, "High-power proxies for enhancing RFID privacy and utility," in *Privacy Enhancing Technologies*, 2005.

[21] A. Juels and S. Weis, "Authenticating pervasive devices with human protocols," in *International Cryptology Conference (CRYPTO)*, 2005.

[22] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in E-passports," in *Security and Privacy for Emerging Areas in Communications Networks (Securecomm)*, 2005.

[23] 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.

[24] Kionix, "Application note: screen rotation and device orientation," Available online at http://www.kionix.com/App-Notes/AN011 Screen Rotation.pdf.

[25] J. Liu, Z. Wang, L. Zhong, J. Wickramasuriya, and V. Vasudevan, "uWave: Accelerometer-based personalized gesture recognition and its applications," *Pervasive and Mobile Computing*, vol. 5, no. 6, pp. 657–575, December 2009.

[26] D. Ma, A. K. Prasad, N. Saxena, and T. Xiang, "Location-aware and safer cards: enhancing rfid security and privacy via location sensing," in *WISEC*, 2012, pp. 51–62.

[27] D. Ma, N. Saxena, T. Xiang, and Y. Zhu, "Location-aware and safer cards: Enhancing rfid security and privacy via location sensing," *IEEE Trans. Dependable Sec. Comput.*, vol. 10, no. 2, pp. 57–69, 2013.

[28] K. B. Rasmussen and S. Čapkun, "Realization of RF distance bounding," in *Proceedings of the USENIX Security Symposium*, 2010.

[29] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "RFID guardian: A battery-powered mobile device for RFID privacy management," in *Australasian Conference on Information Security and Privacy (ACISP)*, 2005.

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

[31] 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.

[32] A. Sample, D. Yeager, and S. J., "A capacitive touch interface for passive RFID tags," in *IEEE International Conference on RFID*, 2009.

[33] A. A. Sani, L. Zhong, and A. Sabharwal, "Directional antenna diversity for mobile devices: characterizations and solutions," in *ACM MobiCom*, Sept. 2010.

[34] N. Saxena, B. Uddin, 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.

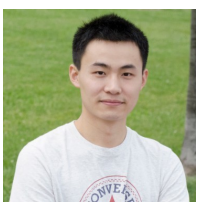
[35] N. Saxena and J. Voris, "Still and silent: Motion detection for enhanced rfid security and privacy without changing the usage model," in *Workshop on RFID Security (RFIDSec)*, June 2010.

[36] J. R. Smith, P. S. Powledge, S. Roy, and A. Mamishev, "A wirelessly-powered platform for sensing and computation," in *8th International Conference on Ubiquitous Computing (Ubicomp)*, 2006.

[37] Sparkfun Electronics, "ADXL330 small, low power, 3-axis ±3 g iMEMS accelerometer," Available at http://www.sparkfun.com/datasheets/Components/ADXL330_0.pdf.

[38] X. Yun, E. R. Bachmann, and R. B. McGhee, "A simplified Quaternion-based algorithm for orientation estimation from earth gravity and magnetic field measurements," *IEEE Tran. on Instrumentation and Measurement*, vol. 57, no. 3, Mar. 2008.


**Tzipora Halevi** Tzipora Halevi is a postdoctoral Researcher in the Dept. of Computer Science and Engineering at the Polytechnic Institute of NYU. Tzipora Halevi received her Ph.D. from Polytechnic Institute of NYU in Electrical Engineering. Her research area is security. Her work focuses on constrained devices, cyber-security and behavioral authentication.



**Haoyu Li** Haoyu Li is a Graduate Student Research Assistant in the Computer and Information Science Department at the University of Michigan-Dearborn. He obtained his bachelor degree in Software Engineering from the Huazhong University of Science and Technology in 2012.

**Di Ma** Di Ma received the BEng degree from Xian Jiaotong University, China, the MEng degree from Nanyang Technological University, Singapore, and the PhD degree from the University of California, Irvine, in 2009. She is an Assistant Professor in the Computer and Information Science Department at the University of Michigan-Dearborn, where she leads the Security and Forensics Research Lab (SAFE). She was with IBM Almaden Research Center in 2008 and the Institute for Infocomm Research, Singapore in 2000-2005. She is broadly interested in the general area of security, privacy, and applied cryptography. Her research spans a wide range of topics, including computation over authenticated/encrypted, fine-grained access control, secure storage systems, wireless network security, smartphone security and privacy, and so on. She won the Tan Kah Kee Young Inventor Award in 2004. She is a member of the IEEE.

**Nitesh Saxena** Nitesh Saxena is an Associate Professor of Computer and Information Sciences at the University of Alabama at Birmingham (UAB), and the founding director of the Security and Privacy in Emerging Systems (SPIES) group/lab. He works in the broad areas of computer and network security, and applied cryptography, with a keen interest in wireless security and the emerging field of usable security.

Saxenas current research has been externally supported by multiple grants from NSF, and by gifts/awards/donations from the industry, including Google (2 Google Faculty Research awards), Cisco, Intel, Nokia and Research in Motion. He has published over 70 journal, conference and workshop papers, many at top-tier venues in Computer Science, including: IEEE Transactions, ACM CCS, ACM WiSec, ACM CHI, ACM Ubicomp, IEEE Percom, and IEEE S&P. On the educational/service front, Saxena is a co-director for UABs MS program in Computer Forensics and Security Management. He was also the principal architect and a co-director of the M.S. Program in Cyber-Security at the Polytechnic Institute of New York University (NYU-Poly). Saxena has instructed over a dozen core fundamental courses in Computer Science, including Computer Security, Network Security, Modern Cryptography and Discrete Structures. Saxena has also advised and graduated numerous graduate (Ph.D. and M.S.) and undergraduate students as well as a few high school students. He is serving as an Associate Editor for flagship security journals, IEEE Transactions on Information Forensics and Security (TIFS), and Springers International Journal of Information Security (IJIS). Saxenas work has received extensive media coverage, for example, at NBC, MSN, Fox, Discovery, ABC, Bloomberg, ZDNet, ACM TechNews, Yahoo News, Slashdot and Computer World.

**Jonathan Voris** Jonathan Voris is an Adjunct Assistant Professor and Postdoctoral Research Scientist at Columbia University, where he is a member of the Intrusion Detection Systems Lab. He obtained his Ph.D. from Polytechnic Institute of New York University in 2012. Jon is interested in improving security and privacy, particularly that of wireless, ubiquitous, and embedded systems. His recent work has been focused on developing techniques to combat insider threats.

**Tuo Xiang** Tuo Xiang is currently working as a Technology Analyst at Goldman Sachs. He obtained his master degree in Electrical Engineering from Electrical and Computer Engineering Department at the University of Michigan-Dearborn in 2013 and bachelor degree in Electrical Engineering from the Huazhong University of Science and Technology in 2011.