Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model

Nitesh Saxena and Jonathan Voris

Computer Science and Engineering
Polytechnic Institute of New York University

Abstract. Personal RFID devices – found, e.g., in access cards and contactless credit cards – are vulnerable to unauthorized reading, owner tracking and different types of relay attacks. We observe that accessing a personal RFID device fundamentally requires moving it in some manner (e.g., swiping an RFID access card in front of a reader). Determining whether or not the device is in motion can therefore provide enhanced security and privacy; the device will respond only when it is in motion, instead of doing so promiscuously. We investigate extending the concept of min-entropy from the realm of random number generation to achieve *motion detection* on an RFID device equipped with an accelerometer. Our approach is quite simple and well-suited for use on low-cost devices because the min-entropy of an accelerometer's distribution can be efficiently approximated. As opposed to alternative methods, our approach does not require any changes to the usage model expected of personal RFID devices.

Keywords: *RFID; min-entropy; activity recognition; context recognition*

1 Introduction

The importance of inexpensive wireless devices, such as those utilizing Radio Frequency Identification (RFID) technology, continues to grow as their deployment in various applications and settings becomes increasingly common. These devices are primarily designed to be inexpensive and as such are equipped with minimalist hardware, often having just enough processing power and memory to achieve their primary function and perhaps also a few low-cost sensors, such as accelerometers and thermometers. Providing security and privacy services in systems consisting of such low cost appliances presents unique challenges due to their highly constrained nature. In order to keep hardware costs down, it is critical to use existing and inexpensive components for these devices as efficiently and in as many ways as possible.

RFID is a wireless technology designed primarily for computerized identification that has been growing in popularity as of late. An RFID infrastructure consists of two main components: tags and readers. Tags are small transponders that store data about their corresponding subject, such as a unique identifier.

Readers are used to query these tags over a wireless radio channel. In most cases, tags are passive or semi-passive. This indicates that they derive the power to transmit data to a reader from the electromagnetic field generated when a reader issues a query to a tag. Additionally, tags typically have memory only in the range of 32 to 128 bits, perhaps just enough to store a unique identifier [15]. These ultra-low memory, computational, and power constraints are necessitated by the fact that RFID tags are designed to be placed ubiquitously in consumer products, appliances, and, in the case of implantable tokens, even users themselves.

RFID tags can already be found in a wide variety of personal devices, including access cards, contactless credit cards, passports, and driver's licenses. In many cases, RFID tags store sensitive personally identifiable information. For example, a US passport stores the name, nationality, date of birth, digital photograph, and (optionally) fingerprint of its user [12]. When stored on an RFID tag, such information can easily be subject to clandestine eavesdropping and unauthorized reading. This data can then be used in order to track the owner of the tag [11]. In addition, the information gleaned from an RFID enabled device may also be utilized to clone the tag, which provides adversaries with the capability to impersonate users [11].

Perhaps even more troubling is the fact that RFID tags are susceptible to "ghost-and-leech" relay attacks [17]. In this type of an attack, an adversary, called a "ghost," relays the information surreptitiously read from a legitimate RFID device to a colluding entity known as a "leech." The leech can then transmit the forwarded information to a corresponding legitimate reader and vice versa. Thus, a ghost and leech pair can succeed in impersonating a legitimate RFID device without actually possessing the device, which violates the security these devices are designed to provide. Although cryptography may be used to address the problem of promiscuous tag transmissions, ghost-and-leech attacks are more stubborn as all known reader-to-tag authentication protocols are vulnerable to this type of attack [7].

1.1 Research Challenges

The common thread among all of the threats to the security and privacy of RFID tags is that the owners of these devices are not in full control of when their tags transmit or which readers the tags transmit to. Techniques aiming to address this dilemma fall into three categories. First, tags could be equipped with a method of determining whether a given reader has been deemed safe to transmit to, which is called *reader-to-tag authentication*. *Tag-to-reader authentication*, on the other hand, can be used as a means to prevent tag cloning and impersonation. Of course, these overarching techniques are easier stated than achieved. Each comes with its own set of shortcomings and design challenges due to the minimalist capabilities of passive RFID tags. In particular, traditional cryptographic techniques may not be suitable for these tags. To this end, there has been a growing interest in designing novel lightweight cryptographic protocols [15, 1, 16, 6].

Rather than having an RFID reader authenticate to the tags, tags can be programmed to detect what is occurring in their environment and only communicate when it makes sense to do so. This third strategy, which is the focus of this paper, is known as *context or activity recognition*. Context recognition can serve as a means of selective tag locking and unlocking and thus addresses the issues of tag privacy, unauthorized reading, and ghost-and-leech attacks. For example, a tag could be programmed to transmit only when it detects a valid context, such as when a user intends to enter his or her office building or make a payment. When not in a situation that is deemed to be relevant, the tag remains in a locked state. As with tag-to-reader and reader-to-tag authentication, activity recognition would be trivial to achieve if RFID tags were rich in computing resources. However, this is clearly not the case in practice. The resource constraints of RFID tags severely hamper the complexity of the algorithms that can be used to judge what activity a tag is undergoing. This process can be outsourced from the tag to the reader [2], but this only exacerbates the issue of reader trust.

Another obstacle confronting activity recognition is the lack of ways in which users can interact with their tags. RFID devices, in contrast to other personal devices, were designed to be as transparent as possible to their users, and as such do not possess any input or output interfaces, such as buttons, displays, or speakers. Furthermore, recall that these passive devices lack a power source of their own. Therefore, in terms of energy, they are wholly reliant on being activated by a reader. Having an intermittent power supply means that it is not possible for a tag to control precisely when it will be able to take readings using the few sensors it may have on board. This makes it very difficult for a tag to reliably receive data about its environment, in turn making activity recognition a challenging problem. Finally, it is very important that any form of context recognition must not alter the expected usage model of the devices they protect in any way. Even subtle changes may have an adverse effect on an RFID system's efficiency and usability, and may severely undermine the benefits the RFID technology was supposed to provide in the first place.

While the security and privacy challenges faced by RFID tags are not specific to this class of devices, their unique combination of minimalist hardware and an atypical usage model necessitates new solutions. In order to fully secure an RFID infrastructure, a combination of tag-to-reader authentication, reader-to-tag authentication, and context recognition might be necessary. The central research challenge presented by RFID tags is how to accomplish these objectives given their constraints and limitations. The focus of this paper is on developing a viable lightweight context recognition technique suitable for low cost RFID tags.

1.2 Overview of Contributions

RFID systems can generally be divided into two main categories in terms of mobility. In a *mobile reader system*, tags are immobilized by embedding them into stationary objects and a reader is carried around to read these tags at fixed

locations. An example of this scenario is RFID tags that are encased in concrete at a construction site to monitor the substance's solidification progress [19]. In a *mobile tag environment*, on the other hand, tags are associated with free moving objects which are read when brought within the range of a fixed reading device. Personal RFID tags, found in contactless access cards and payment tokens, fall into this grouping. This paper focuses on providing improved security and privacy to RFID tags of the mobile variety.

We utilize a theoretical concept from the realm of random number generation, *min-entropy*, to address the issue of context recognition. Our proposal involves the estimation of the min-entropy of a sensor's sample distribution, specifically that of an accelerometer, as a way of performing a limited and simplistic kind of activity detection, which we dub *motion detection*. This approach hinges on the straightforward observation that accessing a personal mobile RFID device fundamentally involves moving it in some manner; the device needs to be brought close to the reader so that its contents can be read, which implies motion of some form. For example, an RFID access card is commonly swiped in front of an antenna in order for a reader to extract its contents. Thus, determining whether or not this type of device is in motion provides a means of controlled locking and unlocking, which in turn provides enhanced privacy as well as protection against ghost-and-leech relay attacks. Intuitively, when motion detection is in place, a device will only respond when it is mobile instead of doing so promiscuously. In other words, if the device is *still*, it remains *silent*. A working prototype implementation of this motion detection technique, on Intel's WISP tags [21, 24], is provided and several associated experiments have been conducted as evidence of its applicability to low-cost RFID devices.

Motion detection, as a downside, is not capable of performing nearly as fine grained activity assessments as full fledged context recognition. However, we argue that this technique is sufficient for preventing some of the most common attacks on RFID devices. In fact, its simplicity is a boon in terms of the range of devices that are capable of supporting it. Moreover, and more importantly, as opposed to all recently proposed alternatives (we review these in Section 2), this approach does not require any changes to the usage model expected of typical RFID devices.

Although we demonstrate the viability of our motion detection method on low cost RFID devices, the method is not limited solely to RFID devices. It extends easily to more traditional mobile devices such as laptops, cell phones, personal fitness aids [18], MP3 players, and video game remote controls. Out of these, mobile phones, fitness aids, and video game controllers are the most likely to come pre-equipped with accelerometers.

Paper Organization: The rest of this paper is organized as follows. We first provide a comparison of our motion detection approach with other solutions in Section 2. We discuss the design of our motion detection approach, the associated experiments and implementation in Section 4. Finally, we discuss several salient features of our proposal and its other applications in Section 5.

2 Related Work: Motion Detection vs. Other Solutions

In this section, we discuss other solutions to the problem of selective unlocking of an RFID device. We provide a side-by-side comparison of motion detection with other relevant approaches in Figure 1.

Secret Handshakes: A recent approach, called "Secret Handshakes" [4] relates closely to our proposal. In order to authenticate to an accelerometer-equipped RFID device (such as a WISP [21, 24]) using Secret Handshakes, a user must move or shake his or her device in a particular pattern. For example, a user might be required to move his or her tag parallel with the surface of an RFID reader's antenna in a circular manner. A number of these kinds of patterns were studied and shown to exhibit low error rates [4].

A central drawback to this method is that a special-purpose movement pattern is required for tags to be unlocked in this fashion. This requires subtle changes to the expected RFID usage model. While a standard, insecure RFID setup only requires users to bring their RFID tags within range of a reader, when tags are secured using "Secret Handshakes", users are required to consciously move their tag in a certain pattern. This may result in a degradation of usability and an increase in the time taken to authenticate to an RFID reader, due to the explicit manual involvement. A full usability study of this scheme has not yet been conducted and its user acceptability is unknown.

Unlocking Technique	Requires explicit user involvement?	Works while tag is stored in a wallet or other objects?	Affects tag form factor?	Auxiliary device needed?	False unlocking possible?
Motion Detection	No	Yes	No	No	Yes, when the tag is mobile
Secret Handshakes	Yes	Yes	No	No	Yes, when a pattern is accidentally executed
Onboard Button	Yes	No	Yes, in case of a physical button	No	No
NFC Phone	Yes	N/A	No (tags are virtual)	Yes, an NFC phone	No
Temperature Detection	Yes	No	No	No	Yes
Sound Detection	Yes	No	Somewhat	No	Yes
Light Detection	Yes	No	No	No	Yes

Fig. 1. Comparison of Motion Detection with Alternative Solutions (highlighted cells represent positive features)

In contrast, the main advantage of the motion detection approach presented in this paper is that it requires no conscious effort on behalf of users and no changes to the standard RFID usage model. Tags will simply detect whether or not they are in motion at the time at which they are read and respond accordingly. Our approach adheres more closely to a typical RFID usage model

and as such is not at all demanding and is already psychologically acceptable. It is also a much simpler and more efficient scheme due to the fact that it only entails an analysis of the frequency of sensor values and not the values themselves. As a result, motion detection is better suited for use on inexpensive wireless devices. A detailed comparison of motion detection and Secret Handshakes, in terms of efficiency, usability and other factors, is provided later in Section 5.

A shortcoming of motion detection relative to the Secret Handshakes approach to context recognition is that the latter is more secure, as the patterns it detects can be somewhat unique and therefore less likely to be executed during the course of routine activities. While securing a tag via motion detection provides no protection against unauthorized reads while the tag is mobile, secret handshake patterns are also likely to be unknowingly exhibited in a user's daily activities as reported in [4]. Thus, a more full fledged form of context recognition such as Secret Handshakes does not rule out the possibility of unauthorized tag reading or ghost-and-leech attacks.

Onboard Button: A simple way to allow a user to selectively activate her tags is by making use of an on-board tag button. In fact, some vendors have started producing such tags for access card applications [3]. This approach, however, requires the user to take out the card from her wallet or purse whenever access is needed. Buttons may also impact the size and shape of the card containing the tag. Our proposal, on the other hand, addresses these drawbacks; the size, shape and bulk cost of an accelerometer might also compare favorably to that of a button. Some vendors have been selling low-power 3 axis accelerometers for around $1 [5]. Note that the mass manufacturing cost of a WISP tag equipped with an accelerometer is also expected to be close to $1 [2]. Instead of a physical button, it is possible to use a virtual button based on capacitive sensing, as proposed in [22]. However, this will still require explicit user involvement, as the tags need to be first removed from the objects (such as wallets) in which they are often stored and carried [4].

NFC Phones: NFC (Near Field Communication) technology is also relevant to the subject of this paper. NFC allows RFID tags to be integrated with a phone and to use the phone as tags. Unlocking of tags can be trivially achieved by having the user press a button on her phone. NFC technology relies on the assumption that mobile phones are almost constantly available to their users. Although emerging in some countries, NFC phones are not widespread today, however. Moreover, NFC is not compatible with other RFID standards, such as Electronic Product Code (EPC); this means that an NFC phone/tag may not work with an EPC reader. As pointed out in [25], deployment of NFC phones is still in early stages and it is likely that for some time to come, the user's tags and the phones will continue to remain as physically separate devices.

Alternative Sensors: It is logical to wonder whether sensors, other than accelerometers, can also be used for selective tag activation, in a similar or superior capacity. Unfortunately, unlike accelerometers, no other type of sensor seems capable of monitoring whether or not passive wireless equipment should be unlocked. In a system consisting of mobile RFID tags and stationary readers, the

movement of a tag implies a context in which it is safe for the tag to transmit. As a motion sensor, accelerometers are exceptionally qualified to serve this function. Different sensors monitor different environmental factors, however, none of which are indicative of an unattacked state. For example, microphones can be quite sensitive to ambient noise, but an increase or decrease in volume level does not imply anything about whether or not it is safe for an RFID tag to transmit its data. Similarly, a thermometer could be used to record the temperature of a device's environment, but there is nothing unique about the temperature near a legitimate reader that would allow an appliance to discern it from a malicious piece of equipment.

Beyond this, the unique RFID usage model must also be taken into consideration when determining the usefulness of various sensors for detecting different contexts. One of the crucial benefits of using RFID tags is that they may be left stowed in a wallet, backpack, purse, or some combination thereof when in use. The ability of sensors to collect information about their surroundings may be severely curtailed when stored in this manner. For example, photometers will be obstructed from collecting ambient light, external sounds will be muffled for microphones, and thermometers will be insulated against external sources of heat. Unlike these forms of sensory equipment, accelerometers can operate unhindered in an enclosed environment. This characteristic also contributes to the unique suitability of accelerometers to the task of securing inexpensive mobile hardware.

Other Approaches: Other approaches to selective tag blocking are "blocker tag" [13], RFID Enhancer Proxy [14] and RFID Guardian [20]. All of these approaches, however, require the users to carry an auxiliary device (a blocker tag in [13] and PDA like special-purpose device in [14, 20]); such an auxiliary device may not be available every time access to RFID tags is needed. 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)[1] would be needed and the tag would need to be removed from the cage in order to be read, thus requiring explicit user involvement. Moreover, building a true Faraday Cage that shields all communication is known to be a challenge.

3 Background

3.1 WISP Tags

In order to investigate motion detection on inexpensive wireless devices, we utilized a special type of RFID tag designed by Intel Research known as a Wireless Identification and Sensing Platform (WISP) [21, 24]. WISPs are passively-powered RFID tags that are compliant with the Electronic Product Code (EPC) protocol. Specifically, we utilized version 4.1 of the WISP hardware, which partially implements Class 1 Generation 2 of the EPC standard. By following this protocol and deriving power only from the transmissions of a commercial off-the-shelf RFID reader, WISPs closely model the type of RFID tag one might

[1] These products are available in the market. See, e.g., MobileCloak: `http://www.mobilecloak.com/mobilecloak`.

expect to find in a typical contactless access token. Where the WISP differs from standard tags, however, is in its inclusion of an onboard Texas Instruments MSP430F2132 microcontroller and sensors such as the ADXL-330 three-axis $\pm 3g$ accelerometer. This 16-bit MCU features an 8 MHz clock rate, 8 kilobytes of flash memory, and 512 bytes of RAM. WISPs are the first programmable passive RFID devices. They have seen use in studies on a variety of topics, from energy harvesting experiments [10, 9] to monitoring animal behavior [8, 23]. Unlike standard RFID tags, which are fixed function and state machine based, the flexibility of WISP tags allowed us to implement novel security solutions on a live, passive RFID device. Recall that the manufacturing cost of a WISP tag is expected to be close to $1 [2].

3.2 Random Number Generation Theory

In this section, background information on the generation of random values is presented. This is necessary due to the fact that the motion detection system presented in this work is based on a concept from the domain of cryptographic random number generation. When designing cryptosystems, an infinite source of perfect randomness is often assumed to be present. This assumption raises several important questions. In practice, how can this ideal randomness be realized? And exactly what are the properties that the random output should possess?

Cryptographic applications demand "strongly" uniform numbers. The bits of the number must be independent and uniformly distributed, or as close to this as attainable. In other words, each bit should be the result of an idealized, unbiased coin toss where there is always an even chance that the outcome is a 0 or a 1. If this type of random value was naturally occurring, utilizing it would be a relatively simple matter of recording it and handing it to the cryptographic application. Unfortunately, such "strong" randomness is unlikely to be available in practice. While many naturally occurring phenomena are unpredictable, they necessarily contain some bias rather than being distributed uniformly. From the perspective of a cryptographic application expecting high quality randomness, this bias is unacceptable because it could potentially be exploited by an adversary to extract information about the cryptosystem's internal state.

Extraction functions have been created to bridge the gap between the expectations of cryptographic designers and the realities of entropy availability. An extractor is a function that takes a string of unpredictable but biased, or "weakly" random, bits as input and returns a string of close to uniform, or "strongly" random, bits as output. Because unpredictable bits derived from observations of natural phenomena are unlikely to have a known mathematical structure, extractors have been developed that can be used on forms of input that can have any structure, but are instead required to have a certain amount of min-entropy. Min-entropy, a mathematical property of a distribution, is defined as follows:

Definition 1. *The min-entropy of a given distribution X on $\{0,1\}^n$ is:*

$$min\text{-}entropy(X) = \min_{x \in \{0,1\}^n} \log_2 \frac{1}{Pr[X = x]} \quad (1)$$

In words, the min-entropy of a distribution is equal to the probability of the most likely element in X being drawn from X. From a different perspective, if a distribution X has a min-entropy of k, the likelihood of drawing any single element x from X does not exceed $1/2^k$ for all $x \in X$.

Min-entropy is an important measurement of a distribution because it captures the amount of randomness a distribution is capable of supporting. Despite the fact that elements of X are n bits in length, due to the bias of the distribution, X may not contain enough entropy to actually support the extraction of n unbiased bits. Only k "strongly" random bits can be derived from a distribution that has a min-entropy of k regardless of the distribution's element length n.

4 Motion Detection

In this section, we describe the design of our motion detection technique and the associated experiments. Recall, from Section 1.2, that accessing a mobile RFID device always involves the device being moved. Thus, determining whether or not the device is in motion is sufficient to provide a reasonable level of security and privacy in the context of most common usage scenarios. This is because motion implies an unlocked state and stillness implies a locked state. The aim of these experiments was to create a lightweight mechanism that, while being unable to differentiate between many types of motions, would still be capable of detecting movement properties in a way that is simple enough to be implemented on low-cost wireless devices, irrespective of their hardware restrictions.

For such a mechanism, we turned to the measurement discussed in Section 3.2 to evaluate the amount of randomness contained within a distribution – min-entropy. Clearly, the min-entropy of a distribution of accelerometer readings is closely related to how the RFID tag housing the accelerometer is moving. Min-entropy estimation is a very simple measurement, however. While this simplicity is attractive from the perspective of what devices it can be estimated on, it remained to be seen whether this was also a hindrance in terms of whether or not the measurement would be of any use at all in terms of movement recognition accuracy. Thus, we set out to determine whether or not the measurement of min-entropy is sufficient to accomplish motion detection.

The equation for calculating min-entropy based on a sample distribution was shown in Definition 1. This is computationally simple enough that it can be performed on a wide range of wireless devices. Prior to performing any tests by implementing this on the WISP tags, however, we observed that in order to approximate the min-entropy of a sensor sample, the min-entropy value itself does not actually need to be computed. This is because with a fixed distribution size, min-entropy is a function with only one input, namely the number of occurrences of the most frequently occurring value within the distribution. Thus, rather than actually calculating min-entropy using the equation in Definition

1, the device can quickly develop a rough estimate of a sample distribution's relative min-entropy by instead keeping track of the frequency at which each value occurs and dividing the count of the most common value by the size of the distribution. (Pseudocode for the motion detection algorithm we employed is shown in Algorithm 1).

If acceleration samples could be taken over an extended time interval on a lightweight wireless device, it would ensure an accurate estimate of the sensor's min-entropy. Unfortunately, this is not possible. First, the limited memory capacity of this class of wireless devices renders storing these many samples implausible. Furthermore, processing a large number of samples would be taxing for a device with low computational and power resources. Finally, aside from hardware restrictions, gathering this many samples would simply take too much time to result in a usable security solution. For this reason, we settled on a sample size of 40 as a level that would be attainable on even the most minimalist hardware, such as a passive RFID tag.

4.1 Experiments

Accelerometer samples were taken from a wireless sensor while various types of motions were performed. These were necessary in order to determine the feasibility of differentiating between movement and stillness. Measurements were recorded over a 10 minute interval while a variety of different movements were performed with the tags. The sample with the least amount of motion involved was the *stationary test*, where the WISP tag was simply left sitting on a desk. This test was meant to model a scenario where a tag is placed in front of an (adversarial) RFID reader's antenna without actually being held by a user. The *overnight test* was identical to the stationary test, only the tag was left to be queried by the reader overnight rather than for just 10 minutes.

Fig. 2. WISP tag inside of a wallet in front an Impinj RFID Reader

The *hand test* measured the min-entropy of the accelerometer readings while the WISP tag was held in the palm of a hand. This test was meant to model a scenario where a tag is presented in front of an RFID reader's antenna while being hand-held by a user. Along the same lines, the *hand wallet test* was performed with a tag placed inside a wallet while the wallet was being hand-held

(see Figure 2). The *arc swipe* sample involved moving the WISP tag in an arc like half circle pattern from the middle left hand side of the reader's antenna, to the center top of the antenna, then to the middle right hand side of the antenna, and then back again. This test was meant to model a scenario where a tag is swiped in front of an RFID reader's antenna in a certain manner while being held by a user.

For the *drop test*, the WISP tag was repeatedly picked up and vertically dropped in from the antenna. This test was meant to stimulate items being deposited in front of an RFID reader as they move down a conveyor belt in a factory or retail checkout, or simply when the device accidentally falls. Next on the list is the *triangle test*, for which the WISP tag was moved in a triangular pattern from the bottom left hand corner of the reader's antenna, to the top center of the reader's antenna, then to the bottom right hard corner, before being moved back to the bottom left. For the *alpha test*, the tag was moved in a loop resembling a lower-case Greek letter alpha. Both the alpha and triangle tests were also meant to model a scenario where a tag is swiped in front of an RFID reader's antenna in a certain manner while being held by a user.

Instead of moving the tag parallel to the reader surface, for the *key twist test*, the tag was held relative to the antenna but spun in circles around its central axis. This test represents the motion underwent by an RFID tag embedded in a key when opening a door. The *circle test* saw the WISP tag moved roughly in a circle in front of the antenna, once again to model a scenario where a tag is swiped in front of an RFID reader's antenna in a certain manner while being held by a user. The arc swipe, triangle, alpha, key twist, and circle motions were first suggested in the study of Secret Handshakes [4] and were included to provide a basis for comparison with this work.

For the *sitting still test*, a 10 minute sample was taken while sitting motionless on an office chair. The WISP tag was placed in a side pocket of the tester's pants while the RFID reader's antenna was placed alongside the tester's thigh. The setup for the *sitting shaking test* was similar, but instead of not moving while sitting, the tester rocked and shook back and forth on the chair. This test was meant to simulate the effect of sitting on a train, bus, or other form of mass transit as it moved along bumpy tracks or a poorly-maintained road. We also simulated the effect of *walking or running* on the tag by placing the tag in a side pants pocket and walking or jogging in place for 10 minutes while the reader's antenna was held alongside the leg where the tag was placed.

Personal Fitness Aids: We also considered other personal devices, such as the "Nike + iPod Sports Kit". The Nike Kit is a wireless appliance that works with Apple iPods and iPhones. It consists of a wireless sensor which users place in one of their shoes as well as a receiver that they attach to their iPod or iPhone. The sensor records information during a user's workout and transmits it over the wireless channel to the receiver, which then relays it to the user through audio output. The authors of [18] demonstrated that the information this device transmits, specifically, a unique identifier, is subject to eavesdropping and illicit user tracking, even while users are not working out. Although the sensor is

equipped with an On/Off button, once the sensor is placed inside the shoe, users no longer have access to this switch. Our motion detection technique can be used to address this problem.

Fig. 3. WISP tag fastened to a shoe in front of an Alien Antenna connected to an off-camera Impinj RFID Reader

Rather than purchasing and working directly with a Nike Kit, several supplemental measurements were taken with a powerless WISP tag and its onboard accelerometer to reproduce the expected usage scenario for this appliance. Each of these tests was performed with a WISP tag affixed to the tester's sneaker using inexpensive electrical tape. For the *shoe stationary test*, a 10 minute sample was taken with this RFID enhanced shoe left sitting still on the floor and the antenna of the RFID reader placed alongside it. See Figure 3 for a pictorial representation of this setup. The *shoe walking* and *shoe jogging* were, as one might anticipate, modifications of the walking or jogging samples where the WISP tag was mounted on the subject's shoe rather than placed in his or her pocket. In both instances, the antenna attached to the RFID reader was again shifted to the floor several inches away from the tag in order to be capable of reading it while the tester's foot was in motion.

Samples with Different Users: All of the samples taken thus far were performed by the same test subject. While little variation was anticipated in the non-interactive samples, such as the stationary ones where a tag was left sitting on a desk, we wanted to make sure our tests captured any differences that might exist between the motions when performed by different volunteers. We therefore repeated the hand held and arc swipe tests with four different volunteers.

4.2 Motion Detection Algorithm

Having obtained the samples from our different tests, it next had to be determined how to partition these into 40 unit pieces that could be analyzed for motion detection accuracy. Initially, we simply broke the n length samples into $n/40$ pieces and analyzed them separately. When it came time to implement our motion detection scheme on WISP tags, however, we realized this was a flawed approach. This is due to the fact that testing for motion in this manner

Algorithm 1 Motion Detection Pseudocode

```
sampleList[sampleIndex] = currentSample
sampleIndex = (sampleIndex + 1) mod sampleListSize
for sample1 in sampleList do
  for sample2 in sampleList do
    if sample1 = sample2 then
      occurrences = occurrences + 1
    end if
  end for
  if occurrences > maxOccurances then
    maxOccurances = occurrences
  end if
end for
if maxOccurrences < threshold then
  tag = moving
else
  tag = still
end if
```

meant that a judgment regarding motion could only be made every 40 samples. As an alternative, we adopted a "sliding window" technique. In this approach, 40 samples are still initially buffered before the first decision is made regarding movement. After the next sample is obtained, however, the earliest sample is discarded and replaced with the new one. In this way, instantaneous snap judgments regarding motion are possible because only one additional sample is required after the initial sample buffering period. The pseudocode for our approach is depicted in Algorithm 1.

With the sample determination method settled upon, all that remained was to find suitable thresholds for each of the accelerometer axes. To achieve this, each of the movement samples was iterated over in the sliding window fashion described above. For each of these windows, the number of times each value repeated was counted, and the maximum number of repeated values was noted. Recall that min-entropy is a function of the number of times the most frequently occurring value in a distribution occurs. The minimum, average and maximum number of these maximum occurrences were recorded across all sliding windows for each sample.

These measurements were used to create a range of potential thresholds. This range of thresholds was searched until a suitable value was found. In order to measure the performance of threshold values relative to one another, a scoring metric was used where each time 90% or more of the windows analyzed in a sample were correctly identified as moving or still, the threshold values were awarded a point. The threshold value with the most points was selected as optimal.

4.3 Implementation Challenges

Our motion detection algorithm was designed to be readily used by wireless devices of all kinds, including those whose computing resource are severely lacking. As a result, there were few notable challenges encountered while implementing it on a WISP tag. Minimal changes were needed to port the motion detection code from a traditional computer to the computational RFID device. Rather than storing and comparing the accelerometer readings as binary strings, each axis was converted to a unsigned integer to reduce the amount of storage space required and improve the efficiency of value comparison. Along the same lines, rather than allocating memory for a new temporary sliding window array each time a new sample was introduced, a single array was used where the oldest accelerometer value was overwritten by the newest value each time one was recorded.

4.4 Results, Interpretation and WISP Implementation

Type of Movement	**% Still**	**% Moving**
Overnight #1	100.000%	0.000%
Overnight #2	100.000%	0.000%
Stationary #1	100.000%	0.000%
Stationary #2	100.000%	0.000%
Sitting Still	99.786%	0.214%
Hand	94.091%	5.909%
Volunteer Hand #1	98.246%	1.754%
Volunteer Hand #2	100.000%	0.000%
Volunteer Hand #3	95.950%	4.050%
Volunteer Hand #4	99.354%	0.646%
Hand Wallet	99.663%	0.337%
Shoe Stationary	100.000%	0.000%
Arc Swipe	0.000%	100.000%
Volunteer Swipe #1	0.000%	100.000%
Volunteer Swipe #2	0.000%	100.000%
Volunteer Swipe #3	0.000%	100.000%
Volunteer Swipe #4	0.000%	100.000%
Drop	2.369%	97.631%
Triangle	0.000%	100.000%
Alpha	0.000%	100.000%
Key Twist	0.000%	100.000%
Circle	0.000%	100.000%
Sitting Shake	1.579%	98.421%
Walking	0.000%	100.000%
Jogging	0.000%	100.000%
Shoe Walking	4.318%	95.682%
Shoe Jogging	0.000%	100.000%

Table 1. Accuracy of Motion Detection for Different Types of Movement

The performance of our motion detection scheme with the best possible threshold value is provided in Table 1. For the volunteer hand tests, the average "still" recognition percentage was 98.388% and the mean percentage mistakenly labeled as "moving" came to 1.6125%. The standard deviation values for stillness and motion of the volunteer hand samples were equal to 1.541. For the volunteer swipe motion tests, the motion detection scheme correctly identified all windows as moving for all volunteers. The mean stillness and movement percentage were therefore 0.000%, and 100.000% with standard deviations of 0.

In all cases, this motion detection algorithm was able to correctly identify whether a WISP tag was in motion or at rest for at least 94.091% of the sample windows. This demonstrates the ability of this minimalist technique to correctly capture whether or not a wireless device is in motion at any given time. However, does this meet the desired goal of being applicable to enhancing the security of mobile devices? All the cases where the tag has been identified as still are situations where the tag should not be read. This approach therefore handles these cases without difficulty.

Some of the cases identified as being in motion are problematic, however. Rows colored in dark gray indicate a sample identified as stationary for which it is desirable to keep tags locked. Light gray rows are cases identified as moving for motions indicative of unlocking tags. Medium gray rows are the undesirable cases where tags are identified as moving but it would be beneficial from a security perspective to keep the tags locked. While all the swiping related motions indicate a willingness to unlock the tag, others do not. These troubling cases include Sitting Shake, Walking, Jogging, Shoe Walking, and Shoe Jogging. Thus, while this technique is useful for defending against unauthorized tag access while a tag is held in a motionless hand, pocket, or simply left on a surface, it leaves tags vulnerable while their user is undergoing intense motion such as running. So it would still be possible to perform a man-in-the-middle attack on a person who is walking with their tags or riding a train down turbulent tracks.

Finally, to demonstrate the ability of constrained low-cost wireless hardware to handle this motion detection technique, it was implemented on WISP tags. Rather than programming the tags to transmit only when moving as would be the case in a practical setting, for our tests we programmed the tag to transmit a static EPC identifier indicating three states: insufficient samples to make a judgment regarding motion, still, and moving. This was done because a non-transmitting tag is an ambiguous result; the tag may simply have insufficient power to perform the given computation, for example. Repeating the motions depicted in Table 1 with a tag programmed in this fashion verified that the motion detection technique was indeed functioning as well on the WISP tag as in the sample based simulations. That is, activities where the majority of windows were identified as moving in the threshold tests were also identified as moving by the tag-based movement detection code, and the same was true for movements identified as being still.

5 Discussion

5.1 Efficiency

In our experimental setup, the time between consecutive WISP reads over all 4,254,166 samples taken over the course of our study was 31.245 milliseconds. In terms of timing, our motion detection technique requires an initial 40 samples to draw the first conclusion regarding whether the tag is moving or not, which takes $40 * 31.245$ milliseconds $= 1.250$ seconds to collect. After this, a new conclusion can be drawn as to whether or not the tag is in motion with each sample that is collected approximately every 31.245 milliseconds. Thus, there is no reason why motion detection could not immediately be deployed into present RFID systems.

Please note that the alternative Secret Handshakes solution takes about a second to register a given gesture followed by two seconds of transmission over the device's wireless interface [4]. In contrast, motion detection takes 1.25 seconds on average to first notice whether or not a device is in motion and approximately 31 milliseconds for each subsequent judgment, inclusive of all necessary reader-to-tag and tag-to-reader transmission overhead. Motion detection therefore compares favorably to Secret Handshakes in terms of efficiency.

5.2 Usability

Both Secret Handshakes and motion detection were tested with a small group of three or four users and were found to be robust to variations caused by minute differences between the way different people performed different motions. It may be possible that Secret Handshakes suffers from usability issues that were not captured in this study, however. For example, prior to testing for false positives (i.e., the possibility of the tag remaining locked even when the user intends to unlock it) when using Secret Handshakes, users were allowed to practice the gesture in question for five minutes [4]. It may be the case that in practice, when trying to recall the precise pattern required to unlock a tag, it may take a user several attempts to perfect the gesture, leading to an increase in false positives and a decrease in usability as users are effectively denied the services of their access token or have to repeat the process. Since motion detection does not rely on the ability of users to recall a single gesture, it does not suffer from this drawback. Additionally, when faced with a device that is not operating as expected, a common user response is to jostle the device. In the unlikely event that a tag is not undergoing sufficient motion to be unlocked when presented to a reader, the intuitive user action of shaking or tapping the tag will automatically activate it. Thus, another usability benefit of motion detection is that it requires little to no training.

Furthermore, Secret Handshakes requires a registration phase in which a motion template is constructed that can infer user's movements. This is undesirable for several reasons. First, having to perform this registration step puts an unnecessary burden on the device's user. The authors of [4] suggest that it might be possible to construct a single generic motion template that would work for every

user. However, it is unclear how this would be accomplished in practice and, perhaps more critically, what the implications of such a template would be for the level of false negatives (i.e., false unlocking) and false positives experienced by individual users. The motion template must also be stored on each user's RFID tag, using up some of the device's precious storage resources and leading to further complications. How would a tag receive a new template? If it is transmitted to the tag over its wireless interface, this leads to the possibility of a malicious entity replacing a user's desired template with one of their own design. An attacker could use this opportunity to craft a template that either never unlocks a users tag, thus launching a denial of service attack on the RFID infrastructure, or always unlocks a tag, undermining the level of protection which this scheme was designed to offer. Since motion detection does not hinge on an RFID tag's capacity to detect one individual's specific hand motion, it does not require any enrollment prior to use and is therefore exempt from having to address these challenges as well.

A final aspect in which the usability of motion detection and Secret Handshakes differs lies in the flexibility it offers to users in terms of where they may choose to keep their tags during the authentication process. One of the central benefits of Secret Handshakes is the fact that it provides increased security and privacy without requiring that users remove their tags from their wallets. Survey results presented in [4] show that this is by far the most popular way in which RFID tags are utilized, since it is preferred by 64.4% of contactless access card users. It is still far from the only way in which users have become accustomed to stowing their passive access tokens, however. The same study found that 13.6% of users held their wireless devices on a lanyard, either above or below their clothing. It is unclear how applicable Secret Handshakes is to this class of users, as the attachment of the tag to an object or themselves via a cord may severely hamper their ability to freely move the device in a specific Handshake pattern.

Along the same lines, performing a Secret Handshake seems even less plausible for the 5.2% of users who responded that they keep an access card stored loose in a purse. This is because moving a large bag containing an RFID tag, among its many contents, in a specific pattern does not imply that the tag will register the exact same movement as a tag on its own or in a smaller means of storage such as a wallet. The other objects in the bag, as well as the material of the bag itself, will surely have an impact on the motion the tag undergoes. The results of this study did not report preferred forms of contactless identification storage that are similar to tags being loosely placed in a purse, such as tags that are placed loosely in a backpack, tags in wallets that are placed in a purse, or tags in wallets that are placed in a backpack. Secret Handshakes seems similarly problematic for users who typically utilize these storage techniques, which means that the percentage of users to which this method does not apply may be higher in practice. Since motion detection is agnostic to the manner in which an RFID device is stored, it is applicable to a wider array of users and their varied access token usage habits. Thus, in several regards, motion detection demonstrates improvements in usability over Secret Handshakes.

5.3 Simplicity

Due to its uncomplicated design, motion detection is not capable of differentiating between motions of all kinds. It is not capable of discerning whether a wireless device is in motion due to a particular gesture or because its owner is in motion, for example. However, including this mechanism on wireless devices would raise the bar required for attacks to succeed by eliminating many of the most common attack scenarios, such as those where an unattended tag is read without its owner's consent or knowledge. Furthermore, motion detection has several advantages over more robust forms of activity recognition. One such asset is its ability to be implemented on all wireless devices, regardless of their hardware limitations. Secondly, including motion detection as a security measure requires absolutely no change in usage by end users, as opposed to the subtle changes required by alternative schemes such as Secret Handshakes.

5.4 Other Applications

In this paper, our focus was on personal RFID devices. However, our motion detection technique can in principle also be used to improve the security and privacy of impersonal tags carried by users, such as the ones on clothing products, books and other items. The only problem with using our approach on an impersonal tag is the increased cost due to the requirement of an onboard accelerometer. Note that such tags need to be very inexpensive due to their deployment in massive numbers. Motion detection can also be applied to secure vehicle toll payment tokens under the condition that a vehicle must always be accelerating or decelerating when the tag is to be authenticated, as an automobile moving at a constant velocity will obviously not cause an accelerometer to register any change in speed. Note that even with this restriction in place, recognizing motion is better suited to this scenario than more specialized forms of detecting activity, such as Secret Handshakes.

In addition, motion detection can be used to augment security in scenarios that do not involve mobile devices directly. One such application is providing physical security by affixing RFID tags to objects which need to be stationary such as safes, lock boxes, or other containers for storing valuables. If a thief were to try to steal an object with a motion recognizing tag embedded in it, the object will have to be moved. As a result, the tag would detect the motion and could take a precautionary measure such as activating an alarm.

5.5 Applicability to Other Devices

Throughout this work, we have illustrated the viability of our proposal by implementing it on WISP RFID tags. This does not imply that this approach is only applicable to these appliances, however. WISP tags were selected as our primary target because they represent the lowest common denominator of wireless devices. This is due to their ultra-low cost hardware and passive backscatter power source. Having shown that the technique of motion detection works by

implementing it on these devices implies that it will also be capable of functioning on more full featured hardware. While this proposal may be most beneficial for hardware with constraints that rules out any alternative methods of activity recognition, it is applicable to all wireless devices.

6 Conclusions and Future Work

In this paper, motion detection, a novel approach to activity recognition, was described. By reducing the expectations of the precision of the detection procedure, the applicability and usability of the approach were actually increased. This is particularly beneficial for RFID systems with no tolerance for any usage model changes as well as where hardware constraints put standard activity recognition techniques out of reach. As future work, we intend to investigate several aspects of motion detection in greater detail. We will explore simple mechanisms which can detect the motion context more precisely and with a finer granularity, such as differentiating the tag swiping context from the one imposed on the tag due to the walking/running of the tag's owner. More accelerometer samples will be taken via a user study. Furthermore, while the samples in this work present strong evidence of the applicability of our approaches to different scenarios, the degree to which the motions performed in the lab may differ from those observed in real life remains an open question. Thus, field experiments can be conducted to compare the laboratory readings to those in the external world, such as while actually riding various forms of mass transit or running a distance.

Acknowledgments

We would like to thank RFIDSec'10 anonymous reviewers for their helpful feedback. This work was partially supported by the United States Department of Education GAANN grant P200A090157.

References

1. J. Bringer, H. Chabanne, and E. Dottax. HB++: a Lightweight Authentication Protocol Secure against Some Attacks. In *Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2006.
2. M. Buettner, R. Prasad, M. Philipose, and D. Wetherall. Recognizing Daily Activities with RFID-Based Sensors. In *International Conference on Ubiquitous Computing (UbiComp)*, 2009.
3. S. Corporation. SMARTCODE Solves the Privacy Issue Relating to Potential Unauthorized Reading of RFID Enabled Passports and ID Cards. 2006.
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. M. Electronics. MMA7660FCR1 Freescale Semiconductor Board Mount Accelerometers. 2009.
6. H. Gilbert, M. Robshaw, and Y. Seurin. HB#: Increasing the Security and Efficiency of HB+. In *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, 2008.

7. G. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *IEEE Symposium on Security and Privacy (S&P)*, 2006.
8. J. Holleman, D. Yeager, R. Prasad, J. Smith, and B. Otis. NeuralWISP: An Energy-Harvesting Wireless Neural Interface with 1-m Range. In *IEEE Transactions on Biomedical Circuits and Systems (BioCAS)*, 2008.
9. B. Jiang, S. Roy, K. Sundara-Rajan, M. Philipose, J. Smith, and A. Mamishev. Energy Scavenging for Inductively Coupled Passive RFID Systems. In *IEEE Instrumentation and Measurement Technology Conference*, 2005.
10. B. Jiang, J. Smith, M. Philipose, S. Roy, K. Sundara-Rajan, and A. Mamishev. Energy scavenging for inductively coupled passive RFID systems. In *IEEE Transactions on Instrumentation and Measurement*, 2007.
11. A. Juels. RFID Security and Privacy: A Research Survey. In *IEEE Journal on Selected Areas in Communications*, 2006.
12. 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.
13. 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.
14. A. Juels, P. F. Syverson, and D. V. Bailey. High-power proxies for enhancing rfid privacy and utility. In *Privacy Enhancing Technologies*, pages 210–226, 2005.
15. A. Juels and S. Weis. Authenticating Pervasive Devices with Human Protocols. In *International Cryptology Conference (CRYPTO)*, 2005.
16. J. Katz and J. Shin. Parallel and Concurrent Security of the HB and HB+ Protocols. In *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, 2006.
17. 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.
18. T. S. J. Lester, C. Hartung, S. Agarwal, and T. Kohno. Devices That tell on You: Privacy Trends in Consumer Ubiquitous Computing. In *USENIX Security Symposium*, 2007.
19. M. O'Connor. RFID Cures Concrete. 2006.
20. 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.
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. Sample, D. Yeager, and J. Smith. A capacitive touch interface for passive RFID tags. In *Proceedings of the 2009 IEEE RFID Conference*, 2009.
23. N. Segawa. Behavior Evaluation of Sika Deer (Cervus Nippon) by RFID System. In *WISP Summit*, 2009.
24. J. Smith, A. Sample, P. Powledge, A. Mamishev, and S. Roy. A Wirelessly-Powered Platform for Sensing and Computation. In *8th International Conference on Ubiquitous Computing (Ubicomp)*, 2006.
25. J. Sutter. CNN Article: Wallet of the future? Your mobile phone, 2009. Available at `http://www.cnn.com/2009/TECH/08/13/cell.phone.wallet/index.html?eref=igoogle_cnn`.