Vibrate-to-Unlock: Mobile Phone Assisted User Authentication to Multiple Personal RFID Tags

Nitesh Saxena
Polytechnic Institute of NYU
nsaxena@poly.edu

Md. Borhan Uddin
Stony Brook University
mduddin@cs.sunysb.edu

Jonathan Voris
Polytechnic Institute of NYU
jvoris@cis.poly.edu

N. Asokan
Nokia Research Center
n.asokan@nokia.com

***Abstract*—Personal RFID tags store valuable information private to their users that can easily be subject to eavesdropping, unauthorized reading, owner tracking, and cloning. RFID tags are also susceptible to relay attacks and likely to get lost and stolen. In this paper, we introduce the problem of user authentication to RFID tags. This allows users to control when and where their RFID tags can be accessed. We present a novel approach for user authentication to *multiple* RFID tags called "Vibrate-to-Unlock" (VtU). This technique uses a mobile phone as an authentication token, forming an unidirectional tactile communication channel between users and their RFID tags. Authenticating to an RFID tag involves touching a vibrating phone to the tag or an object carrying the tag, such as a wallet. We discuss the design and implementation of this new method on Intel's WISP tags. We also report on a preliminary usability evaluation of our VtU prototype.**

I. Introduction

User authentication is one of the most important problems in security. It occurs whenever users have to provide credentials to prove their identity in order to access a computing resource. The goal of this process is to ascertain that only legitimate users are granted access. The increasing popularity of personal devices and the sensitivity of information they store prompts the need for usable authentication mechanisms.

A. RFID Devices and Underlying Threats

Passive RFID (Radio Frequency IDentification) tags are personal devices that are found in access cards, badges, contactless credit cards, e-passports, and driver's licenses. They often store sensitive information. For example, a US passport stores the name, nationality, date of birth, and digital photograph of its user [1]. Unlike other devices, such information can easily be subject to clandestine eavesdropping when stored on RFID tags, which can lead to owner tracking [2]. This information may also be used to impersonate the tag owner via cloning [2]. Moreover, RFID devices can be lost or stolen, which endangers the services they provide. For example, a stolen wallet containing a worker's access card allows unauthorized entry into his or her office building.

Furthermore, RFID tags are susceptible to "ghost-and-leech" attacks [3]. Here an adversary, called a "ghost," relays the information surreptitiously read from a legitimate RFID device to another colluding adversary, called a "leech." The leech transmits this information to a legitimate reader and vice versa, and can thus impersonate the RFID tag. All tag-to-reader authentication protocols are vulnerable to this form of attack [5].

B. Research Problem: User Authentication to RFID Devices

In this paper, we introduce the problem of user authentication to personal RFID tags. Authentication would provide control over when and where RFID tags can be accessed, thus preventing some of the aforementioned attacks. As an example, imagine Alice goes shopping carrying a contactless credit card. The card is in a default locked state and does not respond to read requests. When ready for checkout, Alice unlocks the credit card by authenticating to it. Once the transaction completes, the card again gets locked.

A research challenge confronting RFID user authentication is that RFID devices were meant to be transparent to users. They therefore lack output and input interfaces. Moreover, the RFID usage scenario is atypical since tags may be stored in other objects, such as wallets, while in use [6]. The fact that a user might carry multiple tags exacerbates this issue. Another challenge is that RFID devices are constrained in terms of computation, memory, and power. RFID user authentication is thus quite challenging.

C. Mobile Phones as Authentication Tokens

Mobile phones have become an integral part of users' lives. Unlike other tokens, phones are almost constantly available to users due to their desire to remain socially connected. Mobile phones also provide people with a sense of security [7]. Recent surveys demonstrate an emerging "always on, always with me" phone usage trend [8], [9], [10], [11]. We therefore believe that such devices can be exploited to achieve RFID user authentication. Using mobile phones to authenticate to remote servers has been proposed in prior research [12], [14].

D. Our Contributions and Paper Outline

We make the following contributions. We propose a novel approach to RFID user authentication called "Vibrate-to-Unlock" (VtU). It works by using a mobile phone as an

authentication token that stores tag specific PINs that authenticate to *multiple* RFID tags. Authentication is achieved when a user touches his or her vibrating phone with an RFID tag or its container. To the best of our knowledge, VtU is the first proposal to utilize phones for RFID tag authentication.

Our approach offers several advantages over existing solutions. First, a double layer of protection is provided. To access a tag's service an adversary would need access to the tag as well as its user's phone. This provides improved resilience in the event of loss or theft of tags. Second, the phone acts as a "master key" that allows users to authenticate to multiple tags. Critically, unlocking one tag does not unlock other tags stored in the same container (e.g., a wallet). Third, since each tag can only be unlocked by a unique PIN stored on the phone, unauthorized reading and relay attacks are completely eliminated. In other words, false tag unlocking is not possible. Finally, our approach is automated and transparent to users and does not impose any usability constraints. In particular, users do not need to memorize any PINs. A more detailed comparison of VtU with alternate mechanisms is provided in Section II.

VtU is based on a novel vibrational communication channel. In Section IV, we discuss the design and implementation of this channel. Accelerometers have been used in prior research for activity recognition. However, to the best of our knowledge, this work is the first to use accelerometers for device-to-device (d2d) communication. Designing an effective d2d communication channel is a challenging task due to severe resource constraints on passive RFID tags. We also report on an *initial* usability evaluation of VtU (Section V). Our test results indicate it to be efficient, robust, and user-friendly. Our current VtU prototype takes about 8 seconds to execute and has an error rate of 0% while offering 12-bit security. An efficiency-oriented instantiation of VtU, called VtU-Button, takes only 600 ms while still protecting against unauthorized reading and ghost-and-leech attacks (but not in the face of tag loss or theft). Finally, other important applications and variations of VtU are presented in Section VI-C. Our approach can be used to selectively unlock a variety of accelerometer equipped wireless devices.

II. Related Work

This section discusses relevant prior work. VtU is closely related to a recent approach called "Secret Handshakes" [6]. The main focus of this scheme is to prevent ghost-and-leech attacks, but it can also defend against unauthorized RFID tag reading. To authenticate to an accelerometer-equipped RFID device [15] using Secret Handshakes, a user must move the device in a specific pattern. A number of patterns were studied and shown to exhibit low error rates [6].

Secret Handshakes has some drawbacks, however. *First*, a user might be carrying multiple RFID devices. When the user shakes a wallet in a particular manner in order to unlock a desired tag, *all* of the devices in the wallet will unlock. Attacks can thus be mounted on all other devices. To prevent this, each device must have a *unique* pattern and users must memorize which pattern to use with which device. This will be cumbersome as the number of devices increase. *Second*, handshake patterns are likely to be exhibited during daily activities [6]. Thus, unauthorized reading attacks can not be completely ruled out. The *third* drawback is that there is no protection against device loss or theft. This provides a weaker level of security than the password protection typically employed for other personal devices such as mobile phones. Although it is based on a slightly demanding usage model, VtU addresses these drawbacks. In addition, our method has several other advantages as we will discuss in Section VI-A. Unlike [6], we also validate the feasibility of our approach via a preliminary usability study.

A simpler way to selectively activate tags is by making use of an onboard button. Some vendors have started producing tags with this feature for access card applications [16]. However, this approach requires that users take the card out of its container (e.g., a wallet) whenever access is needed. This approach suffers in terms of usability and higher form factor of the card etc.

Unlike our scheme, NFC (Near Field Communication) is not compatible with other RFID standards like EPC. As pointed out in [19], the deployment of NFC phones is still in the early stages, and thus tags and phones will continue to function as separate devices in the near future. Our proposal fills this gap by leveraging the universal vibration capability of mobile phones. As discussed in Section VI-C, a variation of our approach can also be used to provide NFC functionality to a non-NFC phone.

Other RFID security and privacy approaches, such as "blocker tags" [20] and RFID Guardian [21], require an auxiliary device. Similar to VtU, these two approaches can be embedded on a mobile phone. However, this would again require the mobile phone to have RFID functionality. Besides Secret Handshakes, accelerometers have previously been used to enhance security and privacy of ubiquitous devices [22] by performing activity recognition. Our proposal, in contrast, uses an accelerometer to achieve RFID device-to-device communication.

III. Vibrate-to-Unlock

A. Communication and Security Model

VtU utilizes a mobile phone M as an authentication token for a user to authenticate to a RFID device D. The core of our idea is to authenticate the user to D via M. Unlike a human user, mobile phones are not constrained in terms of memory and computational capabilities. They can thus form the basis of stronger authentication to multiple RFID devices. We abide by the "backward compatibility" property of [6] where RFID tags can be modified but readers can not be. We build a human-perceptible channel between M and D which the former can use to authenticate to the latter.

Authentication can therefore be achieved by transmitting a pre-shared PIN from M to D over this channel. Although M is used to store tag-specific PINs, it is not necessary to protect these secrets using user-to-phone authentication because the phone already provides a layer of protection. To access the service an RFID device provides, an adversary would need access to both the phone and the RFID device.

The adversaries can gain physical access to D and to M. Adversaries are not able to learn the stored PIN or secrets from D, though, because temporary physical access to D will not allow sufficient time for hardware tampering. We assume that M can be remotely compromised, in which case, adversaries can learn the PINs stored on M and force it to behave in an arbitrary manner. We consider the following attacks in our model: (1) *Privacy attack*: The adversary tries to query D to learn its tag specific information and track the owner of D (2) *Impersonation attack*: The adversary attempts to impersonate the owner of D either by cloning or gaining physical access to a tag (3) *Ghost-and-leech attack*: The adversary attempts to relay information surreptitiously read from D to another colluding adversary, who then transmits this information to a reader and vice versa. We do not consider denial of service attacks or malicious readers and eavesdropping attacks while the tag is being read by a legitimate in our model.

B. A Novel Vibrational Channel

We develop a novel authenticated human-perceptible channel that can be used to securely transmit a shared PIN from M to D. This is difficult because of the channel requirements and the RFID usage model. Audio and visual channels will require the RFID tag to have a microphone or light sensor; the latter also requires tags to be taken out from container, while the former does not work in a noisy environment. To remedy this, we focus on designing a tactile channel that utilizes the vibration capabilities of mobile phones. This is a promising direction since vibration is a universal interface on mobile phones. Our channel requires a phone with the capability to vibrate and an RFID tag equipped with an accelerometer. The phone's vibrations are used to encode data to be transmitted, such as a PIN. This can be achieved using an ON-OFF encoding. Users are required to touch their vibrating phone with a tag or its container. The accelerometer on the tag senses the vibrations and decodes the PIN. This channel is automated and therefore efficient. Its timing depends upon the type of accelerometer on the tag and its sensitivity to vibration. We discuss the design and implementation of this channel in Section IV. A one time registration of a shared secret PIN between a phone and a tag is achieved in the same manner as authentication; a phone picks a random PIN and transmits it to a tag over the vibrational channel.

Adversary has access to the phone and/or RFID tag? Attack is possible?				
Phone	RFID	Privacy	Impersonation	Ghost-and -Leech
No	No	No	No	No
Yes	No	No	No	No
No	Yes	**Yes** ($\leq q/2^p$)	**Yes** ($\leq q/2^p$)	**Yes** ($\leq q/2^p$)
Yes	Yes	**Yes**	**Yes**	**Yes**

Table I
POSSIBLE INTRUSION SCENARIOS

C. Role of the User in VtU Authentication

The role of a user in VtU authentication and registration is as follows. First, the user places the mobile phone in contact with the RFID device he or she intends to use. Both the tag and phone should be brought into the range of the RFID reader in order for the tag to receive power. In case the user carries multiple RFID devices, he or she needs to select the tag to authenticate to on the phone. Next, the phone vibrates in a pattern that encodes the PIN corresponding to the selected RFID device. The RFID device then reads the vibrations using the accelerometer, decodes the PIN, and compares with the value that was stored on it during registration. Finally, upon receiving the correct PIN, the RFID device unlocks and transmits its data to the RFID reader. If the PIN is invalid, the device remains locked. The resulting reader event indicates to the user whether the authentication attempt was successful.

D. Security Arguments

We discuss the security of VtU based on the model of Section III-A. We argue whether VtU provides protection against privacy attacks, impersonation attacks, and ghost-and-leech attacks. Assume that the length of the PIN shared between the phone and an RFID device is p bits; p is typically 4 decimal digits or 14 bits. Also assume that the user is only allowed q authentication attempts, typically $q = 3$. Once an adversary has physical access to an RFID device, its probability of succeeding in violating privacy, impersonating a user, or executing a ghost-and-leech attack is at most $q/2^p$. This is equivalent to the security provided by ATM authentication using a 4-digit PIN restricted to 3 trials. If the adversary has physical access to both the phone and RFID tag, he or she can succeed in all three attacks. Just phone access would not be sufficient, though, since the retrieved PINs are useless without the tags. Remotely compromising the phone would not be sufficient to execute these attacks either. Though an adversary could make a user's compromised phone encode a tag-specific PIN, the chances of the phone being in close proximity to the tag and the user being unaware of such vibrations is negligible.

Since VtU makes use of a unique vibrating pattern per tag, launching ghost-and-leech attacks would also not be possible in the case of remote phone compromise. Possible intrusion scenarios are summarized in Table I. An adversary may also

attempt to compromise the secrecy of the PIN transmitted over the vibration channel [4].

IV. Design and Implementation

Here we discuss the design and implementation of VtU on Intel's WISP tags [15]. VtU requires a mobile phone with an application that authenticates using PINs shared with RFID tags. The phone needs to have a vibration feature to encode the PIN. Each RFID tag also needs decoding software and an onboard accelerometer. In the prototype implementation of VtU, the phone software is based on the Java 2.0 Micro Edition platform and the tag side application is written in C++. In the following subsections, we describe VtU's encoding and decoding mechanisms.

A. Overview of the WISP Tag

Intel's WISPs are passively powered RFID tags compliant with the EPC protocol. We utilized WISP 2.0 hardware (Class 1 Gen 1 tag with Texas Instruments MSP430F1232 microcontroller) of the EPC standard. It features 16-bit MCU with 8 MHz clock rate, 8 kilobytes of flash memory, 256 bytes of RAM, and an analog to digital converter capable of sampling an onboard ADXL-330 three-axis, $\pm 3g$ accelerometer. WISPs are the first programmable passive RFID system. WISPs have previously been used in security application designs, including Secret Handshakes [6].

B. Encoding of PIN using Vibration

Due to the WISP's constraints, it can not quickly sample its accelerometer and can not store enough samples to detect different frequencies of vibrations. Thus, we developed a simple time interval based ON-OFF encoding scheme. We use a 4-digit PIN which is equivalent to 14 bits. Three additional bits, '110', are used as a "Start" sequence indicating the beginning of the transmission. Each '1'-bit is converted into a vibration of 200 ms and each '0'-bit is converted into 200 ms of stillness. To transmit a 4-digit PIN, a total of 17-bits of transmission are therefore required. Thus, we require a transmission time of 17×200 ms$= 3.4$ seconds.

C. Decoding of Vibration

1) WISP Programming for Vibration Decoding: Since the tag does not have its own power, it needs to be in proximity of the reader to run our algorithm. The microcontroller does not have any Digital Signal Processing features for performing fast computation. As the WISP tag has only 256 bytes of RAM, some of which is used by the RFID protocol stack, the amount of RAM available for the decoding application is limited. Due to this constraint, we also can not afford to store enough accelerometer samples required to run a Fast Fourier Transform to detect vibration. Instead, we implemented a circular queue based real-time processor for decoding. To understand the behavior of the accelerometer under different scenarios, we collected accelerometer data

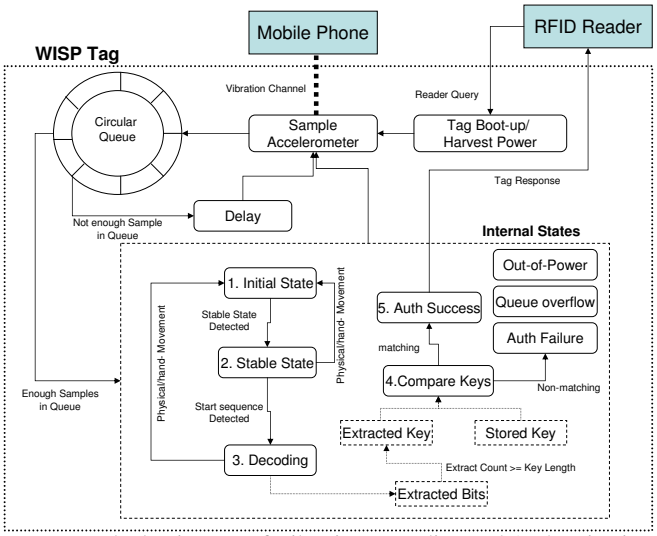
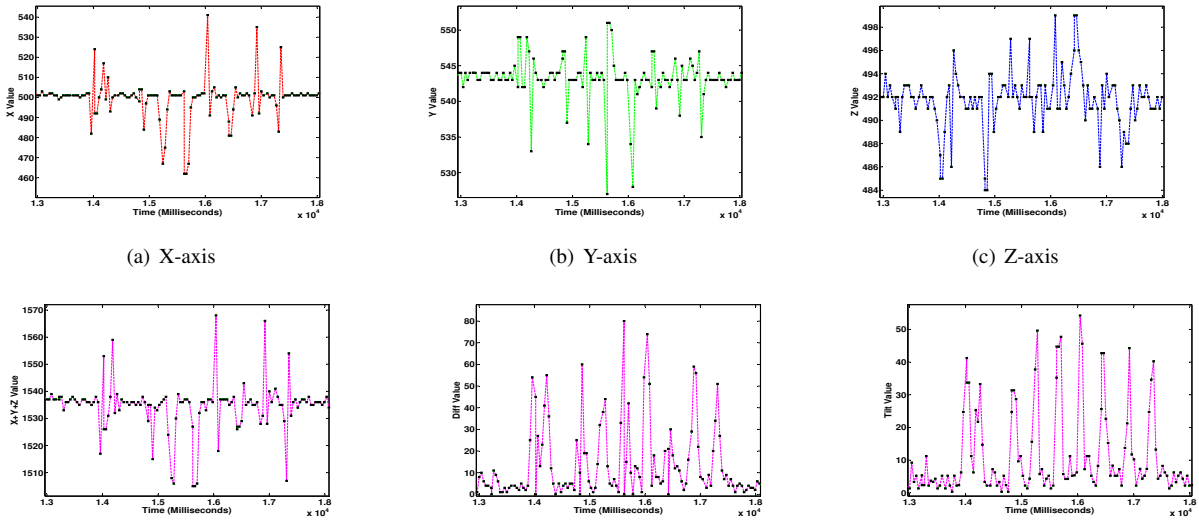


Figure 2. Block Diagram of Vibration Decoding and Authentication Algorithm on WISP Tag

through the RFID reader interface and plotted it to test for patterns. Figure 1 shows the Matlab plot of X, Y, Z, and functions "diff" and "tilt" (see Equations 1 and 3) of the accelerometer data collected on the computer via polling the tag through the RFID reader for the bit sequence "00011001010101010100", where bit '0' indicates no vibration and bit '1' indicates vibration.

We determined the criteria necessary to learn patterns from these plotted graphs. We then estimated the amplitude and count of samples for vibration, no vibration, physical, and hand movements conditions. We also determined what functions of the X, Y, and Z values were good metrics to identify these. Next, we analyzed how these metrics vary for all possible usage scenarios to determine threshold values and window sizes for distinguishing between the four aforementioned movements. We first designed our decoding algorithm on a traditional computer, then ported our decoding program to a WISP tag and adjusted the threshold values and window sizes on a trial-and-error basis to compensate for the higher sampling rate on the tag.

2) Decoding Algorithm: Figure 2 depicts a block diagram of VtU. When the tag receives a query, it boots up. Next, the tag's accelerometer starts listening for the correct vibration sequence. If it is received, i.e., the decoded vibration sequence matches the PIN stored on the tag, the tag transmits its response to the reader. The tag does not transmit anything otherwise. After recording an accelerometer sample, the tag places the sample in a circular queue. If the queue contains enough samples, it switches to one of the "Internal States" shown in Figure 2 and discussed below. If it does not, the tag waits and records another accelerometer sample after a certain delay. This delay is introduced in order to synchronize with the tag's accelerometer sampling rate. After executing the current state, the tag always tries to free up corresponding samples in the queue. The tag decides the



(a) X-axis (b) Y-axis (c) Z-axis

(d) X+Y+Z (e) Diff (as defined in Equation 1) (f) Tilt (as defined in Equation 3)

Figure 1. Plotted axis and function values of accelerometer data of tag, polled from computer through Alien reader interface for bit sequence '000110010101010101010100' (here, '0' encodes no-vibration and '1' encodes vibration)

next state based on its current state and switches back to recording another accelerometer sample. At the beginning of execution, state 1 is active. All five "Internal States" are shown in Figure 2 and described below.

1. Initial State: The tag remains in this state while it detects physical or hand movements until it reaches a stable state. Physical and hand movements are measured by taking the first derivative of consecutive samples as follows:

$$diff_i = a \times |X_i - X_{i+1}| + b \times |Y_i - Y_{i+1}| + c \times |Z_i - Z_{i+1}| \quad (1)$$

In this state, the tag always tries to detect a stable state where the forward differences of consecutive samples are below a predetermined threshold value for a threshold count of consecutive samples.

2. Stable State: In this state, the tag measures the current average ($\overline{S^s_{n+1}}$) of stable samples ($S^s_1, S^s_2, \cdots, S^s_n, S^s_{n+1}$) for each of X, Y and Z axes using the following formula:

$$\overline{S^s_{n+1}} = \frac{\overline{S^s_n} \times n}{n+1} + \frac{S^s_{n+1}}{n+1} \quad (2)$$

Here, $\overline{S^s_n}$ denotes the previous average and $\overline{S^s_1} = S^s_1$.

From this stable state, the tag checks for vibration, hand, or physical movements by measuring forward differences of incoming samples (using Equation 1) and matching for tilt. This is computed by comparing the incoming samples in the queue with current average of stable samples using the following equation:

$$\begin{aligned} tilt_i &= a \times tilt(X_i) + b \times tilt(Y_i) + c \times tilt(Z_i) \\ &= a \times |X_i - \overline{X^s_i}| + b \times |Y_i - \overline{Y^s_i}| + c \times |Z_i - \overline{Z^s_i}| \end{aligned} \quad (3)$$

Here, the stable state averages for each axis (i.e., $\overline{X^s_i}$, $\overline{Y^s_i}$, $\overline{Z^s_i}$) are calculated using Equation 2, tilt at i-th sample $tilt_i$ is calculated by taking equal proportionate components ofthe tilt in X, Y and Z-axis (i.e., $tilt(X_i)$, $tilt(Y_i)$ and $tilt(Z_i)$) and equal proportion coefficients a, b and c (for both of the Equations 1 and 3) are computed as follows:

$$a = \frac{max(\overline{VibTiltX}, \overline{VibTiltY}, \overline{VibTiltZ})}{\overline{VibTiltX}}$$

$$b = \frac{max(\overline{VibTiltX}, \overline{VibTiltY}, \overline{VibTiltZ})}{\overline{VibTiltY}}$$

$$c = \frac{max(\overline{VibTiltX}, \overline{VibTiltY}, \overline{VibTiltZ})}{\overline{VibTiltZ}}$$

Where

$$\overline{VibTiltX} = Mean(|X_i - \overline{X^s_i}|)$$

$$\overline{VibTiltY} = Mean(|Y_i - \overline{Y^s_i}|)$$

$$\overline{VibTiltZ} = Mean(|Z_i - \overline{Z^s_i}|)$$

$Mean(\ldots)$ is calculated using Equation 2 only on samples of the vibration event.

If the samples match the vibration thresholds and window sizes, the tag checks for the initial Start sequence. If it received the Start sequence, it moves to the decoding state, as explained next.

3. Decoding: The tag decodes the bits from samples matching with NO_VIB_TH and VIB_TH while matching the window sizes and current tilt of samples. The tag remains in this state until it detects all the bits in the PIN.

4. Key Comparison: If the tag extracts a number of bits equivalent to the PIN size, it compares the extracted PIN with the one it has stored. If the two match within some error tolerance, the tag authenticates the user. If the PINs do not match, the tag maintains a count of consecutive non-matching cases and locks itself after a certain number of consecutive authentication failures. We will discuss the error tolerance issue later in Section VI-A.

5. Authentication Successful: In this state, the tag authenticates the user and sends the response to the RFID reader along with other tag-specific information or executes a tag-to-reader authentication protocol.

1. What is your age?
2. What is your gender?
3. What is the highest level of education you have completed?
4. I have used a contact-based access or payment card.
5. I have used a contactless access or payment card.
6. Do you keep your access card in your wallet while trying to enter into the building or remove it?
7. I feel comfortable using computers.
8. I feel comfortable using cell phones.
9. The security of my cell phone is an important concern to me.
10. The security of my access cards is an important concern to me.
11. The privacy of my access cards is an important concern to me.
12. I keep my cell phone with me at all times.
13. The access process was easy to perform.
14. The access process was enjoyable.
15. The access process was professional.
16. The steps I had to follow to were intuitive.
17. The access process took a long time.
18. The access process was mentally difficult.
19. The access process was physically difficult.
20. I would like to use this access process occasionally.
21. I would like to use this access process every time I use an access card.
22. I would rather use this access process than use an access card normally.
23. My mobile phone is powered on and with me when I arrive at my workplace at the beginning of each day.
24. My mobile phone is powered on and with me when I am checking out at supermarket or grocery store.
25. My mobile phone is powered on and with me when I check in with an airline.
26. My mobile phone is powered on and with me when I board a bus, train, or other form of mass transit.

Figure 3. The Questionnaire

V. Experimentation and Usability Evaluation

A. Testing Framework

In our testing framework, users manipulated a phone with an affixed WISP. We avoided direct manipulation of the tag by users to minimize the potential to damage it. A piece of foam was inserted between the tag and phone to simulate the effect of storing an access card inside a wallet and touching it to a phone. This setup approximates a realistic RFID usage scenario for a access card closely enough. A Python script was developed to issue queries from the reader and log its responses. Minor changes were made to the WISP's behavior for testing purposes. Tags would usually not transmit until receiving the correct vibration pattern from the mobile device. The WISP's firmware was altered so it transmitted a "Start" value upon first receiving power. This allowed us to measure the timing of authentication. Instead of having the tag transmit its value upon receipt of a PIN, the WISP transmitted the decoded PIN value. This was done so that the value obtained by the tag could be recorded without attaching wires or cables to the WISP.

B. Test Participants and Questionnaires

20 participants evaluated our VtU prototype. They were drawn from people at our university campus and recruited through posters, email requests, sign up sheets, flyers, and word of mouth.

Age distribution of users was 18-24: 50%, 25-34: 20%, 35+: 30%. Half of the users were more than 24 years old. Half of the subjects were male. Among them, 55% were bachelor's, 30% master's, and 10% doctorates. 55% users keep their RFID access cards inside their wallets or purses.

In the post-condition survey there were two yes or no, four multiple choice, and twenty 5-point Likert scale questions. All queries were posed during a post-condition questionnaire rather than conducting a pre-condition survey to avoid security priming [13]. Figure 3 shows the precise questions that were posed.

The average 5-point likert responses were as follows – Q7: 4.8, Q8: 4.45, Q9: 4.35, Q10: 4.3 and Q11: 4.35.

Q12 and Q23 through Q26 concerned cell phone habits. Most users always had their mobile device with them (Q12: 3.75). Test participants have their mobile device ready when they arrive at work (Q23-Q24: 4.3 Avg). Participants have their cell phone available while boarding mass transit(Q25-Q26: 4.25 Avg). Positive responses to these questions provide evidence in the support of the assumption that the required use of a mobile device in our system does not hinder its practicality. Q13 – Q22 will be discussed in Section V-D.

C. Testing Process

Study participants followed a simple procedure. To start, the cell phone and WISP tag were placed beyond the range of the reader, which was set to query for tags. Users moved the phone and tag in front of one of the reader's antennas. Subjects then pressed a button on the phone that caused it to transmit its PIN over the vibration channel. When the expected number of bits had been decoded by the tag, the received PIN value was issued to the reader. This process was repeated a total of five times by each participant. Of these, the first attempt corresponded to one-time registration phase and the rest to authentication phases. After each user completed the main testing phase, they were presented with a final form containing the post-condition questionnaire.

D. Test Results, Analysis and Interpretation

All subjects completed one trial registration and four authentication attempts for a total of 20 registration cases, 80 authentication cases, and 100 test cases overall.

1) Errors: We did not encounter any errors caused by mobile device manipulation mistakes. Thus users have no difficulty performing the steps necessary to authenticate to an RFID tag via a vibratory channel. The only errors that occurred were due to the transmission between the mobile phone and WISP tag. While performing these 100 tests, 67% of the PINs were transmitted accurately, 28% were off by a single bit, and 5% were off by two bits. *No* test cases were incorrect in more than two bits. Any transmission channel will usually be subject to noise and our prototype was no exception. In order to mitigate this, tags can be programmed to accept one or two bit errors which would yield an *effective error rate of 0%*. While this would slightly reduce the provided level of security, it would still provide a measurable level in practice. Refer to Section VI for further robustness discussion.

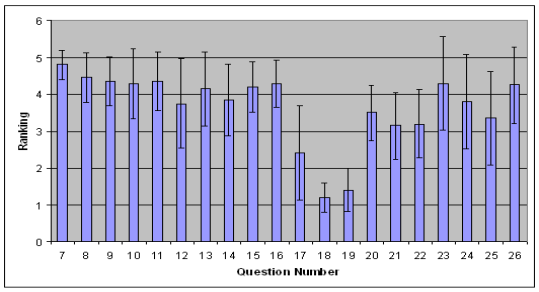


Figure 4. Mean and standard deviation of responses to post-condition Likert survey (questions 7 to 26)

2) Test Timing: The average time taken to complete authentication over all test cases was 8.01 seconds with a standard deviation of 1.12 seconds. Out of this, vibration transmission took 3.4 seconds and user manipulation was responsible for 4.6 seconds.

Between-Subjects Analysis: Based on unpaired t-tests at 95% confidence level, we found the following significant differences with respect to timing. Users in the 18-24 age group took less time than those belonging to 25-34 age group ($p = .040$). Test cases resulting in 2-bit errors took longer to execute than those resulting in 1-bit errors ($p = .015$) or no errors ($p = .040$). We did not find any significant effects of gender, education, or access card usage (that is, whether or not users kept their card inside a wallet) on timing.

3) User Feedback: Responses to our post-condition survey (Q7-Q26) are provided in Figure 4. Looking at the survey as a whole, average user responses agreed with positive statements and disagreed with negative ones. Q13 through Q16 were all positive statements and got average responses of 3.85 or higher, while the following three negative statements received average responses below 2.5. Users agreed that they would like to use this system some of the time or everyday. Responses were somewhat less positive for the final question implying replacement of standard access card usage with the our new scheme setup.

Observed Correlations: Pearson correlation coefficients between the average responses to the survey were calculated in order to find relevant linear dependencies. Many of the correlated responses that were uncovered were obvious. For example, respondents who reported that they would like to use VtU all the time (Q21) also said they would prefer to use it over normal usage (Q22) (ρ value of .853). Similarly, anyone who thought the access process was easy (Q13) also said it was not physically difficult (Q19) or lengthy (Q17), since these questions yielded ρ values of -.609 and -.508 respectively. There were few users who cared about their device's security but did not care about its privacy, as questions Q10 and Q11 demonstrated a ρ of .721. In general, subjects who gave positive responses to some questions were unlikely to provide negative replies to other positive questions, or positive responses to negative ones.

VI. Discussion

A. Speed and Robustness of VtU Prototype

The usability study results show that our VtU prototype takes 8 seconds on average to complete. The underlying vibration channel results in 28% 1-bit and 5% 2-bit errors, but none in more bits. In our case, these errors occur due to vibrations that confuse the accelerometer. Error detection and correction techniques can be used to solve this, but these techniques might not be viable on constrained devices and can also reduce the process's speed. An alternative is to accept all errors of 2 bits or less. This implies a 2-bit loss in security. A 14 bit PIN used in our method will provide a security equivalent to that of a 12 bit PIN instead with a *0% error rate*. If 12-bit security is not sufficient, a 16 bit PIN can be used to provide the original level of security at the cost of an additional 2-bits of transmission.

Now we compare the VtU technique with that of the Secret Handshakes method [6]. An accelerometer sampling rate of approximately 48Hz was used in [6] in order for the hand-movement to be recognized in a second. However, the length of the whole authentication process is unclear from [6]. Since no usability tests were reported in [6], user induced delays were not accounted for. Some users might take longer to perform the gestures. The results of [6] do not indicate any errors either. This is surprising because in practice, activity recognition is likely to be error prone. Since VtU is a real authentication method in contrast to Secret Handshake, comparing the two is perhaps not meaningful. VtU-Button, a variant where only the Start sequence is transmitted, provides the same level of security as Secret Handshakes. VtU-Button takes 600 ms without any user delays and thus compares favorably to the timing of [6].

B. "Fall-Back" Authentication

Fall-back authentication is a common solution to both dealing with unavailable phones that are used as authentication tokens and handling forgotten passwords. This can be achieved by personal questions [23]. However, this is not applicable to RFID tags due to their lack of interfaces. One possible solution is a tapping mechanism with which users can transmit a master PIN to a tag. An onboard tag button based on capacitive sensing would work as well [24]. Designing secure RFID fall-back authentication is an interesting future work item. We believe, however, that due to current mobile phone usage habits, fall-back use will be occasional. As stated in the New York Times, "In surveys of cell phone users, respondents say there are three things they always take with them when they leave home: *wallet*, *keys* and *cellphone*" [8].

C. Other Useful Applications and Variations

Wireless implantable medical devices (IMDs) are susceptible to a wide variety of serious attacks [25]. Halperin et al. suggest zero-power defenses where a passive RFID device

is attached to an IMD. When the RFID device receives a query, an audio transmitter integrated with the RFID tag beeps to alert its patient. A problem with this approach is that patients may not notice this beeping. VtU-Button is orthogonal to this approach. Here, IMDs remain in a locked state. When access to the IMD is needed, a patient or doctor can touch a vibrating device to patient's chest to unlock it. This addresses the previous proposal's drawback.

The authors of [26] demonstrated that the information transmitted by the Nike+iPod Sports Kit is subject to eavesdropping and user tracking even when the device is not in use. The sensor on it is equipped with a switch that turns it off. This is not accessible once the sensor is placed inside a shoe, however. VtU-Button can also address this issue. It would allow users to touch their vibrating phone to their shoe to selectively unlock the sensor during exercise. Further work is necessary to test for the effect of vibration dampening inside a shoe and this approach's usability.

Our basic design can also support another usage scenario which we call a "Relay Tag." Here tags do not store anything. Instead, they merely relay information, received from the phone over the vibration channel, to a reader. In this case, there is a single tag and the actual credentials used with the reader reside virtually on the phone.

This is a cheaper alternative to phones equipped with NFC functionality. The advantage provided by virtual credentials is their logistics savings. Virtual credentials can be provisioned and managed remotely. This combination of a phone and relay tag is limited in comparison with NFC-capable phones, however, as it is only a one-way channel with limited bandwidth.

VII. Conclusions

We proposed a novel approach for user authentication to multiple RFID tags called VtU. Our approach leverages a pervasive device, such as a personal mobile phone, that has become an inseparable part of most users' lives. It uses this mobile device as an authentication token, forming a unidirectional communication channel between the user and her RFID tags. Authenticating to an RFID tag involves a user simply touching the vibrating phone with the object carrying the tag. We discussed the design and implementation of our new authentication method on Intel's WISP tags. We also reported on our preliminary usability evaluation of the proposed method, the results of which indicate it to be reasonably efficient, robust, and user-friendly.

References

[1] A. Juels and D. Molnar and D. Wagner, "Security and Privacy Issues in E-passports," in *Security and Privacy for Emerging Areas in Communications Networks*, 2005.

[2] A. Juels, "RFID Security and Privacy: A Research Survey," in *Journal on Selected Areas in Communications*, 2006.

[3] Z. Kfir and A. Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard," in *Security and Privacy for Emerging Areas in Communications Networks*, 2005.

[4] T. Halevi and N. Saxena, "On Pairing Constrained Wireless Devices Based on Secrecy of Auxiliary Channels: The Case of Acoustic Eavesdropping," in *ACM Conference on Computer and Communications Security (CCS)*, 2010.

[5] G. Hancke, "Practical Attacks on Proximity Identification Systems," in *Symposium on Security and Privacy*, 2006.

[6] A. Czeskis and K. Koscher and J. Smith and T. Kohno, "RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications," in *Conference on Computer and Communications Security*, 2008.

[7] J. Nasar and P. Hecht and R. Wener, "'Call if You Have Trouble': Mobile Phones and Safety among College Students," in *International Journal of Urban and Regional Research*, 2007.

[8] S. Lohr, "As Cellphones Bulk Up, How Much Is Too Much?" in *New York Times*, Available at http://www.nytimes.com/2005/05/04/technology/techspecial/04lohr.html, 2005.

[9] Knowledge Networks, "New Study Shows Mobile Phones Merging New, Established Roles: Communicator, Shopping Aide, Entertainment and Research Hub," Available at http://www.knowledgenetworks.com/news/releases/2008/091808_mobilephones.html, 2008.

[10] R. Kim, "The World's a Cell-phone Stage," in *San Fransisco Chronicle*, Available at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/02/27/BUG2IHECTO1.DTL, 2006.

[11] T. Wikle, "America's Cellular Telephone Obsession: New Geographies of Personal Communication," in *Journal of American and Comparative Cultures*, 2001.

[12] B. Parno and C. Kuo and A. Perrig, "Phoolproof Phishing Prevention," in *Financial Cryptography*, 2006.

[13] S. Schechter and R. Dhamija and A. Ozmen and I. Fischer, "The Emperor's New Security Indicators," in *IEEE Symposium on Security and Privacy*, 2007.

[14] M. Mannan and P. van Oorschot, "Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer," in *Financial Cryptography*, 2007.

[15] J. Smith and A. Sample and P. Powledge and A. Mamishev and S. Roy, "A Wirelessly-Powered Platform for Sensing and Computation," in *Conference on Ubiquitous Computing*, 2006.

[16] SmartCode Corporation, "SMARTCODE Solves the Privacy Issue Relating to Potential Unauthorized Reading of RFID Enabled Passports and ID Cards," http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=1735, 2006.

[17] Mouser Electronics, "MMA7660FCR1 Freescale Semiconductor Board Mount Accelerometers," Available at http://www.mouser.com/search/ProductDetail.aspx?qs=uDmhV2jwPReFrqFV70kRUw==, 2009.

[18] M. Buettner and R. Prasad and M. Philipose and D. Wetherall, "Recognizing Daily Activities with RFID-Based Sensors," in *Conference on Ubiquitous Computing*, 2009.

[19] J. Sutter, "Wallet of the future? Your mobile phone," Available at http://www.cnn.com/2009/TECH/08/13/cell.phone.wallet/index.html?eref=igoogle_cnn, 2009.

[20] A. Juels and R. Rivest and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," in *Conference on Computer and Communications Security*, 2003.

[21] M. Rieback and B. Crispo and A. Tanenbaum, "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management," in *Australasian Conference on Information Security and Privacy*, 2005.

[22] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," in *Pervasive*, 2007.

[23] A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook," in *Symposium on Usable Privacy and Security*, 2008.

[24] A. Sample and D. Yeager and J. Smith, "A Capacitive Touch Interface for Passive RFID Tags," in *Conference on RFID*, 2009.

[25] D. Halperin and T. Heydt-Benjamin and B. Ransford and S. Clark and B. Defend and W. Morgan and K. Fu and T. Kohno and W. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in *Symposium on Security and Privacy*, 2008.

[26] T. Saponas and J. Lester and C. Hartung and S. Agarwal and T. Kohno, "Devices That Tell On You: Privacy Trends in Consumer Ubiquitous Computing," in *USENIX Security Symposium*, 2007.