Decision Support Systems 102 (2017) 12–21

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Lightweight non-distance-bounding means to address RFID relay attacks

Yuju Tu[a], Selwyn Piramuthu[b,*]

[a]Management Information Systems, National Chengchi University, Taipei, Taiwan
[b]Information Systems and Operations Management, University of Florida, USA

ARTICLE INFO

Article history:
Received 31 January 2017
Received in revised form 28 May 2017
Accepted 29 June 2017
Available online 3 July 2017

Keywords:
RFID
Relay attacks
Non-distance-bounding
Authentication

ABSTRACT

A relay attack is accomplished by simply relaying messages between a prover (e.g., an RFID tag) and a verifier (e.g., an RFID reader) with the goal of convincing the verifier of its close physical proximity to the prover. In almost all relay attack scenarios, the verifier essentially communicates with a prover that is outside the verifier's read-range. Relay attacks are notorious since they occur without the knowledge of the reader and/or tag, and has the potential to cause damage to honest parties (here, RFID reader and/or tag). Almost all means to address relay attacks in RFID systems to date are based on the proximity check idea that involves the measurement of message round trip times between tag and reader. With the speed of light at play, such measurements need not necessarily be accurate and could result in the false assumption of relay attack absence. Our review of published literature on approaches that use non-distance-based means to address relay attacks revealed ambient conditions' potential. We critically evaluate ambient conditions and develop a lightweight mutual authentication protocol that is based on magnetometer readings to address relay attacks.

1. Introduction

As RFID (Radio-Frequency IDentification) tags [6,7] gain widespread adoption and use in several application areas, it is essential to ensure that the security and privacy requirements of the tagged items are satisfied. For example, with RFID-based Passive Keyless Entry and Start (PKES), the key is no longer required to be physically inserted to unlock or start the vehicle. The only requirement is that the physical key is present in or near the vehicle, and there is no need to manually retrieve the key from one's pocket or bag since automated wireless verification seamlessly takes place through an RFID-based mutual authentication mechanism. While this is convenient, wireless authentication opens up the possibility for security threats in the form of relay attacks. As recently reported, it is possible to break into a PKES-enabled vehicle without any need for identity theft or decryption even while the vehicle's key is physically far away from the vehicle [5,17]. Similarly, when an RFID-enabled credit card is used to pay through wireless means, someone nearby can relay this information to make payments elsewhere [15,18,19,29]. Also, although biometric passports are protected through the use of encryption, the identities in those passports can possibly be wirelessly relayed to facilitate entry through automated border control systems. RFID-enabled voting mechanism leaves the possibility of a similar vulnerability [2,26,27,36,43].

A good example of relay attack in another domain is the chess grandmaster problem in which a novice simultaneously plays chess with two grandmasters by playing each move of one grandmaster with that of the other grandmaster [10]. The setup is such that each of the grandmasters is led to believe that they are playing against the (same) novice and not against each other [4]. A recent example occurred during the 2010 chess olympiad where Sébastien Feller was found to have obtained outside help during the games [16].

These (relay) attacks should not be mistaken for classical identity theft. In an RFID system, identity theft necessarily results in an RFID tag successfully impersonating another RFID tag's identity to the reader. A common means to counter identity theft involves prevention of cloning or the copying of identity token or password by unintended parties, whereas such measures do not have any effect on the types of (relay) attacks encountered in these scenarios. For example, banks in some countries commonly use one-time passwords as tokens to verify the identity associated with each transaction. These passwords are designed such that their validity lasts only for a short time duration (e.g., 3 min), which is enough to thwart

* Corresponding author.
E-mail address: selwyn@ufl.edu (S. Piramuthu).

http://dx.doi.org/10.1016/j.dss.2017.06.008
0167-9236/

most identity theft attempts. In the case of relay attack, an adversary can prompt for the generation of a new one-time password and relay the conversation without the knowledge of the owner of the compromised account. Relay attack is entirely different from identity theft, and requires far less resource to accomplish.

Relay attacks do not depend on message decryption or the physical separation between reader and tag. These attacks operate by relaying messages between (honest or dishonest) tag and a honest reader where the reader and tag always believe that they are communicating with an honest tag and reader respectively. Relay attacks are among the most severe attacks that are faced by contactless smart cards (e.g., in mobile payment applications), and are relatively easy to accomplish since there is no need to understand or decrypt any of the messages. Given this, it is not trivial to address relay attacks through cryptographic means.

However, one of the common means to address issues that are associated with relay attacks is through the use of cryptography, specifically with the encryption of messages that are passed between tags and readers. Since wireless medium is used to pass messages between tags and readers in almost all of these applications, it is difficult to safeguard these messages from being intercepted, read, and/or modified by unintended parties. Therefore, an important role of encryption in these communications is to ensure that secrets are not unintentionally revealed through these messages. It is also important to prevent adversaries from successfully impersonating tags to readers and vice versa based on passed messages between tag and reader.

RFID cryptography is a very active area of research. Dozens of protocols for various configurations (e.g., single-tag/single-reader, multi-tag/single-reader) have been proposed that address security/privacy vulnerabilities [28,39]. Almost all of these protocols rely on message encryption to ensure that even a resourceful adversary would be unable to determine secrets through capture and analysis of any/all messages that are passed between any given reader/tag combination. Typical passive RFID tag communication range is within 10 cm for high-frequency tags and up to about 10 m for ultra high-frequency tags. A majority of RFID authentication protocols implicitly assume that the reader and tag are in close physical proximity of each other since they can communicate with each other only when the tag is in the field of the reader. However, unless the authentication protocols are specifically developed for protection against relay attacks, they are almost certainly vulnerable to such attacks.

Relay attacks come in a few different flavors that include mafia fraud and terrorist fraud. Mafia fraud is where an adversary successfully relays messages between an honest reader and an honest tag [14]. An example of mafia fraud is the use of relayed messages to open a building door using a smart card that is not in close physical proximity to the reader at the door. Terrorist fraud occurs when the tag is dishonest and colludes with the adversary to misrepresent its physical location [13].

Based on the proximity check idea [4], Brands and Chaum [8] proposed a protocol to address mafia fraud. The essence of this protocol is the measurement by the verifier of round trip times taken by 1-bit messages between prover and verifier. Hancke [23] illustrated mafia attack with an RFID tag and reader from a distance of 50 m, and Hancke and Kuhn [24] then developed a distance-bounding protocol based on proximity check for RFID applications. Distance-bounding protocols have since then been implemented in commercially available RFID tags (e.g., MIFARE Plus from NXP).

A core of distance-bounding protocols is their reliance on the relationship between distance and signal travel time. Since signal takes more time to travel farther, an unusual delay could signal the possibility of a relay attack. However, with the speed of light, accuracy is measured in terms of nanoseconds when the distance is in meters. The distance-bounding protocols therefore depend on the accuracy of the clock on the reader-side. To ensure that a tag is just meters away from the reader, the clock needs to have accuracy at nanosecond scale. While this may not necessarily be an issue (e.g., commonly used GPS clocks have accuracies in nanoseconds), the turn-around time at the tag-side might be an issue. In other words, if the turn-around time is in terms of microseconds for whatever reason, it might be difficult to distinguish reader-tag separations that are kilometers apart from those that are just a few meters apart. This necessitates the exploration of other (i.e., non-distance-bounding-based) options to address relay attacks. From our survey of existing literature on RFID relay attacks, it was clear that almost all existing protocols use some distance-bounding variant. To address this void, we consider other possible (e.g., ambient conditions) avenues to approach and address relay attacks.

To this end, we critically examine several possible facets of ambient conditions from the perspective of relay attacks and choose magnetometer readings to determine the tagged item's location and develop a mutual authentication protocol that is secure against relay attacks. Our approach has several merits. First, we avoid the limitations with respect to round-trip distance measurement as in existing distance-bounding protocols. Second, our approach is generalizable across various RFID applications since it is neither sensitive to the tagged item's movement nor restricted to the orientation of the tagged item with respect to reader. Third, it is economically feasible since it relies on already available battery-less passive tag technology that is in accordance with EPC Gen-2 standard.

The contribution of this paper is two-fold: (1) we consider non-distance-bounding alternatives to address relay attacks through detailed evaluation of possible alternatives, and (2) we develop a lightweight authentication protocol with the incorporation of magnetometer readings that is secure against relay attacks. Although we use magnetometer readings in the proposed mutual authentication protocol, the protocol itself is not specific to magnetometer sensors in that any sensor reading can be used as long as the ambient condition measured satisfies basic requirements (e.g., non-directional) for such applications.

The remainder of this paper is organized as follows: We briefly review distance-bounding approaches against relay attacks in the next section. In Section 3, we consider several possible non-distance-bounding options that include both the use of ambient conditions and others where it is possible to use battery-less RFID tags. We then present the proposed protocol and its security analysis in Section 4. We conclude the paper in Section 5 with a discussion on non-distance bounding approach to address relay attack with a specific focus on the proposed protocol.

2. Distance-bounding approaches against relay attacks

Relay attack becomes an issue when close physical proximity of RFID tag and reader cannot be confirmed with certainty. It is not difficult to envision adversaries positioned between tag and reader to relay messages between them when they are physically farther apart and are oblivious to relay attack as it happens.

Distance-bounding approaches to address relay attacks operate with the premise that the distance between two entities (here, RFID tag and reader) can be precisely measured through the round-trip time taken by single bit messages to pass between these entities. While this may be valid under ideal conditions where there is no unintended delay anywhere, it may not necessarily be true in reality. A small delay in (microseconds, for example) turn-around time at the tag side can easily wash out differences in distances of miles vs. meters. The tag needs to receive the bit, decide what to do with it, and then return the bit to the reader. This involves *computation time* that can easily overshadow the *communication time* between tag and reader.

We use the following notations throughout the remainder of this paper:

- T: Tag
- R: Reader
- ||: Concatenation operator
- $\oplus$: Exclusive-OR (XOR) operator
- $wt_H(A)$: Hamming weight of vector A
- $rot(A,\rho)$: Function to rotate entries in vector A by ρ places
- u, v, w, TM, RM: k-bit temporary vectors
- r_R: random k-bit nonce generated by the reader
- r_T: random k-bit nonce generated by the tag
- h: keyed hash function
- x, y, z: tag's k-bit shared secret with the reader
- T_R: tag temperature as measured by the reader
- T_T: tag temperature as measured by the tag
- T_{mag}: The k-bit measured magnetic field by tag
- R_{mag}: The k-bit measured magnetic field by reader
- Δ_{mag}: Allowed tolerance level for difference in detected magnetic fields
- $T_{mag*}^{i\in 1..m}$: A set of m optional T_{mag} generated by reader on the basis of $R_{mag} \pm \Delta_{mag}$
- N_t: k-bit noise generated by tag with a random mix of $\frac{k}{2}$ bits $=$ 1 and $\frac{k}{2}$ bits $= 0$
- N_r: k-bit noise generated by reader with a random mix of $\frac{k}{2}$ bits $= 1$ and $\frac{k}{2}$ bits $= 0$
- $A \approx B$: signifies $wt_H(A \oplus B) = 0.5k$, where $k = length(A) = length(B)$
- P_R, P_T: Public key of the reader and tag respectively
- s_R, s_T: Private key of the reader and tag respectively
- Q: the generator of a cyclic subgroup of points on the elliptic curve for the reader and tag
- ϵ: allowed tolerance for temperature difference between reader and tag measurements
- $f_a(b)$: encrypted value of b with key a and pseudorandom function f; $f: \{0,1\}^* \rightarrow \{0,1\}^{2k}$
- L, R: the left and right parts, k bits each, respectively of the encrypted value
- t_i^s, t_i^f: start and finish times, respectively, of fast bit iteration i
- $\Delta t_{\max}$: maximum allowed round-trip time

To understand the essentials of distance-bounding protocols, we now discuss the core of the earliest RFID-based distance-bounding protocol that was proposed by Hancke and Kuhn as illustrated in Fig. 1. This protocol comprises two phases, with an un-timed first phase and a timed second phase [24]. The reader has the clock. The first phase is used to generate $R^0 \parallel R^1$. During each iteration of the timed phase, either R^0 or R^1 is chosen at random and a bit from its $(i-1)$th position is sent to the tag during the ith iteration. At the end, (a) each of the n round trip times are checked to ensure that it is at most a pre-defined value ($\Delta t_{\max}$) and (b) the R (R^0 or R^1) values are valid. When either of these tests fails, it signifies the presence of a relay attack, and the protocol is aborted.

Since the first phase is not timed, an adversary can capture and hold r_R thereby prolonging the un-timed phase, and repeatedly send a fixed (say, 0) value to the tag during its timed phase and gather all its responses. Then when the reader is ready, upon reception of r_T from the adversary, the adversary can impersonate the tag and respond with the R values it captured from the tag. This would only ensure that the adversary is correct in at least half its responses to the reader during the timed phase. For the other half of the time, the adversary can correctly guess 50% of the time on average. This results in an accuracy probability of $\left(\frac{3}{4}\right)^n$ in a mafia fraud scenario. However, this protocol is vulnerable to a terrorist fraud attack where a dishonest tag colludes by sharing $R^0 \parallel R^1$ with the adversary and successfully fakes its distance from the reader. Reid et al. developed a modified protocol in which the (dishonest) tag is forced to not share anything with the adversary since that would involve revelation of its secret information to the adversary [42]. This modified protocol too has its issues, as discussed in [38]. A majority of RFID-based distance-bounding protocols that claim to be resistant to relay attacks include timed one-bit exchanges between tag and reader as their main component to ensure that the distance traveled by the

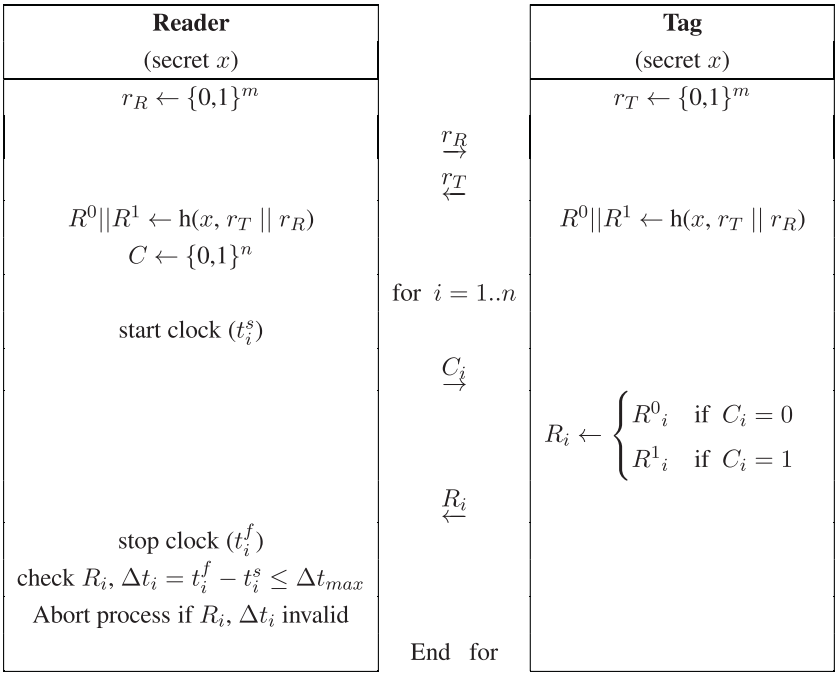

Fig. 1. The distance-bounding protocol of Hancke and Kuhn [24].

messages reflect the claimed distance between tag and reader. The timed messages are intentionally kept at one bit length to (a) stay in compliance with the goal to keep the computational overhead at the tag side to a minimum and (b) to facilitate measurement of round-trip times as the primary focus with the elimination or reduction of other activities that involve time.

Several minor variations of the distance-bounding protocol with both timed and un-timed phases have been proposed over the years. These protocols include modifications to the outer loop [48], the use of mixed challenges [30], response pre-computation [33], among others. There have also been attempts at measuring round-trip times without the use of single-bit exchanges such as the one in Rasmussen and Čapkun, which was later shown to be vulnerable to mafia fraud attack [34,41].

3. Non-distance-bounding approaches against relay attacks

With the dominance of distance-bounding approaches for RFID relay attacks, it is no surprise that there is a paucity of published research that consider means other than distance-bounding ones. We now consider a few approaches that do not include a distance-bounding component to address relay attacks. Other than distance-bounding approaches, published literature on RFID-based relay attacks include those that are based on system noise, ambient conditions, posture recognition, and location awareness.

3.1. System noise

Hamida et al. use two calibration coil antennas at the reader and card side to develop a means to detect noise due to statistic variations when a relaying communication occurs in an amplifier and forwards relay attacks. Their means is featured with the use of physical layer characteristics. They show through experiments that when relay attacks occur in the far-field channel, the presence of an adversary may impact the noise level in that channel. In other words, they argue that the occurrence of relay attacks must be positively associated with the increase of noise change in communication. However, their method relies on setting up a judgmental threshold in order to determine whether there is a significant increase in noise change variance [22,44,45].

3.2. Ambient conditions

Ambient conditions comprise several different facets that include temperature, humidity, pressure, light intensity, sound, among others. To our knowledge, there are about a handful of published research that either directly or tangentially discuss the use of ambient conditions to address RFID relay attacks. We therefore do not limit our discussion to just these papers and instead critically consider several ambient conditions from the perspective of relay attacks in order to evaluate all feasible options with specific emphasis on available RFID-based sensors.

The core idea with the use of ambient conditions to thwart relay attacks is fundamentally different from that of distance-bounds, although they all share the common goal of identification of relay attacks when they occur. Whereas the physical proximity of RFID tag and reader is verified through one-bit signal transmission time in the distance-bounding protocols, the premise in the approaches that use ambient conditions is that the RFID tag and reader are bound to experience the same ambient conditions when they are in close physical proximity to each other [11,21,37,46].

Technology advances during the past several years have resulted in improvements in wireless sensors, specifically with respect to their footprint and data transmission capabilities. With their widespread adoption and use, unit sensor cost has come down as well. Their applications span a wide range that include livestock habit monitoring to manufacturing process fault detection. It was also the case that since passive RFID tags do not have access to a power source, the use of associated sensors was beyond question. Recent years have witnessed breakthroughs in this regard as well. For example, we now have WISP (Wireless Identification and Sensing Platform) RFID tags that are essentially battery-free RFID tags with sensing capability at very reasonable cost [37]. Several researchers have considered the use of WISP tags to address relay attacks.

Halevi et al. illustrate the possibilities of using on-board sound and light sensors for countering relay attack with the use of two (Nokia N97) mobile phones with NFC capability [21]. They experimentally verify sound and light readings without their incorporation in an associated authentication protocol. The reasoning here is that when the two phones are next to each other, they both most likely experience the same light and sound conditions. While this premise is generally true, the fact is that both light and sound waves are directional and the relative orientation of the detection mechanism can affect what is measured. Unless the RFID tag and reader are in close physical proximity with the same orientation and experience no reflection or other effects, it is difficult to ensure that the (sound or light) readings from reader and tag would be the same or even similar.

Another ambient condition that has been considered in published research on relay attacks is temperature. Urien and Piramuthu consider the use of temperature sensor-enabled WISP RFID tags [49]. As with the use of other ambient conditions, measured temperature by the on-board sensor of an RFID tag would be very similar to that of its reader, if the tag and reader are in close enough physical proximity to each other. Moreover, the observed tag temperature is very difficult to be modified to that of the reader if the tag is far away from the reader. With this consideration, they propose a mutual authentication protocol (Fig. 2) that uses both the surface temperature of the tag as measured by itself as well as the reader and a distance-bounding measure with the use of one-bit messages. In that sense, this authentication protocol is not based purely on ambient condition measurements since it also uses the distance-bounding measure.

Urien and Piramuthu [49] use elliptic-curve cryptography to avoid the key distribution problem. In addition, they use surface temperature measurements of RFID tag by both the tag itself and by the reader (T_T and T_R). They assume that when an RFID reader senses a tag somewhere outside, it is able to scan the surface temperature of the tag. Next, the reader will send the temperature to the tag (T_R). Similarly, the tag will also scan the temperature on its own and send it to the reader. Thus, they can check with each other on their temperature measurements as a proxy to determine their distance from each other. Ideally, the temperature readings should be very similar, since the RFID tag and reader are physically located close to each other. In other words, if the readings differ within a specific tolerance level (ϵ), the protocol would allow the authentication process to continue. In their experiments, they use infrared temperature scanners. The results show that 27.84(0.24)°C and 30.83(0.08)°C are the average (standard deviation) tag temperature measurements from a smartcard after it was removed from a wallet on the chip area and the plastic area respectively. 35.23(0.34)°C was the temperature measurement of a smartcard that is in a wallet inside a pant pocket. Moreover, such temperature differences are all statistically significant ($p < 0.01$) according to pair-wise t-test for samples with unequal variances.

Although not related to relay attack, Piramuthu and Doss [40] consider the use of temperature sensors to confirm the close physical proximity and simultaneous presence of two RFID tags in the field of the reader. After considering a few different ambient condition measures such as light, pressure, and sound, they chose temperature as the ambient condition of interest for this application due to its non-directional property.

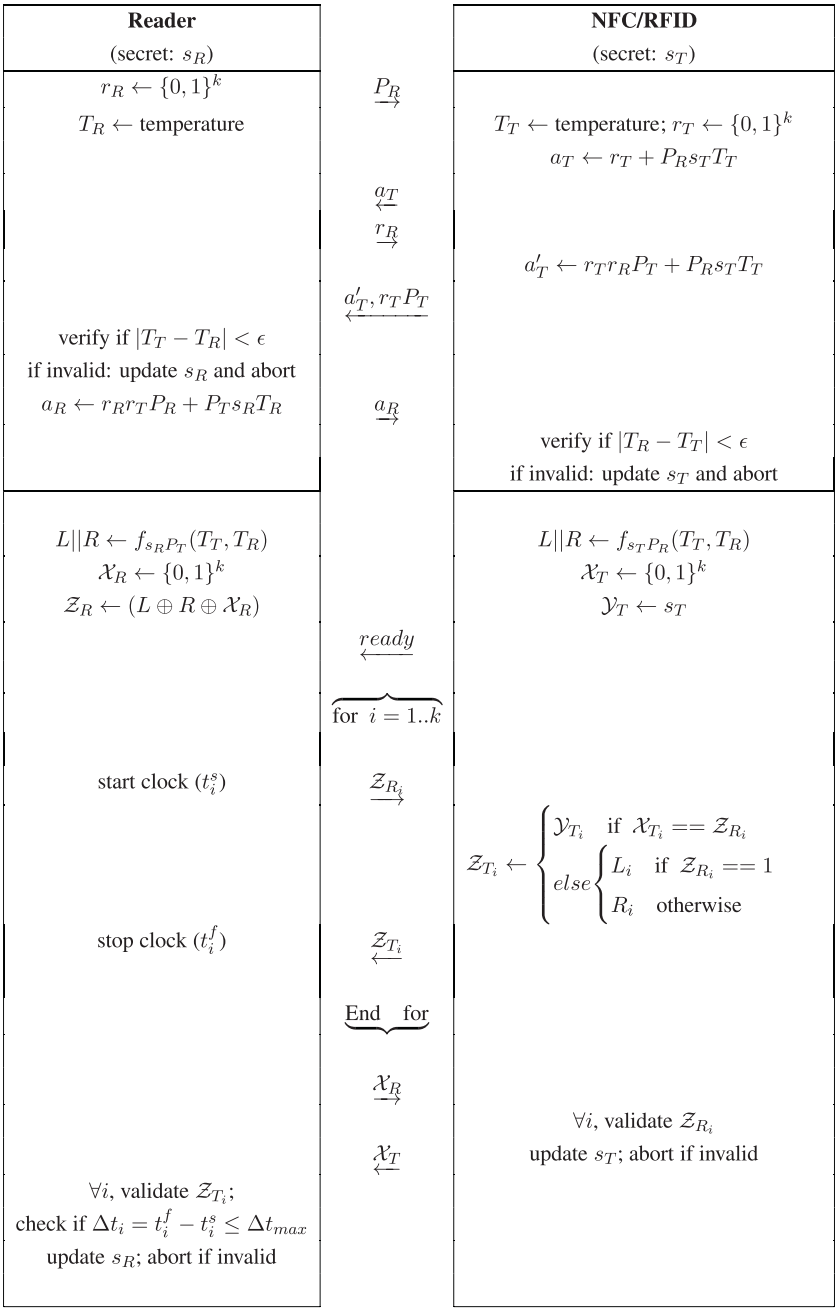

Fig. 2. Temperature use to address relay attacks Urien and Piramuthu [49].

Among the different ambient conditions that have been discussed in the literature with respect to RFID authentication and related relay attacks, temperature stands out in terms of its non-directionality property. However, temperature may not be suitable for use to thwart relay attacks under all circumstances. For example, it is possible for the tag temperature to be close to that of its reader's ambient temperature during a relay attack even though the tag and reader are miles apart. A worse scenario is where the tag temperature is markedly different from the ambient temperature, with the reader unable to measure the tag's surface temperature even though they are in close physical proximity of each other. For example, an RFID-based authentication in a PKES car key might fail if it's based on temperature since it is possible for a tag that's inside the pocket of the driver to have a tag surface temperature that is close to the person's body temperature which may be significantly different from that of the ambient car temperature.

What has not been discussed in existing literature on RFID authentication is the use of the earth's magnetic field to determine the absolute orientation at any RFID tag's location. A magnetometer can be used to measure the magnetic field at any given location which can then be used to verify the location of the tagged entity. Magnetic field measurement has been shown to be a reliable means for location determination (e.g., [47]). To our knowledge, none of the published literature on RFID relay attacks consider the use of magnetometer for this purpose. RFID tags with magnetometer have been commercially available at least since 2013 when Farsens

introduced Magneto, a battery-less magnetometer tag that can be used to measure and transmit magnetic field measurement data to an EPC C1G2 reader.

3.3. Posture recognition

Other than ambient conditions, personal patterns can also be used against relay attack. For example, Halevi et al. [20] present a posture-sensing approach. They use magnetometer and accelerometer readings to determine posture and to unlock the WISP RFID tag only when a pre-determined posture is identified. The premise of their approach is that the tag owner's posture can be used in a valid context where RFID tag is truly near reader. For instance, in a possible use of posture recognition to start a car with a variant of PKES (Passive Keyless Entry and Start system), the driver is assumed to be in a pre-defined posture while sitting on the car seat. Thus, their approach verifies the proximity of RFID tag to RFID reader by profiling the patterns of the tag owner's posture. The patterns used here include the postures at real-time and those that are recorded for that person sitting in that car. Thus, if the patterns are matched, the tag would be switched on for communication with the reader. If the patterns do not match, the tag would remain switched off. In other words, the mechanism needs additional training sessions. During the training sessions, the mechanism profiles the owner's postures, such as that with respect to the owner's accessories (e.g., pocket and wallet) and then elicit their patterns. As a result, if the owner changes the patterns when using the tag, the owner needs to go through a new training session to make necessary updates. The results presented in Halevi et al. show that the mechanism is promising. However, they stop with their provision of evidence through experimental data, and do not take a step further to develop an authentication protocol that incorporates this functionality. The average success rate of their mechanism remained acceptable, even in scenarios where owner's postures varied during their experiments. An issue with posture recognition to authenticate driver is the possibility of a high percentage of false positives due to the limited space between the driver's seat and the steering wheel that allows for a rather limited set of posture variants and related calibration challenges.

3.4. Location awareness

A related idea is the use of location-awareness where the physical location of the tag and reader are compared to determine whether they are in close physical proximity to each other. For example, Ma et al. [32] show that the implementation of GPS function in an RFID tag to counter relay attack is feasible. They use a low cost external GPS sensor that is attached to a WISP tag to operationalize their experiment with fixed reader locations. The reader locations are stored in the RFID tag, which gets unlocked and is ready for communication with readers only when it senses that it's in one of the (stored) reader's locations. They show that this setup works reasonably well when the tag is 2, 3, and 5 m from the reader as well as when the tag is mobile at 15, 25, and 35 miles per hour. The GPS sensor they use has an update rate of once per second. They do not take the next step to show that this could be incorporated in a protocol that automatically accomplishes what they show in multiple manual steps. Some of the challenges with this setup include (a) WISP RFID tag memory, which is about 8KB to enable storage of a reasonable number of reader locations, (b) its applicability when the reader is mobile, (c) the ease with which the tag's GPS measurements is messed with, including issues related with penetration of GPS signals in buildings or thick foliage cover, and (d) form factor, since the GPS sensor that they use is large and inflexible.

3.5. Discussion

In sum, the non-distance-based approaches we discussed largely hinges on the quality of sensor data and the appropriateness of the ambient condition for this purpose. According to existing literature, sensor data readings of high quality often have the potential to provide differentiable readings across various locations and orientations that include indoor locations and non-directional setups.

Conventionally, if a sensor measurement of an ambient condition is directional, the quality of that sensor data would be low. For example, although GPS is widely used, the quality of GPS data is rather poor because of various issues. Based on that perspective, the use of temperature is justified since temperature is non-directional. Thus, the quality of temperature sensor data is often higher for applications that involve proximity determination, because the sensor is capable of providing consistent readings regardless of relative tag and reader orientations. However, there are some issues with temperature since the tag temperature may be different from that of its environment and may not necessarily be accurately measured by a reader. This may not necessarily be an issue if only the self-reported (i.e., tag reporting its own temperature and the use of this in the authentication protocol) values are used. However, this will not work if the tag is not visible to the reader as required by an authentication protocol (e.g., [49]).

When properly calibrated, magnetometer measurements can be reliably used to determine proximity of tag to reader. Table 1 summarizes the profile of the ambient conditions/sensors that are possible candidates for addressing relay attacks. We could not find a reference for the use of pressure for this purpose in existing literature. Since there could be other facets of ambient conditions that are better candidates to address relay attacks, the set of ambient conditions considered here is not meant to be complete. However, we are not aware of any other obvious ambient condition candidates.

We experimentally evaluated the sensors mentioned in Table 1, except for GPS and posture sensors since it was not possible for us to obtain usable readings from GPS sensors inside a building and posture sensor use in the original study [20] was for a specific application (automobile driver seat) only. We used results from Piramuthu and Doss [40] (Table 2) for all but the magnetometer reading values since the purpose is to measure those readings from two objects that are in close physical proximity of each other. These measurements were obtained with two physically close tags. Each of the entries in the second and third columns in Table 2 were the

Table 1
Profile of context-awareness sensors.

Type	Strength	Weakness	Literature
GPS	Convenient	Outdoor use only; easy to jam, spoof, disable	[3,9,12,32,37]
Posture	Ease of use	Directional; calibration challenges	[11,20,46]
Pressure	Convenient	Easy to replicate, minor variation across short distances	
Temperature	Not directional	Measurement when tag not in reader's line-of-sight	[21,49]
Light	Hard to replicate	Directional	[20,40]
Sound	Hard to replicate	Directional	[20,40]
Magnetic field	Not directional	Variations due to ferromagnetic interference	[1,47]

Table 2
Ambient condition readings from two sensor-based tags T_1 and T_2 in close physical proximity.

Ambient sensor	T_1 mean(StDev.)	T_2 mean(StDev.)	p-Value (paired two-tailed t-test)
Light (cd/m^2)	8636.33(1514.12)	11,879.67(671.88)	$\ll 0.0001$
Pressure (mm HG)	30.459(0.0019)	30.458(0.0017)	0.317
Sound (dB)	93.33(3.23)	101.267(3.237)	$\ll 0.0001$
Temperature (F)	81.7067(0.3383)	81.6567(0.352)	0.5581
Magnetic declination (milliradians)	111.72(0.087)	111.74(0.067)	0.2431

result of 30 readings. Statistical significance of the differences in the mean values of these pairs of measurements are given in the last column. Based on the statistical significance values, it is clear that measured light and sound values were significantly different for the two tags due to the directionality property of light and sound. The pressure measurement at the two tags were not significantly different. Nevertheless, pressure measurements are not useful for our purpose since it reflects the elevation at the measured location, and elevation doesn't vary over significant distances in most areas. Given its non-directional property, the difference in measured temperature values at the two tags were not statistically significant. The differences in magnetometer declination readings were also not statistically significant. Based on the characteristics of the different sensors discussed above as well as their appropriateness for incorporation in a mutual authentication protocol that also addresses relay attack issues, we decided on the use of magnetometer readings in our proposed protocol. Please note that the protocol itself is generic in the sense that it is sensor-agnostic.

4. Proposed mutual authentication protocol

To circumvent issues associated with distance-bounding through round-trip time measurements, we develop a mutual authentication protocol that does not depend on round-trip distance measurement. The protocol also satisfies the following properties: (a) its functionality must not be sensitive to tag movement within the field of the reader, (b) it should not need human input during authentication, (c) all, if any, sensor measured quantities must be independent of directionality at that location, (d) the sensor should be readily available for any passive (i.e., battery-less) tag in accordance with either EPC Gen-2 or WISP standards, and (e) the protocol must be lightweight. We first present and discuss the protocol and then present its security analysis.

4.1. Relay attack-resistant mutual authentication protocol

The proposed mutual authentication protocol is given in Fig. 3. We use readings from magnetometer-enabled RFID tags and reader to operationalize this protocol. Specifically, the core of the protocol is the fact that the two magnetometer readings (i.e., the ones taken by tag and reader) are bound to be the same or very similar when such measurements are taken in close physical proximity of each other. An adversary cannot successfully relay messages between a reader and a tag that's physically farther away from the reader and still pass the authentication test since the tag-read measurement will be significantly different from that at the reader's end. Moreover, unless the adversary identifies vulnerabilities in the authentication protocol that allows for modification of magnetometer reading values in the protocol, it is not possible to accomplish a successful relay attack.

To ensure that the authentication protocol is lightweight, we only make use of exclusive-OR (XOR) and rotation functions. The RFID tag and reader share three secrets x, y, and z. Our rationale behind the use of three shared secrets instead of just one shared secret between tag and reader is that knowledge of any one of the secret will not compromise the authentication protocol by rendering it vulnerable to attacks by an adversary. To ensure that an adversary does not block messages between reader and tag and disrupting the process, the reader expects a response from the tag after it sends its initial

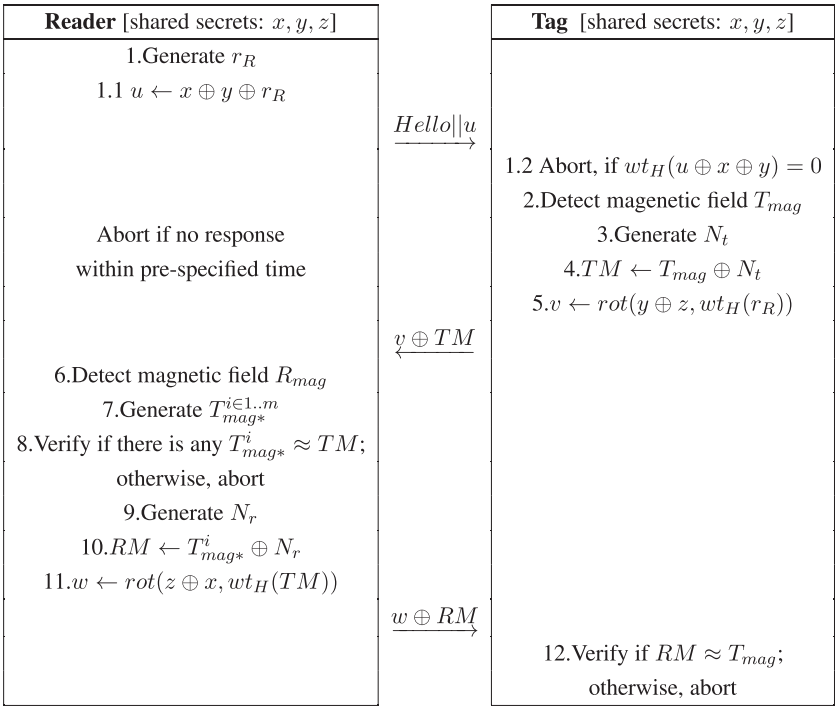

Fig. 3. The proposed authentication protocol.

message. If this message from the tag is not received within a pre-specified amount of time, the reader aborts the protocol. Note that all communication between reader and tag occur through wireless medium.

The reader initiates the authentication process by generating a random k-bit nonce r_R and XORs this with the XOR of two of its shared secrets $(x \oplus y)$ resulting in u. The reader then sends a hello message along with u to the tag. Upon reception of this message, the tag ensures that r_R is non-zero by computing the Hamming distance of $u \oplus x \oplus y$ and aborts the authentication process when the Hamming distance is zero. To proceed, the tag detects the magnetic field T_{mag} and then generates N_t, which is a k-bit noise with a random mix of $\frac{k}{2}$ bits $= 1$ and remainder of the $\frac{k}{2}$ bits $= 0$. The even split of 0s and 1s is to ensure that its information content is zero and the adversary does not benefit by guessing its value. The tag generates TM by $T_{mag} \oplus N_t$. It also rotates the XOR of two shared secrets $y \oplus z$ by $wt_H(r_R)$ places to generate v. The tag can now generate $v \oplus TM$, which sufficiently hides its magnetometer reading from an adversary.

Upon reception of $v \oplus TM$ from the tag, the reader generates its own magnetometer reading R_{mag}, which it uses to compare against that from the tag. Since the readings from the magnetometers at the tag and reader side may not necessarily be exactly the same, we allow for some tolerance. Moreover, the difference between the readings, if any, are bound to be minor due to reader calibration. Therefore, the differences are likely only at the least significant bit level in binary representation. So, we consider all possible variants of the least significant bits $\left(T^{i \in 1..m}_{mag*}\right)$ for a match with the knowledge that half of the bits in the tag's readings are flipped. When a match is not found, the authentication protocol is aborted. Otherwise, the reader generates N_r, which is a k-bit noise with a random mix of $\frac{k}{2}$ bits $= 1$ and $\frac{k}{2}$ bits $= 0$. The reader takes XOR of N_r and T^i_{mag*} to generate RM. The reader also rotates the XOR of first and third shared secrets $(x \oplus z)$ $wt_H(TM)$ bits to form w. Next, the reader sends $w \oplus RM$ to the tag. When it receives $w \oplus RM$, the tag validates RM, and aborts the protocol if RM is invalid.

4.2. Security analysis

The proposed protocol has several characteristics that ensure its security. Freshly-generated nonce (r_R) is used during every run of the protocol. Moreover, the noise vectors generated by the tag (N_t) and reader (N_r) add to this characteristic. Independent magnetic field measurements by both reader and tag and the encryption of messages passed between tag and reader ensures that it is secure against mafia fraud attacks. The protocol is also secure against terrorist attack since a (dishonest) tag has to share its secrets $(y \oplus z)$ with an adversary to accomplish such an attack.

Knowledge of any one of the shared secrets (x, y, z) does not lead to any advantage to the adversary. Knowledge of at least two of the three shared secrets would compromise the security of the protocol. However, it is difficult to retrieve any of the shared secrets from passively observing the messages passed between tag and reader or even through active capture and modification of messages.

We now consider a few specific attacks on such authentication protocols.

Tag/Reader Anonymity: The tag and reader identification information (e.g., secret keys) are protected from the possibility of information leakage since this information can be used to track and/or trace the tag or (mobile) reader. This is significant since knowledge of such information can allow for the possibility of cloning the tag or reader. We include the possibility of the reader being mobile, as is the case in some RFID applications.

Forward Security: If all shared secrets are somehow known to an adversary, these secrets cannot be used to decrypt all earlier messages since TM and RM do not involve these shared secrets and both these are encrypted messages.

Tag/Reader Location Privacy: Since the messages are seemingly random between any two authentication rounds, it is difficult for an adversary to use any of the messages to track the tag and/or the (mobile) reader.

Secrecy/Data Integrity and Authenticity: The integrity of the messages passed between tag and reader is ensured by not sending anything that could compromise the security of the protocol in cleartext. Even though the protocol is lightweight, it is designed to be secure and to maintain its secrets regardless of active or passive attacks from adversaries.

DoS/Desynchronization: Since the shared secret keys are not updated after every authentication round, desynchronization is not an issue. The possibility for Denial of Service (DoS) attacks in the proposed protocol is only through blocking and/or modification of message(s). Blocking messages will not grant an adversary any advantage: the reader waits for acknowledgement message from the tag within a pre-determined amount of time, and aborts if this does not happen; since the tag is not expected to have an onboard clock, it is not affected when an adversary blocks the second message from reader to tag since its signature is not the same as the first message from the tag - i.e., the tag can tell a fresh authentication round from one that is in-process and responds accordingly. Modification of any of the messages by an adversary similarly will not allow for protocol compromise.

Passive Replay: Passive replay of any of the three messages that are passed between tag and reader from a previous authentication round will not result in successful authentication due to the existence of r_R, N_t, and N_r that introduce sufficient randomness in the passed messages during each authentication round.

Reader/Tag Impersonation Attack: For an adversary to impersonate a reader to a tag or a tag to a reader it should have the ability to generate messages that seem appropriate and valid to the recipient. In the proposed authentication protocol, the first message (from reader to tag) passes muster. However, since the second message ($v \oplus TM$ from tag to reader) depends on r_R, and therefore the first message from reader to tag, an adversary cannot send any random message from reader to tag and hope that it is a step in successful impersonation of reader to tag. In other words, an adversary cannot successfully impersonate a reader to the tag. An adversary also cannot successfully impersonate a tag to a reader since it requires knowledge of the secrets $(y \oplus z)$.

5. Discussion

Relay attacks have the potential to cause serious damage to privacy and security in contactless applications. Existing solutions to relay attack mostly involve some variant of distance-bound, while there is some interest in other approaches such as those related to context awareness. An easy way to avoid relay attacks is by shielding the tag from unintended reads such as a pocket made of RFID-blocking fabric [35]. However, this approach is often not sustainable because it defeats the original intended purpose of automation with minimal human input. Context-awareness has also been used to selectively unlock the devices, but the reliability of such a mechanism depends entirely on related sensors. Some researchers have proposed the use of RFID signal strength measurement to counter relay attack. However, its applicability is limited due to the fact that signal strength is highly prone to errors [25,29,31].

Distance-bounding approaches are based on the belief that if the signal travel distance is short, the travel time can not be long. The distance-bounding approaches rely on such a time-distance relationship to check for the physical proximity of RFID tag and reader. The premise of context-awareness approaches is that if RFID tag

and reader are near each other, their ambient conditions would be similar. After all, the RFID tag and reader must share similar space if they are near each other. Namely, the context-awareness approaches depend on such a space-wise constraint to verify physical proximity. Both the distance-bounding and context-awareness approaches have been shown in previous studies as reasonably effective defense against relay attacks. However, distance-bounding protocols are vulnerable when the computation/processing time at the tag's side during the fast bit exchange process is in the order of microseconds since this would wash away any accurate round-trip time measurement. This is a serious issue in distance-bounding-based means to address relay attacks.

We therefore considered possible non-distance-bounding approaches to identify relay attacks as they occur. Specifically, we critically evaluated several facets of ambient condition since a reader and tag in close physical proximity should experience the same ambient conditions. For relay attacks to work, an adversary has to either find vulnerabilities in the protocol or somehow ensure that the ambient condition near the tag and reader are identical. Both of these have their own challenges, depending on the strength of the authentication protocol and the ambient condition facet(s) of interest. Our analysis led to our choice of magnetometer reading due to its dominant beneficial characteristics. We then developed a lightweight protocol with the incorporation of magnetometer readings at both the tag and reader levels. Unlike most existing protocols that claim to defend against relay attacks, the proposed authentication protocol uses magnetic field for proximity check. The protocol is flexible in the sense that any sensor readings can be used instead as long as such readings are reliable and valid. Given the limitations that are associated with the use of time to measure distance in such applications, we also do not use the time component for this purpose. We evaluated the protocol against commonly seen vulnerabilities in such authentication protocols and found the proposed protocol to be secure.

A limitation with the proposed protocol is associated with how relay attacks have traditionally been defined. As modeled in existing literature, the adversaries in relay attack scenarios only attempt to show that the actual physical separation between tag and reader is closer than what it is in reality. This is done to show that the tag and reader are indeed in close physical proximity of each other. However, there could be scenarios where an adversary may want to show that the tag and reader are physically farther apart. Our protocol will not work in that scenario since the sensor readings of tag and reader will need to be different. To our knowledge, none of the published authentication protocols that purport to address relay attacks consider this possibility.

The ease with which relay attacks are accomplished and the extensive harm such vulnerability renders, it is necessary to identify relay attacks when they occur and stop the process. While existing authentication protocols that use round-trip time measurements are a good start, they have serious issues. The proposed authentication protocol is a step in the direction of addressing relay attacks with fewer issues.

References

[1] R.N. Akram, I. Gurulian, C. Shepherd, K. Markantonakis, K. Mayes, Empirical Evaluation of Ambient Sensors as Proximity Detection Mechanism for Mobile Payments, 2016, 1–13. arXiv preprint, arXiv:1601.07101.

[2] M. Azizi, N. Bagheri, A. Mirgadri, Providing a distance bounding protocol named Pasargad in order to defend against relay attacks on RFID-based electronic voting system, Int. J. UbiComp 2 (3) (2012) 69–82.

[3] B. Bacheldor, Hybrid tag includes active RFID, GPS, satellite and sensors, RFID J. (2009)February 24.

[4] T. Beth, Y. Desmedt, Identification Tokens - or: Solving the Chess Grandmaster Problem, 537. CRYPTO LNCS. 1990, 169–176.

[5] E. Biba, Does Your Car Key Pose a Security Risk? 2005, http://pcworld.about.net/news/Feb142005id119661.htm.

[6] I. Bose, A.K.H. Lui, E.W.T. Ngai, The impact of RFID adoption on the market value of firms: an empirical analysis, J. Organ. Comput. Electron. Commer. 21 (4) (2011) 268–294.

[7] I. Bose, A.C.M. Leung, Radio frequency identification for customer relationship management, in: T. Blecker, G. Huang (Eds.), RFID in Operations and Supply Chain Management: Research and Applications, Erich Schmidt Verlag Publishing. 2008, pp. 273–288.

[8] S. Brands, D. Chaum, Distance-Bounding Protocols, 765. EUROCRYPT, LNCS. 1993, 344–359.

[9] M. Buckner, R. Crutcher, M.R. Moore, S.F. Smith, GPS and Sensor-Enabled RFID Tags, Unclassified Document, Oak Ridge National Laboratory. 2001, http://www.ornl.gov/webworks/cppr/y2001/pres/118169.pdf.

[10] J.H. Conway, On Numbers and Games, Academic Press. 1976.

[11] A. Czeskis, K. Koscher, J.R. Smith, T. Kohno, RFIDS and secret handshakes: defending against ghost-and-leech attacks and unauthorized reads with context-aware communications, Proceeedings of the ACM Conference on Computer and Communications Security (CCS), 2008. pp. 479–490.

[12] D.E. Denning, P.F. MacDoran, Location-based authentication: grounding cyberspace for better security, Computer Fraud & Security, 1996. pp. 12–16. Feb.

[13] Y. Desmedt, Major Security Problems With the Unforgeable (Feige)-Fiat-Shamir Proofs of Identity and how to Overcome Them, 6th Worldwide Congress on Computer and Communications Security and Protection, 1988, 147–159.

[14] Y. Desmedt, C. Goutier, S. Bengio, Special Uses and Abuses of the Fiat-Shamir Passport Protocol, 293. CRYPTO, LNCS. 1987, 21–39.

[15] S. Drimer, S.J. Murdoch, Keep your enemies close: distance bounding against smartcard relay attacks, Proceedings of the USENIX Security Symposium, 2007. pp. 87–102.

[16] F.I.D.E. Ethics Commission, 2011. Judgement Report Available At:. http://www.Fide.Com/Images/Stories/NEWS_2012/FIDE/2_Ethics_Commission_Judgement_In_The_Case_French_Team.Pdf.

[17] A. Francillon, B. Danev, S. Capkun, Relay attacks on passive keyless entry and start systems in modern cars, Proceedings of the Network and Distributed System Security Symposium (NDSS), 2011.

[18] L. Francis, G. Hancke, K. Mayes, A practical generic relay attack on contactless transactions by using NFC mobile phones, Int. J. RFID Secur. Cryprography (2013) 92–106.

[19] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, Practical relay attack on contactless transactions by using NFC mobile phones, Proceedings of the Workshop on RFID and IoT Security (RFIDsec 2012 Asia), 2012. pp. 21–32.

[20] T. Halevi, S. Lin, D. Ma, A.K. Prasad, N. Saxena, J. Voris, T. Xiang, Sensing-enabled defenses to RFID unauthorized reading and relay attacks without changing the usage model, Proceedings of the IEEE International Conference on Pervasive Computing and Communications, 2012. pp. 227–234.

[21] T. Halevi, D. Ma, N. Saxena, T. Xiang, Secure proximity detection for NFC devices based on ambient sensor data, Proceedings of the European Symposium on Research in Computer Security (ESORICS), 2012. pp. 379–396.

[22] S.T.B. Hamida, P.H. Thevenon, J.B. Pierrot, O. Savry, O.C. Castelluccia, Detecting relay attacks in RFID systems using physical layer characteristics, Proceedings of the 6th Joint IEEE-IFIP Wireless and Mobile Networking Conference (WMNC), 2013. pp. 1–8.

[23] G. Hancke, A Practical Relay Attack on ISO 14443 Proximity Cards, 2005, http://www.cl.cam.ac.uk/gh275/relay.pdf.

[24] G. Hancke, M. Kuhn, An RFID Distance Bounding Protocol, SecureComm. 2005, 67–73.

[25] J. Hering, The BlueSniper Rifle, Presented at 12th DEFCON, Las Vegas, 2004.

[26] M. Hlavac, T. Rosa, A Note on the Relay Attacks on E-Passports, International Association for Cryptologic Research, 2007, http://eprint.iacr.org/2007/244/pdf.

[27] International Civil Aviation Organization, 2015. http://www.icao.int/.

[28] G. Kapoor, W. Zhou, S. Piramuthu, Multi-tag & multi-owner RFID ownership transfer in supply chains, Decis. Support. Syst. 52 (1) (2011) 258–270. december.

[29] Z. Kfir, A. Wool, Picking virtual pockets using relay attacks on contactless smartcard systems, Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm), 2005. pp. 47–58.

[30] C.H. Kim, G. Avoine, RFID distance bounding protocol with mixed challenges to prevent relay attacks, Proceedings of the International Conference on Cryptology And Network Security, 2009. pp. 119–133.

[31] I. Kirschenbaum, A. Wool, How to build a Low-Cost, Extended-Range RFID skimmer, Cryptology ePrint Archive: Report 2006/054, 2006.

[32] D. Ma, A.K. Prasad, N. Saxena, T. Xiang, Location-aware and safer cards: enhancing RFID Security and privacy via location sensing, Proceedings of the ACM Conference on Wireless Network Security (WiSec), 2012. pp. 51–62.

[33] S. Mauw, J. Toro-Pozo, R. Trujillo-Rasua, A class of precomputation-based distance-bounding protocols, Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), 2016. pp. 97–111.

[34] A. Mitrokotsa, C. Onete, S. Vaudenay, Mafia fraud attack against the RC Distance-Bounding protocol, Proceedings of the IEEE International Conference on RFID -Technologies and Applications (RFID-TA), 2012. pp. 74–79.

[35] RFID-Blocking READY Jeans, Protected by norton, https://www.betabrand.com/mens-_rfid-_blocking-_pocket-_norton-_denim-_jeans.html.

[36] O. Oren, A. Wool, Attacks on RFID-based Electronic Voting Systems, IACR Cryptology, ePrint Archive, 2009, 422.

[37] M. Philipose, J.R. Smith, B. Jiang, K. Sundara-Rajan, A. Mamishev, S. Roy, Battery-free wireless identification and sensing, IEEE Pervasive Comput. 4 (1) (2005) 37–45.
[38] S. Piramuthu, Protocols for RFID tag/reader authentication, Decis. Support. Syst. 43 (3) (2007) 897–914. april.
[39] S. Piramuthu, RFID Mutual authentication protocols, Decis. Support. Syst. 50 (2) (2011) 387–393. January.
[40] S. Piramuthu, R. Doss, On sensor-based solutions for simultaneous presence of multiple RFID tags, Decis. Support. Syst. 95 (2017) 102–109. March.
[41] K. Rasmussen, S. Čapkun, Location Privacy of Distance Bounding, Proceedings of the Annual Conference on Computer and Communications Security (CCS), 2008. pp. 149–160.
[42] J. Reid, J.M.G. Nieto, T. Tang, B. Senadji, Detecting relay attacks with timing-based protocols, Proceedings of the 2nd ACM Symposium on Information, Comput. Commun. Secur. (2007) 204–213.
[43] Z. Riha, Book chapter: the future of identity in the information society, IFIP Adv. Inf. Commun. Technol. Vol. 298 (2009) 151–159.
[44] W. Shen, H. Xu, R. Sun, P. Wang, Research on defense technology of relay attacks in RFID systems, International Conference on Computer Science and Intelligent Communication (CSIC 2015), 2015, 2015. pp. 18–22.
[45] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, M. Srivastava, PyCRA: physical challenge-response authentication for active sensors under spoofing attacks, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015. pp. 1004–1015.
[46] Y. Shu, Y. Gu, J. Chen, Sensor-data-enhanced authentication for RFID-based access control systems, Proceedings of the IEEE Mobile Ad Hoc Sensor Systems (MASS), 2012. pp. 236–244.
[47] S. Taghvaeeyan, R. Rajamani, Nature-inspired position determination using inherent magnetic fields, Technology 2 (2) (2014) 161–170.
[48] Y.-J. Tu, S. Piramuthu, RFID distance bounding protocols, 1st Int. EURASIP Work. RFID Technol. (2007) 67–68.
[49] P. Urien, S. Piramuthu, Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks, Decis. Support. Syst. 59 (2014) 28–36.

Yu-Ju (Tony) Tu is an assistant professor of MIS at National Chengchi University, Taipei, Taiwan. He received his Ph.D. in IS from the University of Illinois at Urbana-Champaign. His research interests include RFID systems, IT portfolio management, learning-based DSS, and service science.

Selwyn Piramuthu is Professor of Information Systems at the University of Florida. His research interests include RFID systems.