Localization Privacy

Florida State University, Tallahassee, Florida, U.S.A.
burmester@cs.fsu.edu
http://www.springer.com/lncs

Abstract. Location-aware technology and its applications are fundamental to ubiquitous computing. Essential to this technology is object localization and identification. RFID (radio frequency identification) technology has been shown to be very effective for identification and tracking applications in industry, transport, agriculture and healthcare. However it can also be used for accurate object localization. Indeed RFID technology is ideally suited for such applications, and more generally for context-aware computing, because of the low cost, low power, light weight and endurance of RFID tags. In this chapter we study the security issues of RFID localization.

Keywords: RFID, object localization, localization privacy, location-aware applications, location privacy.

1 Introduction

Radio Frequency Identification (RFID) is a promising technology that is widely deployed for supply-chain and inventory management, for retail operations, healthcare and the pharmaceutical industry. Other applications include tracking animals, vehicles, and more generally, automatic identification. The main advantage of RFID over barcode technology is that it does not require line-of-sight reading. RFID readers can also interrogate RFID tags at greater distances, faster and concurrently. One of the most important advantages of RFID technology is that tags may have read/write capability, and an integrated circuit allowing stored information to be altered dynamically.

The most common type of RFID tag is a *passive* tag that has no power source of its own and thus is incapable of autonomous activity. As with all other types, it has an antenna for receiving and transmitting radio signals and can store information. Such tags may also have an integrated circuit for processing information.

Passive tags harvest power from an external radio signal generated by an RFID reader to "wake up" and initiate a signal transmission. They are maintenance free and high-endurance. Some passive RFID devices such as WISP (Wireless Identification and Sensing Platform) [47] developed by Intel Labs, have additional features such as a real-time clock (that relies on harvested power) and a 3D-accelerometer. We also have *battery assisted passive* RFID tags that have a higher forward link capability (greater range). Finally we have *active* RFID tags that contain a battery and can transmit signals once an external source has been identified.

EPCGlobal [16] recently ratified the EPC Class 1 Gen 2 (EPCGen2) standard for passive RFID deployments which defines a platform for RFID protocol interoperability.

This supports basic reliability guarantees and is designed to strike a balance between cost and functionality, but with less attention paid to security.

Several RFID protocols that address security issues for passive devices have been proposed in the literature. We refer the reader to a comprehensive repository available online at [3]. Most RFID protocols use hash functions [44, 38, 20, 4, 15, 35] that are not supported by EPCGen2. Some protocols use pseudo-random functions [8, 46, 10], or pseudo-random number generators, mechanisms that are supported by EPCGen2, but these are not optimized for EPCGen2 compliance. Recently a lightweight RFID protocol was proposed [11] that is based on loosely synchronized pseudo-random number generators.

In this article we study a novel application of RFID in which tags will only respond to a challenge if this is authentic. Authentication is the primary goal for RFID deployments, however it is important that the process used to support it does not have a negative impact on other security goals, such as privacy. If an RFID tag has to reveal its identity to get authenticated, then an eavesdropper can track its movement in the supply chain. For some applications *linkability* is a serious privacy threat. To deal with such threats one typically uses pseudonyms. However this still will not prevent the adversary from detecting the *presence* of responding tags. The location of a transmitting device can be determined by analyzing the RF waveform received from it. Several RFID localization algorithms have been proposed in the literature [51, 50, 5]. Some of these use the signal strength or detection rate [36, 26], while others use statistics or Bayesian inference [7, 33]. We also have kernel-based learning algorithms [36], phase-based algorithms [19, 42], proximity and nearest-neighbor algorithms.

Localization privacy requires that an RFID tag will only respond to a challenge from an RFID reader if it can first ascertain that the challenge is authentic and fresh (current). In particular, that it is not replayed. Since the range of RFID readers is rather short, replay attacks are a major threat for RFID deployments.Localization privacy captures a novel aspect of privacy extending the traditional privacy notions of anonymity and unlinkability to devise discovery. Anonymity and unlinkability (see e.g., [14, 32]) are slightly weaker notions: even though the adversary may not be able to recognize a tag, or link the tag's interrogation sessions, by knowing its location it can identify that tag to some degree, particularly if the tag is static and there are only a few tags in the range of an RFID reader—see Section 4, Application 1. Localization privacy is essentially a steganographic attribute. The goal of steganography is to hide data in such a way that the adversary cannot detect its *existence*, while the goal of localization privacy is to hide a device in such a way that its *presence* cannot be detected.

Paper outline. We discuss a novel application of location privacy for ubiquitous systems in which the location of a hidden device can only be discovered by its rightful owner. In this article, we first overview RFID deployments for passive and active tags—Section 2. Then in Section 3 we discuss fine grain localization technologies and non-linear junction detection mechanisms. In Section 4 we consider applications for localization privacy and present our threat model for localization privacy in a wireless medium. Our main results are in Section 5 where we show that localization privacy can be achieved with RFID tags that possess location and/or temporal mechanisms. Then in

Section 6 we show that localization privacy cannot be achieved with RFID tags that do not possess such mechanisms. We summarize our results in Section 6.

We conclude this Introduction with the following motivating paradigm.

His Late Master's Voice:[1] **barking for location privacy** [9]. Bob died suddenly leaving his treasure to sister Alice. Moriarty will do anything to get it, so Alice hides the treasure together with Nipper, and promptly departs. Nipper is a low-cost RFID device that responds *only* to Alice's calls—making it possible for Alice to locate the hidden treasure later (she is quite forgetful) when Moriarty is not around.

2 RFID deployments

A typical deployment of an RFID system involves three types of legitimate entities, namely *tags, readers* and a *back-end Server*. RFID tags are attached to, or embedded in, host objects (e.g., merchandize) to be identified. Each tag is a transponder with an RF coupling element and may also have a microprocessor. The coupling element has an antenna coil to capture RF power, clock pulses and data from the RFID reader. The microprocessor has small amounts of ROM for storing, among other information, the tag's identification, volatile RAM and (potentially) nonvolatile EEPROM.

An RFID reader is a device with storage, computing, and communication resources comparable to at least those of a powerful PDA. It is equipped with a transceiver consisting of an RF module, a control unit, and an RF coupling element to interrogate the tags. RFID readers implement a radio interface to the tags and also a high level interface to a backend server that processes captured data.

The back-end Server is a trusted entity that maintains a database with all the information needed to identify tags, including their identification numbers. Since the integrity of an RFID system is entirely dependent on the proper (secure) behavior of the Server, it is assumed that the Server is physically secure and not subject to attacks. It is certainly legitimate to consider privacy mechanisms that reduce the trust on the Server, for instance, to mitigate the ability of the Server to collect user-behavior information, or to make the Server function auditable. However, in this article, we consider a Server to be entirely trusted and do not investigate such issues. For an overview of mechanisms that can be used to deal with privacy issues concerning back-end Servers we refer the reader to [44]. As far as resources, we consider the Server to be a powerful computing device with ample disk, memory, communication, and other resources.

Reader-tag coupling. There are several ways an RFID reader-tag coupling can be implemented. These include:

- RFID backscatter coupling,
- RFID capacitive coupling,
- RFID inductive coupling.

[1] The HMV trademark comes from a painting by Francis Barraud who inherited from his late brother Mark a fox terrier, Nipper, a cylinder phonograph and a number of Mark's recordings [21]. The painting portrays Nipper listening to the sound emanating from the trumpet of the phonograph.

The type of coupling used affects several aspects of the RFID system including the tag's range (forward link capability), and the frequencies needed. Capacitive coupling can only be used for very short ranges, while inductive coupling (near field coupling) for slightly longer ranges. RFID backskatter coupling is normally used where longer distances are needed. For localization privacy applications we shall use backskatter coupling.

EPCGen2. To foster and promote the adoption of RFID technology and to support interoperability, EPCGlobal [16] and the International Organization for Standards (ISO) [22] have been actively engaged in defining standards for tags, readers, and the communication protocols between them. A recently ratified standard for passive (Class 1) RFID deployments is EPC Class1 Gen2 (EPCGen2). This is a communication standard that creates a platform on which to build interoperable RFID protocols for passive tags. It supports efficient tag reading, flexible bandwidth use, multiple read/write capabilities and basic security guarantees, provided by an on-chip 16-bit Pseudo-Random Number Generator (RNG) and a 16-bit Cyclic Redundancy Code (CRC-16). EPCGen2 is designed to strike a balance between cost and functionality.

The most basic application of RFID tags is to supply, upon request, an encoded identifier. The identifier may be unique (as in passports or badges), or clustered, that is identify a type of merchandize. The most common RFID type is a passive tag that has no power source of its own and is powered by the radio waves of the reader, with its antenna doubling as a source of RF power. We distinguish three types of passive RFID transponders.

Smart labels. These are Class 1 basic memory devices that are typically Read-Only. They are capable of storing small amounts of data, sufficient for tag identification. Smart labels are low-cost replacements of barcodes and are used for inventory control. They function by backscattering the carrier signal from RFID readers. Smart labels are quite insecure: they are subject to both unauthorized cloning and unauthorized tracking, though in many cases are at least resistant to disabling attacks since they have a single operational state.

Re-writable tags. These are Class 1 tags with re-writable memory containing nonvolatile EEPROM used to store user-and/or Server-defined information. In a typical application [2], they store Server certificates used to identify tags and are updated each time a tag is identified by an authorized reader. These tags can also store kill-keys, used to disable them. Despite this additional functionality, re-writable tags are still insecure: They are subject to unauthorized cloning, and unauthorized disabling, and in cases unauthorized tracking. Indeed a hacker (rogue reader) can record a tags certificate and use it to impersonate the tag, track the tag (only until the next time the tag interacts with an honest reader outside the range of the attacker), and/or replace it with an invalid certificate, to disable the tag.

IC tags. These are Class 2 smart tags with a CMOS integrated circuit, ROM, RAM, and nonvolatile EEPROM. They use the integrated circuit to process a readers challenge and generate an appropriate response. IC tags are the most structured tags and

used with an appropriate RFID protocol can defeat most attacks on RFID systems. Our protocols for localization privacy will use such tags.

3 Fine grain RF localization

RF localization is based on analyzing the RF signals emitted by a source (target). In our applications the source will either be a Class 2 passive IC tag (including tags such as WISP [47]), or a Class 3 battery-assisted tag. These are good candidates for localization since they are inexpensive, small, and easy to maintain.

The received RF waveform is influenced by the paths travelled by the signal. It therefore carries raw information about these paths, which can be used for localization. However, because coarse information such as the detection rates of RFID tags [26], the received signal strength [1, 50, 48, 36], or both [24], is readiliy available at the upper layers, most localization techniques rely on such information. The processing of such information is also often based on simplified assumptions or empirical equations [37, 50]. For example, Landmarc [37] localizes RFID tags by comparing signal strength profiles with reference tags of known location. Such systems cannot achieve high granularity and usually offer granularity at the meter or sub-meter's level, despite the existence of algorithmic optimizations in the upper layers, such as Bayesian inference [1, 43, 33, 51], nearest neighbor search [37, 26, 51], and kernel-based learning [7, 36, 51].

For high granularity the raw signal waveform must be passed to the upper layers and processed using algorithms that understand the intricate relations between the wireless environment and the signal. Such an approach is employed in GPS technology (carrier phase tracking), where the phases from signals coming from different satellites are used to calculate the distances from the GPS unit to the satellites to achieve millimeter accuracy.

Fine grain localization with RF waveform information has been studied recently [42, 29, 12, 28, 27, 27], and shown to be effective for outdoor applications [34] where the received signal phase can be used to infer the length of the line-of-sight path and subsequently the location. Such techniques cannot be applied to indoor applications because of multi-path distortion. In an indoor environment the signal is reflected by metal surfaces or the diffracted by sharp edges [40]). So the received signal is the summation of many different versions of the original signal with different delays and attenuation. While ray-tracing [13, 45, 17] can be used to reconstruct the environment, and therefore to estimate the location and nature of a reflecting surface and a scattering source, and to reconstruct the signal propagation paths, the complexity of indoor environments makes such solutions intractable. Consequently, despite many notable attempts [42, 29, 49, 37, 31, 33, 12], indoor fine-granularity localization is still elusive. However some recent work [19] suggests that phase-difference algorithms may lead to fine grained indoor localization.

RFID localization algorithms. RFID localization is based on modelling the variations of RF signals in space. Theoretically one can calculate the distance between the source and the receiver by using the strength of the received signal or the time-of-arrival. However in practice one has to take into account effects such as fading, absorption and

blocking, that reduce the signal strength; also effects such as refelection and refraction that result in multi-paths; finally signals from other sources may interfere with the signal and collide at the receiver.

RFID localization algorithms can be classified into two groups [51]. Algorithms that callibrate the RF signal distribution in a specific environment and then estimate the location of the target, and algorithms that directly compute the location of the target based on signal strength. Algorithms of the first kind include: (i) *multilateration algorithms* [18, 5, 37] that estimate the coordianates of the target from the distances measured between the target and reference points (with known coordinates), and (ii) *Bayesian inference algorithms* [33] in which evidence or observations are used to infer that a hypothesis (a candidate location) may be true. Algorithms of the second kind include: (iii) *nearest-neighbor algorithms* in which an object is localized by its neighbors, (iv) *proximity algorithms* in which a mobile reader scans a square area subdivided into cells, with the target determined by intersecting the set of active cells in each reading, and (v) Kernel-based learning algorithms.

Non-Linear Junction (NLJ) detectors. These are used to detect covert electronic listening devices (bugs), regardless of whether the devices are emitting signals, turned on or even turned off.

A *non-linear junction* is a junction between different materials for which a change in the voltage applied across the junction does not produce a proportional change in the current flowing through the junction. NLJs are found in semiconductor components such as diodes, transistors and integrated circuits (which use p-n junctions). However, NLJs also occur in crystals, rocks, building materials, metal/oxide junctions, etc, when dissimilar metals and/or other materials come into contact with one another. Subjecting a NLJ to a strong high frequency radio signal, typically a spectrally pure microwave RF signal (usually 888 or 915 MHz), will cause an electric current to flow through the junction which, because of the non-linearity, consists of harmonics of the originating radio signal (typically the 2nd, 3rd and 4th harmonics).

A non-linear junction (NLJ) detector floods a small region of a target space with high-frequency RF energy and analyzes any signals that are emitted for harmonics of the flooding frequency. The detector has a sensitive receiver tuned for these harmonics, and can be used to identify and locate the target device [25, 6].

Since integrated circuits use semiconductors with p-n junctions, a NLJ detector will detect almost any un-shielded electronics, whether the electronics is on or off. Of course it will also detect other things that are not electronic in nature, so there will be a large number of false alarms (positives).

4 Applications and threat model

In this section we discuss the threat model for localization privacy. To motivate our approach we first consider two applications for localization privacy.

Applications

1. *Device discovery.* This involves one-time tag interrogations: when the device is discovered it is recovered and the task for that device terminates. An example of such an application involves the deployment of tagged plastic mines. More generally, applications in which objects are hidden so that they can only be recovered later by authorized agents. For such applications, for each object, localization privacy lasts for only one interrogation.
2. *Sensor deployments in hostile territory.* Tagged sensors can be deployed by casting them from aircraft over hostile territory. The sensors are used for monitoring the deployment area but are not networked for localization privacy. Instead an armored RFID reader traverses the deployment area interrogating those tags on its route that are in range (the route must go though every cell of the sensor range grid). For this application localization privacy should endure for several interrogations.

In both applications only the RFID reader is mobile, while the location of the RFID tag is fixed for the lifetime of the system. Consequently if a Global Positioning System (GPS) is used, this will be activated only once. It follows that the tag can be equipped with a small battery and a GPS used to establish its position on deployment. Several hybrid RFID solutions are currently available (see *e.g.*, [41]).

Threat model

RFID tags are a challenging platform from an information assurance standpoint. Their limited computational, communication, and storage capabilities, preclude the use of traditional techniques for securing communication protocols and incentivizing adoption of lightweight approaches. At the same time the robustness and security requirements of RFID applications can be quite significant. Ultimately, security solutions for RFID applications must take as rigorous a view of security as other types of applications.

Accordingly, our threat model assumes a Byzantine adversary: the adversary controls the delivery schedule of all communication channels, and may eavesdrop on, or modify, their contents. The adversary may also instantiate new communication channels and directly interact with honest parties. In particular, this implies that the adversary can attempt to perform impersonation, reflection, man-in-the-middle, and any other passive or active attacks that involve reader-to-tag communication. To address localization privacy, we adapt this model to a wireless medium that allows for: (i) *localization (or surveillance) technologies* that analyze radio signals (based on strength, direction, phase differences, etc) and (ii) *radio jamming technologies* that override signals emitted by devices.

We distinguish two types of adversary: (i) *ubiquitous*, that can access all deployed tags,[2] and (ii) *local*, whose wireless range is approximately that of authorized RFID readers. In our threat model for localization privacy we shall constrain the impact of localization and signal jamming technologies by assuming that:

[2] This can be achieved in several ways, *e.g.*, by using a hidden network of listening devices—although setting up such a network may be perilous in a plastic mine deployment.

1. The adversary *cannot* localize a tag while it is inactive, *e.g.*, by using a non-linear junction detector (Section 4), or more generally a device that floods a target area with an RF signal and analyzes the reflected signal.[3]
2. The adversary *cannot* localize a tag while it verifies a challenge from a reader and/or while it computes its response to the reader.[4]
3. The adversary *cannot* localize a tag during an authorized interrogation if the tag's response is too weak to be received by the RFID reader.[5] In particular the adversary cannot localize a tag by aggregating partially leaked location information. Similarly, the adversary *cannot* localize a tag during an interrogation (in the presence of the reader) by jamming its response (to prevent the reader from getting it).[6]
4. The adversary must eavesdrop on *at least one* complete response from the tag (more generally, a radio signal of a certain duration) to localize the tag.

From Assumption 3 it follows that we either have:

3. *Reliability.* If a tag is in the range of an authorized RFID reader that interrogates it, then the interrogation will be completed,

or there is a DoS-deadlock between the authorized reader and the adversary. We shall assume that in the second case, the authorized reader always wins—the intruder is located and destroyed.

Ubiquitous adversaries. A ubiquitous adversary can eavesdrop on all communication channels and therefore can also localize any tag that is interrogated by an authorized RFID reader, *after* the reader has localized it (by Assumption 4; disruption attacks are restricted by Assumption 3). For ubiquitous adversaries localization privacy is restricted to one-time tag interrogations. After the tag is localized it is inactivated/killed. We therefore shall assume that:

4. *One-time tag interrogation.* A ubiquitous adversary *cannot* localize (discover) a tag that has already been located by an authorized reader.

The scope of replay attacks against localization privacy with one-time tag interrogations (*e.g.*, device discovery), is restricted to replaying reader challenges beyond the range of the reader (by Assumptions 3 and 4, since a tag will only respond once, when the challenge is authentic).

Local adversaries. Local adversaries are restricted by their broadcast range: protection against such adversaries assures only weak localization privacy. In our threat model for local adversaries we constrain the impact of localization and signal jamming technologies by assuming that:

[3] Such detectors must operate at close proximity to a target device. In applications where the reflected harmonics may be detected, the IC circuit of the RFID device should be shielded.

[4] Typically any signals emitted during an internal calculation of the tag are very weak. In applications where the variations of the emitted signals may be detected, a small battery may be used to control the fluctuations.

[5] The tag will only respond to the reader's signal if this is sufficiently strong.

[6] The reader will either identify, locate and destroy the intruder or refrain from interrogating the tag.

5. A local adversary *cannot* localize a tag from its response while it is interrogated by an authorized reader.[4]

This assumption highlights the weakness of local adversaries. It is partly justified by noting that the tag's response (a modulated backscatter) is much weaker than the reader's challenge, and attenuates as the inverse fourth power of traveled distance. Without it we cannot have localization privacy with multiple tag interrogations since the location of the tag would be revealed the first time it responds to an authorized challenge. This effectively reduces our applications to *backscatter* tags, and not capacitive or inductive tags (Section 2).

Focus/Scope. In this article we investigate privacy and security issues of ubiquitous RFID systems at the protocol layer. We do not address issues at the physical or link layers, such as the coupling design, the power-up and collision arbitration processes, or the air-RFID interface. For details on such issues and, more generally, on RFID standards, we refer to the Electronic Protocol Code [16] and the ISO 18000 standard [22].

5 RFID protocols for localization privacy

5.1 The RFID tags know the current time and their location

To motivate our application we start with the case when RFID tags have clocks and know their location.

In our first protocol (and the following) the RFID reader shares with each tag a unique secret key k. Let $time_r$ be the time the reader sends its challenge and loc_r the location of the reader (as measured by the reader); and let $time_t$ be the time the challenge was received by the tag and loc_t its location (as measured by the tag).

Protocol 1

Step 1. The RFID reader sends to the tag the challenge:

$$time_r,\ loc_r,\ x = MAC_k(time_r, loc_r).$$

where MAC_k a keyed message authentication code (*e.g.*, OMAC [23]).

Step 2. The tag checks the challenge. If the authenticator x is valid, $|time_t - time_r| < \delta_{time}$ and $dist(loc_r, loc_t) < \delta_{range}$, where $\delta_{time} > 0$, $\delta_{range} > 0$ are appropriate bounds, then the tag responds with

$$y = MAC_k(x).$$

Step 3. The RFID reader checks the response y. If this is valid it accepts the tag (as authentic).

Step 1 of this protocol authenticates the RFID reader to the tag, and can be thought of as the response to a "time and location" query from the environment (a trusted entity that is not under the control of the adversary). The tag only responds if the time the

challenge was sent and the location of the reader are within acceptable ranges related to its own time reading and location. This assures localization privacy. Replay attacks beyond the range of the reader are thwarted by having the location of the reader included in the challenge; replay attacks in the range of the reader (at a later time) are thwarted by having the time the challenge was sent included in the challenge. The tag's response authenticates the tag to the reader, so we have mutual authentication.

The actual location of the tag is determined by analyzing its response in Step 2, *i.e.,* its radio signals using a localization algorithm. Such algorithms determine the source of a transmission by using signal strength and/or direction (triangulation algorithms [39]), or the phase difference [19]. More than one reader will be needed but only one reader needs to broadcast the challenge. The following theorem captures formally the security aspects of our first protocol.

Theorem 1. *Protocol 1 provides mutual authentication with localization privacy for one-time tag interrogation applications against ubiquitous adversaries. For applications where tags may be interrogated several times we only get weak localization privacy.*

Proof. (Sketch) First consider a ubiquitous adversary with one-time tag interrogations. By Assumptions 4 the adversary cannot discover a tag that is already discovered (interrogated). Also, the adversary gains no advantage when the interrogation fails by Assumption 3. If the tag is not present while it is interrogated then the adversary can replay the reader's challenge to other areas where the tag may be. This is thwarted because the challenge contains location information. The only remaining attack is to forge the keyed message authentication code: if a cryptographic hash function is used this is not feasible.

Next consider applications where tags can be interrogated several times, with a local adversary. By Assumption 5 the adversary cannot localize a tag while it is interrogated. However it can replay the challenge of the reader in the same place at a later time: this attack is thwarted because the challenge contains temporal information. If the tag is not in the range of the RFID reader when it is challenged, then the adversary can replay the challenge to other places where the tag may be. This attack is thwarted because the challenge contains location information. Finally forging the message authentication code is not feasible as observed earlier.

We get mutual authentication because the RFID reader is authenticated to the tag in Step 1 and the tag is authenticated to the reader in Step 2. □

Remark 1. In Protocol 1 the RFID reader must send a different challenge to each tag (using the shared key k). If the number of tags is large and the reader does not know the approximate location of each tag (as possibly in the sensor deployment discussed in Section 4) then tag interrogation can be time consuming—the protocol is not scalable. For such applications we may use Public Key Cryptography: the RFID reader authenticates the time and its location with an Elliptic Curve Cryptography (ECC) signature [30]: $sig_{\mathrm{SK}_r}(time_r, loc_r)$, instead of the message authentication code $MAC_k(time_r, loc_r)$. Here SK_r is the private key of the RFID reader. The tag can

verify this using the public key PK_r of the RFID reader. However verifying ECC signatures can be computationally expensive.[7]

5.2 The RFID tags know their location only

In our second protocol the RFID reader shares with each tag a secret key k as well as a counter *ct* which is updated with each interrogation. The reader stores in a database for each tag a pair (k, ct) containing the key and the current value of the counter. The tag stores in non-volatile memory a list (k, ct^{old}, ct^{cur}) containing an old value and the current value of its counter. The stored values at the reader and tag are updated by: $ct \leftarrow next(ct)$ and $ct^{old} \leftarrow ct^{cur}$, $ct^{cur} \leftarrow next(ct^{cur})$, respectively, with the tag's update made only if the value of the received counter ct is the same as the stored value of ct^{cur}, where the operator $next(\cdot)$ gives the next value of the counter. At all times at least one of the two values of the counter of the tag is the same as that stored at the reader. Initially $ct = ct^{old} = ct^{cur}$.

Protocol 2

Step 1. The RFID reader sends to the tag the challenge:

$$ct, loc_r, x = MAC_k(ct, loc_r).$$

Step 2. The tag checks the challenge. If $dist(loc_r, loc_t) < \delta_{range}$, where $\delta_{range} > 0$ is an appropriate parameter, and if x is valid for either $ct = ct^{old}$ or $ct = ct^{cur}$ then it responds with:

$$y = MAC_k(x),$$

and if $ct = ct^{cur}$, sets: $ct^{old} \leftarrow ct^{cur}$ and $ct^{cur} \leftarrow next(ct^{cur})$.

Step 3. The reader checks y. If this is valid then it updates its counter $ct \leftarrow next(ct)$, accepts the tag (as authentic), and sends to the tag,

$$z = MAC_k(y).$$

Step 4. The tag checks z. If this is valid then its sets: $ct^{old} \leftarrow ct^{cur}$.

In this protocol the RFID reader updates its counter after receiving a response from the tag (Step 3). If a response is not received, then the same value of the counter is used the next time. This is why the tag must keep the old value of the counter ct^{old}. This value will only be updated when the interrogation is completed. It follows that at all times, at least one of the values of the counters of the tag is the same as that of the counter of the reader.

Below we shall show that Protocol 2 provides mutual authentication with localization privacy for one-time tag interrogation applications. For applications where a tag

[7] If the tag responds with the message authentication code $MAC_k(time_r, loc_r)$, then we still have a scalability issue (but this time on the search time rather than the number of broadcast challenges): the reader must check the response for all keys k in its database. For one-time interrogation applications, the tag can include its tag ID, or a preassigned pseudonym.

can be interrogated several times we only get weak localization privacy. This is because even though a local adversary cannot discover a tag while it is interrogated by an authorized reader (Assumption 5), it can eavesdrop on the interrogation and later replay the reader's challenge (in the same location) and use a localization algorithm to locate the tag.

Theorem 2. *Protocol 2 provides mutual authentication with localization privacy for one-time tag interrogation applications against ubiquitous adversaries. For applications where tags may be interrogated several times we only get weak localization privacy.*

Proof. (Sketch) As in Theorem 1, a ubiquitous adversary will not succeed while the tag is interrogated, and will not succeed by replaying the reader's challenge to some other areas when the tag is not present during an interrogation, because the challenge contains location and information. Also forging the message authentication code is not feasible. The only remaining attack is to de-synchronize the counters of the reader and the tag. This is not possible because that tag always keeps an old value of the counter, and the counters are only updated when the interrogation is completed.

Next consider applications where tags are interrogated several times and the adversary is local. Again the adversary cannot localize a tag which is interrogated, but can replay the challenge either in the same location (later) or other locations. The first attack is thwarted because the reader and tag have updated their counters; the second because the challenge contains location information. Finally forgery and de-synchronization attacks fail as in the ubiquitous adversary case.

Mutual authentication is as in Theorem 1. □

Remark 2. In Protocol 2, loosely synchronized counters partly capture the functionality of loosely synchronized clocks in Protocol 1. However there is a subtle difference between these protocols. If the adversary in Protocol 2 is allowed to prevent the reader from receiving the tag's response in Step 2 (Byzantine adversaries schedule communication channels) then the reader will abort the session without updating its counter. The adversary may later replay the reader's challenge to localize the tag: since the counter was not updated the tag will respond. This attack is prevented by Assumptions 3,3. Protocol 1 is not subject to this weakness.

5.3 RFID tags know the current time only

In our third protocol the RFID reader shares with each tag a secret key and the reader and tags have loosely synchronized clocks.

Protocol 3

Step 1. The RFID reader sends to the tag the challenge:

$$time_r\ ,\ x = MAC_k(time_r).$$

Step 2. The tag checks the challenge. If $|time_t - time_r| < \delta_{time}$, where $\delta_{time} > 0$ is an appropriate parameter, and if x is valid then it responds with:

$$y = MAC_k(x).$$

Step 3. The RFID reader checks y. If it is valid then it accepts the tag (as authentic).

This protocol does not provide (strong) localization privacy. A ubiquitous adversary can use an online man in the middle attack to relay the flows of the RFID reader to the tag, when the tag is not in range of an authorized reader—unless the tag and reader have highly synchronized clocks. We have:

Theorem 3. *Protocol 3 provides only mutual authentication with weak localization privacy, unless highly synchronized clocks are available.*

Proof. (Sketch) As observed in Section 5.3, a ubiquitous adversary can use an online man in the middle attack to relay the flows of the RFID reader to the tag, when the tag is not in range of an authorized reader—unless the tag and reader use highly synchronized clocks (which is not practical for lightweight applications). The tag will then accept the reader's challenge and respond. So we cannot have localization privacy.

Next consider applications where tags are interrogated several times with a local adversary. Again the adversary cannot localize a tag while it is interrogated by an authorized reader. However it can replay the challenge, later. Replaying it locally will not succeed because the tag will have updated its counter—it will complete its interrogation by Assumption 3. Replaying it to another location will not succeed because the challenge contains temporal information (this is an offline man in the middle attack, so the difference between the send and receive time will be greater than δ_{time}). Finally as in Theorem 2 forgery and de-synchronization attacks will fail and we have mutual authentication. □

Remark 3. Observe that temporal mechanisms in Protocol 3 cannot replace the location mechanisms of Protocol 2. The reason is that online man in the middle attacks on location mechanisms are constrained by the broadcast range of RFID readers (tags can determine their location in this range), while such attacks on temporal mechanisms are constrained by the speed of light (tags can only detect such attacks if they, and the reader, have highly synchronized clocks)—which for most applications is not lightweight.

6 Limitations for RFID localization privacy

6.1 The RFID tags do not know the time or location

Theorem 4. *Localization privacy cannot be achieved when the tags are static if neither temporal nor location information is available to the tags.*

Proof. The proof is by contradiction. Suppose that neither temporal nor location information is available. First consider a ubiquitous adversary. If a tag is not in range of the

RFID reader that challenges it, then the adversary can use an online man-in-the-middle relay attack to forward the reader's challenge to another area of the deployment zone were the tag may be. The tag has no way of checking that the challenge was sent from far away and/or much earlier. So it will respond. This violates localization privacy.

Next consider a local adversary. In this case suppose that the tag is not present during the interrogation. Then the adversary may record the challenge of the RFID reader and replay the challenge later (an offline man in the middle attack). Again the tag has no way of detecting that the challenge was sent from another location earlier, and will respond. □

7 Conclusion

We have shown that for static RFID tags, in the presence of a ubiquitous adversary, localization privacy can be achieved if the tags know either (i) their approximate location (Theorem 1, Part 1; Theorem 2, Part 1), or (ii) the *exact* time (highly synchronized clocks—Theorem 3). In this threat model, localization privacy is restricted to one (complete) interrogation per tag.

For applications that require multiple interrogations per tag, we only get localization privacy for local adversaries (Theorem 1, Part 2; Theorem 2, Part 2; Theorem 3, Part 2)—that is for adversaries whose eavesdropping range is restricted, and this *only if* the tags either know their approximate location or the time (loosely synchronized clocks).

If the RFID tags do not have temporal of location information then we cannot have localization privacy (Theorem 4).

Acknowledgement. The author would like to thank Xiuwen Liux and Zhenghao Zhang for helpful discussions on accurate localization technologies and security issues and Jorge Munilla for helpful comments on the protocols and localization.

References

1. C. Alippi, D. Cogliati, and G. Vanini. A statistical approach to localize passive RFIDs. In *Proc. of the IEEE Int. Symp. on Circuits and Systems (ISCAS)*, pages 843–846, Island of Kos, Greece, 2006.
2. G. Ateniese, J. Camenisch, and B. de Medeiros. Untraceable RFID tags via insubvertible encryption. In *Proc. ACM Conf. on Computer and Communication Security (ACM CCS 2005)*, pages 92–101. ACM Press, 2005.
3. Gidas Avoine. RFID Security and Privacy Lounge. http://www.avoine.net/rfid/, 2010.
4. Gildas Avoine and Philippe Oechslin. A scalable and provably secure hash-based rfid protocol. In *PERCOMW '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 110–114, Washington, DC, USA, 2005. IEEE Computer Society.
5. Paramvir Bahl and Venkata N. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *INFOCOM*, pages 775–784, 2000.
6. Bruce R Barsumian and Thomas H. Jones. U.s patent #6,163,259, dec 19, 2010.
7. M. Brunato and R. Battiti. Statistical learning theory for location fingerprinting in wireless LANs. *Computer Networks*, 47:825–845, 2005.

8. M. Burmester, T. van Le, and B. de Medeiros. Provably secure ubiquitous systems: Universally composable RFID authentication protocols. In *Proceedings of the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006)*. IEEE Press, 2006.
9. Mike Burmester. His late master's voice, barking for location privacy.
10. Mike Burmester and Breno de Medeiros. The Security of EPC Gen2 Compliant RFID Protocols. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, *ACNS*, volume 5037 of *Lecture Notes in Computer Science*, pages 490–506. Springer, 2008.
11. Mike Burmester and Jorge Munilla. Flyweight authentication with forward and backward security. *ACM Trans. Inf. Syst. Secur.*, 12:accepted 8/27/2010, available at http://www.cs.fsu.edu/ burmeste/103.pdf, 2011.
12. H.-L. Chang, J.-B. Tian, T.-T. Lai, H.-H. Chu, and P. Huang. Spinning beacons for precise indoor localization. In *ACM Third International Conference on Embedded Networked Sensor Systems (SenSys 08)*, November 2008.
13. S. Coco, A. Laudani, and L. Mazzurco. A novel 2-d ray tracing procedure for the localization of em field sources in urban environment. *IEEE Transactions on Magnetics*, 40(2):1132–1135, 2004.
14. George Danezis, Stephen Lewis, and Ross Anderson. How Much is Location Privacy Worth? Fourth Workshop on the Economics of Information Security (WEIS 2005). Harvard University, 2/3 June 2005.
15. Tassos Dimitriou. A secure and efficient RFID protocol that can make big brother obsolete. In *Proc. Intern. Conf. on Pervasive Computing and Communications, (PerCom 2006)*. IEEE Press, 2006.
16. EPC Global EPC tag data standards, vs. 1.3. http://www.epcglobalinc.org/standards/ EPCglobal_Tag_Data_Standard_TDS_Version_1.3.pdf.
17. S. J. Fortune, D. M. Gay, B. W. Kernighan, O. Landron, R. A. Valenzuela, and M. H. Wright. Wise design of indoor wireless systems: practical computation and optimization. *IEEE Computational Science & Engineering*, 2(1):58–68, 1995.
18. D. Hahnel, W. Burgard, D. Fox, K. Fishkin, and M. Philipose. Mapping and localization with rfid technology. In *in Proceedings of IEEE International Conference on Robotics and Automation*, pages 1015–1020, 2004.
19. Cory Hekimian-Williams, Brandon Grant, Xiuwen Liu, Zhenghao Zhang, and Piyush Kumar. Accurate localization of rfid tags using phase difference. In *2010 IEEE International Conference on RFID*, RFID 2010, pages 89–96. IEEE, 2010.
20. D. Henrici and P. M. Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *Proc. IEEE Intern. Conf. on Pervasive Computing and Communications*, pages 149–153, 2004.
21. His Master's Voice. http://en.wikipedia.org/wiki/His Master's Voice.
22. ISO/IEC. Standard # 18000 – RFID Air Interface Standard. http://www.hightechaid.com/standards/18000.htm.
23. Tetsu Iwata and Kaoru Kurosawa. Omac: One-key cbc mac. In Thomas Johansson, editor, *FSE*, volume 2887 of *Lecture Notes in Computer Science*, pages 129–153. Springer, 2003.
24. D. Joho, C. Plagemann, and W. Burgard. Modeling RFID signal strength and tag detection for localization and mapping. In *Proceedings of the IEEE International Conference on Robotics and Automation (ICRA)*, pages 3160–3165, Kobe, Japan, May 2009.
25. Thomas H. Jones and Bruce R Barsumian. U.s patent #6,057,765, may 2, 2010.
26. A. Kleiner, C. Dornhege, and S. Dali. Mapping disaster areas jointly: RFID-coordinated SLAM by humans and robots. In *Proc. of the IEEE Int. Workshop on Safety, Security and Rescue Robotics (SSRR)*, 2007.

27. Branislav Kusy, Akos Ledeczi, and Xenofon Koutsoukos. Tracking mobile nodes using rf doppler shifts. In *SenSys '07: Proceedings of the 5th international conference on Embedded networked sensor systems*, pages 29–42, New York, NY, USA, 2007. ACM.
28. Branislav Kusy, Janos Sallai, Gyorgy Balogh, Akos Ledeczi, V. Protopopescu, J. Tolliver, F. DeNap, and M. Parang. Radio interferometric tracking of mobile wireless nodes. *In Proc. of MobiSys*, 2007.
29. Akos Ledeczi, Peter Volgyesi, Janos Sallai, Branislav Kusy, Xenofon Koutsoukos, and Miklos Maroti. Towards precise indoor rf localization. In *HOTEMNETS'08*, Charlottesville, VA, June 2008.
30. Yong Ki Lee, Lejla Batina, Dave Singelee, Bart Preneel, and Ingrid Verbauwhede. Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware. In Ahmad-Reza Sadeghi and David Naccache, editors, *Towards Hardware-Intrinsic Security, Information Security and Cryptography – THIS 2010*, pages 237–257. Springer, November 2010.
31. B. Li, J. Kam, J. Lui, and A. G. Dempster. Use of directional information in wireless lan based indoor positioning. In *IGNSS Symposium 2007*, 2007.
32. Ling Liu. From data privacy to location privacy: models and algorithms. In *Proceedings of the 33rd international conference on Very large data bases*, VLDB '07, pages 1429–1430. VLDB Endowment, 2007.
33. David Madigan, Eiman Elnahrawy, Richard P. Martin, Wen-Hua Ju, P. Krishnan, and A. S. Krishnakumar. Bayesian Indoor Positioning Systems. In *Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 2, pages 1217–1227, 2005.
34. Miklos Maroti, Branislav Kusy, Gyorgy Balogh, Peter Volgyesi, Karoly Molnar, Andras Nadas, Sebestyen Dora, and Akos Ledeczi. Radio interferometric geolocation. In *ACM Third International Conference on Embedded Networked Sensor Systems (SenSys 05)*, pages 1–12, San Diego, CA, November 2005.
35. David Molnar, Andrea Soppera, and David Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In *Proc. Workshop on Selected Areas in Cryptography (SAC 2005)*, volume 3897 of *LNCS*. Springer, 2006.
36. X. Nguyen, M. Jordan, and B. Sinopoli. A kernel-based learning approach to ad hoc sensor network localization. *ACM Transactions on Sensor Networks*, 2005.
37. Lionel M Ni, Yunhao Liu, Yiu Cho Lau, and Abhishek Patil. LANDMARC: Indoor Location Sensing Using Active RFID. *ACM Wireless Networks*, 10(6):701–710, 2004.
38. M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic approach to "privacy-friendly" tags. In *Proc. RFID Privacy Workshop*, 2003.
39. J.L. Poirot and G.V. Mcwilliams. Navigation by back triangulation. *IEEE Transactions on Aerospace and Electronic Systems*, AES-12(2):270–274, 1976.
40. T.S. Rappaport. *Wireless Communications - Principles & Practice, 2nd Edition*. Prentice Hall PTR, 2003.
41. RFIDNews. EarthSearch launches GPS-RFID hybrid solution. http://www.rfidnews.org/2009/03/16/earthsearch-launches-gps-rfid-hybrid-solution.
42. Janos Sallai, Akos Ledeczi, Isaac Amundson, Xenofon Koutsoukos, and Miklos Maroti. Using rf received phase for indoor tracking. *HotEmNets*, June 2010.
43. V. Seshadri, G. V. Zaruba, and M. Huber. A Bayesian sampling approach to in-door localization of wireless devices using received signal strength indication. In *Proc. of the IEEE Int. Conf. on Pervasive Computing and Communications (PerCom)*, pages 75–84, 2005.
44. S. E. Sharma, S. A. Weiss, and D. W. Engels. RFID systems and security and privacy implications. In *Proc. of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 20002)*, volume 2523 of *LNCS*, pages 454–469. Springer, 2003.

45. A. Tayebi, J. Gomez, F. Saez de Adana, and O. Gutierrez. The application of ray-tracing to mobile localization using the direction of arrival and received signal strength in multipath indoor environments. *Progress In Electromagnetics Research*, 91:1–15, 2009.
46. T. van Le, M. Burmester, and B. de Medeiros. Universally Composable and Forward-Secure RFID Authentication and Authenticated Key Exchange. In *Proc. of the ACM Symp. on Information, Computer, and Communications Security (ASIACCS 2007)*, pages 242–252. ACM Press, 2007.
47. WISP. Wireless Identification and Sensing Platform, Intel Labs, Seattle. http://seattle.intel-research.net/wisp/.
48. M. Youssef and A. Agrawala. The horus WLAN location determination system. In *MobiSys*, pages 205–218, 2005.
49. Ting Zhang, Zhenyong Chen, Yuanxin Ouyang, Jiuyue Hao, and Zhang Xiong. An Improved RFID-Based Locating Algorithm by Eliminating Diversity of Active Tags for Indoor Environment. *The Computer Journal*, 52(8):902–909, 2009.
50. Y. Zhao, Y. Liu, and L.M. Ni. Vire: Active rfid-based localization using virtual reference elimination. In *Proceedings of ICPP*, 2007.
51. J. Zhou and J. Shi. RFID localization algorithms and applications, a review. *Journal of Intelligent Manufacturing*, pages 1–13, 2008.