Protecting the privacy of passive RFID tags

Nimish Vartak, Anand Patwardhan, Anupam Joshi, Tim Finin, Paul Nagy*
Department of Computer Science
and Electrical Engineering
University of Maryland, Baltimore County
Email: {nimishv1, anand2, joshi, finin}@cs.umbc.edu, pnagy@umm.edu

***Abstract*— Radio Frequency Identification (RFID) is an emerging wireless technology with many potential applications, including supply chain management, personnel tracking and point of sale checkout. Its wide spread adoption raises concerns about known security and privacy vulnerabilities, including the ability of rogue RFID readers to access the unique identifier and data of RFID tags. To prevent the eavesdropping of tag through communication channel, methods like one-way hashing, cryptography and one-time pads have been used; however they do not prevent the clandestine tracking of tags using their unique identifier. We describe a novel scheme to protect the identity of tags, and prevent them from being clandestinely tracked and inventoried.**

Our approach uses inexpensive passive RFID tags, an RFID reader, an authenticating agent, and a local entity that can dynamically reprogram tags to protect their identity. We ensure visibility of goods to authorized RFID readers at any point in the transit of RFID tagged goods from one location to another, while denying information to unauthorized readers. The approach protects the identity of the RFID tags without significant changes to the existing infrastructure and obviates the need for expensive active RFID tags. We present our scheme in the context of a transit vehicle like a truck which carries RFID tagged goods from one place to another.

I. Introduction

Although RFID can best be described as a technology in its nascent stage, it is already becoming pervasive. Due to strong capabilities of non-line-of-sight operation and unique identification for an item, it is extensively deployed for purposes of tracking items. From the supply chain management perspective, RFID ensures traceability of goods from manufacturing through sale and even beyond it. EPC Global Inc. has developed the EPC Global Network [1] which has services to uniquely identify any RFID tagged item, and get the tag information. The tag's unique identifier acts as a pointer to the item's details in a secure database. The database security and access controls do not however prevent the item from being tracked by an adversary based solely on its unique ID. The RFID tag's unique identifier typically is a key in database tables which hold more details of the item. Instead of trying to compromise the database access controls, an adversary could find alternate means to determine the details of the tags. RFID readers are easily available e.g. in certain cell phones [2]. Hence it is possible for an adversary to read the RFID tag and correlate its time and place to learn more about the tag. Tracking a tag bearer is possible today with many leading clothing manufacturers [3] and shipping companies [4] using RFID tags. This problem of clandestine tracking [5] is not overcome even if another (unrelated) identifier is stored onto the tag, so long as the identifier remains static. The privacy problem gets more complicated if the tag itself holds details of the item like the price. An adversary may eavesdrop on a genuine reader-tag communication including the singulation[1] [6] protocol. A variety of schemes have been proposed to protect this communication. These include encryption mechanisms [7], hashing [8], and use of one-time pads [9]. The problem is more aggravated for basic passive (identity EPC class 1 [9]) RFID tags, as a basic interrogation of a RFID tag by an RFID reader may be sufficient to reveal this unique identifier. Although the most recent specification of the EPC Class 1, Generation 2 [9] specifies access-control mechanisms for tags; the access control is meant for the ability to write or kill a tag but does not prevent a tag from being read.

To solve this problem of unauthorized read access, ideally each tag should be capable of computation and be able to choose whether or not to identify itself, requiring credentials from the interrogating RFID reader. Further, a tag could possibly reveal different granularity of information to each reader, by say masking off bits of the identifier. However, this requires considerable computation capability on part of the tag, which common and inexpensive tags lack. Since such a solution using expensive active tags would not be economically viable, our focus is on using existing technology and passive tags. We introduce a local entity to enforce the security for tags in the vicinity, ensuring information availability to only authorized entities. We explain our scheme in

[1]Singulation is defined as "Identifying an individual tag in a multiple-tag environment" by EPC Global Inc.

context of securing the identity of valuable items in transit. While the EPC Global Network caters largely to supply chain management as a whole, we concentrate on protecting the privacy and preventing clandestine tracking of the RFID tagged goods in transit. We design a scheme to dynamically change the RFID tag identifier and maintain information in a secure and distributed manner. We ensure that an authorized reader can have access to information about the tag, at any point in transit. The remainder of the paper is organized as follows: Section II gives the background and related work for the paper, Section III describes our approach, followed by Section IV which details our design. Sections V and VI detail the feasibility of the mechanism and the security aspects involved. We describe our future work and conclusions in sections VII and VIII.

II. Background and Related Work

To secure our privacy preserving scheme, we need to secure the RFID reader-tag communication and require a mechanism to uniquely identify each tag. In terms of identifying the tag uniquely and from an architectural perspective as well, we compare our scheme with the EPC Global Network [1]. EPC Global Inc. provides a mechanism to weave in all the RFID tagged items into a single integrated world. Though the EPC Network is able to identify the goods uniquely, it does not provide explicit mechanisms for protecting goods in transit from being clandestinely tracked. Further, it provides for inventory management at pre-defined or static locations only. Our scheme ensures the visibility of goods to authorized entities at any point in transit.

With respect to the security of the reader-tag communication, various methods for protecting tag identity have been proposed as discussed below. We look at the most light weight solution from cryptography [7], or hashing [8]. EPC Class 1 Generation 2 [9] requires the use of one-time pads for communication with the tags. Public cryptography involving re-encryption using a single public-private key pair [10] and Universal re-encryption [11] (with limitations) have been suggested; however our scheme involves a large number of keys used on a temporal basis as we re-encrypt the original tag identifier with a different key (or key pairs) over a period of time. Our work is different from Ateniese et al. [12], who provide a solution based on randomization without the use of a Local entity to enforce privacy. The Authenticating Agent, unlike the Mobile Agents mentioned in [13] is located at the transit headquarters and is an authentication server.

III. Our Approach

A. Design Objectives and Focus

The aim of our scheme is protect the identity of tags, and prevent them from unauthorized access, without hampering their visibility to authorized readers. Our design objectives include:

1) To prevent the RFID tag identifier from unauthorized access
2) To ensure integrity of the RFID tag identifier
3) To provision for tracking at any point in transit
4) To provide different levels of access to information about a RFID tag
5) To provide flexibility to Dispatcher of goods to choose a privacy policy for tags (and possibly update it)

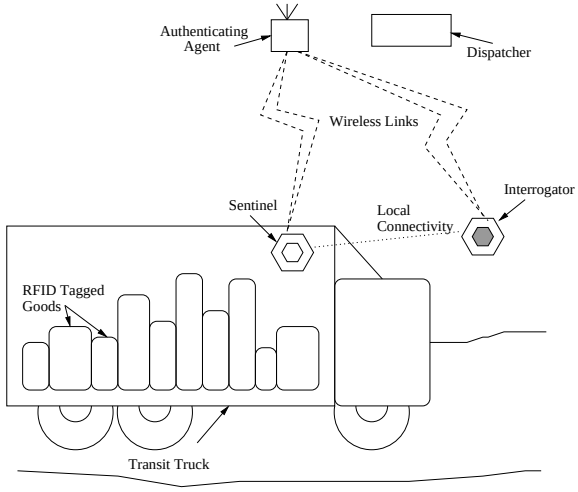

Fig. 1. Auth. Agent and Sentinel collaborate to give an authorized Interrogator access to tag identifiers

Using a local entity (the Sentinel) and an Authenticating Agent, we provide the access control which would otherwise require custom manufactured expensive tags. We note that our scheme is suited for applications like tracking of shipments, and we consider a threat model where an adversary seeks to clandestinely track the items in transit, but assume physical security of the truck and its contents.

B. Assumptions

We are concerned with the security of the RFID communication and hence assume secure channels of communication (like wireless links/local communication) in the scenarios we describe. Similarly, we assume the physical security of the devices involved, like an intruder not being able to have physical access to the contents of the truck and other entities as well. We

assume that the RFID tag reprogramming events are timed so as not to interfere with the read attempts of authorized RFID readers.

IV. Proposed Design

A. Entities

Our scenario involves the following entities - the Sentinel which travels with the transit truck, the Authenticating Agent which is the central authority, the Interrogator which wants to identify goods and finally the Dispatcher which has dispatched the goods. As shown in Fig 1, the Sentinel and Authenticating Agent share the responsibility of protecting the identity of RFID tags. A Sentinel is an RFID reader on board the truck, which can store a number of keys to encrypt tag identifiers and has the ability to write the tag identifiers on the items being transported. The Authenticating Agent is an authority which issues cookies, and can issue keys using Public Key Infrastructure or can be like a Kerberos server. It maintains a record of keys/cookies it has issued. Further, it has details of all tags, including their original identifiers and their respective passwords. An Interrogator may be a genuine entity like a customs officer, or may be a thief planning to steal expensive items off the truck, hence wants to know the identity of tags. The Dispatcher decides on the level of detail to be revealed to different interrogators, thus deciding the privacy policy in use at the Authenticating Agent. We note that each entity, during its interaction verifies others' identity using credentials such as certificates, and interaction occurs over a secure channel.

B. Overview of Interaction

The steps an Interrogator follows to learn the identity of the RFID tags on board the transit truck are illustrated by Fig 2. The Interrogator reads the encoded RFID tags, but cannot understand the tag identity, hence communicates with the Authenticating Agent and gets cookies for the tags. On presenting these cookies to the Sentinel, it is issued decrypting keys to compute the original tag identifier. The Authenticating Agent is the final authority which gives (possibly different levels of) information about the item from its identifier to the Interrogator.

C. The Protocol

Our protocol has encryption at tag level. We are not bound to any specific implementation, we can choose from any method (symmetric/asymmetric) of encryption, or one way hashing of tags scheme which permits individual encoding and decoding of tags. The security protocol shown by the dashed lines in Fig 2 involves the Sentinel connecting to the Authenticating Agent over

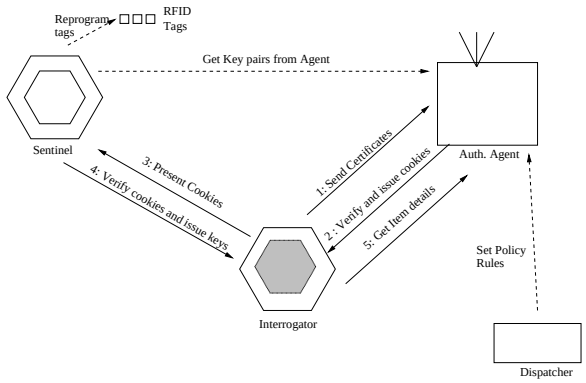

Fig. 2. Interrogator communication with the Authenticating Agent and Sentinel to learn the tag identifiers

periods of time to request keys. The Authenticating Agent generates a large number of keys (or key pairs), and issues a new set of keys to a requesting Sentinel at each request. The query protocol (shown by solid lines) involves an interrogator attempting to learn item details. The Interrogator is in proximity of the tags and reads them. However, the Interrogator cannot identify items as they have been encrypted by the Sentinel. The Interrogator is directed to the Authenticating Agent (preprogrammed or could be learned from the Sentinel via local connectivity). The Interrogator supplies its credentials and information about tags it wishes to identify. After verifying certificates and checking Interrogator access privileges for the tags, the Authenticating Agent issues access in form of cookies to the Interrogator. An additional level of security is added by the Sentinel being the entity that issues decrypting keys to the Interrogator. The Interrogator can now track the tag until the tags are reprogrammed by the Sentinel. The Interrogator uses the decryption keys to obtain the original tag identifier. As the final step in the interaction, the Interrogator communicates with the Authenticating Agent to get tag details. The Authenticating Agent can use a policy-based mechanism (as chosen by the dispatcher) to reveal tag details. Note that cookies expire with time, and the Interrogator will have to repeat the query protocol to get decrypting keys or tag details.

V. Feasibility Study

We look at the implementation aspects of the protocol. The requirements of our system in terms of RFID can be listed as follows:

1) Ability to uniquely identify a single tag
2) Ability to rewrite a particular tag with a new identifier
3) Authorized write mechanism

We explain the feasibility considerations for all the above scenarios. Uniquely identifying a single tag is also known as Singulation. Variations of a binary tree walking protocol like Silent Binary-Tree Walking [14] or Randomized PRF Tree Walking Algorithm [15] can be used to singulate a tag in addition to any proprietary protocol implemented by the RFID vendors. We compare the solutions offered by two leading vendors of passive RFID systems. Rewrite of a particular tag with a new identifier is possible in EPC Class 1 Generation 2 [9]. In previous implementations, while one vendor allows to selectively erase a tag in a group of tags, while the other simply overwrites all tags in range with the new identifier. For the authorized write mechanism, we note that EPC Class 1 Generation 2 [9] provides access controls in form of a password to modify the tag's data. For previous implementations, we could either have custom modification to the tag by which it allows a write only on being supplied the password, or we alternatively design a work-around for the same. Some vendors implement variants of this mechanism in prior implementations. One vendor offers support for locking tags with a specific password, which means that the data on the tag cannot be replaced, until the tags are reprogrammed (or killed[2]) using the password to reset its data and subsequently writing new identifier onto the tag.

The following factors contribute to the timing characteristics of the proposed system:

1) Encoding methods for tag identifiers
2) Tag reprogramming
3) Communication delays

Depending on the method chosen for encoding tag identifiers, like encryption (including symmetric encryption or asymmetric encryption) or hashing (which involves lookup for values in a hash table), the complexity and consequently the time required for calculating the new tag identifier changes. Besides the computing overhead, the time required for an actual write to the tag needs to be accounted for. This includes the time required by an RFID reader to singulate a particular tag to write to it. Our preliminary experiments we noticed an increase in write time for a single tag from 100 ms to order of 500 ms when a group of tags is present. We attribute this to singulation protocol followed by the device. We consider re-programming of tags be feasible, so long as we limit the number of tags in the transit vehicle. Communication delays exist in terms of access time via the communication media. Such communication with a central server is possible as exemplified by GE VeriWise Asset Intelligence system [16]. Further, our protocol has a security parameter that defines the length of the encryption key(s) and the time interval for reprogram of a tag.

[2]Some vendors prior to Generation 2 erase the tag memory, but permit subsequent tag reuse after a 'kill' of the tag.

VI. Security Analysis

We note that our scheme is deployed only while the goods are in transit. When items are dropped off (to say the storage depot), the original tag identifier is written back to the tag and the sentinel conveys this information back to the Authenticating Agent. This enables the items to be uniquely identified in using the EPC Global tag identification mechanism in the storage. Similarly, if the items are being loaded onto another truck, the Sentinel of that transit truck now takes the ownership of this item, and reprograms its identifier. We have assumed the physical security of the truck and hence the Sentinel and the items. If the Sentinel were to go offline for some reason, like running low on batteries, the Authenticating Agent learns of it, since the Sentinel fails to request the new set of keys at the next time interval. Note that the Authenticating Agent knows the set of keys which it last issued to the Sentinel, hence it programs a new Sentinel with the passwords and the set of keys. The trade-off being that the new Sentinel needs to try different key combinations before it can match the exact tag identifiers.

A. Resilience to Attacks

We consider the impact of different kinds of attacks on the system. In terms of RFID entities, these attacks include attempts by adversaries to write to tags, copying data off tags, possibility tampering tag data and spoofing tags, while from computation perspective attacks include access to multiple keys. A swapping attack on the data identified in [5] would be one in which an Interrogator swaps the EPC identifiers on the RFID tags. We rule out this attack since we assume that only the Sentinel can write the data back to the tags (assuming the existence of password protected write for the tag). Further, since the communication is secure, by using encryption or one-time pads, eavesdropping does not reveal the password or the tag identifier. Our scheme similarly does not suffer from the problem of re-encryption (in which the original identifier may get corrupted), since the decoding keys are used to retrieve the original identifier before re-encrypting it. Copying of tag data off the tag does not constitute an attack since its temporal and encrypted. The truck being physically secure, no unauthorized entry or exit of goods (with possible fake or duplicate identifiers) is possible. Although a rogue reader cannot write a tag without knowing the password, if a rogue reader hacks a tag to retrieve the password using side-channel attacks as described by Shamir et al. in [17], a rogue

reader may overwrite or corrupt the tag data. This is a Denial-of-Service attack on in which adversary actually learns nothing about the tags, but prevents the Sentinel from following its reprogram protocol, and hence can be detected. Similarly, in the computational aspect, an Interrogator having access to multiple keys also does not pose a threat. This is because each key matches just one tag and interrogator cannot get any useful information about any other tag and the temporal nature of keys thwarts reverse-engineering attempts on a set of keys. As stated earlier, if a Sentinel fails to communicate with the Authenticating Agent due to channel disruption or any other causes, it can be detected by the Authenticating Agent.

B. Shortcomings

We assume that attacks on physical security of the transit vehicle or the contained RFID tags are not possible, and further our system cannot defend against an attack involving use of "Radio finger-prints" of RFIDs as mentioned in [18], or attacks that disrupt RFID communication. A possible attack which a rogue interrogator could mount is Denial of Service attack on the Authenticating Agent by flooding it with invalid requests. When a large number of trucks (and hence sentinels) are involved, the Authenticating Agent could become a bottleneck and hence a central point of failure. We can provide a hierarchy of Authenticating Agents, similar to the Domain Name Service infrastructure. For an extreme case in which an adversary continually copies (and updates on every reprogram cycle) all tag identifiers and reprograms fake goods on another truck, we would need a separate method by which we can tell the two trucks apart.

VII. Future Work

In the future, we would try to make the system more intelligent by making the Sentinel context-aware, and equipping it with a GPS system to monitor the movement of the truck. The Authenticating Agent could also have an ontology based system to help if identify the various interrogators to learn their access levels. From a data mining perspective, the Authenticating Agent could maintain a log of all the interactions of the Sentinel en route and use it to find trends in the entities encountered, and perhaps suggest an alternative route for the transit.

VIII. Conclusion

With RFID rapidly becoming a pervasive technology, the security and privacy considerations of RFID tags are paramount. With commodities as varied as bank notes, airport luggages, clothing items, the privacy aspects of each system need to be individually addressed. For example, it may not be advisable to allow writes to RFID tags like those on E-Z Pass [19], or bank notes. We presented a solution for ensuring the privacy of a group of RFID tagged items while in transit to their destination. Our scheme can be deployed without any changes to the existing EPC Class 1 protocol and can be integrated with the EPC Global Network [1].

References

[1] EPC Global Inc., "The EPCglobal Network:Overview of Design, Benefi ts, & Security." urlwww.epcglobalinc.org/news/EPCglobal Network Final 09 24 004 Final.pdf.

[2] "Nokia 5140 RFID Reader." url-http://www.mobilemag.com/content/100/104/C2607.

[3] Marks and Spencers, "Background to Marks & Spencer's business trial of RFID in its clothing supply chain." urlhttp://www2.marksandspencer.com/thecompany/mediacentre/pressreleases/2005/com2005-02-18-00.shtml.

[4] "UPS Pressroom: Fact Sheets." url-http://www.pressroom.ups.com/mediakits/factsheet/0,2305,1202,00.html.

[5] A. Juels, "RFID Security and Privacy: A Research Survey," in *IEEE Journal on Selected Aread In Communications, Vol. 24, No. 2*, pp. 381–394, 2006.

[6] RSA Security Inc., "Technical Characteristics of RFID,"

[7] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," in *Proc. Cryptographic Hardware and Embedded Systems 2004 - 6th Int. Workshop*, pp. 201–212, 2004.

[8] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identifi cation Systems," in *Security in Pervasive Computing: 1st Int. Conf., Germany*, pp. 201–212, 2004.

[9] EPC Global Inc., "EPC RFID Class-1 Generation-2 UHF RFID Protocol 860 MHz - 960 MHz." url"http://www.epcglobalinc.org.

[10] A. Juels and R. Pappu, "Squealing Euros: Privacy protection in RFID-enabled banknotes," in *Proc. Financial Cryptography, R.Wright, Ed. New York: Springer-Verlag, vol. 2742, LNCS*, pp. 103–121, 2003.

[11] P. Golle, M. Jakobsson, A. Juels, , and P. Syverson, "Universal re-encryption for mixnets," in *Proc. RSA Conf. -Cryptographers Track (CTRSA), T. Okamoto, Ed., vol. 2964, LNCS*, pp. 163–178, 2004.

[12] G. Ateniese, J. Camenisch, and B. de Medeiros, "Untraceable RFID Tags via Insubvertible Encryption," in *Proceedings of ACM Conference on Computer and Communication Security*, pp. 92–101, 2005.

[13] I. Satoh, "Linking Physical Worlds to LogicalWorlds with Mobile Agents," in *Proceedings of the 2004 IEEE Intl. Conf. on Mobile Data Management*, pp. 332–343, 2004.

[14] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identifi cation Systems," in *D. Hutter et al. (Eds.): Security in Pervasive Computing (LNCS 2802)*, pp. 201–212, 2003.

[15] L. Bolotnyy and G. Robins, "Randomized pseudo-random function tree walking algorithm for secure radio-frequency identifi - cation,"

[16] "Veriwise asset intelligence." urlhttp://www.geveriwise.com.

[17] "Epc tags subject to phone attacks." url-http://www.rfi djournal.com/article/articleview/2167/1/1/.

[18] G. Avoine and P. Oechsli, "RFID Traceability: A Multilayer Problem," in *IFCA, Financial Cryptography, Pre-Proceedings version*, 2005.

[19] "E-Z Pass." urlhttp://www.ezpass.com/.