Achieving Privacy and Security in Radio Frequency Identification

Aaditeshwar Seth and Mirza Beg

School of Computer Science
University of Waterloo, Canada
{a3seth, mbeg}@cs.uwaterloo.ca

Abstract

Radio Frequency Identification RFID *systems are gaining popularity in a wide variety of applications like asset tracking, personnel identification, and sensor networks. However, unique security and privacy issues arise in these systems because low computation capabilities of* RFID *tags prevent the use of complicated cryptographic protocols, and wide deployment of tags opens up room for illegal tracking of people and objects. In this paper, we first describe a basis-set of requirements that need to be necessarily satisfied to mitigate security and privacy problems in* RFID *systems. We then outline some recent proposals that try to solve these issues, and then explore in detail a research publication by Molnar, et al [1] that uses a pseudonym based tree walking security scheme, and claims to meet all the requirements. However, we identify some attacks that are still possible in this scheme in slightly different threat models, and then extend the scheme to mitigate these attacks. We also address the issue of secure establishment of session keys to exchange information between tags, readers, and centralized trusted centers, which had not been proposed earlier. Our extensions make the overall scheme complete, and provides a comprehensive solution to security and privacy issues in* RFID *systems that meets all the requirements in the basis-set.*

1 Introduction

Radio Frequency Identification (RFID) systems have gained immense popularity during recent years. The motivation behind the pervasive use of RFID systems is the need to fully automate remote tracking and identification of objects by embedding cheap and low power RFID tags in the objects. The data transmitted by the tag may contain identification or location information, or specifics about the product being tagged, such as price, color, date of purchase, etc. In addition to the capabilities of the passive tags described above, active tags may have an internal power source and some computational capability, which increases their 'read range' and allows for simple cryptographic computations. Other than the use of RFID tags for keeping tabs on people, pets, products, and vehicles, their use is even being extended to drivers licences, national identification cards, passports [3,5], and also bank notes [10]. However, the RFID technology is rife with problems related to security and privacy. Some of these issues are explained in [4, 6, 11], and outlined below.

- **Surveillance of individuals and objects:** RFID tags are likely to be embedded into objects and documents with or without the knowledge of the individual. As radio waves travel easily and silently through fabric, plastic, and other materials, it is possible to read RFID tags sewn into clothing or affixed to objects contained in purses, shopping bags, or suitcases making it possible to track the location of items or the owner.

- **Massive data aggregation:** The Electronic Product Code (EPC) [9] potentially enables every object on earth to have its own unique ID. The use of unique ID numbers could lead to the creation of a global databases in which every physical object is identified and linked to its purchaser or owner at the point of sale or transfer. These records can be linked with personal identifying data and can be later used for different objectives such as identifying consumer habits without consent of the consumer.

- **Forgery:** Tags can potentially be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate. This information can potentially be used to clone tags and forge identification documents such as passports and licences for various nefarious purposes.

1.1 Our contributions

In this paper, we describe a basis-set of requirements that should necessarily be met in order to deal with the attacks mentioned above. We then survey research on security and privacy issues in RFID systems and explore in detail the protocol by Molnar, et al [1]. We look at scenarios in which the protocols fail to meet the basis-set of requirements, and propose enhancements on how to improve the scheme to make it secure. More specifically, the protocol fails to handle a clone attack between two consecutive reads of the tag. It also fails to secure the tag from a DoS attack which can render the tag unusable. We present enhancements to the protocol to successfully prevent both the above mentioned attacks. In addition to that, we also present techniques to provide secure and authenticated communication in cases where the tags must transfer information to the reader when RFID tags are used in sensors. Also we propose a scheme to renew the key of a tag when it is about to expire. In all, our extensions provide a complete RFID scheme that meets all the security and privacy goals in the basis-set.

2 Basis set of goals for security and privacy in RFID systems

We see that attacks can be made in RFID systems due to violations in one or more of the following basis set of requirements:

1. **Tag authentication:** This is required to prevent tag cloning because duplicated tags can lead to impersonation attacks. Cloning attacks on unprotected or weakly-protected tags can be conducted if any of the following are possible.

   (a) An adversary is able to overhear transmission from valid tags, and replay the transmissions when it is queried by a tag reader.

   (b) If security mechanisms are built such that direct replay attacks are not possible, an adversary is able to reproduce the response of a valid tag by collecting enough information from compromised tags to be able to break the security scheme.

2. **Privacy:** This is required to prevent movement tracking of RFID tagged items. Privacy can degrade if any of the following are possible.

   (a) Adversary readers are able to pretend to be valid readers and query tags to obtain their IDs. Over time, colluded readers are able to track the movement of tags in physical space.

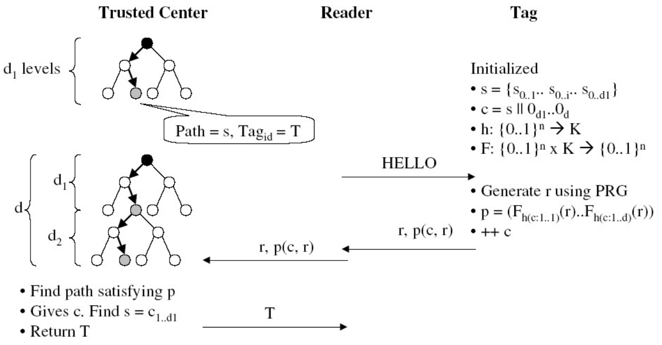
   (b) If IDs are not transmitted as such but are encoded through some security mechanisms, eavesdroppers are able to disambiguate between different tags based on the uniqueness properties of communication arising from different tags. Since eavesdroppers are able to uniquely identify the tags, over time colluded eavesdroppers can then track the movement of tags.

Our goals in this paper are to design a security mechanism that can meet the requirements stated above without involving any high cost cryptographic procedures that cannot be implemented on RFID tags.

3 Related work

Ohkubo et al [7] propose a method of changing RFID ID's on each read using pseudonyms. The drawback of this scheme is that it does not mutually authenticate the reader and the tag.

Juels [8] proposes a security model for low-cost passive tags. The model assumes that the adversary comes into close proximity of the tag only on a periodic basis, and it puts a cap on the number of times that the tag can be read before going into *private* mode during which it can only be read by an authentic reader. This however, requires the tag to be refreshed at frequent intervals, and leaves it vulnerable to attacks during the intermediate phases.



Trusted Center
Reader
Tag
d_1 levels
Path = s, Tag_{id} = T
d
d_1
d_2
Initialized
• s = {$s_{0..1}$.. $s_{0..i}$.. $s_{0..d1}$}
• c = s || 0_{d1}..0_d
• h: $\{0..1\}^n \rightarrow K$
• F: $\{0..1\}^n \times K \rightarrow \{0..1\}^n$
HELLO
• Generate r using PRG
• p = ($F_{h(c:1..1)}$(r)..$F_{h(c:1..d)}$(r))
• ++ c
r, p(c, r)
r, p(c, r)
• Find path satisfying p
• Gives c. Find s = $c_{1..d1}$
• Return T
T

Figure 1. Basic protocol

Molnar et al [1] propose a key pre-distribution scheme for the tags that claims to handle all the issues with the schemes enumerated above. We explain the scheme in detail in Section 4. However, we find that the scheme fails in certain attack models which we discuss in this paper, and we propose some extensions to the scheme in Section 5 to mitigate the attacks.

4 Scalable, delegatable, pseudonym protocol [1]

The authors have defined an RFID *pseudonym* protocol in [1] where the tag emits a different pseudonym each time it is queried by a tag reader. The tag reader cannot decipher the identity of the tag from the pseudonym alone. It queries a TC (Trusted Center) which maps the pseudonym to the tag ID and returns the ID to the reader. Privacy is ensured because (a) only trusted readers are allowed to query the TC, and (b) an eavesdropper cannot disambiguate between any two pseudonyms to determine whether it was the same tag that emitted both the pseudonyms or not. Through an interesting tree-walk algorithm, the protocol is also able to provide ownership transfer primitives and time-limited delegation to offline readers.

4.1 Protocol

Fig. 1 shows the operations of the protocol. Each tag maintains a state variable *c* instead of its ID. The prefix of *c* is unique for each tag however, and the TC maintains a mapping between the unique prefix and the tag ID. Based on *c* and a pseudo-random variable *r*, the tag generates a unique pseudonym *p* in response to each HELLO message from a reader. The reader forwards *p* and *r* to the TC, which is able to recalculate *c* given *p* and *r*. The TC then finds the tag ID based on the unique prefix of *c*, and returns it to the reader. At the same time, the tag increments *c* upon each transaction.

When bootstrapping a new tag, the TC assigns a unique identifier *s* to each tag. This identifier may be the same as the tag ID, or mappings of (*s*, ID) can be maintained locally in a database. As shown in Fig. 1, *s* corresponds to an ordered traversal [1] in a binary tree of height d_1 from the root to a unique leaf node. This is done as follows. The integer *s* is represented in binary, with a 0 denoting the left branch and 1 denoting the right branch. Thus, each path in a tree from the root to a leaf node at level d_1 corresponds to a unique integer *s*. The protocol works by extending this tree by an additional d_2 levels, where each value of *c* corresponds to an ordered traversal up to a node in the tree between levels d_1 and d_2. The first d_1 bits prefixing *c* are equal to *s*. The value of *c* for each tag is incremented from $(s_0 ... s_{d_1}||\{0\}^{d_2})$ to $(s_0 ... s_{d_1}||\{1\}^{d2})$, corresponding to the bottom-left-most and bottom-right-most nodes respectively in the sub-tree for the given value of *s*. Instead of transmitting *c* as such, the tag encodes it in a pseudonym *p* containing (d_1 + d_2) pseudo-random numbers, calculated on the basis of a pseudo-random variable *r* and the current value of *c*. Each pseudo-random number p_i in *p* is calculated on the first *i* bits of *c*. The TC decodes *p* by reconstructing *c* through a simple DFS algorithm that matches at each level *i* the received p_i with the p_i calculated on $(c_0 ... c_{i-1}||0)$ and $(c_0 ... c_{i-1}||1)$. The exact algorithms are shown in [1].

Three pseudo-random functions are needed on the tag: A hash function *h*: $\{0,1\}^n \rightarrow K$, a pseudo-random generator PRG, and a pseudo-random function *F*: $\{0,1\}^n \ X \ K \rightarrow \{0,1\}^n$. As explained in [1], all these functions can be implemented using the same implementation of *F* with fixed salt values. The authors suggest using AES for implementing *F* because AES implementations have been shown to be possible within 500 gates on low-cost tags [2]. Further optimizations are possible by just implementing the restriction of *F* on *s* (that is, $F|_s$) on the tags. Ownership transfer and time-limited offline delegation can be done by offloading appropriate restrictions of *F* on suitable subtrees to trusted readers so that these readers need not have to query the TC while the values of *c* are within the restrictions given to them.

4.2 Security analysis

[1] provides replay-only security against impersonation and privacy attacks against a radio-only adversary because tag disambiguation is guaranteed. Replay-only security is also provided against impersonation attacks even if an adversary can compromise tags because each tag has at least one secret not shared with any other tag. To perform a successful non-replayed impersonation, the adversary would need to predict the value of a pseudo-random function keyed with such a secret.

Authentication is not done because privacy is guaranteed even otherwise. However, as we will show next, certain attacks still remain possible unless the basic scheme is not extended suitably.

4.3 Replay attack

Consider a situation where RFID tags are used to control access to a building. An attacker can go into a bar where employees working in the building generally hang out, and scan a few tags. The radio-only attacker can do this easily by sending a HELLO message to a tag and then store the (*p*, *r*) pair. The attacker can next retransmit the (*p*, *r*) pair to a trusted reader that controls access into the building. Thus, impersonation attacks can be launched even if the TC keeps track of the expired values of *c* for each tag, provided that the tag is not queried by a valid reader just before the attack is launched. This is a classic man-in-the-middle attack, and can occur because a challenge-response protocol is not part of the query procedure. We later show how to mitigate this attack, by taking advantage of physical proximity between the tag and the reader.

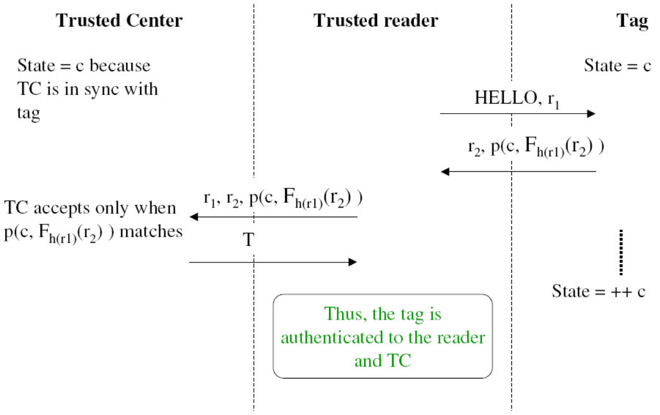

Trusted Center
Trusted reader
Tag
State = c because TC is in sync with tag
State = c
HELLO, r_1
r_2, p(c, $F_{h(r1)}(r_2)$)
r_1, r_2, p(c, $F_{h(r1)}(r_2)$)
TC accepts only when p(c, $F_{h(r1)}(r_2)$) matches
T
State = ++ c
Thus, the tag is authenticated to the reader and TC

Figure 2. Mitigation of replay attack

4.4 DoS attack

Since any radio-only adversary can query a tag even if the adversary is not able to decipher the tag's ID, repeated querying can eventually lead to a buffer overflow on the tag by successive increments of *c*, and render the tag useless. In addition, a reader can query the same tag repeatedly and collect enough information about the tag secret to be able to break the scheme.

5 Extensions

5.1 Solution to the replay attack

As shown in Fig. 2, we mitigate the replay attack by introducing a mechanism to authenticate the tags. The readers now send a random nonce r_1 to the tags, and the tags use r_1 along with their own randomly generated nonce r_2 to calculate $r = F_{h(r_1)}(r_2)$. This *r* is then used as before to find *p*. The TC can redo the calculations in the same way as earlier by using $F_{h(r_1)}(r_2)$ in place of *r*. Here, we assume that r_1 expires quickly so that attackers cannot launch the same man-in-the-middle attack as before. This assumption is practical to make because tags and readers will only exchange messages when they are physically close to each other. The key observation here though, is that our modifications in the query procedure make it easy to impose the physical proximity assumptions, which can otherwise be violated in the unmodified protocol.

5.2 Solution to the DoS attack

DoS attacks on tags can be prevented through the extensions shown in Fig. 3, by authenticating valid readers to tags. The TC first verifies valid tags as explained in the previous section, and then sends back to valid readers a pseudonym calculated on a new pseudo-random number r_3. The reader forwards this pseudonym to the tag, and only upon verification does the tag increment *c*.

[1] An ordered traversal can be a preorder or postorder traversal.

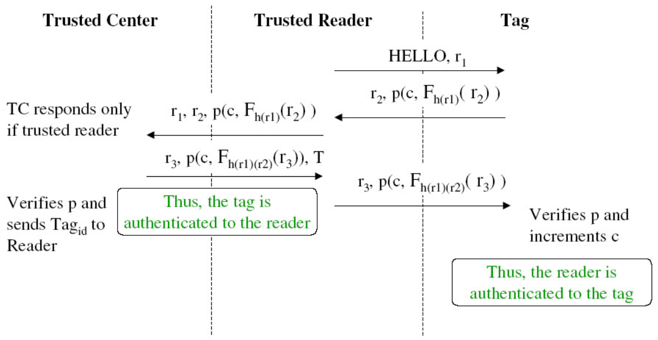

Trusted Center
Trusted Reader
Tag
HELLO, r_1
r_2, p(c, $F_{h(r1)}(r_2)$)
TC responds only if trusted reader
r_1, r_2, p(c, $F_{h(r1)}(r_2)$)
r_3, p(c, $F_{h(r1)(r2)}(r_3)$), T
Verifies p and sends Tag_{id} to Reader
Thus, the tag is authenticated to the reader
r_3, p(c, $F_{h(r1)(r2)}(r_3)$)
Verifies p and increments c
Thus, the reader is authenticated to the tag

Figure 3. Mitigation of DoS attack

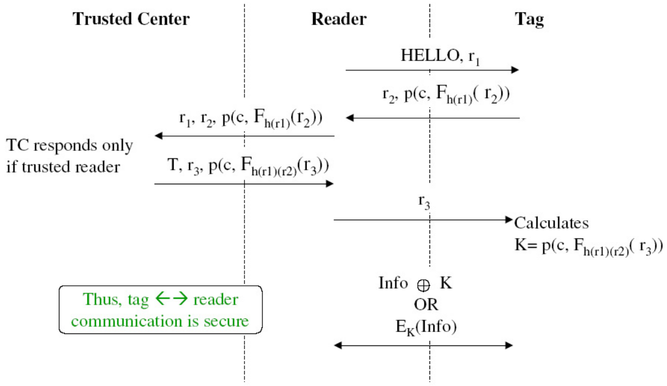

Trusted Center
Reader
Tag
HELLO, r_1
r_2, p(c, $F_{h(r1)}(r_2)$)
r_1, r_2, p(c, $F_{h(r1)}(r_2)$)
TC responds only if trusted reader
T, r_3, p(c, $F_{h(r1)(r2)}(r_3)$)
r_3
Calculates K= p(c, $F_{h(r1)(r2)}(r_3)$)
Info ⊕ K
OR
E_K(Info)
Thus, tag ←→ reader communication is secure

Figure 4. Secure communication between reader and tag

Divulsion of too much information about the tag secret can be prevented by introduction of a sufficiently large wait-time on the tag so that the same reader can be prevented from rapidly sending HELLO messages with the same value of r_1. Thus, most attacks can be avoided in realistic scenarios.

5.3 Secure transfer of data

RFID tags are likely to find use as sensors because of their low power consumption characteristics. In such cases, there will be data that resides on the tags and not with the TC, as is assumed in [1]. Transmission of this data in a secure manner requires the establishment of session keys between the tags and readers, and between tags and the TC. Similarly, session key establishment is also needed in case the TC is required to send data to tags in a secure manner, for example, to renew tags with new secret keys when tag state counters are about to overflow. We explain below the procedures required to provide secure transfer of data.

5.3.1 Secure transfer between tags and readers

Fig. 4 shows the communication protocol for secure transfer between a reader and tag. The TC calculates a pseudonym based on a new pseudo-random number r_3 and sends this to the trusted reader in response to a tag query. The reader only forwards r_3 to the tag; the tag calculates the corresponding pseudonym itself. Thus, the pseudonym can now be used as a secret key between the reader and tag. The data to be securely transferred can either be encrypted using the same AES implementation, or else a simple XOR of the data with the session key can also be used.

Note that the authentication mechanism explained earlier for reader authentication can be added to this extension as well. We did not show it in Fig. 4 to keep the explanation simple.

5.3.2 Secure transfer between tags and TC

This is almost the same as the previous protocol. The TC calculates a new pseudonym but only sends the pseudo random number r_3 to the reader. The reader forwards this to the tag, which calculates the corresponding pseudonym on its own and uses it as the secret session key for secure communication with the TC.

It is even possible to sign encrypted messages using the same principles. Note that this signature scheme can be included in the previous scheme for secure transfer between readers and tags.

6 Conclusions

In this paper, we identified a basis-set of requirements necessary for security and privacy in RFID systems, and then surveyed available research works to observe the extent to which they fulfil this basis-set. We then selected the scheme proposed by Molnar, et al [1], and outlined attacks that are possible on the scheme in different realistic scenarios. Next, we successfully extended the scheme to mitigate these attacks and meet all the requirements. We also proposed mechanisms to establish session keys on tags, readers, and trusted centers, to allow secure transfer of data between the entities. These extensions make the overall scheme complete and solves the security and privacy challenges that arise in RFID systems.

References

[1] D. Molnar, A. Soppera, D. Wagner, "A Scalable, Delegatable, Pseudonym Protocol Enabling Ownership Transfer of RFID Tags," Selected Areas in Cryptography, Aug 2005.

[2] M. Feldhofer, S. Dominikus, J. Wolkerstorfer, "Strong Authentication for RFID systems using the AES algorithm," In Proc. CHES, 2004.

[3] International Civil Avaiation Organization ICAO "Document 9303, machine readable travel documents (MRTD)," part 1: Machine Readable Passports, 2005

[4] A. Juels, S. Garfinkel, R. Pappu "RFID Privacy: An overview of problems and proposed solutions" IEEE Security and Privacy, 3(3):34-43, May/June 2005

[5] A. Juels, D. Molnar, D. Wagner "Security and Privacy issues in e-passports" In IEEE CreateNet SecureComm, IEEE 2005

[6] M. Ohkubo, K. Suzuki, S. Kinoshita "RFID privacy issues and technical challenges," In Communications of ACM, 2005.

[7] M. Ohkubo, K. Suzuki, S. Kinoshita "Cryptographic approach to a privacy friendly tag," In RFID Privacy Workshop at MIT, 2003.

[8] A. Juels "Minimalist cryptography for low-cost RFID tags," In 4th International conference on Security in Communication Networks, 2004.

[9] EPCglobal Inc. "Standards" http://www.EPCglobalinc.org, 2005.

[10] A. Juels, R. Pappu, "Squealing Euros: Privacy protection in RFID enabled banknotes" In Financial Cryptography 2003.

[11] G. Avoine, P. Oechslin, "RFID Tracability: A Multilayer Problem." In Financial Cryptography, 2005.