RFID TAG SECURITY, PERSONAL PRIVACY PROTOCOLS AND PRIVACY MODEL

Suchitra Majumdar #1, Kanchan Dhuri #2, Sandhya S. Dongre #3 Minakshi R. Badwaik #4
1Electronics and Telecommunication, Saraswati College of Engineering, Kharghar, Mumbai University, India.
2Electronics and Telecommunication, Vidyalankar Institute of Technology, Wadala, Mumbai University, India.
3 Electronics and Telecommunication, A.C Patil Engineering College, Kharghar, Mumbai University, India
4Electronics and Telecommunication, Datta Meghe Engineering College, Airoli, Mumbai University, India

Abstract: Radio Frequency Identification (RFID) is a method of remotely storing and retrieving data using small and inexpensive devices called RFID tags. In this work we propose a proxy agent framework that uses a personal device for privacy enforcement and increased protection against eavesdropping, impersonation and cloning attacks. Using the proxy a user decides when and where information carried in a tag will be released. In particular, the user can put tags under her control, authenticate requests, release tags, transfer them to new owners, and so on. This is the first framework that unifies previous attempts and presents detailed protocol.

I INTRODUCTION

Radio Frequency Identification (RFID) is a technology for automated object identification. An RFID tag is an electronic device that is typically attached to an item and upon request transmits item information such as date of manufacture, product characteristics, and so on. RFID tagged items can have remarkable applications. One could imagine refrigerators issuing warnings about expired food or about remaining bottles of milk. Laundry machines could select washing cycles based on color and sensitivity of clothes. Waiting times at checkout lines could be reduced since RFID readers can scan tags at rates of hundreds per second. Products may be tracked as they move from location to location, improving manufacturing logistics, supply chain management and better inventory procedures. Animals could be retrieved in case they are lost. Even more controversially, RFID chips have been used for “tagging” people, especially school children and club-goers wishing to gain access to VIP areas.

However, the mere fact that communication between tags and readers is wireless and does not require physical contact opens up the possibility for abuse and violation of user privacy. Currently, RFID tags respond to any reader request within range. Consequently, a person carrying a tagged item effectively broadcasts a fixed identifier to nearby readers. Thus anyone with a reader can read the information in the tag, potentially violating the owner’s privacy.

Our contribution: In this work we propose a new framework for enhancing the privacy of users carrying RFID products. Our method uses a mobile phone (or any other similar device) as a proxy for interacting with readers on behalf of the user carrying tagged items; thus the user can specify when and where information will be released. However, apart from enforcing policies and controlling tag state, our method maintains a number of desirable characteristics. In particular, we make sure that only authorized users can acquire and put tags under their control, user access to tags is authenticated, and when a user no longer needs the tagged product she can either make it readable to everybody or transfer it to another user. Furthermore, we make sure that privacy is maintained even if a user’s tag responds directly to scan requests.

II BACKGROUND ON MOBILE RFID TECHNOLOGY

- Overview of Mobile RFID: Networked RFID comprises an expanded RFID network and communication scope to communicate with a series of
networks, inter-networks and globally distributed application systems, engendering global communication relationships triggered by RFID, for such applications as B2B, B2C, B2B2C, G2C (Government to Customer), etc. The mobile RFID loads a compact RFID reader into a cellular phone, thereby providing diverse services through mobile telecommunications networks when reading RFID tags through a cellular phone. Since the provision of these services was first attempted in Korea in 2005, their standardization has been ongoing. Korea’s mobile RFID technology is focusing on the UHF (Ultra High Frequency) range [4,8,9]. Thus, as a kind of handheld RFID reader, in the selected service domain the UHF RFID phone device can be used to provide object information directly to the enduser using the same UHF RFID tags that have been widely distributed.

- **Network Architecture Component** The mobile RFID service has been defined as the provision, through the wireless Internet network, of personalized secure services – such as searching for product information, purchasing, verifying, and paying for products – while on the move, by building the RFID reader chip into the mobile terminal. The mobile RFID service structure is defined to support ISO/IEC 18000-6 A/B/C through wireless access communication between the tag and the reader; however, as yet there is no RFID reader chip capable of supporting all three wireless connection access specifications so that the communication specification for the mobile phone will be determined by the mobile communication companies.

### III MOBILE RFID-ORIENTED VULNERABILITY

The security vulnerability of the mobile RFID is the infringement of owners’ privacy and the physical attack in cyber space. Typical exposures include threats to individual privacy due to the approval of unlimited access to an RFID tag owned by a person. Access to the information must be limited to those who need it for an application. An individual RFID tag also may become a means to track and locate its owner. The infringement of privacy in the internet world results from the collection, storage, and use of customers by companies, but it has grown more serious in the mobile RFID world in that anyone with an RFID reader can read any information on anyone who keeps a tag-attached object.

It is also possible to hack tags, prevent the normal use of tags or get incorrect information from them by altering tag information or using a tag-kill function.

### IV SECURE MOBILE RFID SERVICE ENVIRONMENT

There are many ways to interfere with RFID circumstances, issues which are not only approved theoretically but also possible practically. Besides security vulnerabilities in RFID security like passive signal interception attack on RFID tags and readers, reading of RFID tags by unauthorized readers, falsifying tag or reader identity, use of attack tools against RFID tags, neutralization of RFID tags, and elaborate attack on RFID tags, with cryptographic hacking methods, there are also similar vulnerabilities and possible infringement of privacy in mobile RFID circumstances. It requires proper security technologies.

### V DESIGN GOALS

In this section we present a list of general security goals that should be true for any RFID protocol and then proceed with more specific characteristics we expect from our proxy protocol.

- **Privacy**: No secret information should leak from the tag that can help in identifying tag contents or the bearer of the tag. Another closely related problem to that of violating consumer privacy is location privacy which may lead to tracking of individuals by the tags they carry. Thus we require that no fixed identifiers should be emitted by the tags or the proxy.
- **Protection against tag spoofing or cloning**: A tag cloning attack would allow a person to either install a replacement tag or simply query the tag and forward its response to a near by reader. Although, we enable the proxy with the capability to relabel tags to protect user privacy, this should be done in a way that prevents cloning and ensures the privacy of subsequent owners.
- **Protection against impersonation attacks**: An adversary should not be able to impersonate either a tag or the mobile proxy. The first attack could lead to removal of a user’s tagged items since a fake tag could still answer to proxy’s challenges. The second attack could be useful in tracking a user’s movements.
- **Policy enforcement and access control**: We expect the proxy to act as mediator for tag access in order to minimize the privacy risks inherent in the use of RFID.
technology. So, in certain cases it should be possible to release information about tags while in others to block such requests entirely using proper cryptographic mechanisms.

- **Transferability and tag release**: In many situations it is necessary to bring a tag to its original state (tag release) or transfer it to a new user. In the first case, we require that the current owner should not be able to lie about the original ID of the tag, while in the second we make sure that the privacy of the new owner is guaranteed.

- **Simplicity and Efficiency**: The messages exchanged between tags and proxy should be protected against eavesdropping done in a way that does not put too much burden on the tags or even inhibit proper tag identification. Finally, we require that the proxy itself be a simple device capable of communicating with tags and readers, perform various cryptographic operations and perhaps have the available GUI (or other) interface to interact with a user.

**VI BACKGROUND**

Formally, the hash chain is built starting from a random seed vo and generating the values vj+i = H(vj). In RIPP-FS, every tag receives as starting point the value vo, that is its first private symmetric key, and will evaluate the values vj (with j > 0) to send to the reader. The original RIPP-FS protocol can require a considerable number of hash computations when a tag loses a large amount of queries: namely, if the tag has lost x queries, it has to perform x iterations of the function H, in order to evaluate the key Ki to use for authentication. To reduce the number of hash computations for a query response, we have to study the problem of how to efficiently generate the elements of an hash chain. A trivial solution is to evaluate every value, starting always from the starting point v0: actually, if m is the length of the chain, this solution requires 0(m) computations per value to be output. Another trivial solution can be to store all the values of the chain. In this way, to generate each desired value, only a look-up is required in the corresponding chain (memory) position. Such a solution has a memory complexity of 0(m). Further, it is possible to trade off memory and storage by storing some fraction of the values, and computing the desired values from such stored points. It can be seen that such variations of these trivial approaches all will have a memory/times computational complexity of 0(m).

There have been many papers in the literature that attempt to address the security concerns raised by the use of RFID technology. For a survey the reader is referred to [1]. Here we will emphasize on the concept of having users protecting tags they carry by means of personal devices ([2], [3], [4]). The Guardian [2], is a device that acts as an intermediary between tags and readers and must always be alert in protecting tag responses from unauthorized read attempts. It has to either allow reader queries, appropriately re-issuing queries in encrypted form, or actively block tag answers. Thus if the Guardian fails, security is lost. Furthermore, it does not deal with such issues as tag acquisition and ownership transfer. The RFID Enhancer Proxy or REP [3] assumes the identities of tags and simulates them in the presence of reading devices by continuously relabelling their IDs. Although similar inspirit to the framework we propose here, the REP suffers from a number of shortcomings such as corruption of tag data, tag to-REP desynchronization and difficulty in tag release that are attributed to the fact that tag identities need to be partially generated by the tag and match portions of its true ID. Finally, the authors in [4] propose a scheme called MARP (Mobile Agent for RFID Privacy) that assumes the secrets of tags and uses them to mediate with reader requests once the tag has been put to sleep. However, this scheme does not ensure privacy since the back-end server still knows the tag secrets and is always engaged in providing answers to reader requests. Furthermore, the scheme relies on the use of heavy public key cryptography.

**VII Security Comparison with Previous Works**

In this section, we compare the security properties achieved by our proposed protocol with those of previously protocols, namely universal re-encryption [2] proposed by Golle et al., an improved version of universal re-encryption called “With a Check” [10] proposed by Saito et al., and insubvertible encryption [11] proposed by Ateniese et al. Universal re-encryption has advantage that it can be used to randomize cipher text stored in a tag without knowing the corresponding public key. However this technique leaves a serious security problem that an adversary may store a new
cipher text of some other plaintext under his own public key to a tag, so that no matter how many times the tag is randomized later, the adversary is able to decrypt it and trace it. Therefore actually it provides no IND, BIND, SP, SWP and OT. Saito et al. pointed out the security problems of universal re-encryption and proposed two improved versions, “With a Check” and “Using a One-Time Pad”. In “With a Check” method, the tag will perform some check operations before accepting a new cipher text. However these two methods still leave out the same security properties as universal re-encryption. Atieniese et al. later proposed an RFID protocol using the insubvertible encryption. It allows authorized users to store an encrypted message into a tag that can be randomized by anyone. Also unlike universal re-encryption schemes, insubvertible encryption includes certificates proving that the cipher text can only be decrypted by authorized parties. It achieves the integrity of cipher texts randomized by authorized users. However, this protocol leaves other security problems such as tag spoofing and swapping valid data.

Our protocol is constructed by applying the insubvertible encryption, and we involve guardian proxy in our protocol. Therefore our protocol not only fulfills all the security requirements mentioned in Section 2.3, but also provides a detailed ownership transfer protocol. We summarize the comparison in Table 1. We denote universal re-encryption by UR, “With a Check” method by WAC and insubvertible encryption by IE, respectively. Also for the ownership transfer, our protocol gives a detailed protocol for this purpose. Although C.H.Lim and T.Kown in their paper [5] claim that their proposed solution enables perfect ownership transfer, they give neither detailed protocol nor security proof. In Saito et al.’s paper [9] they give an ownership transfer protocol in symmetric key infrastructure and their tag has to do some encryption operations.

VIII SECURITY ANALYSIS

To acquire better security, a RFID structure must be equipped with applied functions of inter-authentication, privacy anonymous and with abilities of relieving the invasion and destroy from the illegal attackers. We here have detailed explanations of the proposed structure for the private anonymous and inter-authentication. Inter-authentication: There exist a common code, an updated system code and an EPC of Tags in Tags and in Data-Base for Inter-authentication. After a random code generation and encryption, the trust of Reader is attainable at this situation that both the decryption computation and EPC are legally communicated when message is transmitted at the cases of safety and confidence.

- **Privacy and anonymous**: The EPC message was not directly transmitted, which indicates the EPC message to be hidden with random number and the secret key can effectively protect Tags private information from disclosing to make customers privacy secret, which is important for data confidence. We now explore and analyze the possible attacks happening in the application of the RFID. The various attack modes such as replay attack, counterfeit attack, forward key security and guessing attack appearing in the data transmission were overcome by the proposed structure.

- **Replay attack**: The Reader and Tags in the proposed structure for each stage codes and for updated system authentication codes were randomized and executed by XOR computation, which can avoid illegal attackers to grab Data-Base authentication even if the previous key was accessed.

CONCLUSION

In this work we have presented a framework for enhancing RFID security by means of a proxy, a personal device that assumes control of a user’s tags. The proxy interacts with the tags but does more than simply simulating tags or acting as “device-in-the-middle” between tags and readers, encrypting reader queries and decrypting tag responses, as previous solutions do. To the best of our knowledge this is the first work that unifies past approaches and presents detailed protocols for such issues as tag acquisition, proxy authentication, resistance to privacy attacks, ease of transfer and release, and so on. Once the proxy performs some initial transformations to the tags under its control, it can either mediate between tags and readers or let tags directly respond to scan requests. In the first case, the proxy can specify a number of policies that readers must comply with. In the latter, we make sure that tags do not emit any static identifiers thus providing ID anonymity and helping prevent tag tracing. Overall, using the protocols described in the
framework the user has full control of the tags she carries in a way that guarantees user’s privacy and protection from a host of attacks like impersonation, cloning, tag spoofing and so on. However, we also make sure that our framework cannot be abused by malicious proxies. So, we guarantee that only authorized users can acquire and put tags under their control, user access to tags is authenticated, and when a user no longer needs the tagged product she can either make it readable to everybody or transfer it to another user in a way that guarantees the privacy of the new owner.

REFERENCES