RFID 시스템에서의 효율적인 프라이버시 보호 기법

Yuan Yang°, 이태석, XiaoYi Lu, 인 호, 박명순
고려대학교 컴퓨터학과 인터넷 컴퓨팅 연구실
{yy, tsyi, felicity_lu}@ilab.korea.ac.kr, hoh_in@korea.ac.kr, myongsp@ilab.korea.ac.kr

Efficient Privacy Protection in Radio Frequency Identification Systems

Yuan Yang°, Tae-seok Lee, XiaoYi Lu, Hoh Peter In, Myong-Soon Park
Internet Computing Laboratory, Information and Communication Department, Korea University

Summary

In today' s hyper-competitive business environment, Radio Frequency Identification (RFID) technology is expected to enhance the operation efficiency of supplying chain management in both manufactures and retail industries. However, the widespread deployment of RFID tags may create new threats to user privacy, due to the powerful tracking capability of the tags. Many authentication protocols for RFID have been proposed. They are helpful preventing passersby being scanned to determine what articles they are carrying. However, most of them would not prevent the bigger physical tracking problem of RFID, especially when being tracked by the " constellation" of products they carry. We proposed this RFID scheme to prevent these tracking problems.

1. Introduction

The Radio Frequency Identification (RFID) technology is proposed with the expectation of improving the operation efficiency of supplying chain management in both manufactures and retail industries.

Unfortunately, the universal deployment of RFID devices in consumer items may bring new security and privacy risks presently not in closed manufacturing environments. Corporate espionage is one of these risks. Retail inventory labeled with unprotected tags could be monitored and tracked by business competitors. Without protection, a store' s inventory may be monitored by competitors through surreptitious scans, and correspondingly its dynamically changed sales data may be gleaned.

Another risk is the violation of " location privacy" which is caused by tracking an individual by the RFID tags they carry. A tag reader at a fixed location could track RFID-labeled clothes or banknotes carried by people passing by. Correlating data of the target from distributed tag readers could track movements, social interactions, and financial transactions. Concerns over location privacy were recently raised because a major tire manufacturer began to embed RFID tags into all their products. Even if the tags only contain product codes other than unique serial numbers, individuals could still be tracked by the " constellation" of products they carry. So maybe the unique taste in brands could betray the owner' s identity.

Several papers have discussed the protection of user privacy in RFID system with active tags. Such like Hash lock scheme [1], the re-encryption approach [2], XOR based one-time pad scheme [3], etc. They can keep the security of product EPC (electronic product codes) by outputting the related pseudo code (meta-ID) instead of original EPC code. However, this may also allow tracking of tags via their pseudonym output or meta-IDs thus defeat their whole purpose.

This paper introduces a new privacy-protecting technology related to RFID active tags. To prevent unauthentic read in our protocol, a tag is authenticated to a reader only after the reader has already authenticate itself to the tag, the following figure 1 described the scheme. In order to defend the location attack, one important feature is that: the RFID tag need to output differently even though it has been scanned by an unauthenticated reader. In our protocol, the RFID tag changes the pseudonym output, pseudo-code α, when scanned by any readers. The reader authenticates the tag by releasing a key β; this key β is unique to a given pseudonym α, once the reader has been authenticated to the tag, the tag authenticates itself to the reader by releasing an authentication key γ. Like β, this authentication key γ is unique to an identifier α. In order to keep information security guaranteed, all output value is encrypted with hash function H. Briefly stated, we propose a kind of challenge-response protocol.

The rest of this paper is organized as follows. In section 2, we describe our proposed RFID protocol. In section 3, the security analyses are given. We consider system efficiency in section 4. Finally, the conclusion is given in section 5.

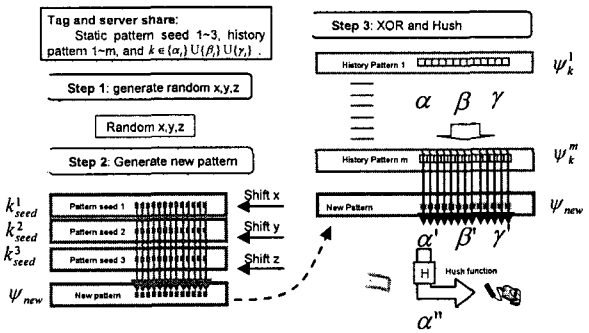

Figure 1. RFID encrypt scheme

2. Proposed RFID Protocol

In face of multiple probing attacks by an adversary and in order to maintain the integrity of a tag over an extended period of time, we take a approach in our protocol of having the reader and tag update the history pattern, Δ_k, which was used to encrypt the authenticate code k in an RFID tag. Δ_k is upgraded after the successful mutual authentication between tag and reader.

2. 1 Protocol Detail

We assume that the initialization of all the entities is done by a trusted party, who can generate a history pattern set $\Delta_k = \{\psi_k^{(1)}, \psi_k^{(2)}, ..., \psi_k^{(m)},\}$, k_{seed}^1, k_{seed}^2, k_{seed}^3 for every tag and distribute this to both the tag and the back-end server.

Tags are equipped with a one-way hash function, and also have a random number generator. Tags respond to reader queries by generating a random new pattern ψ_{new} and hashing their $k \in \{\alpha_i\} \cup \{\beta_i\} \cup \{\gamma_i\}$ concatenated with ψ_{new} and $\psi_k^{(m)}$, and then sending the hashed values to the reader. A legitimate reader connected with back-end server can identify one of its tags by performing a brute-force search, calculation of all possible candidates in the database, until it finds the match.

In the protocol, the reader does not need to transmit update " key" to the tag used to update its shared history pattern Δ_k values. Provided that an eavesdropper could not obtain the padding data, and had no idea of the updated tag values. We may think that the authentication process renew the keys used to " encrypt" and thereby update the $\{\alpha_i\}$, $\{\beta_i\}$ and $\{\gamma_i\}$ values.

As explained above, we employ a strategy of updating tag values using semantic authentication from authentication sessions. Let k be some value stored in a tag, i.e., $k \in \{\alpha_i\} \cup \{\beta_i\} \cup \{\gamma_i\}$. For every value k, we maintain history patterns of the tag as a vector $\Delta_k = \{\psi_k^{(1)}, \psi_k^{(2)}, ..., \psi_k^{(m)},\}$, the pad $\psi_k^{(m)}$, which is referred to as the live pad, is the basic factor used to encrypt the tag value k. Particularly, when encrypt k, the tag computes $K \leftarrow k \oplus \psi_k^{(m)} \oplus \psi_{new}$. Here, ψ_{new} is a new pattern which is generated by element-wise XOR pattern seeds k_{seed}^1, k_{seed}^2, k_{seed}^3 and shifted with random numbers x, y, z. Once a tag and a reader mutually authenticate each other, the pads in tag Δ_k are updated with new pattern seed ψ_{new}. And after this, the indices of all the other pads in Δ_k are shifted downward, and the element-wise calculation is also done, i.e., in increasing index order, we set $\psi_k^1 = \psi_k^{new}$ and $\tilde{\psi}_k^{(i)} = \psi_k^{(i+1)}$ for $1 \le i \le n-1$. We let $\tilde{\psi}_k^m = 0^l$, $\tilde{\Delta} = \{\tilde{\psi}_k^{(1)}, \tilde{\psi}_k^{(2)}, ..., \tilde{\psi}_k^{(m)}\}$. Finally, we " overlay" the newly generated vector $\tilde{\Delta}_k$ on the existing vector Δ_k by performing an element-wise XOR, in which we let $\psi_k^{(i)} = \psi_k^{(i)} + \tilde{\psi}_k^{(i)}$.

This approach can provide much more security to information-theoretic. Thus an adversary that has no idea of previewing the last m history pads would not know about ψ_k^m at all. Thus, when the live pad is employed to update k, the adversary learns no information about the new value of Δ_k.

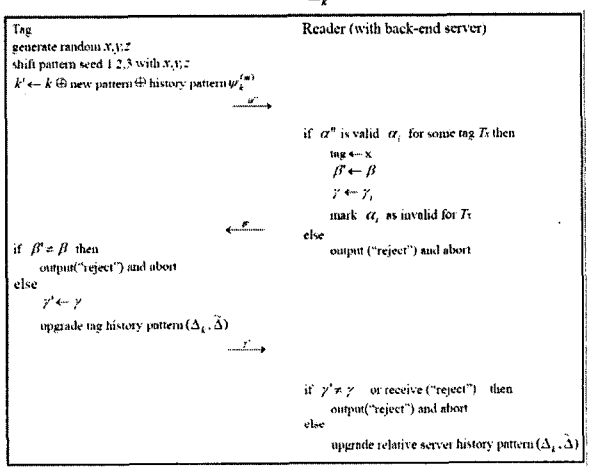

Figure 2. Proposed RFID protocol

Details of our protocol are described in Figure 2. Here, we use the notation $update(\Delta_k, \tilde{\Delta}_k)$ to denote the function that updates Δ_k and " overlays " it with $\tilde{\Delta}_k$. We let " $k' \leftarrow k \oplus$ new pattern $\oplus$ history pattern" denote the ' encrypt' of k using the live pad ψ_k^m and new pattern seed ψ_{new}. In case of a message-delivery failure, we assume the output of " reject" could lead to protocol termination.

3. System Security

This section will discuss the security of our scheme. Obviously, to ensure the anonymity of the tag ID, the tag could not output either its ID or any constant data. Our scheme satisfies this

requirement. Moreover, this scheme offers the tag output indistinguishable property.

For the purpose of this analysis, we assume that the attacker could not interfere with the physical artifacts in the system (RFID tags and readers) or with the backend system. However, we do expect that the attacker could attempt to attack in one of the following processes.

1) Attacking RFID Tags

In these attacks, the attacker is masqueraded as a valid reader. This kind of attack is defeated by the shared secret because the tag could not recognize the masqueraded reader, so the masqueraded reader can not get any required authenticate information by previous interception, and thus only a real reader is able to present a valid authentication request and make the tag output the hashed product ID.

2) Attacking RFID Readers

In this case, the attacker is masqueraded as a valid tag in attacks. This kind of attack is defeated by the shared secret because the reader can not identify the tag, for the masqueraded tag is only able to response unauthenticated message α_i.

4. Discuss and System Efficiency

One open question is whether the pseudo-random function ensembles can be implemented significantly easier than symmetric encryption. Designing efficient implementations of these perfect one-way functions [4] may be a relevant avenue of the research as well.

It is important to note that the level of security and privacy depends on the application. Increasing pattern seeds length and history pattern level can make system more secure, but it may also bring the problem of requiring more computing resource and increasing tag cost.

We would like RFID tags in our system to output read-protected information by continually unauthenticated scan. On the other hand, an important feature to protect consumer privacy in our system is the inability of an attacker to mount rapid on-line attacks due to their slow processing and transmission capabilities. For example, an RFID tag might be designed to switch to a low data rate model while being continually scanned by unauthenticated readers, and then can delay subsequent guessing from an attacker. It is our belief that this feature could be incorporated into RFID tags at little cost.

With the development of computing technology, search in large data base become easier today. Following simulation shows performance searching for one to ten tags in a SQL database which stores 10000 tags' all possible output pseudo-codes, simulation result shows that by using our scheme, searching speed and database capacity is sufficiently enough to make this system to be used in general large market.

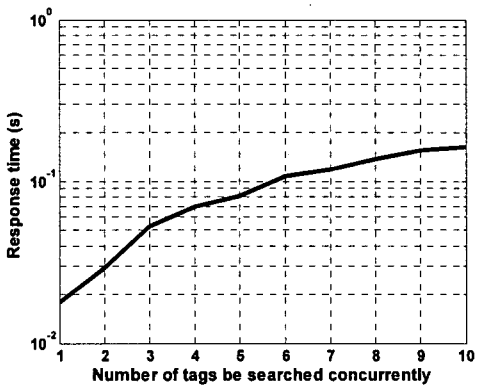

Figure 3. Database searching speed emulation

6. Conclusion

We have proposed a RFID system design that requires the capabilities of the current generation of RFID tags to achieve stronger consumer privacy.

RFID tags have the possibility of bringing revolution to the whole society. While getting convenience from their advantages, we must also know their risks. Implementing ubiquitous network connectivity in social life will demand a close examination of personal privacy from both the technical and social aspects. However, the privacy problems raised by their indiscriminate nature are serious enough to demand a comprehensive and effective technique that can ensure user privacy as well as retain their benefits.

Although there are several existing schemes, none provide a complete solution. Some of them may forbid tag ID output, but they still allow tag output including relatively constant information, and these static tag output still allows some form of location tracking taking place. In our proposed protocol, the RFID tag changes the pseudonym output when being scanned by readers, which make location tracking impossible.

References

[1] Ari. Juels, " Privacy and Authentication in Low-Cost RFID Tags" , submission 2003.

[2] Ari. Juels, Ravikanth. Pappu, " Squealing euros: Privacy protection in RFID-enabled banknotes" , In Proceedings of Financial Cryptography - FC' 03, 2003.

[3] Ari. Juels, Ronald. L. Rivest and Michael. Szydlo, " The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy" , In Proceedings of 10th ACM Conference on Computer and Communications Security(CCS 2003), Oct. 2003.

[4] Auto-ID Center, " 860MHz-960MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical communication Interface Specification Proposed Recommendation Version 1.0.0" , Technical Report MIT-AUTOID-TR-007, Nov. 2002.