Practical Considerations for RFID System Security and Privacy Risks

김정태
목원대학교
RFID 시스템 보안 및 위험 요소를 위한 실제적인 고려 사항
Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@gmail.com

요 약

The fear of unauthorized, hidden readouts has dominated the radio frequency identification (RFID) privacy debate. Therefor all published and previous works for privacy mechanisms so far require consumers to actively and explicitly protect read access to their tagged items. This paper introduces the underlying mechanism of our extension to considerations for security and analyzes its tracking resistance and identification performance, and discusses deployment aspects

Ⅰ. Introduction

The more RFID tags and readers become popular, the more convenient our lives are widespread. However, the problems which are caused by reading privacy information form RFID tags will increase. The beneficial aspects of RFID tags are numerous, including means to track, locate, and identify a specific object of interest in real-time, ensuring that the object has been handled properly theft detection/reduced shrinkage, identification of spurious/counterfeit products, and overall improved service levels. It is very important to protect consumers' privacy information. In order to deal with RFID privacy protection, some stakeholders publish the privacy protection guidelines for RFID use. In the coming near future, RFID tags attached to consumer items as "smart-labels" may become an efficient way for tracking purpose. However, the universal deployment of RFID systems may create new security and privacy problems that can be a barrier to the widespread adoption of RFID technology. Also, from an economical point of view, the cost of an RFID tag should be made much lower for being well acceptable by the logistic/retail/manufacturing industry.

II. Trends of technology

In light of these issues, this paper investigates a three step process to protect the corporate system from intrusion on the tag. First, the RFID tag checks the tag readerID stored in part in the tag memory. Once confirmed, the reader transmits a random number of the tag generated back to the database. The random number is then processed through the hash on the server and on the tag. If both sets of ciphered data match, mutal process is authenticated to retrieve tagID related data. The final step is optional and involves updating the tag memory with regard to location changes so that the tag has the correct readerID and location

coordinates as it moves to different warehouses. In regards to consumer privacy issues, users may be protected using a privacy bit, a blocker tag, or a biometric encryption. For instance, the privacy bit would allow an RFID tag to behave like an Electronic Article Surveillance(EAS) tag. Clearly, RFID is a powerful technology with numerous application possibilities. It's also a technology that raises serious privacy and security risks. Several RFID features make it particularly vulnerable among information systems, including the wireless transmission between the tag and reader; the tag's low computational power, which is often insufficient for strong security measures; and the tag's small size, which means that people can carry one without their consent or even knowledge.

III. Attack models

In order to define the notions of "secure" and "private" for RFID tags in a rigorous way, we must first ask: "Secure" and "private" against what? The best answer is a formal model that characterizes the capabilities of potential adversaries. In cryptography, such a model usually takes the form of an "experiment," a program that intermediates communications between a model adversary, characterized as a probabilistic algorithm (or Turing machine), and a model runtime environment containing system components (often called oracles). In the model for an RFID system, for example, the adversary would have access to system components representing tags and readers. In most cryptographic models, the adversary is assumed to have more-or-less unfettered access to system components in the runtime environment. Some well known attacks are as RFID tags fit into generally three categories.

1. Logistical applications that require quick reading and very low security. These devices are used in shipping and receiving.
2. Consumer applications that requires high end security but no bulk reading capabilities. These are found in smart cards.
3. Vertical applications that need special security features tailored for specific use.

A good example is those RFID tags used in casino poker chips.

A. Threats to RFID systems

Like all information systems, RFID-based systems are subject to generic attacks that threaten system security and user privacy. However, there are also many attacks that specifically target RFID system technologies [1].

- eavesdropping
- relay attacks
- unauthorized tag reading
- tag cloning
- People tracking
- replay attacks
- tag content changes
- Physical tag destruction
- Blocking and jamming
- Overall threat analysis

B. Framework for evaluating risks

We evaluate risks on the basis of three criteria: system deployment range, the link between the tag and identity-related data , and the domain's security demands. The most critical applications should be considered.

- System deployment range
- Links between the tag and identity-related data
- Demand for security

C. vulnerability

- application domains implant-based - medical information systems

implant-based
- access-control systems
- e-passports

IV. Security requirements and common-keys effect

To describe the elements of characteristics of security mechanism, we mainly focus on Privacy, Cloning resistance, Forward secrecy, and Untraceability as the fundamental security requirements of RFID privacy-preserving authentication. In RFID systems, a private authentication protocol should meet the above security requirements.

A. Privacy.

Any user's private information should not be leaked to any third party during authentication.

B. Cloning resistance.

All the valid tags should not be faked or impersonated. Replay attacks, in which adversaries may repeat the messages sent before to victims tag or readers, should also be infeasible to the authentication procedure.

C. Forward secrecy.

Achieving forward secrecy is that keys stored in a compromised tag cannot reveal the previous outputs of this tag.

D. Untraceability.

A tag should have no correlation with its authentication messages for avoiding tracking.

V. Symmetric and Asymmetric key tags

We focused on class of RFID tags with richer security capabilities, those capable of computing symmetric-key functions. Just as important as the effective use of symmetric-key cryptographic primitives for privacy or authentication is the efficient design and implementation of these primitives. A large body of work in RFID privacy is concerned with lowering the requirements for cryptographic functions implemented on RFID hardware, such as the work by Feldhofer et al. on using AES or the use of elliptic curve cryptography. Some researchers target the limited hardware capabilities of standard EPCglobal-tags, providing algorithms that only rely on simple XOR operations or the presence of a random number generator [2]. A few papers explore primitives geared specifically at the very tightly constrained environments of RFID tags.

- Vajda and Buttyán [3] propose a medley of lightweight cryptographic primitives for RFID-tag authentication.
- Feldhofer, Dominikus, and Wolkerstorfer [4] propose a lightweight hardware implementation of a symmetric-key cipher, namely, a 128-bit version of the Advanced Encryption Standard (AES). Their design requires just over 3500 gate equivalents—considerably more than appropriate for basic RFID tags, but suitable for higher cost RFID tags.
- Juels and Weis [5] propose a lightweight authentication protocol called that has security reducible to a problem called Learning Parity with Noise. To implement, tags need only generate random bits and compute binary dot products. The key lengths required for good security are as yet unknown, however, and the security model is limited.

Public-key authentication, an alternative approach, doesn't require reader-backed communication. In these protocols, readers and tags store public and private keys. To establish communication, the reader sends a notification and receives a random challenge from the tag. The reader uses its private key to encrypt the challenge and

then sends it back to the tag. By decrypting the received cipher text and comparing it to the original challenge, the tag verifies whether the reader possesses the required private key. If the resulting plaintext is equal to the issued challenge, the tag establishes the communication session. Unfortunately, public-key cryptography requires the tag to perform complex mathematical computations [5]. Because low-cost RFID tags offer extremely limited resources, it could be problematic to implement a public-key authentication protocol while keeping the tag's cost low. As of this writing, the most compact implementation of a public-key encryption scheme is the elliptic-based public-key encryption cipher(ECC), which requires roughly 15,000 logical gates on a tag. Cryptographic primitives required to implement hash-based authentication schemes are more compact. The Secure Hash Algorithm 1 (SHA-1), for example, only requires approximately 4,300 gates, whereas the Advanced Encryption Standards (AES) symmetric cipher requires roughly 3,400 gates. An on-tag scheme requires the tag to implement at least one of these primitives. Yet, some argue that current RFID chips costing below US$0.50 dispose of only 2,000 to 10,000 logical gates, approximately 200 to 2,000 of which are available for security needs.5 Consequently, not enough resources are currently available to implement any of the proposed authentication mechanisms [6].

VI. Conclusion

From a privacy perspective, we conclude that the user scheme is an important strategy for meeting the consumer's needs. Furthermore, we review the considerations for privacy research to put more effort into this line of thinking about RFID privacy and security mechanism.

References

[1] Paweł Rotteri, "A Framework for assessing rFiD System Security and Privacy risks" Security & Privacy, 2008, P.70-77.

[2] Chien H-Y, Chen C-H (2007) Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. Comput Standards Interfaces 29(2):254–259

[3] I. Vajda and L. Buttyán, "Lightweight authentication protocols for low-cost RFID tags," in Proc. 2nd Workshop on Security in Ubiquitous Comput., 2003.

[4] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in Proc. Workshop on Cryptographic Hardware and Embedded Syst., M. Joye and J.-J. Quisquater, Eds. New York: Springer-Verlag, 2004, vol. 3156, Lecture Notes in Computer Science, pp. 357–370.

[5] A. Juels and S. Weis, "Authenticating pervasive devices with human protocols," in Proc. Advances in Cryptology. New York: Springer-Verlag, 2005, vol. 3621, Lecture Notes in Computer Science, pp. 293–308.

[6] Sarah Spiekermann and Sergei evdokimov, "Critical RFID Privacy enhancing technologies" IEEE Security & Privacy, 2009, pp.56-62