Analyses of Framework for Enhanced RFID Security and Privacy

김정태
목원대학교

개선된 RFID 보안 및 비밀성을 위한 프레임워크의 분석

Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@gmail.com

요 약

Radio Frequency IDentification (RFID) is a method of remotely storing and retrieving data using small and inexpensive devices called RFID tags. In this paper 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 model a user decides when and where information carried in a tag will be released. In particular, the user can put tags under her/his control, authenticated requests, release tags, transfer them to new owners, and so on. In this paper, we analyses a new type of simple a framework for enhancing RFID security by means of a proxy, a personal device that assumes control of a user's tags.

Ⅰ. Introduction

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. As RFID devices hold personal information and keep track of purchases, serious privacy issues have been raised. In an attempt to protect consumer privacy, legislation is being proposed requiring products with RFID tags to be announced and labeled. The lack of cryptography in basic RFID is a big impediment to security design; cryptography, after all, is one of the lynchpins of data security. On the other hand, the lack of cryptography in basic tags poses intriguing research challenges. As we shall see, researchers have devised a algorithm of lightweight technical approaches to the problems of privacy and authentication.

II. Related work

There have been many papers in the literature that attempt to address the security concerns raised by the use of RFID technology. The Guardian[1], 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. RFID technology is an amazing invention of its kind, which has the ability to convey embedded information in a tag without any physical contact with it. The reference is an excellent tutorial on RFID basics [1]. RFID is the next revolutionary step for various businesses such as supply chain management, apparel industry, inventory control, toll pay on fly etc. RFID is vulnerable to security breaches such as cloning, clandestine tracking and inventorying. Rather than relying on public RFID readers to enforce privacy protection, users might instead carry their own privacy-enforcing devices for RFID such as mobile device. Several proxying approaches have been proposed such as "Watchdog Tag, RFID Guardian, RFID Enhancer Proxy [2].

III. Threats of attacks

Some well known attacks and considerations are as follows:[3].

A. attacks

Physical Attacks: Some examples of physical attacks are probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock glitching, among others.

- Denial of Service (DoS): A common example of this type of attack in RFID systems is the signal jamming of RF channels.
- Counterfeiting: There are attacks that consist in modifying the identity of an item, generally by means of tag manipulation.
- Spoofing: When an attacker is able to successfully impersonate a legitimate tag as, for example, in a man-in-the-middle attack.
- Eavesdropping: In this type of attacks, unintended recipients are able to intercept and read messages.
- Traffic analysis: Describes the process of intercepting and examining messages in order to extract information from patterns in communication. It can be performed even when the messages are encrypted and can not be decrypted.

B. Considerations

- Privacy:
- Protection against tag spoofing or cloning:
- Protection against impersonation attacks:
- Policy enforcement and access control:
- Transferability and tag release:
- Simplicity and Efficiency:

IV. System model

We now present the protocols that can be used in acquiring and managing a set of tags with the help of a personal device (called proxy in the remainder of the paper) such as for example a mobile phone enabled with reader capabilities

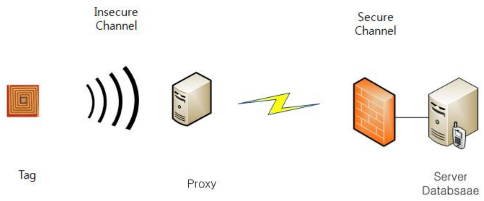

Figure 1. Block diagram of system configuration

In RFID communication, a reader typically does not know which tags are in its vicinity. Thus, in order to identify one or more RFID tags, it simply sends out a broadcast message asking for all tags (or all tags of a specific type) to reply. Our proposal includes the following items.

a) We propose the features required for a secure contactless credit card (RFID credit card).

b) We identify a mobile RFID reader architecture and propose its functionalities to enable secure online transactions.

c) We propose the functionalities of RFID middleware collocated with the authentication server to provide security against fraud. The functionalities designed at the RFID middleware eliminate the need for users to remember any PIN or other key information.

The Proxying Approach: Rather than relying on public RFID readers to enforce privacy protection, consumers might instead carry their own privacy-enforcing devices for RFID. As already noted, some mobile phones include RFID functionality. They might ultimately support privacy protection. Researchers have proposed several systems along these lines [4].

- Floerkemeier et al. propose and briefly describe a prototype "Watchdog Tag," essentially an audit system for RFID privacy. The Watchdog Tag monitors ambient scanning of RFID tags, and collects information from readers, like their privacy policies.
- Rieback et al. and Juels et al. propose very similar devices, respectively, called an "RFID Guardian" and "RFID Enhancer Proxy" (REP). A Guardian (to use the first term) acts as a kind of personal RFID firewall. It intermediates reader requests to tags; viewed another way, the Guardian selectively simulates tags under its control. As a high-powered device with substantive computing power, a Guardian can implement sophisticated privacy policies, and can use channels other than RFID (e.g., GPS or Internet connections) to supplement ambient data. For ex-ample, a Guardian might implement a policy like: "My tags should only be subject to scanning within 30 m of my home (as determined by GPS), or in shops that compensate consumer tag-scanning with coupons for a 10% discount." The logistical questions of how a Guardian should acquire and release control of tags and their associated PINs or keys are tricky ones that merit further research. 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.

V. Fundamental security requirements

We review fundamental security requirements against mainstream attacks [4].

A. Fundamental Defense Measurements

- Privacy protection:
- Cloning attack:
- Forward secrecy:
- Tracking:

B. Compromising Attack

Tree-based approaches suffer from compromising attacks because of the key components shared among tags. A compromising attack mainly depends on the differences between the victim tag T and other tags.

C. Desynchronization Attack

The desynchronization attack unusually focuses on synchronization based RFID approaches, but it also has a serious impact on any RFID authentication protocols when combined with the tracking attacks.

An emerging application is ubiquitous. The use of RFID tags for anti-counterfeiting by embedding them into a product is widespread. Public key cryptography (PKC) offers an attractive solution to the counterfeiting problem but whether a public key cryptosystems can be implemented on an RFID tags or not remains unclear. RFID based on identification is an example of an emerging technology which requires authentication as a cryptographic service. This property can be achieved by symmetric as well as asymmetric primitives. Previous work considered only symmetric key algorithms such as AES. It is not clear whether public key algorithms can be implemented in constrained devices, such RFID tag, and still depends on the area, performance and power requirements in typical of these applications. Recently, a few papers discussed feasibility of ECC based PKI on RFID tags [5]. We analyzed various standardized cryptographic algorithms which have a high level of security, optimized the implementation for application in passively powered RFID tags. This helps protocol designers to estimate costs more accurately. Table I explains the main features of the realized crypto modules SHA-256, SHA-1, MD5, AES-128, and ECC-192. Table I shows that public key computation (ECC-192) take much longer. Moreover, ECC is in terms of power consumption and chip area more cost intensive. The implementation in a modern process technology could solve in future. The comparison of the other algorithms shows that AES-128 is best suitable for implementation in passive RFID tags because it requires by far the smallest chip area. AES-128 also features the lowest power consumption. Additionally, the higher level of security (128 bits) in comparison to competing algorithm MD5 puts the slightly higher 1,032 clock cycles into perspective. The comparison gives strong arguments for favoring AES [6].

VI. Conclusion

We analyses a new type of simple a framework necessity 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. For security and privacy problems mostly cryptographic techniques can be used. Additional techniques like intelligent application behaviour could be developed to bring more security to RFID systems. Because RFID requires involvement of many different areas.

References

[1] M. Rieback, B. Crispo, and A. Tanenbaum, "RFID Guardian: A Battery-powered Mobile Device for RFID Privacy Management," in Australasian Conference on informaiton Security and Privacy - ACISP 2005, vol. 3574 of LNCS, pp. 184-194, July 2005.

[2] A. Juels, P. Syverson, and D. Bailey, "High-power proxies for enhancing RFID privacy and utility", Privacy Enhancing Technologies (PET), 2005

[3] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions," in 11th IFIP International Conference on Personal Wireless Communications – PWC06, ser. Lecture Notes in Computer Science, vol. 4217. Springer-Verlag, September 2006, pp. 159 – 170.

[3] T. Dimitriou, "A Secure and Efficient RFID Protocol that Could make Big Brother (partially) Obsolete", in Proceedings of IEEE PerCom, 2006.

[4] Ari Juels, "RFID Security and Privacy: A Research Survey," IEEE journal on selected areas in communications VOL. 24, NO. 2, Feb 2006, 381-394

[5] C.P.Schnorr. "Efficient identification and signatures for smart cards", Advanced in Cryptology, Crypto'89, v.LNCS435, pp.239-252, Springer, 1989.

[6] Martin Feldhofer, "Strong crypto for RFID Tag, - A comparison of low power hardware implementation", 2007 IEEE, pp.1839-1842.