International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 5 (2013), pp. 425-432

http://www. irphouse.com /ijict.htm

Security in RFID Networks and Protocols

Kapil Singh

Indira Gandhi National Open University.

Abstract

RFID identification is a new technology that will become ubiquitous as RFID tags will be applied to every-day items in order to yield great productivity gains or "smart" applications for users. However, this pervasive use of RFID tags opens up the possibility for various attacks violating user privacy. I outline a research agenda for networks and protocols for densely populated RFID based systems covering a wide geographic area. This will need multiple readers collaborating to read RFID tag data.

Radio frequency identification (RFID) networks are an emerging type of network that is posed to play an important role in the Internet-of-Things (IoT). One of the most critical issues facing RFID networks is that of security. Unlike conventional networks, RFID networks are characterized by the use of computationally weak RFID tags. These tags come with even more stringent resource constraints than the sensors used in sensor networks. In this chapter, we study the security aspects of RFID networks and communications.

I designed our protocol with both tag-to-reader and reader-to-tag authentication in mind; unless both types of authentication are applied, any protocol can be shown to be prone to either cloning or privacy attacks. My scheme is based on the use of a secret shared between tag and database that is refreshed to avoid tag tracing. However, this is done in such a way so that efficiency of identification is not sacrificed. Additionally, our protocol is very simple and it can be implemented easily with the use of standard cryptographic hash functions.

1. Introduction

Radio frequency identification (RFID) technology consists of small inexpensive computational devices with wireless communication capabilities. Currently, the main

application of RFID technology is in inventory control and supply chain management fields. In these areas, RFID tags are used to tag and track physical goods. Within this context, RFID can be considered a replacement for barcodes. RFID technology is superior to barcodes in two aspects. First, RFID tags can store more information than barcodes. Unlike a barcode, the RFID tag, being a computational device, can be designed to process rather than just store data. Second, barcodes communicate using an optical channel, which require the careful positioning of the reading device with no obstacles in-between. RFID uses a wireless channel for communication, and can be read without line-of-sight, increasing the read efficiency. The pervasiveness of RFID technology in our everyday lives has led to concerns over whether these RFID tags pose any security risk. The future applications of RFID make the security of RFID networks and communications even more important than before. The ubiquity of RFID technology has made it an important component in the Internet-of-Things (IoT), a future generation Internet that seeks to mesh the physical world together with the cyber world . RFID is used within the IoT as a means of identifying physical objects. For example, by attaching an RFID tag to medication bottles, we can design an RFID network to monitor whether patients have taken their medications.

2. RFID Technology Overview

An RFID system can be broken down into two key dimensions. The technical infrastructure includes the actual data capture technology comprised of tags, readers, and transmission medium.

2.1 An infrastructure of an RFID system

The technical infrastructure comprises a radio transponder and receiver, more commonly known as a tag and reader. Information related to a given object is stored on an affixed tag and transmitted to a reader over a radio frequency (RF) connection. The reader in turn connects via wired or wireless networks to servers hosting RFID applications that make use of transmitted RFID data, and, in the case of supply chain applications, middleware manages the flow of RFID data between readers and enterprise applications. Figure 1 shows the key technical components of an RFID system.

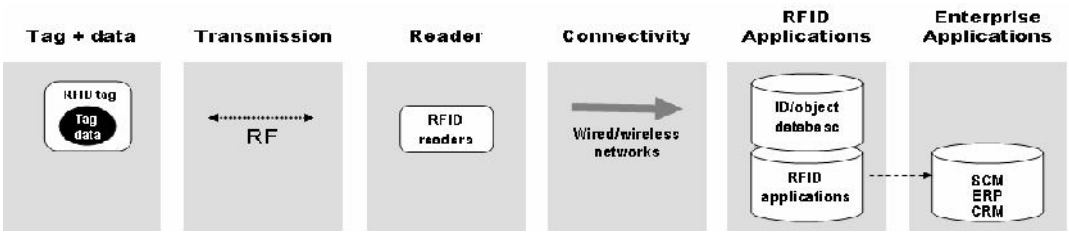

Figure 1: Technical components of an RFID system. This photograph appears courtesy of (This photograph appears courtesy of by Natalie Klym, Charlie Fine).

2.2 RFID Tags

Tags contain a microchip and a transponder. The microchip stores data related to the object and the transponder transmits that data to readers. Tags are initially programmed (data is written to the tags) at the point of manufacture (factory programming), but can also be programmed by an OEM or end user (field programming). Tag data usually includes a unique identifier code and sometimes additional information, depending on the application and the amount of memory on a tag. Tags are either passive or active. Passive tags are smaller -- about the size of a grain of rice, and getting smaller. They are activated when they enter the range of a reader's signal. The reader's antenna sends power to the transponder, activating the data stream. (Semi-passive tags have a battery that runs the circuitry of the chip, but does not power transmission of data to the reader.)

Passive tags are much smaller in size and memory than active tags, and cheaper to manufacture. Tags can be printed on paper or plastic and attached to an object, or they can be embedded under the skin of animals and humans.

Types of RFID Tags: - There are three general types of RFID tags, active, semi-active, and passive RFID tags.

- *Active tags:* - This type of RFID tag contains an internal battery which is used to let the tag perform more complex operations, such as monitor temperature, as well as boost the communication with an RFID reader. The communication range of an active tag can be over 100 meters. An active tag is the most powerful type of RFID tag, and is also the most expensive.
- *Semi-active tags:*-This type of tag also contains an internal battery, but unlike an active tag, the battery is only used for the tag's internal operations, and not for communication. A semi-active RFID tag relies on RFID reader to supply the necessary power for communication. Note that semi-active tags are sometimes known as semi-passive tags.
- *Passive tags:* - This type of RFID tag have the lowest cost (pennies per tag), and unsurprisingly, are the most prevalent type of RFID tags. A passive tag has no internal batteries, and relies on the RFID reader to supply the power needed to perform all tag operations and communication. In the rest of this chapter, our focus is on this type of tags.

2.3 RF Connection

Tags transmit data to readers over different radio frequencies, depending on the application needs. RF frequencies are dividing into several bands including low frequency (LF), high frequency (HF), ultra-high frequency (UHF), and microwave. Passive tags transmit at all frequencies while active tags transmit at higher frequencies only (those in the UHF and microwave bands). The exact frequency that can be used within the various bands, as well as power (output) levels, are controlled by the

regulatory body of each country. Each frequency varies in terms of regulation, performance (range, bandwidth, output), and the size and cost of the associated technology. Over the last few decades, RFID solutions have emerged around only a few frequencies, each of which optimizes these variables to meet the needs of the different application types.

2.4 RFID Readers

Readers are larger, more complex, and more expensive pieces of RFID hardware compared to tags. The reader captures the information transmitted by a tag, decodes it and delivers it to a host computer for ID resolution (if applicable) and further processing. Some readers come with "write" capabilities, meaning they can add or change (reprogram) the data on a tag. Readers have traditionally connected to the host computer over wired networks, but some of the newer readers will use Bluetooth, WiFi, or WiMax connections to transfer data to servers. For example, the IDBlue is a handheld Bluetooth-enabled RFID reader that connects to the RFID application server via a Bluetooth connection.10 Readers embedded in cell phones connect to content using the mobile phone network.

3. Security Requirements in RFID

The challenges in security RFID networks lie in securing the operations involving RFID tags. This is because the severe resource limitations of tags make it difficult to implement conventional security mechanisms. RFID readers and backend servers on the other hand, can be secured using existing security techniques.

3.1 Threats on RFID System

Spoofing, Insert, Replay, and Denial of Service (DOS) attacks.

3.1.1 Spoofing: *Spoofing* attacks supply false information that looks valid and that the system accepts. Typically, spoofing attacks involve a fake domain name, Internet Protocol (IP) address, or Media Access Code (MAC).

3.1.2 Insert: Insert attacks insert system commands where data is normally expected. These attacks work because it is assumed that the data is always entered in a particular area, and little to no validation takes place. *Insert* attacks are common on Web sites, where malicious code is injected into a Web-based application. A typical use for this type of attack is to inject a Structured Query Language (SQL) command into a database.This same principle can be applied in an RFID situation, by having a tag carry a system command rather than valid data in its data storage area.

3.1.3 Replay: In a *replay* attack, a valid RFID signal is intercepted and its data is recorded; this data is later transmitted to a reader where it is "played back." Because the data appears valid, the system accepts it.

3.1.4 DOS: *DOS* attacks, also known as *flood* attacks, take place when a signal is flooded with more data than it can handle. They are well known because several large DOS attacks have impacted major corporations such as Microsoft and Yahoo.

3.2 RFID Network Security requirements: Prevent unauthorized access, prevent illicit tracking, and prevent or detect skimming. These form the basic requirements for most RFID applications.

3.2.1 Prevent unauthorized acces: There are two ways which unauthorized access can occur. The first is when an unauthorized RFID reader queries and obtains usable information such as the tag ID from the RFID tag. RFID tag design requires the tag to respond to any query. Any reader can query the tag and get a response. Preventing unauthorized access refers to allowing only authorized readers to obtain usable information. The second way which unauthorized access can occur is via eavesdropping. An adversary obtains usable information by observing the over-the-air communications between a legitimate reader and a tag.

3.2.2 Prevent illicit tracking: This requirement addresses one of the main privacy concerns over the use of RFID technology. Illicit tracking exploits the fact that RFID tags always respond to reader's query. An adversary that queries and obtains the same tag response at multiple locations can infer that the same tag has visited those locations. Since RFID tags are affixed to physical objects, for instance clothing, this implies that the same person has visited those locations. Note that satisfying the first requirement does not automatically satisfy this requirement. A tag that returns a constant, encrypted response will prevent unauthorized access, since the adversary cannot determine the tag contents. However, the constant cipher text can be used to perform illicit tracking.

3.2.3 Prevent or detect skimming: Skimming is an attack whereby the adversary observes the interactions between a legitimate RFID reader and a tag, and tries to create a fake RFID tag that mimics a real one. The adversary succeeds when his fake tag can pass off as a real tag. Skimming is a concern when RFID is used to authenticate documents such as driver licenses or passports. For instance, an adversary that tries to create a fake drivers license may attempt to observe the interactions of an RFID tag embedded in a legitimate drivers license to create his fake RFID tag. Generally, the adversary performing a skimming attack does not have physical access to the RFID tag.

3.2.4 Defending against Mafia fraud: The mafia fraud has emerged as a challenging problem for RFID applications. This type of attack cannot be defended by the protocols mentioned earlier because a legitimate RFID reader is accessing data from a legitimate RFID tag. In other words, this type of attack can still work even if both the reader and the tag authenticate each other. Consider an application which uses RFID tag to open a door. The RFID reader will first read the tag and then transmit the

information to the backend server. Once the backend server verifies the tag is legitimate, the door will open. To launch a mafia fraud attack, the adversary will first be in close proximity with a person holding a legitimate RFID tag. We refer to this person as the target. The adversary's accomplice will be standing near to the door. When the legitimate RFID reader issues a query, the adversary's accomplice will relay this message to the adversary, who will in turn issue it to the target's RFID tag. The target's RFID tag will respond to the adversary, who will then relay this back to his accomplice to transmit to the RFID reader. Since the RFID reader obtains the response from a legitimate RFID tag, the door will open and the adversary can gain access. Therefore the choice of protocol does not defend against this type of attack. The intuition behind the defending against a mafia fraud is to accept an RFID tag's response if it is both valid and timely. Since the wireless transmission speed, the RFID tag computational time, and distance between the reader and tag are known, the RFID reader can estimate the amount of time needed to receive a response. If the arrival of the RFID tag response is late, the reader can deduce the distance travelled is longer than what is allowed, and thus reject the tag answer.

4. Conclusion

In this chapter, i studied the problem securing RFID networks and communications. This paper focused on the weakest link, which is between the RFID reader and the RFID tag. I described the characteristics of each of the components that make up an RFID network, and then categorized the security requirements for an RFID network. I studied the conventional protocol based approach towards RFID security. I studied protocols that can address the basic security requirements of preventing unauthorized access, illicit tracking, and skimming. I then turned our attention to security protocols that provide more advance security requirements of preventing mafia attack and providing grouping proofs. This paper summarizes some of the key research in the security of RFID networks and communications, and i hope that my work can be used as a building block for future investigations into this problem.

References

[1] Alomair, Basel, and Radha Poovendran. "Privacy versus Scalability in Radio Frequency Identification Systems." *Computer Communication, Elsevier.* 2010.

[2] Avoine, Gildas. *RFID Security & Privacy Lounge.* 2011. http://www.avoine.net/rfid/.

[3] Avoine, Gildas, Kassem Kalach, and Jean-Jacques Quisquater. "ePassport: Securing International Contacts with Contactless Chips." *Financial Cryptography* . 2008.

[4] Avoine, Gildas, Muhammed Ali Bingol, Suleyman Kardas, Cédric Lauradoux, and Benjamin Martin. "A Framework for Analyzing RFID Distance Bounding Protocols." *Journal of Computer Security -- Special Issue on RFID System Security*, 2010.

[5] Bolotnyy, Leonid, and Gabriel Robins. "Generalized "Yoking-Proofs" and Inter-tag Communication." In *Development and Implementation of RFID Technology*. I-Tech Education and Publishing, 2009.

[6] Burmester, Mike and de Medeiros, Breno and Motta, Rossana. "Provably Secure Grouping- Proofs for RFID Tags." *Smart Card Research and Advanced Applications (CARDIS)*, 2008.

[7] Cai, Shaoying, Yingjiu Li, Tieyan Li, Robert H. Deng, and Haixia Yao. "Achieving High Security and Efficiency in RFID-tagged Supply Chains." *International Journal of Applied Cryptography*. 2010.

[8] Capkun, Srdjan and El Defrawy, Karim and Tsudik, Gene. *GDB: Group Distance Bounding Protocols.* arXiv.org, 2010.

[9] Chatmon, Christy, Tri van Le, and Mike Burmester. *Secure Anonymous RFID Authentication Protocols.* Florida State University Technical Report, 2006.

[10] Chothia, Tom, and Vitaliy Smirnov. "A Traceability Attack against e-Passports ." *Financial Cryptography*, 2010.