Security in RFID Tags

M. Angel Jasmine Shirley
M.C.A., M.Phil., M.Ed., Ph.D Research Scholar, JJT University, Rajasthan, India

Abstract: Radio Frequency Identification RFID is a wireless automatic identification and data capture technology that uses radio waves to identify objects such as products, animals or persons, collecting data about them, and entering that data directly into computer systems. RFID-tags are a new generation of bar-codes with added functionality. They are becoming very popular tools for identification of products in various applications mainly for anti-counterfeiting by embedding them into a product. A passive RFID tag is a microchip that is capable of transmitting a static identifier or serial number for a short distance. It is typically activated by a query from a nearby reader, which also transmits power for the operation of the tag. Privacy is one of the most important security concerns in RFID. One approach to addressing privacy and security threats is to use a tag authentication scheme in which a tag is both identified and verified in a manner that does not reveal the tag identity to an eavesdropper. Another possible solution is the use of a privacy-enhancing cryptographic protocol to protect RFID communications.

Keywords - *RFID, authentication, Cryptography, cipher text*

I. INTRODUCTION

In recent years, the growth of counterfeit goods has experienced a rather steep increase. Such increase translates into a large source of losses for manufacturers. In the copyright industry, almost 50% of all motion picture videos, more than 40% of all business software, and a third of all music recordings are pirated copies, about 10% of clothing, fashion and sportswear are fake and the online sales of luxury goods reaches 25 billion USD annually, in the automotive industry 5% to10% of all spare parts are counterfeits, and between 5% and 8% of the 500 billion USD in medicines sold worldwide are counterfeit as estimated by WHO, In developing countries the percentage of counterfeit drugs account for up to 60% of all drugs. Counterfeit products have a direct (negative) impact on the health and life of thousands of people worldwide. It is clear that new technologies need to be put in place to thwart the counterfeiting threat. RFID has been identified as one of these technologies.

The use of RFID as an anti-counterfeiting technology is at present rather primitive. The whole security relies on the premise that an RFID tag is harder to copy than a bar code. RFID-tags contain some secret reference information that is used to check their authenticity. In order to avoid counterfeiting, RFID-tags have to be unclonable. First, it should be hard to make a physical clone. Secondly, retrieving the secret reference information by attacking the protocols that are carried out between the reader and a tag (proving its authenticity) should be unfeasible [5]. Protection against physical unclonability is provided by using physical countermeasures such as Physical Unclonable Functions and protection against active or passive attacks on the protocols is provided by cryptographic techniques such as digital signatures and secure identification protocols [1, 2]. In short, RFID-based 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 [5].

II. AUTHENTICATION PROTOCOLS

A customer holding an RFID ticket might not want anybody else to be able to track his movings. One option to preempt such a worry is to build secure RFID authentication protocols, in order to ensure privacy for RFID users. Thus, an RFID system should provide *anonymity* (the identity of the tag should be kept secret) and *untraceability*(it should not be possible to link two different tag communications) for a user[6]. Thereby, the design of secure and privacy-preserving RFID protocols requires an attentive and methodical analysis of its characteristics.

III. SYSTEM ARCHITECTURE

The system architecture is shown in Fig. 1. The whole system consists of three main parts, namely, active RFID tag, RFID reader, and back-end processing platform. The back-end processing platform includes two parts: key center and database system. Both the RFID tags and RFID readers are composed of power-saving microprocessor MSP430 and low-power RF module. The RFID reader is equipped with power management function so that it can be powered by AC power as well as alkaline batteries to provide more flexibility to the system.

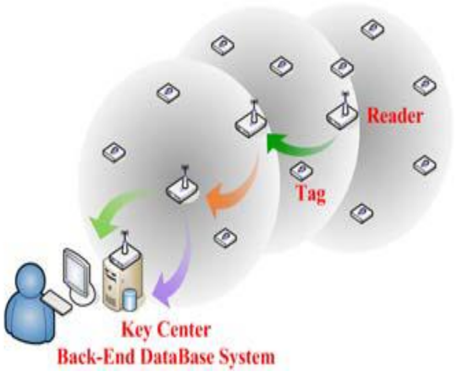

Fig. 1.RFID system architecture.

The RFID reader plays an important role in the RFID system. In the wireless transmission network, the RFID reader not only can receive the data in the tag within transmission range but also can relay the received and collected data to the next reader closer to the back-end processing platform. In this multi-hop relaying mechanism, the data can eventually be transmitted to the back-end processing platform. The last reader that is connected to the back-end platform is responsible to convert the received data packets to RS-232C frames and to send the data to the key center and the database system for further processing[1,2].

The tags have to go through the following steps as in fig 2.

- The tag has to be registered to the back-end processing platform before it is distributed. The key center will record the information of the tag, the public key Kpublic and private key Kprivate in the database in the back-end processing platform.

- After the registration the tag will store the registered sequence number and the public key Kpublic in its memory that will be used to encrypt the plain text message sent back to the reader [5].
- The reader will include in the challenge command a random number that will be used to authenticate the tag. The tag will include this number in its plain text that will be sent back after encryption.

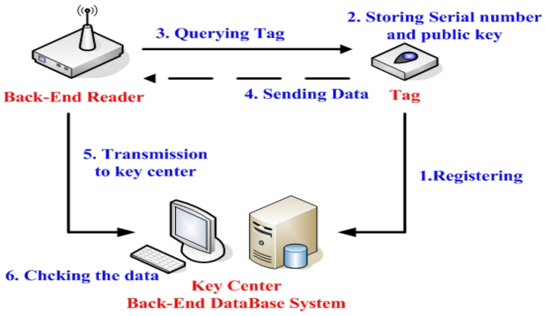

Fig. 2.The setup flow diagram.

- After receiving the challenge command from the reader the tag extract the random number in it whichwill then be combined with the registered sequence number and a random number that is generated by the tag itself as the content of plain text. The plain text will then be encrypted using the public key .The cipher text will then be transmitted to the reader. The random number is included in the plain text so as to produce different encrypted packets even if the tag receives the same packets every time to prevent tracking from attackers using forged reader packets.
- After receiving the response packets from the tag the reader will transmit the packets to the back-end authentication server via multi-hop relaying mechanism.
- After receiving the cipher text transmitted from the reader the back-end server will use the private key Kprivate to decipher it and to verify whether the registered sequence number and the random number in the plain text are the same as the one in database and the one transmitted by the reader respectively. If they are indeed the same then it can be concluded that the data is really transmitted by a legal tag and subsequently terminate the whole authentication process.

IV. CRYPTOGRAPHIC PRIMITIVES

Cryptography is the study of mathematical techniques to hide information. The fundamental objective of cryptography is to enable two parties to communicate over an insecure channel in such a way that an adversary cannot understand and/or manipulate what is being said. This channel could be a telephone line, computer network, or wireless interface. Cryptographic techniques can be divided into symmetric and asymmetric techniques, depending on the nature of the keys used[3].

V. SYMMETRIC TECHNIQUES

In a symmetric cryptographic algorithm, the sender and receiver must share a secret key.

A. Symmetric Encryption

There are a variety of different types of symmetric encryption techniques, also known as secret key encryption algorithms. The most widely discussed class of symmetric cipher is the block cipher. In a block cipher, data are processed in blocks, for example, of 64 or 128 bits. A block cipher algorithm is made up of encryption and decryption functions. Encryption takes as input a block of plaintext and a secret key, and outputs a block of cipher text. Decryption, when given the same secret key, always maps a cipher text block back to the correct plaintext block [1,3,4].

B. Message Authentication Codes

A Message Authentication Code (MAC) algorithm is a cryptographic function that takes as input a message and a secret key, and outputs a short, fixed length, block of bits known as the MAC. This MAC is then sent or stored with the message, and acts to protect its integrity and guarantee its origin. If the recipient of a MAC is equipped with the correct secret key, then the key can be used with the received message to re-compute the MAC value and if this value agrees with the MAC value sent or stored with the message, then the recipient knows that the message has not been changed and that it must have been sent by someone who knows the secret key [4].

C. Hash Functions

Hash functions do not use keys. A hash function takes an input an arbitrary data string and gives as output a short, fixed-length value that is a function of the entire input; this output is known as a hash code or hash value . Hash functions must have the one-way property, that is, they must be designed so that they are simple and efficient to compute.

D. Pseudo-Random Bit Generators

A pseudo-random bit generator (PRBG) is a deterministic algorithm which, given a truly random binary sequence of length m, outputs a binary sequence of length l > m which appears to be random. The input to the PRBG is called the seed, while the output of the PRBG is called a pseudo-random bit sequence [2,4].

VI. ASYMMETRIC TECHNIQUES

In asymmetric cryptography (public key cryptography), every participating entity has its own key pair, made up of a private key, which is kept secret by its owner, and a public key, which can be disseminated freely. These public and private keys are related mathematically, and an entity's private key cannot be derived from its public key. Two main classes are asymmetric encryption algorithms and digital signature schemes.

A. Asymmetric Encryption

Asymmetric encryption, involves an encryption operation that transforms blocks of plaintext into cipher text blocks, and a decryption operation that reverses this process. The main difference from symmetric encryption is the way in which keys are used. The public key of the intended recipient of a message is used for encryption and the recipient's private key is used for decryption [1,2,3]. A user's public key is made available to anyone who wants to encrypt a message intended for that user. The recipient's private key is used to decrypt received encrypted messages.

B. Digital Signatures

A digital signature is computed as a function of the message to be signed using the signer's private key, and can then be verified by anyone equipped with the signer's public key. When computing a signature, a hash function is applied to the message being signed. The most common form of a signature gives a value that, much like a MAC, is sent or stored with the message it is protecting .One key difference from a MAC is the way in which signatures are verified. Verifying a MAC essentially involves re-computing it. However, verifying a digital signature uses a special verification function that takes as input the signature, the message and the public verification key, and gives as output an indication as to whether the signature is valid or not [3,4].

CONCLUSION

Currently RFID technologies have been applied to various applications. Examples for RFID tags are the small plaques mounted on car windshields for the purpose of automated toll payment, the theft-detection tags attached in shops to consumer goods such as clothing, and the proximity cards used to control physical access to buildings [6]. The privacy and security of data have become major issues in these RFID applications. Simple hash functions, symmetric or asymmetric encryption algorithms, or even hardware have been used to solve the security problem. To reduce the cost, researchers have hoped to use software to replace hardware. The focus has thus been on the development of security algorithms. With the introduction of authentication and security technologies, we do not have to worry any more about the stealing of information from illegal readers or from stealers. The multi-hop mechanism can transmit data collected by the remote readers via relaying so that we do not have to set up a computer for each single reader. This can substantially reduce the total system cost. Thus, devising appropriate formalism for use in specifying and analysing RFID protocols remains a challenging and potentially fruitful topic.

References

[1] J. Menezes, P. C. van Oorschot, and S. A. Vanstone, “Handbook of Applied Cryptography”, volume 6, CRC Press, 1996.

[2] B.Schneider, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, John Wiley & Sons, Inc., New York, NY, USA, 1996.

[3] W. Stallings, “Cryptography and Network Security: Principles and Practice”, Prentice Hall, Upper Saddle River, New Jersey, second edition, 1999.

[4] D. Stinson, “Cryptography: Theory and Practice”, CRC Press, Boca Raton, Florida, second edition, 2002.

[5] F. Thornton, B. Haines, A. M. Das, H. Bhargava, A. Campbell, and J. Kleinschmidt. RFID Security. Syngress, Massachusetts, USA, 2006.

[6] A. Laurie. “Practical attacks against RFID. Network Security”, pp.4-7, September 2007