Chapter 16

Security of Information Exchange Between Readers and Tags

Nabil Kannouf  
Mohammed I University, Morocco

Mohamed Labbi  
Mohammed I University, Morocco

Mohammed Benabdellah  
Mohammed I University, Morocco

Abdelmalek Azizi  
Mohammed I University, Morocco

ABSTRACT

RFID (radio frequency identification) systems tend to be one of the most predominant computing technologies due to their low cost and their broad applicability. Latest technologies have brought costs down, and standards are being developed. Now the RFID technology is very important and essential. It is used for innovative applications in personnel services. RFID technology is based on tags, distance and frequency, communication mode, antenna and power transfer, and communication. The attacks are based on the way the RFID systems are communicating and the way that are transferred between the entities of an RFID network (tags, readers). Securing information exchange between readers and tags needs some cryptography methods like symmetric (affine method, block stream method, etc.) or asymmetric (RSA, ECC, etc.) key methods. In this chapter, the authors compare methods based on complexity and power. Then they choose the best for securing communication between RFID tags and RFID readers.

INTRODUCTION

RFID Systems are going the most useful in several domains such as logistics, library, health care and other domains. Roy Want defines RFID system by radio frequency identity technology has moved from obscurity into main stream applications that help speed handling of manufactured goods and materials.
In the last years, RFID technology replace barcode technology because it gets more advantage such as independence of line sight, store more information and scanning more than one tag in same time. The question is how we can secure the exchanging information between Tag and Reader?

RFID technology was passed on several stages, from his creation to know. The first using of this technology is from World War II between 1940 and 1950. Know the RFID technology is very important and essential for our life. It is used for innovative applications in personnel services.

RFID technology is based on tags, distance and frequency, communication mode, antenna and power transfer and communication. Tags are classed on three categories: passive, semi-passive and active tag. Distance and frequency are the most characteristics of RFID technology. Communication mode, there are many operation and communications modes of tags, are following: read only, reading and / or writes multiple, reading and / or writing protected using passwords and secure and encrypted read and / or writing. Antenna and power transfer, with regard to transponders, there are many types of differentiated by their shapes, components, their earnings and producing technologies. They are always special for transponder type (according to be characteristics of the integrated circuit or other), application and frequency of use. From the form point of view, we can mention the antennas in one shape (round flat square, eight, etc.) or two-dimensional (cylindrical, etc.). Communication, passive tags do not have a power source. Instead of this, tags are powered by the reader and can only respond after receiving a message from the reader. The communication is half-duplex, simultaneous transmission and reception are not allowed. The communication between tag and reader in the EPC Gen2 system is organized in 3 stages: Selection, Inventory and also Access stages.

BACKGROUND

RFID Tags and RFID Readers

In this section, the authors begin the detailed discussion of RFID technologies starting with the most components of every RFID system; that is the reader and the tag. These two devices have an asymmetric relationship in the tag is simple and offers few facilities besides holding and transmitting the code, while the reader takes the leading role at the cost of higher complexity.

RFID Tags

Different types of RFID transponders exist, a device without built-in circuit, hold in the printed electronics tags, the Surface Acoustic Wave tags and the Thin Film Transistors Circuit (TFTC) tags (Kannouf, Douzi, Benabdellah & Azizi [KDBA], 2015). Also, a semiconductor device (excluding integrated circuit), this device in constructed by diode capacity. Similarly, a device to constructed circuit, still account the greatest part of the RFID market. With last type, tag is broadly classified as active, semi-active or passive. An active tag requires a power source and is either connected to a powered device or to a battery and is often limited by the lifetime of its source because is used to send and processing an integral data. Being dependent on a power source puts limitations on active RFID tags. Price, length, lifetime make them no practical for regular use. Also, a semi-passive tag needs a power source and it used for processing an integral data. On the other side, passive RFID is interest because the fact they are independent of power source and maintenance (Figure 1).