International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST

New Applications of RFID And Security Threats

Ankesh Kumar[1], Dr. K. B. Singh[2], Dr. Pankaj Kumar[2]
[1]Research Scholar, University Department of Physics, B. R. A. Bihar University, Muzaffarpur, Bihar, India
[2]P. G. Department of Physics, L. S. College, Muzaffarpur, B. R. A. Bihar University, Muzaffarpur, Bihar, India

ARTICLEINFO

Article History:

Accepted: 10 Nov 2023
Published: 24 Nov 2023

Publication Issue
Volume 10, Issue 6
November-December-2023

Page Number
521-525

ABSTRACT

In this research paper, we have described the various cryptographic properties and security features of RFID systems. Radio-frequency identification is a technology for the automated identification of objects and people. RFID is one of the most challenging devices in recent years in many fields such as wireless communication, circuits and electromagnetic areas. The reason is that there are so many potential or ongoing applications of RFID systems such as supply chains, livestock/inventory tracking, toll management, airline baggage management, access control, and so on. Operational and security requirements for RFID systems such as system scalability, anonymity, and ant-cloning are difficult to obtain due to constraints in area, memory, etc.

Keywords - RFID, RFID Tags, Counterfeiting, Authentication, Adversary, Ant-Cloning.

I. INTRODUCTION

RFID (Radio Frequency Identification) is one of the most challenging devices in recent years. It is being used in many fields such as wireless communication, circuits, and electromagnetic areas. The reason is that there are so many potential or ongoing applications of RFID systems such as supply chains, livestock/inventory tracking, toll management, airline baggage management, access control, and so on. It can also be used to discriminate between counterfeits and authentic products. Especially since the adoption of EPCglobal Gen2 [1], the RFID is expected to completely replace the barcode systems soon. For commercial markets, RFID systems should overcome not only the restriction of cheap RFID tags but also operational and security problems such as scalability, the tracking problem, and the cloning problem. In many cases, the security part is simplified to minimize a tag's price. For example, Class-1 EPCglobal Gen2 [1] has a very simple authentication scheme where a password is transmitted in plain text, which can cause many security problems. Fortunately, the CMOS technologies steadily advance, and the fabrication costs decrease, which allows stronger security solutions on tags. Moreover, some applications such as expensive goods and access control systems that should be highly secured can afford more expensive

tags which may include more resources such as an extra power source, gate area, and memory.

RFID is supposed to be the successor of the optical barcode printed on consumer products, with two individual advantages:

i. Unique identification: A barcode indicates the type of object on which it is printed, e.g., "This is a 50-gram bar of XYZ brand 70% chocolate." An RFID tag goes a step ahead. It emits a unique serial number that distinguishes among many millions of identically manufactured objects; it might indicate, e.g., that "This is 50 grams bar of XYZ brand 70% chocolate, serial no. 887891873." The unique identifiers in RFID tags can point to a database entry containing rich transaction histories for individual items.

ii. Automation: Barcodes, being optically scanned, require line-of-sight contact with readers, and thus watchful physical positioning of scanned objects. Except in the most rigorously controlled environments, barcode scanning requires human intervention. In contrast, RFID tags are readable without line-of-sight contact and precise positioning. RFID readers can scan tags at rates of hundreds per second. For example, an RFID reader by a warehouse dock door can today scan stacks of passing crates with high accuracy. In the future, point-of-sale terminals may be able to scan all of the items in passing shopping carts [2].

II. REVIEW OF THE WORK

In this section, we have described the technology of RFID system, frequencies in RFID, and RFID tags.

A. The Technology RFID

With RFID, the electromagnetic or electrostatic coupling in the RF (radio frequency) portion of the electromagnetic spectrum is used to transmit signals. An RFID system consists of an antenna and a transceiver, which reads the radio frequency and transfers the information to a processing device (reader) and a transponder, or RF tag, which contains the RF circuitry and information to be transmitted. The antenna provides the means for the integrated circuit to transmit its information to the reader that converts the radio waves reflected from the RFID tag into digital information that can then be passed on to computers that can analyze the data. In RFID systems, the tags that hold the data are broken down into two different types. Passive tags use the radio frequency from the reader to transmit their signal. Passive tags will generally have their data permanently burned into the tag when it is made, although some can be written. Active tags are much more sophisticated and have an on-board battery for power to transmit their data signal over a greater distance and power random access memory (RAM) giving them the ability to store up to 32,000 bytes of data.

B. Frequencies of RFID

Much like tuning in to your favorite radio station, RFID tags and readers must be tuned into the same frequency to enable communications. RFID systems can use a variety of frequencies to communicate, but because radio waves work and act differently at different frequencies, a frequency for a specific RFID system is often dependent on its application. High-frequency RFID systems (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) offer transmission ranges of more than 90 feet, although wavelengths in the 2.4 GHz range are absorbed by water, which includes the human body, and therefore have limitations.

C. RFID Tags

RFID tags are small devices used for identification purposes in many applications nowadays. It is expected that they will enable many new applications and link the physical and the virtual world shortly. Since the processing power of these devices is low, they are often in the line where their security and privacy are concerned. It is widely believed that devices with such constrained resources cannot carry

out sufficient cryptographic operations to guarantee security in new applications. RFID tags consist of an antenna connected to a microchip. Because of the presence of this microchip, they can be considered as the next-generation bar codes. One of their main advantages over bar codes is that they can be read out without line of sight. It is expected that shortly trillions of these devices will be deployed. They will be used to identify goods and provide a link between the physical and the virtual world. It is predicted that this connection will lead to the next revolution after the Internet: The Internet of Things. Currently, the main applications for RFID tags include goods tracking in supply chain management, automated inventory management, automated quality control, access control, payment systems, etc. In the future, however, tagged items will also communicate with intelligent devices in the home (intelligent fridges, washing machines, etc.) and provide additional benefits to consumers. Recently a lightweight version of such an authentication protocol was developed in [3]. The security of the protocol is based on the Learning Parity in the presence of Noise (LPN) problem. The protocol in [3] is proven secure against passive and active adversaries in a detection-based model.

D. Common use of RFID System

RFID systems can be used just about anywhere, from clothing tags to missiles to pet tags to food - anywhere that a unique identification system is needed. The tag can carry information as simple as a pet owner's name and address or the cleaning instructions on a sweater to as complex as instructions on how to assemble a car. Here are a few examples of how RFID technology is being used in everyday places: RFID systems are being used in some hospitals to track a patient's location, and to provide real-time tracking of the location of doctors and nurses in the hospital. In addition, the system can be used to track the whereabouts of expensive and critical equipment, and even to control access to drugs, pediatrics, and other areas of the hospital that are considered "restricted access" areas. RFID chips for animals are extremely small devices injected via a syringe under the skin. Under a government initiative to control rabies, all Portuguese dogs must be RFID tagged within a given time limit. When scanned the tag can provide information relevant to the dog's history and its owner's information. RFID in retail stores offers real-time inventory tracking that allows companies to monitor and control inventory supply at all times. The Orlando/Orange County Expressway Authority (OOCEA) is using an RFID-based traffic-monitoring system, which uses roadside RFID readers to collect signals from transponders that are installed in about 1 million E-Pass and Sun Pass customer vehicles.

E. The features of RFID

RFID is said by many in the industry to be the frontrunner technology for automatic identification and data collection. The biggest, as of yet unproven, benefit would ultimately be in the consumer goods supply chain where an RFID tag attached to a consumer product could be tracked from manufacturing to the retail store right to the consumer's home. Many see RFID as a technology in its infancy with untapped potential. While we may talk of its existence and the amazing ways in which this technology can be put to use, until there are more standards set within the industry and the cost of RFID technology comes down we won't see RFID systems reaching near their full potential anytime soon.

III.MODEL OF RFID SYSTEM

RFID authentication system has three components: tags T, readers R, and a trusted server S. Tags are wireless transponders: they typically have no power of their own and respond only when they are in an electromagnetic field. Readers are transceivers and generate such field: they challenge by broadcasting any responding tag. There are two types of broadcast challenges: multicast and unicast. Multicast challenges are addressed to all tags in the range of the reader, whereas unicast challenges are addressed to specific

tags. In our protocols below we have both types of challenges. However, our multicast challenges are just random strings, and all tags in the range of a reader R are challenged with the same random string. This kind of action is not usually counted as a communication pass.

We shall assume that all “honest” tags T adhere to the system specifications and the requirements of the authentication protocol. The same applies for the reader R and of course the trusted server S - they are all “honest". Tags are issued with private keys K which they share (only) with the trusted server S. These keys are used by the tags for identification. We denote by K the set of all authorized keys (issued by S). Figure 1 illustrates the flow of exchanged data between a tag T and the trusted server S via the reader R, during the authentication of T.

$$T \leftrightarrow R \Leftrightarrow S$$

Figure 1: The authentication flow in an RFID system

We shall refer to the interaction between T and R as a conversation and the data as an authentication transcript. In our RFID authentication protocols, we shall assume that R and S are linked by a secure communication channel (reliable and authenticated). Therefore, our protocols are essentially two-party protocols, one party being a tag T and the other a reader $R = R^S$, with secure access to a server S. These parties are abstracted as probabilistic Turing machines. T-machines with severely restrained resources, and R-machines with adequate resources. For “optimistic" authentication protocols, the resource must be minimized for both machines.

This model describes the setting for the “honest" parties: the tags that are authenticated with private keys $K \in K$, that adhere to the protocol, the readers R that adhere to the protocol, and the trusted server.

IV. CONCLUSION

In this research, we have discussed various important security problems and the cryptographic properties of RFID Systems. It is astonishing how a modest device like an RFID tag, essentially just a wireless license plate, can give rise to the complex melange of security and privacy problems that we explore here. RFID privacy and security are stimulating research areas that involve rich interplay among many disciplines, like signal processing, hardware design, supply-chain logistics, privacy rights, and cryptography. The majority of the articles treated in this survey explore security and privacy as a matter between RFID tags and readers. Of course, tags and readers lie at the fringes of a full-blown RFID system. At the heart will reside a massive infrastructure of servers and software. Many of the attendant data-security problems like that of authenticating readers to servers involve already familiar data-security protocols.

V. REFERENCES

[1]. “Specification of RFID Air Interface”, http:// www.epcglobaline.org.

[2]. D. White. NCR: RFID in retail. In S. Garfinkel and B. Rosenberg, editors, RFID: Applications, Security, and Privacy, pages 381–395. Addison-Wesley, 2005.

[3]. A Juels and S A Weis Authenticating pervasive devices with human protocols.In V. Shoup, editor, Advances in Cryptology: Proceedings of CRYPTO 2005, volume 3621 of Lecture Notes in Computer Science, pages 293 308. Springer-Verlag, 2005.

[4]. P. Tuyls and L. Batina RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, Topics in Cryptology - CT-RSA 2006, Lecture Notes in Computer Science, San Jose, USA, February 13-17 2006. Springer Verlag.

[5]. C. Kocher, J. Jaffe and B. June . Differential Power Analysis,CRYPTO99

[6]. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, Cryptographic Hardware and Embedded Systems, CHES 2004, volume LNCS 3156, pages 357-370. Springer, 2004.

[7]. SStephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels ”Security and

Privacy Aspects of Low-Cost Radio Frequency Identification Systems", in The First International Conference on Security in Pervasive Computing SPC 2003, March 2003.

Cite this article as :

Ankesh Kumar, Dr. K. B. Singh, Dr. Pankaj Kumar, "New Applications of RFID And Security Threats", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 6, pp. 521-525, November-December 2023.
Journal URL : https://ijsrst.com/IJSRST52310638