International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:1, 2016

Privacy of RFID Systems: Security of Personal Data for End-Users

Firoz Khan

***Abstract*—**Privacy of RFID systems is receiving increasing attention in the RFID community. RFID privacy is important as the RFID tags will be attached to all kinds of products and physical objects including people. The possible abuse or excessive use of RFID tracking capability by malicious users can lead to potential privacy violations. In this paper, we will discuss how the different industries use RFID and the potential privacy and security issues while RFID is implemented in these industries. Although RFID technology offers interesting services to customer and retailers, it could also endanger the privacy of end-users. Personal data can be leaked if a protection mechanism is not deployed in the RFID systems. The paper summarizes many different solutions for implementing privacy and security while deploying RFID systems.

***Keywords*—**RFID, privacy, security, encryption.

I. Introduction

RFID is a contactless, wireless technology that is used to identify items and capture data about these items in a system. RFID is widely used in a large range of markets, including, but not limited to large inventory supermarkets, warehouse management and logistics systems, tracking products in a supply chain system, passports, livestock identification, vehicle identification while passing through road tolls, library book systems, transportation systems like metros and buses, and patient identification in the healthcare industry.

RFID uses wireless technologies that use radio signals to identify an item, animal or person. RFID systems consists of three main components; RFID tags, RFID readers and a backend server. A tag is a computer chip with an antenna coil around it which has encoded identification information that is attached to an item [2]. The communication between the RFID tag and the reader is contactless, using wireless technologies. The tag is readable within a certain distance from the reader. The reader is a device that detects the presence of tags and reads the information supplied by it. RFID readers send queries by broadcasting an RF signal and all tags within its range responds with the identifying information. This tag information is subsequently sent to the backend server, which may have further information about the tag. This information is then passed on to a supporting application for further processing.

This paper is written by Firoz Khan towards his MS studies in Information, Network and Computer Security, NYIT, as part of the course INCS741– Cryptography. He is currently pursuing his second Master while working as a CIS faculty member at the Higher College of Technology at the Dubai Men's Campus in UAE (e-mail: fkhan@hct.ac.ae).

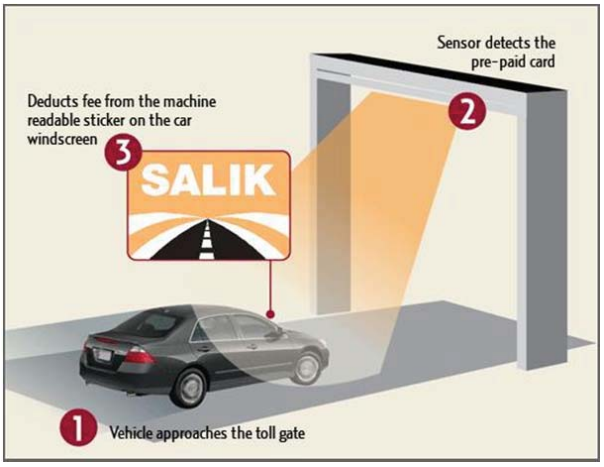

Fig. 1 A toll payment system in Dubai, called SALIK, using RFID technology [1]

The popularity of RFID systems has increased due to the various benefits it offers. RFID systems can provide automatic inventory control and management. The systems can be used to read multiple tags at the same time and send this data for event processing and system analysis. The systems can also be used to track items in large warehouses where physical access is difficult. However, privacy is compromised as the item or a person who is carrying the tag can be easily identified using unauthorized tag readers. Another negative aspect is the physical structure of the tag itself. The limited amount of memory and processing power in the tag is a major inhibitor in the implementation of secure encryption algorithm to provide privacy and security [3]. Due to this reason, any authentication and security protocols that will be used for RFID system need to take into account these limited capabilities.

In this paper, the different industries where RFID systems are implemented are initially discussed. Then we will look at the privacy issues and security threats that affect RFID systems. This paper will further look at the various solutions that can address these issues. The final section will summarize the results of these solutions.

II. RFID Systems in the Real World

RFID systems are used in a wide range of industries all over the world. Some examples include the use of RFID tags to provide a seamless toll payment method on the roads. The RFID tags are preloaded with money that is stuck on vehicles and payment is deducted when these vehicles pass under gates which have RFID readers as shown in Fig. 1, of a system that is implemented in Dubai [1]. Other implementations include

the use of RFID tags instead of traditional bar codes. These systems are used to replace traditional POS systems which read barcodes in supermarkets and they are also used to effectively track book issues in libraries. Further uses of RFID systems will be highlighted in the following sections.

A. RFID in Healthcare Industry

At hospitals, patients wear a bracelet which has a built-in RFID tag. This tag is used to identify the medical needs of these patients. Hospital personnel carry RFID-enabled tablet PCs that recognizes the band worn by the patients and use wireless access to query the backend server about patient information and update the patient information when needed [2]. Newborn babies have RFID tags placed on their ankles to ensure that they are not moved without permission [4].

The issue in this industry is the possibility of patient's private information being stolen by malicious people. Patient information and medication details can be determined this way and can be misused.

B. RFID for Personal Identification

The RFID chips are used on passports as a medium of personal identification. Details like name, nationality, gender, date of birth and a digitized photo can be read from these passports by a RFID reader. RFID-enabled passports are often encrypted and the data is revealed only after a process of challenge-response protocol that proves knowledge of a pair of keys and derives a session key, which provides authentication.

A malicious user can eavesdrop using special hardware, comprised of an antenna, an amplifier to boost signal capture, a radio-frequency mixer and filter, and a computer to store the data, in this communication while the data is being transferred from the passport to the reader. Even if the raw data which has been sniffed is encrypted, he can use software to interpret this data [5]. With this information, the perpetrator can create a fake passport and commit financial fraud in the name of the original passport holder.

C. RFID for Secure Payment

The RFID technology is also being used in the transportation industries like buses, trams, and metros for contactless payment. There are two type of such cards in use in the Dubai Roads and Transport Authority. A paper based one-time use ticket and a permanent card which can be refilled with cash whenever needed. These cards are held close to a reader device in front of a gate to make a payment for the journey. These payment methods also have privacy concerns. A malicious user should not be able to issue bogus payments or impersonate legitimate users of the system. These users need to be identified and prevented. Another issue is that malicious users or the transportation system should not be able to identify or trace users by exploiting the payment system. A final concern involves the infrastructure of the readers [6]. The readers may not be connected to the back-end system at all times. In such cases, the readers must be able to verify tags while being offline and quickly, whether a payment is valid or not.

D. RFID in Libraries

Libraries make use of a back-end system called a bibliographic database to track circulation information of the items in its collection. Each item in the library is assigned a unique number when acquired. The RFID tags which are fixed on the item contain this unique number along with shelf location, last checked out date, author, and title. When a patron checks out an item, the RFID tags are read and the association between the tag and item is looked up in the bibliographic database [7]. If found, the status of the item is changed to checked-out and later when the item is returned, the status is changed to checked-in in the same way.

The RFID tag is also used as a security device. Several RFID sensors are placed at the exit of the library. An alarm rings if a patron exits the library with an item that has not been checked out.

Privacy issues arise when malicious users can read these tags. The user can get the reading habits of a person and he can also determine which library the item belongs to, which can be used to deduce the origins of a user, called hotlisting [8]. Reading detailed information like these can lead to profiling of a particular user.

E. RFID in Credit Cards

More and more banks are now providing contactless payment through their credit cards, by issuing credit and debit cards with RFID tags built into them. The credit cards can be used for quick payment without the need for swiping the credit card reading machine. These credit cards can be a security nightmare as there is a chance of being electronically pick-pocketed. Reading RFID chips is easier and quicker than traditional magnetic strips found on credit cards. A malicious user with a rouge RFID reader can easily read the tag and have all the data from the credit card without the card being even removed from the wallet [9]. Special credit card sleeves and wallets with protective shielding material is being sold to block RFID reading by these malicious users.

F. RFID in Supply Chains

RFID systems in supply chain industries are implemented on a bigger scale than other industries. The backend database accessible through the Internet by multiple supply chain partners, has informational data about product details. A minimal amount of information, such as product IDs are stored on the tags which are attached to containers, pallets or items. When items are received by a supply chain partner, RFID readers are used to collect product information and then is sent to a backend database for interpretation and processing [10].

One of the security and privacy issues faced by the supply chain industry is authoritative access of RFID tags. The tags placed for a particular partner should only be readable and updatable by the readers of the same partner and delivering partner of the same transaction.

Another issue is when a malicious user is able to read tags in the inbound material flow and the outbound material flow. The system should prevent the user from analyzing these two

flows and determine if both the material flows are on the same tag.

A major privacy issue is supply chain visibility for a manager to see the last partner who processed the item, without revealing it to a malicious user.

III. Possible Solutions for RFID Implementations

To implement privacy and security solutions, an understanding of the different types of tags and how they work is needed. There are generally three major types of RFID tags. **Active tag** – This is a tag which has its own power supply. It can transmit data back to the reader by itself without the reader's query signals. **Passive tags** – These types of tags do not have any power supply in them. They are designed to absorb power from the incoming signal of the reader to trigger the circuit and transmit the data stored in the chip back to the reader. **Semi-active tag** – These are tags which have their own power supply, but also absorb power from the reader's signal.

The problem with the tag is that it has limited computational capabilities. Due to this limitation, the use of traditional symmetric and asymmetric cryptography is not a practical option. Therefore, protocols that involve bitwise exclusive-OR (XOR) and hash operations are in high demand in RFID implementations [11]. Some of the privacy and security solutions are highlighted in section below:

A. Privacy Enabled Architecture

In [12], Lee and El-Khatib propose the use of crowd systems developed by Riter and Rubin. The methodology protects the location privacy of RFID tag carrying people from a malicious user. In a crowd of N person-tag associations crowd members, when co-located, can exchange trade tag identifiers with each other before moving away from the crowd zone. Due to this formation of the crowd, person tag relationships are completely hidden from the malicious user. This behavior can be further used to create confusion by interacting the real user with more crowd zones. A malicious user tracing a person's location through the network using their RFID tag will have no clarity regarding the location of the user after a period of time. This increases the location privacy of the user.

B. Lightweight Authentication with Forward and Backward Security

In [13], Burmester and Munilla have proposed a lightweight mutual authentication protocol that supports forward and backward security. The protocol uses minimal overhead with constant lookup time. A Pseudo Random Number Generator (PRNG) is used to draw numbers (3 or 5) and then used to exchange these with the backend server. Past tag interrogations are protected from being linked to captured data. This achieves forward security. Backward security is achieved by protecting the future tag interrogation from traffic analysis attacks, which involves targeting of information leaked by tags. Burmester and Munilla [13] further explain that the solution offered protects against man-in-the-middle attacks, as the protocol they suggest allows RFID tags to pre-compute their response to backend server challenges.

C. Double Challenge Response Protocol

In [14], Good and Benaissa propose a protocol that ensures privacy by preventing any active or passive attacker from gaining any information which is distinguishable from a random sequence. In this protocol, the reader first issues a challenge consisting of a random value, to which the tag must respond. The random value is Nr. The tag takes this value, and generates a random value of its own, Nt. These values are combined in the tag with a secret identifier, ID, using a cryptographic encryption. This encrypted output is then reduced to the required length and broadcast by the tag as an authentication code together with the random value which the tag generated. The reader then uses the tag's response to query a backend server containing known tag identifiers to determine which identifier the tag knows. This process is repeated a second time with a different random value Nr to achieve the security level and prove the authenticity of the tag.

D. Privacy Using Trusted Computing

In [15], Molnar et al. propose a new architecture for a trustworthy reader that enhances the privacy of RFID systems, while retaining the benefits of RFID technology. In the method suggested, the RFID reader consists of a hardware module which has a Trusted Platform Module (TPM) chip. Even if a malicious user is able to compromise the reader, he will not be able to break into the TPM. A particular organization will be able to choose readers based on their requirements of a privacy policy. Privacy policies on these are supported by the readers having these TPMs. The proposed solution also addresses the issues related to key management of shared keys between readers and tags. This key is used by readers to prove that it is authorized to read the tag or to send commands to the tag. A design for a trusted RFID reader is put forward, in which reader software is split to allow maximum flexibility in changing privacy policies on the fly.

E. Untraceable Tags Using Insubvertible Encryption

In [16], Ateniese et al. propose a system to be used with RFID tags that are read/write. The proposed solution does not make any modification to the basic functionality of RFID tags. The broadcasted values from the tags will only be read by the issuing authority. And at the end of each read operation, the reader will be able to replace the contents of the tags with randomized values. This protects the tag from being tracked by malicious users. Only authorized readers will be able to randomize the tag contents.

The system proposed distinguishes between legitimate issuers of marks in the RFIDs and malicious users. The legitimate users can initiate and reset the content of the RFIDs, enabling them to use it for recognizing the tag later. Malicious users can also reset the tags, but any contents they write into the tag will be destroyed by the legitimate readers.

F. Challenge Response Protocol

In [3], Song and Mitchell propose a protocol that makes use of the challenge-response principle. This protocol assumes

that the tag used has some rewritable memory and has the capability to compute a hash function. This hash function is used by the protocol. In low cost RFID tags, the hash function is calculated using non-linear feedback shift registers (LFSR). When these tags are manufactured, it gets a unique identifier and an initiator. The initiator is a bitstring that changes in the tag at each execution of the protocol. The initiator for each tag is a bitstring and the hash value of this pair is stored in the tag. In the server, the value pairs of old and new hashes are stored along with the tag information which is relevant to the reader. This protocol can withstand numerous types of attack. Most importantly, the protocol is both private and secure. The tag will only send random bitstrings when it is asked for authentication, and those values depend heavily on a random number. This number changes over time. If a malicious user disabled the randomness of the random number generator, it will still be necessary to know the function, which can be unique for each tag and is only known to the tag and the server.

The privacy aspect is proven by the challenge-response principle. Every time a tag is queried, the response will be unique due to the random number involved. Because of this, the tag cannot be tracked without breaking the randomness.

IV. Conclusion

The success of the RFID technology is its simplicity. Security and privacy are also paramount in the system. The tag has to identify only to the associated reader and should communicate with the authorized reader only. Many solutions have been mentioned in this paper to address the privacy and security issues associated with RFID technologies. Although many solutions and frameworks have been suggested, solutions depend on circumstances and organizations where the RFID systems need to be implemented.

The system can be set up quite easily and is very easy to use, but it has its own limitations which include limited computing power and memory. For secure communications, encryption can be used, but the type of encryption that can be used is limited due to this. The major requirement of RFID systems is that the communication between the reader and the tag has to be fast. Latency and delay are unacceptable and can contribute to the failure of an implemented system.

References

[1] Image Courtesy Salik (online). Available at: www.salik.gov.ae.
[2] Michael Anshel and Sarah Levitan. 2007. “Reducing medical errors using secure RFID technology”. In SIGCSE Bull. 39, 2 (June 2007), 157-159.
[3] Boyeon Song and Chris J. Mitchell. 2008. “RFID authentication protocol for low-cost tags”. In Proceedings of the first ACM conference on Wireless network security (WiSec '08). ACM, New York, NY, USA, 140-147.
[4] Mohamed K. Saad and Syed V. Ahamed. 2007. “Vulnerabilities of RFID systems in infant abduction protection and patient wander prevention”. In SIGCSE Bull. 39, 2 (June 2007), 160-165B.
[5] Jim Waldo, Alan Ramos, Weina Scott, William Scott, Doug Lloyd, and Katherine O'Leary. 2009. “A Threat Analysis of RFID Passports”. In Queue 7, 9, Pages 10 (October 2009), 6 pages.
[6] Erik-Oliver Blass, Anil Kurmus, Refik Molva, and Thorsten Strufe. 2009. “PSP: private and secure payment with RFID”. In Proceedings of the 8th ACM workshop on Privacy in the electronic society (WPES '09). ACM, New York, NY, USA, 51-60.
[7] David Molnar and David Wagner. 2004. “Privacy and security in library RFID: issues, practices, and architectures”. In Proceedings of the 11th ACM conference on Computer and communications security (CCS '04). ACM, New York, NY, USA, 210-219.
[8] Caldwell-Stone, D 2010, “Chapter 6: RFID in Libraries”, In Library Technology Reports, vol. 46, no. 8, pp. 38-44.
[9] Jaspreet Kaur and Narinder Kehar. 2011. “RFID enabled cards skimming: enhanced technology”. In Proceedings of the International Conference on Advances in Computing and Artificial Intelligence (ACAI '11). ACM, New York, NY, USA, 155-157.
[10] Yingjiu Li and Xuhua Ding. 2007. “Protecting RFID communications in supply chains”. In Proceedings of the 2nd ACM symposium on Information, computer and communications security (ASIACCS '07), Robert Deng and Pierangela Samarati (Eds.). ACM, New York, NY, USA, 234-241.
[11] Renu Aggarwal and Manik Lal Das. 2012. “RFID security in the context of ‘internet of things’”. In Proceedings of the First International Conference on Security of Internet of Things (SecurIT '12). ACM, New York, NY, USA, 51-56.
[12] James Lee and Khalil EL-Khatib. 2009. “A privacy-enabled architecture for an RFID-based location monitoring system”. In Proceedings of the 7th ACM international symposium on Mobility management and wireless access (MobiWAC '09). ACM, New York, NY, USA, 128-131.
[13] Mike Burmester and Jorge Munilla. 2011. “Lightweight RFID authentication with forward and backward security”. In ACM Trans. Inf. Syst. Secur. 14, 1, Article 11 (June 2011), 26 pages.
[14] Good, T, and Benaissa, M 2013, “A holistic approach examining RFID design for security and privacy”, In Journal of Supercomputing, vol. 64, no. 3, pp. 664-684.
[15] David Molnar, Andrea Soppera, and David Wagner. 2005. “Privacy for RFID through trusted computing”. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (WPES '05). ACM, New York, NY, USA, 31-34.
[16] Giuseppe Ateniese, Jan Camenisch, and Breno de Medeiros. 2005. “Untraceable RFID tags via insubvertible encryption”. In Proceedings of the 12th ACM conference on Computer and communications security (CCS '05). ACM, New York, NY, USA, 92-101.

Firoz Khan. BSc in Electronics, Bharatiyaar University, India, 1994. MS in Information Technology, University of Southern Queensland, Australia, 2005. His professional background includes Networking Protocols, Information Systems and Computer Security, Project Management, Academic Coordinator and Teaching.