ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 4, Issue 3, March 2017

RFID Smart Tagged Card Safety Vulnerabilities Solutions

[1] Usha Chauhan,

[1]Department of Electronics and Communication Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

[1] gu1413912423@Galgotiasuniversity.edu.in

Abstract: Increasing use of RFID in all areas of the industry is being made of the RFID technology. RFID technologies have been introduced in order to increase the reliability of their inventory control systems by companies and government agencies. The technology is used in the healthcare industry to save patients ' lives by preventing medical errors and mistreatment, to monitor medical devices and to monitor the administration of medication. Despite all of the advantages of RFID to industry, its use presents obvious security problems. It will recognize the safety risks inherent in RFID technology and will provide a mechanism to protect intelligent tagged cards by using active tags and to avoid cloning tags or sniffing data between tags and readers. The framework proposed is specific to the layer of tag and reader communication. Based on the data received, the controller will take the information and use it. The data can be stored or transferred in an inventory as an entity.

Keywords: Biometrics, RFID, Security, SmartTags.

INTRODUCTION

RFID is able to distinguish artifacts or individuals by using the devices called tags through wireless communication technology. The technology consists of three main components: a tag, a reader and a host system. On a specified radio frequency, the radio tag and reader communicate. If an object with an RFID tag goes to the reader's contact field, the reader tells the tag to return the stored data. After the reader collects the data from the tag, the data is sent through a network connection to the RFID controller (Ethernet, Mobile IP, etc.). Depending on the type of data the controller receives, the information will be taken and used. The data can be stored or transferred in a database as an inventory item.

RFID technology was one of the hottest topics because it automatically monitors and records processes. In contrast to bar code technology, it offers significantly higher information quality and accuracy, real-time reaction efficiency and end-to-end visibility. It has been used in different fields such as retail stock control, supply chain management, fake safety, building security, library systems, speed payment fobs, car recognition, airline luggage, lost pets, forest studies and cattle tracking. The use of RFID technology to save lives, avoid errors, and reduce costs is increasingly important {Formatting Citation}. RFID tags have been implemented by medical organizations to track and maintain medical assets to maximize use and to reduce the need for future spending on equipment duplication. Some use RFID for tracking and tracing by integrating emergency alarm devices into medical monitoring equipment and to ensure the removal of the tagged surgical equipment during operation in order to improve patient safety and medical service.

The use of RFID tags to monitor people's products could create significant risks for both organizations and individuals in terms of security and privacy. A tag automatically addresses a reader without the consent of the owner and even the owner knows it. To order to avoid leakage of information regarding privacy, it is necessary to secure tags as RFID is embedded to patient personal data and medical history. This research looks at the security concerns of RFID's air link between the tag and the user. The standard RFID device is shown in Figure 1 and the protected and unsecured interfaces in that network. Several people and a controller or workstation can be made from the device. A reader can attach to multi-tags, with almost anything (from shelf items, a medical ID bracelet, or a pallet) attached to the tags [1], [3]–[5]. Communication between the tag and the reader in an RFID device is the weakest point of protection. Normally this interface uses no encryption, particularly when passive tags are used. In accordance with company IT security policies, the network interface between the reader and the host system or host network.

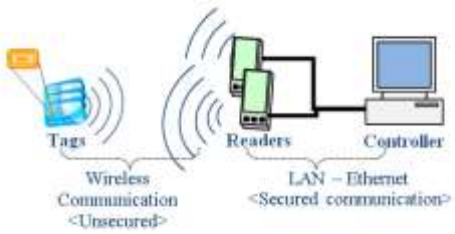

Figure 1. Typical RFID System

RFID Privacy and Security Issues:

Through the use of RFID technology growing, the privacy and security concerns are becoming more and more concerned. In their research RFID chips were identified in supermarket loyalty cards by Customers Invalid and Numbering (CADSPIAN), which included customer identity information without the knowledge of customers. Also, RFID tags can still be transmitted by any reader after the product has been purchased. The data can be read from the tags by all readers with the appropriate frequency range. The connection between the tag and the reader is one of the main drawbacks in RFID technology [6], [7]. Usually for that communication connection, there is no messaging encryption. To resolve this problem, more hardware will be required which will affect size and cost.

RFID Security Threats:

RFID technology security threats may be placed in a number of classes: sniffing, Spoofing, Cloning, Replay, Relaying and denial of service. Sniffing and waking up attacks are the highest security risk for RFID networks. Eavesdropping is an unauthorized tag access. Read and record sensitive and confidential information for a rogue reader. Spoofing attacks also include secret scanning. The transmission of data from a legitimate tag is not only recorded, but the original tag ID is copied and it appears valid [8], [9]. The replay attack involves the use of a tag's response to the challenge of a rogue reader to embody the tag. Relay attacks are the same as replacer attacks, but the valid tag for an authentic reader is delayed. Service denial is the last type of threat. It contravene the RFID system's accessibility and may hit any portion of the system, such as the removal of the RFID tag from a merchandelion before the RFID tag is checked off, and the swapping and placement of tags on lower-cost merchandise. All attacks compromise the credibility of the database on the backend systems due to inventory flaws.

Security Countermeasures:

Many approaches are employed to combat risks to the security of RFID technology. These methods can be grouped into two groups; non-encryption systems and algorithms of cryptography. Non-cryptographic security measures are introduced in order to reduce costs. Tag-Matting is one of the easiest ways to protect consumer privacy. The RFID tag functionality is eliminated by this method when it is sold. The Kill command is included in the RFID tag and executes when the RFID reader at the point of sale sends code or the PIN so that the tag is unusable. Another popular non-cryptographic security approach is the use of read-only tags, which uses a confidential and temporary identification code in the RAM (semi activated tags), and the manufacturer's serial identity number in the tags. As a result, if the tag is in ROM mode object, any user who needs information has unrestricted identifying objects. In RAM mode, object identification is restricted to limited users.

Cryptographic algorithms are more expensive to implement, but they can provide better protection and privacy including hash-based access control, a lightweight, re-encoding and universal re-encoding method, and Advanced Semi-Randomized Access Control (A-SRAC). Hash Based Access Control uses hash-enabled tags with a temporary metaID section reserved for a memory. This enables the tag to be locked or unlocked. A hash algorithm is used to produce an indiscriminate metaID key, the reader must search the local database for a particular hash key to be sent to the tag, the tag will be sent with a metaID hash key and, if it matches, the tag will unlock and allow full reading data.

A list of pseudonyms is used in the minimalistic method that is unique to the keys stored in the RFID tag. After the tag is authenticated, the reader is validated and the tag is checked by the reader via an authentication key. The RFID tag releases the data to the reader once the validation process is complete. The user then renews the tag's authentication keys and username. Re-encryption and universal re-encryption systems use public key encryption methods and require more background server and memory resources due to the type of algorithms used. By using the re-encryption system, they can prevent the tag identifier from being released. The A-SRAC algorithm uses minimum calculations, which keeps the messaging size small. The A-SRAC Algorithm uses Hash, a random generator and uses metaID. The rear-end Servers hold old and new identifiers.

Security Framework for Smart Tags:

They propose to make RFID smart tagged cards, Personal Medical Card (PMC) secure with the protocol A-SRAC when the intelligent tags do not require data transfer or biometric testing to trigger the smart tag. The card contains a number of folders including information on personal identification, medical records, dental records and all other related problems. Different medical providers would publish the medical records. The A-SRAC protocol provides a two-layer security random generator and hatch feature. It also reduces server and readers ' total computational power. The Sleep command means that the user transmits a code of access to remove the tag. Physical activation unlocks the tag by means of biometric scans. The card owner's fingerprint or another special physical personal character is embedded and digitally coded in the smart tag on the card and the card is activated when the card owner matches the fingerprint with the coded fingerprint on the server. The use of A-SRAC requires a smart stag with enough memory and processing power for the sleep controls and biometrics. On the back end, there must be enough server resources for security and transactions to take place.

As a case study, we want to use PMC in secure manner with embedded smart tags to look at the authentication side of card transactions covering the card and reader air interface. The security framework process noted below is shown in Figure 2:

1. When a patient enters a health center with his PMC, a biometric scan unlocks the card and the reader sends a message and the random number to the card.
2. The card uses the hash function to generate a MetaID and sends it to the RFID reader with an embedded key.
3. The reader transmits the information to the server, looks up the key response on the MetaID in their database, generated a random answer number, and monitors the unique combination of the stored MetaID. If not, the server must refresh the random number until the blend is unique.
4. The server must change the key and provide the reader with the details to the name.
5. The tag confirms the information, updating it and transferring health data from the patient's card to the reader if it is correct. 5. To disable the card, the reader sends an access code to the clever tag.
6. The data transferred from the tag is passed to the patient's electronic health diagram with an embedded label and the reader using the

same protocol in step 1–5 when the patient is examined.

7. The health chart is updated by physicians and the card is activated by a touch combination once the treatment is completed and takes 1-5 steps.
8. The reader on the health diagram will update the PMC tag with medical information and will issue the code of access to disable the card to complete the process.

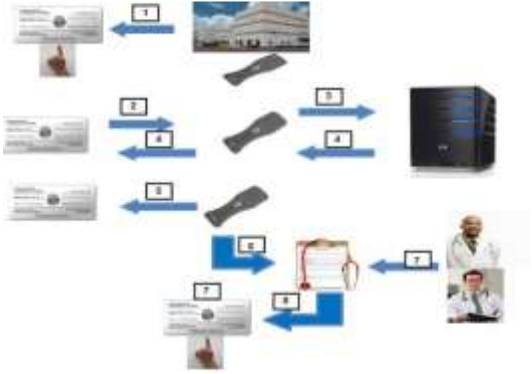

Fig.2: Security Process for a Smart Tagged Insurance

This allows for two levels of security, the one cryptographic and the other physical, to protect the data from the intelligent tag. Possible drawbacks would be to lose the card data through electromagnetic interference and to support the system with enough server resources on the backend.

CONCLUSION

As a technological development for the daily application of smart-tagged passports, assurance carts and bank cards, the development of RFID security protocols is becoming viable. Security protocols such as the A-SRAC provide a twin mechanism of authentication, combined with a non-cryptographic method such as a sleep order, allow a security framework which is useful in RFID technology application.

REFERENCE

[1] "Avery Williamson, L.-S. Tsay, I. A. Kateeb, and L. Burton", "'Solutions for RFID Smart Tagged Card Security Vulnerabilities,'" *AASRI Procedia*, 2013.

[2] L. S. Tsay, A. Williamson, and S. Im, "Framework to build an intelligent RFID system for use in the healthcare industry," in *Proceedings - 2012 Conference on Technologies and Applications of Artificial Intelligence, TAAI 2012*, 2012.

[3] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and near-Field Communication*. 2010.

[4] M. Batty, "Big data, smart cities and city planning," *Dialogues Hum. Geogr.*, 2013.

[5] D. Guinard, V. Trifa, F. Mattern, and E. Wilde, "From the Internet of Things to the Web of Things: Resource-oriented Architecture and Best Practices," in *Architecting the Internet of Things*, 2011.

[6] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things: Vision & challenges," in *IEEE 2013 Tencon - Spring, TENCONSpring 2013 - Conference Proceedings*, 2013.

[7] Y. Mishra, G. K. Marwah, and S. Verma, "Arduino Based Smart RFID Security and Attendance System with Audio Acknowledgement," *Int. J. Eng. Res. Technol.*, 2015.

[8] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Res.*, 2016.

[9] P. J. Hawrylak, N. Schimke, J. Hale, and M. Papa, "Security risks associated with radio frequency identification in medical environments," in *Journal of Medical Systems*, 2012.

[10] X. Shao, "Study on security issue of internet of things based on RFID," in *Proceedings - 4th International Conference on Computational and Information Sciences, ICCIS 2012*, 2012.

[11] J. H. Khor, W. Ismail, M. I. Younis, M. K. Sulaiman, and M. G. Rahman, “Security problems in an RFID system,” *Wirel. Pers. Commun.*, 2011.

[12] Ishleen Kaur, Gagandeep Singh Narula and Vishal Jain, “Identification and Analysis of Software Quality Estimators for Prediction of Fault Prone Modules”, INDIACom-2017, 4th 2017 International Conference on “Computing for Sustainable Global Development”.

[13] Ishleen Kaur, Gagandeep Singh Narula, Vishal Jain, “Differential Analysis of Token Metric and Object Oriented Metrics for Fault Prediction”, International Journal of Information Technology (BJIT), Vol. 9, No. 1, Issue 17, March, 2017, page no. 93-100 having ISSN No. 2511-2104.

[14] VM Prabhakaran, S Balamurugan, S Charanyaa, “Sequence Flow Modelling for Efficient Protection of Personal Health Records (PHRs) in Cloud”, International Journal of Innovative Research in Computer and Communication Engineering, 2015

[15] RS Venkatesh, K Deepika, R Poornima, S Balamurugan, M Sowmiya, “A Novel Dynamic Object Oriented Model for Automated Credit Card Management System”, International Journal of Innovative Research in Science, Engineering and Technology , Vol. 4, Issue 2, February 2015

[162] R Santhya, S Latha, S Balamurugan, S Charanyaa, “Certain Investigations on Methods Developed for Efficient Discovery of Matching Dependencies” International Journal of Innovative Research in Computer and Communication Engineering , Vol. 3, Issue 1, January 2015