Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 4 (2013) 282 – 287

AASRI Procedia

www.elsevier.com/locate/procedia

2013 AASRI Conference on Intelligent Systems and Control

"Solutions for RFID Smart Tagged Card Security Vulnerabilities"

"Avery Williamson Sr., Li-Shiang Tsay, Ibraheem A. Kateeb, Larry Burton" *

"North Carolina A&T State University, 1601 E. Market St. Greensboro NC 27406, USA"

Abstract

The use of Radio Frequency Identification (RFID) technology is seeing increasing use in all areas of industry. Companies and government agencies have implemented RFID solutions to make their inventory control systems more efficient. In the healthcare industry the technology is being used to saves patient lives by preventing medical misidentification, and mistreatment, to monitor medical equipment assets, and to track the administration of medication. In spite of all the benefits that RFID can provide to industry, there are glaring security concerns that come with its use. The paper will identify the security risks inherent in RFID technology and propose a framework to make smart tagged cards more secure using active tags and prevent the ability to clone tags or sniff data between the tag and reader. The proposed framework is specific to the tag and reader communication layer.

Keywords: RFID; Security; SmartTags; Biometrics

1. Introduction

RFID utilizes wireless communication technology to provide the ability to distinctively identify objects or people using devices called tags. The technology is made up of three essential parts: a tag, a reader and a host system. The RFID tag and reader communicate on a specified radio frequency. When an object that has an

* Corresponding author. Tel.:+1-336-451-0288
E-mail address: anwillia@aggies.ncat.edu

doi:10.1016/j.aasri.2013.10.042

RFID tag goes in the communication zone of the reader, the reader tells the tag to send the data that is stored on it. After the reader collects the data from the tag, it sends the data to the RFID controller by a network connection (Ethernet, Mobile IP, etc.). The controller will take the information and use it depending on the type of data it has received. The data can be stored in a database or moved as an object in inventory.

RFID technology has been one of the hottest topics because it makes tracking and tracing processes automatic. It provides much higher data integrity and accuracy, real-time reaction capabilities, and end-to-end visibility compared to the barcode technology. It has been used in various areas, such as retail inventory control, supply chain management, counterfeit prevention, building security, library systems, speed payment fobs, toll collection, vehicle identification, airline baggage, locating missing pets, study wildlife, and tracking livestock. Currently, there is an increasing interest in using the RFID technology to save lives, to prevent errors, and to reduce costs. Medical organizations have adopted RFID tags to track and manage medical assets to improve their utilization and to reduce the need for future expenditures on duplicating equipment. To improve patient safety and medical service, some are using RFID for tracking and tracing by integrating with medical monitoring equipment for emergency alerts and for ensuring the removal of tagged items of surgical equipment during an operation.

Using RFID tags for tracking items carried by people could poses significant security and privacy risk to both organizations and individuals. A tag naturally responds to a reader without the owner's approval and without the owner even noticing it. When RFID are embedded into patients' personal data and medical history, it is indispensable to secure the tags to prevent any leaking of privacy-sensitive information. This study examines the security issues impacting RFID the air interface between the tag and reader. Figure 1 shows a typical RFID system and the secured and unsecured interfaces that exist in such system. The system can be made of many readers and one controller or host workstation. A reader has the ability to communicate to multiple tags, with the tags being able to be attached to almost anything (from shelf products, a medical ID bracelet, or a pallet). The communication between the tag and the reader is the weakest point of security in an RFID system. This interface usually does not utilize any encryption, especially if passive tags are used. The network interface between the reader and host system or host network is covered by the IT security policies of the corporate network.

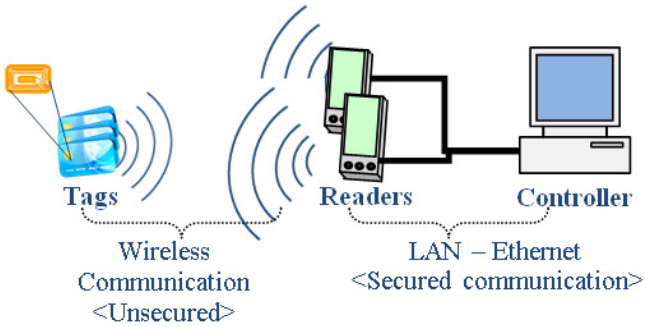

Figure 1. Typical RFID System

2. RFID Privacy and Security Issues

As the use of RFID technology spreads, there is an increasing concern in its associated privacy and security issues. The group Consumers against Supermarket Privacy Invasion and Numbering (CASPIAN) in their research found RFID chips in retailer loyalty cards that held customer ID information without the

consumers' knowledge (Grover & Berghel, 2011). Also, RFID tags in products can still transmit data after the products are purchased and can be read by any reader. All readers in appropriate frequency range are able to read the data from the tags. One of the common weak points in RFID technology is the link between the tag and reader. Usually there is no encryption for the messaging for that communication link. Solving this issue will require more hardware, which will affect the size and the cost.

2.1. RFID Security Threats

The security threats to RFID technology can be put into several classes; Sniffing (or Eavesdropping), Spoofing, Cloning, Replay, Relay, and Denial of service attacks (Grover & Berghel, 2011) (Shih, Lin, & Lin, 2005). The highest levels of security risks to an RFID network are sniffing and eavesdropping attacks. Eavesdropping/sniffing is an unauthorized access to tags. A rogue reader can read a tag and record information that may be sensitive and confidential (Grover & Berghel, 2011). Spoofing attacks involve secretly scanning as well. It is not only recording a data transmission from a legitimate tag but also copying the original tag's ID and making itself appear to be valid. Replay attack involves using a tag's response to a rogue reader's challenge to impersonate the tag (Burmester & Medeiros, 2007). Relay attacks are alike to the replay attack but it delays the valid tag to response to the authentic reader. The last type of threat is the denial of service attack. It is against the accessibility of the RFID system and can hit any portion of the system (tag, reader, and controller-backend computers), such as removing the RFID tag from merchandise before it is checked out of the store (Grimaila, 2007), and swapping and placing tags on merchandise that has a lower cost. All attacks affect database integrity on the backend systems because of the inventory mismatches.

2.2. Security Countermeasures

There are several methods being used as countermeasures to the security threats presented against RFID technology. These methods can be categorized into two groups; non-cryptographic systems and cryptographic algorithms (Shih, Lin, & Lin, 2005). To diminish costs, non-cryptographic security countermeasures are deployed. One of the easiest ways to safeguard consumer privacy is tag-killing (Shih, Lin, & Lin, 2005). This method kills the functionality of the RFID tag once it is at the point of sale. The Kill command is built into the RFID tag and is executed once the RFID reader sends a code or PIN at the point of sale to make the tag unusable (Juels, Rivest, & Szydlo, 2003). Utilizing the tags read-writable memory is another popular non-cryptographic security approach, which uses a secret and temporary ID code in the RFID tag's RAM (semi active tags) and the tag's serial ID number that is put the ROM by the manufacturer. The result is when the tag is in ROM mode object there is unrestricted object identification to whichever user that needs information and in RAM mode there is a restriction of object identification to limited users (Inoue & Yasuura, 2003),.

Cryptographic algorithms are more costly to implement but can provide better security and privacy, including Hash Based Access Control, Minimalist, Re-encryption scheme and universal re-encryption, and Advanced Semi-Randomized Access Control (A-SRAC) (Shamaili, Yeun, & Zemerly, 2010). Hash Based Access Control uses hash-enabled tags that have a segment of memory set aside for a temporary metaID. This allows the tag to function in a locked or unlocked status (Shih, Lin, & Lin, 2005). A hash algorithm is utilized to generate an indiscriminate key for the metaID, the reader checks the local database for the corresponding hash key to be sent to the tag, the tag receives the hash key and checks it against the metaID and if it corresponds, the tag unlocks and allows full data retrieval to the readers (Shamaili, Yeun, & Zemerly, 2010). The Minimalist method uses a list of pseudonyms that is unique to the keys stored in the RFID tag (Juels A. , 2004). The reader is validated after it has been authenticated by the tag and the tag is validated by the reader by sending an authentication key. Once the validation process is complete, the RFID tag releases its data to

the reader. Then the reader renews the pseudonym and authentication keys in the tag. Re-encryption and universal re-encryption systems use public key cryptographic methods and require more memory and server resources on the back end due to the type of algorithms being employed (Shamaili, Yeun, & Zemerly, 2010). They can keep the tag identifier from being disclosed by utilizing the re-encryption system. The A-SRAC algorithm employs minimal calculations and keeping the messaging size small (Shamaili, Yeun, & Zemerly, 2010). The back end servers keep the old and new data from the tags, w The A-SRAC algorithm employs hash functionality, a random generator, and also utilizes metaID.

3. Security Framework For Smart Tags

We are proposing using the A-SRAC protocol to provide security for RFID smart tagged cards, Personal Medical Card (PMC) with the feature to go to sleep when the smart tags do not need to transfer data and biometric verification to activate the card. This card will have different folders, such as personal identification information, medical records, dental records and any other related issues. The medical records would be issued by different medical providers. The A-SRAC protocol offers a random generator and hash functionality that is two layers of security. It also reduces the overhead computing resources of the server and reader (Lee & Verbauwhede, 2009). The Sleep command is a variation of the Kill command, where the reader transmits an access code to deactivate the tag (Grover & Berghel, 2011). The tag is turned on by physical activation through biometrics verification. 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. Using A-SRAC, the sleep command, and biometrics will require a smart tag with sufficient memory and processing power. On the back end, there must be enough server resources for security and transactions to take place.

As a scenario, we want to use PMC with embedded smart tags in a secure manner and look at the authentication side of the transactions involving the card which covers the air interface between the card and reader (Tsay, Williamson, & Im, 2012). Figure 2 shows the process for the security framework noted below:

1. Once a patient enters a healthcare facility with his/her PMC, the card is activated by biometric verification, and the reader sends a query and random number to the card.
2. The card uses the hash function to create a MetaID with an embedded key and sends it to the RFID reader.
3. The reader sends the information to the server and it performs a lookup on its database on the key response on the MetaID, creates a random response number and checks if the combination is unique from the stored MetaIDs. If it is not, the server renews the random number until the combination becomes unique.
4. The server updates the key and sends the information to the reader which forwards the information to the tag.
   The tag validates the information and if it is valid, it updates it and releases the patient's health data from the card to the reader.
5. The reader sends an access code to the smart tag in the card to deactivate it.
6. As the patient is being treated the data that was transferred from the tag is transferred to an electronic health chart that has an embedded tag and reader in it using the same process in steps 1 – 5.
7. The health chart is updated by the medical professionals and once the treatment is completed, the card is activated by a touch combination and goes thru steps 1-5.
8. The reader in the health chart updates the tag in the PMC with the updated medical data and issues the access code to deactivate the card, which will complete the process.

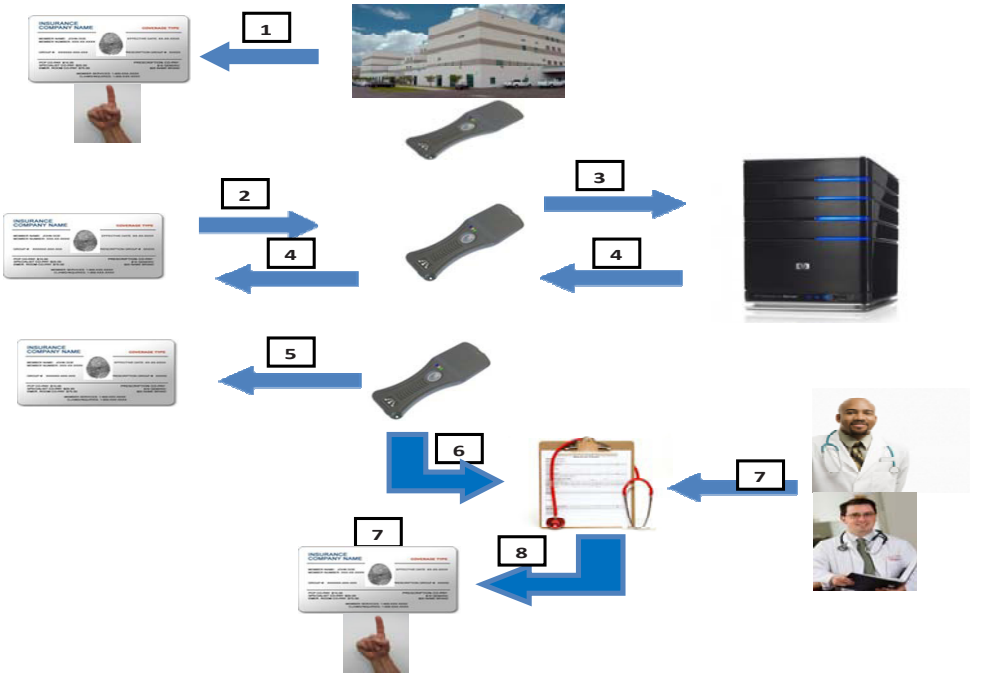

Figure 2. Security Process for a Smart Tagged Insurance

This process allows for two layers of security to protect the data on the smart tag, one cryptographic and the other physical. Possible weaknesses would be losing the data on the card by electromagnetic interference and having enough server resources on the backend to support the proposed system.

4. Conclusion

Because of the advances in security protocols for RFID, it is becoming viable as technology for use for everyday applications such as smart-tagged passports, insurance cards, and bank cards. Security protocols like A-SRAC provide a double authentication process and coupled with a noncryptographic scheme such as the sleep command allow for a security framework that is practical in its application in RFID technology.

References

[1] Burmester , M., & Medeiros, B. D. (2007). RFID Security: Attacks, Countermeasures and Challenges. *The 5th RFID Academic Convocation, The RFID Journal Conference (2007).*

[2] Grimaila, M. (2007). *RFID Security Concerns*. Retrieved March 2013, from Slideshare.net: http://www.google.com/url?sa=t&rct=j&q=rfid security issues&source=web&cd=10&cad=rja&sqi=2&ved=0CHAQFjAJ&url=http://www.slideshare.net/PeterSam67/rfid-security-

[3] Grover, A., & Berghel, H. (2011). *A Survey of RFID Deployment and Security Issues*. Journal of Information Processing Systems, Vol.7, No.4, December 2011.

[4] **Inoue**, S., & Yasuura, H. (2003). *www.c.csce.kyushu-u.ac.jp.* Retrieved Feb 2013, from System LSI Lab: http://www.c.csce.kyushu-u.ac.jp/lab_db/papers/paper/pdf/2003/sozo03_5.pdf

[5] Juels, A. (2004). *www.rsa.com/rsalabs.* Retrieved Feb 2013, from RSA Laboratories: http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/minimalist/Minimalist.pdf

[6] Juels, A., Rivest, R., & Szydlo, M. (2003). *www.rsa.com/rsalabs.* Retrieved Feb 2013, from RSA Laboratories: http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/minimalist/Minimalist.pdf
[7] Lee, Y., & Verbauwhede, I. (2009). *https://www.cosic.esat.kuleuven.be/index.html.* Retrieved Feb 2013, from COmputer Security and Industrial Cryptography: http://www.cosic.esat.kuleuven.be/publications/article-663.pdf
[8] Shamaili, M. B., Yeun, C. Y., & Zemerly, M. J. (2010). Smart RFID Security, Privacy, and Authentication. In M. B. Shamaili, C. Y. Yeun, & M. J. Zemerly, *Computational Intelligence and Modern Heuristics* (pp. 175-189). InTech.
[9] Shih, D., Lin, C., & Lin, B. (2005). Privacy and Security Aspects of RFID Tags. *Soutwest Region Decision Sciences Institute.*
[10] Tsay, L.-S., Williamson, A., & Im, S. (2012). Framework to Build an Intelligent RFID System. *Technologies and Applications of Artificial Intelligence (TAAI)* (pp. 109-112). TAAI.