Security and Privacy Concirns with Radio Frequency Identification Technology

Kevin Kirwin
College Of St. Benedict St. John's University
Collegeville, United States
kdkirwin@csbsju.edu

***Abstract*— The adoption of RFID technology has grown significantly over the past twenty years. Implemented in fields such as supply chain management and access control systems, RFID offers a plethora of advantages. However with this technology, a number of privacy and security concerns exist. Specifically within the area of physical access control, as many RFID tags are susceptible to cloning, giving attackers the ability to capture and utilize another person's credentials. A prototype system was created using RFID reader/writer hardware and appropriate tags, to demonstrate how easily RFID tags can be read. The prototype highlights a security vulnerably also present within CSBSJU Saint's ID badges allowing for the successful cloning of identifying information. As RFID technology continues to gain ground, concerns will continue to grow over the security and privacy implications of this emerging technology. Additional research must be conducted to create a set of standards to govern secure RFID protocols.**

Keywords-rfid; security; radio frequency identification

I. INTRODUCTION

From the simple record book to the barcode, people have been attempting to create more efficient means of managing anything from inventories to livestock or even people for hundreds of years. The introduction of Radio Frequency Identification (RFID) technology has enhanced humanity's ability to monitor, identify, manage, and track assets throughout the world. While RFID technology is facing unprecedented growth [1], a number of significant security and privacy issues are developing a cause for concern.

II. HISTORY

RFID technology was first developed out of necessity in World War 2 with the purpose of identifying airplanes on radar. In the early days, German aircraft would rock the wings of their planes as they approached, thus changing the reflected radar signal. This, the first primitive RFID system, provided German ground crews an advanced warning of allied aircraft. However, it was not until the 1940's when British physicist Watson-Watt developed the "Identify Friend or Foe" system, the first true RFID implementation. As planes approached, a passive transmitter implanted on the plane would activate when stuck by radar waves, sending back a unique frequency identifying the craft as friendly. Shortly thereafter, additional research was conducted to determine how RFID technology could be put to use in businesses and track inventories. Upon its initial commercial inception it was used as an anti-theft device; a single transponder (carrying either a value of 0 or 1) was placed inside product packaging and sensors were placed near business exits. When a consumer left the business, their items were scanned and if the incorrect value was received, an alarm would sound.

Further research in commercial applications continued well after the war. The Los Alamos National Laboratory, a research institution operated by the United States Department of Energy, developed a system designed to track and manage inventories of nuclear material. The laboratory suggested implanting RFID tags within trucks which could be remotely read by scanners at secure facilities. This was the first effective implementation of a RFID based inventory management system.

Development of RFID chips continued, expanding their data capacity and radio transfer range. However it was not until 1999, when the fundamental implementation of RFID technology changed. Professors David Brock and Sanjay Sarma proposed deploying very simple RFID tags throughout a company's SUPPLY CHAIN [2]. Rather than carrying a significant amount of data on the chip such as product type, date of manufacture, shipping destination, etc., the chips simply carried a unique identifier that would act as a primary key to a database containing more detailed information. This instrumental change significantly reduced the complexity and power requirements of the RFID tags by reducing the cost of production. In years following, RFID technology found its way into hundreds of companies, including key business leaders such as Target, Wal-Mart, and the United States Department of Defense [1].

Today RFID technology is primarily used for physical access control, identification, and asset management. In physical access control, companies such as HID Global use RFID technology and a centralized management system to enforce physical access controls. Common implementations can be seen through their use on the CSBSJU campus. The

majority of buildings across both campuses are secured via the "HID Proximity" RFID access control system.(HID Corporation 1-3) The use of RFID access control systems provides security professionals with the ability to track user's physical access history and instantly grant or deny access permissions, providing users with flexibility far superior to RFID's competitor, the key. RFID technology is also used as identification and can be found in United States Passports, driver's licenses, credit cards, and even car keys. For example, current U.S. passports contain a name, nationality, gender, date of birth, place of birth, and a digitized photograph [3]. Companies have even leveraged this technology to enhance their supply chain, improving asset management, reducing costs, and improving production accuracy. Companies able to enhance distribution efficiencies are able to pass savings on to consumers, gaining a significant competitive advantage. Wal-Mart, the world's largest discount retailer, has been able to achieve an estimated four percent competitive advantage over industry rivals through the installation of state of the art AUTOMATED DISTRIBUTION CENTERS [4].

III. TECHNICAL UNDERPINNINGS

A. *RFID Operations*

Modern RFID systems are comprised of the following three components: tags, readers, and a centralized management solution. All RFID tags contain a small microchip and an antenna (See Fig. 1). The chip is used to store the tag's uniquely identifiable information and manage the transmission of the chips data. The antenna is used to broadcast data to a RFID reader. However, tags are further divided into two sub categories, passive and active. Passive tags utilize radio frequencies emitted from a RFID reader to power the tag through electromagnetic induction. A phenomenon discovered by Michael Faraday in 1831 where a primary coil, in most implementations a RFID reader, generates a magnetic field. While the RFID tag passes through the field, a voltage increase is incurred on the antenna, resulting in power applied to the tag. Once powered, the tag is able to broadcast data contained on the chip. Active tags contain an independent power source used to amplify the tag's wireless signal and ensure the tag can broadcast regardless of its location relative to a reader. For most tags, the data contained on the tag's chip is merely a set of binary numbers used to identify the card.

Figure 1 - An RFID Tag, Chips holding data are located in the center, while the antenna used for power and transmission circles the tag.

Furthermore, the data, format, associated permissions etc. are unknown to the tag itself. In the case of "dumb" tags, its function is merely to relay the stored data [5].

RFID readers simply provide power to passive tags and receive the radio broadcast. Upon receiving the broadcast, the reader will translate the data to a common network protocol and pass the data along to the central controller. Similar to the tag, readers do not compute the data received and readers are not aware of any associated access privileges, they serve to only transmit the tag's data to the controller [5].

Once the data is received, the central control system reads and processes the data. On most systems, the controller performs a number of checks to ensure data integrity and then processes data accordingly. In a physical access implementation, the controller would check a central database to verify access for the given reader, log the access attempt, and permit or deny access accordingly [5].

As a direct result of the demand for low cost tags, manufacturers have continued to produce and deploy simple tags which lack any sort of data protection mechanisms [6]. Most RFID solutions will willingly transmit the data they contain to any reader in plain text. The transmission of data in clear text to whatever device requests it presents a number of security concerns. RFID cloning, the process of reading and copying data on a tag, presents a major risk to "dumb" RFID tags. These vulnerabilities present a significant risk for physical access implementations.

B. *Proposed Demonstration*

For our demonstration, we plan on showing how easily, cheaply, and quickly RFID data can be read and then written on new tags. To successfully demonstrate this process, we will need to acquire a RFID reader/writer along with re-writable RFID tags, gather RFID data, and develop a computer program to read and write data to cards. To acquire a RFID reader and writer, we plan on purchasing a device from one of many available online retailers. The CSBSJU computer science department has agreed to fund the project.

For data acquisition, we plan on using the CSBSJU Saints ID cards which contain a 125 kHz RFID chip. Upon a successful acquisition of the data, we plan on writing the unique identifier to separate cards to successfully clone the saint's id. we will then demonstrate how the cloned id can be used to successfully gain access to secured areas of campus. As part of the demonstration, we will develop a computer program to interface with the reader and writer. To be successful, the program must be capable of correctly reading and decoding the "format" of the specific RFID tag implementation. With the CSBSJU Saints ID card, the 26-

bit H10301 format is used to store the tags identifying information. The format specifically dictates the number of bits used as a "site" code, data identifying a specific implementation, and a "credential number" identifying the tag (see Fig 2).

1-11111111-1111111111111111-1

Figure 2 - H10301 Format, buffer bit, followed by site code, credential code, and trailing buffer bit.

C. *Current Security And Privacy Practices*

Three schools of thought define the current approach to RFID tag security. 1, no security is necessary. 2, the notion of a pre-shared key used to encrypt communications between the reader and the writer. 3, a "negotiated" key implying a reading and writing of keys ultimately determining the encryption method used.

With no encryption, RFID tags are susceptible to being read by unauthorized readers or data being intercepted over the airwaves. This particular solution is extremely popular in asset management solutions as the RFID tag serves a primary purpose of tracking equipment, not authenticating or granting access. Tags with no privacy data protection mechanisms are significantly cheaper to produce and deploy. The physical capabilities of modern passive tags are not powerful enough to employ advanced encryption technologies without costly circuitry and power considerations. This additional overhead stifles the low cost incentive which has directly resulted in the increased use of RFID technology [7]. RFID cards employing cryptographic capabilities increase costs by up to 50X [8]. Additionally, as the computing capabilities increase, power requirements rise, thus reducing the viability of passive RFID tags.

Pre-shared keys provide the data an additional level of protection. However, data integrity relies on a single secret. In a pre-shared key system, the tag uses an encryption key to protect data. The data is encoded in a manner that requires that the receiver to know the key before the transmitted data can be decrypted and used. Passive listeners and unauthorized readers are unable to decipher and use the data stored on the tag. Unfortunately, data integrity is dependent on a single secret, should an adversary learn of the secret, data on the tag and likely other tags associated with the system will be compromised [6]. This means of protection only offers integrity and confidentiality of data. Confidentiality is reasonably ensured through the use of the private key encryption process while data integrity is reasonably ensured through the decryption process. Common data encryption protocols utilize Cyclic Redundancy Checks (CRC), a binary hashing function used to detect anomalous changes in data, after decryption to verify that only whole, un-manipulated data has been decrypted.

Negotiated encryption solutions offer the greatest level of protection; however, power and computational costs are incurred. In a negotiated encryption system the reader and the tag establish authentication, determining that communication between the devices is acceptable and a secure means of data transfer. Often these systems use a public key encryption system to secure communications and ensure data integrity. Unfortunately, negotiated encryption requires additional circuitry, additional computations, and additional power to ensure data integrity [9]. In an effort to design a cost effective means of RFID security offering integrity, confidentiality, and authentication, a number of proposals have been made, most notably the "Tag Reader Mutual Authentication" (TRMA) scheme. The TRMA scheme operates much like a three way handshake commonly utilized in high level internet protocols such as the Transmission Control Protocol (TCP). A description of the TRMA schema can be found below (see Fig 3.)

D. *Description of the TRMA Schema*

Tag → Reader: EPC, R_1^{Tag}, R_2^{Tag}

First, the tag initiates communication by broadcasting its Electronic Product Code (EPC) to inform the reader it is ready to communicate. The reader requests two pseudo random 16-bit numbers, the Tag (1) generates the requested numbers R_1^{Tag}, R_2^{Tag} and replies to the reader.

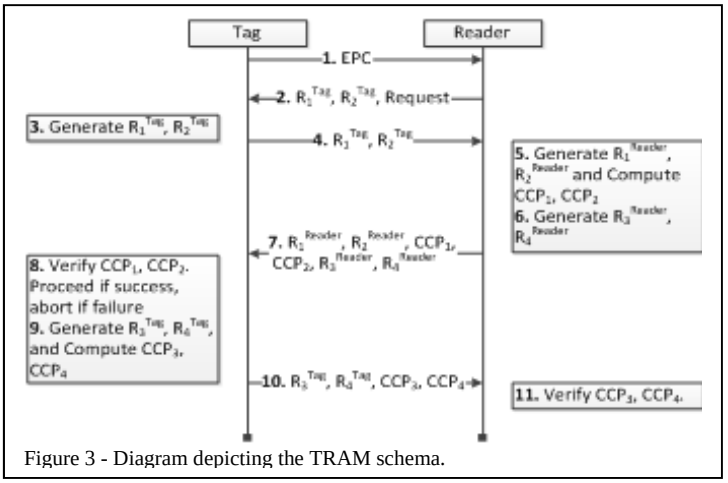

Figure 3 - Diagram depicting the TRAM schema.

Reader → Tag: R_1^{Reader}, R_2^{Reader}, CCP_1, CCP_2, R_3^{Reader}, R_4^{Reader}

The reader generates two additional 16-bit random numbers R_1^{Reader}, R_2^{Reader}. Using the four random numbers, R_1^{Tag}, R_2^{Tag}, R_1^{Reader}, R_2^{Reader}, and the reader's private key (PWD), two responses CCP_1 and CCP_2 are crafted where:

$$CCP_1 = PWD_M \oplus PAD_1$$
$$CCP_2 = PWD_L \oplus PAD_2$$

Where PWD_M and PWD_L are the 16 most significant and 16 least significant bits of the 32-bit private key. PAD_i is the result of the protocol specific function PadGen()(See Fig. 4). The reader then generates two additional 16-bit random numbers R_3^{Reader}, R_4^{Reader} and sends them to the tag.

Tag → Reader: R_3^{Tag}, R_4^{Tag}, CCP_3, CCP_4

The tag then verifies the integrity of CCP_1, CCP_2. If the values are found to be correct, the process continues. Otherwise, the tag aborts communication. If successful, the tag generates two additional random numbers, R_3^{Tag}, R_4^{Tag}, and utilizing the PadGen() function and creates:

$$CCP_3 = PWD_M \oplus PAD_3$$
$$CCP_4 = PWD_L \oplus PAD_4$$

At this point the tag now has the private key needed to communicate with the reader. R_3^{Tag}, R_4^{Tag}, CCP_3, CCP_4 are then sent to the reader.

Reader: The reader then verifies the validity of CCP_3, CCP_4. If valid, the reader now has the Tag's private key and the relationship between the tag and reader is authenticated. [9]

E. Description of the PadGen() Function

The PadGen() function is used to create a cover-coding pad to hide the private key during transmission. The function breaks up the 32-bit private key into two parts, PWD_M and PWD_L, then uses the two randomly generated numbers R_i^{Tag} and R_i^{Reader} to indicate a bit address within PWD_M and PWD_L. PadGen() then selects those bits from PWD_M and PWD_L to form the 16-bit output pad. As such PAD_i (for i = 1, 2, 3, 4) can be expressed as: $PAD_i = PadGen(PWD, R_i^{Tag}, R_i^{Reader})$[9]

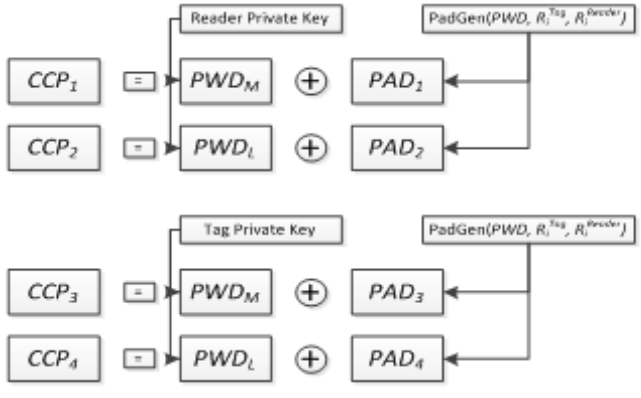

Figure 4 - Visual depiction of the required inputs to create the CCP token.

IV. Future Trends

The history of RFID technology is rich with innovation, and use is continuing to expand. Over the next four years a number of business and security implementations will drive forth adoption and ease a number of privacy concerns. As a result consumers and businesses will be less apprehensive in implementing RFID based solutions.

Within the business world, RFID technology will provide solutions to problems in asset tracking, manufacturing efficiency, payment systems, and a number of unique implementations. Within asset tracking, businesses will be able to better manage and track assets, reducing asset loss and improving efficiency. For example, Air Canada implemented an active RFID solution to track catering carts used worldwide. The system, tracked and managed over 10,000 food carts, reduced unexplained material loss, eliminated the need for inventory counts, and ultimately reduced expenses by two million dollars every year [10].

Similarly, RFID offers a number of advantages to manufacturing facilities. Factory workers will be able to wirelessly fill work orders and ensure all parts are on hand for a given project. This ability to instantly inventory and pull parts has resulted in dramatic increases in efficiency for companies such as Club Car. Club Car invested "millions of dollars in designing and deploying a new manufacturing process" leveraging RFID technology. As a result, the company has decreased the production time of each vehicle from 88 minutes to 46 minutes [11].

Likewise, over the next few years we expect RFID technology to be further implemented in payment systems such as credit cards, pay tolls, and grocery stores. Wireless highway toll systems have been well received and allow drivers to pass through expressways, be charged, all without slowing down. Minnesota has implemented the "MnPass" system in the Minneapolis/St. Paul metropolitan area, which is built on RFID technology and provides commuters access to express lanes along the city's busiest routes. In the next few years we expect grocery stores to adopt RFID systems that deprecate the checkout process. RFID tags affixed to food items will simply be scanned as the customer leaves the store, dramatically reducing the time customers spend shopping.

Other creative implementations, such as child tracking and proximity based advertising, have also been proposed. Dolly's Splash Country, a water park in Tennessee, piloted a child tracking system in which park attendees were given bracelets containing RFID tags. As patrons moved throughout the park their location was tracked and in the event of an emergency, parents could track the location of their children. Furthermore, in the future, advertisers will leverage RFID technology to

deliver personalized advertisements to consumers. Consider the grocery store: advertisers could scan customers carts as they walk down the aisle and promote items that complement existing products the consumer already intends on buying.

Future implementations of RFID technology will also address a number of security and privacy concerns plaguing existing implementations. First and foremost, we believe additional standardization will result in a uniform set of classifications and requirements for tags based upon their intended use. For example, product RFID tags such as those found in stores, which contain no personal consumer data, would not require protective measures be put in place to safeguard data. RFID tags used for physical access or identification, such as CSBSJU Saint's ID cards or U.S. Passports, would require a robust set of security features. These standards, and possible future legal requirements, would protect consumers and businesses from risks associated with today's most common RFID implementations.

In addition to improvements in RFID technology, we foresee organizations deploying additional protective measures when dealing with high security RFID implementations. For example, many U.S. government buildings require the use of multi-factor authentication for RFID physical access systems. Many times, users are required to present their RFID tag and enter in a PIN on a keypad to gain entry to secure areas. Additionally, some organizations may require users to hold RFID enabled identification badges inside a protective sheath, which dramatically reduces the range at which the RFID tag can be activated. This shielding measure will protect the tag from unintended readings.

Over the next four years the use of RFID technology will continue to expand as businesses leverage its cost saving abilities and consumers utilize its convenience. Early adopters such as Air Canada and Car Club have demonstrated how RFID technology can dramatically reduce costs and increase efficiency in the workplace. Minnesota drivers have leveraged the conveniences of RFID technology to reduce their commute times through the state's MnPass systems, and U.S. government organizations have taken steps to increase the security of RFID systems. These early adopters have set a precedent and demonstrated the true value of RFID technology, as result we expect RFID solutions to become a more important part of business and consumer operations.

V. Concluding Statements

As we have seen, a number technical security challenges exist within the realm of RFID technology. A variety of solutions have been proposed which address concerns surrounding both privacy and price. Like the history of RFID technology itself, innovation in privacy protocols will continue to grow. [12] I expect additional research will be conducted in creating a new set of standards to govern RFID protocols in a similar manner to many internet protocols which are standardized today. Once privacy and security concerns are addressed, I believe consumers and businesses will see the real value this technology has to offer and will be less apprehensive implementing RFID based solutions.

References

1. The History of RFID Technology [Internet]: RFID Journal; c2010 [cited 2010 02/09]. Available from: http://www.rfidjournal.com/article/print/1338.

2. Niederman F, Mathieu RG, Morley R, Ik-Whan K. EXAMINING RFID APPLICATIONS IN SUPPLY CHAIN MANAGEMENT. Commun ACM 2007;50(7):93.

3. RAMOS A, SCOTT W, SCOTT W, LLOYD D, O'LEARY K, WALDO J. A threat analysis of ***RFID*** passports. Communications of the ACM Dec 2009;52(12):38-42.

4. Thomson AA, Strickland A, Gamble J. The five generic competitive strategies. In: McGraw-Hill; 2009. .

5. HID Corporation. **How an HID card is "read"**. 2005:1-3.

6. Langheinrich M. A survey of RFID privacy approaches. Personal Ubiquitous Comput. 2009;13(6):413-21.

7. Privacy-aware security applications using RFID technology. CSIIRW '09: Proceedings of the 5th annual workshop on cyber security and information intelligence researchNew York, NY, USA: ACM; 2009. .

8. RFID authentication protocol for low-cost tags. WiSec '08: Proceedings of the first ACM conference on wireless network securityNew York, NY, USA: ACM; 2008. .

9. Mutual authentication in RFID: Security and privacy. ASIACCS '08: Proceedings of the 2008 ACM symposium on information, computer and communications securityNew York, NY, USA: ACM; 2008. .

10. RFID Journal LLC. Air canada GETS asset tracking. .

11. RFID Journal LLC. Golf car maker scores with RFID. .

12. Spiekermann S. RFID and privacy: What consumers really want and fear. Personal Ubiquitous Comput. 2009;13(6):423-34.