ICEB 2010 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-1-2010

A Taxonomy of Security Threats and Solutions for RFID Systems

Daniel Firpo

Woohyun Kang

Peter Ractham

A Taxonomy of Security Threats and Solutions for RFID Systems

Daniel Firpo, School of Information Systems and Technology, Claremont Graduate University, Claremont, California USA. E-mail: daniel.firpo@cgu.edu

Woohyun Kang, School of Information Systems and Technology, Claremont Graduate University, Claremont, California USA. E-mail: woohyun.kang@cgu.edu

Peter Ractham, Faculty of Commerce and Accountancy, Thammasat University, Bangkok, Thailand. E-mail: Peter.ractham@gmail.com

Abstract

RFID (Radio Frequency Identification) is a method of wireless data collection technology that uses RFID tags or transponders to electronically store and retrieve data. RFID tags are quickly replacing barcodes as the "identification system of choice" [1]. Since RFID devices are electronic devices, they can be hacked into by an outsider, and their data can be accessed or modified without the user knowing. New threats to RFID-enabled systems are always on the horizon. A systematic classification should be used to categorize these threats to help reduce confusion. This paper will look at the problem of security threats towards RFID systems, and provide a taxonomy for these threats.

1. Introduction

Radio Frequency Identification (RFID) systems are a subset of Automatic Identification (Auto-ID) systems. These systems originally found common usage in access control and security applications, when they were used primarily to track products through the supply chain or manufacturing process, and to identify products at the point of sale or service [2]. Since the early 1970's, bar code technology has been primarily used for Auto-ID systems. RFID systems have been seen by many industry professionals as the replacement for barcodes as the Auto-ID system of choice [1]. RFID tags are small electronic tags that function much like barcodes. The advantage of using RFID over barcodes include the fact that information about products with RFID tags can be transmitted from several products simultaneously, from a distance, and sometimes through physical barriers [3]. RFID is a contactless technology, and tags can be read whenever they are within range of a transmitted radio signal, and do not need to be brought within line of sight a scanner as does barcode technology. This is one of the main advantages of the use of RFID technology, since it reduces or eliminates most problems associated with other similar technologies that require contact or line-of-sight in order to be scanned or read. Because of this, RFID tags also avoid several problems that plague barcode systems, such as labels that get worn, dirty, bent, torn, or otherwise deteriorated so much so that they can no longer be scanned, making RFID tags ideal for dirty or wet environments in which barcode labels would quickly deteriorate. There are several other aspects of the technology that make it favorable to barcodes. While barcodes only contain a product ID, RFID tags can hold sensors that transmit back to readers information on specific attributes of the product it is affixed to, such as temperature. This advancement in data transmission also enables companies to automatically update their databases, which could provide greater benefit for different activities within their value chain. Unlike barcodes, users can also change the data on certain RFID tags.

RFID tags are also processed more quickly than barcodes, with the average RFID system receiving and processing data simultaneously from hundreds of tags per second. The average time it takes for a good read on a Read-Only RFID tag is between 30-100 milliseconds. This allows RFID systems to simply scan tagged products as they enter a facility through gate readers and proximity devices embedded in company facility floors, rather than to manually retrieve a distinct individual visual reading of each barcode label. A truck's cargo would not need to be unloaded to be scanned by an RFID reader, since the RFID tags on the cargo could be read through the sides of the truck. The idea behind RFID is that eventually, when RFID tags and readers are so inexpensive that every product in the supply chain can be tagged, RFID will allow managers to keep tabs on every minute detail of the supply chain, such as verifying that the right product is loaded on the right truck [1,4]. Unlike barcode, RFID is also quite difficult to copy.

Of the billions of barcodes scanned daily worldwide, most are only scanned once over the product lifetime [2]. Since RFID-tagged objects can be tracked from anywhere on the globe in an instant as long as it is within range of an RFID transceiver, everyone in an RFID-enabled supply chain, “from the manufacturers at the factory to the inventory trackers at the retail location” can instantly obtain information on the location or condition of any particular object [1].

With the increasingly widespread adoption of RFID systems such as passports and drivers licenses, a systematic classification of the security risks would be useful for potential adopters. The motivation for creating a taxonomy for RFID security threats is to condense and classify large amounts of data into a more easy-to-navigate format, and to direct potential users to further resources [5].

This paper will present an overview of RFID technology, an overview of security threats to RFID-enabled systems, a taxonomy for categorizing these threats and possible solutions to these threats, and finally cover some of the factors in evaluating risk exposure in RFID systems for practitioners.

2. Background

2.1 Uses

The growth in the industry in the middle of the decade was driven by the adoption of RFID technology by large organizations such as Wal-Mart and the Department of Defense [6,7]. The RFID industry grew to $5.56 billion in 2009, having tripled over the last 5 years, and analysts estimate that the fast growing RFID market in China will fuel continued growth for the industry [8].

The different kinds of tags can be used for a wide variety of purposes. Low frequency tags can be used for identifying lost pets, passport inspection, in supermarket checkout lines, or in automobile anti-theft systems. High frequency tags can be used for tracking airline baggage or books in libraries.

One of the most common uses of RFID systems are on toll booths, often called e-Tolling or Intelligent Traffic Systems. Toll road authorities have given out transponders that drivers connect to their credit cards. A reader in the toll booth automatically collects tolls from vehicles that pass through at up to 40 miles per hour, dramatically speeding the flow of traffic. Other uses include RFID-equipped Security Badges that not only control employee access to certain parts of a facility, but allow management to track the locations of employees within the facility. Several countries, including the United States, the United Kingdom and Ireland, most of the European Union, Australia, Japan, South Korea, Taiwan, Hong Kong, the Philippines currently insert RFID tags into passports, Livestock tracking can also use RFID tags to track their growth and food intake to improve the raising of animals such as cows, pigs, and chickens.

Another use for RFID is tracking livestock on large farms through RFID tags embedded under the skin Other uses include RFID-equipped bracelets given to children at amusement parks, so that lost children can quickly be found by RFID readers placed around the park. One of the most common uses for RFID is for tracking goods through container loading facilities.

Also, readers placed in heavily trafficked areas like airports would be able to easily monitor currency flows and illegal activities such as money laundering [9].

2.2 RFID System Components

The typical RFID system is made up of three components: The transceiver on the RFID reader, the transponder on the RFID tag, and the back-end database.

RFID readers can communicate with RFID tags using either near-field or far-field methods. In near-field RFID systems, the reader would contain an antenna (in the form of a coil), which produces a low-level radio frequency magnetic field. This magnetic field serves “as a ‘carrier’ of power from the reader to the RFID card or tag.” When a signal is sent from a tag to the reader, the reader will detect and process this signal, and verify whether the signal is valid. If it is, the data is restructured and sent to the end-user’s host system. Far-field systems would communicate with electromagnetic waves, rather than magnetic fields.

Typical RFID tags are made up of three components: The antenna, a silicon chip, and the enclosure. Tags in far-field RFID systems would contain a dipole-like antenna. Meanwhile, similar to the antenna on a reader, the antenna on a near-field RFID tag is made up of a coil. The antenna receives signals from tag readers and transmits data from the chip, which stores data associated with the tag. The antenna’s chip needs a small amount of electric power to function. The antenna gathers energy present in the magnetic field produced by the reader and converts it into a source of electric power for the chip. This allows the tag’s antenna to transmit the contents of the chip to the reader via an electromagnetic signal. The enclosure is the packaging around all the components in the tag. RFID tags can be affixed to any object that needs to be tracked, such as pets, vehicles, items in a store, shipping containers, or even people. These tags have antennas that allow them to communicate and respond to queries on the status of the object with RFID transceivers via radio signals.

As of 2010, Hitachi has made the smallest RFID chip ever manufactured, at 0.075mm by 0.075mm [10].

2.3 Tag Varieties in RFID Systems

RFID tags come in two forms: passive tags and active tags.

Passive tags contain no power source and must use the electromagnetic waves from the reader to send back signals. These are the most commonly used tags. Passive tags have a much shorter range than active tags. Passive tags are often used as ID badges for employees, who only need to walk by a reader for the tag's data to be read. As passive tags do not depend on a battery, they are much cheaper to produce than active tags. Passive tags are created with unique identification numbers, and the contents of their chips can never be changed. Their unique identification number is generally all that is transmitted to readers when queried. Passive RFID tags boast a moderate range from 10 mm to 6 meters. Having no power supply means that passive tags have an incredibly long shelf life. Another advantage is that the lack of a power supply means that the tag can be very small. The smallest commercially available RFID tags are passive tags.

Active tags contain a battery. The battery energy, along with a larger antenna allows the tag to transmit stronger signals up to 1500 feet. Active tags are also beneficial in areas with high tag travel speeds. One of the main drawbacks to this however, is the dramatic increase in tag size. The smallest active RFID tag has dimensions of 26mm x 23mm x 7.3mm [11]. While the presence of a battery makes active tags more expensive to produce than passive tags, active tags are more accurate and reliable than passive tags. Active tags have the same shelf life of their battery power source, which is usually between 3 to 10 years. Active tags do not require special readers and can "readily satisfy applications that require a mix of both passive and active tags." Due to the battery power, active tags can hold much more data than passive tags, and this data can be written, re-written, or deleted using an external read/write device. Likewise, active tags are much more expensive than passive tags, and have more security issues dealing with hackers that attempt to modify and overwrite the information of the chip.

Active RFID tags can be further broken down into three categories: Read-Only (RO), Read-Write (RW), and Write-Once-Read-Many (WORM). The data on Read-Only tags are programmed when the tag is manufactured and cannot be changed or altered in any way. The content of a Read-Write tag can be written-to and read-from by users via readers that double as "writers," and is usually used in applications such as prepaid value cards, , and industrial compliance marking, and toll collection. Write-Once-Read-Many tags are essentially Read-Only, in that once the data is written onto the tag, it cannot be altered. The difference from Read-Only tags is that the data is not written onto the tag at manufacture, and the data can be written by the user once after manufacture.

A further categorization of RFID systems can be found in [5].

3. Security Issues in Practice

RFID tags have numerous benefits for security. Airline passenger and baggage tracking can be simplified by the use of RFID systems. Authentication systems can utilize RFID in applications such as key-less entry systems for cars. RFID tags embedded in documents, products, or currency, can also combat forgery or money laundering [2]. However, there are several security issues raised by the use of such technology. RFID tags are the "quintessential Pervasive Computing technology" [3]. A common issue with any sort of wireless system is security, and just as with wireless LANs, anyone with the correct kind of reader within range can read tag data. A hacker might even be able to overwrite data on active tags [12]. The choice between passive and active tags also present a number of issues. Active tags have greater security concerns, but are several times more sophisticated.

RFID systems have a number of traits that lend themselves to exploitation by malicious users. While RFID tags have extremely limited complexity, the middleware, such as reader interfaces and back-end databases, have plenty of source code that hackers can exploit. The reliance of generic Internet protocols and facilities for RFID middleware means that the system inherits their security vulnerabilities. The financial or personal nature of data handled in RFID systems and back-end databases, along with the false sense of security RFID systems give users, also presents malicious users with an extremely tempting target [3].

To highlight the ease at which some RFID systems can be exploited, in 2009, Chris Paget, a white hat using $250 worth of off-the-shelf components – some purchased off of eBay – built a mobile platform capable of cloning RFID tags used in drivers licenses and passcards (passport-like identification cards used for travel between the US, Mexico, and Canada) [13]. These tags use no encryption and can be read from distances of over a mile, making them susceptible to tracking and spoofing. Using an RFID reader, an antenna mounted to the side of his car, and a laptop connected to the RFID reader via Ethernet cable. The laptop runs an application Paget developed which continuously prompts the reader to look for tags, logging the serial number each time one is detected. The equipment can pick up tags from 30 feet away, meaning Paget can glean info from license and passcard owners as he drives by them. With more expensive equipment, he can widen the range to read tags from over a mile away.

The RFID tags only contain a record pointer to a secure database, rather than personally identifiable information. However, this information can serve as a sort of electronic license plate, in order to track the movements of the passport or license's owner, making this an example of a Traffic Analysis attack. This electronic license plate can be complemented with information gleaned from other sources in the user's tag constellation, "such as electronic toll-booth payment systems or RFID-based credit cards" [13].

3.1 Security Requirements for RFID: The CIA-DAD Triad Model

High-security RFID systems must be able to defend against the unauthorized reading of tags in order to duplicate or modify data, the placing of spoofed or counterfeit tags within the interrogation zone of an RFID reader, and the eavesdropping of RFID communications for the purpose of traffic analysis or setting up replay attacks [14].

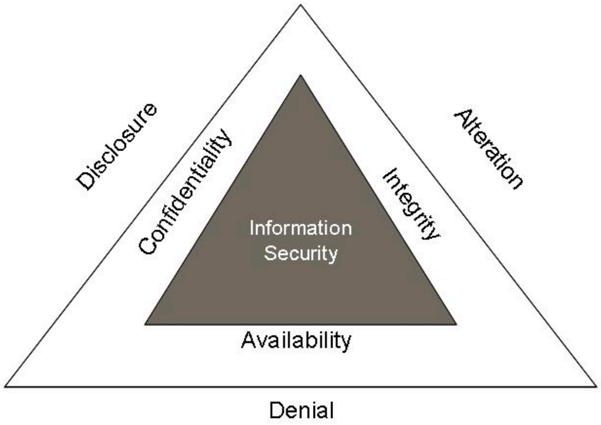

Figure 1. CIA-DAD Triad Model

As shown in Figure 1, every system should have three main security requirements, highlighted in the CIA-DAD model of security threats [15].

CIA stands for the three main security goals:

- Confidentiality: The data can only be read by authorized parties
- Integrity: Only authorized parties can modify data
- Availability: Requires data to be available to authorized parties

DAD, respectively, stands for the three main goals of hackers trying to attack the system:

- Disclosure: Access to confidential information by unauthorized parties
- Alteration: The modification of data by unauthorized parties
- Denial: Denying services to authorized users.

Confidentiality is a difficult goal to achieve in RFID systems, as tags indiscriminately reveal sensitive information when queried by readers. Some of the common threats to RFID systems include the physical manipulation of RFID tags, denial of service attacks by signal jamming radio frequency channels, modifying the identity of an item through tag manipulation, and spoofing legitimate tags by writing properly formatted tag data onto blank or rewritable transponders [3,16]. This technique was used by researchers from John Hopkins University and RSA Security when they spoofed a legitimate RFID tag and used it to unlock an RFID-based car immobilization system [3,17]. Eavesdropping, sometimes called sniffing, is another common security threat. Mark Weiser, an early visionary of ubiquitous computing, noted that privacy was a major problem that ubiquitous computing would have to solve [18]. RFID tags can be read from a distance by any compliant reading device without anyone's knowledge. A similar threat is malicious users using traffic analysis to gain critical information from the patterns of communication. This is a dangerous threat, because critical information can be obtained from the traffic and not the actual content of the messages. Thus, this technique can be performed even when encryption is utilized [3,16]. This is a major concern to those who believe the widespread use of RFID tags could compromise their privacy. They fear that with widespread adoption of tags in the products they buy, eavesdroppers would be able to scan the contents of their home or even their pockets. Even if tags only contain product codes, individuals could still be identified and tracked by the unique set of products (the "constellation") they carry [19]. This perceived assault on privacy has led to the creation of organizations opposed to the use of RFID technology, such as CASPIAN [20] or FoeBuD [21]. Finally, RFID relay devices can be used to set up replay attacks by intercepting and retransmitting RFID queries [22].

Security requirements in RFID systems are often hampered by low-cost issues. Consider an RFID system where one would like to implement access control and authentication. Symmetric or public key cryptography can offer a solution. However, RFID tags have extremely limited resources. Oftentimes, they only have between 2000 to 3,000 logic gate in which to available for on-tag security features [23]. This limitation immediately disqualifies use of several standard encryption algorithms. A standard implementation of Advanced Encryption Standard (AES) symmetric key encryption requires around 20,000 to 30,000 logic gates [16]. Furthermore, many RFID system performance requirements often dictate that a certain number of tags must be read (oftentimes around 100 to 200) every second, further limiting the number of clock cycles that can be devoted to encryption algorithms [19]. Strong cryptography is beyond the resources of low cost tags (which cost around or less than $0.10 per tag) [2,24], although there are solutions for more sophisticated and expensive tags, such as NTRU [25] or TEA [26]. Symmetric key encryption algorithms also introduce an overhead for complex key management. Such tags must also be protected from physical attacks on the tags themselves that can be used by attackers to reveal their entire contents [19]. An attacker who can gain a shared key compromises the security of the entire system, thus tags cannot be trusted to store long-term secrets without protection from physical attacks.

4. A Taxonomy for RFID Security Threats:

Considering the large volume of knowledge on RFID security, this taxonomy serves the purpose of condensing some of that knowledge to make it easier to navigate, and direct potential adopters to further resources, and to give academics interested in the topic an overview of which subtopics can be expanded upon with further research [5]. The taxonomy is presented in the form of a tree node structure. The branches are not mutually exclusive. The following is a taxonomy for attacks on RFID systems.

Attacks
- Target
- Method

Every attack has a target and a method.

Target
- Confidentiality
- Integrity
- Availability
- Authenticity

4.1. Target

The targets of an attack can be categorized using the CIA-DAD triad model [15], however, a fourth category, Authenticity, has been added. An attack can aim to compromise a system's confidentiality through disclosure. An attack can compromise a systems integrity by altering data that the attacker is not authorized to modify. An attack can compromise a system's availability with a denial of service attack. Finally, an attacker can bypass a system's access control to gain unauthorized access to the system without establishing authenticity, or without the attacker's identity being verified by the system.

Method
- Passive
    - Eavesdropping
    - Traffic Analysis
- Active

4.2. Method

An attack can either be passive or active [27].

4.2.1. Passive Methods. Passive attacks include eavesdropping (sometimes referred to as "sniffing") and traffic analysis (sometimes referred to as "tracking"). Passive attacks are attacks in which no data is modified. Instead, these attacks involve monitoring messages for malicious intent. Thus, these attacks do not fall into the categories of Integrity/Alteration or Availability/Denial in the CIA-DAD model.

Eavesdropping. Eavesdropping involves gaining unauthorized access to data. An example of an eavesdropping attack highlighted by cryptography guru Bruce Schneier, involves the case of passports embedded with RFID tags [28]. Such tags are readable by any reader, not just those carried by passport control, and have been read at distances of up to 30 feet. An eavesdropper could be able to read passport information (name, age, nationality, etc.) from anyone nearby, completely undetected. While the proponents of such passport systems claim that tags would only be readable from a few centimeters, Schneier asserts that wireless protocols can "work at much longer ranges than specified" [28]. RFID tags have multiple read ranges that vary depending on the setting and operational scenario [29].

Traffic Analysis. A traffic analysis attack is like an eavesdropping attack, only instead of monitoring the content of the messages, the attributes of the message traffic are observed. Who's sending messages to whom? How often? What is the "constellation" of tag ID's does an individual have at the moment? Patterns in communication are observed. Because the content of the messages are not the target of such attacks, this kind of attack can be performed even when messages are encrypted.

- Method
    - Passive
        - Eavesdropping
        - Traffic Analysis
    - Active
        - Physical Attacks
        - Masquerade
            - Counterfeiting
            - Spoofing
        - Replay
        - Denial of Service
        - Malware
            - Exploits
                - Buffer Overflows
                - Code Insertion
                - SQL Injection
            - Worms
            - Viruses

4.2.2. Active Methods. Active attacks are attacks that involve more sinister attacks than just monitoring messages.

Physical Attacks. The first category involves actual physical manipulation of the RFID tags in a system. RFID tags usually offer little to no resistance to these kinds of attacks [16]. These attacks are especially dangerous, because they are oftentimes unexpected. An RFID system can have extremely sophisticated electronic security, but it is useless if an attacker can easily walk into the building and steal a tag or reader without being noticed.

Masquerade. Masquerade attacks include counterfeiting and spoofing. Counterfeiting involves modifying the identity of an item, while spoofing involves impersonating legitimate tags [16]. Examples of such include rewriting tags on expensive products in a store or warehouse with counterfeit data from much cheaper products, or spoofing a legitimate tag on a product so that the store or warehouse's security systems mistakenly believe the product is still on its shelf [19].

Replay. Replay attacks occur when a hacker intercepts and rebroadcasts an RFID query with an RFID relay device [22]. Revisiting Bruce Schneier's example of a passport system where each passport is equipped with an RFID tag, a replay attack could be used to gain unauthorized access at a border crossing [30]. In his example, a group of people are in line at a border crossing. An attacker could gain access by relaying messages to and from another traveler with a legitimate passport. A customs agent's reader sends a query to the attacker's RFID tag. The attacker receives the query and rebroadcasts it to the other traveler's tag. The traveler's tag responds as if the customs agent's reader had broadcasted the query, sending a reply back to the attacker. The attacker relays this reply back to the customs agent's reader. In doing this, the attacker has successfully impersonated the other traveler. Encrypting the messages would not prevent such an attack, since the attacker "is simply acting as an amplifier" [30]

Denial of Service. Denial of Service attacks aim to reduce the availability of the system to zero. In RFID-enabled systems, this is usually done by using signal jamming to prevent RFID tags from being read [3].

Malware. Malware, or malicious RFID code, is another category of active attacks. Rieback et al 2006 categorizes malware into three different categories: RFID-based exploits, RFID-based worms, and RFID-based viruses [3,31]. RFID-based exploits include buffer overflows, code insertion, and SQL injection. Many devastating exploits can be written onto an RFID tag even with its memory constraints. Buffer overflows are where the attacking RFID tag tries to access and modify out-of-bounds array values. For example, for an array, Array[10], code should not be able to modify Array[k] for k >= 10. Code insertion is the use of scripting language to insert malicious code onto user applications. SQL injection is a variant of code insertion that performs unintended SQL queries on the victims' databases. Short commands such as ";shutdown--" or "drop table…" can be especially devastating [3,33]. RFID worms and viruses are self-replicating RFID exploits that copy the malicious code across the network and infect other RFID tags by writing the exploit code over their data. Worms do not require any user activity to propagate, however they are reliant on the presence of a network connection [34]. In Rieback et al 2006, researchers demonstrate the feasibility of a self replicating RFID virus using only 127 characters on a tag with 896 bits of data [3].

To reiterate, the branches of this taxonomy are not mutually exclusive. Some attacks combine attributes of several branches of the tree structure. Even active attacks sometimes begin with passive attacks. For example, replay attacks begin with eavesdropping to gain a message that can be retransmitted.

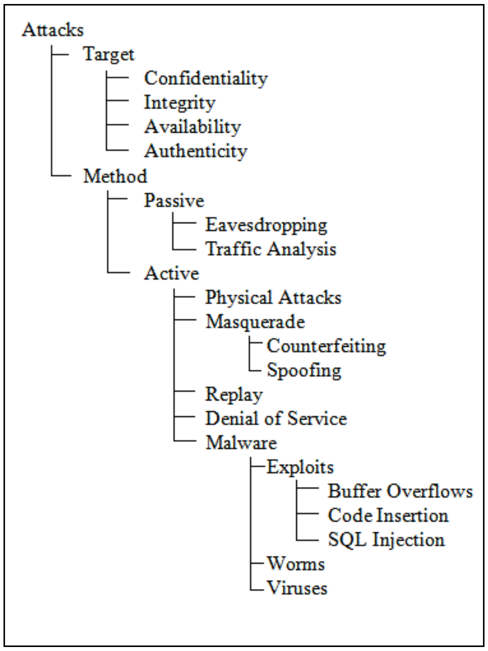

Figure 2. Proposed Taxonomy Architecture (Security Threats)

5. Solutions for Defending Against RFID Security Threats

To combat these threats, clear security goals need to be established before implementation. Products with RFID tags should not betray the privacy of those who purchase them. Information should not be disclosed to unauthorized readers, and it should not be possible to set up long-term tracking associations between RFID equipped products and users who purchase or use them. To prevent long-term associations, public tag output should be randomized or easily modified, while private tag contents should employ access control and/or encryption. Users should be able to detect and disable any tags in the products they use. Tags and readers should be protected from the spoofing of either party, replay attacks, and eavesdropping [2].

The following is a taxonomy for defending against security threats to RFID systems. Again, the branches are not mutually exclusive. The same system can – and should – employ several of these methods.

Defense
Target
Method

As with attacks on RFID systems, defense involves a target to defend against and a method to employ to protect the system.

Target
Confidentiality
Integrity
Availability
Authenticity

The targets to defend against are also categorized using the CIA-DAD triad model.

Method
Physical Access Control
Electronic Access Control
Anti-Malware

There are several potential solutions to RFID threats. They can be fit into three categories: Physical Access Control (e.g. disabling or killing tags), Electronic Access Control (e.g. read access control for tags), and general techniques used for fighting RFID malware.

Physical Access Control
Disabling Tags
Faraday Cages
Jamming
Blocker Tags

5.1. Physical Access Control

The first solution category is physical access control, usually through shielding, disabling, or killing tags [35]. As tagged products go from one link on the supply chain to the next, or as they reach the hands of consumers, users can disable the tags, partially or completely. Killing tags is the most straightforward defense against RFID security threats: A product's RFID tag is killed before it enters the hands of consumers. For example, at a retail store, checkout clerks would kill the RFID tags in purchased goods so that no purchased goods contain active tags [36]. However, this also gets rid of many of the benefits of using RFID tags in the first place, especially as new RFID applications are starting to emerge for consumers, like airline tickets embedded with RFID tags for simpler tracking of passengers [36]. One solution to prevent tags from being eavesdropped is the use of Faraday Cages. Faraday Cages are containers made of metal mesh or foil that can block radio signals. These containers can be used to keep unused tagged products to prevent passive attacks on these products [16]. However, these may be cumbersome and thus impractical for certain RFID-equipped object. Another approach to ensure privacy is the active jamming of radio frequency signals, to disrupt nearby RFID readers that might try to eavesdrop the user's tagged possessions. However, this approach can disrupt other legitimate RFID systems nearby [37]. The use of smart "blocker tags" is another privacy solution. Blocker tags can simultaneously simulate all possible RFID tags to block RFID readers. By simulating a selected subset of ID codes, the blocker tag can selectively block RFID readers used by outsiders [37].

Electronic Access Control
    Encryption
    Random Access Control

5.2. Electronic Access Control

Another solution to RFID threats is electronic access control, through the use of classic cryptography algorithms, such as symmetric or public-key encryption. However, as stated earlier, low-cost RFID tags are not sophisticated enough to handle some encryption algorithms. A potential solution is the use of read access control methods, like Hash-Based Access Control [19]. In hash-based access, tags are capable of carrying out a one-way hash function. A one-way hash is a function that is easy to compute, but for which it is difficult or impossible to compute its inverse. A simple example would be f(x) = x^2. Finding the square of a number is a simple procedure, but doing the inverse, finding a number's square root, is much more difficult without the aid of a calculator. Each tag is associated with a key, and each tag stores the hash of its key. In Hash-Based Access Control, each tag has two states: locked and unlocked. While in a locked state, the tag will respond to any and all queries by returning the hash of its key. To unlock a tag, the reader queries the tag in order to receive the hash of its key. The reader then looks through the back-end database for the tag's corresponding key. The reader transmits the key to the tag. The tag hashes the key and compares it to the hash stored in its memory. If it is a match, the tag then unlocks. There are two downsides to this approach. First, it is susceptible to replay attacks. An attacker could query a tag for the hash of its key, and then replay it for the reader in order to obtain its key. Also, since locked tags always output the same value (the hash of its key), this can be used as an identifier that malicious users can use to track tags in traffic analysis attacks.

A way of overcoming this is with Randomized Access Control [19]. In this solution, tags are also equipped with a random number generator. Instead of always responding with the same reply, which could be used by attackers in replay attacks, the tag concatenates its ID with a random number before hashing. The tag then sends two values to the reader: the random number, and the hashed value. The reader uses these two values to search the back-end database for the value that unlocks the tag. The downside of this method is that it is only practical for systems with a small number of tags, as the overhead increases significantly with the number of tags in the system. Poschmann et al. 2009 describes a cryptography algorithm using randomized access control for RFID systems that can be implemented within the oft-cited 2000-3000 gate equivalent limit [23], and more recently, Alomair et al. 2010 propose a protocol for establish unconditional secrecy and unconditional integrity through randomized access control for use in low-cost RFID (i.e. potential tag price at or less than $0.10) systems [23].

In addition, Eisenbarth et al. 2007 chronicle several further lightweight Cryptography Implementations [38].

Anti-Malware
    Bounds-checking
    Input sanitization
    No back-end scripting
    Limiting database access
    Parameter binding

5.3. Anti-Malware

Four years have passed since the first paper detailing the plausibility of an RFID virus. However, as of 2010, the threat of an actual case of an RFID virus has yet to materialize, and thus, steps to defend against an RFID virus is not yet concrete. Most defense against RFID malware then focus on RFID-based exploits. To defend against RFID-based exploits, there are several steps that can be taken [3]. Bounds-checking can be done to prevent buffer overflows. This is the process of ensuring that array values being accessed are within bounds. To fight code insertion or SQL injection, the input can be sanitized by several means to get rid of characters that these attacks usually use, such as "<," ">," "&," or "%." For example, it can be required that all input consist only of alphanumeric characters. However, this sometimes presents a problem, as there are times when the input needs these characters. Other methods include eliminating back-end scripting support, limiting database access (i.e., making most or all database tables read-only), and parameter binding [3].

The solutions for RFID security threat described above are summarized in Figure 3 below. Table 1, further below, also details the pros and cons associated with each viable security solution, for potential adopters of RFID systems to weigh security options against each other.

6. Risk Analysis and Measurement: Balancing Cost and Risk in RFID Security

Balancing cost and risk is a crucial aspect of securing RFID systems. If RFID technology is to replace barcodes as the Auto-ID system of choice, then RFID tags will substantially contribute to the cost of items that would otherwise be affixed with barcode tags. Even if the price of tags equipped with secure cryptography can be driven to $0.10, it would be impractical to attach them to low-cost items – “When retailers are to choose between tags that can perform sophisticated cryptographic operations and cheaper tags that cannot, it seems inevitable that the cheaper tags will prevail” [24].

An example of the costs that a system can incur from not adequately protecting itself from security threats can be seen in the case of the Mifare Classic smartcard [39]. There are an estimated 2 billion Mifare Classic cards used worldwide as payment cards for transportation networks or for access to schools, hospitals, and government buildings. In 2008, a group of researchers from Radboud University Nijmegen in the Netherlands managed to hack the Mifare Classic smartcard. After learning of the breach, the Dutch Government postponed a one billion euro transport system similar to Mifare, moved to spend millions of euros upgrading its systems – including replacing the cards of all 120,000 civil servants at 5 euros per card, and posted armed guards outside all its buildings [40]. Mifare is an example of a large public application connected to a service product. Such a large-scale and open application requires rigorous security. However, NXP Semiconductors, the developer of the Mifare system, allegedly protected their system with poor or sloppy cryptography, and suffered both financially and in terms of reputation when the research team from Radboud University publicized their work [41]. In order to assess what methods should be used to protect RFID systems, one must compare the costs of implementing such systems versus the risk of not having such protections in place. This risk factor, sometimes called the “Risk Exposure,” can be measured with the following equation:

$$RE = P(UO) * L(UO),$$

where RE is the Risk Exposure, P(UO) is the probability of an Unsatisfactory Outcome, and L(UO) is the loss to the stakeholders if such an outcome occurs [42].

If the costs of implementing security protocols is far greater than the risk exposure, than it would probably

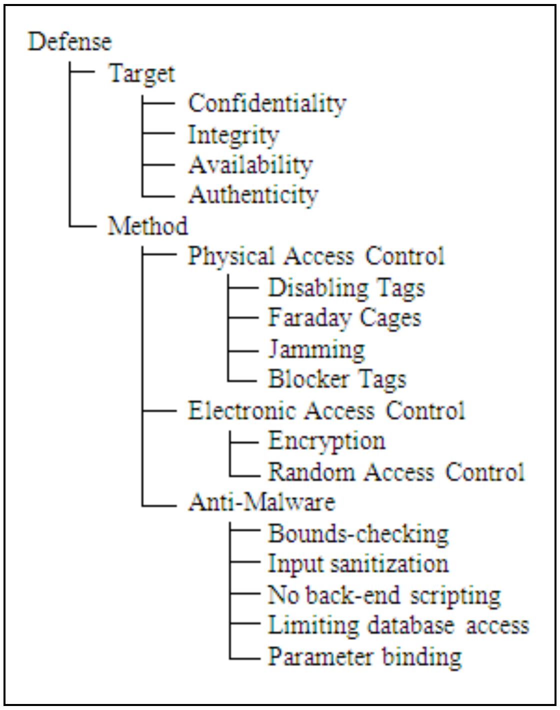

Figure 3. Proposed Taxonomy Architecture (Security Solutions)

Table 1. Solutions for RFID Security Threats

Solution	Pros	Cons
Physical Access Control 1. Disabling Tags 2. Faraday Cages 3. Jamming 4. Blocker Tags	Establishes Confidentiality, Availability 1. Can handle many if not most privacy concerns 2. Severely or completely eliminates opportunities for Passive and DoS attacks 3. Eliminates opportunities for Passive DoS attacks 4. Can selectively block RFID readers used by outsiders	1. Limits usability of the system, especially as more RFID applications emerge 2. At best a partial solution. Maybe cumbersome for certain RFID-equipped objects 3. Can disrupt legitimate RFID systems nearby. Could be illegal.
Electronic Access Control 1. Encryption 2. Random Access Control	Establishes Confidentiality, Authenticity 1. More viable with cheaper tags 2. Provides more security than simple	1. Susceptible to Replay and Traffic Analysis attacks. 2. Solves this, but the overhead limits this solution to small systems
Anti-Malware 1. Bounds-checking 2. Input sanitization 3. No back-end scripting 4. Limiting database access 5. Parameter binding	Establishes Integrity 1. Safeguards against Buffer Overflows 2-5.Safeguards against Code Insertion and SQL Injection	1. Sometimes produces run-time delays 2. Input characters sometimes needed

be better to take a risk and forego such protocols. This can be highlighted with two example RFID applications: A closed industrial application and a public application connected to monetary and material goods. With the closed industrial application, only a small group of people are authorized to access the system. A malicious user could bring the system down, but at no personal benefit. Since the probability of an attack on this kind of application is extremely low, a cheap system with little or no security logic is acceptable. However, the public application is open to anyone, and a successful attack by a hacker could cause large-scale financial damage and ruin reputations. Such an application requires utmost security [14].

In addition to measuring Risk Exposure to help decide which security investments to make to protect an RFID system is, potential adopters can also calculate Risk Reduction Leverage (RRL). Risk Reduction Leverage measures return of investment on a risk reduction technique, using the following equation:

$$RRL = (RE_{before} – RE_{after}) / \text{Risk Reduction Cost},$$

where RRL is the difference between the system's Risk Exposure before and after a risk reduction activity is implemented, divided by the cost of implementation [43].

7. Implications and Future Work

The taxonomy presented above organizes and summarizes many of the security issues present in RFID systems, and highlight areas for future researchers to develop improved solutions to RFID security issues. However, more iterations and further research is required before they become a definitive source for classifying RFID security threats and RFID security solutions. According to Hassan & Chatterjee 2006, a systematic study of a field is "a precursor to any detailed research of the field" and that "some classification knowledge gives a ground plan" for study of the field [5]. Therefore, this study has value for potential practitioners and adopters of RFID-based systems as a guideline for comparing solutions from multiple vendors and evaluating the costs/benefits and pros/cons of each.

8. Conclusion

RFID systems are rapidly evolving, and as organizations and governments increasingly seek to adopt these systems, RFID security will become even more of a critical issue. In this paper, we attempt to explore the current state of RFID security, and describe a taxonomy for RFID security threats in order to give practitioners a clearer picture of the risks they must defend against, and serve as a road map for choosing possible solutions. Finally, we discussed the issues that arise when having to balance potential risks to the system and the costs of implementing safeguards.

9. References

[1] The RFID Gazette, "RFID 101 – The Future is Here: A Beginner's Guide to RFID". The RFID Gazette June 28, 2004, at *http://www.rfidgazette.org/2004/06/rfid_101.html* (last accessed June 15, 2010)

[2] Sarma S., Weis S., Engels D., "RFID systems and security and privacy implications." *Cryptographic Hardware and Embedded Systems - CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13-15, 20. Revised Papers*, Springer Berlin / Heidelberg, 2003, pp. 454-469.

[3] Rieback M., Crispo B., Tanenbaum A., "Is Your Cat Infected with a Computer Virus?," Proc. *4th Ann. IEEE Int'l Conf. Pervasive Computing and Comm.*, IEEE CS Press, 2006, pp. 169–179.

[4] Material Handling Solutions, "Is RFID For You?". Material Handling Solutions , at http://www.milesdata.com/_pdf/04q2_solutions_p8-9.pdf (last accessed June 15, 2010)

[5] Hassan T., Chatterjee S., "A Taxonomy for RFID." *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006.

[6] Angeles, R. "RFID Technologies: Supply-chain applications and implementation issues". *Information Systems Management*, (Winter 2005).

[7] TechWeb News. "Sales of RFID tags forecast to rise quickly." *Information Week*, (Jan 12, 2005).

[8] Das, R., Harrop, P., "RFID Forecasts, Players and Opportunities 2009-2019." IDTechEx report (Q3 2009).

[9] Juels A., Pappu R., "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes". *Financial Cryptography*, Springer Berlin / Heidelberg, 2003.

[10] Noda, H., Usami, M., "0.075 x 0.075 mm Ultra-Small 7.5 μm Ultra-Thin RFID-Chip Mounting Technology". *Proceedings of 2008 Electronic Components and Technology Conference. IEEE: Florida,* (May 2008).

[11] Nikkei Electronics Asia, "Orizin Launches 'World's Smallest' Active Asset RFID Tag". Nikkei Electronics Asia (November 2008), at

http://techon.nikkeibp.co.jp/english/NEWS_EN/20081124/161707/ (last accessed June 15 2010).

[12] Molnar, D and Wagner, D. "Privacy and Security in Library RFID Issues, Practices, and Architectures". *Proceedings of the 2004 ACM Conference on Computer and Communication Security. ACM: New York*, (October 2004).

[13] Goodin, D., "Passport RFIDs cloned wholesale by $250 eBay auction spree". The Register (February 2009), at http://www.theregister.co.uk/2009/02/02/low_cost_rfid_cloner/ (last accessed June 10 2010).

[14] Finkenzeller K., "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification," 2nd Ed. John Wiley & Sons, Ltd., 2003.

[15] Solomon, M.G., Chapple, M., "Information Security Illuminated," 1st Ed. Jones and Bartlett Publishers, 2005.

[16] Peris-Lopez P., Hernandez-Castro J., Estevez-Tapiador J., Ribagorda A., "RFID-systems: A survey on security threats and proposed solutions." *Personal Wireless Communications*, Springer Berlin / Heidelberg, 2006, pp. 159-170.

[17] Bono S., Green M., Stubblefeld A., Juels A., Rubin A., Szydlo M., "Security analysis of a cryptographically enabled RFID device." In *14th USENIX Security Symposium*, pp. 1–16, Baltimore, Maryland, USA, July-August 2005. USENIX.

[18] Weiser M., "The computer for the 21st century." *Scientific American*, 265(3):94–104, September 1991.

[19] Weis S., Sarma S., Rivest R., Engels D, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems" *Security in Pervasive Computing*, Springer Berlin / Heidelberg, pp. 201-212, 2004.

[20] CASPIAN. *http://www.nocards.org/*, 2010.

[21] FoeBuD *http://www.foebud.org/* 2010.

[22] Kfir Z., and Wool A., "Picking virtual pockets using relay attacks on contactless smartcard systems." In *1st Intl. Conf. on Security and Privacy for Emerging Areas in Communication Networks*, Sep 2005. *http://eprint.iacr.org/.*

[23] Poschmann, A., Robshaw, M., Vater, F., Paar, C., "Lightweight Cryptography and RFID: Tackling the Hidden Overheads". *International Conference on Information Security and Cryptology,* Dec 2009.

[24] Alomair, B., Lazos, L., Poovendran, R., "Securing Low-cost RFID Systems: an Unconditionally Secure Approach". *Journal of Computer Security*, August 2010.

[25] Hoffstein J., Pipher J., Silverman J., "NTRU: A Ring-Based Public Key Cryptosystem." *Lecture Notes in Computer Science*, 1423:267–, 1998.

[26] Wheeler D., Needham R., "TEA, a Tiny Encryption Algorithm." Technical report, Computer Laboratory, University of Cambridge, 1995.

[27] Stallings W., "Business Data Communications." 5th Ed. *Prentice Hall* (22 March 2004).

[28] Schneier B., "RFID Passports" *Schneier on Security* (4 October 2004), personal blog available at *http://www.schneier.com/blog/archives/2004/10/rfid_passports.html*

[29] Juels, A., "Strengthing EPC tags against cloning." in *ACM Workshop on Wireless Security (WiSe)*, pages 67-76. ACM Press, 2005.

[30] Schneier B., "RFID cards and Man-in-the-Middle Attacks." *Schneier on Security*. (25 April 2006) personal blog at *http://www.schneier.com/blog/archives/2006/04/rfid_cards_and.html*

[31] Rieback M., Crispo B., Tanenbaum A., "RFID Malware: Truth vs. Myth," *IEEE Security & Privacy*. Vol. 4, No. 4, July/August 2006, pp. 70-72.

[33] Anley C., "Advanced SQL injection in SQL Server applications". *http://www.nextgenss.com/papers/advanced_sql_injection.pdf.*

[34] Weaver N., Paxson V., Staniford S., Cunningham R., "A taxonomy of computer worms." In *First Workshop on Rapid Malcode (WORM)*, 2003.

[35] Gao X.; Xiang Z.; Wang H.; Shen J.; Huang J; Song S. "An approach to security and privacy of RFID system for supply chain" *IEEE International Conference on E-Commerce Technology for Dynamic E-Business*, pp. 164-168, 2004.

[36] Kumar, R., "What Does Privacy Mean in the Context of RFID?" RFID Switchboard at http://www.rfidsb.com/index.php?page=rfidsb&s_ID=9&s_page=1 (last accessed June 15, 2010).

[37] Juels A.,. Rivest R, Szydlo M.. "The blocker tag: Selective blocking of RFID tags for consumer privacy." In *ACM CCS'03*, pages 103–111. ACM, ACM Press, October 2003.

[38] Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., Uhsadel, L., "A Survey of Lightweight Cryptography Implementations". *IEEE Design & Test of Computers – Special Issue on Secure ICs for Secure Embedded Computing*, 24(6):522 – 533, November/December 2007.

[39] Koning Gans, G., Hoepman, J.H., Garcia, F.D., "A Practical Attack on the MIFARE Classic," *CARDIS 2008*, September 2008.

[40] Mostrous, A., (2008, June 21). Alert over security as researchers show Oyster card can be cracked with laptop. *The*

Times at http://technology.timesonline.co.uk/tol/news/tech_and_web/article4184481.ece (last accessed June 15, 2010).

[41] Schneier, B., (2008, August 7). Why being open about security makes us all safer in the long run. *The Guardian* at http://www.guardian.co.uk/technology/2008/aug/07/hacking.security (last accessed June 15, 2010).

[42] Boehm, B., "Software Risk Management: Principles and Practices." *IEEE Software*, pp. 32-41, January 1991, at *http://greenbay.usc.edu/csci577/fall2006/site/coursenotes/ep/Risk.pdf*.

[43] Boehm, B., *Tutorial: Software Risk Management*, Les Alamitos, CA, IEEE Computer Society, 1989.