Table of Contents

10 Figure List

Background

Imagine a world in which every person is tied to a unique barcode-like identification number. These numbers, concealed in clothing, credit cards, license plates, and even currency are incredibly small and can be read without physical contact or line of sight access. Retailers and government institutions can use these identification numbers to track shopping habits, authorize access or payment, pinpoint fraud, or even check for outstanding parking tickets. Is this a futuristic Orwellian nightmare? No, it's a possible, if highly implausible, scenario in which radio frequency identification (RFID) tags are introduced into society without security or privacy protection for individual consumers. While this is certainly a very far-fetched picture, it illustrates the fact that there is a significant amount of security enhancement and public education required before consumer and retailers fully utilize the benefits of RFID systems.

As is to be expected, RFID tags which contain sensitive information: mobile payment devices, bank cards, and building access or identification devices, contain high levels of data security processes including password protection and encryption. These systems provide more than adequate defense against attacks, but also significantly increase the cost of the security-enabled tags. As an example, consider an access card which unlocks a room containing personal data such as social security or credit card numbers. In this case, paying $5 to $10 for multiple layers of data security on a single RFID enabled card is justified, because the cost of an unauthorized intrusion would be significantly higher. Now consider a carton of toothbrushes which would also benefit from RFID functionality (e.g. for shipment tracking, inventory management, or self-checkout). The current electronic product code (EPC) RFID tags, used to identify common retail items like

toothbrushes, cost between 5 and 10 cents apiece, but contain limited security functions.[1] Would the retailer, or the consumer for that matter, be willing to pay for a 20% to 30% toothbrush cost increase to facilitate improved security? No, the price increase is obviously not justified considering the benign nature of the information being stored within the tag. However, this raises an interesting point, what is the standard for which information is benign and which is private? This of course depends on the owner of the tag; consider for example an RFID enabled bottle of prescription medication. The manufacturer of the medicine needs the tag information to be available so that they can track shipments, batch numbers, and comply with stringent government regulations regarding prescription medications. The retail pharmacy which sells the medicine also needs the tag data for inventory management and theft prevention. However, once the medication is purchased, the consumer no longer wants the RFID data to be freely available. In addition to the personal and possibly embarrassing nature of some prescriptions, dissemination of such information could have possible dire consequences, such as denial of insurance coverage if a preexisting condition was not disclosed.[2]

As is evidenced by the above example, the requisite security protocols for an EPC-type RFID tag change depending on the current tag ownership. For example, stringent security for data access would impede the inventory and shipment tracking requirements of supply chain RFID systems. Incorporating additional security protocols into a tag or reader would increase the time required to read the tag's data. This would mean an escalation in the number of misread items and a drop-off in the efficiency of the RFID system. Therefore, an RFID data security system which is implemented in the tag architecture, or travels with the tag is obviously not practical for EPC-type tags. Due to

tag cost and power constraints, the flexibility of such a system would be too limited to meet all of the manufacturer's, retailer's and consumer's needs. However, a significant market exists for security and privacy enhancement in EPC-type RFID applications. This paper presents a mobile, consumer-supported security device which protects against realistic RFID privacy concerns.

Practical RFID Information Security Threats

As mentioned previously, in retail or supply chain applications, the RFID tags change hands multiple times and at each interchange, the new owner of the tag may no longer want the same RFID functionality. This leads to situations in which the owner of the tag may be unaware of the information contained in the tag, or even the tag's existence. In these instances, information security is especially important because line of sight is not necessary to access the data contained in the RFID tag. In order for RIFD tags to be widely embraced by consumers and retailers, the realistic security threats and measures for preventing them must be understood. In the former case, security and privacy concerns with passive RFID tags can be broken down into essentially three categories; direct unauthorized access to the data on the tag, inferred collection of tag data, and location tracking using unique tag IDs.

The first possible security concern with RFID tags involves an unauthorized reader accessing the data on a tag. Because current EPC standards do not require the reader to transmit any identification information to the tag, the data is vulnerable to unauthorized reads.[1] Therefore, in the absence of encryption, the tag simply "wakes up" using power from the reader and transmits the data stored in its memory. If encryption is present, then a series of authentication commands are passed between the reader and the tag, obviously

increasing the tag security. However, as will be discussed later, encryption is impractical for EPC-type tags. For EPC tags without encryption an additional level of security is necessary, in this case it is accomplished by having a third-party managed external database of tag identification, Figure 1. In other words, the binary data stored in the tag's memory cannot be correlated to the identity of the item (e.g. "chicken noodle soup") without access to the database. Ideally, the information in the database cannot be compromised, however several recent high profile third-party database security breakdowns make this unlikely.[3-5]

Figure 1: Tag Data Translation via Database ID Storage

The second security problem with RFID tags is a variation of the unauthorized read-access method discussed above. Because of the querying algorithms used for tag-reader communication (covered in detail later), the data on the tag can be inferred using simple signal analysis. In essence, if the "questions" that the reader asks and the "answers" that the tag returns can be intercepted, then the data on the tag can be inferred without directly querying the tag. It is helpful to think of this process as eavesdropping on a game of twenty-questions in which the "yes or no" answers are replaced by binary digits. As with the unauthorized data access, the inferred data collection method still requires access to the third-party ID database if the tag's information is to be correlated with the product's identity. However, inferred identification is a much more sinister proposition than unauthorized access for two reasons; it is almost impossible to detect and it requires access to the reader, not the tag. The latter consideration is especially important because tags are usually mobile and have a much shorter broadcast range than readers. Therefore,

if the tag data can be collected by intercepting analog broadcasts from a stationary reader, it is much easier for an unauthorized party to access the information.

The final security issue with RIFD tags involves location tracking based on the unique tag identification number. Unlike the previous methods, in this instance the actual information on the tag is not the target of the attack, rather the real-time location of the tag. Because of the storage capabilities of even the simplest EPC tags, 64 or 92 bits of binary data, each tag can have a unique identification number.[1] Contrasted against traditional bar codes, the product type (e.g. "butter") can be augmented with RFID tags to include an individual serial number (e.g. "butter number 3271"). In the 92 bit tag case, there are approximately 5 octillion possible ID combinations, over 750 quadrillion for every person on earth. Figure 2 shows the memory structure of common EPC type tags. As mentioned previously, if tag encryption is not present, then the data on the tag can be freely gathered, leading to situations in which a person can be tracked based on the unique tags that they possess. Because of the small size of the RFID tag, the owner would most likely be unaware of the tag's existence, for example, a tag included as a theft detection device in an article of clothing. Additionally, because of memory and cost constraints, EPC tags are unable to maintain a count or clock-time of every read-access to the tag.[1] Therefore, it is possible to envision a situation in which a person can be tracked using an item of which they are unaware or ignorant.

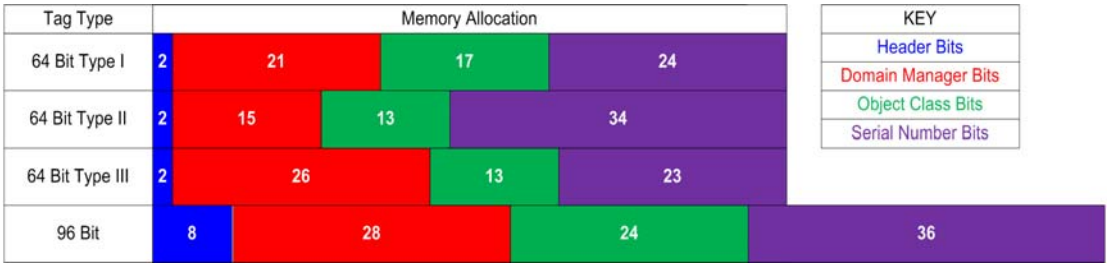

Figure 2: Memory Allocation for Common EPC-Type Tags[1]

Perhaps the best example of this phenomenon involves the Identification Friend or Foe (IFF) systems used by allied pilots in the Korean War. IFF devices were precursors to RFID systems, designed to uniquely identify planes, preventing friendly fire by anti-aircraft batteries. However, a lack of understanding by the pilots meant that they left their IFF systems on when traveling into enemy territory, allowing their movements to be tracked.[6] The following quote comes from the commanding officer of an American pilot operating in the Korean theater:

> "If you're going to cross the Yalu [river separating China from North Korea] for god's sake, turn off your identification friend or foe system, because we can track you on the radar."[7]

It is relatively simple to track a unique RFID tag, especially if the consumer is unaware of it, as was the pilot in the above example. Because access to the product ID database is not required, the only layer of security present is the close proximity required for RF signal broadcasting. As RFID technology becomes more prevalent, however, the number of readers will increase as will their broadcast power, making location tracking via RFID a very real possibility.

Existing Protection Methods for RFID Data

Once the security threats associated with RFID tags are outlined, it is necessary to examine countermeasures to safeguard the information stored on the tag and the privacy of the consumer. While it is true that a few of the above security scenarios are unlikely, reasoning based on statistical probability is not prudent in this instance. In other words, even if the consumer is wholly ignorant of RFID technology and the security threat is only perceived, there will still be a market for RFID security enhancement tools. As an

example, consider "spyware" software that has become a must-have for personal computers. Although the average consumer cannot explain the method of attack, or the realistic threat posed by spyware, security software generates almost 550 million dollars a year in corporate revenue.[8] The same logic can be applied to RFID tags, with the future proliferation of RFID technology leading to a similar market value.

To protect against unauthorized access to RFID data via the direct or inferred methods as well as unique ID location tracking, several methods currently exist. However, each of these pre-existing security measures has inherent drawbacks that make them unsuited for EPC-type RFID tags. To understand these limitations, the present RFID security methods are discussed briefly below. In essence, they can be separated into three categories based on the method of RF protection: physical interference devices, on-tag protocols, and off-tag security.

Physical interference devices function precisely as their name implies: they block RF energy from reaching the RFID tag. Because passive tags require this energy in order to function, physical interference effectively "pulls the plug" on RFID devices. The first, and simplest, example of this method is a faraday cage, a metal mesh or shell designed to absorb RF energy. The earliest use of this method dates back to World War II and the aforementioned IFF identification systems. During the war, pilots would dump "chaff", aluminum strips cut to one-half of the enemy's radar wavelength, from their aircraft, Figure 3.[6] These strips were designed to produce echoes on an enemy's radar system, simulating the presence of thousands of aircraft. For present-day RFID applications, chaff has been replaced by aluminum foil sheets placed in wallets, clothing, or shopping bags. This foil interferes with tag-reader communication, and is mostly

Figure 3: US Airman Preparing to Dispense Chaff

employed to spoof theft-detection devices. Although this method sounds far-fetched, it has already caught the attention of law enforcement officials. A 2001 Colorado law made it a misdemeanor to make or possess aluminum underwear![9]

Another popular physical interference method involves actively jamming the RF signals around the tag. This method is much more adaptive than a faraday cage approach, since the geometry of some RFID enabled items precludes them from being enclosed in a metal lining. Active RF jamming works on the same principals as cell phone signal jamming outlined in Figure 4.

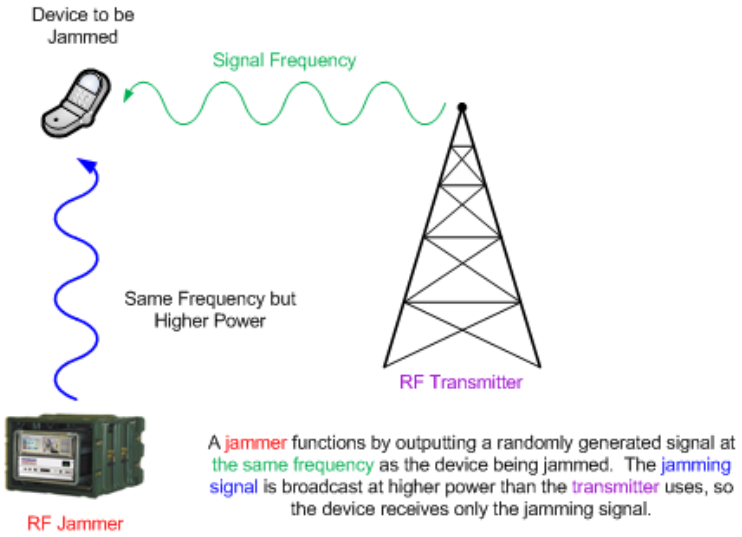

Figure 4: Explanation of Active Jamming of Radio Frequency Signals

Legality is the main issue with physical interference devices. For instance, active jamming of cell phone signals is currently illegal on the federal level, and active RF jamming is likely to follow.[10] As for personal faraday cages, they suffer from both questionable legality and utility. There are many high value items that would benefit from RFID theft detection devices (e.g. televisions, musical instruments, and computers) that can't be concealed beneath clothing or inside a metal cage. On a personal protection level, it is much more likely that a consumer would choose to buy items without RFID functionality instead of wrapping their clothing with chain link mesh. Additionally, from a retail standpoint, it is difficult to envision designer purses, wallets or jackets that come equipped with aluminum foil interiors. In the end, physical interference devices push the limits of convenience and of personal privacy; a person is entitled to block someone from reading their RFID tags on their own property but not necessarily in public and definitely not in a retail environment.

A second privacy protection method available for RFID tags involves security protocols directly integrated into the tag architecture. The most basic of these is the "kill-tag" functionality outlined in the EPC RFID standards.[1] The kill-tag feature destroys the tag by permanently deactivating it using a command sent from the reader. Once the kill flag on the tag is activated, the tag will no longer respond to reader queries. Typically, this command is an 8-bit string which protects the tag against unauthorized deactivation and theft.[11] While this method may seem ideal for preventing the security issues outlined previously, an item's tag could be deactivated once it is purchased for example, the kill tag approach has several serious limitations. The main reason that the kill-tag method doesn't work is that in most instances, it is desirable to have the tag remain active

after an item is purchased. Specifically, if an item is recalled by the manufacturer, or returned by the customer, it would be ideal for the manufacturer to be able to relate the unique product ID to the defective item. As a simple example of the adverse cost associated with a kill-tag security system, take the consumer-returned product industry. The National Retail Federation (NRF) estimates that 7.3% of all gifts purchased are eventually returned, resulting in a net returned value of 9.6 billion dollars a year.[12] If just 50% of the returned items were RFID kill-tag enabled, and each item had an average value of $25, then 192 million tags would have to be replaced following return. Assuming a cost of $0.10 per RFID tag, the cost of replacing all of the deactivated tag per year would be 19.2 million dollars, not including labor costs. It's clear that while the kill-tag method possesses the requisite functionality of an RFID security system, it is unlikely to be embraced by retailers who must either pay the cost of replacing tags, or pass the cost on to consumers. Kill-tag or other deactivation solutions are heavy-handed methods which limit the ingress of RFID technology into new retail applications.

On-tag data encryption is another example of security protocols incorporated into the tag architecture. Encryption enabled RFID devices, also called "smart tags", either have their data encoded (public-key cryptography), or transposed (hash-locking). In either case, data security is achieved by preventing an unauthorized party from reading the actual values of the information contained in the tag. Public-key cryptography, Figure 5, takes the tag data and a known public encryption function, or "key", as inputs. Decryption of the public-key secured data is then performed using a separate, private key. Because the encryption and decryption keys are different, this method is also called asymmetric cryptography. It is important to note that this method requires storage of the

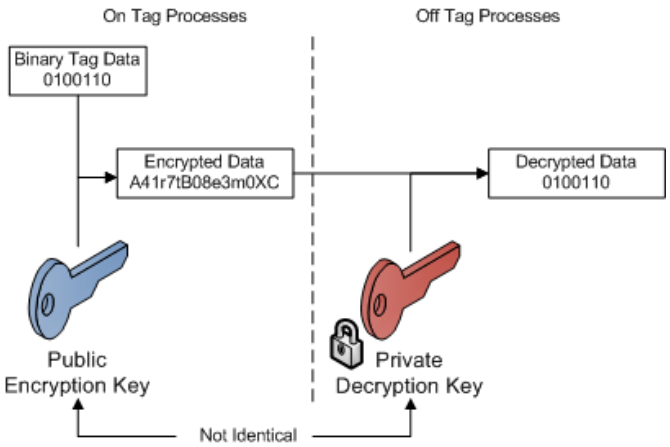

Figure 5: Schematic of Asymmetric Key Encryption

encrypted data as well as the related key. Because encryption increases the size of the data, the resultant memory requirements of an encryption enabled RFID tag are much greater than that of a standard ID only tag.

Hash functions, another on-tag data security method illustrated in Figure 6, take the data stored in the tag's memory and swap and transpose it according to shared algorithms. Hash-locking differs from cryptography in that the "key" is a known function or table, and thus hash-locking is not technically encryption; it is more accurately defined as data manipulation. One of the distinct advantages of using hash-locks instead of cryptography in RFID devices is that the locked value, denoted Ω in Figure 6, is actually smaller in size than the original data. However, this means that

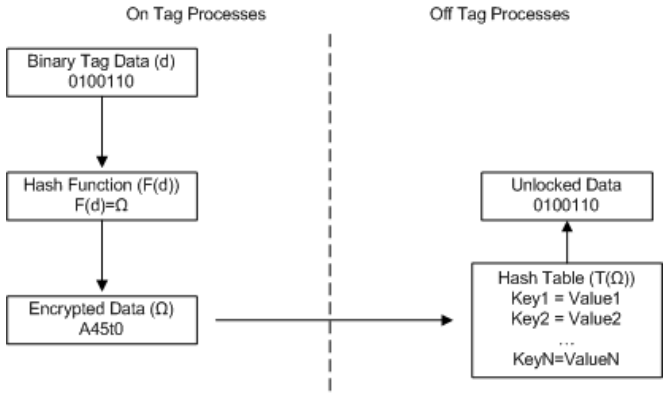

Figure 6: Schematic of Data Hash Locking

cryptography is much more secure than hash-locking, so it is difficult to find a compromise between security and memory requirements. The main problem with all on-tag security protocols is that they violate constraints on EPC-type tag memory, power, and cost. For asymmetric cryptography, the amount of memory required for the encrypted data and the decryption key would make the tags economically unfeasible. It is unrealistic to assume that a company would pay for the requisite tag memory increase (approximately a four-fold memory augmentation would be required for EPC tags); in order to protect their customer's shopping habits. In the case of hash-locking, the main cost incurred would result from the necessary addition of an unlock table, (T(Ω)) in Figure 6, incorporated into the RFID middleware or the third-party ID storage database. In addition, for mass-produced read-only tags, the encryption key or hash function stored in the tag's memory could never be updated. This means that if the security of a single tag was compromised, all tags with the same key would also be compromised. Because EPC tags on consumer goods change hands frequently, it would be relatively simple for someone to purchase a tagged item, decode the tag's key and then access all tags with the identical key.

The final possible security enhancement mechanism for EPC-type RFID tags involves protocols performed away from the tag. Passive, or selective, blocking systems are one example of such a system. It's important to note that in this instance, the term passive refers to the blocking or jamming mechanism, not the power requirements of the tag. For instance, an active RFID tag (i.e. powered by an internal battery) can perform passive blocking functions. The passive connotation refers to the fact that interference with an RF signal is only activated at select times, unlike the active RF jamming detailed in

Figure 4. Passive RFID blocking is preferable to the physical interference and on-tag security measures discussed above for several reasons: it is legal, the current EPC-type tags do not need to be modified, and the cost of the system is optional and incurred by the customer. In order to show how a passive RFID blocking system works, it's necessary to first explain the anti-collision and singulation algorithms used for tag-reader communication.

Anti-Collision and Singulation Algorithms

Because most readers possess a single antenna, they can only receive a response from one tag at any given time. If more than one tag responds to a reader query, then the reader is effectively overwhelmed and a "collision" occurs. In this case, a collision can be defined as the simultaneous response of two or more distinct tags at an instant in time. As a rudimentary metaphor for tag-reader collisions, consider a radio station that awards a prize to a listener who calls the station. The station (reader in this example), sends the prize message to all listeners (tags) within its broadcast range. Ideally, the listeners respond by calling with their name (transmitting their ID). However as anyone who has ever called a radio station knows, almost all of the time the caller receives a busy signal and never passes on their information, since the station has received more calls than it can handle. Collisions are obviously undesirable in RFID applications, and in the above radio station example, because they prevent the reader from communicating with the tag and accessing the data stored in the tag's memory. In order to prevent these collisions from occurring, RFID readers come equipped with singulation algorithms, designed to ensure that one tag at a time communicates with the reader. In the following section, two

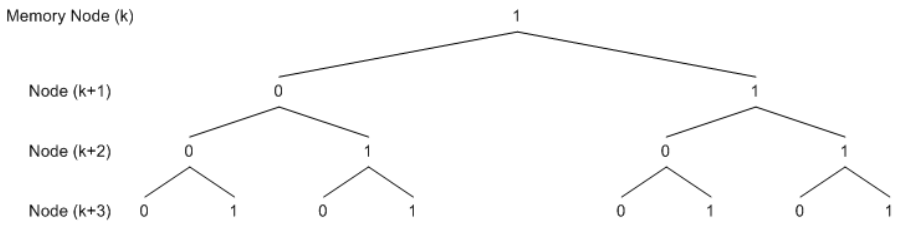

Figure 7: Binary Data Arranged in a "Binary Tree"

of the most popular singulation algorithms; tree-walking (for 900 MHz tags) and the ALOHA protocol (for 13.56 MHz tags) will be discussed.[11]

Tree-walking is a recursive algorithm which utilizes the unique properties of the binary strings stored in a tag's memory. The "tree" portion of the algorithm's name comes from representation of data in a binary tree, as shown in Figure 7. From the figure, it is evident that binary strings possess the following useful properties:

1) For a string with (n) bits, there are 2^n different combinations, each expressed as a "leaf" on the binary tree.
2) Each of these combinations can be expressed as the concatenation of the leaf with the branches on the tree above it (e.g. 1010 = 101 concatenated with 0).
3) Distinct strings can be separated into two segments; a segment common to both strings and a unique segment that is different for each. For example, in Figure 8, the strings 0100 and 0110 share the prefix branch "01" but subsequently diverge.

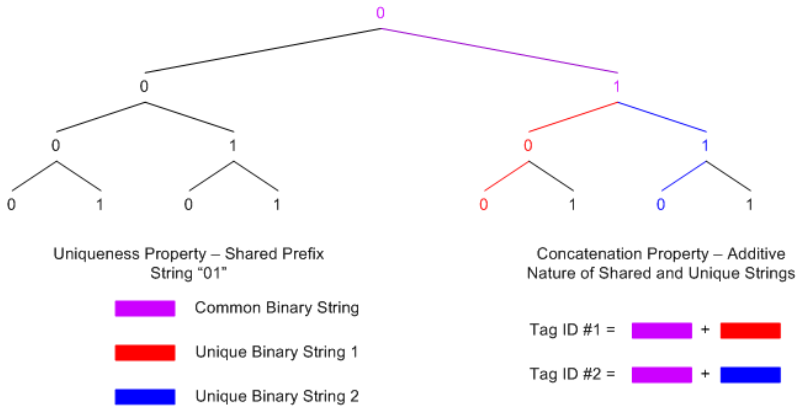

Figure 8: Example of Concatenation and Uniqueness of Binary Strings

Singulation via tree-walking works on the premise that there are three possible scenarios for tag response: a collision occurs, data is transmitted freely, or there is no response. If a reader detects a collision at node (k) of a binary tree, then tags must exist in both branches (k+1) of the binary tree. In this case, concatenation of the current string with both a 0 and a 1 must be explored. The reader subsequently recurses on each of the branches below the one at which a collision was detected and repeats the process. If the reader receives data from the tag without collision, then only one branch of the tree is populated and the non-populated branch is ignored. If the reader does not obtain a response then neither branch contains a tag and both branches are ignored. While the process appears tedious, in reality it is expedient for large memory systems in which a small number of tags are present, almost all of the branches are empty in these cases. In the converse scenario, this algorithm requires exceptional computational power if large numbers of the leaves are present, since almost every branch must be explored in this case, leading to 2^n number of transmissions. Figure 9 presents an example of how this algorithm works using three tags, each with 4 bit identification numbers.

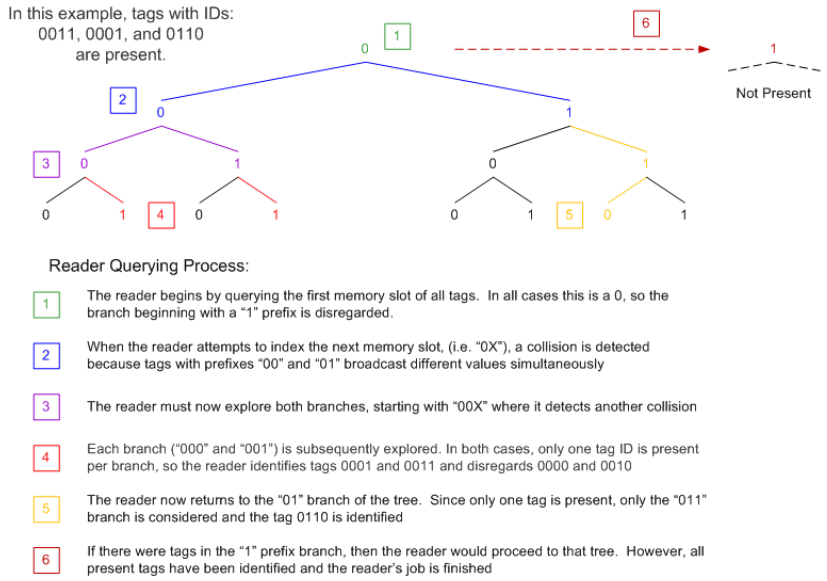

Figure 9: Binary Tree-Walking Example for 3 Tags with 4 Bit Memory

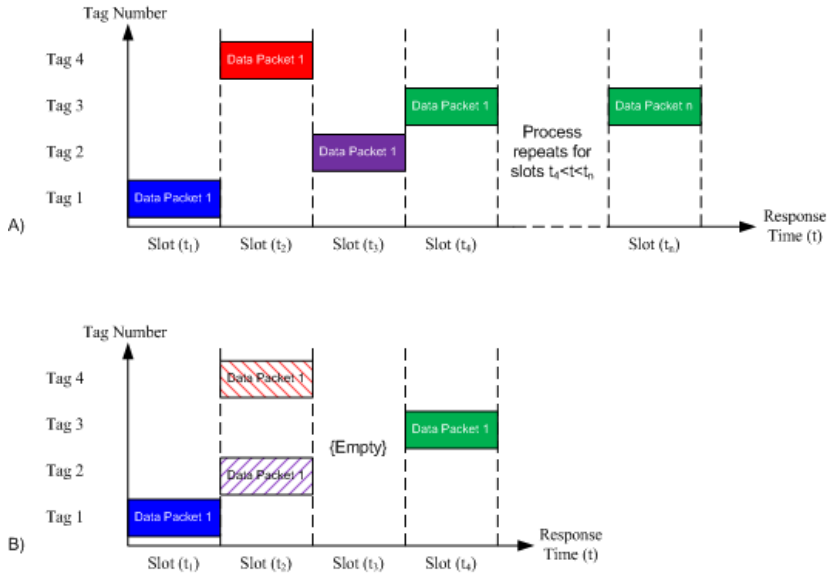

Figure 10: ALOHA Protocol Data Transfer Schematic for (a) Complete Transfer (b) Data Collision

The ALOHA protocol is a slightly different singulation method, which was originally designed to facilitate radio frequency communications between computer networks and is considered a precursor to the Ethernet protocol widely used in PCs today.[13] Unlike the tree-walking algorithm, the ALOHA protocol is not a bit-by-bit transmission method, tags send multi-bit "packets" of information to the reader at set transmission times. Essentially, ALOHA can be summarized with the following two rules:

1) If prompted, send the data packet at a pre-determined time (slot).

2) If a collision occurs, re-slot the packet and resend.

As it applies to RFID tag-reader communications, the ALOHA protocol works as shown in Figure 10. The reader sends each tag a specific return broadcast slot, the size of the data packet to send, and a continuation flag, which signals the position in the tag's memory at which the current data packet should come from. If the reader detects a collision, it can re-slot the particular tag. Because the data transmission rate is high, and the packet size is very low (on the order of bits), the slot times can be very small, which

allows the reader to query a large number of tags in a small amount of time. As with the tree-walking algorithm, the ALOHA protocol will require incredible computational resources if the number of tags is so large the re-slotting must occur constantly. In other words, the reader cannot handle multi-tasking, reading, and re-slotting over an extended period of time.

Employing Singulation Protocols in Blocking Systems

The main idea behind an off-tag RFID blocking system is that the singulation algorithms, and by extension the reader, can be overwhelmed if the number of tags is greater than a certain tolerance. In theory, the maximum number of unique tags that can be accessed scales exponentially with the memory size of the tag. In practice, however, the reader tolerance is much smaller than the theoretical limit because of computational limitations. Although this tolerance value depends on the reader type and the specific singulation protocol used, it is typically accepted to be on the order of thousands to ten thousands of individual tags.[11] Transferring this result to the binary domain, the maximum memory size of unique tags that can be identified if all possible tag combinations are present is between 10 and 13 bits. Therefore, assuming the minimum EPC data storage mandate (64 bits) and the maximum reader tolerance (13 bits), if the reader was overwhelmed, then the number of tag ID combinations that would not be read would be approximately 2250 trillion. In other words, if the reader can be manipulated into believing that it has been overwhelmed, then it will be unable to identify any of the tag IDs which are present. In the next section, a concise method for disrupting the tree-walking singulation algorithm is presented, and the same principals can be applied to the ALOHA protocol with several small differences as noted.

As previously discussed, the tree-walking singulation algorithm uses the presence or absence of collisions to determine which branches of the binary tree are populated. In the extreme case, if a collision was detected at the node of each branch of the tree, then by default, the maximum possible number of tag IDs (2^n) would be present, and the reader would be unable to read all of the IDs. From Figure 9, when the reader queries the tags within its range, they reply with the binary value stored in that particular position in their memory. Now, consider a tag which possesses and broadcasts both a 0 and a 1 at the memory location in question (the logistics of creating such a tag are discussed later in the design section). This tag would automatically force a collision since it would respond with both possible values. If this procedure is extended to all possible memory positions, the result would be a tag which is "super compliant", in other words it responds to all possible reader queries with both a 0 and a 1.[14]

To further explain the concept of super compliance, consider a tree-walking process which begins with the reader querying the tag's first memory slot (k=1). The tag sends a 0 and a 1 back to the reader, causing the reader to proceed to slot (k=2), starting with all tag IDs that begin with a 0. When the reader queries this next slot, the tag responds again with a 0 and a 1, telling the reader that tags are present with the following binary prefixes: "00", "01", and "1". This process is repeated as the reader recurses over the entire binary tree. It finds a collision at each memory slot and will eventually quit before exploring all of the possible ID space. Figure 11 displays a schematic of the first ten-thousand tags that would "appear" to be present. Obviously, this is only a microscopic subset of the possible IDs that the reader would be unable to check.

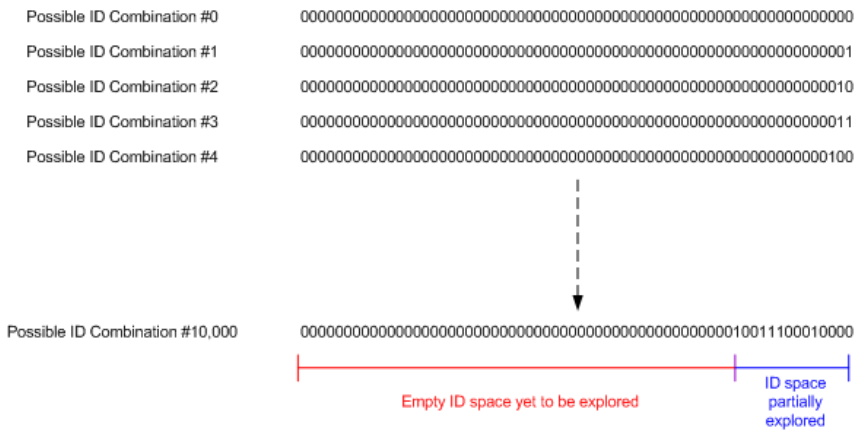

Figure 11: First 10,000 Possible ID Combinations Explored by the Tree-Walking Algorithm

Disrupting the ALOHA protocol works on the same dual transmission method; with the main difference being that only a single antenna is necessary (two antennae would be required to simultaneously broadcast a 0 and a 1 in the tree-walking case). For the ALOHA protocol, the super compliant tag utilizes any EPC-type tags which are present to function as secondary antennae and force a collision. When the reader sends out its slot allocations at the beginning of the querying process, the super compliant tag stores all of the slots and responds with an arbitrary packet of data at each of the assigned times, Figure 12. Because the present EPC tags each respond at their individual slot times, each response causes a collision between the EPC tag and the super compliant tag. The reader subsequently re-slots both tags and collisions will occur indefinitely until the reader is finally overwhelmed.

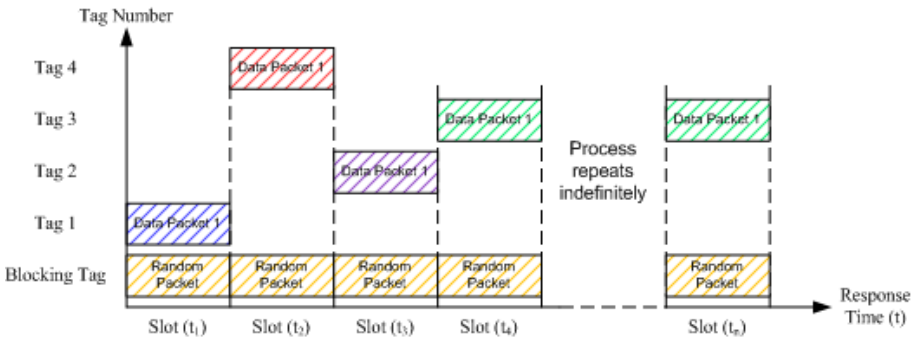

Figure 12: Blocking Diagram for the ALOHA Protocol

On its own, this concept of a super compliant tag is not very useful. Although such a tag could disrupt the reader singulation algorithms, its utility is limited unless an actual EPC-type ID only tag is present. If a super compliant tag and an EPC tag are within the reader broadcast range, then the super compliant tag acts as a "mask" for the EPC tag, effectively blocking it from view of the reader. Considering the tree-walking algorithm, if the EPC tag ID was within the subset of IDs that appear before the reader is overwhelmed (the blue area in Figure 11), there would be no way for the reader to determine if the tag was actually present or just one of the possible ID permutations presented by the super compliant tag. On the other hand, if the tag ID was in the much larger subset of tag IDs that are unable to be read, then it is "invisible", because the reader is unable to explore that particular branch of the binary tree. The same unexplored subset principal applies for the ALOHA protocol, the reader is unable to verify the existence of any tag in the presence of a super compliant tag because it always detects a collision. In all cases, the reader is unable to distinguish between the real EPC tag IDs that are present and the fictitious IDs presented by the super compliant tag, thus the identity of the EPC tag is effectively blocked from the view of the reader.

RFID Blocking System Design and Application

To deploy the singulation disruption algorithms discussed previously, an active RFID tag is required. The main technical reason for using an active RFID method is that a standard passive tag is not capable of rapidly altering its ID or storing multiple slot times, requirements for disrupting the tree-walking and ALOHA protocols respectively. Incorporating this functionality into a passive tag would greatly increase its cost and complexity, since current passive tag standards do not contain the requisite memory or

power. However, a blocking system which consists only of a single active tag would be impractical for a consumer to carry around at all times. An elegant solution to these problems would be to integrate the active blocking tag into a personal digital assistant (PDA). Because a significant amount of people carry PDAs or other battery powered devices, it makes sense to integrate the blocking platform as an add-on to these systems.[16-19]

As far as the tag itself is concerned, its design is mainly governed by the disruption algorithm constraints and not by power or memory restrictions, since these can be "farmed out" to the PDA. Because an active tag draws its power from an attached battery, in this case the PDA's internal power supply, it is capable of performing the more rigorous computational requirements of the disruption algorithms without needing a large battery of its own. In addition, the advanced storage capabilities and fast processor speed of the PDA are employed by the active tag, which cuts down on the size and cost of the blocker system. Finally, if the tag is to block both the tree-walking algorithm and the ALOHA protocol, it needs three separate antennae:

1) To broadcast binary value 0 at 900 MHz
2) To broadcast binary value 1 at 900 MHz
3) To continuously broadcast data packets at 13.56 MHz over a short time period

To activate the blocking system, the user positions the PDA close to the tag which is to be blocked, as shown in Figure 13. Since an active tag can broadcast as well as receive, the system broadcasts a signal to the tag at both 13.56 MHz and 900 MHz to determine the tag type. For the 13.56 MHz tag, the blocker remains inactive until the tag is queried by a reader. When the reader sends out the time response slots, the blocker

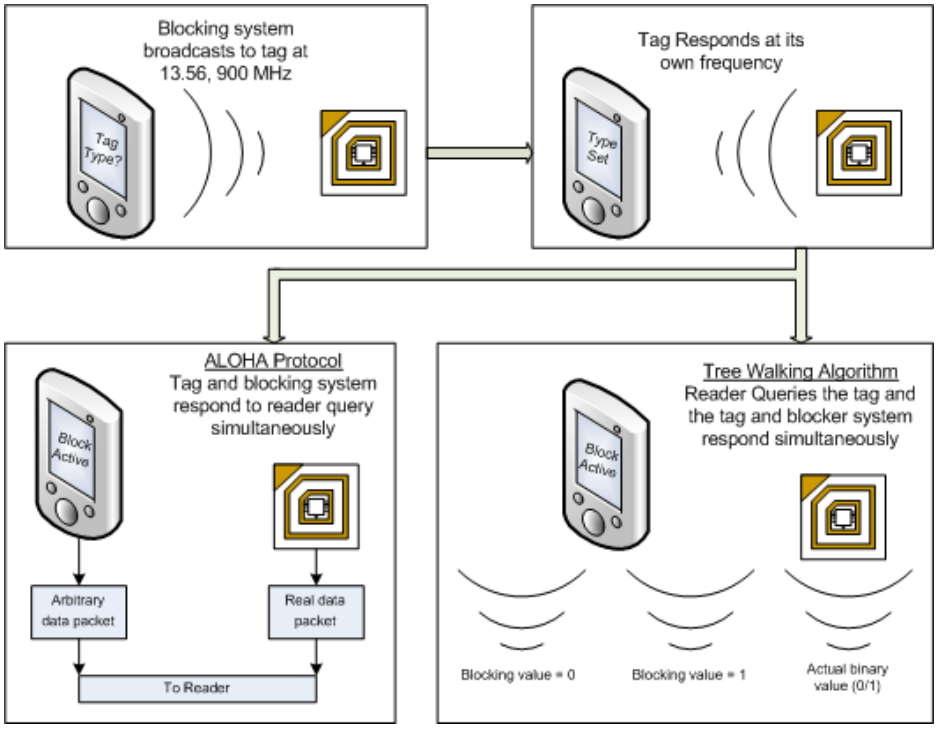

Figure 13: User Application of a PDA-Based Blocking System

stores each slot in the shared memory and responds by sending an arbitrary data packet at every time value. This process is repeated until the reader ceases to allocate time slots, signifying that the tag is out of the reader's broadcast range. For the 900 MHz tags, the process is much simpler. The blocker system responds to each reader query by simultaneously broadcasting from both antennae. When the system no longer receives any queries, it has either overwhelmed the reader or is out of range. In either case, the system goes into sleep mode until it detects another reader.

In addition to outsourcing the power and memory requirements, another advantage of combining the active tag and PDA systems is that it enables the PDA to log all of the times that a tag has been queried. This auditing process is very similar to that employed by a firewall, with the main difference being that the RFID auditing procedure does not perform any reader authentication or authorization.[18] In other words, the system is able

to discern when it has been scanned by a reader, but not if that reader was authorized to perform the scan. This limitation is due to EPC tag standards, which do not require authentication from the reader.[1] However, auditing is still a useful feature which can be used to identify the locations of RFID readers and protect against location tracking.

The utility of the active blocking system can be further enhanced by using the concept of privacy zones.[16] From Figure 2, it is clear that there is a certain amount of data contained in the tag that does not pose a privacy threat to the consumer (i.e. the tag manufacturer identification number). However, information such as the product ID and the unique serial number should be kept private, to prevent unauthorized snooping and tracking, respectively. Therefore, the data on the tag can be classified into two zones; public and private, based on the user's preference. When the reader queries memory locations in the public zone, the blocker system does not respond, which allows the reader to gather a limited amount of information. Once the reader crosses into memory slots in the private zone, then the blocking system deploys its singulation disruption algorithms and the reader is unable to identify the tag data, Figure 14. The privacy zone method is a powerful tool that provides flexibility to the user by allowing the tag to retain some functionality while protecting personal information. With a PDA interface,

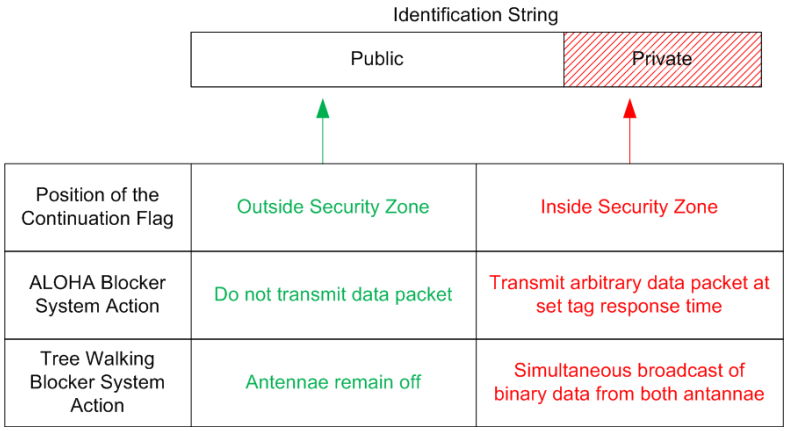

Figure 14: Privacy Zone Concept for Tree-Walking and ALOHA Algorithms

managing and storing the privacy zones for various tags is relatively simple if it is implemented in the user interface.

From a practical standpoint, a PDA-based active RFID system controlled by the consumer makes much more sense than any passive security methods. Because the consumer purchases and manages the hardware, the manufacturer incurs no extra cost for tag encryption or security, which is not the case for security protocols involving passive tags. Additionally, an active blocking system introduced at the point-of-sale does not impact existing EPC standards or RFID functions such as, supply chain management, inventory control, and self-checkout, Figure 15. As a result, a consumer supported blocking system does not impact the manufacturer in any way, apart from slight modifications required for RFID theft detection discussed in the next section.

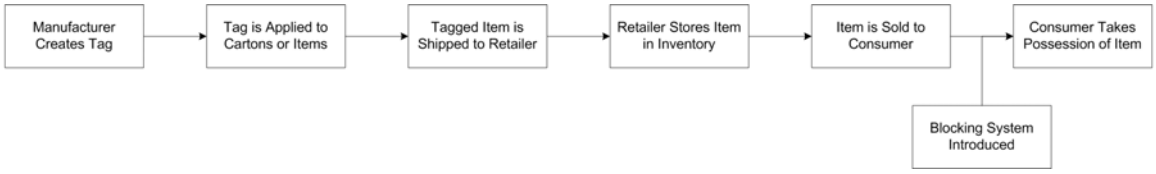

Figure 15: Incorporation of a Consumer Blocking System in the RFID Supply Chain Process

In addition to the benefits to the manufacturer and retailer, from the consumer's standpoint there are multiple advantages to an active tag based blocking system. The most important aspect to point out is that this blocking system is optional. Whether or not a person elected to pay for the blocker, they would still be privy to the convenience of a retail RFID system. Additionally, because the blocking system uses an active tag and is incorporated into a PDA, the system has a large amount of memory and power which allows for a high degree of flexibility. The user could set their preferences anywhere from the most obtrusive security setting, all privacy zones blocked on all tags, to the most

benign setting, auditing and logging all reader queries. Finally, because the tag does not actively block RF signals, its legality would not be an issue.

Reader-Based Detection of Malicious Blocking Systems

For all of the possible privacy benefits of a PDA based active RFID blocking system, it is easy to image the same device used to abuse theft detection or inventory management systems. As an example, consider a situation in which a retailer prevents items from being stolen by changing a preset bit in the tag's memory from a 0 to a 1 upon checkout. When a customer walks out of the store, an RFID reader at the exit scans all of the tags on the customer and checks the tag IDs for the specific "purchase bit". If a thief went into the store equipped with a PDA, they could easily read the RFID enabled item using the blocker system, hide the item on their person, and then use the blocking method to shield the item from the theft detection device. Malicious or illegal usage of the RFID blocking system would significantly impact its utility, since items which can be used for both licit and illicit purposes are often tightly controlled (e.g. cold medicine used for methamphetamines, spray paint used for vandalism). In other words, the most effective and well-designed blocking system would be useless if there were no means of detecting its presence. In the next section, two different methods for identifying the presence of a tree-walking algorithm type blocking system are introduced: the maximum population method and the differential signal analysis (DSA) method. The same systems could be applied to an ALOHA protocol case with minor modifications which are not included for brevity. Both the maximum population and DSA methods are capable of detecting the blocking system, but are incapable of accessing the tag contents, which keeps the blocking system effective and legal.

The first possible malicious blocking system deterrent, the maximum population method, involves setting a theoretical limit on the number of tags that would be practically read by the reader over a set period of time. As previously mentioned, blocking systems function by simulating a much larger number of tags than could actually be contained in a store, much less carried by a single person. For example, if the privacy zone of a blocker system was 24 bits, then the reader would register the presence of approximately 16.8 million tags. Because this value is far larger than the typical number of tags processed by a theft detection system, it can be used as a flag to identify if a blocking system is being used, Figure 16. In practice, at the theft detection site, the reader or its middleware would contain a preset tolerance value, corresponding to the maximum number of tags present at any time. If the reader registers a tag population greater then the tolerance, then the theft detection alarm would be sounded. It is important to note that this method does not interfere with the legal usage of an RFID blocking system. If the customer chooses to activate the blocker inside the store, then

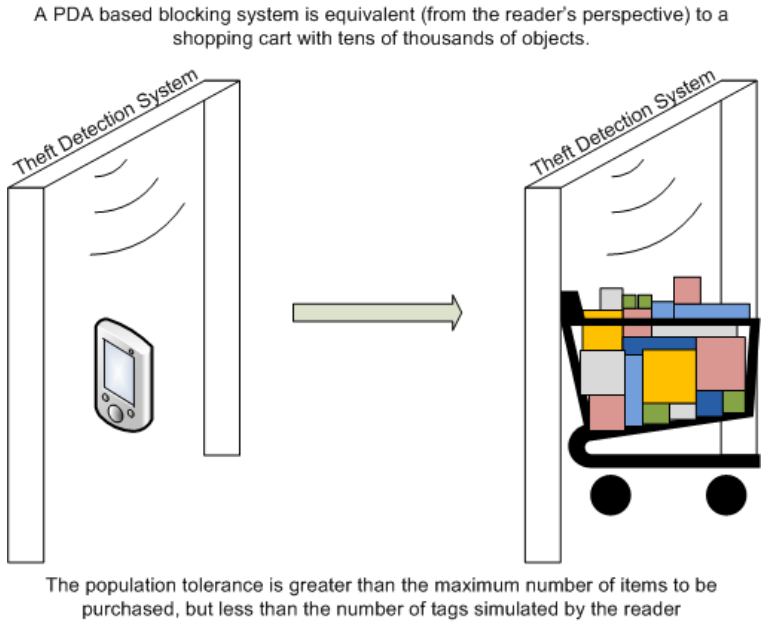

Figure 16: The Maximum Population Method for Detecting Blocking Systems

they would simply need to keep their receipt to prove that they purchased all of the items in their possession. A far more likely scenario is that the customer activates the blocking system outside the store, which would not interfere with the theft detection system at all.

Differential signal analysis is a second possible method of detecting a malicious RFID blocking device.[15] The main assumption with DSA is that for the majority of the querying process, the blocker tag is the only one communicating with the reader. In other words, if a blocking system is designed to protect a privacy zone of 16 bits, and two actual 64 bit EPC-type tags are present, the reader would be forced to check 65,536 nodes of the binary tree. However, the EPC tags would only respond at 0.026% to 0.049% of these nodes, depending on the tag ID numbers. DSA involves recording the analog signals returned from the querying process and performing a statistical analysis on their resulting amplitudes. In this case, there are two important values; the amplitude average and the amplitude mode. The average is the summation of all amplitudes divided by the sample size, while the mode is the most commonly occurring value. If a blocking system is not present, then the signal average and mode will not be similar, since each EPC tag would respond in a unique fashion. However, if a blocking system were being used, then the vast majority of responses would come from the blocking system only. In this case, the mode would obviously be equal to the blocking system amplitude, and the average would be almost identical to the mode, since the responses from the EPC tags would be statistically insignificant compared to the blocking system responses. Figure 17 shows how the DSA process would look for two EPC tags and a security zone of 4 bits. Like the maximum population method, DSA employs the fact that the actual number of tags to

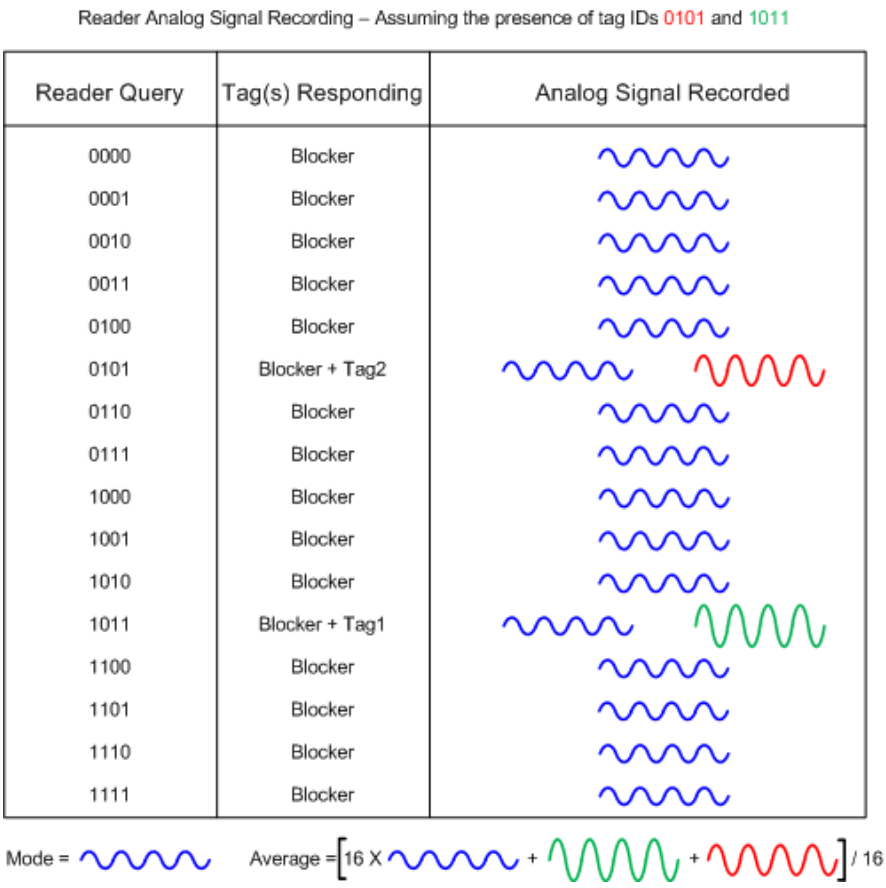

Figure 17: DSA Analog Signal Response for Two EPC Tags and a 4 Bit Privacy Zone

be queried by the reader is much smaller than the number simulated by the blocking system. However, DSA is a much more robust analytical tool which makes it more suited for implementation in RFID readers or middleware.

Conclusion

The utility of EPC-type RFID tags in supply chain, retail, and consumer industries have lead to their implementation in a wide variety of applications. As the cost of individual tags continues to drop, it is evident that RFID devices will make ingress into new markets and functions. However, the cost, power requirements, and available memory of such tags make them incredibly susceptible to information security attacks. In particular, for EPC-type tags, unauthorized data access, inferred identification and

location tracking via unique ID are of particular concern. The methods currently available to prevent these security threats suffer from either a lack of practicality or utility. Physical interference devices run the risk of being illegal, and on-tag security protocols often exceed tag power, cost, or memory requirements. Because a large market exists for personal information security protection devices, an off-tag security device has considerable promise. The PDA-based device discussed in this paper functions by disrupting the anti-collision algorithms employed by 900 and 13.56 MHz RFID readers. This disruption either masks the presence of the tag in question by simulating a large number of non-existent tags simultaneously, or confuses the reader and prevents the tag from ever being accessed. Additional functionality like flexible security zones and reader query auditing improve the utility of this system. However, because such a device could easily be used maliciously to defeat RFID theft detection systems, two minor reader modification strategies were discussed to detect nefarious usage of RFID blocking. Either the maximum population method or the differential signal analysis approach could be integrated into current generation readers and would prevent theft concerns without impacting the effectiveness of the PDA-based blocking system or requiring changes to the current EPC standards.

Works Cited

1. Auto-ID Center. (2002, November 14). 860MHz–930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1. Technical Report
2. Girion, L. (2007, November 9). Health Insurer Tied Bonuses to Dropping Sick Policy Holders. *The Los Angeles Times*, pp. A1
3. BBC News Service. (2003, February 18). *Credit Card Database Hacked*. http://news.bbc.co.uk/1/hi/business/2774477.stm
4. Consumer Affairs. (2006, December 12). *Massive Data Breach at UCLA Endangers 800,000*. http://www.consumeraffairs.com/news04/2006/12/ucla_data.html
5. MSNBC News Service. (2007, March 30). *TJ Maxx Theft Believed Largest Hack Ever*. http://www.msnbc.msn.com/id/17871485/
6. Rieback, R., Crispo, B., and Tanenbaum, A. S. (2006). The Evolution of RFID Security. *IEEE Journal of Pervasive Computing*, 5 (1), 62-69.
7. W. Mahurin (Speaker). (1997). Interview with Col. Walker 'Bud' Mahurin. http://www.acepilots.com/korea_mahurin.html
8. The Radcati Technology Market Research Group (2005). Corporate Anti-Spyware Market 2005-2009. Private Market Research Study.
9. *Amendment to the Colorado Revised Statutes: House Bill 01-1221*. Statue Section 1, 18-4-407. Approved May 18, 2001.
10. *Amended Communications Act of 1934*. 47 U.S.C Sections 301, 302a, and 333.
11. Juels, A., Rivest, R. L., and Szydlo, M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. *Proceedings of the 10th ACM Conference on Computer and Communications Security*. 101-113.
12. The National Retail Federation (2007). 2007 Holiday Survival Kit. Press Release.
13. Layer Networks. (2007, November 21). *The ALOHA Protocol*. http://www.laynetworks.com/ALOHA%20PROTOCOL.htm
14. Juels, A. and Brainard, J. (2004). Soft Blocking: Flexible Blocker Tags on the Cheap. *Workshop on Privacy in the Electronic Society (WPES)*. 1-7.

15. Rieback, R., Crispo, B., and Tanenbaum, A. S. (2005). Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags. *13th International Workshop on Security Protocols*. 1-6
16. Juels, A., Pappu, R., and Garfinkel, S. (2005). RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Journal of Security and Privacy*, 3 (3), 34-43.
17. Grossman, W. (2007, July). Jam Session: A Design to Block RFID Tags. *Scientific American*, 26.
18. Rieback, R., Crispo, B., and Tanenbaum, A. S. (2005). RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. *10th Australasian Conference on Information Security and Privacy*. 184-194.
19. Reade, W., Ellingson, D. L., and Lindsay, J. US Patent No. 7,221,900 B2, 2007.