[[1]](#footnote-1)

State of RFID Security

Robin T. Kimzey and George F. Mudrak

*Abstract*— While Radio Frequency Identification (RFID) technology has been in use since 1935, the technology continues to advance at an increasing pace as manufacturing techniques, process and materials improve, yielding greater options at reduced costs. With manufacturing and costs improving, RFID device acceptance and adoption continues forward at an impressive pace. RFID adoption is occurring in nearly all segments of the consumer market and product deliver chain as well as military and financial applications. While some applications are benevolent, a significant lack of understanding regarding current security measures exists. This incredible proliferation of RFID devices is on par with embedded systems which has been shown to have significant risk associations [1] and therefore must require that RFID devices be secure. This paper explores the recent state of RFID Security in light of increased adoption across a spectrum of industries.

*Index Terms*—RFID, embedded security, radio frequency identification, RFID security.

# INTRODUCTION

R

FID or Radio Frequency Identification, traces its roots to the original pre-World War II, radar systems discovered by Sir Robert Alexander Watson-Watt [2]. Radio signals were sent out and incoming aircraft would bounce those signals back to the broadcast antenna. The technology was effective at acknowledging that aircraft were incoming, however, ineffective at discriminating between friend or foe.

 Subsequent work by Sir Robert Alexander Watson-Watt led to the creation of a new transmitter that when it received a signal from ground radar stations, would begin to broadcast a signal that would identify the plane as friendly. [3] This simple act of being able to identify a specific target and query it for information (friend or foe?) provided the foundation for the coming RFID market. RFID technology was about to receive to additional milestones for its acceptance.

 As innovations continued through the coming decades, two significant RFID milestones were achieved in 1973. The first was the patenting of an RFID tag with re-writable memory by Mario W. Cardullo. This now provided capabilities for tags to updated and changed through use and processes. A significant improvement over tags that contained WORM (write-once, read-many) memory. The second milestone occurred that same year when Charles Walton received a patent for a passive transponder to unlock a door without a key. This breakthrough demonstrated another capability, aside from holding data, that RFID tags could be used to provided "keys" to affect their physical environment.

 While over these years RFID technology has continued to advance, the core operational read process remains the same. An antenna is used to broadcast a "send" signal to local RFID tags. Any tag that receives the signal will power-up and broadcast its information back. Once the antenna receives the RFID information, it passes on to a transceiver for decoding then to a computer for processing. The read-write process functions exactly the same as the read process with the additional steps that information would be returned from the computer, through the transceiver and broadcast out by the antenna to the RFID tag, at which point the new data would be written.

**Figure 1**: The standard read-write operation pattern for an RFID tag. The read-only process operates the same, just no return trip back to the tag as indicated by the bi-directional arrows.

RFID tags and their antennas operate in one of four radio frequency ranges.

|  |  |  |
| --- | --- | --- |
| **Frequency Name** | **Low End** | **High End** |
| Low Frequency (LF) | 50 KHz | 500 KHz |
| High Frequency (HF) | 13.56 MHz | -- |
| Ultra High Frequency (UHF) | 860 MHz | 960 MHz |
| Microwave | 0.9 GHz | 2.5 GHz |

**Table 1**: Industry standard operating frequency ranges for RFID devices.

These operating frequencies translate into operating ranges in the physical world for the maximum distances over which the RFID tag can receive and successfully broadcast its signals. Devices operate from a few inches to an optimistic maximum range of 100 yards, or 300 feet. Costs increase as the need for greater range come into play because to effectively increase the RFID tags range, the device needs to use a higher broadcast frequency and greater power to achieve the distances. These factors increase costs and so low ranges devices are significantly more common.

 Modern RFID tags are classified into one of three categories based on their power demands and broadcasting requirements. Passive, Semi-Passive and Active tags will be found in use to varying degrees depending on the tracking needs.

 Passive RFID tags constitute the majority of tags that consumers have been exposed to as they exist in all phases of a product delivery and retail chain. These tags are quite a bit cheaper than Semi-Passive and Active tags as they do not use an independent on-board power supply in order to function. Instead, they utilize the radio frequencies broadcast to them in combination with their own antenna to create an electro-magnetic field that charges the circuit for a temporary and short duration. The duration is long enough to broadcast their data to any listener.

 Semi-Passive tags contains internal batteries used to power their integrated circuits. However, this power supply does not power the broadcasting of the data. Similar to the Passive RFID tag, a Semi-Passive tag requires the presence and power input of an RFID tag reader in order to power its broadcast of stored data.

 An Active RFID tag contains its own internal battery that powers both the internal integrated circuit and the tags broadcasting of stored data. By being broadcast self-powered, Active RFID tags can achieve a greater broadcast range by a factor of 10x over comparable Passive and Semi-Passive tags. Additionally, by not requiring a reader to power the broadcast unit, Active tags play a significant roles in mobile tracking uses.

 In the Passive and Semi-Passive RFID tags, they will only broadcast their data upon request, while in contrast the Active RFID tag can broadcast its signal continuously, until its on-board battery is drained.

 Any of the RFID tag types can operate in any of the current four frequencies defined above, with the choice of tag depending significantly on the desired read distance.

 For the storage and persistence of the data that RFID tags track there are several memory operation types and a preferred physical memory solution. The supported memory operations follow standard computing operations today in providing Read-Only, Read-Write and WORM modes of operation. Read-Only functions as the name states. After the necessary data has been written to the RFID tag, the tag is "locked" to prevent further writes from taking place. With Read-Write operation, the core part of the RFID tag is "locked" after being initialized and an additional section of storage remains available for subsequent reads and writes from a tag reader. The WORM, or Write-Once, Reader-Many, functions in same fashion as the standard CD / DVD burner found in today's personal computer. After the tag is initialized and that portion of the tag data "locked" remaining sections of memory are available for subsequent writes. The principle difference in these operations versus the Read-Write operations is that on WORM memory, once a write occurs, you cannot write back over that section of memory. Each type of memory operation offers advantages and disadvantages to use that mirror the common usages in the personal computer domain.

 Given the very low and time-sensitive power available to RFID devices, the type of physical memory must meet very specific operational requirements. FeRAM or FRAM refers to FerroElectric Random Access Memory and remains the memory of choice for RFID tags based on the following criteria[4]:

|  |
| --- |
| **Desirable Characteristics of FRAMs** |
| Low power needs | Non-volatile |
| High write speeds | Stable without power |
| Long lasting (multiple writes) |  |

**Table 2**: These characteristics set FRAM apart from standard and flash based memory solutions. While more expensive than conventional memory to produce, the advantages out weight the costs.

 As with all memory types in use, capacity of RFID tags varies significantly and remains driven by intended usage. On the low-end you could have as little as 20 bits of memory, with 128 bits being typical of Class 1 Generation 1 tags [5] up to an incredibly impressive 128 Mbit (16M bytes) with a cell size of 0.252 µm*2* [6]. This represents an amazing amount of data packed into an amazingly small space to fit within an RFID tag.

 As with the operating frequencies, the type and amount of memory used by an RFID device will be dictated by the desired goal(s) the RFID tag is intended to meet.

 Given the above characteristics, plus easily usable scale coupled to low costs, we can begin to see why RFID devices have made such an amazing impact on all facets of our modern world. Everything available short of the molecular level, can be RFID tagged. You will find tags in your clothing, in your tools, in your pets, in your car, in books, in video game packaging, in your work ID badges, in your passport, in your driver's license, in your quick pay credit-card cards, in health equipment, in your money, in people, in military war equipment, in boxes, in containers of all shapes, sizes and densities.

 RFID tags are small, everywhere and they carry data with them. Sometimes nonsensical data and sometimes identify critical data. Data that we would not want openly broadcast or unencrypted. Your personal SSN, your bank account information, your medical history. All information we want secure.

 And herein lies our problem. RFID tags are inherently insecure and vulnerable to compromise. And the problem becomes worse as the incredible increase in RFID tag usage continues growing.

# The Problem

While use of RFID tags remains highly controversial, manufacturers and inventory control systems make extensive use of them. While originally used to track high cost items in inventories, with the decreasing costs of manufacturing RFID tags, they are now used everywhere.

## Physical Size

Modern RFID tags can be smaller than a grain of sand [7] and thereby become viable unencumbered tracking and data storage systems. This makes RFID tags extremely difficult to detect from a physical, visual scan. Figure 2 provides an illustration with a human finger used as reference to indicate production size of this Passive RFID tag.



**Figure 2**: World's smallest RFID tag measures a measly 0.05 x 0.05 millimeters!

Tags of this size can be placed anywhere to provide tracking. For example, you could place a tag of this size on a monetary instrument such as a $20 dollar bill without anyone noticing or affecting the use of the bill. Some current discussion on the internet concern the placement of such small RFID tags in the foods we consume at restaurants and scanning the contents of a patrons stomach to determine how much to charge them, as they exist the restaurant.

## Highly Connected Systems

Current operational procedure for RFID devices puts them in the highly connected category for interaction with other devices. With the current classification of mobile embedded devices as being, Isolated, Semi-Isolated and Highly Connected [8] we can determine an implicit level of security based on connectivity from these categories.

RFID tags cannot be categorized as Isolated devices as by definition this goes against the inherent connected and available-to-connect, state that RFID tags operate in.

RFID tags could be classified as a Semi-Isolated device. Semi-Isolated devices have connectivity on a on/off basis that is not consistently on. The security advantaged to this is that a device can be removed from availability periodically making it harder to identify and compromise as attacks take time. In the case of an RFID tag, the Passive and Semi-Passive tags functionally operate in a Semi-Isolated mode as they will only broadcast when requested.

The final classification of Highly Connected refers to devices that maintain a constant connection. Active RFID devices fall into this category in terms of their self-powered state and always-broadcast nature. We state that Passive and Semi-Passive tags should also be classified as Highly Connected as no barrier exists when these types of tags have power. From Figure 1, we see that these two types of tags will broadcast upon request and power up. There are no checks to determine if the broadcast should occur, it simply occurs into the open public space. As such and given their 100% availability when powered, we consider them to be Highly Connected Systems with all of the inherent security risk that Highly Connected devices must account for. RFID devices do not take minimal security into account let alone the security rigors required.

## Physical Security

Physical security of the RFID tag itself represents a significant issue. RFID tags are typically placed on the product of interest, where the tags are physically accessible. In the security world, a foundational tenant of preventing physical access must be met. In the RFID tag world, this concept exists only as a convenience when packaging permits. This leads to compromise of the tag as both a security and tracking device. The tag itself can now be easily accessed, damaged, removed, and/or even just moved. This is certainly not an issue when the tag is tracking a package of gum, however this becomes an issue when the tag begins tracking items of greater value. With security systems today relying on a tag being present, the lack of a tag increases the probability of a successful theft.

Furthermore, as memory storage increases on tags and becomes cheaper, expect tags to begin storing more information that may be compromised via simple removal of a tag for data mining purposes. For example, a product is sold by a retailer to Person A. Person A's activation information is stored in the tag on the product. After a period of time, Person A decides to sell the product on the secondary market to Person B. Person B's activation information is stored in the tag as well. At such point in time, the physical tag is removed from the newly stolen device and the thief has the activation information for all prior owners of the device, simply because the data is stored in the tag.

## Digital Security

While the physical security represents a significant barrier for RFID tags to overcome, digital security will become the barrier of tomorrow as FeRAM capacities continue to increase past today's 128 Mbit capacities and industry uses push the tags to the limit of both what they can store and in how to track them.

When we consider that RFID technology was originally developed to identify and incoming plane via radio frequencies in radar systems, we can begin to picture that something as simple as that may not represent the idea medium for transmission of sensitive information without the proper encryption (as done with today's WiFi networks). The technical difficulty associated with the proper digital securing of data via any form of encryption remains the computation power necessary for the encryption to take place. RFID tags represent a simple device with some local memory for data storage and an antenna to activate the device to broadcast the stored data. They do not have the computational power necessary today to perform the necessary encryption and decryption of data on board. While this dilemma can be solved by pre-encrypting the data prior to RFID storage, it no longer becomes a flexible device that any reader can access requiring manufacturers to provide cipher keys to their readers and thus increasing costs. As such, manufacturers are not quickly adopting a pre-encryption scheme.

Further, RFID tags themselves currently do not distinguish between specific readers. Therefore any reader available becomes a potential capture host for broadcast data and by nature of how the devices operate, any reader can become a power source for RFID tags. The difficulty with this RFID promiscuity means that an RFID tag cannot be expected to remain faithful to a particular reader or family of readers. And as an RFID tag cannot perform decryption, readers cannot uniquely identify themselves with an encrypted "broadcast" request.

Unintentional broadcasts can occur if an appropriate radio signal at the frequency of the RFID tag is being broadcast by any device - it does not have to be an RFID reader. In these cases, the stray RF signals will still power up the RFID for broadcasting its data to whomever is present. This represents a deeper concern with RFID tags in that the tag owner / user has no knowledge that their RFID tag is powering up and broadcasting their data to any listeners in the area. It is possible for someone sitting in a coffee shop to have a concealed RFID tag reader that sends out the appropriate RF signals as patrons walk past, and captures the responding broadcast data from the RFID tag. All occurring in the few seconds it takes to walk past the criminal and without the tag owner / user ever knowing their tag has broadcast their information.

RFID tags were not originally designed to securely store or transmit their data and this becomes essential when a technology becomes as mainstream as RFID technology is becoming.

# Scope of the Problem

The scope of the problems remains hard to quantify in terms of identifying the number of RFID tags currently "in the wild" as no concrete worldwide production numbers exist. We can however, get a small handle on the scope by simply projecting within certain industry segments. In 1996, 74 million units sold and in 2009 273.5 million units of video games within the industry were sold [9], with each packaged video game having one associated RFID tag. We can simply project growth for the next 5 years at a reasonable 10% in the number of units sold each subsequent year.

**Figure 3**: Simple RFID project for the number of units sold in the gaming industry projected at a 10% growth rate per year.

This simple projection yields approximately 500 million RFID tags for this one industry. Let us next examine the automotive industry. Approximately 16.5 million cars are sold within just the United States alone each year. If we conservatively assume each car/truck has 1 thousand parts we are interested in tracking with an RFID tag, then approximately 16.5 billion RFID tags exist to track these parts. If we follow a simple project from 2010 through 2015 then we end up with approximately 99 billion RFID tags used to track the parts within 99 million vehicles. Take the sum of these two industries and you have 99.5 billion tags by the end of 2015. In essence, you have a minimum of 331 tags per person in the United States! And this is just tracking two domains.

**Figure 4**: Simple projection of RFID tag usage of 16.5 million vehicles sold per year in the US, tracking 1thousand tags per vehicle.

With this level of penetration into a given population, it remains logical that this acceptance plus the increasing power and storage of RFID devices will yield more sensitive uses across an even broader market. The medical industry now utilizes RFID tags to track equipment and even patients. VeriChip Corporation provides RFID solutions for various financial and medical needs of people.[10] The VeriChip as used for medical purposes within people works by implanting an RFID tag into the body of a person. This tag has a unique identification number that any reader can receive from a scan. This identification tag can then be used to access the VeriChip website to access the medical records of the person with the embedded chip. The intended purpose is to provide emergency response personal a method of identifying the medical needs and constraints of an unresponsive individual. This is a good cause but a significant amount of medical information behind a "thin-veil" that does not hold up to protecting the privacy of the individual. This has already been demonstrated with a successful compromise of a VeriChip RFID tag [11]. Within a matter of seconds a hacker was able to retrieve the RFID unique identifier from an embedded VeriChip and impersonate the victim.

# Current Solutions

There are currently no on tag technological solutions in place to prevent the abuse and misuse of RFID tags, readers and broadcasters. Some solutions have been proposed but we feel they are more of a hack. For example, place your RFID document (drivers license, passport, etc) into a RF secure container to prevent radio signals from reaching the tag to activate it. While this solution certainly works, it only address the security of tags that can be placed within a container. For tags on large products or on people this solution is not viable.

The scary part is that no real solutions exist while the adoption of RFID tags moves at an incredible pace into nearly every aspect of our lives.

# Conclusion

RFID technology has made significant advances since its initial inception with the radar systems of the pre-WWII era. Since that time we have seen the same technological advances in miniaturization of circuits, improved antenna technology and significant improvements in memory technologies.

All of these improvements has directly impacted the effectiveness and usefulness of RFID tags. Pet owners can now find lost pets, inventories can now scan immediately versus conducting long running and physically intensive inventories of entire warehouses. Retailers have reduced theft by tagging products that must have the tag deactivated after a legitimate purchase and prior to leaving the store.

But with the wonderful advances and applications of the technology a darker side has begun to immerge as personal information stored on the tags themselves or accessed via keys stored on the tags, now become the targets of theft. Corporate identities can now be stolen with a simply walk-by of the intended victim.

The ease with which an RFID identity can be stolen will generate a whole new brand of identity theft as now your corporate identity can be stolen off your card.

Widespread use of RFID technology will create an increase in criminal activity in the financial, identity theft and even computer virus space, all without the victims even knowing a crime has occurred against them. In 2010, the first documented human to be infected with a computer virus was Dr. Gasson from the University of Reading. Dr. Gasson demonstrated how his embedded RFID tag was infected by a computer virus and was able to pass the computer virus on to other computers. [12]

All of these new flavors of old criminal activity are made possible by the incredible lack of modern security practices being applied to RFID tags. Until these security issues are resolved, you should not rely on any RFID device to store secure information for you or even financial information. Just because it's convenient doesn't mean it's safe!!

References

1. Kopps, M. and Mudrak, G. Embedded Systems Authentication, UCCS CS502, August 2010. <http://cs.uccs.edu/~cs502/studentproj/projM2010/mkopps/doc/EmbeddedSystemsAuthentication_KoppsMudrak.docx>
2. M. Roberti, The History of RFID Technology, [Online] 2010. [Cited: December 6, 2010] <http://www.rfidjournal.com/article/view/1338>.
3. M. Roberti, The History of RFID Technology, [Online] 2010. [Cited: December 6, 2010] <http://www.rfidjournal.com/article/view/1338>.
4. J. Handy, The Basics of FerroElectric Memories: FRAMs or FeRAMs, [Online] June 3, 2010. [Cited: December 6, 2010] <http://www.professormemory.edn.com/blog/professor-memory-blog/basics-ferroelectric-memories-frams-or-ferams>
5. Y. Oren and A. Shamir, Power Analysis of RFID Tags, [Online]. [Cited: December 6, 2010]. <http://www.wisdom.weizmann.ac.il/~yossio/rfid/>
6. TOSHIBA, Toshiba Develops World's Highest-Bandwidth, Highest-Density, Non-Volatile RAM. [Online] February 8, 2009. [Cited: December 6, 2010]. <http://www.toshiba.com/taec/news/press_releases/2009/memy_09_554.jsp>
7. C. Thangham, World's Smallest and Thinnest RFID Tag is Powder Made by Hitachi, [Online] October 31, 2007. [Cited: December 6, 2010]. <http://www.digitaljournal.com/article/244321>
8. Kopps, M. and Mudrak, G. Embedded Systems Authentication, UCCS CS502, August 2010. <http://cs.uccs.edu/~cs502/studentproj/projM2010/mkopps/doc/EmbeddedSystemsAuthentication_KoppsMudrak.docx>
9. Entertainment Software Association, Video Games & the Economy, [Online] 2010. [Cited: December 6, 2010]. <http://www.theesa.com/gamesindailylife/economy.asp>
10. Wikipedia.Org. VeriChip. [Online] [Cited: December 7, 2010] <http://en.wikipedia.org/wiki/VeriChip>
11. A. Newitz, The RFID Hacking Underground, [Online] [Cited: December 7, 2010] <http://www.wired.com/wired/archive/14.05/rfid_pr.html>
12. Bbc.co.uk, First human 'infected with computer virus' (2010, May). <http://www.bbc.co.uk/news/10158517>
1. R. T. Kimzey, is with the University of Colorado at Colorado Springs, Colorado Springs, CO 80907 USA. (e-mail: rkimzey@uccs.edu).

G. F. Mudrak is with the University of Colorado at Colorado Springs, CO 80907 USA, (e-mail: gmudrak@uccs.edu). [↑](#footnote-ref-1)