

Security Concerns for RFID Technology

By Michael Grimala

Radio Frequency Identification (RFID) technologies have garnered significant interest due to the benefits they can provide across a wide variety of applications.

Radio Frequency Identification (RFID) technologies have garnered significant interest due to the benefits they can provide across a wide variety of applications. RFID technologies provide the means to uniquely identify physical objects using wireless communication technology, with commercial, military and personal applications. The security and privacy issues surrounding RFID passports have recently focused popular media attention on RFID. Before implementing any technology, one needs to be aware of the implications and consequences of using that technology – including its security aspects.

This article introduces RFID technology, presents a brief history of the evolution of RFID applications, examines security concerns with RFID technologies, discusses countermeasures one can employ to mitigate these concerns, and presents a summary of the findings.

What is RFID?

Radio Frequency Identification (RFID) is a technology used to identify, categorize, and track physical items¹. An RFID system typically consists of RFID interrogators (hereafter called a reader), RFID tags (hereafter called tags), and an information system. The reader contains antennas and electronics necessary to communicate with the tags. The reader is responsible for initiating a read operation by transmitting out a message to all tags. All of the tags within range of the reader respond with their individual identification numbers, and possibly other data contained within the tag. The reader passes the received information collected from the tags to the information system, where it is collected, processed and transformed into knowledge based upon the specific application².

RFID readers can be either fixed or mobile. Fixed readers are used when tags are known to pass within range of the reader. Examples include toll booths, warehouses, points of sale, checkout stands, or any other choke point. Mobile readers are usually handheld devices that are used for inventory control applications that require the reader to be frequently moved. RFID tags can be attached or embedded into anything of value³. For example, tags have been placed in shipping pallets, cases, or individual products; apparel; automobiles; books; electronic devices; livestock; luggage; and human beings⁴. For this reason, RFID is an ideal security technology in that it can detect the presence or absence of a unique physical item. Tags are available in a variety of configurations and vary in cost, size, speed, and storage capability based upon their intended application⁵.

RFID tags have been placed in shipping pallets, cases, or individual products; apparel; automobiles; books; electronic devices; livestock; luggage; and human beings.

Since RFID uses radio waves to transfer data between the reader and tags, it does not require physical contact or line of sight between the reader and the tag⁶. This is an enormous benefit over competing

1 Juels, Molnar, & Wagner, 2005; Juels, 2006; Le-Pong Chin & Chia-Lin Wu, 2004; Xingxin Gao et al., 2004

2 Borriello, 2005; Juels, 2006; Ohkubo, Suzuki, & Kinoshita, 2005

3 Borriello, 2005; Ohkubo et al., 2005; Rieback, Crispo, & Tanenbaum, 2006

4 Eckfeldt, 2005; McCoy, Bullock, & Brennan, 2005; Molnar & Wagner, 2004; Phillips, Karygiannis, & Kuhn, 2005; Stajano, 2005; Xingxin Gao et al., 2004

5 Ohkubo et al., 2005; Rieback et al., 2006

6 Borriello, 2005; Juels, 2006; Vacherand & ois, 2005

technologies such as bar codes, in that an RFID system can operate in environmental conditions that provide physical barriers (boxes, containers, wrapping paper) and optical barriers (rain, fog, paint, dirt) between the reader and the tag⁷. For these reasons, RFID has become increasingly popular in a large number of data collection and identification applications.

The history of RFID

Contrary to popular belief, RFID is not a new technology. The first recorded use of RFID has been attributed to the German military during World War II⁸. Specifically, the German military had been exploring the use of “radio detection and ranging” (radar) as a means to track distant aircraft⁹. German radar operators encountered the problem that when aircraft entered the range of their radar signals, they could not discriminate between blips on their radar screens caused by groups of friendly aircraft returning from a mission, and groups of enemy bombers seeking to destroy their cities and factories. Then it was discovered that by moving the wings of their aircraft up and down, also known as a roll maneuver, pilots could change the reflected radar signal in a unique and distinguishable manner¹⁰. When his plane had been equipped with a means to detect when it had entered radar range, a pilot could initiate a roll maneuver to enable the radar operator to recognize his aircraft as friendly¹¹. While this

It was discovered that by moving the wings of their aircraft up and down, pilots could change the reflected radar signal in a unique and distinguishable manner.

was a very crude passive RFID implementation, it proved very effective and enabled German radar operators to dispatch their fighter interceptor aircraft only when they detected non-German aircraft. The system is passive in that the German aircraft did not require any power source to signal the radar operators¹². It is interesting to note that this first recorded use of RFID was for a military security application.

British pilots began to notice that German aircraft occasionally exhibited the unusual behavior of simultaneously conducting a roll maneuver, and British military analysts questioned why this synchronization was occurring. After studying this behavior for an unspecified period, the British analysts detected a coded signal transmitted from the ground that always preceded the maneuver. This information, in conjunction with their knowledge of radar, proved that the aircraft were conducting the roll maneuver to signal their radar operators that they were German aircraft¹³.

Having learned of this application, the British established a secret project in order to develop their own automated system. The goal of

the project was to provide their radar operators with the capability of discriminating between friendly and unfriendly aircraft without requiring any pilot action. This project resulted in the development of the Identify Friend or Foe (IFF) active RFID system¹⁴. The IFF system requires that each friendly aircraft be equipped with a powered transmitter and receiver pair, also known collectively in this application as a transponder. The IFF system was designed so that it could either continuously transmit an identification signal or broadcast the signal only in response to a coded signal sent from a ground station.

The IFF (Identify Friend or Foe) system could either continuously transmit an identification signal or broadcast the signal only in response to a coded signal sent from a ground station. It is now standard equipment for all civilian and military aircraft.

The IFF system is now standard equipment for all civilian and military aircraft. It is classified as an active system because it requires a powered transmitter in the aircraft to send signals back to the ground station. In contrast, the German method discussed above is classified as a passive system because the aircraft reflects energy from the radar signal.

Commercial use of RFID technology began in the 1960s with the introduction of the Electronic Article Surveillance (EAS) system¹⁵. At the core of the EAS system is a small, inexpensive, passive one-bit RFID tag. When the tag is passed in proximity of an active EAS monitor, the tag responds with a coded signal which indicates the presence of the tag. The EAS system was designed as an inexpensive means to detect theft¹⁶. The tag can be attached to merchandise and, when the merchandise is legitimately purchased, the tag is disabled and the purchased item can pass by the EAS monitor without responding. An obvious shortcoming of this approach is that if someone removes the tag from the merchandise, they can steal the item without the EAS system detecting it. Despite this limitation, EAS proved to be very effective and is the first and most widespread commercial use of RFID technology¹⁷.

The 1970s proved to be a period of development for several new RFID applications. Significant system development during this time included applications in animal tracking, factory automation, and vehicle tracking¹⁸. In the 1980s application domains continued to expand, but varied somewhat by geographic location. In the United States, development was focused primarily upon transportation and personal identification applications, while in Europe the focus was upon short-range systems for animal tracking, business, and industrial applications¹⁹. Also, the first RFID toll-collection systems entered operation in the United States and Norway.

7 Borriello, 2005; Juels et al., 2005; Juels, 2006; Le-Pong Chin & Chia-Lin Wu, 2004; Libicki, 2005; McCoy et al., 2005

8 RFID Journal, 2005

9 Rieback et al., 2006

10 RFID Journal, 2005

11 Rieback et al., 2006

12 The Dean Boys, 2005

13 The Dean Boys, 2005

14 RFID Journal, 2005

15 RFID Journal, 2005

16 Eckfeldt, 2005; Juels, 2006; Phillips et al., 2005; RFID Journal, 2005

17 RFID Journal, 2005; Stajano, 2005

18 RFID Journal, 2005; Stajano, 2005

19 Juels et al., 2005; Juels, 2006; RFID Journal, 2005

The 1990s ushered in the widespread deployment of RFID across a large number of applications including automobile alarms, fuel-dispensing systems, gaming checks, remote vehicle starting systems, ski lift passes, and vehicle access systems²⁰. In addition, during the 1990s virtually all toll roads in the United States were equipped to allow toll collection using RFID systems. Standardization of RFID systems for toll collection allowed a single RFID tag to be used on multiple toll roads²¹. By 1999, a group of manufacturers proposed a set of standards that would help insure product interoperability and help drive down cost²². In 2004, the Department of Defense announced a requirement that all of their suppliers would soon be required to use RFID tags to enable tracking of purchased items²³. A number of organizations are pilot-testing new RFID applications before mass deployment. In 2005, Wal-Mart ran a pilot study where it used RFID tags in all its Texas distribution centers to track more than 10 million cases of goods²⁴. By March 2006 over 1,800 RFID-related patents had been issued by the U.S. patent office, and more RFID-related patent applications are being invented each year.

RFID technology security concerns

We will now examine security concerns that may occur with RFID technologies. This section presents examples of particularly vulnerable RFID applications, and lists countermeasures that can be used

The major threats to an RFID system can be divided into four general categories of attack: Sniffing, Spoofing, Replay, and Denial of service

to mitigate the threats. Note that since our organization is a military contractor and all of our work is classified, only security concerns are discussed. There are a significant number of privacy concerns related to the use of RFID technology, but they are outside the scope of this paper.

The major threats to an RFID system can be divided into four general categories of attack: Sniffing, Spoofing, Replay, and Denial of service²⁵. It should be noted that the categories are not mutually exclusive. The attacks are presented in order of sophistication to provide the necessary background to understand each successive type of attack.

Sniffing attacks

Sniffing attacks represent one of the greatest threats to an RFID system²⁶. Sniffing attacks are not unique to RFID technology, as every wireless communication medium suffers from this vulnerability. Anyone with an antenna can intercept legitimate communications between an RFID tag and reader if they are range of the

transmission. The frequency bands used by standard RFID systems are public knowledge and can be easily obtained on the Internet. Nonstandard systems using proprietary frequency bands can easily be characterized by a skilled person using a spectrum analyzer. In either case, it is easy to obtain or build equipment to detect and store these transmissions.

Further, such equipment no longer requires a large physical space or large power sources – this is clear in the evolution of cellular telephones. As a result, one can easily hide a receiver on his or her person and capture transmissions between a tag and a reader without the consent or knowledge of the tag holder²⁷. While other wireless communication systems can employ encryption to defeat the possibility of such an attack, the limited power and processing capabilities of existing RFID tags often eliminate this as a viable option. Recent advances in technology have resulted in such enhanced tag capabilities as read-write capability, increased computational power, longer battery life, and larger memory storage space²⁸. However, these enhancements significantly increase the tag cost when compared to simple, mass-manufactured tags, and can only be used in those special cases when the additional cost can be justified.

A sniffing attack may be characterized as either passive or active²⁹. A passive sniffing attack requires only a radio receiver tuned to the frequency band of interest and the ability of the attacker to get within proximity of the tag when it communicates with the reader. The passive sniffing attack can collect data transmitted by a tag, but can also capture the coded message sent by the reader used to query tags. An active sniffing attack is more sophisticated in that it requires both a transmitter and a receiver, as normally contained in a legitimate reader, tuned to the frequency band of interest as well as the knowledge of how a legitimate reader queries a tag. In the active attack, the attacker does not need to be in proximity to a legitimate reader. One can locate an illegitimate reader anywhere there may be RFID tags. In this case, the reader sends a special coded message, and all tags tuned to that frequency, within range of the receiver, respond with their data.

Sniffing attacks corrupt the confidentiality of the data transmitted from the tag to the reader and can undermine the integrity of the whole RFID system by revealing details of the encoding scheme used to query tags³⁰. Sniffing is usually not a significant threat in retail inventory control, where a simple single-bit tag is used to indicate the presence or absence of an item. However, other applications that use tags to uniquely identify individuals or items can be exploited in a variety of ways. If anyone can carry an RFID-enhanced passport or drive a vehicle with an RFID-enhanced license plate, a terrorist could build a bomb containing an illegitimate reader that only detonates within close proximity to the bomb³¹. And optionally, by placing illegitimate readers in various locations one could track the movement of a tag over time.

One countermeasure to the sniffing attack involves placing the tag in a shielded enclosure when the tag is not in use. This will prevent information leakage to unauthorized readers. The shielded enclosure acts as a Faraday cage which effectively blocks all electromagnetic radiation into and out of the enclosure³². Such a protection mechanism prevents a hidden reader from querying the tag and blocks all

20 Eckfeldt, 2005; Juels, 2006; RFID Journal, 2005

21 Juels, 2006; Karthikeyan & Nesterenko, 2005

22 Feder, 2006; Phillips et al., 2005

23 Feder, 2006

24 Feder, 2006

25 Borriello, 2005; Juels et al., 2005; Juels, 2006; Karthikeyan & Nesterenko, 2005; Le-Pong Chin & Chia-Lin Wu, 2004; McCoy et al., 2005; Molnar & Wagner, 2004; Ohkubo et al., 2005; Phillips et al., 2005; Rieback et al., 2006; Xingxin Gao et al., 2004

26 Juels et al., 2005; Juels, 2006

27 Juels, 2006

28 Karthikeyan & Nesterenko, 2005

29 Juels, 2006; Ohkubo et al., 2005; QED Systems, 2002; Stajano, 2005

30 Juels, 2006; Ohkubo et al., 2005; Phillips et al., 2005; Rieback et al., 2006

31 Juels, 2006

32 Juels, 2006

tag emissions, rendering the sniffing attack ineffective. While this countermeasure is effective, it may not be feasible in all applications – such as where the tag must always be available to be queried.

Spoofting attacks

Spoofting attacks program blank tags with the correct encoded data so they appear as legitimate tags³³. The information required to perpetrate this attack may easily be gathered, as discussed in the previous section. This type of attack could be used to retag items in a point-of-sale application where RFID tags are used to uniquely identify the product to determine its cost. For example, in an RFID-enhanced supermarket one could remove the tag applied to a frozen lobster and retag the lobster with a tag corresponding to significantly lower-cost items, such as a pack of mints.

Another version of this attack is tag cloning. In this case, a legitimate tag is cloned and used to steal services or gain access to a restricted area. For example, researchers at John Hopkins University were able to clone an existing legitimate tag and used it to buy gasoline and unlock an automobile³⁴. Spoofting attacks compromise the integrity of the RFID system by making it impossible to uniquely identify a physical object. Countermeasures to these types of spoofting attacks include shielding tags when they are not in use for legitimate reading, using strong encryption, or embedding nonstandard response schemes that are difficult to characterize³⁵.

Replay attacks

Replay attacks are a simple combination of the sniffing and spoofting types of attacks³⁶. A replay attack occurs when someone can query a tag, receive the information it sends, and retransmit this information at a later time. Replay attacks compromise the confidentiality and integrity of the RFID system. This type of attack is troubling in numerous applications, but especially so in those involved with authentication.

For example, suppose that an employee carries an RFID-enhanced identification badge to access a secured facility. In this case, the badge is manufactured so that it contains an RFID tag. When the individual is within proximity of a legitimate badge reader, the badge reader will query the tag. The badge will respond with a code which represents the wearer's access credentials. The reader associates the access credentials with the individual and authenticates the employee to determine if they are allowed access to the facility³⁷. Now consider the same employee at lunch at a local deli, and passing by someone hiding a badge reader in their briefcase. The attacker triggers the briefcase to send a query and then records the responses from any badges within its proximity. The attacker can now program a blank RFID-enhanced badge and gain access to the secured facility³⁸.

One countermeasure to this type of attack is to utilize the read-write capability present in newer tags. In this case, when someone accesses the secured facility their code is authenticated and a new code is uploaded into the tag³⁹. This reduces the amount of time that a captured code can be used and dramatically increases the likelihood that an il-

legitimate user will be exposed⁴⁰. Despite these precautions, systems being proposed are nonetheless vulnerable. For example, in the UK trials are underway to test battery-operated RFID-enhanced license plates capable of transmitting their signals more than 300 feet⁴¹. The system was designed to be simple and low cost, and as a result does not address the security issues it presents.

Denial-of-service attacks

A denial-of-service attack against an RFID system is an attack against the availability or usability of the system, and can be perpetrated in many different ways. One can attack any combination of the reader, the tags and the information system that processes the data read from the RFID tags. Since the reader only detects the presence of the tags, one possible attack involves the removal of the tag before it passes in proximity of the reader. This attack is commonly employed by thieves attempting to steal tagged items from a retail store⁴². By removing the tag from an item, they can hide the item from view and pass by the reader undetected. Countermeasures to

...the state of Colorado made it a criminal offense to make or wear aluminum underwear...

this type of attack include hiding the tag in the item, making the removal of the tag difficult, or designing the tag such that its removal causes irreparable damage to the item⁴³.

Another attack involves placing the tagged item into a foil-lined bag or other enclosure which acts as a Faraday cage. In this case the thief does not need to remove the tag, but instead simply places the whole tagged item into the foil-lined bag, and passes by any readers undetected. One countermeasure to this would be to prohibit the carrying of individually owned bags into retail stores, but this is often expensive to enforce in terms of labor; it can also be defeated if someone fabricates a Faraday cage in his or her clothing. This attack became so prevalent that in 2001 the state of Colorado made it a criminal offense to make or wear aluminum underwear, in order to reduce theft in convenience stores⁴⁴.

In another type of denial of service, the attacker pulls tags off their intended items and relocates them onto other items⁴⁵. In the automatic payment scenario found in a retail store, a thief can swap tags from low-value items to high-value items. In this case the thief appears to be properly paying for items while in fact defrauding the retail store. In certain applications such an attack will corrupt the database stored on the information system, and can cause significant loss of trust and loss of integrity for the RFID system. If a warehouse were to use an RFID system to maintain a product inventory, an attacker could relocate tags from one pallet to another and cause the complete loss of integrity of the inventory stored on the information system⁴⁶. A possible countermeasure to this type of attack is to manufacture the tag into the item; to make the tag otherwise inaccessible;

33 Juels, 2006; Rieback et al., 2006

34 Juels, 2006

35 Juels, 2006; Phillips et al., 2005; Rieback et al., 2006; Xingxin Gao et al., 2004

36 Borriello, 2005; Juels et al., 2005; Juels, 2006; Molnar & Wagner, 2004

37 Juels, 2006

38 Juels et al., 2005; Neumann, 2003; Ohkubo et al., 2005

39 Karthikeyan & Nesterenko, 2005; Xingxin Gao et al., 2004

40 Juels, 2006; Ohkubo et al., 2005; Rieback et al., 2006

41 Eckfeldt, 2005; Juels, 2006; Ohkubo et al., 2005

42 Juels, 2006; Phillips et al., 2005

43 Juels, 2006; Xingxin Gao et al., 2004

44 Rieback et al., 2006

45 Juels, 2006; Xingxin Gao et al., 2004

46 Juels, 2006; Neumann, 2003

or to cause destruction to the item if the tag is removed. The risks of this type of attack are growing everyday due to the widespread availability and low cost of RFID equipment and information.

Summary

RFID is unique in its ability to identify physical items in a wide range of harsh environments which are problematic for other types of identification technologies, such as bar-coding. However, RFID technology suffers from a large number of inherent security vulnerabilities, which must be accounted for in a formal risk assessment before the technology may be deployed. Given the benefits of RFID technology across numerous application domains, awareness of RFID security concerns is important to all security professionals.

About the Author

Michael Grimaila, PhD, CISSP, CISM, GSEC Gold, is an Assistant Professor at the Air Force Institute of Technology. His research interests focus on the Management of Information Assurance. He is a member of the ACM, AIS, IEEE, ISACA, ISSA and ISSEA. Dr. Grimaila serves on the Editorial Advisory Board of the ISSA and is an active member of the ISSEA Metrics Working Group.

References

- Borriello, G. (2005). Introduction. *Communications of the ACM*, 48(9), 34-37.
- Eckfeldt, B. (2005). What does RFID do for the consumer? *Communications of the ACM*, 48(9), 77-79.
- Feder, B. J. (2006). Out of consumers' sight, radio tags gain ground. Retrieved April 4, 2006 from http://www.nytimes.com/2006/04/04/technology/techspecial4/05radio.html?_r=1
- Juels, A. (2006). RFID security and privacy: A research survey. *Selected Areas in Communications, IEEE Journal on*, 24(2), 381-394.
- Juels, A., Molnar, D., & Wagner, D. (2005). Security and privacy issues in E-passports. 74-88.
- Karthykeyan, S., & Nesterenko, M. (2005). RFID security without extensive cryptography. *SASN '05: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, VA, USA, 63-67. from <http://doi.acm.org/10.1145/1102219.1102229>
- Le-Pong Chin, & Chia-Lin Wu. (2004). The role of electronic container seal (E-seal) with RFID technology in the container security initiatives. 116-120.
- Libicki, M. (2005). Are RFIDs coming to get you? *Security & Privacy Magazine, IEEE*, 3(6), 6-6.
- McCoy, T., Bullock, R. J., & Brennan, P. V. (2005). RFID for airport security and efficiency. 9.
- Molnar, D., & Wagner, D. (2004). Privacy and security in library RFID: Issues, practices, and architectures. *CCS '04: Proceedings of the 11th ACM Conference on Computer and Communications Security*, Washington DC, USA, 210-219. from <http://doi.acm.org/10.1145/1030083.1030112>
- Neumann, P. G. (2003). Risks to the public in computers and related systems. *SIGSOFT Softw.Eng.Notes*, 28(6), 6-14.
- Ohkubo, M., Suzuki, K., & Kinoshita, S. (2005). RFID privacy issues and technical challenges. *Communications of the ACM*, 48(9), 66-71.
- Phillips, T., Karygiannis, T., & Kuhn, R. (2005). Security standards for the RFID market. *Security & Privacy Magazine, IEEE*, 3(6), 85-89.
- QED Systems. (2002). Active and passive RFID. Retrieved March 18, 2006 from http://www.autoid.org/2002_Documents/sc31_wg4/docs_501-520/520_18000-7_WhitePaper.pdf
- RFID Journal. (2005). The history of RFID technology. Retrieved March 20, 2006 from <http://www.rfidjournal.com/article/articleview/1338/1/129/>
- Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006). The evolution of RFID security. *Pervasive Computing, IEEE*, 5(1), 62-69.
- Stajano, F. (2005). RFID is x-ray vision. *Communications of the ACM*, 48(9), 31-33.
- The Dean Boys. (2005). Identification friend or foe (IFF) systems: IFF questions and answers. Retrieved March 20, 2006 from <http://www.dean-boys.com/extras/iff/iffqa.html>
- Vacherand, F. (2005). New technologies for contactless microsystems. *SOc-EUSAI '05: Proceedings of the 2005 Joint Conference on Smart Objects and Ambient Intelligence*, Grenoble, France, 13-17. from <http://doi.acm.org/10.1145/1107548.1107556>
- Xingxin Gao, Zhe Xiang, Hao Wang, Jun Shen, Jian Huang, & Song Song. (2004). An approach to security and privacy of RFID system for supply chain. 164-168.