

RFID SECURITY THREAT MODEL

Dale R. Thompson, Neeraj Chaudhry, Craig W. Thompson
Department of Computer Science and Computer Engineering
University of Arkansas, Fayetteville, AR 72701
{drt, nchaudh, cwt}@uark.edu, 479-575-5090

Abstract: Radio Frequency Identification (RFID) technology promises benefits that accrue from being able to identify and track individual goods in commercial supply chains. This helps in inventory management, reduces theft, can be used in conjunction with other sensor technology to identify damaged goods, and promises cost reductions. The objective of this paper is to identify potential threats to commercial supply chains related to the use of RFID technology.

1 INTRODUCTION

Radio Frequency Identification (RFID) technology is quickly evolving in the supply chain because it increases visibility of the movement of supplies providing opportunities for increased efficiency. RFID tags can uniquely encode the individual identity of a particular product. Because many tags can be read at a distance (often measured in feet) by readers at known locations, they also provide information on location at time of read, and this information can be used to track tagged items. Manufacturers, suppliers, and retailers stand to benefit from RFID by knowing where goods are within and between businesses in the supply chain.

EPCglobal Inc. is a global not-for-profit standards organization commercializing the Electronic Product Code™ (EPC) and RFID worldwide. The vision of EPCglobal is a standardized system running on different platforms with a standardized protocol. It builds on existing technologies such as servers, clients, databases, wireless communication, and Internet protocols, all with their own potential vulnerabilities, which are out of scope for the following discussion.

Security issues should be addressed before RFID implementations become universal. How secure is an RFID system?

RFID system is no-contact, non-line-of-sight and invisible identification, which is different from ubiquitous barcode identification system [4]. Hence, it is difficult to completely stop the signals from being emitted from the tags. Tags are placed on pallets, cases, and individual items and can be scanned from between inches to meters, revealing the EPC number. The EPC number is the key to a database entry that contains information about the product and its owner. This has the potential to reduce purchase anonymity and privacy advocates are worried about disclosing such information.

Certain privacy issues did arise when Gillette Company decided to apply 500 million RFID tags from Alien Technology Corp. to its Mach III turbo razors [5]. Consumer privacy advocates criticized embedding RFID chips in merchandise products, fearing uncontrolled level of observation that makes users identifiable. Some critics like the head of the Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) call for the global boycott of Gillette and Benetton after their plan to endorse RFID chips in their products [6]. Some consumers see those techniques as a marketing strategy to collect information about the interests of a customer and do not want their interests to be disclosed.

Today, passive tags do not possess enough power and circuitry to send the information directly to the reader or to implement strong cryptographic encryption functions [12]. An intruder with an intelligent reader can read and modify the tag's contents like EPC number, because of the nonexistent or weak security. These security functions require a significant amount of processing power. Adding the necessary circuitry and power to the passive tags adds undesirable cost. The EPC Class-1 Gen-2 tags do have enhanced security that was added to address some concerns but it may not be enough.

Functionality of a tag is easily increased by increasing its cost. But even these expensive tags are not considered safe and can be reverse engineered. Two students reverse engineered Texas Instrument's DST transponder that is used in the anti-theft system of vehicles and for speed passes that permit a user to quickly buy gas [7]. They were able to start a vehicle with the cloned key and buy gas with a cloned RFID tag.

2 STRIDE THREAT MODEL APPLIED TO RFID

The first step in building a secure system is to understand the threats [8]. *Threats* are potential events that cause a system to respond in an unexpected or damaging way. It is useful to categorize threats to determine strategies for mitigating them. In this paper, threats to RFID are categorized using the well-known STRIDE model used in the design of secure software systems [8]. STRIDE is an acronym for six threat categories that are listed below.

- **Spoofing identity.** Spoofing occurs when an attacker successfully poses as an authorized user of a system.
- **Tampering with data.** Data tampering occurs when an attacker modifies, adds, deletes, or reorders data.
- **Repudiation.** Repudiation occurs when a user denies an action and no proof exists to prove that the action was performed.
- **Information disclosure.** Information disclosure occurs when information is exposed to an unauthorized user.
- **Denial of service.** Denial-of-service denies service to valid users. Denial-of-service attacks are easy to accomplish and difficult to guard against.
- **Elevation of privilege.** Elevation of privilege occurs when an unprivileged user or attacker gains higher privileges in the system than what they are authorized.

2.1 Spoofing Identity

Spoofing occurs when an attacker successfully poses as an authorized user of a system. Listed below are spoofing threats.

- A competitor or thief performs an unauthorized inventory of a store by scanning RFID EPC tags with an unauthorized reader to determine the types and quantities of items. An unauthorized reader can query the tag for the EPC number because most tags used in the supply chain respond to any reader. The EPC number is only a number. However, because of the standard way of creating an EPC number, an attacker can determine the manufacturer and possibly the product number. It is likely that the number assigned to all manufacturers will become public knowledge as well as the product number after some short period of time.
- An attacker determines what organization is assigned an EPC number by posing as an authorized EPC's global Information Services (IS) Object Name Service (ONS) user. An attacker can pose as an authorized ONS user and submit queries of either gathered EPC numbers or random EPC numbers to ONS. Middleware queries ONS with the EPC number to determine the URL of the database that contains information on this particular EPC number. If an attacker can pose as one of the authorized middleware users, s/he can submit queries and gather URLs determining the location and possible identification of the organization that contains information on the EPC number.

- An attacker determines the complete information about an object by posing as an authorized user of the database referenced by ONS. An attacker can pose as an authorized ONS user and submit queries to ONS gathering URLs and then look up the EPC number in the appropriate database after being authenticated. A user of ONS authenticates itself with the database after finding the location of the database with ONS to find the mapping between the EPC number and information about the product that has the tag. An attacker that poses as an authorized user can determine the manufacturer, product description, and serial number of a case or a large number of cases.
- An attacker poses as an ONS server. It can gather EPC numbers quietly or respond with invalid URLs leading to either a tampering of data or a denial-of-service attack.

2.2 Tampering with Data

Data tampering occurs when an attacker modifies, adds, deletes, or reorders data. Listed below are data tampering threats.

- An attacker modifies a tag.
 - An attacker modifies the tag in a passport to contain the serial number associated with a terrorist or criminal.
 - A terrorist or criminal modifies a passport tag to appear to be a citizen in good standing.
 - An attacker modifies the EPC number on tags in the supply chain, warehouse, or store disrupting business operations and causing a loss of revenue. An attacker could ship a rogue reader that periodically comes on while being shipped. Or the attacker could walk through a store.
 - An attacker modifies a high-priced item's EPC number to be the EPC number of a lower cost item.
- An attacker adds a tag to an object.
 - An attacker adds a tag in a passport that contains the serial number associated with a terrorist or criminal.
 - An attacker adds additional tags in a shipment that makes the shipment appear to contain more items than it actually does.
- An attacker deletes data on a tag.
 - An attacker kills tags in the supply chain, warehouse, or store disrupting business operations and causing a loss of revenue [9]. EPCglobal proposed that a tag have a "kill" command to destroy it to protect consumer privacy. If implemented in the tag, an attacker can "kill" the tag if the password is known. Class-0, Class-1 Gen-1, and Class-1 Gen-2 tags have kill commands [1], [2], [3]. An attacker could ship a rogue reader that periodically comes on while being shipped. Or the attacker could walk through a store.
 - An attacker erases the tags setting all values including the EPC number to zero in the supply chain, warehouse, or store disrupting business operations and causing a loss of revenue. An attacker could ship a rogue reader that periodically comes on while being shipped. Or the attacker could walk through a store.

- An attacker removes or physically destroys tags attached to objects [7]. This is used by an attacker to avoid tracking. A thief destroys the tag to remove merchandise without detection.
- An attacker reorders data on a tag or reorders tags.
 - An attacker exchanges a high-priced item's tag with a lower-priced item's tag. Barcodes have been subject to this attack for years.
- An attacker modifies the return signal from the tag to the reader.
- An attacker poses as an ONS server and responds with the incorrect URL in response to an ONS query from a manager.
- An attacker modifies, adds, deletes, or reorders data in a database that contains the information about EPC numbers. This is under the category of database security.

2.3 Repudiation

Repudiation threats occur when a user denies an action and no proof exists to prove that the action was performed. Listed below are repudiation threats.

- A retailer denies receiving a certain pallet, case, or item. A non-repudiation protocol is required to ensure that neither the sender nor the receiver can deny actions.
- The owner of the EPC number denies having information about the item to which the tag is attached. This could lead to a user being denied warranty repair or returns.

2.4 Information Disclosure

Information disclosure occurs when information is exposed to an unauthorized user. It is a threat to privacy if it is information about an individual. Listed below are information disclosure threats.

- A bomb in a restaurant explodes when there are five or more Americans with RFID-enabled passports detected.
- A smart bomb positioned at a street corner explodes when a particular individual with an RFID-enabled passport is detected.
- A smart bomb positioned at a street corner explodes when an individual carrying one or more specific items with tags is detected. An individual could be marked by reading the tags that they typically carry. Or any individual buying certain products could be marked.
- A mugger marks a potential victim by querying the tags in possession of an individual to determine if they are carrying valuable or wanted items.
- An attacker blackmails an individual for having certain merchandise in their possession.
- A fixed reader at a retail counter identifies the tags of a person and shows the similar products on the nearby screen to a person to provide individualized marketing.
- A competitor or thief performs an unauthorized inventory of a store by scanning tags with a reader to determine the types and quantities of items. An unauthorized reader can query the tag for the EPC number because most tags used in the supply chain respond

to any reader. The EPC number is only a number. However, it is an index and there are standard ways of creating them. Because of the standard way of creating an EPC number, an attacker can determine the manufacturer and possibly the product number. It is likely that the number assigned to all manufacturers will become public knowledge as well as the product number after some short period of time. A competitor gains information on the types and quantities of items in a store. A thief could query a warehouse, truck, or store to help locate high-priced items.

- A thief creates a duplicate tag with the same EPC number and returns a forged item for an unauthorized refund.
- A sufficiently powerful directed reader reads tags in your house or car.

2.5 Denial of Service

Denial-of-service denies service to valid users. Denial-of-service attacks are easy to accomplish and difficult to guard against. Listed below are denial-of-service threats.

- An attacker kills tags in the supply chain, warehouse, or store disrupting business operations and causing a loss of revenue [9]. EPCglobal proposed that a tag have a “kill” command to destroy it to protect consumer privacy. If implemented in the tag, an attacker can “kill” the tag if the password is known. Class-0, Class-1 Gen-1, and Class-1 Gen-2 tags have kill commands [1], [2], [3]. An attacker could ship a rogue reader that periodically comes on while being shipped. Or the attacker could walk through a store.
- A shoplifter carries a blocker tag that disrupts reader communication to conceal the stolen item [9]. The blocker tag is used against the tree walking anti-collision protocols. An attacker can simulate many RFID tags simultaneously causing the anti-collision to perform singulation on a large number of tags making the system unavailable to authorized use [9]. Singulation is the process in the deterministic anti-collision protocol of systematically choosing one tag to respond [11]. Plans for a blocker tag already exist [9]. A blocker tag is a cheap passive RFID device that simulates many ordinary RFID tags simultaneously and renders specific zones to be private or public. The blocker tag could simulate all RFID tags or it could simulate portions of the EPC address space.
- An attacker carries a special absorbent tag that is tuned to the same frequencies used by the tags. Instead of switching the impedance in and out of the antenna to modulate the reader signal it would just absorb the energy reducing the amount of reader energy. It could be a passive device. This would decrease the amount of energy available for reading other normal tags.
- An attacker removes or physically destroys tags attached to objects [9]. This is used by an attacker to avoid tracking. A thief destroys the tag to remove merchandise without detection.
- An attacker shields the tag from being read with a Faraday Cage [9]. A Faraday Cage is a metal enclosure such as a bag lined with aluminum foil that prevents the reader from reading the tag. In the debate over embedding tags in passports, it has been suggested that the passports be inserted into a foil holder to prevent this type of attack [10].
- An attacker with powerful reader jams the reader by creating a more powerful return signal than the signal returned from the tags and thus making the system unavailable to authorized users [9].

- An attacker performs a traditional Internet denial-of-service attack against the servers gathering EPC numbers from the readers.
- An attacker performs a traditional Internet denial-of-service attack against ONS.
- An attacker sends URL queries to a database causing it to do database queries and therefore denying access to authorized users.

2.6 Elevation of Privilege

Elevation of privilege occurs when an unprivileged user or attacker gains higher privileges in the system than what they are authorized. Listed below are elevation-of-privilege threats.

- A user logging on to the database to determine product information can become an attacker by raising his/her status in the information system from a user to a root server administrator and write or add malicious data into the system.

3 CONCLUSION

This paper is purposely limited in scope to providing a model for RFID threats to the security of a system. It does not cover privacy or threat mitigation. Many RFID threats can be detected and/or managed by conventional security management approaches but not if system developers fail to identify potential threats. Future work will include assigning risk to each threat to obtain a quantitative score, sorting threats from the highest to lowest risks, and proposing and evaluating techniques to mitigate the threats with higher risks.

REFERENCES

- [1] *Draft Protocol Specification for a 900 MHz Class 0 Radio Frequency Identification Tag*, Auto-ID Center, MIT, Cambridge, MA, Feb. 23, 2003. Available: <http://www.epcglobalinc.org/>.
- [2] *860 MHz – 930 MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation*, ver. 1.0.1, tech. report, Auto-ID Center, MIT, Cambridge, MA, Nov. 14, 2002. Available: <http://www.epcglobalinc.org/>.
- [3] *EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz*, ver. 1.0.9, EPCglobal Inc., Jan. 31, 2005. Available: <http://www.epcglobalinc.org/>.
- [4] Sarma, S. E., S. A. Weis, D. W. Engels, "RFID systems and security and privacy implications," in *Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, August 2002, pp. 454-470.
- [5] Clarke, P., "Start-up gets big order for fluidically assembled RFID chips," *EE Times*, <http://www.eet.com/news/latest/showArticle.jhtml?articleID=10800626>
- [6] Gilbert, A., "MIT bows out of controversial RFID tag research," *silicon.com*, <http://software.silicon.com/security/0,39024655,39116580,00.htm>
- [7] Bono, S., M. Green, A. Stubblefield, A. Juels, A. Rubin, M. Szydlo. "Security analysis of a cryptographically-enabled RFID device," in *Proc. USENIX Security Symposium*, July-August 2005.
- [8] Howard M., D. LeBlanc, *Writing Secure Code 2nd ed.*, Redmond, Washington: Microsoft Press, 2003.
- [9] Juels, A., R. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *Proc. Conference on Computer and Communications Security - ACM CCS*, October 2003.
- [10] Schneier, B., "Fatal flaw weakens RFID passports," *Wired NEWS*, Nov. 2003, pp.1- 2.
- [11] Law, C., K. Lee, and K.-Y. Siu, *Efficient Memoryless Protocol for Tag Identification*, tech. report, Auto-ID Center, MIT, Cambridge, MA, Oct. 2000. Available: <http://www.autoidlabs.org/whitepapers>.
- [12] Chaudhry, N., D. Thompson, C. Thompson, "RFID Technical Tutorial and Threat Modeling," ver. 1.0, tech. report, Dept. of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, Arkansas, Dec. 8, 2005. Available: <http://csce.uark.edu/~drt/>