RFID FOR SECURITY ISSUES

EXECUTIVE SUMMARY

RFID data security is important. Security is a critical issue that must be addressed correctly—from both a technical and business process point of view—to ensure widespread ubiquity of RFID technology.

RFID must meet the public demand for data security. The general public must perceive RFID technology as safe and secure to alleviate legitimate concerns about data security and personal privacy.

Today's EPC security is acceptable for now. Current levels of data protection provided by the EPCglobal Generation 2 protocol represent an advance over previous protocols and are acceptable for today's limited RFID deployments within the supply chain.

The key security threats are to front-end RF communication. IP communication between RFID readers and the network is secure, thanks to standard IP network security solutions. The real threat is RF communication between tags and readers. These issues must be addressed by future protocols and additional research and development.

Data security threats take different forms. Rogue/clone tags, rogue/unauthorized readers, and side-channel attacks (interception of reader data by an unauthorized device) all threaten data security.

Future deployments will need new security and a new protocol. As deployment of RFID reaches the consumer-item level, new security enhancements will be needed, triggering a need for a new Generation 3 protocol.

Security comes at a cost. New security measures must balance effectiveness with cost and complexity implications.

Data security is an evolving story. Future generations of tag protocols will enable RFID to take security to a new level.

INTRODUCTION TO RFID SECURITY

Identity theft, stolen credit card information, viruses, hackers, and other threats have raised data security, once an arcane topic relevant only to programmers, to high levels of public awareness. Keeping data secure is a vital concern for individuals, corporations, and governments. Data security is an issue that has broad implications for business practices and technology. And it's a highly emotional issue—what could be more personal than your Social Security number, address, or personal preferences?

Increasing adoption of Radio Frequency Identification (RFID) technology opens a new frontier for data threats and data security measures. Broadly speaking, RFID includes a full spectrum of wireless devices of varying capabilities, power, and sophistication, including ExxonMobil SpeedPasses, vehicle immobilizers, Electronic Product Code (EPC) tags, and more. RFID tags are small, wireless devices that emit unique identifiers upon interrogation by RFID readers, which emit powerful electromagnetic fields and "read" tag information.

This white paper focuses on the simpler, low-cost EPC tags that are used increasingly to bring new efficiency to commercial supply chains—serving as a 21st-century evolution of bar codes. As implementations of RFID technology of this type become more widespread, ambitious, and ubiquitous, they create new potential data security threats, new concerns among consumers, and new misconceptions.

This paper explores the key types of data security threats raised by RFID and highlights possible solutions using the capabilities defined by the EPCglobal (the RFID industry standards group) Class 1 Generation 2 standard, known as Gen 2. It explores the current data security needs and suggests best practices for optimizing the capabilities of Gen 2. It also looks beyond Gen 2 to envision new data security capabilities. And it highlights and evaluates several recent news stories about RFID data security.

AN OVERVIEW TO RFID SECURITY

Defining Data Security

It's important to have a clear idea of what data security means. Only then can you truly measure whether an RFID implementation is truly secure. Here are three qualities that define data security in an RFID context:

- Controlled access to the data—only authorized entities (people, systems) can read and write information
- Control over access to the system—only authorized entities can configure and add to the system, and all devices on the system are authentic and trustworthy
- Confidence and trust in the system—users share a general perception that the system is safe and secure, although this is a more subjective but nonetheless important criteria

Levels of Data Security

Every communication system has its own appropriate level of data security, from wireless devices to the Internet. Not every type of data merits the highest level of security. Escalating levels of security tend to introduce extra cost and technological complexity, and RFID is no exception. It's critical to balance security threats against security costs.

Public Perception of Data Security

At some point, Internet users became confident enough in online commerce that they would participate in potentially risky processes, such as buying products or trading stocks. Why? Because the level of data protection and its perception has reached a high enough bar that the general public has confidence and trust in the system. For widespread acceptance, RFID technology must achieve a similar level of confidence and trust.

Stakeholders in RFID Data Security

Who is concerned about RFID data security?

- Consumers want to ensure that their personal information isn't misused and that RFID tags are used responsibly

- Corporations want to use RFID technology to increase efficiency, serve consumers better, and gain a competitive advantage
- Governments want to create standards that ensure the public trust
- RFID Solution Providers want to ensure the reliability and security of their systems, as well as their usefulness and competitiveness

WHERE SECURITY MATTERS

Security is only as strong as its weakest link. In your home, the most powerful locks on your door will do nothing to keep your house secure if your windows are open. So it is with RFID security. All elements of an RFID system need to be secure, and the links between each element must be carefully considered with data security in mind.

The Importance of the Tag Reader

In RFID systems, tag readers are the communications crossroads and pivotal junctures in the security of the entire system. Tag readers communicate in two directions and each must be secure:

- Back-End Communication (via IP)–Tag readers convey data via Internet Protocol (IP) communication
- Front-End Communication (via RF)–Tag readers provide and collect data to and from tags via low-power Radio Frequency (RF) communication

Back-End Network Security

The key threat on the back-end communication side is unauthorized access to the network. No company wants to implement a system that leaves a clear opening for rogue devices (or just plain rogues) to access their network. Again, it would be like leaving all the windows open in a house, which is not good for security.

Fortunately, network security is a highly evolved, mature technology that brings plenty of powerful tools and technologies to bear on the challenge of keeping networks safe. RFID reader makers can implement standard, proven security technologies, such as Secure Sockets Layer (SSL) and Secure Shell (SSH). They can close ports that are not secure (e.g., with Telnet). And they can implement secure processes, such as certificates for authentication, which keep out unauthorized readers, competitors, hackers, and other potential threats.

In short, the data security story for back-end communication is simple and strong. Security at this juncture is controlled by RFID reader manufacturers (e.g., ThingMagic), who have plenty of powerful, standard tools available to ensure data security. These proven, widely used security capabilities—de facto standard features of today's IP networks—exist to support data security and should be an essential feature of any RFID reader and RFID implementation. They are not yet common in RFID products, however. So users should be diligent in ensuring that the RFID readers they select conform to industry-standard security practices.

Front-End RF Security

The front-end side of the RFID reader is a different story, one that is more challenging, complex, and evolving. The vital connection between tags and readers occurs in the air via RF communication. This connection enables the powerful capabilities of RFID, but it also leaves the window open to several key threats, such as:

- Unauthorized access to tags
- Rogue and clone tags
- Side channel attacks

These threats are explored in more detail in the following sections. However, it's important to point out that front-end RF security is the weakest link in today's RFID systems.

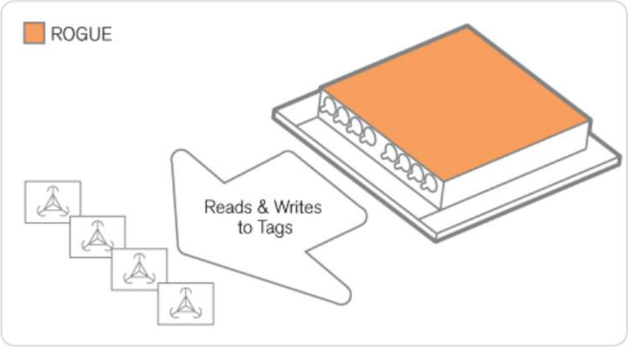
This area, controlled by the tag protocol standards process, has evolved in the latest standard introduced by EPCglobal, Generation 2. But there is still plenty of research and development and innovative thinking necessary before the front-end is as secure as the back-end. Today, front-end RF communication is vulnerable. It's the Achilles' heel of RFID systems.

KEY FRONT-END SECURITY ISSUES

Most of the front-end threats to RFID security involve deception, manipulation, or misuse of the RF communication between tag and reader. Here we explore three common threats: unauthorized access to tags, rogue and clone tags, and side channel attacks.

Unauthorized Access to Tags

Tags are evolving quickly in complexity, power, and flexibility. However, all types of tags share a critical vulnerability to rogue RFID readers. A rogue reader can read a tag, recording information that may be confidential. It can also write new, potentially damaging information to the tag. Or it can kill the tag. In each of these cases, the tags respond as if the RFID reader was authorized, since the rogue reader appears like any other RFID reader. This capability has broad implications, since tags may contain data that should not be shared with unauthorized devices.

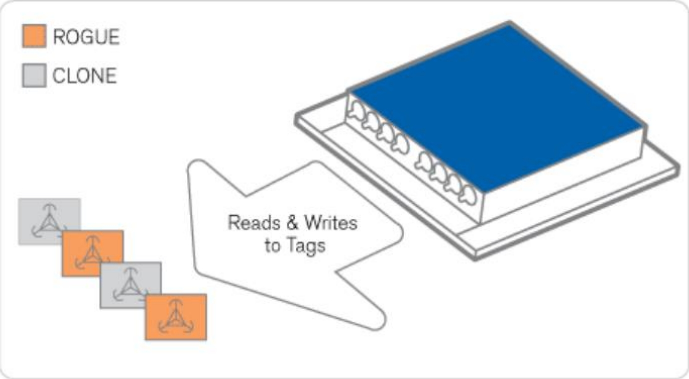


Example: Unauthorized Access to Tags

A rogue RFID reader might be able to measure the inventory on a store shelf and chart sales of certain items, providing critical sales data to a rival product manufacturer. This unauthorized information could play a key role in developing a competitive strategy informed by corporate espionage, e.g., negotiating more shelf space or better product placement.

Rogue and Clone Tags

On the other end of the tag-reader connection, consider the threat of rogue and clone tags. Rogue tags are tags from unauthorized sources, while clone tags are unauthorized copies of real tags. These tags connect with the RFID reader via RF and send false data.

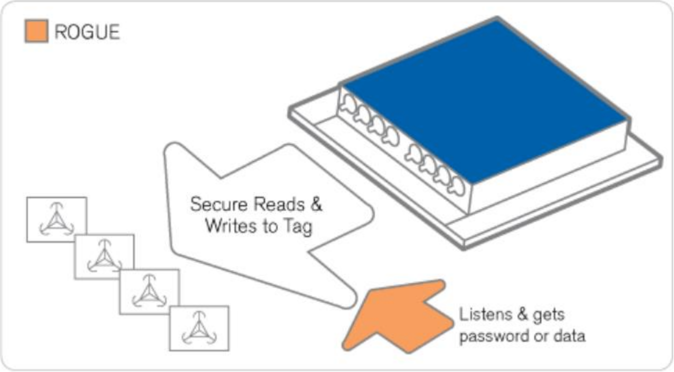


Example: Rogue and Clone Tags

A bootleg product could appear to be an actual product if it bears a clone tag. A rogue tag placed within proximity to a RFID reader could contribute false data to the reader. In both cases, these tags affect the integrity of the system and undermine security for both consumers and the companies that rely on RFID.

Side Channel Attacks

The biggest vulnerability in today's RFID systems occur when interloper RFID readers or other rogue devices eavesdrop on authentic transactions and RF communications between authorized tags and readers. The rogue device can access passwords or data using standard, inexpensive lab equipment. Like wiretapping (without the wires), this capability exposes confidential information to others who may put it to new and nefarious uses.



Example: Side Channel Attack

A rogue device outside a large retail store might gather confidential data, such as who is buying anti-depressants, which could conceivably be sold to competitors, the tabloid press, or others.

AN ASSESSMENT OF GENERATION 2 SECURITY

RFID security is an evolving story, driven by the needs of the marketplace, the technological ingenuity of engineers engaged in developing next-generation solutions, and above all, the tag protocol standards process.

Evaluating Current Security Levels

The Generation 2 protocol is an improvement on Generation 1 and previous tag protocols. It includes key capabilities that companies implementing RFID can leverage to help ensure security:

- Kill command — Tags can be "killed" or permanently rendered inoperable by command under the Gen 2 protocol. Killing tags at point-of-sale enables greater data security and personal privacy. In short, "dead tags don't talk." The Gen 2 kill command is protected by a tag-specific, 32-bit password, which offers a basic level of security to the tag and helps protect against inadvertent or malicious disablement of tags.

- Disguised EPC number — During most transactions, the tag's EPC number (its unique identifier) is somewhat disguised, helping protect tag identity—and tag data.

Does Generation 2 provide sufficient security?

Yes and no. Yes, given current deployments, and no for next-generation, broader deployments that will take RFID into more public environments. The current security features add up to an acceptable level of security given the current state of the market. In a time when RFID is still evolving, deployment levels are relatively low. And the focus of most implementations is on the back-end of the supply chain, primarily case and pallet-level tagging, where security risks are inherently lower, since physical access to the system is limited to employees and therefore somewhat controlled.

Shortcomings of Generation 2

Simply killing tags isn't enough to cure all security issues inherent in RFID. Under the Gen 2 protocol, there are several clear issues that serve as potential roadblocks to more ubiquitous deployments at the consumer level:

- Weak data encryption - Potentially private or sensitive data (an EPC could identify a personal product, such as Viagra) is not encrypted, but cover coded by means of a pseudo-random number transmitted by the tag. This code can be compromised very easily by a side-channel attack.

- Weak password protection - Like data, passwords are not encrypted, but cover coded, which is less robust than a strong cipher.

- No tag or reader authentication—Lack of authentication introduces the risk of rogue/clone tags or rogue/unauthorized readers to an RFID implementation.

Clearly, the level of security in Generation 2 is not sufficient to meet the original criteria of data security discussed at the outset of this white paper. Access to the data is not tightly controlled. Access to the RFID system is similarly open to manipulation and attack via the three main types of front-end threats. And most importantly, security levels are not high enough to generate the high levels of consumer trust that will enable widespread acceptance of RFID at the item level.

Current Best Practices

Given the current level of data security provided by Gen 2, what can companies using RFID technology do to help achieve maximum security? Here are some basic considerations and best practices to consider:

Back-End Security

- Ensure that your back-end security uses industry-standard network technology

Front-End Security

- Avoid putting confidential information on the tag
- Use information pointers, rather than actual information

Impact of Ubiquity on Security

As RFID moves toward great ubiquity in the marketplace, such as widespread item-level tagging, it will become more and more vulnerable to attack. The key contexts for EPC tags represent an evolving progression toward ubiquity via three general phases:

- **Phase 1.** Inside the supply chain (now)—factories, transportation, retail backrooms

- **Phase 2.** Transition zone (near future)—customer-facing portions of retail stores, where tagged items are purchased by consumers

- **Phase 3.** In the outside world (future)—locations including consumer homes and beyond

As deployments move through these phases, tags become more widely used. More tags (item-level tagging will result in many more tags than case- or pallet-level tagging) and more RFID readers (ubiquitous tags will result in wider deployment of readers) mean new opportunities for attack, and new threats designed to exploit security shortcomings. Side channel attacks are a particular risk once tags are deployed at the item level. And new threats will emerge as RFID becomes more of a target for espionage and hacking.

The success of RFID in the marketplace will place new security demands on it and an increased need for robust security in emerging tag protocols.

BEYOND GENERATION 2

From this examination of security threats to Generation 2, it's clear that a future EPC Generation 3 protocol will need to add higher security levels to RF front-end communication to ensure broader use of RFID technology. New technical and policy approaches will have to solve the real privacy and security concerns identified by industry analysts, technologists, and public watchdogs. If not, restrictive legislation or public backlash could thwart widespread acceptance and limit the powerful benefits that RFID offers businesses and consumers.

Technologies that Enhance Security

Possible technological approaches that can enhance security in future protocols include:

- Encryption — Cryptography provides greater data security by storing encrypted serial numbers on tags. However, it raises the significant technological challenges of key management (distributing/managing the corresponding decryption key). Encryption doesn't eliminate tracking, it simply makes it more complex. And any onboard encryption operations would boost the computational demands on tags, introducing new overhead and boosting the price per tag.

- Tag passwords — Basic RFID tags already have sufficient resources to verify PINs or passwords, which could be a possible solution for data protection. For example, a tag could emit critical information only if it receives the correct password. However, password management poses a significant challenge.

- Tag pseudonyms — Another approach to password-based security is the use of tag pseudonyms. Under this approach, RFID tags aren't programmed with passwords, but change serial numbers each time they are read. This approach would make unauthorized tag tracking more difficult, but also introduces issues of pseudonym management.

These are just some of the approaches that can help bring new security to RFID implementations.

NEXT STEPS TOWARD GREATER DATA SECURITY

Careful consideration and investigation by key players in the RFID technical community, as well as an open and rational public debate, will help identify the approach that provides the right level of security, without introducing burdensome computational demands, technological complexity, or manufacturing cost increases.

Future generations of the EPCglobal protocol will lead the way to greater data RFID security and broader acceptance of RFID technology in the marketplace. It is clear that while EPC Generation 2 technology represents a step forward in RFID security, it is not the end of the journey. We should not try to force-fit security into the existing Generation 2 protocol. Item-level tagging will require a higher level of security that can only really be attained with new, Generation 3 technology.

RFID SECURITY IN THE NEWS

The latest stories help to evaluate the real level of threat.

RFID Virus[1]

A group of Dutch scientists from the Faculty of Sciences in Amsterdam wrote recently in a joint paper that RFID systems were vulnerable to viruses because RFID tags could be compromised and infected with viruses by hackers. In short, they claimed that viruses could be transmitted via tags, breaching the security of the RFID systems.

Level of Risk: Very low
This scenario is highly theoretical and unlikely in real-world implementations. Hackers cannot infect an RFID system by compromising the tag, unless that system treats data as if it were code, an improbable and amateurish security mistake. Any well-designed RFID implementation would eliminate the risk entirely.

Cell Phone Side Channel Attack[2]

At the 2006 RSA Security annual conference, cryptographers and data security specialists described a side channel attack on a Generation 1 RFID tag using “power-analysis” of the system’s energy consumption. The attack required an oscilloscope and directional antenna. However, the group predicted that similar power analysis attacks could be performed using common devices, such as a cell phone. These devices could be modified to eavesdrop on an RFID system, infer passwords, gain access, and send inappropriate “kill” messages.

Level of Risk: Low
The technical complexity of this experiment, conducted by expert cryptographers, is very daunting. Eavesdropping on RFID systems is quite possible, even using less-complicated equipment, i.e., a rogue reader. However, the 32-bit password protection provided in Generation 2 provides a higher barrier to eavesdropping. And power analysis is not something most hackers are going to be capable of performing. In short, this attack is too complex to be worthwhile, and unlikely to succeed in almost any scenario.

ExxonMobil SpeedPass Hack[3]

Researchers at Johns Hopkins University recently performed a successful hack of the Texas Instruments RFID Digital Signature Transponder (DST) used in ExxonMobil SpeedPass systems. In a detailed academic paper, the authors highlighted the steps they took to crack the key from a deployed DST device using advanced, but widely available equipment, and some very smart thinking. They used the information gathered to access the ExxonMobil system and purchase gasoline.

Level of Risk: Real
This experiment highlights the need for stronger password protection within any RFID system. However, it's important to point out that the type of tags (DST) used within this level of RFID system are very different than those used within EPC implementations. SpeedPass systems use older technology with weak password protection. And the researchers conducting this experiment had access to information on the password design that they located on the Internet. Less agile hackers would have had a harder time making this security breach happen, but it is entirely possible. This attack highlights the need for strong password protection and careful design to reduce the likelihood of an attack within an EPC RFID implementation.

Sources:

1. "Is Your Cat Infected With A Computer Virus" http://www.rfidvirus.org2/
2. "EPC Tags Subject to Phone Attacks" RFID Journal http://www.rfidjournal.com/article/articleview/2167/1/1/
3. "Analysis of the Texas Instruments DST RFID" RFID Analysis http://rfidanalysis.org/