A new challenge

Plugging security gaps

by Matthew J. Harmon and Natascha E. Shawver

The number of RFID applications in everyday use has exploded over the last decade, with tiny radio frequency (RF) tags now tracking products, animals and assets all over the world. The benefits of the technology range from improved supply chain management to efficient inventory tracking.

Some of the largest organizations in the world, such as the US Department of Defense and the retail giant Wal-Mart, use RFID to track shipments. Cattle ranchers tag livestock. Hospitals maintain chains-of-custody for drugs and supplies. RF tags are found in passports, credit cards and library books – and they're even used to track endangered species.

No single countermeasure is 100 % effective.

While RFID has proven its usefulness in many areas of modern life, significant challenges must be resolved before the technology's full potential can be realized. With falling prices and enhanced capabilities eliminating many obstacles, attention has shifted to the security component of RFID deployments.

Hacking evolves

Breaches in RFID security – both real and potential – have been well publicized in the media, creating unease among consumers, companies, policy makers and other RFID security stakeholders. Most RF tags do not encode personally identifiable information (PII).

So far, there have been only a few instances of RFID applications being compromised, but a successful "drive-by cloning" of RFID tags in passports by a British hacker (in which data was copied from documents carried in the owners' pockets and purses) showed that the potential for damage is real. The past history of computer hacking makes it clear that new attack methods will evolve over time.

Hacking poses a threat to the confidentiality, integrity and availability of RFID systems. It can disrupt business, cause serious privacy breaches, and undermine trust in the technology itself.

The RFID industry has recognized these challenges by actively working to add security measures such as encryption and authentication to the tags. Because encryption reduces the available storage space on a tag and authentication slows reading response times, the challenge is to strike a balance among the requirements for efficiency, the demand for low-cost RFID solutions, and the privacy requirements of a concerned public. International Standards are the solution.

Data protection at every step

A security breach can happen at the tag, at the reader (also referred to as an interrogator) or, less often, at the network level. ISO/IEC TR 24729-4:2009, *Information technology – Radio frequency identification for item management – Implementation guidelines* – Part 4*: Tag data security,* defines RFID security as the prevention of unauthorized reading or changing of RFID data. This means protecting the data on the tag, and the data transmitted between the tag and reader to ensure it is accurate and safe from unauthorized access.

In broad terms, RF tags are small wireless devices, consisting of a microchip and an antenna, which emit information when interrogated by RFID readers. Hundreds of models of commercially available tags fall into two basic categories: active and passive tags.

Passive tags, currently the most commonly used devices, require higher power interrogators that create a continuous radio wave. The passive RF tag receives the radio wave and reflects (or modulates) a return signal to the interrogator consistent with the data programmed into the passive tag.

Active tags have an embedded transmitter and generally transmit at far less power than passive tags. Most active tags currently in use incorporate batteries, though future energy-harvesting techniques may change that.

The basic difference between active and passive tags is that the active tags transmit and passive tags reflect a received signal.

Vulnerabilities

Tags, readers and the air interface between them are susceptible to a number of possible attacks that fall into three main categories: mimicking, gathering and denial of service.

Mimicking encompasses spoofing, cloning and applying malicious code. To spoof tag data, the data is duplicated and transmitted to a reader. Cloning involves duplicating the data from one tag onto another tag. An example would be exchanging a container seal with a cloned tag after a thief breaks into the container to steal or tamper with its contents.

Malicious code put on the tag could hypothetically compromise an entire enterprise system and disrupt a business, although the risk of such damage is currently limited due to the memory and range restrictions of most tags.

Gathering information from the tag takes place through skimming (unauthorized reading of data on a tag); eavesdropping (unauthorized listening/intercepting through the use of radio receiving equipment of an authorized transmission); data tampering (unauthorized erasing of data to render the tag useless or altering of the data, for instance to change the price of a tagged item in a store).

Denial of service attacks occur when multiple tags or specially designed tags are used to overwhelm a reader's capacity to differentiate tags, rendering the system inoperative. Readers can also be jammed and tags can be physically blocked to disrupt reading. The tag can be mechanically or electronically "killed" to prevent it from being read.

Standards for application security

As RFID technology and security threats evolve, so does the need for standards. In 2009, the technical report ISO/IEC TR 24729-4 giving guidelines on RFID tag data security was published. The report was based on the work developed by the RFID Experts Group (REG) set up by the Association for Automatic Identification and Mobility (AIM) – the global trade association for the automatic identification and data capture (AIDC) industry.

The challenge is to strike a balance.

The ISO/IEC report assesses risks according to the Open Web Application Security Project's (OWASP) "DREAD" model by looking at:

- The potential damage a threat represents
- The chance of reproducibility
- What is needed to exploit a threat
- How many users would be affected
- How easy it is to discover a threat.

The group analyzed the probability of a threat and its potential impact in various scenarios by looking at supply chain tags, smart cards, customer loyalty cards, contactless payment cards and other RFID applications to discern the security implications for each scenario.

The guidelines recommend a number of countermeasures to safeguard security, such as the use of a unique tag identification as defined in ISO/IEC 15963:2009, *Information technology – Radio frequency identification for item management – Unique identification for RF tags.*

This may include password protection, encryption, and various authentication measures. No single countermeasure is 100% effective in all situations. Combinations of countermeasures can be used to increase RFID data access security.

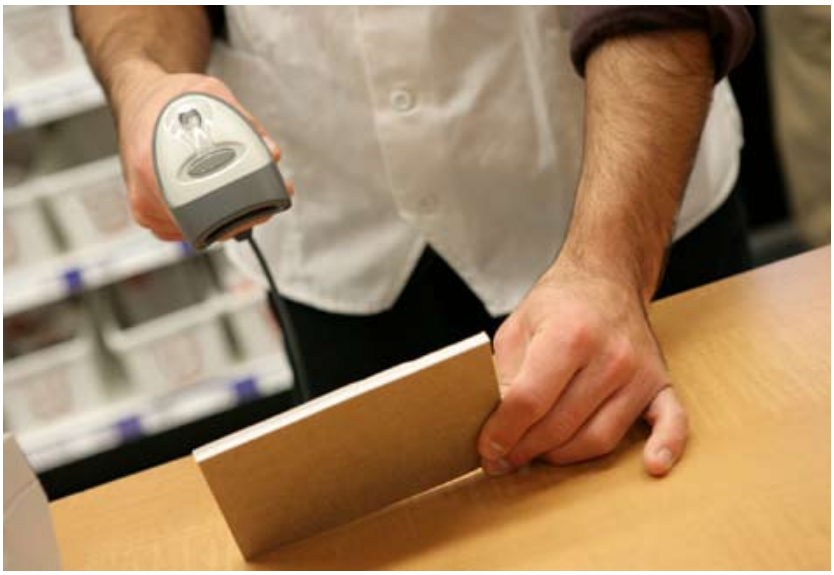
Existing RFID standards that already have specific security components built in to them include the following:

- ISO/IEC 7501 series for machine readable travel documents
- ISO 13181 series on Communications Access for Land Mobiles (CALM)
- ISO/IEC 15693 series for vicinity cards (i.e. cards which can be read from a greater distance as compared to proximity cards)
- ISO/IEC 15963:2009 for RF tags
- ISO/IEC 18000 series for item management
- ISO/IEC 21451-7 for transducers to RFID systems communication protocols and transducer electronic data sheet formats.[1)]

Basic framework standards for security are being or have been developed by ISO/IEC JTC 1, *Information technology*, subcommittee SC 27, *IT Security techniques*, and ISO/TC 8, *Ships and marine technology*.

In the pipeline

The recently created working group WG 7, *Security for item management,* of ISO/IEC JTC 1/SC 31, *Automatic identification and data capture techniques*, will "provide standards and a framework for security of automatic identification and data capture systems, particularly the air interface and other SC 31 wireless communications components."



It has also set goals to define appropriate secure file management techniques for various memory sizes and configurations, to identify risks and potential controls and to deliver a suite of solutions that enable the implementation of various tiers of security for item management.

ISO/IEC JTC 1/SC 31/WG 7 will have to deal with some important requirements. One is the demand for low prices – security features add to the cost of the tag. Another is efficiency, since reading tags becomes slower when security features are added. And there is also the need for interoperability, which is already an issue due to the conflicting needs of proprietary solutions and supply chains.

Building on existing standards

Challenges arise from RFID's pervasive use in highly disparate areas, including ports, health care, financial services, networks, audio-visual, biometrics, personal identification, databases, home electronics, printing, intelligent transportation systems, industrial automation, anti-counterfeiting and what is commonly referred to as "the" supply chain (where, in truth, there are many).

A search of the ISO database reveals some 240 standards that include "security" in their title. We clearly need to build on existing security standards to provide:

- A common, harmonized framework for a more secure supply chain, for example in health care and port security where the risks are too high to ignore
- A base of transparency and privacy for consumers
- Technical guidance for policy makers addressing these issues.

If the technology is to become as ubiquitous as the promise appears today, it is imperative for the RFID community to develop comprehensive solutions for both security and privacy. SC 27 and SC 31 are working hard to provide those solutions. ■

1) Currently under development.

About the authors

Matthew J. Harmon is the Vice President of Security and Risk Management at QED Systems, and he serves as the US Technical Advisory Group Chair for ISO/IEC JTC 1, *Information technology*, subcommittee SC 31, *Automatic identification and data capture techniques*, working group WG 7, *Security for item management*. He is also the SC 31 liaison to ISO/IEC JTC 1/SC 27, *IT Security techniques,* and a member of the ISO Technical Management Board Privacy Steering Committee.

Natascha E. Shawver is a freelance journalist with a focus on the societal effects of information technology. She holds a Masters Degree in political science from the University of Heidelberg, Germany and a journalism diploma from the Free Journalism School in Berlin, Germany.