Editors: Ramaswamy Chandramouli, mouli@nist.gov
Tim Grance, tim.grance@nist.gov
Rick Kuhn, kuhn@nist.gov
Susan Landau, susan.landau@sun.com

Security Standards for the RFID Market

Ted Phillips
Booz Allen Hamilton

Tom Karygiannis and Rick Kuhn
US National Institute of Standards and Technology

Originally viewed as essentially remotely-readable bar codes, radio frequency identification (RFID) technologies have been available for many years. However, RFID technology recently gained widespread public attention when European retailers such as Great Britain's Marks & Spencer and Germany's Metro Group began experimenting with passive RFID tags embedded in individual consumer products, and the US Department of Defense and Wal-Mart announced moves to use passive RFID tags for shipment tracking. Other large retailers followed suit, suggesting that RFID technology will become nearly universal for shipment tracking in the next few years. As RFID tags continue to decrease in price while offering increased capabilities, consumers are encountering them in library books, high-end electronics, automobile tires, and packaging for household items. Efforts are currently under way within the industry that could provide unique identifiers for every individual item in the retail supply chain. As further evidence of RFID's growth, the industry's standards consortium, EPCglobal, recently awarded Verisign a contract to manage the Object Naming Service (ONS), which will serve as the root directory for the EPCglobal Network, a system that combines passive RFID technology with electronic product codes (EPCs) to enable business partners to exchange information throughout their supply chains.

RFID has also attracted the attention of security researchers and hackers. During the 2004 BlackHat conference in Las Vegas, Lukas Grunwald and Boris Wolf released RFDump (www.rf-dump.org), an open-source tool that allows anyone to read RFID tags designed to the ISO 15693 and 14443 standards as well as proprietary standards used in some smart-card financial transactions. In 2005, researchers at Johns Hopkins University also demonstrated that an inexpensive toolkit built with a minimal amount of customized hardware can brute-force cryptographic keys from one of the most widely sold RFID tags.[1]

It's all about the application

It's not an easy task to design, engineer, implement, and optimize a complex RFID system. When a passive RFID tag moves down a conveyor belt at 20 miles per hour, for example, it has only a split second to capture and use as much power as possible from reader devices that can be more than 10 centimeters away. Thus, the RFID system selected for this type of application will depend on the user's requirements. Some applications, however, require higher power demands and a lower tolerance for latency, so the RFID systems' available power, amount of onboard data storage, radio frequency, and security requirements will vary.

For example, let's say a rancher needs to identify and track individual cattle from the ranch to the processing center. Given that cattle tend to chew off ear tags while in the feedlot,

Introducing Emerging Standards

IEEE Security & Privacy announces the formation of a new department for the magazine—Emerging Standards. Tim Grance, Ramaswamy Chandramouli, and Rick Kuhn, of the US National Institute of Standards and Technology, and Susan Landau from Sun Microsystems, are the co-editors of this department, which will concentrate on security issues arising from deployment of new technologies, with a focus on security standards and research challenges. As systems are deployed, security issues must be addressed—not only for the new technology, but also for the technology's interaction with existing/legacy products and services. This department will highlight security challenges and solutions in the engineering and operation of new technologies as well as significant security concerns in existing technologies and applications. Topics include security solutions that are still evolving and areas where new algorithms are required to address vulnerabilities of existing security solutions. Contributions are welcome on these and other topics related to emerging technologies.

Types of RFID technology

Radio frequency identification (RFID) technology can be divided into two main categories:

- *Passive* systems, such as those used in gasoline station point-of-sale systems and building access control systems, contain no onboard power source. Tags receive their operational power from RFID reader devices. The tag's antenna captures the radio frequency (RF) energy from the reader, stores it in a capacitor, and then uses it to power the tag's logic circuits. After completing the requested commands, the tag uses the capacitor's remaining energy to reflect or backscatter a signal to the reader on a different frequency.
- *Active* systems use tags with onboard power sources, such as batteries. These tags are used for applications such as tracking cargo and collecting tolls electronically. Active tags can support more sophisticated electronics with increased data storage, sensor interfaces, and specialized functions. In addition, they use their batteries to transmit signals back to the RFID reader.

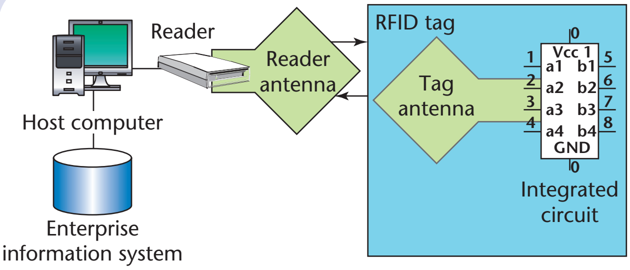

Figure A. A radio frequency identification system. Such systems incorporate RFID readers, host computers to control the readers, and back-end enterprise information systems to implement business rules.

As Figure A shows, an RFID system includes more than just the tag. Advanced security in RFID tags requires additional electronic components to support cryptographic processing, random number generators, key management functions, and other security-specific features. This increases the amount of energy the tag consumes and increases the latency and transaction times. Passive tags that support security functions must stay within the tag reader's electromagnetic field longer than simpler tags. For active tags, security features result in slower read times and potentially shorter battery life. Advanced RFID tags, including some with anti-tamper properties, are also finding their way into supply-chain applications, especially in international commerce and the pharmaceutical industry.

The complexity of the RFID market provides a large variety of security features in commercially available tags. However, security features aren't implemented in a consistent and interoperable manner among different RFID technologies.

many ranchers now use implantable low frequency (LF) tags enclosed in glass capsules because they're less susceptible to attenuation from water and living tissue than ultrahigh frequency (UHF) tags. Such a tracking application requires RFID tags that can be securely attached or implanted in the animals, read through the skin from a relatively close distance to minimize multiple reads, and have limited onboard storage. In most cases, these requirements narrow the RFID tag selection down to a single product category—an encapsulated, LF transponder that has limited read/write capability as specified by the ISO 11784 and 11785 standards. ISO 11784/5 transponders allow easy reprogramming of ID codes, however, and therefore provide insufficient security for applications such as tracking endangered species or high-value show animals. Standards for animal-tracking RFID tags that meet more demanding security requirements are now in development.

Policy concerns

Recognizing the growing concerns of consumers and privacy advocates, as well as the relative weaknesses of existing RFID security mechanisms, lawmakers have started to explore ways to protect consumer privacy. For example, the Identity Information Protection Act of 2005—a bill introduced in the California legislature in 2004—proposed some of the first privacy regulations on the use of RFID technology. Although businesses would've been able to use RFID to collect the information already available from bar codes—product identification codes and serial numbers, for example—they wouldn't have been able to use the technology to track customers once they left the store. The act also would've established a temporary moratorium on embedding RFID in drivers' licenses and outlawed surreptitious interception of RFID signals. Responding to privacy concerns, the American Electronics Association convinced legislators in September 2005 to set the bill aside for at least a year while RFID security and privacy technologies improved. Manufacturers recognize that market success depends largely on their ability to convince consumers and legislators that RFID products will preserve privacy while improving efficiency for retailers.

Businesses that implement RFID security based on proprietary standards, such as those used in the point-of-sale systems, potentially introduce risk to their business and customers because the "security through obscurity" approach almost always yields solutions that are easily compromised. Fortunately, the RFID industry is actively developing international standards to meet these security needs, such as incorporating the Advanced Encryption Standard (AES) and designing advanced authentication techniques into some of the most extensively used RFID systems.

Current RFID standards

RFID technology is exceedingly diverse: more than 500 tag types are commercially available, including passive, semi-passive, active, semi-active, LF, HF, UHF, microwave, onboard sensors, ruggedized housings, and implantable. As RFID technology evolves, standards are showing an interesting interplay between cost and security. RFID applications fit roughly into three categories:

- *logistical* applications that require fast, low-latency, easy-to-read tags with little or no need for security mechanisms, such as those used for shipping and receiving;
- *consumer* applications that require security, but not bulk-reading capabilities, such as smart cards used in financial transactions; and
- *vertical* applications that tailor security features to a specific business process, such as the use of RFID-enabled poker chips in casinos.

As RFID tag and infrastructure costs have declined over the past decade, the potential range of RFID applications has expanded, making it economical to embed RFID tags in all sorts of consumer items. As a result, we now need tags with both bulk-reading capabilities and security features that protect consumer privacy. In addition, there continues to be a sizeable market for RFID systems with semi-custom or highly tailored security mechanisms.

Yet, the addition of security mechanisms doesn't come without potential trade-offs. Data encryption not only increases a tag's cost, it reduces the tag's onboard storage capacity and increases the latency of read cycles. Authentication adds latency to the read/write process and introduces key-management overhead. Other security measures, such as those designed to protect data integrity, have similar effects. The overall impact could be to reduce the number of tags read per second in crowded environments such as warehouses, or increase the time per read in high-speed conveyor belt systems.

As RFID technology and standards continue to evolve, users will place an increasing emphasis on the availability of security features in the products they implement. Table 1 highlights the technical and security features of some important RFID standards. Several technical features have a direct effect on security, such as frequency band, read range, and onboard data capability. In addition, most of the RFID standards have defined one or more security features that provide confidentiality, integrity, or availability services.

EPC tags

EPC tags are used for supply-chain and logistical applications—to follow razors on the journey from factory to store, for example—because they're simple and cheap. The engineers who wrote the EPC standards were focused on producing low-cost, low-latency tags with high potential read rates that supported tag singulation (separating one tag from a large quantity of tags). A critical design factor was the physical tag configuration—these tags could be built on flexible substrate material and laminated into smart labels. Security of EPC tags wasn't initially a high priority. Thus, first-generation EPC tags lack the computational resources for strong cryptographic authentication. Like all passive RFID tags, first -generation EPC tags draw power from radio signals emitted by tag readers. EPC tags don't have internal clocks, and can't perform any operations independently of tag readers. As a result, they can't devote much computing power to security operations—at most, 2,000 gate equivalents. In contrast, common Data Encryption Standard (DES) implementations require tens of thousands of gates, and even lightweight AES implementations require approximately 5,000 gates,[2] which puts them both out of range for today's first- and second-generation passive EPC tags.

Consumer fear over the prospect that RFID technology could be used to surreptitiously read the product IDs of everything they've purchased,[3] along with pressure from privacy advocates, led to the inclusion of the `kill` command in the EPC standard. This command, when sent to a single tag by a reader service, renders it permanently inoperable. The majority of the logistics community opposed the command's inclusion because of its potential for unauthorized system disruption, but EPCglobal included it in the Generation 1 and Generation 2 standards to protect consumer privacy. Executing the `kill` command on individual Generation 1 EPC tags is relatively simple—it's protected by only an 8-bit password and no key-management infrastructure is available. Indeed, making the situation worse, some major retailers reportedly ordered millions of tags configured with the same password. The EPC Generation 2 standard, which will be implemented in the first half of 2006, requires longer passwords for protecting the command, but there's still no key-management function.

Smart cards

In contrast to EPC tags, the security features in RFID-enabled, contactless smart cards, which were driven primarily by the banking community's needs for protecting wireless payment systems, addressed security issues from the beginning. Nonetheless, power issues are a significant concern for the RFID technology used in contactless smart-card transactions. Passive smart cards (following the ISO 14443 and 15693 standards) have implemented secu-

Table 1. Radio frequency identification security features.

TECHNOLOGY	TECHNICAL FEATURES			SECURITY FEATURES		
	BAND	RANGE (METERS)	DATA	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
EPC Class 0/0+ (supply chain)	Ultrahigh frequency (UHF)	3	64- or 96-bit with read/write (R/W) block	None in standard.	• Parity bit. • CRC error detection.	Identification rate >1,000 tags/sec.
EPC Class 1 Generation 1 (supply chain)	UHF	3	64- or 96-bit with R/W block	None in standard.	• Commands have 5 parity bits. • CRC error detection.	`Lock` command permanent and not protected.
EPC Class 1 Generation 2 (supply chain)	UHF	3	R/W block	• Masked reader-to-tag communications using the one-time pad stream cipher. • Tags addressed by 16-bit random numbers.	• CRC error detection.	Numerous readers can operate in dense configurations.
ISO/IEC 18000-2 (item management)	Low frequency (LF)	< .010	Up to 1 Kbyte R/W	• No protection on the `read` command. • “Reader talks first” protocol. • No encryption or authentication.	• CRC error detection. • Permanent, factory set 64-bit ID. • Optional, lockable identifier code.	None in standard.
ISO/IEC 18000-3 (item management)	High frequency (HF)	< 2	R/W	• “Reader talks first” protocol. • 48-bit password protection on `read` commands. • “Quiet mode” in which tags won’t respond to readers.	• CRC error detection. • No `write` protection in Mode 1. • Mode 2 has 48-bit password on `write` commands.	Multiple tag modes are noninterfering.
ISO/IEC 11784-11785 (animal tracking)	LF	< .010	64-bit identifier	• “Reader talks first” protocol. • Tags addressed by 16-bit random numbers. • Quiet mode.	• Retagging counter. • CRC error detection.	None in standard.
ISO/IEC 10536 (contactless smart cards)	HF	< 2	R/W	• “Reader talks first” protocol. • Masked reader-to-tag communications. • Tags addressed by random number. • Quiet mode.	• CRC error detection.	• Probabilistic/slotted random anti-collision algorithm. • Multiple tag modes are noninterfering.
ISO/IEC 15693 (vicinity smart cards)	HF	1.5	Up to 1Kbyte R/W	• No protection on the `read` command. • No onboard encryption or authentication.	• Optional protections on `write` command. • Error checking on air interface.	Optional password protection on the `lock` command.

rity features, including cryptographic challenge–response authentication, for years. Newer releases of these cards include the 128-bit AES, triple-DES, and SHA-1 algorithms. As a result of the increased overhead, the smart cards must be placed close to their readers for relatively lengthy periods to be read. Despite these advanced security features, the privacy and security threats to these cards are still significant. Government and industry will continue to refine the risk-mitigation strategies for these cards over the coming years.

Few RFID smart cards on the market are built around “pure” standards-based implementations. Most vendors use the basic standard suites as starting points for developing their products and then extend them with proprietary features tailored for specific vertical applications. For instance, Philips’ Mifare technology, which is used extensively in Europe for access to mass transportation, is built around the ISO 14443 air link standard but is supplemented with a proprietary data format and security features.

Interoperability is also a concern for devices using RF. Some of the unlicensed frequencies used for RFID in the US are used for mobile phones in Europe and Asia, for example. Conformance testing and certification are essential for reducing interoperability problems with any standard, even with the development of multiprotocol, frequency-agile reader devices. Most RFID testing is conducted under the auspices of relevant industry groups. For example, new ISO/International Electrotechnical Commission (IEC) 14443 contactless smart-card platforms might receive MasterCard certification for use in e-commerce. EPCglobal has recently contracted with third-party laboratories to conduct conformance testing for Generation 2 EPC standards. At the same time, EPCglobal has established a working group to submit the EPC Generation 2 protocols for ISO standardization (ISO 18000-6c). Ironically, one risk of international standardization is that a protocol might be modified as it moves through the process, so the EPC group will try to maintain consistency with the current specification.

As the RFID market expands, we'll see the continued proliferation of RFID tags built for highly specialized vertical markets, which means greater variety and the consequent need to ensure interoperability. A great deal of research and development is currently under way in the RFID security field to mitigate both known and postulated risks. Manufacturers, business managers, and RFID systems engineers continue to weigh the trade-offs between chip size, cost, functionality, interoperability, security, and privacy with the bottom-line impact on business processes. In the coming months, security features supporting data confidentiality, tag-to-reader authentication, optimized RF protocols, high-assurance readers, and secure system engineering principles should become available.

Security and privacy in RFID tags aren't just technical issues; important policy questions arise as RFID tags join to create large sensor networks and bring us closer to "ubiquitous computing." With public attention focused on the RFID landscape, security and privacy have moved to the forefront in RFID standards work, and the results will be worth watching. □

Acknowledgments

Certain commercial entities, equipment, or materials may be identified in this article in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the US National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

References

1. S.C. Bono et al., "Security Analysis of a Cryptographically-Enabled RFID Device," *Proc. 14th Usenix Security Symp.* Usenix Assoc., 2005, pp. 1–16.
2. O. Günther and S. Spiekermann, "RFID and the Perception of Control: The Consumer's View," *Comm. ACM,* vol. 48, no. 9, 2005, pp. 73–76.
3. A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols," *Advances in Cryptology: Proc. 25th Int'l Cryptology Conf.*, LNCS 3126, V. Shoup, ed., Springer-Verlag, 2005, pp. 293–309.

Ted Phillips *is a senior associate at Booz Allen Hamilton. His research interests include RFID engineering, supply-chain automation, and information security. Phillips has an MS in telecommunications from Virginia Commonwealth University. He is a member of the International Society of Logistics Engineers and EPCglobal. Contact him at phillipsted@bah.com.*

Tom Karygiannis *is a senior researcher at the US National Institute of Standards and Technology. His research interests include wireless security, ad hoc networks, and mobile commerce. Karygiannis has a PhD in computer science from George Washington University. Contact him at karygiannis@nist.gov.*

Rick Kuhn *is a computer scientist with the US National Institute of Standards and Technology. His research interests include information security, software verification and testing, and empirical studies of software failure. Kuhn has an MS in computer science from the University of Maryland at College Park. He is a senior member of the IEEE and the IEEE Computer Society. Contact him at kuhn@nist.gov.*