How Secure Is RFID?

Sixto Ortiz Jr.

Radio frequency identification technology, of minor importance in the marketplace not long ago, is surging in popularity and finding use in a growing number of applications.

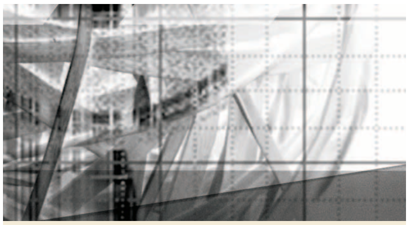
Vendors are using RFID in place of product bar codes in stores, in employee identification badges for building access, in car keys to enable vehicle startup, and even to identify lost or stolen pets.

In the near future, the technology might become part of more high-profile applications, such as passports, credit cards, airport luggage-tracking systems, and hospital badges used to identify patients and the medications and dosages they require.

Despite RFID's growing profile, some researchers worry that potential security problems could cloud the technology's future, particularly as it is used for more critical purposes. There are concerns that hackers could tamper with or steal RFID data, such as product prices or patients' or credit-card holders' private information.

"The security of today's systems is appallingly bad," said Peter G. Neumann, principal scientist at the Computer Science Lab at SRI International, a research institute. "There are many potential risks in the use of RFID tags."

RFID is subject to the same complexity-related security problems that have affected the entire IT industry, added Vrije Universiteit PhD student and researcher Melanie Rieback.



However, many of the vulnerabilities flagged by skeptics either don't exist in most real-world implementations or could not be practically exploited by hackers, said Dan Mullen, president of the Association for Automatic Identification and Mobility (AIM), an RFID industry consortium.

Meanwhile, proponents say, they are always making the technology more secure.

RFID PRIMER

The technology behind RFID has been in use since World War II, when the British used it to identify whether planes belonged to "friend or foe."

Work on the technology continued, and in 2004, vendors began pilot projects using RFID tags on products and supplies to store pricing- and inventory-related information, said Bert Moore, AIM's director of communications and media relations.

Large institutions, such as the US Department of Defense, have since implemented RFID, which is now spreading to other organizations and industries.

How it works

RFID systems consist of small radio chips in tags placed on items, as well as readers that can recognize the emitted signals. Most commercial RFID chips, such as those used in place of bar codes on products in stores, are passive emitters and thus have no onboard power source. They send a signal over a range of several feet when a nearby reader activates them.

Active emitter chips, like those used in automatic highway toll-paying devices that let drivers pass through collection booths without stopping, have their own batteries and thus can send signals up to about 300 feet to readers.

RFID transceivers, such as the one that Figure 1 shows, are tiny, resource-constrained computers. In passive systems, they detect a signal arriving from a reader, power up the tag, send a reply, and store a small amount of data. The amount of storage depends on the usage, varying from a few bits for applications such as a small store's inventory-control system to multiple kilobits for applications such as a large business supply-chain system.

The readers perform various functions, like simply displaying data such as a product's price, acting on data such as admitting a person to a building, or communicating with a back-end application such as a toll system's database.

The data in some RFID tags, such as those used to store product prices, is read-only. Other tags are read-write, so information can be stored as the need arises. For example, this type of system could write location and other information about a product to a tag as it moves through a supply chain, explained Jack Brandon, manager of business development for Socket Communications, a vendor of data-collection and network-connectivity products for mobile devices.

Advantages

Because RFID is simple, it is generally inexpensive, which is practical for use in high-volume settings such as stores and warehouses.

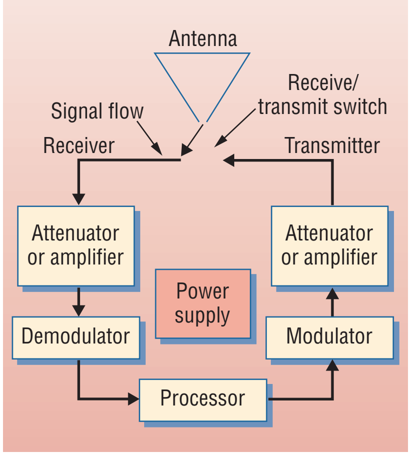


Figure 1. An RFID tag consists of a radio transmitter and receiver, an antenna, a processor, a modulator and a demodulator to put data onto and remove data from signals, attenuators, or amplifiers to modify or strengthen signals, and sometimes onboard power sources.

In addition, the technology transmits signals through materials such as cardboard, making it good for merchandise tracking, added Joe Melo, RFID product manager for vendor Psion Teklogix.

SECURITY ISSUES

Even though RFID chips have little memory, they can send malicious data to unsecured back-end databases and other systems that are susceptible to common attacks such as viruses, buffer overflows, and denial-of-service (DoS) assaults, said Vrije Universiteit's Rieback.

"Of even greater concern can be the lack of definitive binding between the tags and the objects they purportedly correspond to," added SRI International's Neumann.

For example, he said, terrorists or smugglers could switch tags or disable one tag and add another to evade future RFID-based airport luggage-scanning systems.

Edith Cowan University: DoS attacks

Edith Cowan University's School of Computer and Information Science Security Research Group says it showed how hackers could launch DoS attacks against some types of RFID systems, including those in which tags communicate via frequency-hopping spread-spectrum modulation.

FHSS entails the repeated switching of frequencies during transmission, which reduces interference and makes intercepting signals more difficult.

The Edith Cowan researchers used RF jamming, which sends signals across the entire spectrum range in which an FHSS-based RFID system functions, explained university lecturer Andrew Woodward.

This technique continuously sent signals to an RFID tag, which left it unable to respond to or communicate with legitimate traffic.

Vrije Universiteit: viruses

Security experts have not reported finding any RFID viruses in the wild.

However, researchers with Vrije Universiteit's Computer Systems Group say their work indicates hackers could create viruses and embed them in RFID tags. A reader could encounter the tag and transmit the data to the application that uses it. The viruses could then exploit application vulnerabilities and cause a buffer overflow or some other problem that could infect a back-end system with the malware.

"If improperly secured," Rieback said, "back-end systems … could execute malware as code."

For demonstration purposes, she noted, the researchers didn't experiment with actual RFID systems but instead replicated them in software. They also created a proof-of-concept, self-replicating RFID virus that inserts malicious Structured Query Language code into a database.

According to Rieback, RFID tags, even with their small memories, could easily transport the small amount of code—some commands are a single word—typically needed for SQL injection attacks.

Once a database is infected, Rieback noted, RFID applications that access its information could write the malware into other tags and thereby propagate the infection.

According to Rieback, the Vrije group made its findings public to encourage RFID designers to use secure programming practices. She said some designers have been reluctant to acknowledge their products' vulnerabilities. However, she added, others have privately sought her research group's help.

Rewriting tags

Hackers with the proper equipment could record data from an RFID chip that is on an inexpensive product and upload the data to a chip that is on an expensive product, thereby getting the latter for a lower price, noted Lukas Grunwald, a consultant with DN-Systems Enterprise Solutions, an information-security consultancy.

Grunwald developed the RFDump application, which runs on a mobile device and reads and writes data to and from RFID tags.

Such programs could find their way onto the Internet and become available to hackers, he said.

Stealing cars

Many new cars won't start unless an RFID reader, called an *immobilizer*, detects the encrypted RFID tag embedded in the owner's key. When someone inserts a key into a car ignition, the immobilizer sends a "challenge," in the form of encrypted data, to the tag, which then must send a required "response" using the same cryptographic key. If the tag responds properly, the immobilizer lets the vehicle's fuel-injection system operate.

A hacker could use an electronic cloning device—which consists of an antenna and modulation/demodulation routines that can intercept, record, and manipulate RFID signals—to eavesdrop on transmissions between the RFID tag on a car key and an immobilizer. The cloner would then extract the car key's required response and obtain the encryption key, which, if weak enough, the hacker could break via a brute-force attack.

The thief could then demodulate, replicate, and store the response and subsequently broadcast it via a software radio to steal the vehicle.

Cloning implanted RFID tags

Implantable RFID tags are used for applications such as smart cards, like those in badges that give employees access to a building. The tags are also used in small devices that let a driver pay for gasoline by simply waving the device near a pump.

However, researchers at Johns Hopkins University's Information Security Institute and at RSA Laboratories have demonstrated that hackers could clone implanted tags in much the same way that thieves steal RFID-protected vehicles.

Hackers could use cloners to intercept a tag's digital identification signature, which the chip transmits along with data. The hacker could then crack the encryption and use a software radio to simulate the legitimate tag, thereby fooling the reader.

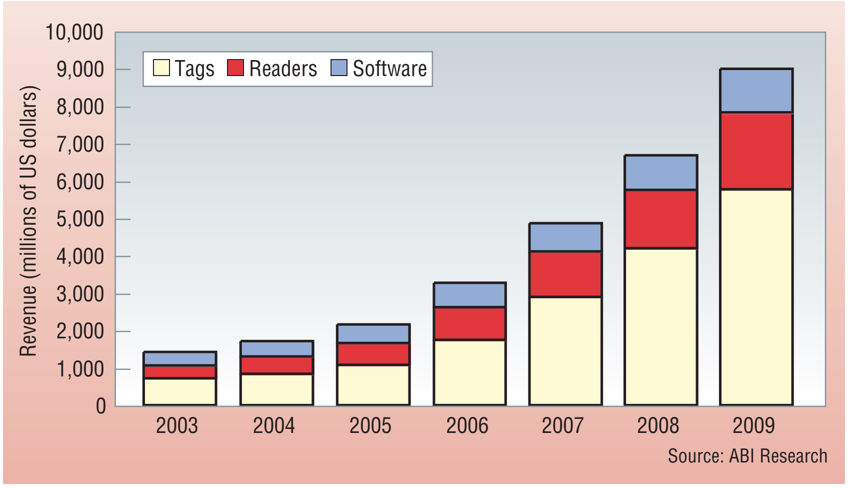
RFID INDUSTRY RESPONSE

The RFID industry says it has built numerous security features into its products.

For example, some systems include encryption to limit signal theft. To do this, developers add encryption algorithms and routines to the APIs that program the tags.

However, this adds cost, noted Psion Teklogix's Melo. Thus, he noted, systems deployed for purposes such as product tracking don't include encryption because users don't consider the information that the tags contain to be valuable enough to steal.

Some RFID tags have writable memory that users can lock. This approach is designed to keep hackers from writing malicious data to tags. However, many users might not lock the memory because they either don't know how or don't want to spend the time necessary to do so.



Source: ABI Research

Figure 2. Global revenue from RFID-related sales grew steadily during the past three years and is expected to continue doing so during the next three years.

Generally, tags have such a small memory capacity, implanting all but the smallest viruses would be difficult, explained Kevin Ashton, marketing vice-president for RFID vendor ThingMagic.

"In addition," he said, "RFID tags do not execute code, malicious or otherwise; they just store data."

Moreover, RFID systems are designed to verify that data read from tags matches predefined parameters such as the proper number of digits in a product code, said AIM's Mullen. Thus, he said, it is unlikely a hacker could infect a system via malware copied into a tag's memory because the code probably wouldn't fit the necessary format. In this case, the reader would ignore the code.

Researchers claim they can get a system to at least transmit malicious code to back-end applications. According to Ashton, researchers did this only by creating vulnerabilities in their experimental systems that are unlikely to occur in commercial RFID systems.

Also, he said, hackers would need inside information—such as the data formats with which a reader works or how an RFID application interacts with a back-end database or reader—to plant a hostile program in an RFID system.

However, said Vrije Universiteit's Rieback, if the RFID industry really believes its systems are immune to attack, they should allow researchers to test them via simulated attacks. Other software vendors have done this, she noted, offering a reward for defeating an application's security, and this has improved their products.

Market statistics indicate the RFID industry will continue growing rapidly. As Figure 2 shows, ABI Research, a market-analysis firm, predicts global RFID revenue will surge from $1.42 billion in 2003 to $8.98 billion in 2009.

"As RFID deployments grow and reach consumer-level applications, new security measures will be required," contended ThingMagic's Ashton. He said some new RFID programs will contain highly sensitive information that must be protected vigorously. These applications will require measures such as stronger encryption or passwords, he explained.

According to Vrije's Rieback, sound software-development techniques will help make RFID more secure. ■

Sixto Ortiz Jr. is a freelance technology writer based in Spring, Texas. Contact him at sortiz33@houston.rr.com.

Editor: Lee Garber, *Computer*, l.garber@computer.org