

Security Risks With RFID

Companies need to protect their data by ensuring that the RFID technology they adopt supports their corporate security policies.

May 16, 2005—Radio frequency identification technology has proven to be reliable, especially in supply chains, and is already showing tremendous benefits. But an automated supply chain mandates the necessity for data privacy, identity and non-refutability, and organizations should ensure the RFID technology they adopt supports their security requirements. Companies need to be aware of the security risks, such as profiling, eavesdropping, denial of service attacks and inventory jamming.

Currently, there is a tremendous push for consolidation of RFID technology with regards to capability. Yet, with multiple standards and developers seeking to gain the upper hand through their own intellectual property, many businesses are adopting the technology before it is fully ripened, which includes any unresolved issues surrounding security. Companies should be able to query tags securely while unauthorized parties should not be able to trace them. Unfortunately, Generation 2 tags have yet to be subject to the same rigorous, open and mathematically provable security analysis that has encouraged the explosive growth of Web-based transaction services.

The Privacy Debate

The possibility that a business could lose control of the privacy of its information is one of the largest risks associated with RFID. For example, the potential exists for tag "sniffing" of a running production line from the parking lot. Like Ethernet networks, wireless tag communications are subject to capture and analysis. With all but the strongest data security algorithms subject to successful brute-force cracking using portable or networked computing resources, the cryptographic capabilities of tags becomes an important consideration in their selection.

The information inside RFID tags is vulnerable to alteration, corruption and deletion. The first question to be answered is how vulnerable the tag data is. Tag security can be expressed in terms of the strength of the cryptography employed, the processing speed of the tag and the amount of time it takes to establish a secure channel of communication with that tag. Compromising the security techniques employed in an effort to reduce tag complexity—and cost—yields tags whose mean time to "crack" is measured in mere minutes.

The security of information between RFID tags and readers is only now being strengthened to meet commercial needs with Gen 2 tags. Tags that present surmountable barriers for compromise represent a potential supply chain disruption opportunity. In the extreme, such disruptions might include the purposeful re-programming of tags to reflect errant weight, quantity or size information. Companies that select a weakly secured tag give competitors a low-cost opportunity to passively gain details about their suppliers, quantities on-hand, inventory turns, shifts in product mix and product destinations (customers).

Education Is the Best Policy

Education is the best way a business can ensure it understands the limitations and risks associated with RFID. Businesses should not assume that the risks are small because the RF footprint of current generation tags is constrained. Understanding the mean time to crack—access, alter or deny the use of—the tags is a prerequisite

to ensuring that tag selection embodies the objectives of the company's corporate security policy. RFID technologies and those that draw power by the kilowatt in server rooms present challenges and needs similar to those of the company's IT system; each is subject to multiple attack vectors, and each should be sufficiently and provably resistant to attack. Seeking the assistance of certified auditors may be the most cost-effective way to gain an initial understanding of the risks and means to mitigate them.

Data encryption can be employed to ensure the tag information is secure or, in the worst case, recognized as having been altered. Strong cryptographic techniques are typically deployed to ensure data privacy, proof of originality and non-refutability of the information conveyed. Aside from computational load, it is not more difficult to track the encrypted information and gain a degree of security within the bounds of a factory or warehouse environment. But this scenario gets more complex when the tagged item needs to transfer from one party to another. In this case, each party must agree on the format of the information and the encryption techniques used. In the four-way balance between security, interoperability, convenience and cost, security is often compromised for cost containment.

Many organizations accept risk, but those that strive to maintain their competitive advantage implement policies and make technology choices based on a comprehensive risk-benefit analysis. For example, embracing a "slap-and-go" use of RFID tags rather than fully integrating them into the supply chain process can be viewed as both an expression of financial and technical risk mitigation. Financially, not all firms are up to the task of integrating tags into their production and inventory management systems. Technically, previous-generation tags may not meet the company's IT security policy. But applying tags in a slap-and-go fashion does little to protect the entire supply chain. Companies are still at risk to disruptions should their customers find the tag-based inventory management in chaos due to intentional data disruption.

The Next Generation

RFID technology is continually advancing. Gen 2 tags offer deeper data sets and stronger cryptographic techniques improve the resistance of the on-board data to brute-force recovery, yielding tags that are statistically and significantly less likely than past generation tags to individual tracking and data compromise. Better radio transceivers are less susceptible to remote attack. Paying careful attention to the techniques employed by each tag vendor to achieve specific, provable and verified security results is a necessary precursor to insuring that the RFID tag chosen will not present a risk footprint greater than what the balance of the organization is willing to accept.

Some may choose to disregard the security risks associated with RFID technology until a significant event occurs. Business can be a bruising experience if technology choices are based primarily on cost. The alternative is an eyes-wide-open approach regarding the choice of RFID technology, with adoption based on that which most completely embodies the company's financial and security goals.

Darren Suprina is chief security architect at [Innovativ](#), a business and technology systems integrator, where he develops new initiatives that leverage organizations' needs for security, data management and wireless access. To comment on this article, click on the link below.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved