

# Securing the RFID Revolution

Until encryption methods are employed to protect tag data, RFID will continue to face challenges in the marketplace.

March 27, 2006--The RFID revolution is upon us, and with it come concerns over the issue of how to insure security and privacy for captured data. In 2006, the market for RFID-related products is projected to reach \$2.71 billion, according to [IDTechEx](#). When Mario Cardullo received the first patent for a passive, read-write RFID tag on January 23, 1973, he envisioned many of the uses we have in place today (see [Genesis of the Versatile RFID Tag](#)). He also ran into the first incident of concern regarding security issues.

RFID represents another form of wireless technology and communication, which has become ubiquitous in our lives. One of the most daunting challenges facing IT organizations today is how to guarantee the security of wireless communication. RFID offers similar challenges but with an important difference. While most wireless technology is intentionally closely held, encrypted and protected, RFID only works when it can be easily read. This important difference doesn't preclude RFID companies from attempting to circumvent the issue through increased security measures, but it certainly creates a dilemma.

The challenge becomes one of using captured data for the purpose of consumer marketing, while at the same time keeping that data confidential. Once the information from a reader is captured and enters an organization's system, it falls under the same security guidelines as all other captured communication. The data is typically transmitted via wireless communication, setting up a point of failure for security. This typical wireless issue can be resolved by the use of encryption. However, a greater problem occurs *prior* to this data capture.

When a consumer item is in transit, being unloaded or being purchased, its tag's data is available to anyone interested in reading it. Since RFID tags and interrogators need to be standardized (proprietary tags and readers defeat the purpose), anyone with an interest can access the data. More importantly, the information can be stolen and reused. There are a myriad of documented reports of hackers breaking the codes on RFID applications. Among them are such high-profile incidents as the cracking of the [Exxon Mobil Speed Pass](#), when hackers purchased gas with a simulator (see [Attack on a Cryptographic RFID Device](#)); and the claim by [Delft](#) smartcard security specialist [Riscure](#) that it succeeded in breaking the encryption key in a Dutch passport's embedded RFID tag and accessed the biometric information stored on the tag.

Think of the implications of violating compliancy and privacy laws if embedded information about a person were to be stolen—not to mention the issue of identity theft.

In a [U.S. Government Accountability Office report](#) published in May 2005, issues surrounding security and privacy raised concerns to a new level. The report states, in part, "Without effective security controls, data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users."

Although there is a faction within the RFID community that tends to downplay the issue, stating it is no different than other wireless challenges, the truth is that RFID is a unique technology and the industry must

solve this dilemma that threatens widespread implementation. This does not mean RFID is at risk, or that adoption of the technology will slow its pace. Rather, organizations, manufacturers and vendors have to stop sticking their heads in the sand when it comes to security issues related to RFID applications.

Encryption methods can be employed successfully to insure that RFID data is secure. Cost is a factor in encrypting tags, however, to the extent that the data embedded on them is not easily read. Another big obstacle to widespread adoption is the cost of implementation. As costs decrease for the tags and readers, more money will be spent on securing the data they embed. Widespread adoption will then follow. But until this happens, RFID will continue to face challenges in the marketplace. Stay tuned.

*Ray Cavanagh is president of Cavanagh Consulting Group, which helps businesses select and implement security solutions specific to corporate compliance, network security and RFID.*

Copyright ©2005 RFID Journal, Inc. All Rights Reserved