

Forrester Says RFID Security Falls Short for Some Apps

Companies deploying RFID for payments or other applications requiring strong security are taking risks today, the research firm reports, while users of RFID in small-scale, standalone tagging systems for supply-chain apps are less vulnerable.

By Mary Catherine O'Connor

Sept. 23, 2006—End users of RFID technology are getting mixed messages regarding data security. RFID vendors claim their products are secure, while media reports and researchers sing a different tune: that currently deployed passive RFID systems are prone to eavesdropping and other attacks, and that vendors have to do some important work to bolster data security. In a newly published report by market-research firm Forrester, lead author and senior analyst Paul Stamp concludes that with respect to data security, passive RFID tags and readers as they are currently designed are only appropriate for a limited number of scenarios. “Like any new technology,” the report states, “companies need to balance efficiencies gained from the system against the security and operational risks that RFID introduces.”

Forrester researcher Jen Albornoz Mulligan says that in gathering information and insights into RFID system security, she talked to a number of RFID vendors and data-security firms, a couple of end users of passive RFID technology who are using it for supply-chain optimization and a few academic researchers. “The end users I spoke with didn’t know much about the security issues related to RFID systems,” she says, noting that none of them are encoding sensitive data to the tags they issue.

The current levels of data protection for RFID tags are sufficient with regard to basic slap-and-ship applications of RFID for improved supply-chain visibility, the report says. However, users who want to encode sensitive data to tags, or to store that data in RFID middleware integrated into a company’s back-end IT systems or shared with trading partners, could be taking serious risks. “RFID technology is not mature enough yet to protect your company secrets,” it says.

The report, entitled “Anyone Who Says RFID Is ‘Completely Secure’ Is Selling Something,” describes the main areas of vulnerability within an RFID deployment and provides recommendations in the form of steps companies should take to protect data. The same types of attacks to which any type of database is vulnerable could be levied against RFID middleware, it warns. To secure middleware, the authors urge developers to use secure coding practices and filters that ensure that tag data sent to the middleware is not corrupt. According to the report, as companies begin to integrate RFID software and databases into their enterprise software, and to trade tag data with supply-chain partners, a “corrupt back-end database could wreak havoc on an entire supply chain, negating any efficiency that the RFID system originally provided.”

The report suggests RFID users develop business processes within their RFID deployment that include steps to have employees check the presence and condition of tags attached to products, rather than fully automating the system so that no one checks them. It also notes that RFID tags themselves can be tampered with, rather than just read by unauthorized parties. Thus, it recommends that if RFID tags are used as security tools in a

retail environment, employees should “physically monitor items to ensure that tags have not been removed or replaced.” Otherwise, the report states, a thief could more easily steal the product because it would pass through interrogators undetected.

Passive tags on the market today, including the ISO 14443 inlays used in some credit cards from [MasterCard](#), [Visa](#) and [American Express](#), lack the processing power needed to enable tags to encrypt the data they transmit to readers, Mulligan says. Instead, the reader encrypts its initial request for data from the tag, and the tag responds. This opens up RFID transactions to relay attacks, in which a mole device is placed near a legitimate RFID-enabled card so it can relay the card’s response to the interrogator linked to a point-of-sale system. Through a relay attack, someone could make a transaction by pulling the tag data from an unsuspecting consumer’s RFID tag in his or her wallet (see [The Consequences of Convenience](#)). If successful, this kind of attack would result in an unsuspecting consumer’s account being charged for goods he or she did not purchase.

The article predicts that by the latter half of 2007, passive tags will possess the memory and processing power required to encrypt data before transmitting it back to an interrogator. It adds that companies looking to deploy RFID for applications in which data requires full encryption (both interrogator data and tag data) should wait to deploy until these tags are available. The [National Science Foundation](#) (NSF) recently awarded a \$1.1 million grant to the [Consortium for Security and Privacy](#), which will work to improve encryption schemes on passive tags (see [RFID Security Consortium Receives \\$1.1 Million NSF Grant](#)). Connecticut firm [SecureRF](#) says it has already developed a means of encrypting passive tag data with its Algebraic Eraser tool, which it says consumes less power and memory than conventional encryption methods (see [SecureRF Creates New Encryption Method](#)).

The full, six-page report is available for download from [Forrester’s Web site](#). Current Forrester clients can log into the site for free, while others must pay a \$349 download fee.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved