

NIST Releases RFID Security Recommendations

The group's IT security division offers practical advice on securing RFID systems, for government and non-government users alike.

By Mary Catherine O'Connor

Sept. 26, 2006—A new research document from the Computer Security Division of the National Institute of Standards and Technology (NIST) aims to provide practical recommendations for what organizations can do to mitigate the security risks inherent in RFID deployments.

Understanding the security risks posed by RFID technology, through its transmission of potentially sensitive data that could be intercepted by rogue readers, is important. Still, organizations can benefit from guidance about how to act on such knowledge. "While books and academic papers might describe RFID system vulnerabilities, our document tells you what to do about them," says Tom Karygiannis, senior scientist at NIST, a non-regulatory agency of the United States Department of Commerce's Technology Administration. "We list the risks, and then list the operational, management and technical controls that can be used [to boost security]," he says.

The paper discusses the application of security tools commercially available today, rather than tools or processes still in development. Vendor- and platform-independent, the document's security recommendations are not aligned with any particular operating systems or applications. The document emphasizes the use of RFID protocols and equipment that meet industry and international standards in securing systems, while also discussing proprietary products that offer unique security features.

The Computer Security Division has, as part of its mission, advised agencies on cost-effectively securing federal IT systems. However, the paper's recommendations have applicability beyond the systems analysts, security professionals and engineers responsible for federal government business processes, or the IT systems that support them. Managers and planners at businesses deploying or planning to deploy RFID systems would also benefit from reading the document, Karygiannis maintains.

The document's recommendations take into account the level of security appropriate for RFID applications spanning various different industry sectors. A system used to track animals in a stockyard, for example, does not need to implement certain security measures, such as data encryption, that would be appropriate for other applications in which personal or proprietary data were transmitted between tags and readers in an environment where an unauthorized device might be able to skim the transmissions.

Privacy is not the focus of this paper, as that would involve legal and policy issues that go beyond providing technical guidance. However, it does speak to privacy issues to the extent that they overlap with security issues. It addresses, for example, approaches to privacy protection involving the temporary or permanent disabling of RFID technology, which could potentially introduce a security vulnerability.

The document is currently available on the Computer Security Resource Center for a 30-day public review and comment period. The final version is due out in about two months.

