May 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURING RADIO FREQUENCY IDENTIFICATION (RFID) SYSTEMS

Karen Scarfone, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

RFID is a form of automatic identification and data capture technology that uses electric or magnetic fields at radio frequencies to transmit information. An RFID system can be used to identify many types of objects, such as manufactured goods and animals. RFID technologies support a wide range of applications—everything from asset management and tracking to access control and automated payment. Each object that needs to be identified has a small electronic device known as an RFID tag affixed to it or embedded within it. Each tag has a unique identifier and may also have other features such as memory to store additional information about the object, environmental sensors, and security mechanisms. Devices known as RFID readers wirelessly communicate with the tags to identify the item connected to each tag and possibly read or update additional information stored on the tag. This communication can occur without optical line of sight.

Every RFID system includes a radio frequency (RF) subsystem, which is composed of tags and readers. The RF subsystem performs identification and related transactions. In many RFID systems, the RF subsystem is supported by an enterprise subsystem, which contains computers running specialized software that can store, process, and analyze data acquired from RF subsystem transactions. RFID systems that share information across organizational boundaries, such as supply chain applications, also have an inter-enterprise subsystem. Each RFID system has different components and customizations so that it can support a particular business process for an organization; as a result, the security risks for RFID systems and the controls available to address them are highly varied. The enterprise and inter-enterprise subsystems involve common IT components such as servers, databases, and networks and therefore can benefit from typical IT security controls for those components.

New Guidelines on RFID System Security

The National Institute of Standards and Technology (NIST) Information Technology Laboratory recently published new guidelines on protecting RFID systems. NIST Special Publication (SP) 800-98, *Guidelines for Securing RFID Systems: Recommendations of the National Institute of Standards and Technology*, was written by Tom Karygiannis of NIST, and by Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips of Booz Allen Hamilton. The publication recommends practices for initiating, designing, implementing, and operating RFID systems in a manner that mitigates security and privacy risks.

The guide explains the components and architectures of RFID systems and the standards for RFID components, such as tags and readers. One section is devoted to an overview of types of RFID applications and which RFID technologies are most effective for particular applications. Other topics covered in the publication include the major business risks associated with implementing RFID technology, the various RFID security controls, and an overview of privacy regulations and controls that pertain to RFID systems in federal agencies. Additional sections of the publication provide recommendations that organizations using RFID systems can

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since May 2006:

follow throughout the system life cycle, from initiation through operations to disposition, and present hypothetical case studies that illustrate how the concepts and recommendations introduced earlier in the document could work in practice.

The appendices in NIST SP 800-98 provide extensive supplemental information on the terms used in the guide, and supply listings of in-print and online resources for further exploration. Other useful listings offer additional information on common RFID standards and their security mechanisms, as well as information on permissible radio exposure limits.

NIST SP 800-98 is available from NIST's website at http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf.

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

RFID Applications and Security Controls

RFID technologies are being deployed by many organizations because they have the potential to improve mission performance and reduce operational costs. To achieve these goals, RFID systems must be engineered to support the specific business processes that the organization is automating. Applications for RFID technologies are diverse because of the wide range of business processes that exist. Examples of application types are asset management, tracking, authenticity verification, item matching, process control, access control, and automated payment. Important business drivers that shape RFID application requirements and the resulting characteristics of RFID systems include:

* The general functional objective of the RFID technology (i.e., the application type);

* The nature of the information that the RFID system processes or generates;

* The physical and technical environment at the time RFID transactions occur;

* The physical and technical environment before and after RFID transactions take place; and

* The economics of the business process and RFID system.

Because of the variety of RFID applications, RFID security risks and the controls available to mitigate them are highly varied. Section 7 of the guide contains recommendations for security practices to be applied during each phase of the RFID system's life cycle, from policy development to operations. Examples of security controls for RFID systems are having an RFID usage policy, minimizing the storage of sensitive data on tags, restricting physical access to RFID equipment, and protecting RF interfaces and tag data. Typically, only a subset of the full range of technologies, risks, and controls is applicable to any given RFID implementation.

Organizations need to assess the risks they face and choose an appropriate mix of controls for their environments, taking into account factors such as regulatory requirements, the magnitude of the threat, cost, and performance. Federal agencies should refer to Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, which establishes three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system. NIST SP 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*, provides minimum management, operational, and technical security controls for information systems based on the FIPS 199 impact categories. The information in NIST SP 800-53 should be helpful to organizations in identifying controls that are needed to protect networks and systems, which should be used in addition to the specific practices for RFID systems listed in this document. Federal agencies should also use NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, to evaluate their RFID system and select appropriate security controls.

NIST's Recommendations for RFID System Security

NIST recommends that organizations follow these guidelines in planning, implementing, and maintaining secure RFID systems:

- **When designing an RFID system, understand what type of application it will support so that the appropriate security controls can be selected.**

Each type of application uses a different combination of components and has a different set of risks. For example, protecting the information used to conduct financial transactions in an automated payment system requires different security controls than those used for protecting the information needed to track livestock. Some of the factors to be considered include:

* The general functional objective of the RFID technology. For example, does the system need to determine the location of an object or the presence of an object, authenticate a person, perform a financial transaction, or ensure that certain items are not separated?

* The nature of the information that the RFID system processes or generates. One application may only need to have a unique, static identifier value for each tagged object, while another application may need to store additional information about each tagged object over time. The sensitivity of the information is also an important consideration.

* The physical and technical environment at the time RFID transactions occur. This includes the distance between the readers and the tags, and the amount of time in which each transaction must be performed.

* The physical and technical environment before and after RFID transactions take place. For example, human and environmental threats may pose risks to

tags' integrity while the tagged objects are in storage or in transit. Some applications require the use of tags with sensors that can track environmental conditions over time, such as temperature and humidity.

* The economics of the business process and RFID system. The economic factors for RFID systems are different than those for traditional IT systems. For example, many RFID tags offer few or no security features; selecting tags that incorporate basic security functionality significantly increases the cost of tags, especially if encryption features are needed. Also, the operational cost of some basic IT security controls, such as setting unique passwords and changing them regularly, may be higher for RFID systems because of the logistical challenges in managing security for thousands or millions of tags.

▪ **Effectively manage risk so that the RFID implementation will be successful.**

Like other technologies, RFID technology enables organizations to significantly change their business processes to increase efficiency and effectiveness. This technology is complex and combines a number of different computing and communications technologies. Both the changes to business process and the complexity of the technology generate risk. The major risks associated with RFID systems are as follows:

* Business process risk. Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable. For example, a warehouse that relies solely on RFID to track items in its inventory may not be able to process orders in a timely fashion if the RFID system fails.

* Business intelligence risk. An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system. For example, an adversary might use an RFID reader to determine whether a shipping container holds expensive electronic equipment, and then target the container for theft when it gets a positive reading.

* Privacy risk. Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. As people possess more tagged items and networked RFID readers become ever more prevalent, organizations may have the ability to combine and correlate data across applications to infer personal identity and location and build personal profiles in ways that increase the privacy risk.

* Externality risk. RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people. For example, an adversary could gain unauthorized access to computers on an enterprise network through Internet Protocol (IP)-enabled RFID readers if the readers are not designed and configured properly.

Organizations need to assess the risks they face and choose an appropriate mix of management, operational, and technical security controls for their environments. These organizational assessments should take into account many factors, such as regulatory requirements, the magnitude of each threat, and cost and performance implications of the technology or operational practice.

Privacy regulations and guidance are often complex and change over time. Organizations planning, implementing, or managing an RFID system should consult with the organization's privacy officer, legal counsel, and chief information officer.

▪ **When securing an RFID system, select security controls that are compatible with the RFID technologies the organization currently deploys or purchase new RFID technologies that support the necessary controls.**

To be most effective, RFID security controls should be incorporated throughout the entire life cycle of RFID systems—from policy development and design to operations and retirement. However, many RFID products support only a fraction of the possible protection mechanisms. Tags, in particular, have very limited computing capabilities. Most tags supporting asset management applications do not support authentication, access control, or encryption techniques commonly found in other business IT systems. RFID standards specify security features including passwords to protect access to certain tag commands and memory, but the level of security offered differs across these standards. Vendors also offer proprietary security features, including proprietary extensions to standards-based technologies, but they are not always compatible with other components of the system. Careful planning and procurement is necessary to ensure an organization's RFID system meets its security objectives.

More Information

NIST SP 800-98 recommends that organizations follow effective practices for planning, implementing, and managing secure RFID systems as part of a comprehensive approach to information security. Many NIST publications assist organizations in developing that comprehensive approach. For information about the following publications that are linked to RFID security and to other security-related standards and guidelines issued by NIST, see the web page http://csrc.nist.gov/publications/index.html

FIPS 140-2, *Security Requirements for Cryptographic Modules*.

FIPS 180-2, *Secure Hash Standard (SHS)*.

FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*.

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

NIST SP 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*.

NIST SP 800-41, *Guideline on Firewalls and Firewall Policy*.

NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.

NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*.

NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*.

NIST SP 800-57, *Recommendation on Key Management*, Part 1.

NIST SP 800-63, *Electronic Authentication Guideline*.

NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*.

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*.

NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*.

NIST SP 800-92, *Guide to Computer Security Log Management*.

NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems*.

NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.