

Securing RFID Applications: Issues, Methods, and Controls

Stuart C. K. So, CISSP, CISA, PMP, and John J. Liu, Ph.D.

Radio frequency identification (RFID) is an automatic identification (auto-ID) technology developed by the Auto-ID Center at the Massachusetts Institute of Technology, relying on storing and remotely retrieving data using devices called RFID tags and readers (Auto-ID Center, 2002; Doyle, 2004; EPC, 2004b; Finkenzeller, 2000; Shepard, 2005). With RFID technology, physical assets will have embedded intelligence that allows them to communicate with each other and with the tracking points (Auto-ID Center, 2002; IBM, 2003; VeriSign, 2004).

An RFID tag is a small object that can be attached to or incorporated into a physical asset, such as a book, animal, or person. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer for further processing. As shown in [Table 1](#), there are six classes of RFID tags designed for different applications, including

active tags, which require a battery to operate, and passive tags, which have no battery (Auto-ID Center, 2002).

RFID tag technology generally dictates the operating parameters of an RFID system. As set forth in ABI, Inc. (2002), other than tag power source, operating frequencies is another main factor influencing the type of RFID applications, where the applications can be generally categorized as: (1) low frequency (LF), for access control or point-of-sales (POS) applications, (2) high frequency (HF), for handling baggage or library items in asset management application, (3) ultra high frequency (UHF) for SCM application, and (4) microwave frequency for electronic toll collection application.

SECURITY AND PRIVACY ISSUES IN RFID APPLICATIONS

The data stored on an RFID tag is often publicly accessible or product related, such as electronic product code (EPC) data or product descriptions, such that the data requires low

Stuart C.K. So, CISSP, CISA, PMP, is the Computer Systems and Laboratory Officer in the Department of Logistics at The Hong Kong Polytechnic University, involved in research and technology management. His current research areas concern information security and logistics.

John J. Liu, Ph.D., is the Head and Chair Professor of Maritime Studies in the Department of Logistics at the Hong Kong Polytechnic University. His current research areas include impulse supply order fulfillment systems, make-to-order incentive problems, maritime rescue simulator, and maritime logistics.

TABLE 1 RFID Tag Characteristics of Various Classes

Tag Class	Characteristics
Class 0/Class I	Class I tags are read-only passive identity tags.
Class II	Class II tags are passive tags with additional functionality such as memory or encryption.
Class III	Class III tags are semi-passive tags. They may broadband communications.
Class IV	Class IV tags are active tags. They may be capable of broadband peer-to-peer communication with other active tags in the same frequency band and with readers.
Class V	Class V tags are essentially readers. They power other Class I, II, and III tags as well as communicate with other Class IV tags and with each other wirelessly.

Source: Auto-ID Centre (2002).

security. However, other applications may require storing personal data. The data must be protected when it is in transit; that is, from the tag to the reader and from the reader to the network. It is strongly advised that data of this type be encrypted as it is written to the tag. Two prominent types of RFID application are selected for discussion.

Library Information Systems

RFID essentially helps libraries provide speedy inventory processes, and thus enhance user experience by delivering faster checkouts. It also helps secure physical library materials. HF RFID technology is widely used in library applications, with tag memory size ranging from 256 bits (ISO 18000-3) to 1024 bits (ISO 15693). TAGSYS (2005) proposed the memory mapping for 13.56-MHz passive RFID tag implementation. The memory map is illustrated in [Table 2](#).

Other than the first 192 bits, tag memory that is mainly used for identifying and tracking library items, there are more than 800 free-for-use bits potentially containing patron data, and this is particularly common for tracking patron's preference. Library administrators should pay attention to the security measures concerning confidentiality and data privacy.

Supply Chain Management (SCM)

In a typical SCM application, UHF RFID technology works in combination with EPC, which aims to enhance supply chain

visibility through improving inventory control and providing means to authenticate products. To realize the significant value of using RFID requires a collaborative environment to exchange relevant information. It involves extending local RFID systems to a cross-enterprise EPC network for discovering and sharing about on-tag EPC data among different supply chain members. The EPC network offers three services to facilitate searching and routing of EPC data (EPC, 2004b; VeriSign, 2004):

- Object Name Service (ONS) is a distributed directory of information sources that are available to identify the network location of the item's EPC in the supply chain. ONS was designed to be built on the existing Internet DNS infrastructure.
- EPC information service (EPC-IS) is the data repository used to store and share information about unique logistical items in the supply chain.
- EPC discovery service (EPC-DS) is a chain-of-custody registration service. It enables efficient track-and-trace capabilities with the EPC network through providing a listing of all information services available for a given EPC.

Implementing security controls to safeguard SCM applications is far more complicated than library applications, which are mainly local in nature, because cross-enterprise system-to-system networking is normally required for SCM. EPC/RFID data is routed among the trading partners by

TABLE 2 Proposed Memory Mapping for 13.56-MHz Passive RFID Tag

Field Name	Space (Bits)	Capacity	Area	Write Access	Memory
Reference item	1	Binary Status	Recommended	Library	Write once, then locked
Locating data	5	Up to 32 sorts	Recommended	Administrator	
Item type	4	Up to 16 types	Recommended		
Item identifier	48	A 15-numeric digit	Mandatory		
Multi-item ID	6	barcode number Up to 8 multiple items	Mandatory		
Extending shelving section	32	Up to 16 floors 512 sections/dept 8 shelves	Recommended	Managed by applicative software/administrator access at programming	Read/write
Check-in/check-out data	32	CI/CO binary status Full data of the last operation Etc.	Recommended	Automatic at CI & CO	
Library identifiers	64	Maximum 8 alpha numeric digits, or 2 alpha numeric and 12 numeric digits	Optional	Managed by applicative software/administrator access at programming	Write once, then locked is recommended
Free use	>800b	16 numeric digits	Optional	Free	According to the data stored

Source: TAGSYS RFID Inc. (2005).

EPC network services through the underlying servers and RFID middleware situated at different locations on the supply chain.

On the grounds of the suggestions from EPCglobal® (EPC, 2004b), an overview of some security measures is provided in Table 3. The areas of concern mainly associate with the data, EPC infrastructure hardware, and EPC network services. In summary, the security measures toward the objectives of preserving confidentiality, integrity, and availability (CIA) should be implemented for the RFID/EPC data and its underlying infrastructure hardware. Besides, proper access control should also be implemented in association with EPC network services.

Following the long-anticipated EPCglobal Gen 2 RFID products reaching the markets, upgrade of RFID infrastructure hardware from Gen 1 to Gen 2 is expected to bring additional security issues. The

replacement of RFID tags and software redevelopment as a result of upgrades will demand the implementation of security controls in the areas of system development, project management, and operation support.

METHODS OF PROTECTING DATA PRIVACY ON RFID TAGS

The use of RFID tags constitutes a serious privacy concern for consumers, particularly in POS applications that contain personal data and possibly transactional data. The tag is designed in such a way that each associated consumer product can be uniquely identified through an EPC and will be broadcast to any nearby reader (Juels et al., 2003). This unique information stored on the tags can serve as a pointer to additional information stored elsewhere in a database, presenting a clear potential for privacy vio-

TABLE 3 Proposed Information Security Measures in Hardening EPC Network

Areas of Concern	Security Measures
EPC/RFID data	All information associated with an EPC should be accessible only to authorized users behind firewalls, encoding, and other security measures to preserve confidentiality, integrity, and availability (CIA) of the data. The memory banks on RFID tags storing sensitive data should be protected by password. Confidential data should be avoided for storage on RFID tags. Otherwise, data should be encrypted.
EPC information service	Authentication and access control of EPC data should be established with EPC-IS. Appropriate security measures should be established on the company's information systems that interact with EPC-IS to control the sharing of EPC data.
EPC discovery service	The function of EPC-DS is to enable users to find data related to a specific EPC and to request access to that data. Actual access to EPC data is accomplished locally by the EPC-IS. Therefore, it is recommended that companies implement security controls for EPC-IS as suggested.
EPC infrastructure hardware	The EPC infrastructure hardware contains the RFID tags and readers. Data privacy concerns are raised when considering that EPC-tagged objects move from the supply chain to the consumer. The following security measures are suggested: <ul style="list-style-type: none"> <input type="checkbox"/> Design a data capturing process that does not communicate totally meaningful information; that is, collect only need-to-know data (e.g., EPC identification, the time, data, and location of read). <input type="checkbox"/> Employ the process along the supply chain checkpoints beyond the point of sales (POS). <input type="checkbox"/> The POS is essentially a customer touchpoint. Thus, the chance of the consumer having contact with EPC tags will increase and privacy issues will become significant. Appropriate strategies in dealing with data privacy for RFID tags should be developed.

lation (Bravo, 2005). The following security measures are generally used in protecting data privacy with current RFID technology:

- “Kill tag” approach. An RFID tag is permanently disabled (killed) by a 32-bit kill password stored in reserved memory so that it becomes inoperative before it is placed in the hands of consumers (Bravo, 2005; EPC, 2004a; Juels et al., 2003). The “kill tag” approach is typically used in POS applications, where the tags of purchased goods are killed after checking out.
- Password approach. The RFID tag data is accessed or locked by an optional 32-bit access password stored in reserved memory (Bravo, 2005; EPC, 2004a; Juels et al., 2003). This approach can be applied for controlling unauthorized access to confidential data stored in the tag memory.

- Faraday cage approach. An RFID tag is shielded from scrutiny by a metallic container that is impenetrable by radio signals at a predefined frequency band (Bravo, 2005; Juels et al., 2003). According to Juels et al. (2003), the application of Faraday cages is only a partial solution to consumer privacy, because a vast range of items such as clothing, wrist-watches, and large objects cannot be placed conveniently in containers.
- Active-jamming approach. An electronic device actively broadcasts radio signals to disrupt the operation of any nearby RFID readers (Bravo, 2005; Juels et al., 2003). A drawback for this application is that it could cause disruption to normal operations of nearby RFID systems, which may be illegal.
- Cryptographic approach. Part of the data area on the RFID tag is used to store a cryptographic signature, such as SHA-1

hash, which verifies that the rest of the data reported has not been tampered with and the reported data was encrypted (Bravo, 2005). This approach not only preserves data confidentiality but also authenticates user identity. However, the operation flow should be carefully designed in order not to jeopardize the convenience of use, especially in retail and POS applications.

VIRUS VULNERABILITY OF RFID TAGS

A research paper recently published by a group of European scientists warned that RFID tags have the potential to be infected with viruses that could corrupt the back-end databases and cause major chaos at airports and supermarkets (Millard, 2006; Naraine, 2006; Taipei Times, 2006). As set forth in Rieback et al. (2006), the researchers have highlighted several types of exploits that can be performed by RFID tags through exploiting RFID middleware. These exploits include buffer overflows, malicious code insertion, and SQL injection.

The researchers also demonstrated the creation of a self-replicating RFID virus requiring only an infected RFID tag as an attack vector and discussed the possibility of attacking the back-end database of an RFID application scenario, then infecting the clean new tags.

Hence, security measures need to be adopted to prevent the data from RFID tags from being used to exploit back-end systems. The researchers suggested that RFID middleware writers need to adopt appropriate security measures against RFID viruses, such as bounds checking, filtering of special characters, turning off back-end scripting languages, limiting the rights of database permission, and isolating the RFID middleware server in DMZ so that RFID middleware can be prevented from suffering the potential vulnerabilities experienced by the Internet.

ESTABLISH SECURITY POLICIES FOR USE OF RFID TECHNOLOGY

Security policies are the basis for a sound security implementation in an organization. However, organizations often implement technical security solutions without first creating a foundation of policies, which could result in unfocused and ineffective security controls. Security objectives will not be met if technical solutions are not implemented in a systematic way. Yet, security controls for RFID can be implemented smoothly only with sound information security policies. On the grounds of the suggestions in So (2004), some security measures for handling personal data in RFID applications are proposed in Table 4.

The controls are mainly concerned with the areas of information security, systems security, and personnel security, which are related to handling of the RFID data (either directly from the RFID tags or indirectly from the RFID middleware and its associated systems).

For information security, ownership, accountability and classification of information are the major concerns. To properly mandate the implementation and ensure the application of the security policies, the owners must be identified. Besides, the information must be classified according to confidentiality, integrity, and availability (CIA) to be properly managed by the owners.

For systems security, password management and virus control are mostly concerned with safeguarding the RFID data, no matter whether on tag or on database. The last but not the least personnel security concerns the control of third parties who are able to access or process the data. Administrative controls need to be involved for preserving the confidentiality and integrity of the information.

DESIGN SECURITY METRICS FOR MEASURING THE EFFECTIVENESS OF CONTROLS

Security metrics is the application of analytical techniques to measure the performance

TABLE 4 Security Controls for Implementing an RFID Application

Proposed Area of Control	Descriptions
Ownership and responsibility	Proper roles and responsibilities of people who manage information assets should be clearly defined.
Classification of information	Personal data should be classified according to confidentiality, integrity, and availability (CIA).
Information/process protection	Personal data must be handled under segregated control by following the requirements of specific information classification, and must not be made available outside the business without management authorization.
Control over information transfer and distribution	Personal data should be transported only by a trusted party and protected by appropriate technical measures according to the information classification.
Contract with contractors and trading partners	Personal data access by or transfer to a third party should be based on a formal contract, including at least a confidentiality (non-disclosure) agreement.
Password management	Password management policy is required to control the use and maintenance of: <ul style="list-style-type: none"><input type="checkbox"/> Kill/access password of RFID Gen 2 tag.<input type="checkbox"/> Passwords of computing facilities associated with various EPC network services.
Virus control	All systems and their corresponding operating environment that are vulnerable to viruses must have an approved anti-virus control package installed.

of implementing security controls. A set of commonly acceptable security metrics is necessary to guide security policy makers for the establishment of rational security policies and for security designers to design and select security controls appropriate to the policy of the systems.

Relevant security metrics should be designed to measure the performance of the security controls adopted for the operations. A better approach is to combine security metrics with performance indicators that link to operation processes or service levels to end users such as availability of applications (Vijayan, 2005). Preventsys (2005) also suggested that the security metrics should be based on the consequences of operation processes or the outputs of security applications. Therefore, we attempt to link the security metrics to the frequency of security breaches, which could reasonably reflect the outcomes of deploying the recommended controls. The proposed security metrics are summarized in [Table 5](#).

The security metrics that were aligned with the control areas as specified in the security policies attempt to measure the effectiveness of specific controls deployed, including both administrative procedures and technical measures. Hence, security managers will have a mean to demonstrate the effectiveness of their security initiatives for showing that their investments have provided better protections to their respective organizations.

CONCLUSION

One of the biggest myths about technology is the idea that any company can embrace it and expect results. However, successful deployment of a technology for an organization depends on many factors, and security management is most important. RFID technology is one of the emerging technologies that is worthwhile to study, considering its wide adoption.

In this study, we attempted to briefly explore this technology, highlighting major

TABLE 5 Security Metrics for Measuring the Performance of Controls

Area of Control	Type of Control	Proposed Security Metrics
Ownership and responsibility Classification of information	Administrative (e.g., procedures)	Unauthorized access attempts Unauthorized changes
Information/process protection	Administrative (e.g., procedures, regulatory compliance) Technical (e.g., encryption, access control, logging)	Intrusion attempts Intrusion successes Unauthorized access attempts Unauthorized changes
Control over information transfer and distribution	Administrative (e.g., procedures) Technical (e.g., access control, authorization control)	Intrusion attempts Intrusion successes Unauthorized access attempts Unauthorized changes
Contract with contractors and trading partners	Administrative (e.g., legal agreement)	Unauthorized information disclosures
Password management	Administrative (e.g., procedures) Technical (e.g., access control)	Invalid logins Request for reset password
Virus control	Technical (e.g., installed relevant anti-virus control packages)	Virus detected/filtered in user files Virus detected/filtered in e-mail messages Virus detected/filtered on Web sites

security issues in some common RFID applications. We note that a number of security issues such as access control, data privacy, and virus vulnerability could cause security breaches on the CIA objectives and need to be addressed. As such, we suggest relating the security controls to the handling of RFID data and establishing the security policies as a framework to implement these controls. To measure the effectiveness of implementing these security controls, we have advised some useful metrics for security managers to justify their security investments. ■

ACKNOWLEDGMENT

The authors wish to thank the Research Committee of The Hong Kong Polytechnic University for its financial support of the project.

Reference

- ABI, Inc (2002), "RFID White Paper", Allied Business Intelligence, Inc., USA.
- Auto-ID Center (2002), "Technology Guide", Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA, USA.
- Bravo (2005), "Building Security and Privacy into RFID Systems", Bravo Group, Harvard Extension School, USA. http://www.simson.net/ref/2005/csci_e-170/p1/bravo.pdf (Accessed Feb 2, 2006).
- Doyle, Shaun (2004), "Auto-ID technology in retail and its potential application in marketing", *Journal of Database Marketing & Customer Strategy Management*, Vol. 11, No. 3, pp. 274–279.
- EPC (2004a), "EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz — 960 MHz Version 1.0.8", EPC Global Inc., New Jersey, USA.
- EPC (2004b), "The EPCglobal Network™: Overview of Design, Benefits, & Security", EPC Global Inc., New Jersey, USA.
- Finkenzeller, K. (2000), "RFID Handbook: Radio-Frequency Identification Fundamentals and Applications", John Wiley & Sons, 2000.

- IBM (2003), "Applying Auto-ID to Reduce Losses Associated with Shrink", Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA, USA.
- Juels A., Rivest R.L., and Szydlo M. (2003), "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", ACM Press, USA. <http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf> (Accessed Mar 25, 2006).
- Millard, Elizabeth (2006), "Research: RFID Chips Vulnerable to Viruses", CRM Daily.Com, March 16, 2006. http://www.crm-daily.com/story.xhtml?story_id=02300000KRYM (Accessed Mar 17, 2006).
- Naraine, Ryan (2006), "Dutch Researchers Create RFID Malware", eWeek.Com, March 15, 2006. <http://www.eweek.com/article2/0,1895,1938391,00.asp> (Accessed Mar 17, 2006).
- Preventsys (2005), "Effective Operational Security Metrics", Preventsys White Paper 2005, Preventsys, Inc.
- Rieback M.R., Crispo B., Tanenbaum A.S. (2006), "Is Your Cat Infected with a Computer Virus", *Fourth Annual IEEE International Conference on Pervasive Computing and Communications 2006 (Percom)*, Pisa, Italy.
- Shepard, Steven (2005), "RFID — Radio Frequency Identification", McGraw Hill, New York, pp. 1–54.
- So, C.K. Stuart (2004), "Privacy Implication of Enterprise Data-mining Activities", *Handbook of 21st Info-Security Conference 2004*, Hong Kong.
- TAGSYS (2005), "TAGSYS RFID System for Libraries", TAGSYS, USA. <http://www.tagsysrfid.com/> (Accessed Dec 22, 2005).
- Taipei Times (2006), "Virus Vulnerability of Microchip Tracker Tags Demonstrated", NY Times News services, New York, Taipei Times, March 16, 2006, p. 10. <http://www.taipetimes.com/News/worldbiz/archives/2006/03/16/2003297663> (Accessed Mar 17, 2006).
- VeriSign (2004), "The EPC Network: Enhancing the Supply Chain", VeriSign White Paper 2004, VeriSign Inc.
- Vijayan, J. (2005), "Metrics Fall Short of Mark on Security", *Computerworld*, v39, i39, pp.16–17.

SECURING NETWORKS IN AN UNCERTAIN WORLD

In the face of GROWING NETWORKS, GROWING THREATS, and GROWING STAKES

Make sure you have the latest tools to survive...

INTELLIGENCE SUPPORT SYSTEMS: *Technologies for Lawful Intercepts*

Paul Hoffmann and Kornel Terplan
AU2855, January 2006, 488 pp., ISBN: 0-8493-2855-1, \$89.95 / £49.99

WIRELESS SECURITY HANDBOOK

Aaron E. Earle
AU3378, January 2006, 384 pp., ISBN: 0-8493-3378-4, \$79.95 / £44.99

AUDIT AND TRACE LOG MANAGEMENT: *Consolidation and Analysis*

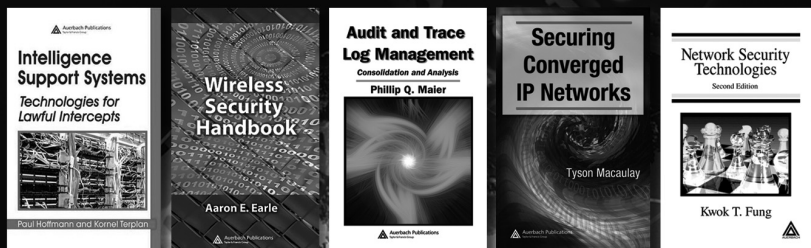
Phillip Q. Maier
AU2725, April 2006, 192 pp., ISBN: 0-8493-2725-3, \$79.95 / £44.99

SECURING CONVERGED IP NETWORKS

Tyson Macaulay
AU7580, May 2006, 280 pp., ISBN: 0-8493-7580-0, \$79.95 / £44.99

NETWORK SECURITY TECHNOLOGIES, *Second Edition*

Kwok T. Fung
AU3027, 2005, 296 pp., ISBN: 0-8493-3027-0, \$79.95 / £44.99



Order these and other outstanding books from Auerbach Publications at
www.crcpress.com