Fall 9-30-2008

Designing Privacy and Security Protection in RFID-enabled Supply Chain

Timon C. Du

Waiman Cheung

Sung-Chi Chu

Designing Privacy and Security Protection in RFID-enabled Supply Chain

Timon C. Du, The Chinese University of Hong Kong, Hong Kong, timon@cuhk.edu.hk
Waiman Cheung, The Chinese University of Hong Kong, Hong Kong, wcheung@cuhk.edu.hk
Sung-Chi Chu, The Chinese University of Hong Kong, Hong Kong, sungchi@cuhk.edu.hk

Abstract

RFID is an automatic identification system that uses radio frequency technology in product tags. The technology brings out the greater enhancement to synchronize the logistics flow and information flow. Unfortunately, it also introduces the great concerns on the privacy and security protection, not only on the individual use but also on the supply chain collaboration. This study proposes an on demand access control to protect the information flow in an RFID-enabled supply chain. The design considers the role in a supply chain as well as the media of carrying the information. A case study on garment industry will be provided for validation.

Keywords: RFID, EPC, Privacy and Security, Access Control, Supply Chian

1. Introduction

Radio Frequency Identification (RFID) can be applied to many areas, such as inventory management, theft prevention, asset tracking (people, animals, tools, and vehicles), express checkouts (highway and tunnel payment or luggage checking), location-based information (travel guides or horse racing), and others. The advantages of RFID tags are that, unlike printed barcodes, they do not need a direct "line of sight," and multiple tags can be identified in a short time (from tens to hundreds per second). Moreover, the tags are resistant to dirt, have a large amount of unique identifiers, and can be read (and written) by readers without being visible. However, the disadvantages are that the signals that are transmitted from the tags can be read by other equipment within range, and interference can occur when more than one reader is transmitting or more than one tag is responding. Possible consumer privacy issues are also a concern.

However, the growth in the use of RFID which enables the unique identification of objects and invisible tracking, has given rise to increased concern about the invasion of privacy [1] [2] [3]. To end consumers, as a result, two notable privacy threats are leaking information pertaining to personal property, and tracking the consumer's spending history and patterns and physical whereabouts [4] [5]. Therefore, how can the adoption of RFID technology to improve supply chain management being balanced with the privacy protection. The provision of guidelines (will discuss in next section) such as those that were published by the Ontario Privacy Commissioner [6] and the Japanese Ministry of Public Management, Home Affairs, Post and Telecommunications [7] to protect privacy is a possible, but passive, solution.

The aforementioned guidelines work as instructions about the extent to which privacy should be protected. However, security tools are needed to achieve true data protection. A privacy coin shows the relationship between privacy protection, security boundaries, and security requirements. The security tools should achieve protection from improper access, protection from interference, the integrity of the data, the operational integrity of the data, the semantic integrity of the data, accountability and auditing, user authentication, the management and protection of sensitive data, multi-level protection, and confinement to avoid undesired information transfer between system programs [8]. These tools ensure that the information does not either explicitly (through placing queries) or implicitly (through inference from related data) flow over the boundary and invade privacy. The other side of the coin indicates that privacy protection cannot be achieved only by security measures, but must also feature authentication and non-repudiation, which ensure that data are correctly provided and received.

This study explores the privacy and security issues manifested by RFID adoption in the supply chain. There are many new challenges and our intention is to address the potential privacy and security concerns raised and propose a scheme to articulate the preference in the sharing of RFID-based data; such scheme is the basis for the design and development of new technology – on-demand access control. The access control is a common term used in database security that mainly differentiated in discretionary security mechanisms and mandatory security mechanisms [9]. The discretionary control specifies the access privileges of users explicitly while mandatory security mechanisms identify the security levels of both subjects and objects. However, neither model provides

mechanism to prevent the information from flowing from authorized to unauthorized users [10]. To support the flow control model such as the lattice model [11] and the RBAC model can be adopted. In the lattice, the flow relationships are organized into classes and the data flowed from one class to another class are constrained explicitly or implicitly. Role-based access control (RBAC), on the other hand, applies permission policy based solely on the role of a user at the time of accessing a data source [12] [13]. A role is a function involved in executing a job with certain authority and responsibilities and thus is suitable for workflow management [14][15]. Roles are pre-determined for a data source.

For RFID-based data and information sharing between supply chain partners access policy is applied base on their relationship of which the role of the requesting side is only one of many attributes. The access policy is further determined by other relationship attributes such as long-term vs. one-time, dominant vs. causal as well as the parties' dual willingness to share. The relationship needs to be determined at the time of sharing as it changes over time even when data requestor's role remains unchanged. Hence, the one-party, pre-determined, role-based access control is not applicable to two-party, derived on demand, "relationship-based" access control requirement for sharing RFID-based data. We validate the model using a garment supply chain. An interview to three RFID users was also conducted to verify the model.

2. RFID Tags and Privacy Protection

In late 1999, a research group, the Auto-ID Center, was setup at the Massachusetts Institute of Technology with sponsors in both the technology sectors and industrial giants, such as Wal-Mart and P&G. The Center proposed a uniquely identifiable Electronic Product Code (EPC) stored in a medium that follows the new Radio Frequency Identification (RFID) standards. These technologies were then transferred to and commercialized by the non-profit making organization EPCglobal Inc. in October 2003.

RFID is an automatic identification technology that uses radio frequencies. An RFID system consists of tags (or labels), readers/antennas, and a backend system or a host. There are two kinds of tags: active and passive. Active tags have a built-in battery, and therefore can transfer a signal over a longer distance (a 100-meter range) whereas passive tags do not have a power source but derived power from incoming electromagnetic waves through their antennae by power reflection from the reader.

An RFID tag is a good medium to carry and collect data that needs to be shared among supply chain partners. A typical tag contains an EPC which has four segments (labeled as 'E' in the ensuing sections next), and in many cases, additional or user memory (as 'A'). In here, we consider RFID tags that are re-writable (e.g., a passive Gen-2 tag). The proposed schemes are intended to guide partners to establish preferences when sharing data with other partners and external parties, ensuring privacy is protected and security is guaranteed. The preference of the willing sharing party is derived based on the nature of the data in three different dimensions: data sensitivity, data location, and data ownership. The coding scheme of the EPC includes four segments: a header, a company manager number, an object class, and a serial number. The header specifies the structure of the encoding on tag, allowing encapsulation of other common coding schemes, such as General Identifier (GID), a serialized version of the EAN.UCC Global Trade Item Number (GTIN) and the EAN.UCC Serial Shipping Container Code (SSCC). The general manager number identifies the company or organization that is responsible for maintaining the next two segments: object class (O) and serial number (S). In general, the combination of O and S segments can be used to identify a unique item of a product of a company. The EPCglobal Gen2 standard covers the UHF RFID tags that are reusable. User memory is also available on some tags (based on designs from TI and NXP) to allow additional data to be stored other than the EPC. The EPCglobal Architecture Framework [16] defines an architectural view of core services such as ONS, for subscribers of the EPCglobal Network. EPCIS [17] or EPC Information Services are proposed as the "primary vehicle" for subscribers such as a supply chain partner to exchange data with others (within EPCglobal Network).

"Privacy is the ability of a person to control the availability of information about, and exposure of, him- or her-self" (en.wikipedia.org). To observe the right to privacy, countries or regions define their own guidelines according to their cultures. A comprehensive guideline that comprises eight privacy protection principles that has been endorsed by 30 countries was issued by the Organization for Economic Co-operation and Development (OECD) [18]. These guidelines were adapted to protect privacy and the trans-border flow of personal data following the evolution of the Internet. RFID is a new medium that facilitates the flow and subsequent sharing of data via international data repositories. Concerns about the collection, processing, and dissemination of data using this new medium must be considered. The eight basic principles are discussed in the context of RFID adoption next.

(1) Collection limitation. Data that allows identification should be collected through lawful and fair means with the consent of the data subject. RFID tags should not provide information without the consent of the data

subject, and high sensitivity data should not be either carried by or associated with the EPC on tags. Therefore, an appropriate design of access control and data encryption is crucial to the use of such tags. Similarly, EPCglobal should not provide information to outside parties without the consent of the data subject.

(2) Data Quality. The collected data should be accurate, complete, and kept up to date. Accordingly, only legitimate data should be written to RFID tags, and the data stored at EPCglobal Network (or Internet EPC-IS) that are associated with the on tag EPC should be maintained in good quality.

(3) Purpose Specification. Data subjects should be informed of the purpose of the data collection no later than the time of data collection. Accordingly, the data in an RFID tag can be collected when read, thus the data subject(s) must be told of and consent to the purpose of collection as well as the situation where such collection would occur. That is, even when the encrypted data in the tag can be accessed, the associated data in both the RFID tag and the EPCglobal Network should still be protected if the purpose of use has not been consented to.

(4) Use Limitation. The use of the collected data should conform to the purpose that has been specified. Accordingly, the access control mechanism in the EPCglobal Network should prevent the disclosure of data to parties that do not satisfy the purpose of use, except when the data subject consents to such disclosure.

(5) Security Safeguards. Data should be protected from unauthorized access, destruction, use, modification, or disclosure. As RFID tags are subjected to damage as they move across the supply chain, both the data (on tag) ownership and the tag ownership must take precautionary steps to protect the data from unauthorized use, especially as overwriting the data in the tag, e.g., either destroying the data integrity or rendering the tag useless. Similarly, the data in the EPCglobal Network should only be accessible to those with special privileges.

(6) Openness. The development, practice, and policies surrounding data should be open to individuals who voluntarily provide personal data. This means that personal or organizational data that are collected through RFID technology should be accessible in or via the EPCglobal Network to the data owner, be the owner be an individual or an organization.

(7) Individual Participation. Individuals or organizations should have the right to obtain and communicate with the data collectors, and to challenge and rectify the data. The EPCglobal Network should provide a due process for individuals or organizations to do so.

(8) Accountability. The data collector should be accountable for compliance with these privacy protection principles. The EPCglobal Network should be accountable to both the data collector and individuals (organizations).

3. Conclusions

Whenever new technology is invented to expedite operations, the issue of invading privacy is always raised, as occurred with the introduction of e-commerce [19] and market research [20]. However, the benefits of new technology can only be enjoyed when a balance between the protection of privacy and operational efficiency is achieved, and this is no less the case with the introduction of RFID.

The objective of this study is to design an appropriate access control scheme that uses security tools to ease concerns about privacy invasion, while allowing some degree of information sharing to expedite supply chain collaboration. Companies in a garment supply chain were interviewed to verify the design. A data sensitivity checklist, developed according to the willingness of supply chain partners to share data [21], is used to determine where data should be located in any of the five locations. An access control scheme is then complete and becoming a guideline for a partner to determine/develop preferences of data sharing based on sensitivity, location, partners and partnership. Each partner can have individual, and likely different preferences with respect to the same data due to their perception of data sensitivity and willingness to share. Some degree of modification would be needed for different industries.

This study serves as a starting point for privacy- and security-assured RFID-based data sharing, and many issues are not addressed. The proposed privacy and security scheme is a step towards a general solution to RFID privacy issues. Data sharing among supply chain partners is relationship-based which is multilateral and often with conflicting sensitivity requirements. The data sensitivity, data locations and roles of partners are the major dimensions of the scheme. Future research should develop on demand “relationship-based” access control. This access control ensures multilateral sharing preferences can be satisfied. The scheme helps partners to place RFID-related data to locations such that the privacy and security preferences can be articulated. Tools, such as preference templates and/or a preference specification language, can then be developed for partners to specify the preferences by filling in the scheme. Preference specification of individual partners is an important step towards relationship-based access control. Multilateral data sharing can then be established by on demand reconciliation of the preferences.

Acknowledgement

This research is partially supported by the Li & Fung Institute of Supply Chain Management & Logistics, The Chinese University of Hong Kong.

References

[1] Bacon, J., Moody, K., and Yao, W. "A Model of OASIS Role-Based Access Control and Its Support for Active Security," ACM Transactions on Information and System Security, 5 (4), November, 2002, pp 492-540

[2] Gunther, O. and Spiekermann, S. RFID and the perception of control: the consumer's view, *Communications of the ACM*, 48, 9, (September 2005), 73-76.

[3] McGinity, M., RFID: is this game of tag fair play? *Communications of the ACM***,** 47, 1, (January 2004), 15-18.

[4] Ohkubo, M., Susuki, K. and Kinoshita, S. RFID privacy issues and technical challenges, *Communications of the ACM*, 48, 9, (September 2005), 66-71.

[5] Eckfeldt, B., What does RFID do for the consumer? *Communications of the ACM*, 48, 9, (September 2005), 77-79.

[6] Ontario Privacy Commissioner (www.ipc.on.ca/docs/rfid-lib.pdf)

[7] Japanese Ministry of Public Management, Home Affairs, Post and Telecommunications (www.soumu.go.jp/s-news/2004/040608_4.html)

[8] Castano, S., Fugini, M., Martella, G., and Samarati, P. *Database Security*, ACM Press and Harlow: England: Addison-Wesley, 1995.

[9] Elmasri, R. and Navathe, S. *Fundamentals of Database Systems*, 3rd ed., Addison-Wesley, Reading MA, 2000.

[10] Du, T., Lee, E. and Wong, J, Document access control in organisational workflows, *Int. J. Information and Computer Security*, Vol. 1, No. 4, 2007.

[11] Denning, D.E. 'A lattice model of secure information flow', Communications *of the ACM*, Vol. 19, No. 5, pp.236–243, 1975.

[12] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., and Chandramouli, R. "Proposed NIST Standard for Role-Based Access Control," ACM Transactions on Information and System Security, 4 (3), August 2001, pp 224–274.

[13] Damiani, M.L., Bertino, E., Catania, B., and Perlasca, P. "GEO-RBAC: Spatially Aware RBAC," ACM Transactions on Information and System Security (TISS), 10 (1), February, 2007, pp1-42.

[14] Sandhu, R.S., "Lattice-based access control models", *IEEE Computer*, Vol. 26, pp.9–19, 1993.

[15] Sandhu, R.S., Coyne, E.J., Feinstein, H.L. and Youman, C.E.. "Role-based access control models", *IEEE Computer*, Vol. 29, pp.38–47, 1996.

[16] EPCglobal, "EPCglobal Architecture Framework", Final Version, 1 July 2005, (http://www.epcglobalinc.org/standards/architecture/architecture_1_0-standard-20050701.pdf; visited August 28, 2007)

[17] EPCglobal, EPC Information Services (EPCIS) Version 1.0 Specification, ratified standard, April 12, 2007 (http://www.epcglobalinc.org/standards/epcis/epcis_1_0-standard-20070412.pdf; visited August 28, 2007)

[18] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2002, Organization for Economic Co-operation and Development, www.copyright.com.

[19] Volokh, E., Personalization and privacy, *Communications of the ACM*, 43, 8, August 2000, 84-88.

[20] Laudon, K., Markets and privacy, *Communications of the ACM***,** 39, 9, (September 1996), 92-104.

[21] Du, T., Wong, M., Cheung, W., and Chu, S.C. "A Privacy and Security Framework for the EPC Network Infrastructure," BA Working Paper Series, WP-06-02, The Chinese University of Hong Kong, 2006.