Designing Privacy Policies for Adopting RFID in the Retail Industry

Haifei Li[1], Patrick C. K. Hung[2], Jia Zhang[3], and David Ahn[4]
[1]Department of Math and Computer Science, Union University, USA
[2]Faculty of Business and IT, University of Ontario Institute of Technology (UOIT), Canada
[3]Department of Computer Science, Northern Illinois University, USA[1]
[4]Department of Computer Science, Nyack College, USA
E-mails: hli@uu.edu, patrick.hung@uoit.ca, jiazhang@cs.niu.edu, david.ahn@nyack.edu

Abstract

Radio Frequency Identification (RFID) technologies can potentially improve the productivity of retailers. In this paper, we propose a role-based, enterprise-level, RFID-oriented privacy authorization model for supporting the privacy policies in utilizing RFID in retail industry.

1. Introduction

In recent years, Radio Frequency Identification (RFID) has caught attention in retail industry for better productivity. RFID is a generic term for the technologies that use radio waves to automatically identify individual items wirelessly [1], so as to track the entire circulation process of items from suppliers to end users. The actual adoption of RFID in retail industry is quite slow. In addition to the security issue, data privacy is a big concern due to the possible unwanted revelation of confidential or personal data stored within the RFID devices.

Although many authorization technologies can be directly applied to protect personally identifiable information (PII), in our opinion, the traditional view of authorization model should be extended with an enterprise-wide privacy policy for managing and enforcing individual privacy preferences. In addition, other privacy concepts such as purpose and obligation also have to be incorporated. In this paper, we aim to propose a privacy authorization model and explore its implementation issue focusing on language specification.

2. Related work

The Privacy Preferences Project (P3P) working group at World Wide Web Consortium (W3C) develops a P3P specification for enabling Web sites to express their privacy practices in XML format. P3P also provides a language called P3P Preference Exchange Language 1.0 (APPEL), which is used to express the user's preferences [2]. Although these mechanisms capture common elements of privacy policies, they do not provide authorization mechanisms to check a given access request against a stated privacy policy.

The eXtensible rights Markup Language (XrML) is used to describe the rights and conditions for owning or distributing digital media. [3]. Based on the specification of licenses, the XrML agent can determine whether to grant certain right on certain resource to certain principal or not. However, XrML does not consider the privacy entities in their access control model, which must be addressed in the RFID field.

3. RFID-oriented privacy authorization model

The RFID privacy access control is being investigated and developed in the context of services computing. Here we propose an enterprise-level RFID-oriented privacy authorization model as illustrated in Figure 1. A virtual enterprise (i.e., retailer) boundary is introduced to ensure authorization-based privacy. As shown in Figure 1, all users having access to RFID tags are divided into three categories of roles: suppliers, role players, and end users. A supplier is a provider of a RFID tag, who can be either the original manufacturer or another retailer. A role player serves in an enterprise retail store, who can be a cashier, a store manager, etc. An end user takes a RFID tag out of an enterprise retailer, who can be either a professional buyer or another retail store. It should be noted that an entity can play different roles under different circumstances. For example, a retail store can act as a supplier for another retail store, and an end user of yet another retail store. A person can act as a role player in one retail store, and an end user of merchandise if he/she actually pays for it. In other words, the journey of merchandise can start from an original supplier and flow through multiple enterprise retailers before reaching a customer's hand. Figure 1 also shows that the circulation of a RFID tag is a directional flowing from a supplier to an enterprise retailer, and then to an end user.

As illustrated in Figure 1, at the left-hand side,

[1] The third author is also a Guest Scientist of National Institute of Standards and Technology (NIST).

Proceedings of the 2005 IEEE International Conference on Services Computing (SCC'05)
0-7695-2408-7/05 $20.00 © 2005 IEEE

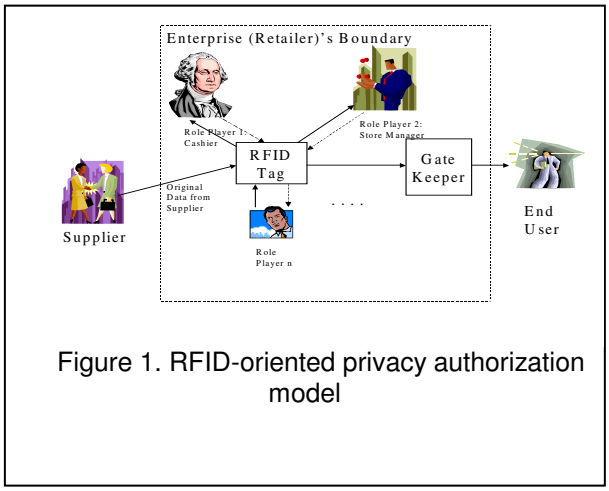

Figure 1. RFID-oriented privacy authorization model

suppliers provide retailers with the original data from the manufacturing facility. The data is embedded and stored into a RFID tag. After the RFID tag enters the enterprise's boundary, different role players (e.g., cashiers) can interact with it. A solid line from the tag to a role player refers to an action of reading of the tag data; while a dotted line from the role player to the tag refers to a possible action of writing of some data to the tag. Before the tag leaves the enterprise boundary, such as a retailer store, the RFID tag needs to pass through a "GateKeeper". The GateKeeper is an automated program to ensure that the customer's privacy will be properly protected. For example, it will examine whether some role players (e.g., cashiers) intentionally or unintentionally write some unauthorized data into the tag. In summary, only role players inside of an enterprise boundary have direct access to RFID tags. The other two types of roles (i.e., suppliers and end users) can only access RFID tags via enterprise interfaces if they are provided.

4. Design and Implementation

Authorization in our model implies two layers of control: authorization over users and authorization over data. The lower layer is authorization over users. Before accessing a RFID tag, a user has to be authorized into a specific enterprise boundary. Furthermore, all role players (e.g., cashiers, store manager, etc) have to use on-site equipments to pass the authorization process. As shown in Figure 1, these role players are delimitated by an enterprise boundary. An enterprise boundary is defined using a specific retailer. Different retailers define their respective boundaries; and different retailers may not share the access of their boundaries.

The second layer of authorization control is applied over data. Not all kinds of information can be embedded and stored into a RFID tag, even from an authorized role player. For example, a cashier may store the last four digits of a customer's credit card into a RFID tag, but may not be allowed to input all the digits of the card.

In order to guard and ensure privacy authorization, one core issue is that we have to explore approaches to precisely describe privacy policies. We implemented the core privacy policies in our model utilizing essential constructs of Enterprise Privacy Authorization Language (EPAL). EPAL is an interoperability language for governing data handling practices for authorization rights [4]. We divide the major RFID privacy policies into two categories: (1) privacy authorization model related to data collection, and (2) privacy authorization model related to data processing. The first category includes privacy policies on cashiers' handling of private information, and policies to guarantee that the same tag cannot be read by other types of RFID readers. The second category includes policies to guarantee that the RFID tag can be destroyed, to guarantee that the RFID tag can be blocked, and to guarantee that the collected data will not be sold to the third party.

Each category and sub-category is then specified by SPEL. For example, for the last sub-category above, a customer may not be willing to reveal the PII to third parties. Therefore, the retailer should define a policy rule to describe it. The following is the essential part of the definition.

<DENY
user-category = "store_manager"
data-category = "RFID"
purpose= "Marketing"
operation = "sell"
condition =
"/CustomerRecord/ThirdPartyConsent = FALSE"/>

5. Conclusions

We just presented our privacy authorization model tailored for enterprise-level of RFID usages, highlighted by following points: (1) the introduction of enterprise (retailer) boundary, (2) the introduction of two-layered authorization model over users and data, and (3) association with capability of precisely defining comprehensive privacy polices.

6. References

[1] Klaus Finkenzeller, RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification, John Wiley & Sons; 2 edition, New York, NY, 2003.

[2] W3C, "A P3P Preference Exchange Language 1.0 (APPEL1.0)", Apr. 15, 2002, http://www.w3.org/TR/P3P-preferences/.

[3] ContentGuard, "eXtensible rights Markup Language (XrML) 2.0 Specification", Nov. 20, 2001,

[4] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter, "Enterprise Privacy Authorization Language (EPAL 1.2)", 2003, http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/.