Privacy in the Digitally Named World with RFID Tags

Inoue, Sozo
System LSI Research Center, Kyushu University

Konomi, Shin'ichi
Center for LifeLong Learning and Design, University of Colorado

Yasuura, Hiroto
System LSI Research Center, Kyushu University

出版情報：Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, 2002-09. Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing
バージョン：
権利関係：

Privacy in the Digitally Named World with RFID Tags

Sozo INOUE*
sozo@c.csce.kyushu-u.ac.jp

Shin'ichi KONOMI †
konomi@cs.colorado.edu

Hiroto YASUURA*
yasuura@c.csce.kyushu-u.ac.jp

Abstract

Recent years' advances in information technology and system LSI technology are spreading computing resources into ubiquitous places in the real world. In such an environment, 'What we should not do' is important as well as 'What we can do', since the problem in the computer science directly results in the problem in the real world. In this paper, we discuss the possibility and challenges in the 'Digitally Named World', which is the environment in which 'radio frequency ID's (RFIDs) are attached to any goods in the world, and any objects in the real world can be found by the readers of the RFIDs and the networked database system. Especially, we address the problem of privacy and life-cycle management of the objects, and we propose the method for managing privacy about the relationship between objects and individuals.

1 Introduction

Recent years' advances in information technology and system LSI technology are penetrating computing resources into ubiquitous places in the real world[4]. Mobile phones, which are equipped with advanced multimedia processing and program execution are an example of the world.

This trend can be considered that, so to say, the impact of the information technology is moving from 'The virtual world realized in computers' to 'the real world where computers reside ubiquitously'. In such an environment, the total system security is a crucial issue, since the problem in the computer science directly results in the problem in the real world. 'What we should not do' is important as well as 'What we can do' for fundamental infrastructure of the ubiquitously computable world.

Our vision of the future world is the *Digitally Named World*, which is the environment in which 'radio frequency ID tags' (*RFID tags*) are attached to any goods in the world, they can be found anytime via the readers of the RFIDs and the networked database system, and they can be managed throughout their life-cycle. RFID tags are silicon chips with their IDs, radio frequency functions and some additional logic and memory[1]. Most of the RFID tags are supplied with power through radio frequency communication from external readers.

In this paper, we discuss the possibility and challenges in the digitally named world. The digitally named world can provide highly efficient object management, and will be widely spread, since the application area lies in any domains related to real objects[3, 2].

Especially, we address the problem of privacy in the digitally named world where objects are identified throughout the life-cycle. Privacy problem is important in the ubiquitous computing world[5, 6]. Careless disclosure of the relationship between a user and an object leads to the privacy invasion. We propose the solution for the problem by private and temporary identification codes, which the user can periodically update, on RFID tags.

In the rest of the paper, Section 2 describes the basic features of RFID tags, Section 3 addresses the challanges in the digitally named world, and Section 4 describes the method we propose for protecting privacy in the digitally named world. Section 5 is a conclusion.

2 RFID Tags

RFID tags are silicon chips with their IDs, radio frequecy functions and some additional logic and memory. In this section, we briefly describe the basic fea-

[a]System LSI Research Center, Kyushu University
6–1 Kasuga-Koen, Kasuga-Shi, Fukuoka 816-8580 JAPAN
[b]Center for LifeLong Learning and Design(L^{3}D)
University of Colorado, Boulder, Colorado 80309-0430, USA

tures of RFID tags.

2.1 Basic features

Figure 1 is the basic architecture of an RFID tag. It has usually no battery, and the power and the clock are supplied via external radio frequency communication. The RFID tag computes with the power and the clock, and sends the result via radio frequency communication. We call the device which communicates with the RFID tag supplying the power and the clock a *reader*. An RFID tag consists of an RF circuit which manipulates wireless communication, logic circuit which processes small steps of computation, and memories such as a read only memory (ROM) or an electrically erasable read only memory (EEPROM).

The memory is currently up to around 64kilobytes. RFID tags are implemented in many shapes such as an IC card, a key ring, and a seal. There exist RFID tags each of whose dimension except the antenna is under 1mm each. [10].

The communication time between a reader and an RFID tag is around 0.5 second, and the maximum communication distance is about 5 meters.

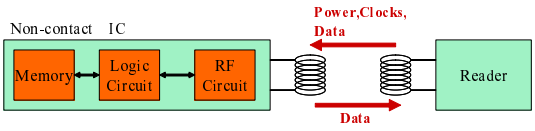

Figure 1: An RFID tag

Compared to other identification systems such as bar-code systems, fingerprint identification, and contacted communication IC cards, there are a lot of advantages of RFID tags: 1. illegal copy or falsifying is difficult, 2. read or write access time is short, 3. memory can be overwritten, 4. memory size is large, 5. RFID tags are hard to be broken, and 6. long-range and wide-range non-contacted communication is possible.

On the other hand, the disadvantage of RFID tags is that the RFID tags' cost is still high. This problem would be solved as the implementation technique progresses.

2.2 RFID applications

RFID tags are mainly used for effectively managing massive objects by setting identification code to the memory of each RFID tag and attach it to each object.

In supermarkets and clothing stores, effective sale and cost reduction are attempted by attaching RFID tags to goods and connecting readers to the POS (point of sale) system. For production and distribution stages of an object, attaching RFID tags to parts or products accelerate the performance of the production or the distribution system. These applications profit the property that RFID tags manipulates non-contacted communication. For example, the total prices of many goods can be instantly calculated without approaching the reader as the bar-code systems.

In libraries, large amount of books can be easily searched by attaching RFID tags to the books. Here, the reader is networked, and located on each bookshelf. The advantage of the system is that the users can search the location of the books without the books are arranged in order.

RFID applications are certain to be widely spread, since the application area lies in any domains related to real objects. Many applications are engaged in many fields such as non-contacted transportation tickets[9], anti-stealing car keys, and domestic animal identification.

2.3 Wireless communication

Wireless data communication is being rapidly popularized, such as Wireless LAN and Bluetooth technology. Although wireless communication provides an advantage of mobile communication, the following disadvantages are accompany:

1. The bandwidth of communication is limited, since several communication devices have to share a space as a communication medium.

2. The content of communication easily leaks to a third party, since the content travels through the air.

For 1, several approaches to share a space are proposed, such as TDMA, FDMA, SDMA, and CDMA. Moreover, for 2, data secrecy has been claimed, such as data encryption, frequency hopping.

Although the technologies above are effective, RFID tags cannot always fully adopt them in the current stage, because of the limitation of processing capability, the size of the RFID tags, and the production costs. The production costs are critical, because billions of people in the digitally named world will have zillions of RFID tags.

3 The Digitally Named World

In this section, we address the features required in the digitally named world.

3.1 Object identification throughout the life-cycle

Figure 2: The life-cycle of an object

One of the fundamental features in the digitally named world is the object identification throughout the life-cycle of the object as illustrated in Figure 2. Efficient recycling of an object is realized by embedding the information about the recycling or reusing the object such as materials, how to retrieve the materials, or how to disassemble. Current tagging techniques such as bar-code systems do not manage such information, because of the limitation of the record size and the limitation of the communication distance up to nearly contacted communication.

To our desirable point, object identification throughout the life-cycle can contribute to reduce the practical cost of RFID tags, since the cost of the RFID tag attached to an object throughout the life-cycle can be shared by multiple services. Each service, such as manufacturers, distributors, shops, users, and recycling merchants, pay less money if one RFID tag is attached to an object for long time. Thus, object identification throughout the life-cycle of the object is the fundamental feature that strongly promotes digitally naming world.

3.2 Security and privacy

In the digitally named world, objects passively have abilities to communicate with RFID tags, whereas the contents of the communication can leak to a third party as addressed in Section 2.3. Thus, information systems in the digitally named world must be designed to be secure even if the communication with an object leaks. Here, the security of a system includes the following:

1. The system is tolerant of attacks from an enemy.
2. The system is dependable against pretenders and data manipulation by by the pretenders.
3. The system can not invade the privacy of the inhabitants in the digitally named world.

In the rest of the paper, we focus on 3, that is, the privacy in the digitally named world, since the 1 and 2 highly depend on the security level of 3.

For 3, the private information leaks either only via the wired network or involving the communication between an RFID tag between a reader. We focus on the latter problem, since the former problem can be solved in a similar way to the old-fashioned computer networks, such as data encryption.

For the latter problem, placing private information on the RAM in an RFID tag, such as writing a credit card number onto the RAM, is obviously dangerous and therefore should be avoided, since the communication with RFID tags can be easily tapped. Furthermore, other cases related to the latter problem appears, which are unique to the digitally named world:

A. The relationship between the ID of an object and its user is known to a third party through the database system on the network.

B. A user is detected through the location of an object.

These cases lead to the result that the user is monitored, or traced by the third party who can obtain the information of the above two cases.

For A, assume an example of the environment in which readers are located everywhere. After the RFID attached to a product and its consumer are set to be related in a POS(point-of-sale) system, the product can be traced by the readers. This leads to the invasion of the privacy of the consumer, since the consumer will be traced through the location of the product. Although it will be convenient for the consumer if he/she can search the product for his/her own, allowing others to search the product is indesirable from the viewpoint of privacy.

B is the problem that a user is detected through the absolute or relative location of an object. For example, as a case of an absolute location, an object

located in a private room implies that the object is owned by the resident of the room. Another example, as a relative case, if a user walk through a ticket gate embedded with an RFID reader, the gate can detect the object the user accompanies, and relate the object and the user from the information of the commutation ticket. The leakage of the relationship between an object and a user, as shown above, leads to the same problem in 1.

4 Privacy Protection in the Digitally Named World

In this section, the solution for the privacy problem addressed in Section 4, which is a method for preventing third parties from detecting the relationship between an object and a user, is proposed. The basic idea of the method introduced is that the ID of an object is defined by the user who owns the object as he/she requires, and thus a third party can not know the ID and the relationship.

Our method can be used on the required stage of the life-cycle. For example, the problem of 1 and 2 is typical in the stage where consumers use the objects, although, the problem is not important in the production, distribution, sale, and recycle stage in Fig. 2. It is rather convenient and ecological if the method can be canceled. Proposed mechanism can employ the method as the user needs.

4.1 The system architecture

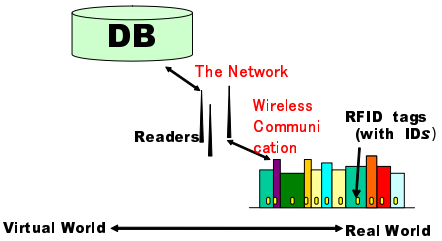

Figure 3: The system architecture

For the digitally named world, we assume the system as shown in Fig. 3. In the figure, the RFID tag attached to an object communicate with readers connected to the network. The user can obtain information which relates the object by searching the database system on the network through the ID of the RFID tag. The object and the readers might be placed on the public place many people shares. Therefore, a method to protect users' privacy, which we claimed as "preventing third parties from detecting the user who is related to an object", is necessary. One approach is the authentications for using a reader when a user is to communicate with an RFID tag through the reader. However, this approach is not sufficient to protect privacy, since the following factors can be considered.

- The users who are authenticated to use a reader can communicate with the RFID tags in the zone of the reader. Therefore, the users can identify the objects owned by another person if the objects are located in the zone.
- The users can identify an object on the site with a private reader, which have no authentication to use, even if the reader is not connected to the network.
- The communication between an RFID tag and a reader can be easily tapped, since an encryption is difficult on the current stage. A third party can identify an object by tapping the communication.

Thus, limiting accesses to an RFID tag to the authenticated reader can be assumed to be impossible, and preventing tapping the communication is also difficult.

The system architecture we assume above, in which RFID tags have an ID and readers are connected to the network, is considered to widely spread to the world, and the same architecture is assumed in the business solution with the Myu Chips[10].

4.2 Object identification for particular users

In this section, we describe the method to restrict object identification to particular users. Figure 4 is the overview of the method.

1. Each RFID tag has a read only memory(ROM) and an electrically erasable read only memory(EEPROM).
2. In the ROM, a unique and permanent identification code of the RFID tag is set by the producer.
3. ROM and EEPROM are used only exclusively. A user cannot read the ROM while a value is set to the EEPROM, and he/she can read the ROM only when the EEPROM has null value. The *ROM mode*, which is the state that the ROM is readable, and the *EEPROM mode*, which

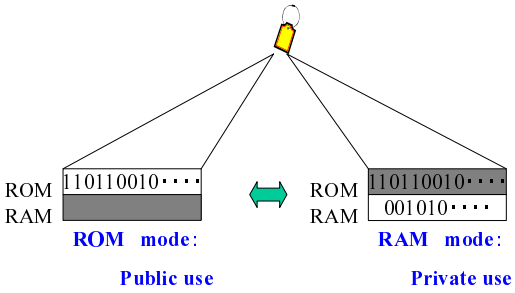

Figure 4: Restriction of identification to limited users

the state that the EEPROM is accessible, are changed by limited users who are allowed to.

For 3, several methods to limit the change the modes exist: to certificate the user for the change, and to restrict the change only via contacted communication or via communication in a short length up to several centimeters. Which method matches the system needs more discussions.

By the method above to limit the accesses to the memories exclusive, the following system manipulation is possible.

- In the ROM mode, unlimited object identification for any users is provided by the identification code of the RFID tag is set to the ROM by the producer.
- In the RAM mode, the restriction of object identification to limited users is achieved, in which the limited users set a private and temporary identification code which is only known to them to the EEPROM. That is, the third parties, who is the users other than the limited users, cannot operate the permanent object identification, even if they can know the private and temporary identification code. With the private and temporary identification code, the third parties can not recognize the relation between the code and the object except the visual information about the object which can be obtained by the on-site communication, since the information about the object in the network is distributed accompanying the permanent identification code on the ROM as a key. Therefore, the third parties have nothing to do with the private and temporary identification code. We discuss this further in Section 4.3.
- An RFID tag can be used in both limited and unlimited identification, and they can be switched for the requirements from the services. For example, an RFID tag on an object can provide unlimited identification with the ROM mode for total management at its production, distribution, and sale stage, and can be switched to EEPROM mode by a consumer when the object is handed to him/her. Afterward, the object can be identified only by the consumer. Moreover, the RFID tag can be switched to ROM mode again by a scrap merchant when the object is discarded, and the merchant can obtain the information about the object from the network with the permanent identification code, and utilize it for recycling. These cycle is realized by the double mode of a single RFID tag.
- The limited user who sets a private and temporary identification code can obtain the permanent identification code by once removing the value of the EEPROM before setting the private identification code onto the ROM, and they can obtain the information of the object from the databases on the network.

4.3 Discussions

Using the method shown in Section 4.2, we can prevent the problem, which we addressed in Section 4, that the relationship between the ID of an object and its user is known to a third party through the database system on the network. For example, a consumer can prevent an object of his/her from being identified by a shop, by setting the EEPROM value after the shop registers the relationship between the user and the object. Even if the value of the EEPROM is read by a reader by one of the methods shown in Section 4.1, users other than the user who set the EEPROM value can not know the relation between the value and the object.

On the other hand, the user who sets EEPROM value can know the object, the value on the EEPROM, and the value on the ROM when he/she sets the EEPROM value. Therefore, he/she can search both of the database about the object on the network and the object in the real world.

Additionally, the system dependability against pretenders and data manipulation, as addressed in 2 in Section 3.2, can be realized by our method. By continuously monitoring RFID tags by readers, and by the readers notifying an update of an EEPROMs to its related user, the related user, usually the owner of the object, can detect if it is a manipulation or an update by himself/herself.

Thus, we can prevent the problem that "the relationship between the ID of an object and its user is known to a third party through the database system on the network", however, this is not enough to prevent the problem that "the user who relates to the object would be detected by the third party". As addressed in Section 4, we must consider the problem that "a user is detected through the location of an object". That is, once the private identification code on the EEPROM are known to a third party, tracing a user by the third party is possible after the relationship between the private identification code on the EEPROM and the user is known. Some examples are shown in the following:

1. The private identification code on the EEPROM of an RFID tag of an object in a private house and the inhabitants are related.

2. A user who passes the ticket gate in a station and the private identification code on the EEPROM of an RFID tag of an object which accompanies the user are related.

For the problem, changing the private identification code on the EEPROM frequently is required.

Conflict management of private identification code is also required in such situation in which users frequently change the identification code of objects. One of the simple solutions is to make a particular area of the identification code the identification of the user who is related to the object, and the make the rest the user-defined identification code for the object. However, this method is not appropriate, since a third party can know the user who is related to the object, and can not prevent the close relationship between the object and the user. Here, we show 2 solutions for the conflict management: one is to establish an organization who manages the private identification codes which each user can use, and the other is to design the whole system which is tolerant to a conflict of the private identification code. The latter has a possibility to be a feasible solution, since the property that the object can not move to a remote place instantly can be utilized as another identification method of objects in the real world.

5 Conclusion

In this paper, we addressed the privacy issue in the digitally named world, in which objects in the real world can be detectable for computers by RFID tags. In the digitally named world, privacy issue arises when an object and a user are carelessly related. We proposed the method for protecting privacy by each user setting private and temporary identification code to each object. This method enables object management throughout the life-cycle of the object, since the permanent identification code can be utilized at the recycling stage, and therefore contributes to ecology.

Acknowledgment

This work has been supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 of the Ministry of Education, Science, Sports and Culture(MEXT) from 2002 to 2006. We are grateful for their support.

References

[1] P. Hewkin, "Smart Tags - The Distributed Memory Revolution". IEEE Review (1989).

[2] S. Konomi, "QueryLens: Beyond ID-based Information Access". To appear in: Proc. 4th Int'l Conf.Ubiquitous Computing (Ubicomp2002) (2002).

[3] R. Want, K. P. Fishkin, A. Gujar, B. L. Harrison, "Bridging Physical and Virtual Worlds with Electronic Tags". Proc. Int'l Conf. CHI 99 (1999) pp. 370–377.

[4] M. Weiser, "Some Computer Science Issues in Ubiquitous Computing". Communications of the ACM, 36(7) 1993, pp. 75–84.

[5] M. Langheinrich, "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems". Proc. 3th Int'l Conf.Ubiquitous Computing (Ubicomp2001) (2001).

[6] X. Jiang, J. Landay, "Modeling Privacy Control in Context-aware Systems Using Decentralized Information Spaces". IEEE Pervasive Computing, Vol. 1, No. 3, (2002).

[7] Finkenzeller, K. , 「RFID Handbook」, Nikkan Kogyo Pbl. Japan (2001).

[8] MIT AUTO-ID Center Homepage, http://www.autoidcenter.org/.

[9] Japan Railway Co. Ltd. East, "Suica Card", http://www.jreast.co.jp/suica/.

[10] Hitachi Co. Ltd., "Myu Chip", http://www.hitachisemiconductor.com/sic /jsp/japan/eng/gain/135/next/