RFID PASSWORD MANAGEMENT METHODS FOR FALSIFICATION PREVENTION IN BOOKSTORE MANAGEMENT USING SECURE RFID TAGS

Yuichi Kobayashi, Yoji Taniguchi
Hitachi, Ltd., Systems Development Laboratory, 1099 Ohzenji, Asao, Kawasaki, Kanagawa, 215-0013, Japan

Toshiyuki Kuwana
Hitachi, Ltd., Tracing & Tracking Systems Division, 890 Kashimada, Saiwai, Kawasaki, Kanagawa, 212-8567, Japan

Masanori Akiyoshi
Graduate School of Information Science and Technology, Osaka University, 2-1 Yamada-oka, Suita, Osaka, 565-0871, Japan

Keywords: RFID, falsification prevention, risk analysis.

Abstract: The receipt data on radio frequency identification (RFID) tags attached to books may be used to prevent shoplifting in bookstores. To protect the receipt data, it is important to manage the passwords of RFID tags. We use Secure RFID tags, which protects data with an RFID password, for preventing falsification of RFID data. We also propose ten methods that manage RFID passwords from the point of the phases of RFID passwords and the ways a password is associated with a Secure RFID tag. We analyze and compare these methods using fault tree analysis. We show that our proposed RFID passwords management methods are effective in preventing falsification for resale.

1 INTRODUCTION

The shoplifting of books is a serious problem in Japan. A report says that there are many shoplifted books for resale. The publishing industry in Japan is examining a method for attaching an RFID tag to books, which records receipt data on the RFID tag memory. However, there is a risk of someone reselling a shoplifted book to a second-hand bookstore, after illegally overwriting the receipt data in the RFID tag. So a method for protecting the data in the RFID tag is needed.

There are several methods that mount hash logic on an RFID tag and authenticate the user to protect the RFID data (Weis 2003; Engberg, Harning & Jensen 2004; Tripathy & Nandi 2006). However, these methods are not realistic in a situation in which an RFID tag is attached to a book because mounting advanced calculation logic on an RFID tag requires a larger IC chip, which increases the cost of the RFID tag.

Secure RFID tags are low cost RFIDs. This type of RFID tag protects data using a simple password authentication method. We chose to use Secure RFID tags because these tags are smaller, cost less, and suitable for attaching to books. It is very important to manage an RFID password when using Secure RFID tags. Therefore we propose ten methods for managing RFID passwords. We analyze their security, and show that they are effective in preventing falsification.

2 BOOK MANAGEMENT SYSTEM WITH SECURE RFID TAGS

In this chapter, we describe the book management system with Secure RFID tags in a bookstore environment.

Kobayashi Y., Taniguchi Y., Kuwana T. and Akiyoshi M. (2008).
RFID PASSWORD MANAGEMENT METHODS FOR FALSIFICATION PREVENTION IN BOOKSTORE MANAGEMENT USING SECURE RFID TAGS.
In *Proceedings of the International Conference on e-Business*, pages 447-453
DOI: 10.5220/0001908504470453

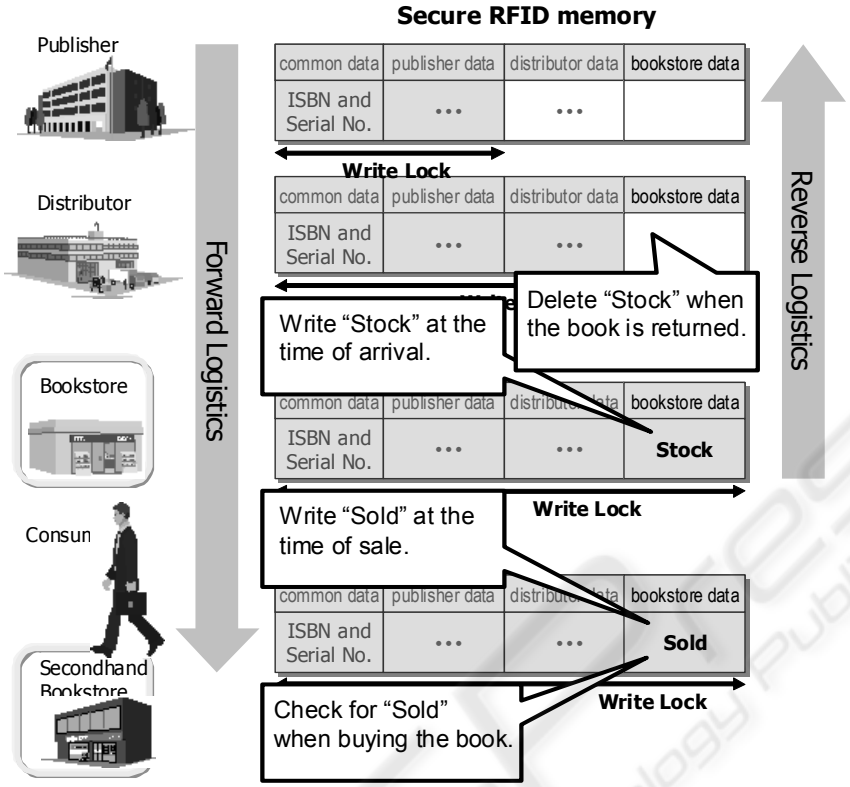

Figure 1: Shoplifter prevention method.

2.1 Book Distribution Procedure for Preventing Shoplifting

The publishing industry in Japan is considering a method for preventing shoplifting by using Secure RFID tags. Figure 1 shows the procedure for preventing shoplifting in a book distribution. First, a bookstore writes in "Stock" onto the Secure RFID tag when a book arrives from a distributor. This denotes the state before being sold. Next, when a consumer buys the book, the bookstore changes "Stock" to "Sold" in the Secure RFID tag. At the entrance of the store, the security system reads the data on the Secure RFID tags to check if the book was purchased. Finally, when a second-hand bookstore buys a book from a consumer, it checks whether the book's Secure RFID tag reads "Sold" or "Stock". Not only bookstores, but second-hand bookstores cooperate with the publishing industry. All the companies relevant to book publishing and selling can examine the system to counter the shoplifting problem.

In order for this system to work, the data of the Secure RFID tag must not be able to be easily rewritten from "Sold" to "Stock". Rewriting information should be done with an access control function with a password of the Secure RFID tag.

2.2 An Existing RFID Passwords Management Method

Figure 2 shows the RFID password management system for a bookstore.

Operation 1: When the book arrives, the book's code written in the Secure RFID tag is read, and the pre-arrival data is checked. After it is checked, the book code is input into the server with the arrival data. Then, the date of arrival, bookstore code, "Stock", etc... are written onto the Secure RFID tag. An RFID password is then set up for the Secure RFID tag, and the memory is locked using that password.

Operation 2: When the book is sold, the book code in the Secure RFID is read, the price is checked, and the sale information is input into the server. At this time, the memory of the Secure RFID tag is unlocked by using the RFID password, and "Sold" is rewritten onto the Secure RFID tag. Finally, the memory is locked again by using the password.

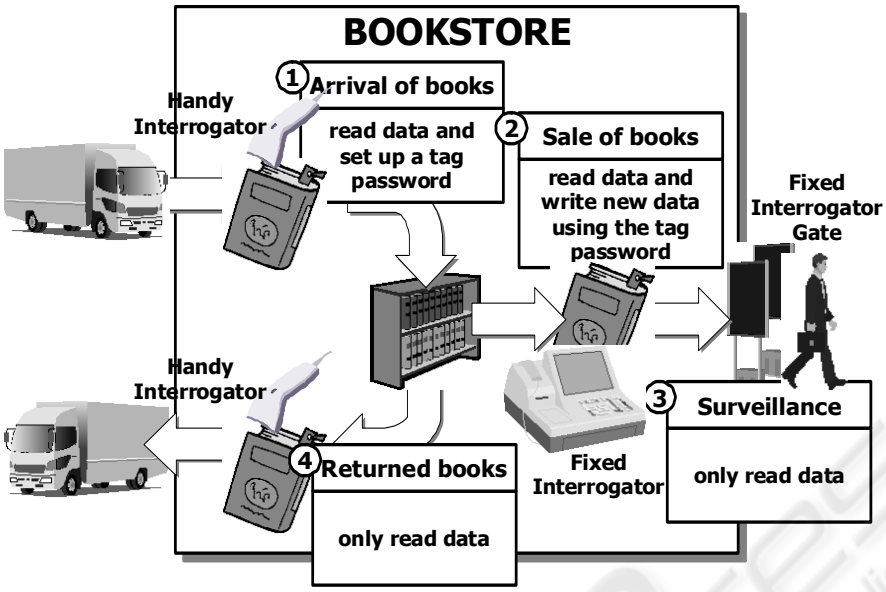

Figure 2: System using the Secure RFID tags in the bookstore.

Operation 3: A gate type interrogator system at the entrance is set up, and the interrogator checks if "Sold" or "Stock" is written on the Secure RFID tag.

Operation 4: If the book is returned, the memory of the Secure RFID tag is unlocked by using the RFID password, and all data from the bookstore and the password are deleted. Afterwards, the returned book's information is input into the server.

The publishing industry in Japan tries to manage RFID passwords by using identical passwords in all bookstores, and applies the RFID password management method for each bookstore. This method has the advantage of being less expensive; however, if one RFID password is stolen, all Secure RFID tags are compromised. The possibility of information being falsified on the Secure RFID tags attached to books stocked in all bookstores is high. Therefore, the distinction between a shoplifted book and a legally bought one becomes difficult in a second-hand bookstore, and the effect of preventing theft by using the Secure RFID tag weakens. It is necessary to manage RFID passwords more carefully.

3 RFID PASSWORDS MANAGEMENT METHODS

We propose ten methods for managing not identical RFID passwords but different passwords so that the risk after a password is stolen will be lessened. It is effective to divide RFID passwords into groups to manage different RFID passwords. For example, the group includes an inspection interrogator, a book, etc… Moreover, because it is usually impossible to read the RFID password set in the Secure RFID tag, it is necessary to set the RFID tag with an RFID password beforehand. Therefore, we present ten methods which can be used to manage RFID passwords from the point of a phase of RFID password management and the ways in which a password is associated with a Secure RFID tag. Figure 3 shows the relationship between the phase of RFID passwords, and the ways passwords are used for a Secure RFID. There are four phases of RFID password management, (1) each bookstore, (2) each inspection interrogator system, (3) each arrival, and (4) each book. On the other hand, there are (a) the way of using a conversion table, (b) the way of using operation logic, and (c) the way of updating a key.

We define the combination of phases of RFID passwords and the ways a password is used for a Secure RFID tag as the RFID password management methods.

3.1 Phases for Managing RFID Passwords

A bookstore that manages RFID passwords separately by each group lessens the risk of RFID tag falsification more than a bookstore that manages identical RFID passwords. We explain the phases for managing RFID passwords as follows.

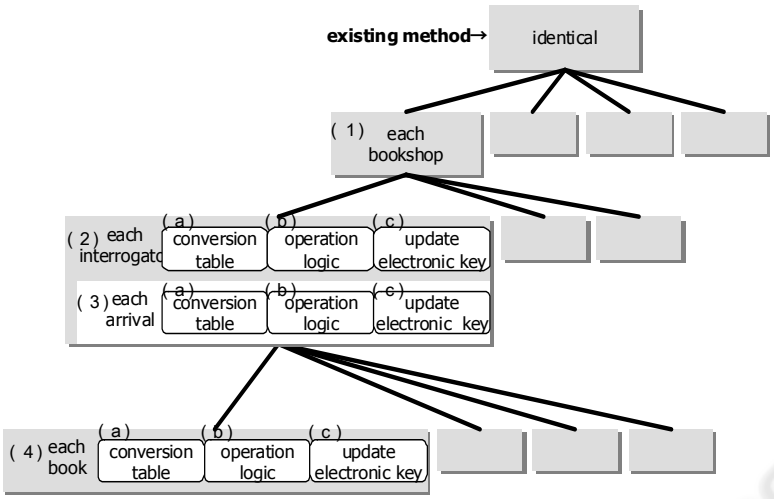

Figure 3: Classification of Password Management Methods.

(1) *Each bookshop*: Manage the different RFID passwords in each bookstore. Each bookstore decides and manages an RFID password.

(2) *Each interrogator system*: Manage the different RFID passwords in each interrogator system in a bookstore when the book arrives. Each interrogator sets up an RFID password and an interrogator's ID to the Secure RFID tag attached to the newly arrived book.

(3) *Each interrogator system and arrival*: Manage the different RFID passwords in each interrogator system in a bookstore when the book arrives and update the RFID passwords each time books arrive. Each interrogator system sets up an RFID password, an interrogator's ID, and the arrival date to the Secure RFID tag.

(4) *Each book*: Manage the different RFID passwords in each Secure RFID tag attached to the book. The bookstore associates the RFID password with a unique ID that identifies the Secure RFID tag.

It is possible to manage the different RFID passwords in each title of the book. However, the titles with only one book in stock accounts for 70% of the inventory in most bookstores. Therefore, we omit the explanation for each title here because each title and each book are almost the same.

3.2 Ways in which RFID Passwords are Associated with a Secure RFID Tag

When a different RFID password is set to a Secure RFID tag, the system should associate that password with that Secure RFID tag. We explain the ways in which this is accomplished.

(a) *Conversion table*: The system generates the RFID password at random, and associates the RFID password with the interrogator's ID, arrival date, or a unique ID written to the Secure RFID tag to identify the phase of RFID password management.

(b) *Operation logic*: Use operation logic with an electronic key. The system generates an RFID password by calculating data, such as the interrogator's ID, arrival date, or a unique ID written to the Secure RFID tag (Kobayashi, Kuwana, Taniguchi & Komoda 2007).

(c) *Update electronic key*: Periodically update the electronic key used in (b).

4 SECURITY EVALUATION OF RFID PASSWORD MANAGEMENT METHODS

In this chapter, we show the results form a fault tree analysis (FTA) of the RFID password management methods, and compare those analysis results.

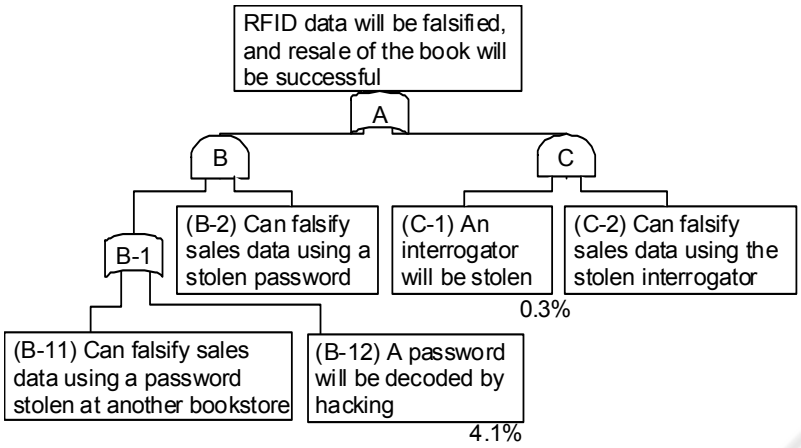

Figure 4: FTA of shoplifting a book.

4.1 Fault Tree Analysis of RFID Passwords Management Methods

We analyzed the security performance of the RFID password management method, which combined the phase of an RFID password and the ways in which the password is associated with a Secure RFID tag described above, using FTA.

We know that the probability of a successful falsification of RFID data for resale is low; the RFID password management method will have a high security performance. Therefore, let a top event of FTA be the probability that the RFID data of a shoplifted book will be falsified, and resale of the book will be successful in one month. Moreover, it is necessary to decipher the RFID password of the Secure RFID tag so that someone may falsify the RFID data. There are two effective attacks for deciphering an RFID password. The first is that someone illegally uses a common interrogator and hacks into the Secure RFID tag like brute force attack. The second attack is that someone steals and illegally uses the handy interrogator of the bookstore. The FTA is shown in Figure 4. The probability of each event of FTA is explained below.

(B-11): This event is the probability of falsifying the RFID data of a bookstore using the RFID password stolen at another bookstore. In the existing RFID password management method, this probability $P_{B\text{-}11}$ is 100% because an RFID password is identical at all the bookstores. In the proposed RFID password management method, this probability $P_{B\text{-}11}$ is 0% because the RFID passwords at least differ for each bookstore.

(B-12): This event is the probability that an RFID password will be decoded in one month by hacking into a Secure RFID tag. This probability $P_{B\text{-}12}$ was obtained from the following expression.

$$P_{B-12} = 1month/E(Time) = 4.1\% \qquad (1)$$

E (Time) is an expected time spent on the hacking attack. The time that a Secure RFID tag is checked whether one password is right using one interrogator is assumed to be about 30 milliseconds and the length of the Secure RFID password is assumed to be 32 bits according to the specification of Secure RFID.

(B-2): This event is the probability of falsifying sales data on a Secure RFID tag in one month using a common interrogator. This probability depends on the number of books that can be falsified using a decoded RFID password. This probability $P_{B\text{-}2}$ is 100% in the case of the existing method or "(1) each bookstore" because all RFID passwords in the bookstore are the same. In the case of "(2) each interrogator", this probability $P_{B\text{-}2}$ is 33% when there are three interrogators for inspection is three. In the case of "(3) each interrogator and arrival", this probability $P_{B\text{-}2}$ was obtained by the following expression.

$$P_{B-2} = 1/IN \times ABN/BN = 27\%, \qquad (2)$$

where *IN* denotes the number of the interrogators for inspection, *ABN* denotes the number of applicable stocked books, and *BN* denotes the number of stocked books. The applicable stocked book means the books that remain unsold for one month because the

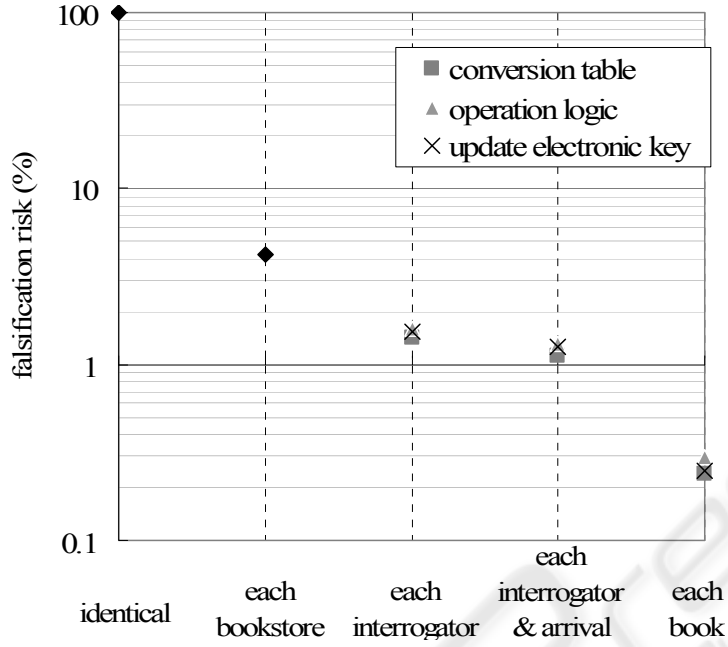

Figure 5: Relationship between the management phases and the falsification risk.

decoded RFID password is associated with those books. *IN* is assumed to be three and *ABN*/*BN* is assumed to be 0.79 because the merchandise turnover is about 17%, and the update frequency of the RFID passwords is once a week. In the case of "(4) each book", this probability P_{B-2} is 1% when the number of books stolen in one month in one store is 100, because the number of books that can be falsified by using the decoded RFID password is only one.

(C-1): This event is the probability that an interrogator will be stolen from a bookstore in one month. Here, this probability P_{C-1} is assumed to be 0.3%.

(C-2): This event is the probability of falsifying sales data on a Secure RFID tag in one month using the stolen interrogator. This probability depends on the ways in which an RFID password is associated with a Secure RFID tag. In the case of "(a) conversion table", this probability depends on the managing phase of RFID passwords because the conversion table is contained in the interrogator of the bookstore. This probability P_{C-2} is 100% in the case of "(1) each bookstore", 33% in the case of "(2) each interrogator" or 27% in the case of "(3) each interrogator and arrival", as well as in the case of the (B-2) event. In the case of "(4) each book" this probability P_{C-2} is 76% because the merchandise turnover is about 17% and the update frequency of the RFID passwords is once a day. In the case of "(b) operation logic", this probability P_{C-2} is 100% because the operation logic is contained in the interrogator of the bookstore. In the case of "(c) update electronic key", this probability can be estimated at 80% when changing the key once a week.

The result of FTA for each RFID password management method is shown in Table 1. The RFID password management methods below from "(1) each bookstore" is classified into the phases of RFID password management and the ways in which an RFID password is associated with a Secure RFID tag. The falsification risk in Table 1 is the probability that falsification of the RFID data for resale will be successful. This falsification risk is low because the security of the method is high.

4.2 Comments of the Results of FTA

Figure 5 shows the probability that a falsification will be successful for each RFID password management method. This figure also shows that the difference between the phases of RFID password management is larger than the difference between the ways in which a password is associated with a Secure RFID tag. We found that it is better to manage RFID passwords in several phase. Moreover,

all the RFID password management methods are effective in preventing falsification for resale because the highest probability that falsification will be successful for "(1) each bookstore" is 4.25% for all the methods.

Table 1: Comparison of the security risk for each RFID password management method.

RFID passwords management method		**Falsification Risk**
Identical		100.00 %
(1) Each bookstore		4.25 %
(a) Conversion table	(2) Each interrogator	1.42 %
	(3) Each interrogator & arrival	1.13 %
	(4) Each book	0.24 %
(b) Operation logic	(2) Each interrogator	1.58 %
	(3) Each interrogator & arrival	1.31 %
	(4) Each book	0.30 %
(c) Update electronic key	(2) Each interrogator	1.53 %
	(3) Each interrogator & arrival	1.26 %
	(4) Each book	0.25 %

5 CONCLUSIONS

We proposed methods that use Secure RFID tags and RFID password management for preventing falsification of RFID data in book distribution. These proposed methods were explained by the point of phases of RFID passwords, and the ways in which a password is associated with a Secure RFID tag. We showed that these methods decreased the probability of falsification to about 5% or less in this situation. These results are useful for RFID password management in bookstores.

ACKNOWLEDGEMENTS

This paper is based on the achievement of a Japanese National Research and Development Project, the "Secure RFID Project" that was conducted by METI (Ministry of Economy, Trade, and Industry) for the eight months from August 2006 to March 2007.

REFERENCES

Weis, S 2003, 'Security and Privacy in Radio-Frequency Identification Devices', Masters Thesis, Massachusetts Institute of Technology.

Engberg, SJ, Harning, MB & Jensen, C 2004, 'Zero-knowledge device authentication: Privacy and security enhanced RFID preserving business value and consumer convenience', in *the Second Annual Conference on Privacy, Security and Trust (PST'04)*, pp.89-101

Tripathy, S & Nandi, S 2006, 'Robust Mutual Authentication for Low-cost RFID Systems', in *4th Int. IEEE Conf. Industrial Informatics (INDIN'06)*, pp.949-954.

Kobayashi, Y, Kuwana, T, Taniguchi, Y & Komoda, N 2007, 'Group Management System of RFID Passwords for Item Life Cycle', in *Emerging Technologies and Factory Automation (ETFA 2007)*, pp.884-887.