applied sciences

MDPI

Article

Mutual Authentication Protocol for Role-Based Access Control Using Mobile RFID

Bing-Chang Chen [1,*], Cheng-Ta Yang [2], Her-Tyan Yeh [1] and Ching-Chao Lin [1]

[1] Department of Information and Communication, Southern Taiwan University of Science and Technology, Tainan 71005, Taiwan; htyeh@stust.edu.tw (H.-T.Y.); 4a3f0030@stust.edu.tw (C.-C.L.)

[2] Department of Multimedia and Entertainment Science, Southern Taiwan University of Science and Technology, Tainan 71005, Taiwan; zada@stust.edu.tw

* Correspondence: bcchen@stust.edu.tw; Tel.: +886-6-253-3131

Academic Editor: Teen-Hang Meen

Received: 31 May 2016; Accepted: 21 July 2016; Published: 29 July 2016

Abstract: The Internet has become the main transmission media in modern information systems due to the popularization of information technology and the rapid development of network technology. To use the Internet, we need complete security mechanisms which include requirements such as integrity, security and privacy to ensure the legal user can login to a remote server to get the service and resources they need. The radio frequency identification (RFID) is a very convenient technology with the property of non-contact reading. It uses the tag embedded in the object to identify the information quickly. Now, more and more devices are equipped with the RFID reader. Hence, the user can use the RFID reader embedded in the mobile device through a wireless network to read the information on the tag and then use the service which is called Mobile RFID. Compared to traditional RFID, the characteristic of mobility makes the reading more flexible. It can deal with the events in real-time and undertake the process faster and more efficiently. The major security problem of Mobile RFID is privacy, which is also a consideration when constructing a Mobile RFID Mechanism. In this paper, we propose a secure authentication mechanism which uses the authenticated delegating mechanism in Mobile RFID to enable the reader to get the specific role authority through a back-end database server. The reader has to undertake mutual authentication with the back-end database server and the tag. Then, it can protect the information and limit the access times of the reader to achieve privacy.

Keywords: mobile RFID; role-based access control; mutual authentication

1. Introduction

The popularization of computers and the development of network technologies have made the Internet an integral transmission medium for modern information systems. Completeness, security, and confidentiality are the requirements when transmitting information over the Internet. Thorough security mechanisms ensure that only legal users log into remote servers to retrieve services and data. The effective prevention of malicious online attacks is an important issue in information security. With advances in radio frequency identification (RFID) technology, handheld devices with an RFID reader have become more prevalent. As such, users can utilize handheld RFID readers via wireless Internet to obtain the information or services stored within electronic tags. The largest problem of mobile RFID is privacy. Therefore, the protection of users' privacy must be considered when establishing a mobile RFID network.

RFID systems are contactless identification systems that transmit data via radio waves so that large amounts of data can be read without requiring any contact. With modern technological advances, RFID has been applied in numerous industries. Mobile RFID and traditional RFID technologies differ

in that the system need not be stored in a fixed location, but can be embedded into a mobile reader, such as a personal digital assistant (PDA) or cell phone. Mobile RFID uses high frequency RFID as a close-range sensor and uses telecommunication services to transmit data. However, the largest issues with this technology are security and privacy for the reader [1].

This study proposes a certification mechanism so that the back-end database can verify readers and authorize them in a mobile RFID architecture. The reader accesses the role-based access control (RBAC) server in a back-end database and receives permission for two-way identification of the database and electronic tag while restricting the number of tag reads and the readable information content.

2. Relative Works

Electronic tags improve upon traditional barcodes, which are read by a barcode reader via the photoelectric effect, converting light information into electronic information to retrieve the data stored within the code. While barcode recognition requires a close proximity to be successfully read, RFID tags can actively or passively emit radio waves, making them able to be correctly identified within range of the waves. The read distances for RFID differ with the output power and frequency used. As radio waves have a high penetrating power, the contents can be scanned through a barrier such as product packaging.

Recently, mutual authentication protocols in RFID systems were proposed [2,3]. In [2], a mutual authentication propocol is achieved with time stamps, hash function function and PRNG (Pseudo-Random Number Generator). In [3], it proposed a lightweight anonymity and mutual authentication protocol. There are some new information security issues of RFID were addressed in [4]. However, there is no literature which discusses the topic for both the RFID authentication and RBAC.

2.1. RFID Security Requirements

Although RFID is contactless and provides quick recognition, the transmission of information through wireless communications poses a problem with regard to privacy and malicious attackers. Therefore, a safe RFID protocol must meet the following requirements:

(1) Data integrity: The RFID should still be able to identify information even if the tag has been attacked and modified.
(2) Confidentiality independence: Even if a tag has been compromised and the key is known, it cannot be used to forge other tags in order to deceive the back-end server.
(3) User privacy: An attacker cannot use the information sent by a tag to retrieve all the data within the tag to determine its location.
(4) Forward secrecy: Even if an attacker is able to compromise a tag and retrieve the data stored within the tag, that information cannot be used to find previously sent data.
(5) Protection against replay attacks: Even if an attacker can obtain the legal information sent from a tag to a reader, repeated sending of this data cannot be used to deceive the back-end server.
(6) Protection against denial of service attacks: Even if an attacker can intercept or block data to cripple the system, the RFID system can still identify tags normally.
(7) Protection against forgery attacks: Even if an attacker illegally obtains some of the information within a tag, it cannot be used to forge a legal tag and deceive a legal reader.

2.2. Mobile RFID Technology

Mobile RFID uses a mobile device such as a cell phone or PDA to quickly retrieve data from a product's electronic tag using wireless Internet. As RFID systems have multiple applications, there are a multitude of possible reading environments and applications. Mobile RFID is mainly used when the electronic tag must be used with a mobile reader. Therefore, this study proposes a mobile reader to read tags based on the mobile RFID infrastructure created by Lee and Kim [5]. After the mobile reader reads the electronic tag, the embedded middleware sends information to the authentication

server (AS), after which the AS, object name server (ONS), electronic product code information service (EPCIS), and service provider send relevant tag information back to the user's mobile reader.

According to the mobile RFID infrastructure proposed by Lee and Kim [5], mobile readers read tags in seven steps (Figure 1).

Step 1: The mobile reader requests to read the electronic tag and receives a reply.
Step 2: The mobile reader reads the information in the electronic tag and sends it to the AS.
Step 3: After AS certification, it inquires the ONS for the detailed information storage address for the electronic tag.
Step 4: The ONS receives the inquiry and sends the electronic tag URL to the AS.
Step 5: The AS retrieves the information in the electronic tag from the object information server (OIS) via the URL.
Step 6: The OIS sends the electronic tag information to the AS.
Step 7: The AS sends the electronic tag information to the mobile RFID reader.

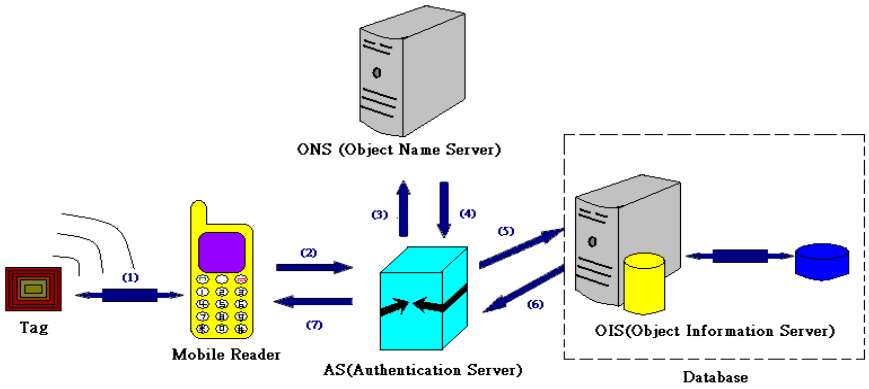

Figure 1. The steps of reading tags for mobile readers.

2.3. Role-Based Access Control

RBAC was introduced in 1992 by Ferraiolo and Kuhn [6] and mainly uses user-role-permission to control user access. Roles are given to users based on their position or work content within an organization. Thus, users indirectly obtain a role-class. When a user's position changes, their role is simply adjusted, thus lowering the administrative cost and increasing convenience. Sandhu et al. [7] later improved the model and named it NIST (National Institute of Standards and Technology) RBAC [6].

Recently, RBAC [7–11] has become a hot topic in the field of access control. Compared to normal access control policies, RBAC adds a role between the user and permission. This simplifies changes to user access and lessens the burden for management.

In actual application systems, with a low number of roles, managers can effectively centralize role management, use, and access. However, as systems have become more complex and as the number of roles increases, in a large distributed environment, system management of the relationship between these roles is a difficult problem. Completely relying on centralized management will place a great burden on managers. Entrusting role access in a distributed system can create an RBAC model that allows users to entrust other users with their role-class so that the entrusted user can complete work for the original user, further reducing the management burden.

Entrusting access is an important technology that improves the application of distributed environments. There are three basic elements that make up RBAC: 1. Users that describe role-class; 2. Permission that describes the tasks for each role, where the tasks in the system may be abstract; 3. Roles that are combinations of users and permissions, with the roles listing users and their respective access.

Access control based on roles includes four elements that each have their own corresponding relationships. These elements are users (USERS), roles (ROLES), permissions (PRMS), which are further

divided into operations (OPS), objects (OBS) and sessions (SESSIONS). Each element is explained in further detail below.

- USERS: Human beings that interact with the system or artificial intelligence, such as intelligent robots.
- ROLES: Work functions or work positions that can be seen as a role within an organization or access control mechanism and are used to determine permissions within a firm.
- PRMS: Authority regarding objects in an access machine, including methods of storage and retrieval or operations.
- SESSIONS: Duration of role assignment, indicating the start and end times that a user has a certain role.

The corresponding relationships between these elements include User Assignment (UA), Permission Assignment (PA), User_Sessions, and Session_roles. These are explained in detail below.

- UA: Users can have more than one role and roles can be assigned to more than one user. Sessions are the unit for access control. During any session, users can only act in one role. Many different roles with different functions simultaneously participate in any session. Conferences include directors, operational managers, marketing managers, and project members. However, for this session, participants may have more than one role.
- PA: Roles can have more than one permission, and permissions can be assigned to more than one role. When maintaining the relationships between users and roles and between roles and permissions, users' roles can be changed, added, or removed, effectively changing, adding, or removing permissions. This simplifies work for managers and work systems which, in turn, reduces costs.
- User_Sessions: When a user wishes to use the role assigned, a user session is created. A single user can create multiple sessions, but a user session can only correspond to one user.
- Session_roles: Session_roles are the roles for the users included in a user session. User sessions can have more than one role and roles can be used in more than one user session.

The hierarchical relationship between roles mimics the actual structure within the organization, such that users can inherit the permissions for each role, reducing management efforts.

Early RBAC was mainly adopted for internal employee access system resources and designed with intelligent agents for a firm's intranet in order to aid in safety control systems where role assignment and permissions could manage access systems.

RBAC can be used on the Internet, where a role-server stores user-role assignments. When users retrieve information, identity is first verified with the role server before the role can be utilized. Then a service request is made with the web server and role information is displayed. Finally, the web server uses role-permission-assignment, the role hierarchy, and relevant restrictions to determine whether this role is permitted to complete the request.

3. System Architecture and Concept

The RBAC server assigns role-classes to restrict the number of times a mobile reader can retrieve information. This study proposes an RBAC role-class appointment certification protocol that can be used in a mobile RFID network where the back-end database assigns role-classes to readers. When a reader retrieves the permissions given to a role, the reader first verifies the permissions with the back-end database and then reads the electronic tag. The proposed method also authorizes readers, and the number of times one reader retrieves tag information is not affected when other readers read the same tag.

3.1. Mobile RFID System Architecture

When an unauthorized reader makes a request to read an electronic tag, it must first undergo two-way verification with the back-end database. The database gives the reader a security certificate

and then restricts its working parameters according to the role-class table in the RBAC server which is illustrated in Figure 2.

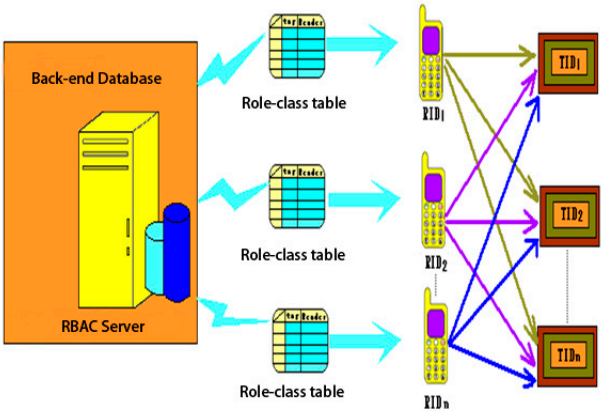

Figure 2. The diagram of role-class assignment.

The RBAC server recognizes the reader's identity to prevent illegal readers from stealing information. In this complex procedure, as RFID readers must be given role-classes, the server must effectively control roles that can read RFID tags. This study proposes that roles serve as keys to authenticate users, assign roles, and manage role keys and user permissions to read RFID tags. If RID_1 reads TID_1, it needs to acquire the relative role-class to access the information of the tag. We will propose the detailed mechanism in Section 3.3.

3.2. RBAC Server Architecture

Before a reader authority is verified with the back-end database, it must first be certified by the RBAC server and retrieve its permissions from the role-class table in the RBAC server to know its executable actions.

Figure 3 shows the process by which the server determines role-class for users. When a user uses the mobile RFID, the back-end database certification system and the RBAC database permissions table determine that user's role-class.

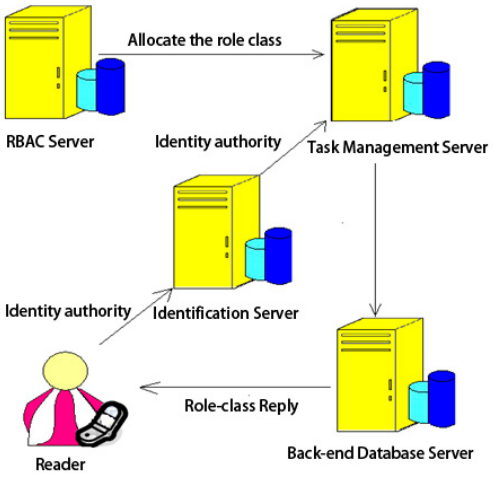

Figure 3. Role-based access control (RBAC) Server Architecture.

For a reader to read an electronic tag, after it is certified by the back-end database, the assigned role-class along with the maximum number of reads can be used to determine the reader's RID_1 and

TID_1 role and permission level. When a reader receives certification from the back-end database, it is also given a role-class level and a maximum number of reads. When a reader reads an electronic tag, one read is sent to the tag and removed from its maximum number of reads.

3.3. Mobile RFID System Architecture

3.3.1. Reader Security Certificate and Role-Class Architecture

Readers must obtain a security certificate from the back-end database and send the command for the electronic tag to the RBAC server to obtain a role-class. Readers obtain role-classes and security certificates from the RBAC server in the back-end database.

A two-way security mechanism was designed for the back-end database and reader to give the reader a security certificate and a role-class. Table 1 shows the symbols used in the certification mechanism, and Figure 4 shows the reader safety certification mechanism.

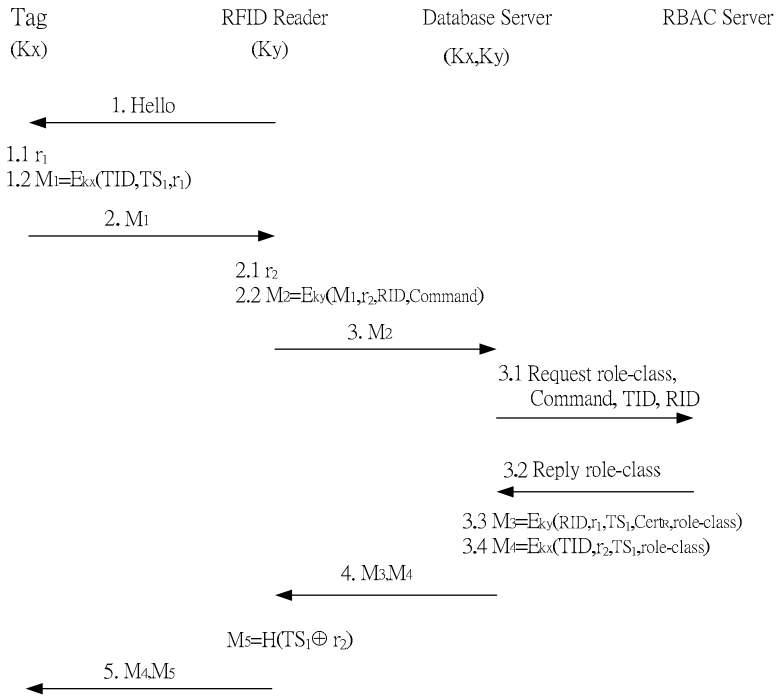

Figure 4. The reader safety certification mechanism.

Step 1: A reader reads an electronic tag by sending a HELO command to the tag

Step 1.1: The tag creates a random number r_1

Step 1.2: The electronic tag ID TID, time stamp TS_1, random number r_1, and the shared key between the back-end database and the tag K_x are used to create an encrypted M_1, which is sent to the reader

Step 2: The electronic tag sends M_1 to the reader

Step 2.1: The reader receives M_1 and creates a random number r_2

Step 2.2: The reader ID RID, tag read request, random number r_2, M_1, and the shared key between the back-end database and reader K_y are used to create an encrypted M_2

Step 3: The reader sends M_2 to the back-end database

Step 3.1: The request role-class command, read tag command, TID, and RID are sent to the back-end database

Step 3.2: A role-class is sent to the reader

Step 3.3: The RID, random number r_2, initial tag time stamp TS_1, reader security certificate $Cert_R$, role-class, and K_y are used to create M_3, which is sent to the reader. The RID, random number r_1, role-class, and K_x are used to create M_4, which is sent to the electronic tag

Step 4: The reader receives M_3 and uses K_y to decrypt random number r_1, initial tag time stamp TS_1, reader security certificate $Cert_R$, and the role-class. TS_1 and r_2 are used in a hash function to create M_5

Table 1. Certification mechanism symbols.

r_1, r_2, r_3	Random numbers generated by the electronic tag reader and back-end database
TID, RID	Electronic tag identification number and reader identification number
$TS_1 \ldots TS_{n-1}$	Time stamp
command	Reading command sent from reader to electronic tag
role-class	Role and permissions
$Cert_R$	Security certificate given to the reader by the back-end database
TC_n	Number of times n a reader can retrieve information
K_x	Shared back-end database key for an electronic tag
K_y	Shared back-end database key for a reader
M_n	Encrypted value using the shared keys K_x and K_y

3.3.2. Number of Reads and Time Stamp Updating

The reader must first be authorized by the back-end database before it is given a security certificate. Then, after certification with the back-end database, it can read the electronic tag. In this mechanism, the back-end database first verifies the reader to permit it to read the electronic tag information. The proposed method authorizes readers, and the maximum number of times one reader can retrieve tag information and the updated time stamp are not affected when other readers read the same tag, in order to increase security. Figure 5 shows the architecture for the maximum number of reads and time stamp updating. Every reader has its allocated reading amount. If a reading is requested, the allocated reading amount will decrease by 1 time. The detailed mechanism is illustrated in Figure 6.

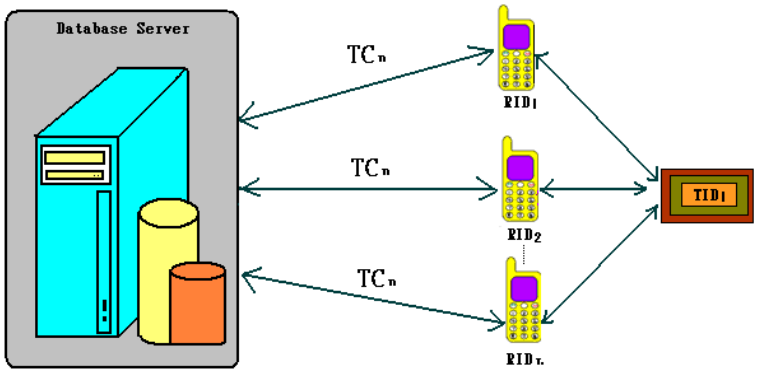

Figure 5. The architecture for the maximum number of reads.

After receiving security authorization, the reader reads the electronic tag and the tag automatically updates the time stamp and uses the shared key to send it to the back-end database. The role-class is compared to the internal table to confirm executable commands, and the remaining number of reads is

sent back to the reader. After the reader is given a security certification from the back-end database and reads an electronic tag, the database notifies the reader of the remaining number of reads and the updated time stamp. These are then recorded in the back-end database. Figure 6 shows the mechanism for the number of reads and RBAC role-class certification.

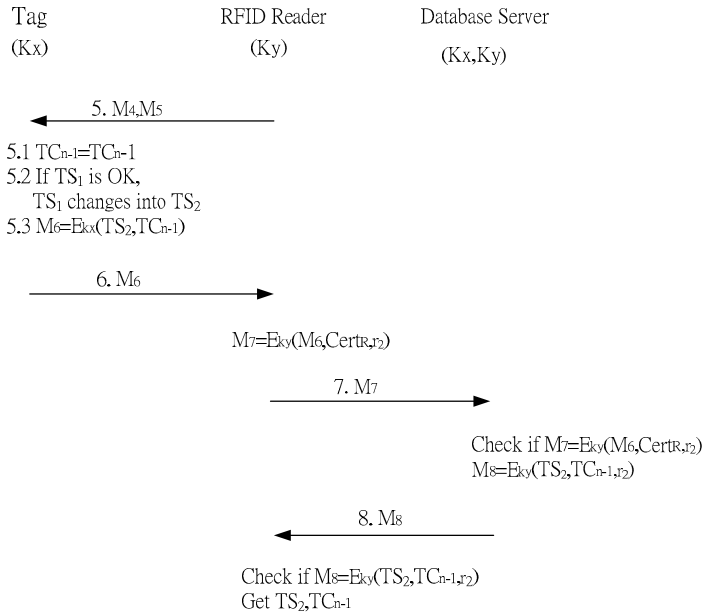

Figure 6. The mechanism for the number of reads and RBAC role-class certification.

Step 5: M_4 and M_5 are sent to the electronic tag. The tag can check the correctness of M_5 using TS_1 and r_2 which were obtained by decrypting M_4. Therefore, the tag can authenticate the reader

Step 5.1: One is subtracted from TC_n to become TC_{n-1}

Step 5.2: TS_1 is verified as the initial time stamp sent from the electronic tag. If it is, it is updated to TS_2

Step 5.3: TS_2, TC_{n-1}, r_2, and K_x are used to create an encrypted M_6, which is sent to the reader

Step 6: The reader receives M_6

Step 6.1: K_y, $Cert_R$, r_2, and M_6 are encrypted to create M_7, which is sent to the back-end database

Step 7: The back-end database receives M_7

Step 7.1: After receiving M_7, K_y is used to decrypt M_6, $Cert_R$, and r_2. If $Cert_R$ verifies the reader is authorized, K_x is used to decrypt M_6 to retrieve the updated time stamp TS_2

Step 7.2: The back-end database uses K_y to encrypt M_8

Step 8: The reader receives M_8

Step 8.1: The reader uses K_y to decrypt TS_2, TC_{n-1} and r_2. r_2 is checked to ensure that the signal is sent from the back-end database

We conclude the performance of Figures 4 and 6 in Table 2. The first number represents the execute times in Figure 4 and the second number represents the execute times in Figure 6.

Table 2. The mechanism performance.

Computation\Role	Tag	Reader	Database
Random number	1/0	1/0	0/0
Encryption	1/1	1/1	2/1
Decryption	0/1	1/1	1/1
Hash	0/0	0/0	0/0

4. Security Analysis

Below is an overview of the security analysis performed for the mechanism proposed in this paper.

(1) User privacy: As the encrypted data sent was calculated using the random numbers generated from the electronic tag and reader, r_1 and r_2, the values were untraceable. Moreover, attackers cannot have the tag key to determine the tag identity. Data is anonymous and untraceable, providing user privacy.
(2) Non-linkability: Tags create different random numbers for each reading. Thus, all response values are different, making it impossible for attackers to determine whether data was sent from the same tag.
(3) Confidentiality: In the proposed mechanism, each tag's key is shared with the back-end database. If the reader is not authorized, it cannot read the electronic tag because it does not have the tag key.
(4) Data integrity: The tag reduces the number of reads based on the data sent from the reader and uses the shared key to encrypt this data before sending it to the reader. Readers must send a certificate to the back-end database to verify its legality. The time stamp and number of reads are only sent to the reader after verification to ensure data integrity.
(5) Protection against replay attacks: As the data sent from the tag M_n is calculated using the random numbers generated from the reader r_2 and the tag r_1, and r_2 is different during each read, even if an attacker captures data sent from a tag, they are unable to resend the captured data.

5. Conclusions

The security of mobile RFID reader privacy was investigated in this study. The back-end database gives a security certificate $Cert_R$ to a reader which allows it to send data to the back-end database when reading an electronic tag, verifying the reader's security and ensuring privacy for the mobile RFID reader. Certified readers also receive a role-class from the back-end database which includes a maximum number of reads and a list of executable commands. The entire process of secure transmissions via the back-end database ensures anonymity and user privacy and prevents unauthorized readers from conducting denial of service attacks.

As this mobile reader architecture is not limited to a fixed operating connection, the security considerations extend beyond insufficient computing resources for electronic tags to the security issues associated with traditional RFID arising from any tag being able to be read from a mobile reader. As mobile RFID readers are easily acquired, they may be used for malicious attacks. Introducing a security certification mechanism to mobile RFID can help remedy these shortcomings.

Acknowledgments: This research work was partially supported by Southern Taiwan University of Science and Technology.

Author Contributions: Bing-Chang Chen contributed to the idea and the organization of the research work. Cheng-Ta Yang and Her-Tyan Yeh contributed the experimental results and all of figures. Ching-Chao Lin contributed to the experiment measurements and data analysis.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ailisto, H.; Matinmikko, T.; Haihio, J.; Ylisaukko-Oja, A.; Strommer, E.; Hillukkala, M.; Wallin, A.; Siira, E.; Poyry, A.; Tormanen, V.; et al. Physical Browsing with NFC Technology. Available online: http://www.vtt.fi/inf/pdf/tiedotteet/2007/T2400.pdf (accessed on 26 July 2016).
2. Zhang, C.; Zhang, W.; Mu, H. A Mutual Authentication Security RFID Protocol Based on Time Stamp. In Proceedings of the First International Conference on Computational Intelligence Theory, Systems and Applications, Yilan, Taiwan, 10–12 December 2015; pp. 166–170.

3. Rahman, M.; Sampangi, R.V.; Sampalli, S. Lightweight protocol for anonymity and mutual authentication in RFID systems. In Proceedings of the IEEE 12th Consumer Communications and Networking Conference, Las Vegas, NV, USA, 9–12 January 2015; pp. 910–915.
4. Nyikes, Z. Information security issues of RFID. In Proceedings of the IEEE 14th International Symposium on Applied Machine Intelligence and Informatics, Herl'any, Slovakia, 21–23 January 2016; pp. 111–114.
5. Kim, I.J.; Choi, E.Y.; Lee, D.H. Secure Mobile RFID system against privacy and security problems. In Proceedings of the Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Istanbul, Turkey, 19 July 2007.
6. Ferraiolo, D.; Kuhn, R. Role-Based Access Control. In Proceedings of the 15th NIST-NCSC National Computer Security Conference, Baltimore, MD, USA, 13–16 October 1992.
7. Sandu, R.; hamidipati, B. Role-based administration of user-role Assignment: The URA97 Model and its Oracle Implementation. *J. Comput. Secur.* **1999**, *7*, 317–332. [CrossRef]
8. Gavrila, S.I.; Barkly, J.F. Formal specification for role based access control user/role relationship management. In Proceedings of the Third ACM workshop on Role-Based Access Control, Fairfax, VA, USA, 22–23 October 1998; pp. 81–90.
9. Tari, Z.; Chan, S.H. A role-based control for intranet security. *IEEE Internet Comput.* **1997**, *1*, 24–34. [CrossRef]
10. Coyne, R.S.E.; Feinstein, H.; Yourman, C. Role-Based Access Control Modes. *IEEE Comput.* **1996**, *29*, 38–47.
11. Choi, S.H.; Yang, B.; Cheung, H.H.; Yang, Y.X. Data management of RFID-based track and trace anti-counterfeiting in apparel supply chain. In Proceedings of the 8th Internation Conference for Internet Technology and Secured Transactions, London, UK, 9–12 December 2013; pp. 265–269.