Computer Communications xxx (2010) xxx–xxx

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

An RFID secure authentication mechanism in WLAN

Ming-Huang Guo [a], Horng-Twu Liaw [a], Der-Jiunn Deng [b], Han-Chieh Chao [c,d,*]

[a] Department of Information Management, Shih-Hsin University, Taipei, Taiwan
[b] Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua, Taiwan
[c] Institute of Computer Science and Information Engineering, Department of Electronic Engineering, National Ilan University, I-Lan, Taiwan
[d] Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
RFID (Radio Frequency Identification)
Two-Factor Authentication mechanisms
WLAN (Wireless Local Area Network)

ABSTRACT

With the thriving evolution of information technology, network technology attains to maturity and Wireless Local Area Network (WLAN) becomes universal as well. To discipline the right of network usage, network system identifies users before providing network services or resources. In the historical researches, the conventional authentication mechanisms frequently adopted the names and passwords of users as login authentication. However, these Single Factor Authentication mechanisms are proved to be defective. In virtue of enhancing security, recent researches on authentication are built on Two-Factor Authentication schemes. Nevertheless, the expensive cost of building Two-Factor Authentication approaches has affected the will of users. For the purpose of lifting the rate of usage, in this paper, we apply low-cost passive Radio Frequency Identification (RFID) tag along with the names and passwords of users as login authentication. The analytic comparison indicates the research not only reduces the cost of Two-Factor Authentication schemes, but provides security in the same way as smart cards technology.

1. Introduction

To provide users with convenience brought by mobility, recent wireless network technology attains maturity and the establishment and usage of Wireless Local Area Network (WLAN) become universal as well. Before providing services, network system demands that users must complete authentication procedure in order to confirm the resources are properly used. At present, though authentication mechanisms do not send the messages in plaintext, the server still store relevant information of user registration. Once the password or verifier table is stolen by hackers, they can damage or login the system via the table. Therefore, to tackle the problems of password or verifier table being attacked, the following authentication mechanisms will be proposed without verifier tables.

The conventional authentication mechanisms frequently use the names and passwords of users as login authentication. However, these Single Factor Authentication mechanisms are proved to be defective. In virtue of enhancing security, recent researches on authentication are built on Two-Factor Authentication schemes. Nevertheless, the expensive cost of building Two-Factor Authentication approaches has affected the will of users. To handle above problems, we will introduce a Radio Frequency Identification (RFID) secure authentication mechanism in WLAN in this paper. The proposal applies low-cost passive RFID tag along with the names and passwords of users as login identification, and proceeds without secure channel assumption. Through analytic comparison, this research not only reduces the cost of Two-Factor Authentication schemes, but provides security in the same way as smart cards.

The organization of this paper is introduced as follows. In Section 2, some related works are discussed. The proposed low-cost secure RFID tag authentication mechanism in WLAN is introduced in Section 3. Section 4 provides comparisons and analysis between our proposal and some related works, and Section 5 concludes this paper.

2. Related work

In the historical researches on RFID secure mechanisms, there are two main categories: one attains secure protection without cryptography which includes Kill Tag [1], Selective Blocker Tag [7], Faraday Cage [11], Noisy Tags [3], etc. The other attains secure protection via cryptography, which is classified into Single Factor Authentication and Two-Factor Authentication mechanisms, using passive or active RFID tags, whether back-end application system possess verifier table and whether using secure channel assumption, and other different features.

From above methods, Single Factor Authentication schemes suggest using RFID technique as the only authentication

* Corresponding author. Address: Institute of Computer Science and Information Engineering, Department of Electronic Engineering, National Ilan University, 1, Sec. 1, Shen-Lung Rd., I-Lan, Taiwan. Tel.: +886 3 9357400 251; fax: +866 3 9354238.
E-mail address: hcc@niu.edu.tw (H.-C. Chao).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.02.033

mechanism, and Two-Factor Authentication approaches combine RFID with other authentication mechanisms such as user names and passwords. Among Single Factor Authentication schemes, Hash Lock mechanism is the most commonly discussed [12]. This mechanism substitutes the real ID with MetaID, and protects the real ID from revealing to illegal frequency reader. However, it is apt to be attacked by location tracing due to the fixed number of every transmission. To solve the problem, the Randomized Hash Lock method adds random number in the mechanism [11], and the Hash Chain method uses two different hash values $G(x)$ and $H(x)$ to protect the data within RFID tags [8].

Though Single Factor Authentication schemes are capable of providing proper security, recent researches all tend to focus on Two-Factor Authentication approaches for enhancing the security of authentication mechanisms. Among existing Two-Factor Authentication mechanisms [2,4,5,9,10], mostly use active smart card as authentication tool which consists of hash function, exclusive or, random number, and timestamp. These methods meet the demands of security, but they all adopt active smart card of higher cost, and secure channel assumption which is condition unnecessarily provided in actual environment.

Consequently, to lower the cost and conform to the actual environment, we will introduce a Two-Factor Authentication mechanism of passive RFID tags in WLAN without secure channel assumption. Apart from fulfilling the demand of security, this researching mechanism also aims to provide a better RFID secure authentication mechanisms in WLAN by achieving the goals of low-cost and high efficiency. The characteristics of the proposal and related works are listed in Table 1. The later experiments will show that our scheme not only lowers the cost, but also provides some proper secrecy.

3. The proposed RFID secure mechanism

The system environment for the proposal is shown in Fig. 1, and notations used in the proposal are defined in Table 2.

In the following discussion, there are three assumptions: First, both tag to reader and reader to ***AS*** connections are accessed in wireless, and the transmission is lack of safety. Second, in order to reduce the cost, the passive RFID tags are adopted in the research. In order to simplify the introduction, there is only one tag for each user. Third, the proposal is a Two-Factor Authentication scheme, and user's identification, user's password, and user's tag are unable to be cracked at the same time.

Table 1
The characteristics for the proposal and some related works.

Items	Schemes					Our scheme
	[2]	[4]	[5]	[9]	[10]	
RFID tags	Active	Active	Active	Active	Active	Passive
Verifier table required	NO	NO	YES	YES	NO	NO
Secure channel required	YES	YES	YES	YES	YES	NO

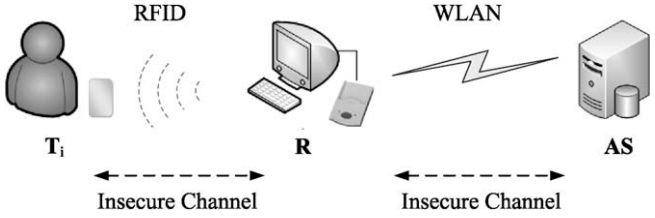

Fig. 1. System environment for the proposed mechanism.

Table 2
Notations in the proposed mechanism.

Notations	Statements
U_i	The ith user
T_i	The tag of U_i
R	Tag Reader
AS	Authentication Server
TID_i	The tag ID of U_i
ID_i	The username of U_i
PW_i	The password of U_i
NPW_i	The new password of U_i
$H()$	Hash function
$\oplus$	XOR
$\|\|$	The string concatenation
$E_{TKIP}()$	TKIP (Temporal Key Integrity Protocol) encryption function
MIC	The Message Integrity Code generated by Michael algorithm [6]
$Auth$	The shared authentication value between R and AS
x	The private value of AS
y	The private value of R
TS_i	The time stamp generated by R for U_i
T^*	The time that AS receives message
PAD	The padding string
$RFTag\{\}$	The operations to write data into tag
SB_i	The field in tag that user requests to write in
$IdSb_i$	The message for field ($Sector=0$, $Block=1$) in tag

There are three phases in the proposed mechanism: Registration Phase, Login and Authentication Phase, and Password Exchange Phase. The details in each phase are introduced as below.

3.1. Registration phase

If U_i wants to be a legal user, s/he has to register to AS first. When Reader receives TID_i from T_i, ID_i, and PW_i from U_i, it calculates $RM_i = (TID_i||H(ID_i)||H(PW_i)) \oplus Auth$, and delivers $E_{TKIP}(RM_i)||MIC$ to AS. In the proposal, in order to simplify the discussion, there is only one reader. If there are many readers, the AS will have different $Auth$ values for different readers. After receiving the message, AS decrypts it and checks if TID_i were registered or not. If TID_i did not register, AS will return A_i to Reader, where $A_i = H(TID_i \oplus H(PW_i) \oplus H(x) \oplus Auth)$. The Reader decrypts the message and writes $ID_i||SB_i||PAD$ and A_i into Tag. The processes in this phase are depicted in Fig. 2.

3.2. Login and authentication phase

In this phase, Reader first reads ID_i and PW_i from U_i, TID_i and $IdSb_i$ from T_i, and decomposes $IdSb_i$ into $\{ID_i||SB_i||PAD\}$. The SB_i is separated into S_i and B_i, where S_i is the first two bits of SB_i, and B_i is the last bit of SB_i. If B_i is 0 or 1, strings with position ($Sector = S_i$, $Block = B_i$) and ($Sector = S_i$, $Block = B_i + 1$) in T_i are

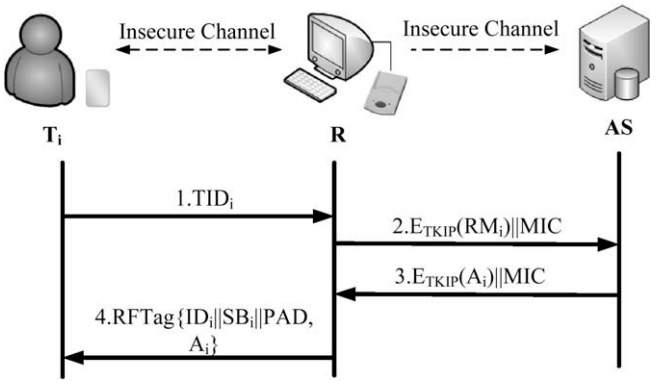

Fig. 2. The process in the registration phase.

Please cite this article in press as: M.-H. Guo et al., An RFID secure authentication mechanism in WLAN, Comput. Commun. (2010), doi:10.1016/j.comcom.2010.02.033

read out as $A1_i$ and $A2_i$, respectively. If B_i is 2, strings with position ($Sector = S_i, Block = B_i$) and ($Sector = S_i, Block = B_i - 2$) in T_i are read out as $A1_i$ and $A2_i$, respectively. Then R sends $E_{TKIP}(A_i||B_i||C_i||D_i)||MIC$ to AS for authentication, where A_i is a string concatenate by $A1_i$ and $A2_i$, B_i is $TID_i \oplus TS_i \oplus H(PW_i)$, C_i is $TS_i \oplus Auth$, and D_i is $H(TS_i \oplus Auth) \oplus y$. In order to check T_i, AS will execute the following steps:

1. It decrypts the message and checks if MIC is integrity.
2. If MIC is integrity, TS_i is calculated with $C_i = TS_i \oplus Auth$. If $T^* - TS_i \leqslant \Delta T$, where T^* is the time stamp when AS received the message, $TID_i \oplus H(PW_i)$ is derived from $B_i = TID_i \oplus TS_i \oplus H(PW_i)$ with given TS_i.
3. Let $A_i^* = H(TID_i \oplus H(PW_i) \oplus H(x) \oplus Auth)$. If A_i^* and A_i are matched, T_i is a legal user.
4. After authenticating T_i, AS returns $E_{TKIP}(E_i)||MIC$ to R, where $E_i = H(TS_i \oplus y)$, and y is derived from $D_i = H(TS_i \oplus Auth) \oplus y$.

After receiving the message, R decrypts it and checks if MIC is integrity. If MIC is integrity, E_i^* is derived from $H(TS_i \oplus y)$, and compared to E_i. If E_i^* and E_i are the same, R knows T_i is authenticated by AS, and the phase is finished. The processes in this phase are depicted in Fig. 3.

3.3. Password exchange phase

To exchange the password, user has to pass the login and authentication phase. After that, R reads the new password NPW_i from user, and sends $E_{TKIP}(CPW_i)||MIC$ to AS, where $CPW_i = H(PW_i) \oplus Auth \oplus H(NPW_i)$. Then AS decrypts the message and checks if MIC is integrity. If all process complete, AS returns $E_{TKIP}(NA_i)||MIC$ to R, where $NA_i = H(TID_i \oplus H(NPW_i) \oplus H(x) \oplus Auth)$. After R decrypts the message and checks MIC is integrity, it will replace A_i in T_i with NA_i. The processes in this phase are depicted in Fig. 4.

4. Analysis and comparisons

4.1. Analysis and comparison in security

In Table 3, there are six security attacks discussed. First, the RFID reader and authentication server are mutually authenticated, so the impersonation attack is able to alleviate. Second, the time stamp is added in the messages, and the replay attack is avoided. Third, the messages exchanged in the study are all encrypted, and the eavesdropping attack is prevented. Moreover, the whole key for RFID reader accessing is ID_i, which is only known by the owner, and the tag modification attack does not occur if the attacker could not get the ID_i. Finally, our scheme is a Two-Factor Authentication mechanism; neither the tag duplication attack nor the tag stolen attack would happen if the illegal users could not have the ID_i and PW_i at the same time. The comparisons in security attacks resisted for some studies [2,4,5,9,10] are shown in Table 3. It is obvious that our proposal provides better secrecy than others.

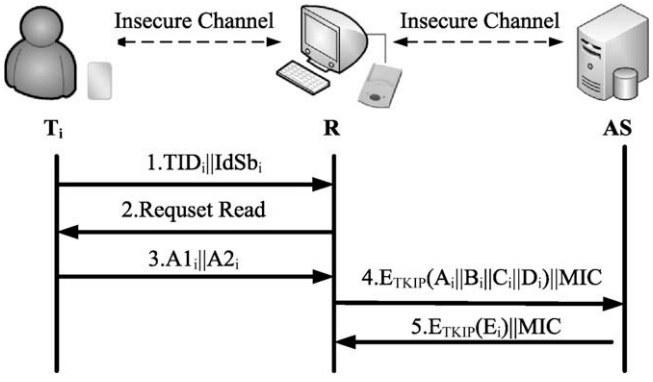

Fig. 3. The process in the login and authentication phase.

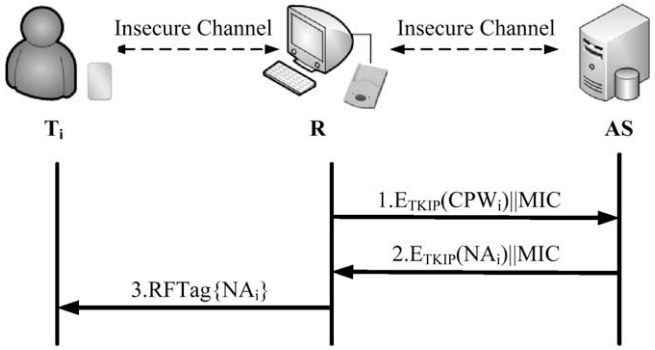

Fig. 4. The process in the password exchange phase.

Table 3
The security attacks resisted for schemes compared.

Attacks resisted	Schemes					Our scheme
	[2]	[4]	[5]	[9]	[10]	
Eavesdropping attacks	YES	NO	NO	NO	NO	YES
Impersonation attacks	YES	YES	YES	YES	YES	YES
Replay attacks	YES	YES	YES	YES	YES	YES
Tag modification attacks	NO	NO	NO	NO	NO	YES
Tag duplication attacks	NO	NO	NO	NO	NO	YES
Tag stolen attacks	YES	YES	YES	YES	YES	YES

4.2. Analysis and comparison in functionalities

To analyze the functionalities in the proposed mechanism, the symbols are defined in Table 4. In some related works [2,4,5,9,10], the user identification is applied with active RFID tags, and the low-cost requirement (C5) is unable to accomplish. The proposal also reaches the goal in C7, C8, C9, and C12, which is an initial study comparing to others. The detailed comparisons in functionalities are shown in Table 5.

4.3. Analysis and comparison in performance

To provide better performance, the operations in each phase should be developed with less time complexity. According to the previous discussions, our mechanism has better secrecy, integrity,

Table 4
Notations for the analysis and comparisons.

Notations	Statements
C1	The verifier table is needless
C2	User can select password
C3	User can change password
C4	Mutual authentication is achieved
C5	Low-cost requirement is provided
C6	The password guessing attack is resisted
C7	The message integrity is guaranteed
C8	User can write messages into the assigned sector and block in tag
C9	The content in tag is encrypted
C10	The secure channel is needless
C11	The user's password is exchanged and encrypted in the registration phase
C12	The messages exchanged are all encrypted

Please cite this article in press as: M.-H. Guo et al., An RFID secure authentication mechanism in WLAN, Comput. Commun. (2010), doi:10.1016/j.comcom.2010.02.033