A Remote Authentication Model of Information Appliances

Huey-Ming Lee [1)] , Hsih-Feng Liao [1)] , Shu-yen Lee [2)]

[1)] Department of Information Management, Chinese Culture University
55, Hwa-Kung Road, Yang-Ming-San, Taipei(11114), TAIWAN
[2)] Dep. of Private Participation in Infrastructures, China Engineering Consultants, Inc.,
26th Fl., 185, Sec. 2, Sin-Hai. Road, Taipei (10637) TAIWAN

Abstract: - In this study, we proposed a remote authentication model of information appliances (RAMIA). The RAMIA comprised of two basic components, namely user identity security authentication module (UISAM) and authority management module (AMM). The function of UISAM is to authenticate the user by account and password, this module is constructed by hash function and exclusive or (XOR)；AMM includes a user authorization data base (UADB) and manages user's authority. Via this model, we can have the more reliable and convenient home network environment.

Key-Words: -Information appliance, authentication, hash function, exclusive or, authority

1 Introduction

Along with the prosperity of information appliances (IAs), there are more and more varied IA products appeared. In the home network environment, the IA control mechanism can provide fine control capability of IA devices.

Lee and Huang [2] proposed an IA controlling model (IACM), which can control IA devices through home management broker. Lee et al. [1] came up with the idea of IAs intelligent agent model (IAIA), making home environments more comfortable and convenient. Lee et al. [5] proposed fuzzy neural network model of information appliances with the functions of self-learning and fuzzy inference, it enables IAIA to maximize efficiency of IAs in a more humane way. Lee and Mao [3] proposed a clustering model of information appliance, it processes user's recognitions of IAs to cluster IA devices, and it facilitates the management of control. Lee et al. [4] proposed a fuzzy aggregative clustering model of information appliances (FACIA) which is capable to cluster the IAs, filter and extract the IAs' messages automatically. Wu and Jan [6] proposed home network management system which integrates WAP and SMS by mobile communication devices, but lack of security authentication. If there is a function of authentication embedded in this mechanism, it not only can avoid the user without authorization to invade the home network system, but also promote the integrated IAs facilities.

In this study, we propose a remote authentication model of information appliances (RAMIA). The RAMIA comprised of two basic modules, namely user identity security authentication module (UISAM) and authority management module (AMM). The UISAM which is constructed by hash function and exclusive or (XOR) is to authenticate the user by account and password; the function of AMM is to record and manage users' authority.

This model not only can avoid user without authorization to invade the home network system, but also promote authorization control mechanism. Via this model, we can have the more reliable and convenient home network environment.

2 RAMIA

In this Section, we presented a remote authentication model of information appliances (RAMIA) under the supervision of IACM [1], as shown in Fig.1. There are two basic modules in RAMIA, saying user identity security authentication module (UISAM) and authority management module (AMM), as shown in Fig.2.

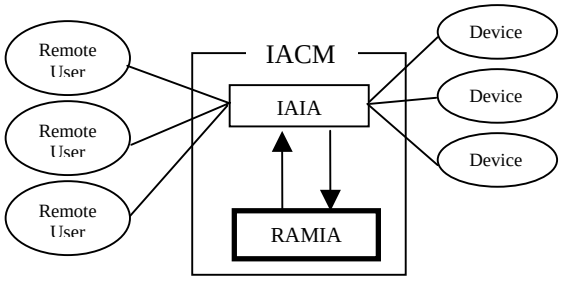

Fig.1 Remote Authentication Model of Information Appliances

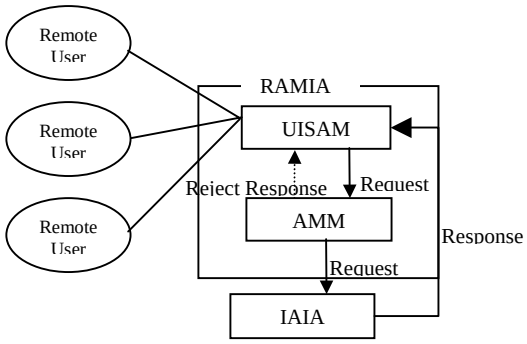

Fig.2 Architecture of Remote Authentication Model of Information Appliances (Dotted line denotes the reject response)

The functions of these modules are as the followings:

- UISAM：it can authenticate users and provide message to AMM
- AMM：it includes a user authority database storing users' authority and can manage the users' authority of controlling home network system.

2.1 UISAM

UISAM can receive messages from remote users and authenticate them. There are two components in UISAM, saying user security authentication component (USAC) and user identity database (UIDB). USAC can authenticate users and UIDB is a database which records the users' message to support USAC. After authentication, UISAM will pass user's ID and command to AMM, as shown in Fig.3.

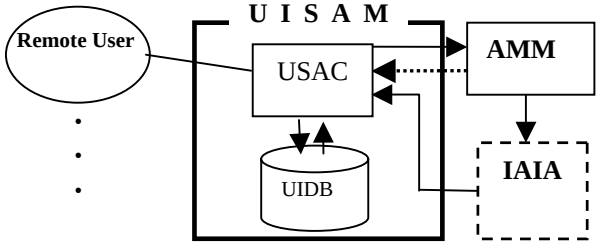

Fig.3 UISAM module (Dotted line is reject response)

The functions of these components are as the followings:

- USAC：USAC which is the core of UISAM can ensure that the user is permitted.
- UIDB：It records users' authentication data to assist USAC identify the user.

2.2 AMM

AMM has a function of authority management for permitted user. It is constructed by two components, namely user authority management component (UAMC) and user authority database (UADB). UAMC is responsible for user's authority management. UADB is a database of users' authority records. Lee et al. [1] proposed IAIA to integrate control of IAs, as shown in Fig.4.

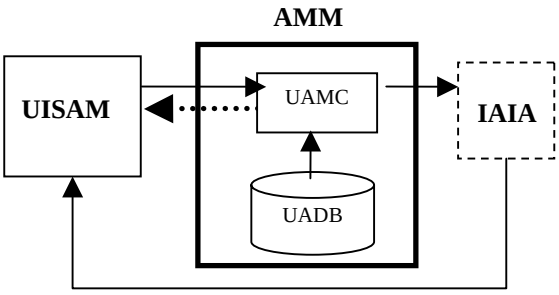

Fig.4 Authority Management Module (Dotted line is reject response)

The functions of these components are as the followings:

- UAMC：UAMC can receive message from UISA to manage users' authority and pass it to IAIA.
- UADB：UADB provides users' authority message for UAMC to manage users' authority.

3 Authentication

In this Section, we express the procedures and algorithms of USAC which is simpler and more reliable.

3.1 Register

User selects an identity (ID) and password (PW) and then sends them to UISAM to register, as shown in Fig.5.

Fig.5 Registering process

Ri in Fig. 5 is $R_i = h(ID_i \oplus X) \oplus PW_i$

3.2 Authentication and data deliver

In this sub-section, we express the authentication process by two routes, namely remote devices to

UISAM and UISAM to remote devices, as shown in Fig. 6 and Fig. 7, respectively.

3.2.1 Remote device to UISAM

- Algorithm in remote device

$C_1^{'} = R_i \oplus PW_i$

$C_2^{'} = h(C_1^{'} \oplus T)$

$\tilde{K} = K \oplus C_1^{'}$

$X_2 = h(K \oplus T)$

$\tilde{M} = M \oplus X_2$

$\tilde{H} = h(M \oplus T \oplus C_1^{'})$

$Send(ID_i, C_2^{'}, \tilde{M}, H, T, \tilde{K})$

- Algorithm in UISAM

$C_1 = h(ID_i \oplus X_i)$

$C_2 = h(C_1 \oplus T)$

$C_2^{'} = ? C_2$

$K = \tilde{K} \oplus C_1$

$X_2 = h(K \oplus T)$

$M = \tilde{M} \oplus X_2$

$H^{'} = h(M \oplus T \oplus C_1)$

$H^{'} = ? \tilde{H}$

where ID: Account,
PWi: Password,
Ri: Public key,
T: Time stamp,
M: Control command

3.2.2 UISAM to Remote device

We only modify the step1 and step2 of UISAM in Fig. 6, as shown in Fig. 7, respectively

3.3 Modify password

It's convenient for user to change his password while he/she gets public key R_i. The algorithm is shown as follow.

$R_i \oplus PW_i = h(ID_i \oplus K_i) \oplus PW_i \oplus PW_i = h(ID_i \oplus K_i)$

$R_{NEW} = PW_{NEW} \oplus h(ID \oplus Ki)$

Store R_{NEW} to smart card.

Then, the password was changed.

4 Authority management

While UAMC receives messages which contain ID and command from UISAM, UAMC will check user's authority with UADB. If they meet, then UAMC can pass the command from user to IAIA and then IAIA will execute the command and send a state message to UISAM, else UAMC rejects the command to UISAM, as shown in Fig. 4.

5 Model implementation and security analysis

To analyze the security of this model, we implement the model in this Section.

5.1 Practical environment

For the purpose of ease manipulation, cross-platform, and remote-control capability, we have adopted Java Server Page (JSP) and Java Servlet written Web Server structure, as well, Java 2 Platform, Standard Edition, v 1.4.2 API Specification is utilized for constructing RAMIA prototype. This model is constructed upon Tomcat server software that employs browsers as its interface; above-mentioned are done with a Pentium III 700GHz Notebook that is powered by O/S Windows Professional and Microsoft Access 2002 database.

5.2 Implementation

We take ID = "Eric", Password = "1234567" and Command = "Power on light" as an example to implement this model. Then, if the Password = "1234567" or Password = "123456", we can have the messages as shown in Table 1. If the password is correct, then the command message will be decrypted and executed. If the password is incorrect, then the command message will be ignored and the user can't control the IA devices in home network system at all. Via this case implementation, we can know that this model is safer and more reliable.

6 Conclusion

At present, there are more and more varied IA products appeared in home network system. Therefore, authentication mechanism is the most significant in IA control mechanism. In this study we propose a remote authentication model of information appliances (RAMIA). It can not only avoid user without authorization to invade our home network system, but also promote authorization management mechanism. Via this model, we can

have the more reliable and convenient home network environment.

References:

[1] Huey-Ming Lee, Yen-Chih Chen, Jan-Jo Chen, "The Intelligent Agent Design of Information Appliance,", JCIS, 2003, Proceeding of the 7th Join Conference on Information Sciences, Cary. NC. USA, pp.1681-1684 September 26-30, 2003

[2] Huey-Ming Lee & Jun-Hong Huang, "The study of IA devices monitoring model", The sixth seminar of the research and practices of information management, pp.430-437, May 2002.

[3] Huey-Ming Lee, Ching-Hao Mao, "A Fuzzy Clustering Model of Information Applicance", Third International Conference on Electronic Business (ICEB2003) Singapore, pp. 241~243, Dec 10-12, 2003.

[4] Huey-Ming Lee, Ching-Hao Mao, Shu-Yen Lee, "A Fuzzy Aggregative Clustering Control model of Information Appliance", WSEAS Transactions on Communication, Vol. 3, No. 1, 2004, pp. 254-258

[5] Huey-Ming Lee, Ching-Hao Mao, Shu-Yen Lee, "A Fuzzy Neural Network of Information Appliance", Fuzzy System & Innovation Computing (FIC) 2004, Kitakyushu, Japan,June 2 - 3, 2004

[6] Chi-Hsiang Wu, Rong-Hong Jan, System integration of WAP and SMS for home network system, *COMPUTER NETWORKS.*

[7] T. ElGamal, "A Public Key Cryptosystems and A Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. 31, no. 4, July 1985, pp.469-472.

[8] M.-S. Hwang, and L.-H. Li, "A new remote user authentication scheme using smart card,", IEEE Trans. on Consumer Electronic, Vol. 46, No. 1, February 2000, pp. 28-30.

[9] M. S. Hwang, C. C. Lee and Y. L. Tang, "A Simple Remote User Authentication Scheme," Mathematical and Computer Modeling, Vol. 36, 2002, pp. 103-107.

[10] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24,1981, pp. 770-772.

[11] S. J. Wang and J. F. Chang, "Smart Card Based Secure Password Authentication Scheme," Computers and Security, Vol. 15, no. 3, 1996, pp. 231-237.

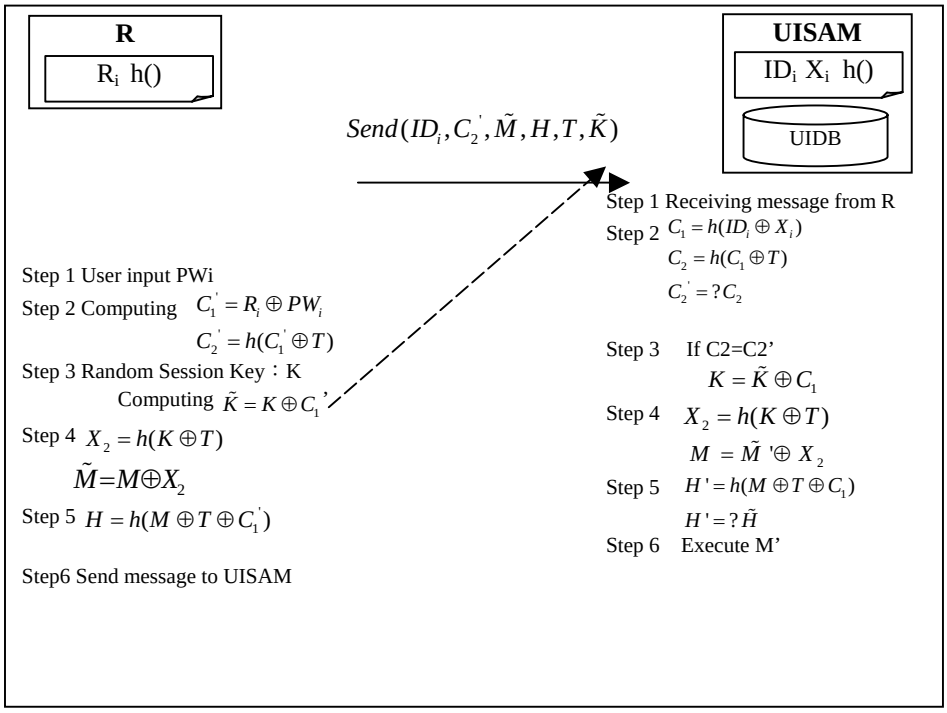

Fig.6 Remote device to UISAM

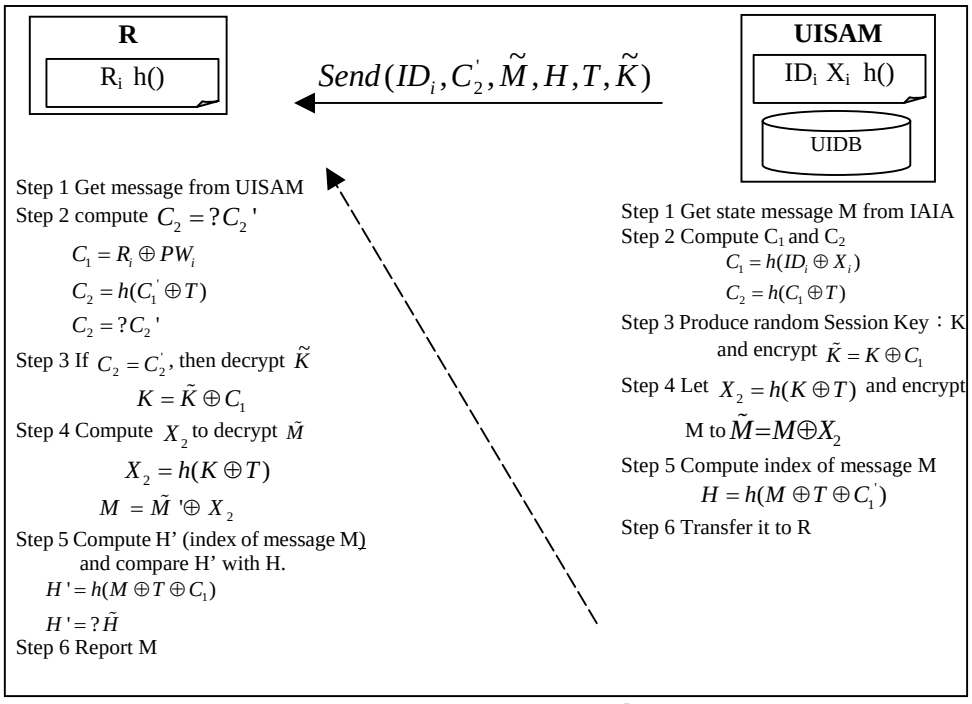

Fig.7 UISAM to remote device

Table 1 Parameter value table

Parameters	ID	PW	Ri'	C1'	C2'	K'	M'	H	C2
Register Step	eric	1234567							
pw error	eric	123456	[B@71dc3d	[B@1326484	[B@16546ef	[B@1428ea	[B@18a49e0	[B@1f82982	
pw correct	eric	1234567	[B@da3a1e	[B@11dba45	[B@16f144C	[B@2af081	[B@113a53d	[B@c5495e	[B@16f144C