Secure Remote Control Model for Information Appliances

Wen-Gong Shieh[1] Jian-Min Wang[1] Wen-Bing Horng[2]
[1]Department of Information Management, Chinese Culture University
55 Hwa-Kang Road, Yang-Ming-Shan, Taipei 11114, Taiwan, R.O.C.
[2]Department of Computer Science and Information Engineering, Tamkang University
151 Ying-Chuan Road, Tamsui, Taipei, 25137, Taiwan, R.O.C.
E-mail: wgshieh@faculty.pccu.edu.tw

***Abstract*—Recently, Lee et al. proposed a Remote Authentication Model of Information Appliances (RAMIA). Unfortunately, RAMIA has a fatal error that opens the entire home network of information appliances to hackers. In this paper, we propose a new Secure Remote Control Model for Information Appliances (SRCMIA) to fix this error. Besides, our model can also achieve both message authentication and one-time secret communication in just one message.**

***Index Terms*—Authentication, information appliance, remote control, confidentiality.**

I. Introduction

In the field of information appliances (IAs) in a home network environment, many scholars [5, 7–9] have proposed various IA control mechanisms. However, the studies of introducing remote authentication [3, 4] to the control of IAs are scanty relatively. Recently, in 2004, Lee et al. [6] proposed a low computation cost Remote Authentication Model of Information Appliances (RAMIA) based on Chien et al.'s [1] authentication scheme. Unfortunately, RAMIA is vulnerable to parallel session attacks and masquerade attacks. Especially, as indicated in [11], a successful masquerade attack will open the entire home network to a hacker, which is a fatal damage in RAMIA. For people, however, it is very convenient to turn on the air conditioner before they arrive at home. Therefore, a control model for IAs with more secure remote authentication is indispensable.

In this paper, we propose a Secure Remote Control Model for Information Appliances (SRCMIA) using a novel authentication and control protocol. The remainder of this paper is presented as follows. In Section II, we demonstrate the protocol of our SRCMIA. In Section III, we analyze the security, efficiency, and functionality of our model. Finally, a concluding remark is given in Section IV.

II. Our SRCMIA protocol

Our SRCMIA not only authenticates a remote user's IA commands through insecure public communication channels but also executes and reports back the execution results of the IA commands. Fig. 1 illustrates our SRCMIA structure, which is similar to that of RAMIA. The remote device can be a mobile phone, a PDA, and so on. The Home Controller cooperates with the remote device to provide remote control services including authentication, encryption/decryption, and IA control. The security objectives of our model include confidentiality, mutual authentication, and easy to use. The SRCMIA protocol consists of three phases: the registration phase, the control phase, and the reporting phase.

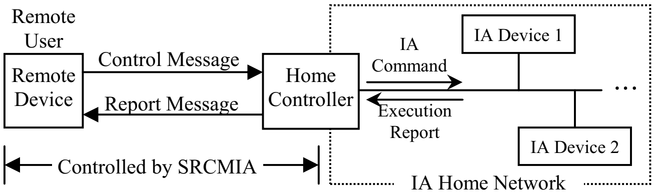

Fig. 1. The proposed SRCMIA structure.

A. Registration Phase

Assume a user U_i submits his identity ID_i and password PW_i to the Home Controller over a secure channel for registration. If the request is accepted, the Home Controller computes $R_i = h(ID_i \oplus x) \oplus PW_i$ and issues U_i a smart card containing R_i and $h(\cdot)$, where x is a secret key maintained by the Home Controller, $\oplus$ is the bitwise XOR operation, and $h(\cdot)$ is a collision-resistant one-way hash function [10].

B. Control Phase

Fig. 2 shows the messages exchanged in the control phase and the reporting phase; the first message is sent in the control phase, while the second message is sent in the reporting phase. When the user U_i wants to control a particular IA through a remote device D_i, he first inserts his smart card into the remote device. Then, he inputs his ID_i and PW_i to the device and selects an IA command M_c that specifies the operation to be performed on the controlled IA. The smart card inside the device D_i performs the following computations:

(1) Compute $C_1 = R_i \oplus PW_i$ $(= h(ID_i \oplus x))$.
(2) Generate a random number P.
(3) Compute $H_c = M_c \oplus h(C_1 \oplus P)$, where $h(C_1 \oplus P)$ is used as a session key to encrypt the IA command M_c.
(4) Compute $C_2 = h(T \parallel H_c \parallel P \parallel C_1)$, where T is current timestamp, and $\parallel$ is the string concatenation operation.

ISI 2008, June 17-20, 2008, Taipei, Taiwan
1-4244-2415-3/08/$20.00 ©2008 IEEE

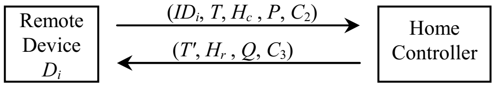

Fig. 2. Messages transmitted in the control phase and the reporting phase.

(5) Send (ID_i, T, H_c, P, C_2) to the Home Controller via the remote device D_i and wait for report until timeout, where timeout is an event signifying the end of the pre-defined waiting period.

(6) If timeout occurs, then report failure to the user U_i and stop.

Upon receiving the control message (ID_i, T, H_c, P, C_2) from the device D_i, the Home Controller performs the following operations:

(1) If T is not in the pre-defined valid time interval, then ignore the received message and stop. Note that in this case, the received message is a replayed message.

(2) Compute $C_1' = h(ID_i \oplus x)$ and $C_2' = h(T \| H_c \| P \| C_1')$.

(3) If $C_2' \neq C_2$, then ignore the received message and stop. Note that the Home Controller may log the event for further investigation.

(4) Compute $M_c = H_c \oplus h(C_1' \oplus P)$.

(5) Accept the received message and send M_c to the specified IA for execution.

Note that we use $h(C_1 \oplus P)$, instead of $h(C_1)$, as a session key to encrypt M_c into H_c for two reasons. First, all IA commands (such as M_c) are structured and known to the public. Second, the total number of all different IA commands is relatively small. Therefore, if $h(C_1)$ is used, an adversary can easily derive $h(C_1)$ from $H_c = M_c \oplus h(C_1)$ using relatively small number of intercepted control messages (ID_i, T, H_c, P, C_2), and thus break our encryption. By using $h(C_1 \oplus P)$ as a session key, the ciphertext $H_c = M_c \oplus h(C_1 \oplus P)$ will become a one-time ciphertext due to the random number P.

C. Reporting Phase

After the specified IA finishes executing M_c, it will send an execution report M_r back to the Home Controller. Then, the Home Controller performs the following operations.

(1) Generate a random number Q.

(2) Compute $H_r = M_r \oplus h(C_1' \oplus Q)$. Note that $h(C_1' \oplus Q)$ is used as a session key to encrypt the execution report M_r.

(3) Compute $C_3 = h(T' \| H_r \| Q \| (C_1'+1))$, where T' is the current timestamp.

(4) Send (T', H_r, Q, C_3) to the remote device D_i.

After receiving the report message (T', H_r, Q, C_3) from the Home Controller, the smart card inside the remote device D_i proceeds as follows.

(1) If T' is not in the pre-defined valid time interval, then ignore the received message and stop. Note that again the report message is a replayed one.

(2) Compute $C_3' = h(T' \| H_r \| Q \| (C_1+1))$.

(3) If $C_3' \neq C_3$, then report failure to the user U_i and stop.

(4) Compute $M_r = H_r \oplus h(C_1 \oplus Q)$.

(5) Accept the received message and report M_r to the user U_i via the remote device D_i.

III. Analysis of our SRCMIA

In this section, we analyze the security of our SRCMIA model in Part A, the efficiency of our model in Part B, and its functionalities in Part C.

A. Security Analysis

In this part, we examine the security of our model as follows:

1. *Secure shared secret.* The shared secret between the legal user U_i and the Home Controller is $C_1 = h(ID_i \oplus x)$. Since C_1 is protected by the collision-resistant one-way hash function $h(\cdot)$, it is infeasible for a malicious person to derive the shared secret C_1 from C_2 or C_3. Note that a collision-resistant one-way hash function $h(\cdot)$ satisfies (i) *one-way*: for any given value Y, it is impossible to find X within useful lifetime such that $h(X) = Y$, and (ii) *collision-resistance*: for any given block A, it is impossible to find another block B within useful lifetime such that $B \neq A$ and $h(B) = h(A)$ [12].
2. *Resistance to replay attack.* Replaying either the control message (ID_i, T, H_c, P, C_2) or the report message (T', H_r, Q, C_3) will be detected due to the freshness check of time stamps. It should be noted that using timestamps must satisfies the time-synchronization requirement. There are many other nonce-based schemes to avoid the synchronization problem. However, using nonces needs extra communications and is thus not suitable in our IA applications.
3. *Resistance to parallel session attack.* Since the difference between C_1 in $C_2 = h(T \| H_c \| P \| C_1)$ and (C_1+1) in $C_3 = C_3' = h(T' \| H_r \| Q \| (C_1+1))$ causes an asymmetric structure on the two message authentication codes transmitted between the remote device D_i and the Home Controller, the parallel session attacks discovered in [2] will fail.
4. *Mutual authentication*. If a malicious attacker modifies the transmitted messages, the modification will be discovered through checking the message authentication codes C_2 or C_3. Except for the user U_i and the Home Controller, no one can obtain the shared secret value C_1 to compute correct C_2 or C_3 to pass the checks. Similarly, if the attacker tries to impersonate a legal user U_i or to masquerade as the Home Controller, he has to prepare the valid control message (ID_i, T, H_c, P, C_2) and report message (T', H_r, Q, C_3) for mutual authentication, respectively. However, no one can create valid message authentication code C_2 or C_3 without knowing C_1.
5. *Confidentiality.* In our SRCMIA protocol, the session key $K_c = h(C_1 \oplus R)$ is used to encrypt IA commands and the session key $K_r = h(C_1' \oplus Q)$ is used to encrypt execution reports, where R and Q are random numbers. A malicious attacker cannot derive the correct K_c and K_r

using only the known random number R and Q without knowing C_1. Besides, both K_c and K_r are real session key because the random number R and Q are different. In addition, even if the attacker obtains the above session keys K_c and K_r, by applying the known random number R and Q, respectively, the person still cannot derive C_1 due to the one-way property of the secure hash function. Therefore, without knowing C_1, no one can derive any other session keys using just known random numbers and the known session keys. As such, the confidentiality of both the encrypted IA commands and their encrypted execution reports is achieved. Since the session keys are XOR-ed with IA commands or execution reports, it implies that the lengths of session keys, all IA commands, and all execution reports are all the same.

6. *Resistance to known plaintext attack.* The purpose of the known plaintext attack tries to derive the encryption key through analyzing the ciphertext and its corresponding known plaintext. In our SRCMIA model, the equation $H_c = M_c \oplus K_c$, where the session key $K_c = h(C_1 \oplus P)$ is used to encrypt M_c. If H_c and M_c are known, then K_c can be derived from $K_c = M_c \oplus H_c$. However, the derived K_c is useless because K_c is a one-time session key. Similar argument can also be applied to $H_r = M_r \oplus K_r$ in encrypting execution report M_r.
7. *Resistance to weak password attack.* In our SRCMIA protocol, there is no password related information transmitted over public network. Hence, an attacker has no target for comparison to guess the password offline.
8. *One-time secret communication.* Based on timestamps and the shared secret C_1, in our model the receiver can successfully authenticate the identity of the sender, verify the freshness and integrity of the received message, and decrypt the attached one-time ciphertext created using a one-time session key. Our protocol can also be used in other applications that need only unidirectional authentication, such as sending just one secret short message.

B. Efficiency Analysis

Because of the limited computation capacity of the smart card, the remote device, and IAs, the issue of communication and computation cost is very important. Our model achieves mutual authentication using just two message exchanges. In terms of computation cost, in the control phase and the reporting phase, the smart card inside the remote device performs only 4 hashing operations, and the Home Controller performs only 5 hashing operations. In other words, our model is very efficient.

C. Functionality Analysis

1. *Confidentiality.* In our model, an IA command M_c and its execution report M_r are encrypted with one-time session keys K_c and K_r, respectively. It guarantees the confidentiality of the transmitted IA commands and execution reports.
2. *Mutual authentication.* In the control phase and the reporting phase, the remote device and the Home Controller authenticate each other with message authentication codes C_2 and C_3. If both the checks on C_2 and C_3 by each receiving side are valid, the mutual authentication is guaranteed.
3. *Low cost and simple computation.* As shown in Part B, efficiency analysis, we can see that our model satisfies the requirement.
4. *Easy to use.* The registration of our model is very simple and the remote users can freely choose their own passwords. When the remote user wants to control an IA remotely, he just needs to input his identity ID_i, password PW_i and the IA command M_c.

IV. Conclusion

In this paper, we propose a novel Secure Remote Control Model for Information Appliances, namely SRCMIA, which extends Chien et al.'s solution and solves the security problem of Lee et al.'s RAMIA model. The advantages of our model include no verification table, freely chosen password, mutual authentication, and low communication and computation cost. In addition, our model satisfies the following requirements of IAs: (1) confidentiality, (2) mutual authentication, (3) low cost and simple computations, and (4) easy to use.

References

[1] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Comput. Secur.*, vol. 21, no. 4, pp. 372–375, 2002.

[2] C.-L Hsu, "Security of Chien et al's remote user authentication scheme using smart card," *Comput. Stand. Interfaces*, vol. 26, no. 3, pp. 167–169, 2004.

[3] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart card," *IEEE Trans. Consumer Electron.*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[4] W.-S. Juang, "Efficient password authenticated key agreement using smart cards," *Comput. Secur.*, vol. 23, no. 2, pp. 167–173 , 2004.

[5] H.-M. Lee, Y.-C. Chen, and J.-J. Chen, "The intelligent agent design of information appliance," in *Proc. 7th Join Conf. Information Sciences*, Cary, NC, USA, pp. 1681–1684, Sep. 2003.

[6] H.-M. Lee, H.-F. Liao, and S.-Y. Lee, "A remote authentication model of information appliances," *WSEAS Trans. Info. Sci. Appl.* vol. l, no. 2, pp. 728–732, 2004.

[7] H.-M. Lee and C.-H. Mao, "A fuzzy clustering model of information applicance," in *3rd Int. Conf. Electronic Business*, Singapore, pp. 241–243, Dec. 2003.

[8] H.-M. Lee, C.-H. Mao, and S.-Y. Lee, "A fuzzy neural network of information appliance," *Int. Workshop Fuzzy System & Innovation Computing*, Kitakyushu, Japan, pp. 7–12, June 2004.

[9] H.-M. Lee, C.-H. Mao, and S.-Y. Lee, "A fuzzy aggregative clustering control model of information appliance," *WSEAS Trans. Commun.,* vol. 3, no. 1, pp. 254–258, 2004.

[10] NIST FIPS PUB 180-2, *Secure Hash Standard*, National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, 2002.

[11] W.-G. Shieh and J.-M. Wang, "Security of Lee, Liao and Lee's remote authentication model of information appliance," *WSEAS Trans. Info. Sci. Appl.*, vol. 2, no. 4, pp. 343–348, 2005.

[12] W. Stallings, *Network Security Essentials: Application and Standards*, 2nd ed., Prentice Hall, New Jersey, 2003.