Secure Authentication Scheme with Anonymity for Wireless Environments

Anna Xiu*, Kun Li **,Hyoung Joong Kim *
*Graduate School of Information Security, Korea University
**Graduate School of Information Security, Korea University
*Graduate School of Information Security, Korea University
e-mail: 19840317xiu@korea.ac.kr

Abstract

With the development of wireless networks and the use of mobile devices, mobile user's privacy issue is becoming more and more important. Privacy includes ID anonymity and unlinkability. Unlinkability requires that any two temporary IDs which have been used before should not be associated with each other. In other words, these temporary IDs should be generated in such a way that no direct relationship among them should be derived. The existing schemes only focus on ID anonymity of mobile users. In this paper, we proposed a scheme not only holding all the merits of previous works, but also achieving unlinkability which is guaranteed by using one-time-use temporary ID. And the mobile user can also updates its one-time-use temporary ID with the help of the visited foreign agent.

1. Introduction

Anyone within the coverage of the wireless information launcher can intercept the data without being detected because of the nature of wireless communication. The security issues in wireless environment are much more severe then those in conventional networks. At the same time, the hardware resources on mobile users are strictly limited and the wireless communication has a higher channel error tate than conventional network, the security protocols which work well in conventional network are no longer suitable.

In the recent years, many secure protocols and researches[1][2][3][4][5][6] for wireless environment have been proposed.

In [1] security issues related to wireless communications and an anonymous mutual authentication scheme along with session key generation are proposed. In the scheme, each MU shares a symmetric key K with HA and a long-term alias is used to hide the MU's real identity. In [2] an authentication and key agreement protocol with anonymity is proposed. In the scheme, a new secure key agreement scheme is proposed. Zhu et. al proposed an authentication with anonymity for wireless environment [3] in 2004. Lee et. al pointed out the weakness of Zhu et. al's protocol then improved it in 2006. Wu et. al showed that Lee's protocol also does not provide user anonymity and proposed a protocol to repairs the security flaws again in 2008. However it still fails to provide identity anonymity. In [6], Xu and Feng pointed out the flaw in [5] and proposed a simple patch which repairs the security flaw.

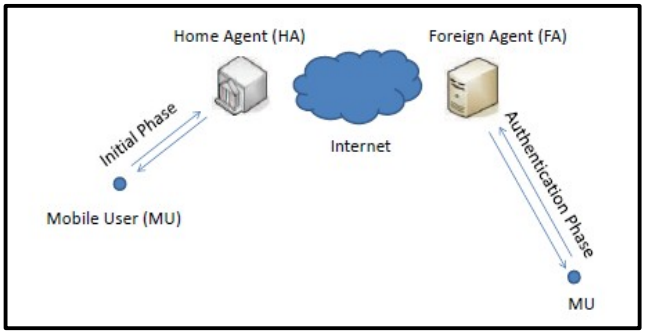
There are some disadvantages in the above papers. The schemes proposed in [1][6] use a long-term alias to achieve MU anonymity, consequently the MU can be linked by adversaries. The scheme proposed in [2] satisfies all the desired security properties, but the computational overhead at MU side is too heavy.

The proposed scheme in this paper firstly enables a MU and the FA to mutually authenticate each other when the MU roams in a visited wireless environment, and it is efficient in the terms of computational overhead. Secondly, one-time-use temporary ID is used to achieve ID privacy as well as unlinkability.

2. Proposed Scheme

In wireless environments, MU refers to mobile user, HA indicates the home agent of a MU, and FA indicates the foreign agent of the network that the

mobile user wants to visit. The HA and FA are connected to the Internet and mutually trusted. When a MU visits the FA, the MU and the FA should be able to mutually authenticate each other and establish a secure session key.



(Figure 1) System Model

Ideally, an authentication mechanism for wireless environment should provide the following desirable properties:

Authentication. Mutual authentications among MU, FA, and HA are necessary before their real communications.

ID Anonymity. When a mobile user roams in wireless environments, it is necessary to protect his real identity privacy as well as position privacy. Otherwise, the mobile user's real identity can be abused or it can also be traced by the adversary.

Implicit session key establishment. After the mutual authentication between a mobile user and a service provider, the mobile user needs to communicate with the server confidentially, which means that a secure session key should be established at both sides in such a way that no third parties can possibly know the session key except the mobile user and the service provider.

One-time-use temporary ID. If a temporary ID is used for authentication for multiple times, the personal or location information of the mobile user can be deduced by the adversary. In order to protect the MU's identity privacy and location privacy, the temporary ID of it should be used only for one time.

Unlinkability. Any temporary IDs which have been used before should not be linked by a third party to deduce that they belong to a same user. In other word s, these temporary IDs should be generated in such a way that no direct relationship among them should be derived.

In Table 1, we list the notations used in our scheme.

Notation	Description
HA	Home Agent of a mobile user
FA	Foreign Agent of the network
MU	Mobile User
ID_{ij}	The j^{th} temporary id of ID_i
LLK_i	The Long-Live Key (LLK) of ID_i
$E_K(M)$	Encryption of a message M using a key K
$S_A(M)$	Signature on a message M using a secret key of A
$P_A(M)$	Asymmetric encryption on a message M with a public key of A
T_A	Timestamp generated by an entity A
$HMAC_K(M)$	A keyed hash on message M with the key K
$\oplus$	Bitwise exclusive-or operation
$A->B:\{M\}$	Denoting that a message M is transmitted from A to B

<Table 1>Notations

The proposed authentication protocol consists of two phases: in the first phase, the MU registers at his HA and gets his first temporary id IDi1 and a long-live key (LLKi) shared with the HA secretly; In the second phase, MU visits FA, they authenticate each other with the help of the HA of MU, meanwhile MU updates his one-time-use temporary ID with the assistance of FA.

Initial phase HA maintains a table, which consists n (the number of MUs that have registered in the HA) tuples, each tuple contains four fields, they are current temporary ID, last used temporary ID, long-live key and real identity. The format of the tuple is as follows:

{IDij || IDi(j−1) || LLKi || IDi}

A mobile user (MU) first sends his/her real identity IDi to the home agent (HA), HA randomly generates long-live key LLKi and the first one-time-use temporary ID IDi1 for the MU. Then HA sends IDij and LLKi to MU through a secure channel and adds the new record {IDij || IDi(j−1) || LLKi || IDi} into the table.

In Mutual-Authentication phase, FA authenticates MU without revealing MU's real identity. Meanwhile the MU updates its one-time-use temporary ID with the help of FA. The steps of this phase are the following (see Fig. 2):

Step 1:

MU−>FA: {a, IDij, T_{IDi}, ID_{HA}, $HMAC_{LLKi}$(IDij|| T_{IDi})}

When a MU enters a new FA, the MU initiates mutual-authentication process with the FA. First MU generates a random number a as a nonce, computes

$HMAC_{LLKi}(IDij||\ T_{IDi})$ with LLKi, where T_{IDi} is a time stamp, which is secretly recorded in tamper-proof device.At last sends a, IDij , T_{IDi} , ID_{HA} and $HMAC_{LLKi}(IDij||\ T_{IDi}\ )$ to the FA.

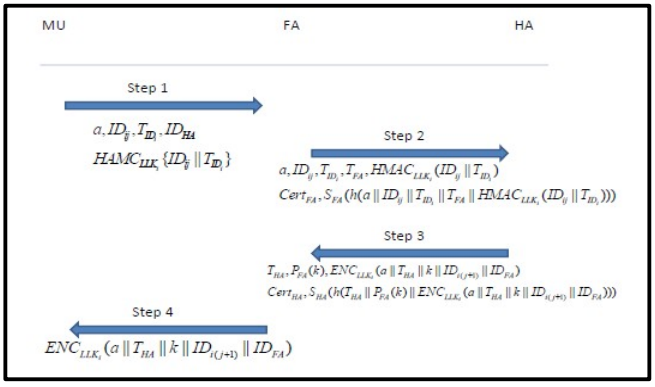


Figure 2: Mutual Authentication Phase

Step 2:
FA−>HA: {a, IDij , T_{IDi} , TFA, $HMAC_{LLKi}(IDij||\ T_{IDi}\ )$, $Cert_{FA}$, $S_{FA}(h(a\ ||\ b\ ||\ IDij\ ||\ T_{IDi}\ ||\ h(T_{FA}\ ||\ HMAC_{LLKi}(IDij||\ T_{IDi}\ )))\ \}$

On receiving the message from the MU, the FA checks if the time stamp T_{IDi} is valid. If it is valid, the FA signs on (a, ID_{ij} , T_{IDi} , TFA, $HMAC_{LLKi}(IDij||\ T_{IDi}$)) using the private key of FA, and sends a, IDij , TIDi , TFA, $HMAC_{LLKi}(IDij||\ T_{IDi}\ )$, and $S_{FA}(h(a\ ||\ b\ ||$ IDij $||\ T_{IDi}\ ||\ h(T_{FA}\ ||\ HMAC_{LLKi}(IDij||\ T_{IDi}\ )))$ to the HA.

Step 3:
HA−>FA: $\{T_{HA}$, $P_{FA}(k)$, $E_{LLKi}(a\ ||\ T_{HA}\ ||\ k\ ||$ IDi(j+1) $||\ ID_{FA})$, $Cert_{HA}$, $S_{HA}(h(T_{HA}\ ||\ P_{FA}(k)\ ||\ E_{LLKi}\ (a\ ||\ T_{HA}\ ||$ k $||$ IDi(j+1) $||\ ID_{FA})))\}$

On receiving the message from FA, the HA first checks if the signature and time stamp T_{FA} are valid. If they are valid, the HA gets the MU's real identity IDi and shared long live key (LLK_i) by looking up the table described in initial phase for IDij. There are two cases as follows:

Case 1. If IDij is found in "current temporary ID" field, the HA computes $HMAC_{LLKi}(IDij\ ||\ T_{IDi}\ )$ and compares it with received one, if they are identical, the legal identity of the MU is authenticated.

Case 2. If IDij is found in "last-used ID" field, it indicates that in the last time authentication phase for the MU, the MU failed to received its new temporary ID. So it still used the old temporary ID for authenticating. Then the HA computes $MAC_{LLKi}(IDij\ ||$ T_{IDi})) and compares it with received one, if they are identical, the legal identity of the MU is authenticated.

HA generates a random number k as the session key between FA and MU and generates the MU's next temporary ID (IDi(j+1)), then the HA computes $P_{FA}(k)$ and $E_{LLKi}(T_{HA}\ ||$ k $||$ IDi(j+1) $||\ ID_{FA})$ and signs on these information with HA's private key. At last the HA sends THA, $P_{FA}(k)$, $E_{LLKi}(T_{HA}\ ||$ k$||$ IDi(j+1) $||\ ID_{FA})$, $Cert_{HA}$, $S_{HA}(h(T_{HA}\ ||\ P_{FA}(k)\ ||\ E_{LLKi}$ (a $||\ T_{HA}\ ||$ k $||$ IDi(j+1) $||\ ID_{FA})))$ to the FA.

After sending the authentication and updating message to FA, the HA saves the IDij into "last-used temporary ID" field and the IDi(j+1) into "current temporary ID" field.

Step4:
FA− > MU : $E_{LLKi}(a\ ||\ T_{HA}\ ||$ k $||$ IDi(j+1) $||\ ID_{FA})$

On receiving the message from the HA, the FA first checks if the signature and time stamp T_{HA} are valid. Next the FA checks if the received b is the same as its original b. If so, the FA is convinced that the MU is a valid user. Then the FA forwards $E_{LLKi}(a\ ||\ T_{HA}$ $||$ k $||$ IDi(j+1) $||\ ID_{FA})$ to the MU.

Step 5:
On receiving the package, the MU decrypt the message with the LLKi and checks if the nonce number a is the original one, if it is, the MU is convinced that the FA is valid. Subsequently the MU replaces old temporary ID (IDij) with received one (IDi(j+1)).

Mutual-authentication phase done, FA and MU can communicate with each other with using the session key k securely until the session ends up.

3. Analysis and Conclusion

We evaluate our protocol in view point of security goals. The proposed scheme satisfies the security goals in wireless authentication protocol that are discussed in previous section.

An efficient authentication protocol with anonymity for wireless environments in this paper. One-time-use temporary ID is adopted in the proposed scheme to hide the real identity of the mobile user. The proposed scheme enables the mobile user and the visited foreign agent to mutually authenticate each other and establish a secure session key. At the mobile user part, only one time keyed-hash operation and one time symmetric

decryption are needed to accomplish the mutual-authentication phase, it is more efficient than the protocols mentioned in section 1.

Acknowledgements

This research is supported by Ministry of Culture, Sports and Tourism(MCST) as Korea Culture Content Agency(KOCCA) in the Culture Technology(CT) Research & Development Pro-gram 2011.

References

[1] Momammad Ghulam Rahman and Hideki Imai, “Security in Wireless Communication”, Wireless Personal Communications, pp.213-228, 2002

[2] J.P. Park, J. Go, and K. Kim, “Wireless Authentication Protocol Preserving User Anonymity”, SCIS 2001, Japan, January pp.23-26, 2001

[3] J. Zhu and J. Ma, “A New Authentication Scheme with Anonymity for Wireless Environments”, IEEE Trans. Consum. Electron, vol. 50, no. 1, PP.231-235, Feb. 2004

[4] C.C. Lee and M.S. Hwang, “Security Enhancement on a New Authentication Scheme with Anonymity for Wireless Environments”, IEEE Trans. Ind. Electron, vol. 53, no. 5, pp. 1683-1686, Oct. 2006

[5] J. Zhu and J. Ma, “A new authentication scheme with anonymity for wireless environments”, IEEE Trans, Consumer Electron, vol. 50, no. 1, pp.231-235, 2004

[6] J. Xu and D. Feng, “Security flaws in authentication protocols with anonymity for wireless environments”, ETRI Journal, pp. 460-462, 2009