A SMART CARD BASED GENERIC CONSTRUCTION FOR ANONYMOUS AUTHENTICATION IN MOBILE NETWORKS

Jing Xu[1], Wen-Tao Zhu[2] and Deng-Guo Feng[1]
[1]*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences*
100190 Beijing, China
[2]*State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences*
100049 Beijing, China

Keywords: Wireless security, Mobile network, Roaming service, Smart card, User anonymity, Password authentication, Key agreement.

Abstract: The global mobility network can offer effective roaming services for a mobile wireless user between his home network and a visited network. For the sake of privacy, user anonymity has recently become an important security requirement for roaming services, and is a topic of concern in designing related protocols such as mutual authentication and key agreement. In this paper we present a generic construction, which converts any password authentication scheme based on the smart card into an anonymous authentication protocol for roaming services. Compared with the original password authentication scheme, the transformed protocol does not sacrifice authentication efficiency, and additionally, an agreed session key can be securely established between an anonymous mobile user and the foreign agent in charge of the network being visited.

1 INTRODUCTION

The global mobility network such as the third generation (3G) network (3GPP, 2010) can offer effective global roaming service for a mobile wireless user between his home network and a foreign network being visited. A typical approach to securing wireless roaming service is to employ strong authentication measures (Suzukiz, 1997). When a mobile user M roams to a foreign network managed by a foreign agent F, he and F may perform mutual authentication under the assistance of his home agent H in the home network; although M and H cannot directly communicate with each other, the foreign agent F services as a relay between them. Usually, a successful and complete authentication ends up with a session key being established between the mobile user M and the foreign agent F to protect further communications between them.

Recently, it has been understood that in the wireless roaming service, it is an important security requirement to protect the identity anonymity for the mobile user. The disclosure of user identity may allow unauthorized entities to locate the mobile user's current whereabouts and even to track his movements, which is a serious violation of his privacy. In the literature, there have been a number of research efforts on user anonymity in mobile communication systems (Tang, 2008)(Yang, 2007)(Wan, 2008).

In the Third Generation Partnership Project - Authentication and Key Agreement (3GPP-AKA) (3GPP, 2010), the solution to user anonymity involves an anonymity key (AK). 3GPP-AKA requires encryption of the sequence numbers of the mobile user M during mobile authentication and key agreement so as to conceal M's identity and location. However, 3GPP-AKA provides user anonymity only when all foreign agents (not just the currently serving one) are benign (i.e., not compromised). Such an assumption for anonymity protection seems to be a bit too strong.

Another approach to user anonymity is to employ an alias, also known as the pseudo-identity (Tang, 2008). The idea is to associate a mobile user with an alias, which appears unintelligible to anybody except his home agent. When the user roams to a foreign network, he issues a service request to the corresponding foreign agent by presenting his alias along with other information needed for authentication, e.g., the identifier of his home network. The foreign agent then forwards the alias to the claimed home network for verification. This way the mobile user conceals his identity during the authentication. However, as

Xu J., Zhu W. and Feng D..
A SMART CARD BASED GENERIC CONSTRUCTION FOR ANONYMOUS AUTHENTICATION IN MOBILE NETWORKS.
DOI: 10.5220/0003511202690274
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2011), pages 269-274
ISBN: 978-989-8425-71-3

indicated in (Yang, 2007), the alias approach has the drawback that a user may have to renew his alias from time to time. Moreover, when the wireless communication link is accidentally broken or when some state information of either party is corrupted, the user and his home agent may loose the alias synchronization.

Yet another approach is based on sophisticated cryptographic constructions, particularly some special public-key operations. For instance, proxy signature (Tang, 2008), identity-based encryption (Wan, 2008) and blind signature (He, 2004) have been used for providing anonymity in mobile networks. Similar technique is observed in (Tzeng, 2006), though the context is for user-to-server anonymous authentication (where the roaming service scenario is not considered). However, these schemes intrinsically suffer from observable inefficiency in terms of computation and/or communication; they may not be practically applicable to mobile devices whose resources are usually constrained.

Recently, by using secure authenticated key exchange protocols (AKEPs) as building blocks, Yang *et al.* proposed a novel construction for anonymous authentication in mobile networks (Yang, 2007). The construction eliminates the alias synchronization, and does not rely on any additional security assumptions on the communication channel between the foreign network and the user's home network. However, the anonymous authentication protocol involves digital signatures; although less expensive than proxy signature (Tang, 2008) and blind signature (He, 2004), public-key operations like ordinary digital signatures are still far inefficient compared with symmetric operations. Moreover, the communication overhead of (Yang, 2007) is higher than those of other anonymous authentication protocols that are not based on underlying AKEPs. Nevertheless, the idea of employing certain security protocol as a building block for a generic construction motivates our work.

In this paper, by using secure password authentication scheme based on the smart card as a building block, we present a secure and generic construction for anonymous authentication for roaming service. Our proposal can generally convert a certain password authentication scheme into an anonymous authentication protocol of interest, and features no encryption or digital signature operation. In addition, we show that the generic construction can be instantiated efficiently, and the computation and communication costs of the instantiation are lower than or comparable to those of similar schemes.

The rest of this paper is organized as follows. Section 2 and Section 3 formally describe a smart card based password authentication (SCBPA) scheme and an anonymous authentication protocol for roaming service, respectively. Our generic construction is presented in Section 4, where security analysis and performance evaluation are also included. Section 5 concludes the paper.

2 SMART CARD BASED PASSWORD AUTHENTICATION

Our anonymous authentication protocol is built upon a smart card based password authentication (SCBPA) scheme.

In a smart card based password authentication scheme, a participant may be a user U or a remote server S. The scheme consists of three phases: registration phase, login phase, and authentication phase.

(1) **Registration Phase (SCBPA.Reg).** When a user U registers with a server S, U selects his password PW and submits it along with his identifier ID to the server S through a secure channel. Then S issues a certain smart card to U.

(2) **Login Phase (SCBPA.Log).** The user U inserts his smart card to a terminal and keys in his identifier ID and password PW. Then the terminal computes and sends on behalf of the user a login request message m to the remote server S. To authenticate the user, a secret value sv should be embedded in the message m in a cryptographic manner (e.g., through encryption), so that only the user U and the server S are able to compute sv, while any other entity cannot obtain sv even if he eavesdrops on the communication channel and thus knows the message m.

(3) **Authentication Phase (SCBPA.Auth).** The server S checks the legitimacy of the received message m by verifying the secret value sv, and consequently determines whether to accept U's login request or not.

As mentioned above, the registration phase (SCBPA.Reg) takes place in a secure environment, and both parties U and S are assumed to be honest and to perform exactly according to the scheme specification. This phase, in the real word, is typically done out-of-band (e.g., at a service counter) so that the transaction is authenticated, confidential, and reliable. In the login and authentication phases (SCBPA.Log and SCBPA.Auth), the communication channel is no longer supposed to be still secure. For example, an *active* adversary $\mathcal{A}$ may have totally control over the wireless communication channel; he may intercept,

insert, delete, or modify any message sent over the air. In addition, we allow such an active $\mathcal{A}$ to (1) either steal a user's smart card and then extract any secretly stored information from it, or (2) compromise the user's password (e.g., with an over-the-shoulder attack), but not both (1) and (2). In other words, we do not consider the case when a user's password and his smart card are both compromised, as then there will be no way to prevent the adversary $\mathcal{A}$ from masquerading as the legitimate user (i.e., the owner of the smart card) (Xu, 2009). Nevertheless, our security assumption is still weaker than most related works. In other words, we expect the SCBPA scheme to be secure in itself instead of relying on certain assumptions that may be too strong in practice.

3 ANONYMOUS AUTHENTICATION IN MOBILE NETWORKS

In an anonymous authentication protocol, a participant may be a mobile user M, a foreign agent F, or a home agent H. The home agent pre-shares a secret key K_{FH} with the foreign agent F, whose network is being visited by M. The protocol consists of a registration phase and a mutual authentication phase.

(1) **Registration Phase.** When a mobile user M registers with his home agent H, he selects his password PW and submits it along with his identifier ID to H through a secure (typically out-of-band) channel. Then H issues a smart card to M.

(2) **Mutual Authentication Phase.** The mutual authentication between M and the foreign agent F is performed under the assistance of the home agent H, who is out of M's reach. If authenticated, M can access the wireless service in the foreign network, and an agreed session key SK (i.e., K_{MF}) is established between M and F for securing future communications. Note that a secret K_{FH} is pre-established between the two agents.

It is desirable for anonymous authentication protocols to possess the following security attributes:

- *User Anonymity:* The real identity of a mobile user M should be protected from being revealed by any other entity except his home agent H.
- *Mutual Authentication:* The mobile user M and the foreign agent F can authenticate each other under the assistance of the home agent H, which implies resistance against impersonation attacks.
- *Confidentiality and Fairness of the Session Key:* The mobile user M and the foreign agent F can securely agree on a random session key, which should be only known to them and contain contributions from both of them.
- *Protection on User Password:* The password of the mobile user M should be protected against the off-line dictionary attack, even if his smart card is stolen.

4 GENERAL CONSTRUCTION FOR ANONYMOUS AUTHENTICATION IN MOBILE NETWORKS

We now propose a generic approach to constructing an anonymous authentication protocol for roaming service. In our proposal, we employ a secure SCBPA scheme as the building block.

4.1 Proposal Description

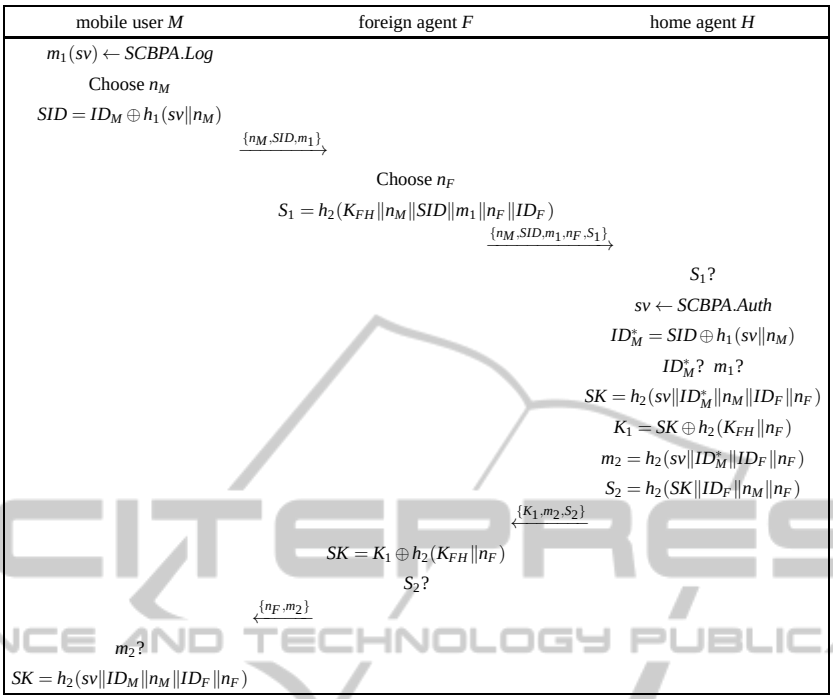
Let *SCBPA* be a smart card based password authentication scheme that is secure as defined in Section 2. Suppose in the login phase, the generated login request message is m_1, where the identity ID_M is not included in m_1, and the secret only known to the user and the remote server is sv. We denote this by $m_1(sv) \leftarrow SCBPA.Log$. As introduced in Section 3, the anonymous authentication protocol consists of a registration phase and a mutual authentication phase.

Phase I: Registration. This phase is the same with the registration phase of the SCBPA scheme (i.e., *SCBPA.Reg*). In addition, H chooses large prime number p and two one-way hash functions $h_1(\cdot), h_2(\cdot) : \{0,1\}^* \rightarrow Z_p^*$.

Phase II: Mutual Authentication. In this phase, the mobile user M and a foreign agent F perform mutual authentication and agree on a session key SK, under the assistance of M's home agent H. The steps of this phase are outlined in Table 1 and explained as follows.

(1) When M enters a foreign network managed by F, he inputs his identity ID_M and his password into the smart card. The device starts the login phase in *SCBPA* and generates the login request message m_1 embedding the secret value sv. The device also appropriately chooses a random number n_M, and computes $SID = ID_M \oplus h_1(sv \| n_M)$, where the identity ID_M is appended η bits of '0' in its binary form, so that the padded ID_M is of the same length with the output of $h_1(\cdot)$. Then the device sends the message $\{n_M, SID, m_1\}$ to F on behalf of M.

Table 1: Mutual authentication phase of the proposed general construction.



(2) Upon receiving the message, F randomly chooses n_F, computes $S_1 = h_2(K_{FH}\|n_M\|SID\|m_1\|n_F\|ID_F)$, where K_{FH} is the pre-shared symmetric key between F and H. Then F sends the message $\{n_M, SID, m_1, n_F, S_1\}$ to H.

(3) Upon receiving the message, H checks whether $S_1 = S_1^*$, where $S_1^* = h_2(K_{FH}\|n_M\|SID\|m_1\|n_F\|ID_F)$ is locally computed. If so, H starts the authentication phase in *SCBPA*, computes the secret value sv, and obtains $ID_M^* = SID \oplus h_1(sv\|n_M)$. Then H checks whether ID_M^* is the identity of a legitimate user and whether the submitted login request message m_1 is valid. If both conditions are met, H computes $SK = h_2(sv\|ID_M^*\|n_M\|ID_F\|n_F)$, $K_1 = SK \oplus h_2(K_{FH}\|n_F)$, $m_2 = h_2(sv\|ID_M^*\|ID_F\|n_F)$, $S_2 = h_2(SK\|ID_F\|n_M\|n_F)$, and sends the message $\{K_1, m_2, S_2\}$ to F.

(4) Upon receiving the message, F computes $SK = K_1 \oplus h_2(K_{FH}\|n_F)$, $S_2^* = h_2(SK\|ID_F\|n_M\|n_F)$, and checks whether $S_2^* = S_2$. If so, F believes that M is an authorized user, and forwards $\{n_F, m_2\}$ to M.

(5) M computes $m_2^* = h_2(sv\|ID_M\|ID_F\|n_F)$, and checks whether $m_2^* = m_2$. If so, M believes that F is authenticated, and computes the agreed session key $SK = h_2(sv\|ID_M\|n_M\|ID_F\|n_F)$.

4.2 Security Analysis

We now investigate the security of our general construction presented above. The analysis concerns the semantic security of the session key as well as the user anonymity .

Theorem 1. Let *SCBPA* be a smart card based password authentication scheme, and *GC* be our proposed general construction depicted in Table 1. Then our general construction *GC* is secure provided that the password authentication scheme *SCBPA* satisfies semantic security.

Proof. The detailed proof can be found in the full version.

Theorem 2. Let *SCBPA* be a smart card based password authentication scheme. If *SCBPA* is semantically secure, then our general construction of the anonymous authentication protocol for roaming service can achieve user anonymity in the random oracle model.

Proof. In our construction, we can see that besides SID and m_2, there is no information related to the identity of the mobile user M. Without knowing sv (which is the secret value in *SCBPA*), SID and m_2 are just the hash results of some unknown values and do not help the adversary obtain any additional information associated with M. Therefore, the user anonymity of our construction reduces to the seman-

tic security of *SCBPA*.

4.3 Instantiation

Following the general construction, we present a concrete example of transforming a SCBPA scheme (Xu, 2009) into an anonymous authentication protocol for roaming service.

Phase I: Registration. To initialize, H selects large prime number p and q such that $p = 2q+1$. The home agent also chooses its secret key $x \in Z_q^*$ and three appropriate one-way hash functions $h(\cdot), h_1(\cdot), h_2(\cdot) : \{0,1\}^* \rightarrow Z_p^*$. Then the protocol proceeds in the following steps:

(1) The mobile user M chooses his ID_M and PW. He then submits the registration request $\{ID_M, PW\}$ to H through a secure channel.

(2) Upon receiving the registration message, the server computes $B = (h(ID_M)^x \cdot h(PW)) \bmod p$.

(3) The server stores $\{B, h(\cdot), h_1(\cdot), h_2(\cdot), p\}$ into a smart card and issues the device to the user.

Phase II: Mutual Authentication.

(1) When M enters a foreign network managed by F, he inputs his identity ID_M and his password PW^* to the smart card. Then the device appropriately chooses $w \in_R Z_q^*$ and a random number n_M, computes $R = B/h(PW^*) \bmod p$, $B' = (B/h(PW^*))^w \bmod p$, $W = h(ID_M)^w \bmod p$, $C = h(T\|B'\|R\|W\|ID_M)$, and $SID = ID_M \oplus h_1(B'\|n_M)$, and sends the message $\{n_M, SID, C, W, T\}$ to F, where T is a time stamp.

(2) Upon receiving the message, F randomly chooses n_F, computes $S_1 = h_2(K_{FH}\|n_M\|SID\|C\|W\|T\|n_F\|ID_F)$, and sends to H the message $\{n_M, SID, C, W, T, n_F, S_1\}$, where K_{FH} is the pre-shared symmetric key between F and H.

(3) Upon receiving the message at time T', H verifies whether the difference between T and T' is within a predefined threshold. Then H computes $S_1^* = h_2(K_{FH}\|n_M\|SID\|C\|W\|T\|n_F\|ID_F)$ and checks whether $S_1^* = S_1$. If so, H computes $B'' = W^x \bmod p$ and obtains $ID_M^* = SID \oplus h_1(B''\|n_M)$. Then H checks whether ID_M^* is a legal identity and whether C equals $h(T\|B''\|h(ID_M^*)^x\|W\|ID_M^*)$. If both conditions are met, M is authenticated, and F is implicitly authenticated. H continues to compute $SK = h_2(h(ID_M^*)^x\|ID_M^*\|n_M\|ID_F\|n_F)$, $K_1 = SK \oplus h_2(K_{FH}\|n_F)$, $m_2 = h_2(B''\|ID_M^*\|ID_F\|n_F)$, $S_2 = h_2(SK\|ID_F\|n_M\|n_F)$, and sends the message $\{K_1, m_2, S_2\}$ to F.

Table 2: Performance comparison between three solutions. "Pre" denotes pre-computed (i.e., offline) operation. A signature operation is counted as an asymmetric encryption.

Performance Metrics		Our scheme	Tang's Scheme	Yang's Scheme
Modular exponentiation	**M**	**2 Pre**	**N/A**	**N/A**
	F	N/A	N/A	N/A
	H	2	N/A	N/A
Symmetric cryptographic operation	**M**	**N/A**	**1**	**N/A**
	F	N/A	1	N/A
	H	N/A	2	N/A
Asymmetric cryptographic operation	**M**	**N/A**	**1**	**2**
	F	N/A	0	1
	H	N/A	0	2
Communication rounds		2	2	3

(4) Upon receiving the message, F computes $SK = K_1 \oplus h_2(K_{FH}\|n_F)$, $S_2^* = h_2(SK\|ID_F\|n_M\|n_F)$, and checks whether $S_2^* = S_2$. If so, it believes that M is an authorized user and forwards $\{n_F, m_2\}$ to M.

(5) M computes $m_2^* = h_2(B'\|ID_M\|ID_F\|n_F)$, and checks whether $m_2^* = m_2$. If so, M believes F is authenticated and computes the agreed session key $SK = h_2(R\|ID_M\|n_M\|ID_F\|n_F)$.

4.4 Performance Evaluation

Next, we evaluate the performance of our instantiation by comparing the mutual authentication phase with those of Tang *et al.*'s scheme (Tang, 2008) and Yang *et al.*'s scheme (Yang, 2007) in Table 2. Particularly, we focus on the numbers of operations that a mobile user M needs to perform (marked in bold font), because mobile devices usually are not as powerful as desktop computers and thus are not suitable for computation intensive tasks.

Table 2 shows that, for the mobile user M, Phase II of our protocol only introduces two extra modular exponentiations, but the modular exponentiations can both be pre-computed off-line. Both (Tang, 2008) and (Yang, 2007) require certain public-key operations, while our construction does not need them (other than the modular exponentiations). Therefore, the computation complexity of our protocol is more efficient than those of (Tang, 2008) and (Yang, 2007).

Next, we look into the communication complexity. Our mutual authentication phase takes only one round of message exchange between M and F, and one round between F and H (recall Table 1), while Yang *et al.*'s scheme (Yang, 2007) takes two rounds of message exchange between M and F, and one round between F and H. Therefore, the communication complexity of our instantiation is comparable to that of (Tang, 2008), but more efficient than that of (Yang, 2007).

5 CONCLUSIONS

In this paper, we have proposed a secure and generic approach to constructing an anonymous authentication protocol for roaming service, employing a secure password authentication scheme based on the smart card as the building block. Our approach eliminates the alias synchronization between the mobile user and his home agent, and does not rely on any signature operations or encryptions. Moreover, the construction can be instantiated efficiently, and the computation and communication costs of the instantiation are lower than or comparable to those of similar schemes.

ACKNOWLEDGEMENTS

This work was supported by the National Grand Fundamental Research (973) Program of China under grant 2007CB311202, the National Natural Science Foundation of China (NSFC) under grants 60970138 and 60873197, and the Knowledge Innovation Program of Chinese Academy of Sciences under grant YYYJ-1013.

REFERENCES

3rd Generation Partnership Project. (2010). Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 9). *Available online at http://www.3gpp.org/ftp/Specs/html-info/33102.htm.*

Suzukiz S. and Nakada K.(1997). An authentication technique based on distributed security management for the global mobility network. *IEEE Journal on Selected Areas in Communications*. vol. 15, no. 8, pp. 1606–1617.

Tang C. and Wu D. O.(2008). Mobile privacy in wireless networks-revisited. *IEEE Transactions on Wireless Communications*. vol. 7, no. 3, pp. 1035–1042.

Yang G., Wong D. S., and Deng X.(2007). Anonymous and authenticated key exchange for roaming networks. *IEEE Transactions on Wireless Communications*. vol. 6, no. 9, pp. 3461–3472.

Wan Z. G., Ren K., and Preneel B.(2008). A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks. In: *1st ACM Conference on Wireless Network Security (WiSec 2008)*. pp. 62–67.

He Q., Wu D., and Khosla P.(2004). Quest for personal control over mobile location privacy. *IEEE Communications Magazine*. vol. 42, no. 5, pp. 130–136.

Tzeng W.-G.(2006). A secure system for data access based on anonymous authentication and time-dependent hierarchical keys. In: *1st ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS 2006)*. pp. 223–230.

Xu J., Zhu W.-T., and Feng D.-G.(2009). An improved smart card based password authentication scheme with provable security. *Computer Standards & Interfaces*. vol. 31, no.4, pp.723–728.