ISSN 2319 – 7595
Volume 2, No.4, July – August 2013
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/pdfs/ijiscs02242013.pdf

Optimal Authentication Scheme for Mobile Communication System

D.Suneetha
esearch Scholar, DRKIST,
Hyderabad, India
suneedmtech@gmail.com

Dr.R.V.Krishnaiah
Principal, DRKIST,
Hyderabad, India
r.v.krishnaiah@gmail.com

ABSTRACT

To meet the security specifications many of existing user authentication schemes require huge computational cost. This Huge computational cost is because many of the authentication methods used exponential operations. But this approach is not suitable for mobile devices. In this paper we propose a low computation cost user authentication scheme for mobile communication. Our scheme uses only one-way hash functions and smart cards and can be implemented efficiently. The proposed scheme addresses the weakness appeared in existing methods and is well suitable for mobile communications.

Key words—Authentication, Smart card, hash function

1. INTRODUCTION

To enhance security in mobile communication user authentication is a prerequisite step and much work is done with many advanced schemes. In 1981, Lamport [1] proposed a user authentication scheme for communication in secure channel. His scheme could resist against replaying attacks: however it needs a password table for the verification schemes [2]-[[5] have been proposed to avoid this kind of drawback. One of the characteristics that passwords are assigned to the registered users by the server is a common disadvantage in most of the authentication schemes.

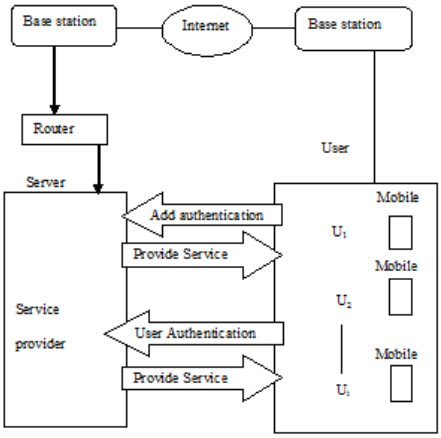

Figure 1: User Authentication Block Diagram

In 2003,Wu and Chieu [6] proposed a user authentication scheme with smart cards to improve the disadvantage.

Their scheme lets users be able to choose and change their passwords freely. However, Yang and Wang [7] pointed out the scheme suffers from the forgery attack in 2004. Besides, their scheme requires costly exponentiation computation and thus it is not suitable for mobile devices [8], [9] with low computation capability. In this article, we propose an improved low cost user authentication scheme for mobile devices, shown in Figure 1, which can solve these problems and spend low computational cost.

2.RELATED WORK

In 2003, Wu and Chieu [6],[10] proposed a scheme with smart cards for user authentication. Their scheme consists of three phase: the registration phase, the login phase, and the authentication phase.

2.1 Registration Phase:

Suppose that a new user *Ui* submit his *IDi* to the system for registration. The system calculates the password *PWi* for the user *Ui* as follows:
$PWi=IDi^{xs} \bmod p$
Where xs is a secret key maintained by the system. The registration center issues a smart card, Which contains the public parameters (*f*, *p*), where f is a one-way function. The registration center is also delivered PWi to the user through a secure channel.

2.2 Login Phase:

Step 1: Generate a random number *r*.
Step 2: Compute $C1 = IDi^{r} \bmod p$.
Step 3: Compute $t = f(T \oplus PWi) \bmod (p\text{-}1)$, where T is the current date and time of the input device. And $\oplus$ denotes an exclusive operation.
Step 4: Compute $M = IDi^{t} \bmod p$.
Step 5: Compute $C2 = M(PWi)^{r} \bmod p$.
Step 6: Send a message $C = (IDi, C1, C2, T)$ to the remote system.

2.3Authentication Phase:

Step 1: Test the validity of *IDi*. If the format of *IDi* is incorrect, then the system rejects the login request.
Step 2: Test the time interval between T and T^0 . If $(T^0-T)<=T$, where T^0 is the current date T denotes the expected legal time interval for transmission delay, then the system rejects the login request.
Step 3: If $C2(C1^{xs})^{-1} \bmod p = (IDi)\ f\ (T \oplus PWi)$, then the system accepts the login request. Otherwise, it rejects the login request.
Some observations on the scheme are shown as follows:
(1) Password chosen by the system
(2) Requiring clock synchronization and delay-time limitation
(3) No server authentication
(4) Revoking the lost cards with changing the user's identities

2.4. Forgery Attack:

1. An intruder can collect the login message m={ID,Bi*,C1,T}
2. From the message he (or she) can obtain the correct value of Bi since Bi*=Bi for a legal user in the login phase.
3. After that, the intruder can forge the verifiable value C1e by computing C1e=h(Te/Bi), where Te is update timestamp.
4. Then the intruder can send the message m={ID,Bi*,C1e,T)e to the server.
5. We can see that, with this, he (or she) will pass through the verification phase and then masquerade successfully as the legal user.

3. BASIC IDEAS OF PROPOSED SCHEME

The proposed remote authentication scheme using smart cards is based on some key ideas which are listed below:

3.1. Breaking the password table into pieces:

To eliminate the password table in a remote login protocol, we can break it into pieces and encrypt each piece, containing the user's identity and (hashed) password, with the secret key of the system. The system then stores the encrypted pieces in the smart cards of the users, respectively, at the registration stage. If a user decides to login the system, she/he must prepare and submit necessary parameters along with the encrypted piece stored in her/his card to the system. Thus, the system can decrypt it and then obtains the user's password for verification without maintaining the password table.

3.2 Two-factor Authentication:

The personal secret information of each user for authentication is divided into two parts. One is stored in her/his smart card issued by the system and the user memorizes the other part. The user is permitted to login the system only when she/he can present both of two parts, the login request will be rejected.

3.3 Secure Channels:

If a user transmits her/his login message in a plain form to the system, the attackers can interrupt and modify the message easily. It will effect the security of the system since the attackers may derive some secret information from the collected messages. In order to prevent the attack, we will establish a user efficient secure channel between the system and the user to transmit login information such that the attack cannot work.

3.4 Mutual Authentication:

If the server alone checks the user authenticity the server may sometimes be faulty. It will effect the security of the system. In order to prevent the attack, we will provide the scope for the user also to authenticate the server with the information sent from the server. Thus we provide mutual authentication. To avoid the intruders from cheating the users and obtaining the secret information from them, the system must provide the way for the user to check whether the messages received are from the legal server. By again verifying the values sent by server with its own the user checks the server in this scheme.

3.5 Low Computation Cost:

If high cost computation exponential functions are used the scheme is not suitable for mobile devices. So this scheme uses the low cost computational hash functions to make it even suitable for mobile devices.

4. THE PROPOSED USER AUTHENTICATION SCHEME

These three phases are described in the following subsections, respectively

The Registration Phase

This phase is invoked when a new user Ui wants to register with the remote system. This phase is similar is similar to Wu and Chieu registration phase with some modifications

Step 1: Ui selects a password PWi, he/she submits his/her identity ID PWi to the remote system through a secure channel.

Step 2: Server s computes :
Ai=h(ID||x)
Bi=h(Ai||h(PW))
Where x is the secret key of the server and h(.) is the one way hash function.

Step 3: Server issues a smart card with the secure information {Id,Ai,Bi,h(.)} and delivers it to user through secure channel .

Login Phase:

In the login phase, the user inserts his/her smart card into the card reader and keys in his/her Identity with the corresponding password, and then the smart card performs the following operations:

1.Smart card computes

$Bi^*=h(Ai||h(PW^*))$and

$C2=Bi^* \oplus Ai$

$C1=h(T \oplus Bi)$

T is the timestamp which includes current date and time.

2. It then sends a message m={Id,C1,C2,T} to the server

Authentication Phase:

In the authentication phase, the server first checks the format of ID to make sure whether it is valid. Then, the server authenticates the user with the following steps:

1. Verify the timestamp T with the current date and time $T^{'}$. If the $(T - T^{'}) \geq \Delta T$ where ΔT denotes expected valid time interval for transmission delay, then the server rejects the login request.

2. Compute

$Ai=h(ID||x)$

$Bi^*=C2 \oplus Ai$

$C1^*=h(T \oplus Bi^*)$

3. Checks whether

$C1^*=C1$ or not

If they are equal, it means that the password PW is equal to PW^*. Then the system accepts the login request. Otherwise, it rejects the login request.

Mutual Authentication:

1. Server computes $C3=Ai \oplus T^*$

2. Server then sends $(C3,T^*)$ to the user.

3. User now computes $Ai^*=C3 \oplus T^*$

4. Now the user compares Ai already available with Ai^*. If the $Ai=Ai^*$ then the server is accepted as the correct one otherwise it is rejected.

Password Change :

1. User u enters his identity and password(ID,PW) and requests password change

2. Smart card computes:

$Ai=h(ID||x)$

$Bi=a(Ai||h(PW))$

3. It then stores the information {Id,Ai,Bi,h(.)} instead of previous information and compares the values with these in the Login Phase.

5. RESULTS

The results are classified into security analysis, computational time analysis and cost.

5.1. Security Analysis

The Proposed scheme overcomes the security weakness of Wu and Chieu scheme. The advantages of the proposed scheme are explained as follows:

It can protect against guessing attack:

It is hard to derive server's secret key x from the hash value of Ai=h(ID||x), by using the security characteristics of the one-way hash function. It is also difficult to legal user's password from the equation Bi=h(Ai||h(PW))

It can protect against Replaying attack:

Replaying attacks cannot work because it will make Step1 of the authentication phase fail. No one can compute valid $C1=h(T \oplus Bi)$ because it must be derived from Ai and T

It can protect against Forgery attack:

Intruder might collect the legal login message m={Id,C1,C2,T) and try to modify it into m_e={Id,C_{1e},C2,T) (where current date and time). In this case, he/she has to compute a correct value $C_{1e}=h(T_e \oplus Bi)$. However, the parameter $Bi=Bi^*$ cannot be obtained from C2 because the value of Ai is unknown. An intruder might forge the message m_e={Id,C_{1e},C_{2e},T} where $C_{2e}=0$. In this case, due to the parameter $Bi^*=h(C_{2e} \oplus Ai)$, he/she has to compute the verifiable value such that $C_{2e}=h(T_e \oplus Bi^*)=h(T_e \oplus Ai)$. However, he/she cannot obtain the correct value of C_{1e} because the parameter Ai is unknown. Since $Bi^*$and Ai are the message digests of SHA-512 (i.e 512 bits in length), the probability of guessing correct values of Bi^* and Ai from C2 is less than $1/2^{512} * /2^{512}$ .It is difficult to obtain the correct values of Bi^* and C1 by just knowing the C2.

5.2. Computational Complexity Analysis:

Table 1: Comparison of computational cost of Wu and Chieu scheme and Proposed scheme

Phases	Wu-Chieu scheme	Proposed Scheme
Registration phase	1 Tmul+1 Texp +2T_H	3 T_H
Login phase	1 Tmul+1 Texp +1T_H+1 Txor	3 T_H+ 2 Txor
Authentication phase	1T_H+1 Txor	2 T_H+ 4 Txor
Total cost	2 Tmul+2 Texp +5T_H+2 Txor	8 T_H+ 7 Txor

In this section we will analyze the efficiency of the proposed scheme in terms of computational complexity and compare it with Wu and Chieu scheme. Here we considered notation T

as the time for computing one way hash function. Table 1 shows the comparison of our scheme and Wu and Chieu scheme in terms of cost. In Wu and Chieu scheme in the Registration phase the server computes one multiplication one exponential and two hash functions and in Login phase user performs one hash function, one exponential function one xor function and one hash function. In Authentication phase server computes one hash and one exponential function.

In the proposed scheme in the Registration phase server uses three hash functions, In the Login Phase the smart card and the user uses three hash functions and two xor functions and in the authentication phase the server uses two hash and three xor functions and user uses one xor function for mutual Authentication as upon receiving the message the user smart card computes one xor function for authenticating the remote system.

5.3. Cost Comparisons

In this section, we compare the computational cost of the three phases (registration, login and authentication) for our scheme with Wu-Chieu's. We define some notations as follow.

T_{EXP}: The modular exponential computation.
T_{MUL}: The multiplication computation.
T_{XOR}: The exclusive-or.

The comparative results are shown in Table 1. We know that a modular exponential computation is much more time consuming than one-way hash function. Besides, the exclusive-or operations can be performed very efficiently. From Table 1, our proposed scheme requires only one-way hash functions and exclusive-or operations that can be implemented efficiently.

6. CONCLUSIONS

In this paper we have shown the drawbacks of the Wu-Chieu scheme and then propose a novel scheme to solve the problems. We also analyze the security and computation cost required for the proposed scheme. From Table 1, we can see that our scheme is much more efficient than Wu-Chieu scheme since it uses only low-cost functions and thus can be executed very efficiently. In a word, our scheme can be easily implemented on a mobile device with low computation capability.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," communications of the ACM, Vol. 24, 1981, pp. 770-772.

[2] T. C. Wu, "Remote login authentication scheme based on a geometric approach," Computer Communications, Vol. 18, No. 12,1995, pp. 959-963.

[3] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," International Journal of Computer Mathematics, Vol. 70, 1999, pp. 656-666.

[4] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, 2000, pp.28-30.

[5] H. M. Sun, "An efficient remote use authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, 2000, pp. 958-961.

[6] S. T. Wu and B. C . Chieu , "A user friendly remote authentication scheme with smart cards," Computers & Security, Vol. 22, Issue 6, 2003, pp. 547-550.

[7] C. C. Yang and R. C. Wang, "Cryptanalysis of auser friendly remote authentication scheme with smart cards," Computers & Security, Vol. 23, Issue 5, 2004, pp. 425-427.

[8] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," IEEE Journal on Selected Areas in Communications, Vol. 11,1993, pp. 821-829.

[9] D. Brown, "Techniques for privacy and authentication in personal communication system," IEEE Personal Communications, Vol. 2, 1995, pp. 6-10.

[10] R. Ramaswamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," International Journal of Network Security, Vol.14, No.3, 2012, PP. 180-186.