Design and Research of a New secure Authentication Protocol in GSM networks

Ai-qin QI[1,a], Yong-jun SHEN[2]

[1]*Northwest University For Nationalities ,China*
[2]*Lanzhou University , China*

Abstract. As the first line of defense in the security application system, Authentication is an important security service. Its typical scheme is challenge/response mechanism and this scheme which is simple-structured and easy to realize has been used worldwide. But these protocols have many following problems In the GSM networks such as the leakage of user indentity privacy, no security protection between home registers and foreign registers and the vicious intruders' information stealing and so on. This paper presents an authentication protocol in GSM networks based on maths operation and modular square root technique . The analysis of the security and performance has also been done. The results show that it is more robust and secure compared to the previous agreements.

1 Introduction

Global mobile communications network GSM originated in 1980s as the Pan-European digital cellular system standard and it is now accepted as the worldwide wireless communication. They convey all sorts of data and messages through wireless channel and can't require the cables. With the development of network applications, security problems arises . As the first defense line of secure application system, the authentication is the most important secure service. However, it is not feasible for GSM networks to use traditional security mechanisms because of its inherent limitations. A kind of simple and efficient authentication protocol needs to be taken into account.

In this paper, we propose a suitable GSM authentication protocol that use mathematical and modular square residual to complete the authentication process. The protocol security analysis has been done. Compared to the previous agreements, it is more robust and secure.

The rest of the paper is organized as follows: Section 2 discusses related work. Section 3 presents the proposed authentication protocol. Section 4 analyzes the security and the performance of the proposed protocol. Section 5 finally concludes the paper.

2 Related work

User authentication is an important topic for communication security and there are many schemes existed for the purpose in the literatures. In 1981, Lamport[1] proposed a user authentication scheme for communication in insecure channel. With the development and application of wireless networks and mobile technologies, people begin to focus on GSM authentication protocol . In 2004, M. S. Hwang and L. H. Li[2] presented an authentication scheme, but it was found that this solution had weakness and a modified version to overcome them has been presented by M. S. Hwang, I.E.Liao and C. C. Lee[3]. The study in the literature [4] has showed that the scheme in [3] also fails to provide anonymity. Two recent studies [5][6] has shown that all above schemes are incapable of providing the anonymity. Later security weaknesses of the approaches in [2-4] have been concluded and an enhanced authentication scheme[7] with anonymity named as EASA has been presented. Through the analysis of the protocol in the literature [7], we find that the scheme is still not to provode anonymity ,it is also vulnerable to insider attack, off-line password guessing attack and forgery attack etc.

In this paper, we propose a suitable GSM authentication protocol using mathematical and modular square residual[8] to complete the certification process. This paper also makes the analysis of security and performance. Compared to the previous agreement, it is more robust and secure.

3 The proposed protocol

Supposing that a mobile user Mu whose home agent is HA will visit a foreign network and the foreign agent is FA . HA Selects two large prime numbers p, q and calculates

[a] Corresponding author: qi-133@163.com

n=pq as the public key. HA selecsts a random number X_{HA} and a primitive g of the multiplicative group Zn* and calculates $Y_{HA} = g^{X_{HA}} \bmod n$. (X_{HA} , Y_{HA}) makes up the master key of HA and the key length is long enough such as 512 bits. For each foreign agent, H_A calculates the corresponding session key which meets $SK_{HF} = h(ID_{FA} \| X_{HA} \| ID_{HA})$ by using Diffie-Hellman key distribution protocol and hash function such as SHA-1 algorithm.

In this section, we present our authentication protocol which has five phases: initialization ,login, authentication , refreshment of session key and refreshment of password. Table 1shows the symbol that would be used in this paper.

Table 1. the symbol description

symbol	Description
Mu	mobile user
ID_x	The identity of mobile user x
pw_u	The passward of mobile user Mu
HA	Home register of mobile user
FA	Fforeign register
$\|$	Connection operation
$\oplus$	Exclusive-OR operation
$h(\cdot)$	Hash function

3.1 Initialization

Mobile user Mu sends his identity Id_U to his home register HA by a secure channel. HA computes $TH_u = h(ID_{mu} \| Y_{HA})$, $SK_{uH} = h(ID_{mu} \| X_{HA})$ and injects the information $\{TH_u, SK_{uH}, h(.), n\}$ into the smart card. Then HA sends the smart card to the mobile user Mu. After receiving the smart card, Mu selects a random password pw_u ,a random number b and calculates $SK_{uH}' = h(ID_{mu} \| pw_u) \oplus SK_{uH}$, $V_{uH} = TH_u \oplus h(ID_{mu} \| h(pw_u \| b))$, $H_{uH} = h(TH_u) \oplus h(ID_{mu} \oplus b)$. $\{V_{uH}, H_{uH}, SK_{uH}', h(.), n, b\}$ is the final information of the smart card.

3.2 Login

Mu inserts the smart card into the terminal and inputs ID_{mu} , pw_u to calculate $TH_u^* = V_{uH} \oplus h(ID_{mu} \| h(pw_u \| b))$, $H_{uH}^* = h(TH_u^*) \oplus h(ID_{mu} \oplus b)$. Mu checks if H_{uH} * equals H_{uH} , if equal the user is a legal user. Then Mu selects a random number n_{mu} ,computes $m_1 = (ID_{mu} \| ID_{FA} \| TH_u \| n_{mu})^2 \bmod n$ and sends m1 to the foreign agent FA.

3.3 Authentication

The authentication phase includes five steps as follows:

Step 1: After receiving the information m1, FA selects a random number n_{FA} and computes $req_{FA} = n_{FA} \oplus SK_{HF}$ and sends the information $m_2 = \{m_1, req_{FA}, h(m_1 \| req_{FA} \| SK_{HF})\}$ to HA.

Step 2: After receiving FA's message, HA decrypts m2 by using the prime p,q to get $ID_{mu}, ID_{FA}, TH_u, n_{mu}$ .Then HA checkes the validity of ID_{mu} and judges if $h(ID_{mu} \| Y_{HA})$ equals TH_u . If correct, HA computes $h(ID_{FA} \| ID_{HA} \| X_{HA})$ and checks if $h(m_1 \| req_{FA} \| h(ID_{FA} \| ID_{HA} \| X_{HA}))$ calculated equals $h(m_1 \| req_{FA} \| SK_{HF})$ received from FA, if the above condition holds, FA is authenticated by HA. HA computes $n_{FA}^* = h(ID_{FA} \| ID_{HA} \| X_{HA}) \oplus req_{FA}$, $K_1 = h(ID_{mu} \| ID_{FA} \| n_{mu}) \oplus h(SK_{HF} \| n_{FA}^*)$, $K_2 = h(h(n_{mu}) \| h(n_{FA}^*) \| SK_{uH})$, $S_1 = h(K_1 \| K_2 \| n_{FA}^* \| SK_{HF})$ and sends $m_3 = \{K_1, K_2, S_1\}$ to FA.

Step3: When receiving the message m3, FA uses the session key SK_{HF} to compute $h(K_1 \| K_2 \| n_{FA} \| SK_{HF})$ and judge if it equals S_1 . If it holds,HA is authenticated by FA. FA calculates $h(ID_{mu} \| ID_{FA} \| n_{mu}) = K_1 \oplus h(SK_{HF} \| n_{FA})$, $K_3 = h(ID_{mu} \| ID_{FA} \| n_{mu}) \oplus h(n_{FA})$ and sends $m_4 = \{K_2, K_3\}$ to the mobile user Mu.

Step4: Mu receives the message m4 , computes $h(n_{FA}) = h(ID_{mu} \| ID_{FA} \| n_{mu}) \oplus K_3$ and judeges if $h(h(n_{mu}) \| h(n_{FA}) \| SK_{uH})$ equals K_2 , if it holds , FA is authenticated by Mu. Mu computes the session key $SK = h(h(n_{FA}) \| h(ID_{mu} \| ID_{FA} \| n_{mu}))$ which is used to communicate with FA. Mu computes $h(h(n_{FA}) - 1)$ amd sends $m_5 = h(h(n_{FA}) - 1)$ to FA.

Step5: FA computes $h(h(n_{FA}) - 1)$ with the number n_{FA} he selected and compares if $h(h(n_{FA}) - 1)$ equals m_5 . If equal, Mu is authenticated by FA. Then FA computes the session key $SK = h(h(n_{FA}) \| h(ID_{mu} \| ID_{FA} \| n_{mu}))$ to be used to communicate with Mu. The authentication proceess ends.

3.4 Refreshment of Session key

When Mu wants to communicate with FA frequently, the session key needs to update periodically. FA sends a temporary certificate $(TCert_u)_{SK}$ that includes life time and other informations to Mu. If Mu wants to visit FA in i-th time, Mu sends $\{TCert_u, (n_i \| TCert_u)_{SK_i}\}$ to FA. The i-th sessinon key $SK_i = h(n_{i-1} \| h(ID_{mu} \| ID_{FA} \| n_{mu})), i = 1, 2, ..., n$ ($n_0 = h(n_{FA})$). FA checks the validity of the certificate , decrypts $(n_i \| TCert_u)_{SK_i}$ with SK_i and compares if $TCert_u$ equals the certificate decrypted. If it holds, FA saves n_i as the next communication . The session key refreshment ends.

3.5 Refreshment of password

Mu inserts the smart card into the terminal to verify the legitimacy of the identity Mu. If it holds , Mu selects a new password pw' and a new random number b' and computes $V_{uH}^* = TH_u \oplus h(ID_{mu}) \| h(pw' \| b'))$, $TH_u^* = V_{uH}^* \oplus h(ID_{mu} \| h(pw' \| b'))$, $H_{uH}^* = h(TH_u^*) \oplus h(ID_{mu} \oplus b')$. The smart card information is $\{V_{uH}^*, H_{uH}^*, SK_{uH}^*, h(.), n, b'\}$ and the refreshment of password ends.

4 Security and performance analysis

4.1 Security Analysis

In Our scheme, the anonymity of Mu is obtained by hash function and Exclusive-OR operation. Assume that an attacker has extracted the information stored in Mu's smart card and the used meaages tranmitted among Mu,FA and HA. However, the attacker can not derive the real identity of Mu without knowing the value of (p, q) and the random number n_{mu} .

In our scheme, the information of the smart card is is $\{V_{uH}, H_{uH}, SK_{uH}', h(.), n, b\}$ .When the user's smart card is stolen or losses ,an attacker can guess the user's identity and password to compute SK_{uH}'' and TH_u^* . In order to verify the correctness of SK_{uH}'' and TH_u^* , the attacker must derive the information from { m_1 , m_2, m_3, m_4 , m_5 } , but the malicious attacker does not know the value of (p, q). According to the residual knowledge of modular square, it is not possible to get the message m_1 , n_{mu} , ID_{mu} , TH_u in a polynomial time. So SK_{uH}'' and TH_u^* can not be derived from the information { m_1 , m_2, m_3, m_4 , m_5 } . Our scheme can resist offline password guessing attack

Our scheme also can resist a foreign agent attack. When A malicious foreign agent such as FA_{j+1} replays the used message m_1 to a legitimate foreign agent such as FA_j , in this case, FA_{j+1} will get the message $m_4 = \{K_2, K_3\}$, but he does not know the news $h(ID_{mu} \| ID_{FA} \| n_{mu})$ and can't get $h(n_{FA})$, so he can not send a response message $m_5 = h(h(n_{FA}) - 1)$. Malicious agents can not mimic legitimate agent identity to deceive mobile users because malicious agents do not know the key SK_{HF} and the random number n_{FA} .He can not generate messages m_4 to the user, the attack failed.

Our scheme also can resist forgery attack. Supposing that malicious attackers forgery into a mobile user or home agent to try to attack. They don't know { TH_u , ID_{mu} }, malicious attackers can not finish the legitimate user authentication through the home agent. They do not know the key (p, q), malicious attackers can not impersonate the home agent to decrypt the message m_1 and perform the authentication through mobile users and foreign agent.

The proposed protocol also can resist known-session key attack , internal attack and replay attack. This scheme also has the characteristics of forward secrecy and so on , which enhance the performance of the protocol.

4.2 Performance Analysis

Our proposed protocol contains only five news exchange in terms of communication load and does not need clock synchronization mechanism, which reduces the consumption of clock synchronization and the timestamp setting. In terms of computational complexity, our protocol uses hash function and Exclusive-OR operation because of the wireless environment restrictions on energy and computing power. The proposed protocol performs not more than 2 msec in OpenSSL running time. Compared with other relevant protocols , our protocol is more simple and efficient.

5 Conclusions

In this paper, we propose an efficient authentication protocol for GSM networks and analyze the security and performance of the protocol. The results show that the protocol is secure and robust.

Acknowledgement

The work is supported by Scientific and technological projects for Central colleges and universities. (No. 31920150079).

References

1. 1.L .Leslie, Comm.ACM **24**, 770 (1981).
2. J.Zhu , J.Ma, IEEE.Tran.C.E **50**,230(2004).
3. C.C.Lee,M.S.Hwang ,I.E.Liao, IEEE. Tran.C.E **53**, 1683(2006).
4. C. C. Wu, W.B.Lee , W. J. Tsaur, IEEE. Com.L **12** , 22(2008).
5. J. S.Lee, D. H. Lee, IEEE.Com. L **13**, 292(2009).
6. P. Zeng,Z.Cao,K.K.R.Choo, S.Wang, IEEE.Com.L **13**,70(2009).
7. C.C.Chang,C.Y.Lee ,Y. C. Chiu,Com.Stan.I **32**,611(2009).
8. J.Y.Liu, *Applied cryptography*(2008).