A New Secure Authentication Mechanism for SIP Using Chaos–based Cryptography

Zhuo Chen[1,a], Jiaoyan Liang[2,b] and Chao Wang[3,c]

[1]School of Computer, Hubei University of Technology, Wuhan, China

[2]School of Computer, Hubei University of Technology, Wuhan, China

[3]School of Computer, Hubei University of Technology, Wuhan, China

[a]Chenzhuo_hust@163.com, [b]imsmallwhite@163.com, [c]carlwangyy@sina.com

Keywords: SIP, secure authentication, chaos password, session.

Abstract. SIP (Session Initiation Protocol) application is used in the field of multimedia communications more and more widely as the core signaling control protocol in NGN (Next Generation Network). The current authentication mechanism in SIP is a digest authentication mechanism based on HTTP, which is vulnerable to off-line password guessing attack, server spoofing attack, etc. In order to overcome the above disadvantages, this paper proposes a new mutual authentication, which is based on the chaotic theory. The chaotic sequence's characteristics of randomness and ergodicity can not only generate nonce for the digest authentication, but also provide a key for the session. Moreover, we should expand some header fields of SIP to meet the needs of the new authentication mechanism.

Introduction

SIP (Session Initiation Protocol) [1] is a signaling control protocol based on the application layer, which is used to create, modify, and terminate multimedia user sessions. SIP has broken the traditional basic model of telecommunication services, its syntax and semantics owes much to the HTTP protocol and SMTP protocol. Making full use of its header field, SIP has higher functionality and business growth potential. However, as SIP messages are text-based, it has two disadvantages: unilateral authentication and the lack of key negotiation. To solve these disadvantages, this paper proposes an improved one-time password method based on the chaotic sequence. It can effectively avoid off-line password guessing attack[2], server spoofing attack and so on.

Security Mechanisms in SIP

Related Work. SIP authentication schemes mainly include mutual HTTP digest authentication mechanisms and PKI authentication mechanisms [3]. Among the articles which have been proposed, there is a paper which demands the client and Registrar Server generate public keys and the corresponding private keys previously. Furthermore, a new reliable authentication method has been proposed which takes advantage of the Guillou-Quisquater algorithm [4].This method has the need to verify the timestamp in order to ensure the time uniform. After analyzing the results of the above studies, we propose a new secure authentication mechanism based on the chaotic sequence [5].

The Authentication Procedure in SIP. The authentication which SIP recommends is derived from HTTP digest authentication, which adopts an authentication scheme called Challenge/Response [6]. The concrete procedure is depicted as Fig. 1. Certification steps are described as follows:

Step1: SIP UA (User Agent) sends Register to Registrar Server or Proxy Server.

Step2: The Registrar/Proxy Server sends a response of challenge to the SIP UA. If it is a Registrar Server, it returns 401 Unauthorized, else it returns 407 Unauthorized. The information such as nonce, realm (a protected area, which contains the Server's domain name) and digest algorithm (MD5) is stored in WWW-Authenticate (a header field).

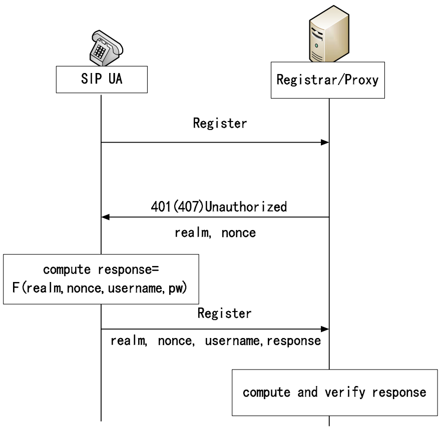

Fig. 1 Authentication procedure in SIP

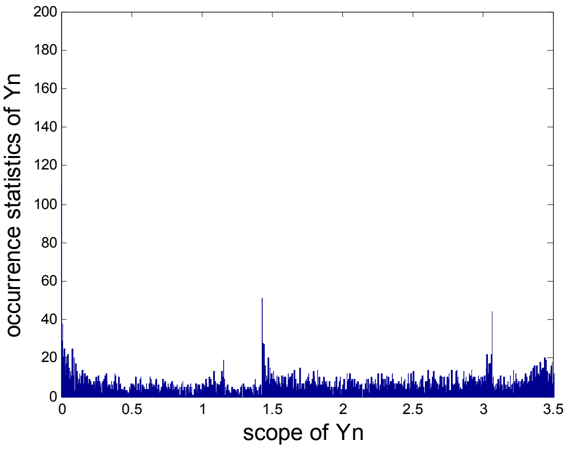

Fig. 2 Chaotic sequence obey uniform distributing

Step3: When the UA receives the 401 or 407 Unauthorized, it firstly obtains the nonce and realm from the response. Then the UA uses its password, username, realm, together with the nonce to calculate a response value. At last the UA sends the request again, including the response value, which is used by the Server to authenticate the UA.

Step4: Registrar/Proxy Server computes F (realm, nonce, username, pw), and then compares the result with the response value which comes from the UA. If they are equal, the Server returns a response of 200 OK (successfully registered); else it returns a response of 403 Forbidden (failed registered).

A New Authentication Mechanism for SIP

Chaos-based Cryptography. Chaotic theory began to get the great attention of modern cryptography in the late 1980s.A Pseudo-random generator can be put forward by using the trace of chaotic motion. The generated Pseudo-random number is called chaotic sequence. Chaotic sequence has the following special features: randomness, certainty, sensitivity to initial conditions and uniform distribution overall which are suitable as encryption password. The chaotic sequence which the paper uses is based on discrete chaotic system model. The equation can be written as follows:

$$Y_{n+1} = A * \sin^2(Y_n - Y_b), \mathrm{n} = 1, 2, \cdots \tag{1}$$

Where A and Y_b are the parameters of the equation. With the changes of A and Y_b ,the system will enter a chaotic state. The following Fig. 2 shows the result, where the iteration is 10000, A=4, Y_1 =1.222222, Y_b =2.5. With this figure, we can find out that it distributes evenly when $Y_n \in (0.5, 3)$, thus the chaotic sequence generated by Eq. 1 is suited as encrypt-password.

A New Authentication Mechanism for SIP. In order to achieve mutual authentication, the initial value and the chaotic equation of UA are stored in the user client and the Server respectively. The iterative sequence generated by the client is marked as $\{X_n\}$, and the iterative sequence generated by the Server is marked as $\{Y_n\}$.Actually， $\{X_n\}$ and $\{Y_n\}$ are two identical chaotic sequences. The concrete procedure is depicted as Fig. 3.Certification steps are described as follows [7]

Step1: SIP UA inputs static password to run the client program, then sends the request of Register or Invite.

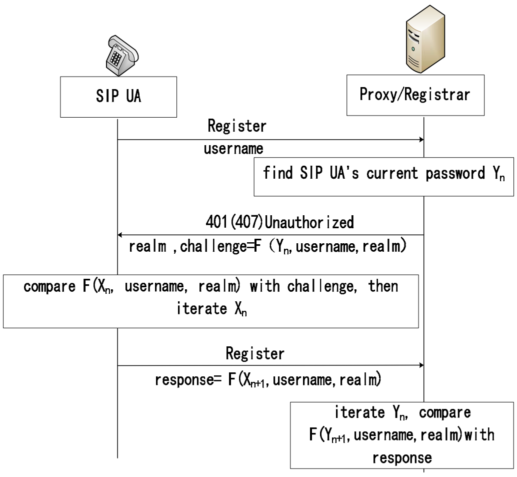
SIP UA
Proxy/Registrar
Register
username
find SIP UA's current password Y_n
401(407)Unauthorized
realm ,challenge=F (Y$_n$, username, realm)
compare F(X$_n$, username, realm) with challenge, then iterate X$_n$
Register
response= F(X$_{n+1}$, username, realm)
iterate Y$_n$, compare F(Y$_{n+1}$, username, realm)with response

Fig. 3 Chaos-based authentication in SIP

Step2: Registrar Server would check whether its username is in the database once receiving the request from SIP UA .And then the Server obtains the UA's current password Y_n stored in the database if the UA is legal. Finally, compute challenge=F (Y_n , username, realm）. At last, the Server transmit the challenge and realm by the WWW-Authenticate in 401/407 Unauthorized.

Step3: After receiving the 401/407 response, SIP UA should firstly compute F (X_n , username, realm) and compare it with challenge'. The Registrar Server is considered legitimate if they are equal. Iterating X_{n+1} , we can get X_{n+1} . Secondly, compute response = F （ X_{n+1} , username, realm）. At last, the UA transmit the response by the Authorization in the request of Register.

Step4: After iterating the current password Y_n , the Registrar Server would compare F (Y_{n+1} , username, and realm) with response'. The SIP UA is considered legitimate if they are equal. Compared with the formerly proposed schemes, chaos-based cryptography has these characters:

As chaotic sequence which stored in the client program was generated in advance, the cryptography can save the authorization time and increase efficiency of the session.

The Extension of Header Fields in SIP

Extension of Digest Authentication. We should add a UAC-Authenticate header which is similar to WWW-Authenticate but has no realm and nonce. The BNF paradigm of WWW-Authenticate can be expressed as follows:

UAC-Authenticate = " UAC-Authenticate " " : " UAC-Authenticate
UAC-Authenticate =1# (Digest algorithm| [realm])
Digest algorithm = " Algorithm " " = " < " >1#algorithm-value< " >
Algorithm-value = " MD5 " | " SHA-1 " |token

The Digest algorithm of UAC-Authenticate, which is given by the user client, indicates the digest algorithm that is supported by the user client.

Extension of Secure Session. We do not have to add header fields but insert two additional attributes into the Message Body. H(M) is stored in the added Digest message and symmetric encryption algorithm (AES or DES) is stored in the new Encryption algorithm. Furthermore, encrypted message E_{ka}(M) is stored in the existing Line-based text data. The BNF paradigm of Message Body can be written as follows:

Message Body = " Message Body " " : " Message Body
Message Body =1# (Line-based text data| Digest-message| Encryption algorithm)
Line-based text data = " Line-based text data " " : " encrypted message
encrypted message = quoted-string

Digest-Message = " Digest-Message " " : " encrypted value
encrypted value = quoted-string
Encryption algorithm= " Encryption algorithm "   " = " < " >1# Encryption algorithm-value< " >
Encryption algorithm -value = " DES " | " AES " |token

Conclusion

SIP can be easily imitated, tampered, and even illegally used by attacker. Especially in the digest authentication process, the current authentication mechanism is vulnerable to the server spoofing attack. At the same time, the important message body cannot be encrypted in the session. To overcome the above disadvantages, the paper proposed a new authentication mechanism, which is based on the chaotic theory. Moreover, the improved method would effectively ensure the reliability of the authentication and the integrity of the session.

Acknowledgments

This work was financially supported by the National Natural Science Foundation of China (grant Nos.61370224) and Natural Science Foundation of Hubei Province of China(2014CFB484)

References

[1] J. Rosenberg, SIP: Session Initiation Protocol, IETF RFC 3261, (2002).

[2] J. L. Tsai, “Efficient nonce-based authentication scheme for session initiation protocol”, International Journal of Network Security, vol.9, no.1, pp.12-16,(July 2009).

[3]H.H.KILINC,Y.ALLABERDIYEV,T.YANIK,andS.S.ERDEM,“Efficient ID based authentication and key agreement protocols for the session initiation protocol”, unpublished.

[4] Q.Chen, “The study of authentication and encryption mechanism of VoIP based on SIP”, Shanghai: Shanghai Jiao Tong University, (2007).

[5] F.C.Zhou, K.N.Gao, G.H. Cao, and G.Y. Zhang. “Identity authentication mechanism based on chaotic theory and its security analysis”, MINI-MICRO SYSTEMS, vol.24, no.12, pp.2088-2091, (2003).

[6] Y. P. Liao and S. S. Wang, “A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves”, Computer Communications, vol.33, pp.372-380, (2010).

[7]X.H. Gu, J.J. Shi, F. Guo. “Security mechanism of SIP and improvement of HTTP digest authentication”,JOURNAL OF DONGHUA UNIVERSITY (NATURAL SCIENCE), vol.36 ,no.2,pp.165-169,(2010).