Two Step Mutual Authentication Scheme for SIP

Mohit Kumar Gokhroo and Jaidhar C. D.

***Abstract*-Voice over Internet Protocol (VoIP) uses Internet Protocol (IP) to transmit voice as packets over an IP network. It achieves desired functionality of Internet telephony using a signaling protocol known as Session Initiation Protocol (SIP). When users need to use SIP service, first server authenticates the user in order to provide the service. In this paper, a new and secure authentication scheme for SIP is proposed. Its major merits are 1) Provides mutual authentication. 2) Generates session key agreed between user and server in two steps. 3) Secure against various possible attacks induced by IP networks.**

***Index Terms*—Attacks, authentication, denial-of-service attack, mutual authentication, perfect forward secrecy, session initiation protocol, session key, voice over internet protocol.**

I. Introduction

Session Initiation Protocol (SIP) is a signaling protocol operating at application layer to initiate, maintain and terminates multimedia sessions across packet networks. Internet Engineering Task Force (IETF) proposed SIP as a signaling protocol for Internet Protocol (IP) based telephony. SIP is designed to be independent of underlying transport layer. It can operate on Transmission Control Protocol (TCP) as well as User Datagram Protocol (UDP) to handles all signaling requirements of Voice over Internet Protocol (VoIP) sessions. Today it is widely used to transmit voice and video over IP.

Issue of security has become extremely important in today's computer networks environment. Two fundamental security services required by SIP are confidentiality and authentication. Whenever user wants to access SIP service from server, mutual authentication is required between two parties. An attacker can obtain user's secret information by forging the identity of server if mutual authentication is not performed. Confidentiality is usually provided by means of encryption. Only intended recipient can decrypt a message and obtain a tangible meaning out of it. Encryption/Decryption uses shared secrets agreed among the communicating entities. If it is different from session to each session, it is known as session key. Identifying caller and callee is an utmost important issue in SIP based application. To guarantee and enhance security features, several authentication schemes have been proposed [1]-[8].

Rest of the paper is organized as follows. Section II presents an overview of previous work. Section III describes the proposed SIP authentication scheme. Section IV discusses security analysis of proposed scheme. Section V presents a comparative analysis of security features and computational costs incurred in proposed scheme with previous schemes. Finally, section VI concludes the paper.

Manuscript received December 28, 2012; revised July 5, 2013.

Jaidhar C. D. is with the Defence Institute of Advanced Technology, Pune-25, gokhroo@gmail.com, jaidharcd@diat.ac.in

II. Previous Work

The SIP Authentication scheme based on HTTP digest has been proposed [1]. It uses challenge and response message to recognize the communicating parties. However, it is vulnerable to offline password guessing attack and server spoofing attack. To overcome these weaknesses, a scheme based on Diffie-Hellman key exchange has been proposed [2]. It maintains preconfigured password used to verify the identity of user or server. Further, security depends on Discrete Logarithmic Problem (DLP) which involves exponential computation. However, it is not suitable for user devices have low computation power and computing capability like smart card and mobile. In addition, computation time to generate a key is large which does not meet the requirements of real time implementations of SIP as a protocol for communication. To meet all these challenges, Elliptic Curve Cryptography (ECC) with key size around 160 bits is an alternative solution because of its security, based on Elliptic Curve Discrete Logarithm problem (ECDL) and operates on group of points on elliptic curve. Moreover, it is faster in computations and provides same security as compared to RSA 1024 bit key [3], [4].

Three way handshake nonce based SIP authentication scheme has been proposed [5]. It uses only one-way hash function and exclusive-or operation for all messages exchanged between communicating entities. Computation cost of this scheme is less. Hence, it is suitable for user devices have low computation power equipment. However, it is vulnerable to offline password guessing attack, Denning Sacco attack, stolen verifier attack and does not provide perfect forward secrecy and modified scheme using ECC proposed to overcome these attacks [6]. It is claimed that scheme has improved capabilities in terms of speed, memory size, computation time and increased security. Different from the above mentioned work, authentication and key agreement scheme for SIP using certificate less public key cryptography has been proposed [7].

Authentication scheme [3] has been proven vulnerable to Denning sacco attack and Stolen verifier attack and modified scheme also has been proposed in order to resist these weakness in [8]. Authentication scheme proposed by Yang and Huang for Session Initiation Protocol [9], [10] has been proved vulnerable to offline password guessing attack [11]. Scheme for SIP using ECC proposed by Wu [12] is also vulnerable to offline password guessing attack.

David Butcher [13] discusses various security features to be considered while designing new authentication schemes

DOI: 10.7763/IJCCE.2013.V2.271

like Denial of Service, Eavesdropping, Alteration of Voice Stream, Toll Fraud, Redirection of Call, Accounting Data Manipulation, Caller ID Impersonation, unwanted Call and Messages. Prominent attacks on SIP include Registration Hijacking, Message Modification, Cancel/Bye Attack, Malformed Command, and Redirection of calls.

This paper proposes a secure mutual authentication scheme for SIP. Security of the scheme depends on Discrete Logarithmic Problem (DLP) which involves exponential computations. It generates session key agreed between user and server in two steps. Thus number of messages exchanged reduces, consequently time needed to establish session is reduced.

III. Proposed SIP Authentication Scheme

This section describes a proposed SIP authentication scheme. Notations used in this paper are described in Table I for convenience of description.

TABLE I: Notations Used in this Paper

Notation	Description
U	User Agent Client (UAC)
S	SIP Server
ID	User Identifier
$h(.)$	Secure one-way hash function
PW	User password
h(PW)	Hash of password
SK	Session Key shared between U and S
r_c	Random integer chosen by user
r_s	Random integer chosen at server
$U \rightarrow S$	U sends a message "M" to S
X_s	Secret Key of Server
$\oplus$	Bit-wise exclusive-or (XOR) operation

There are three phases in this scheme namely

1) Initial System setup Phase
2) Registration phase
3) Authentication phase

Fig. 1 illustrates steps to generate session key agreed between user and server. S stores secrets for each user i.e. ID and $V = h$ (PW) $\oplus$ h(ID, X_s) in its verfication table.

B. System Setup Phase

In this phase, necessary operations for functioning of scheme are performed. Primary values selected at user end are username 'ID', generator 'g', publicly known large prime number for modulus operations 'n', and password 'PW' with its hash 'h(PW)'

C. Registration Phase

When a user U wants to become a new authorized user at S, following step is executed over a secure channel. $U \rightarrow S$ (ID, h (PW)

User U sends a registration request message over a secure channel containing parameters (ID, h (PW)) Upon receiving a request, S computes $V=h$ (PW) $\oplus$ h(ID, X_s) where X_s is a secret key of the server and stores ID, V in server's verification table as corresponding entries of a user.

D. Login and Authentication Phase

User generates a random number r_c. Further it computes M_c and N_c as $M_c = r_c^{h(PW)} \bmod n$ and $N_c = (r_c \times g^{ID}) \bmod n$ to creates login request as shown in Fig. 1

$U \rightarrow S$ REQUEST (ID, N_c, H_c) and sends it to S, where hash value $H_c = h$ (h (PW), M_c) is computed to verify the mutual authenticity among user and server using parameters M_c and h(PW) as shown in Fig. 1.

Upon receiving login request from U, S uses ID from login message and retrieves h (PW) from the its verification table by performing h (PW) $= V \oplus h$ (ID, X_s). Server then computes M_c by performing the following steps.

$$\text{Compute } g^{ID * h(PW)} \bmod n \quad (1)$$
$$\text{Compute } (N_c)^{h(PW)} \bmod n \quad (2)$$

Divide (2)/ (1) to obtain M_c as=$[((r_c^{h(PW)} \bmod n) \times (g^{ID \times h(PW)} \bmod n))/g^{ID \times h(PW)} \bmod n]$

$$= (r_c^{h(PW)} \bmod n)$$
$$= M_c.$$

Server S computes (h (h (PW), M_c)) and verifies it with H_c received in login request to establish authenticity of user. If h ((h(PW), M_c)) = H_c then server S sends a response message else discards login request thus ensuring no attacker is in middle.

Server S sends RESPONSE containing parameters M_s, N_s and H_s back to user enabling session key computation at user end.

$S \rightarrow U$ Response (ID, N_s, H_s)).

where $M_s = r_s^{h(PW)} \bmod n$, $N_s = (r_s \times g^{ID}) \bmod n$, $H_s = h(M_s, h(PW))$

Server computes session key as SK $= M_c \oplus M_s$ SK= $r_c^{h(PW)} \bmod n \oplus r_s^{h(PW)} \bmod n$

Upon receiving response message, U derives M_s by performing the following steps

$$\text{Compute } g^{ID \times h(PW)} \bmod n \quad (3)$$
$$\text{Compute } (N_s)^{h(PW)} \bmod n \quad (4)$$

Divide (4)/(3) to obtain M_s as = $[((r_s^{h(PW)} \bmod n) \times (g^{ID \times h(PW)} \bmod n))/ g^{ID \times h(PW)} \bmod n] = (r_s^{h(PW)} \bmod n) = M_s$

User U Computes h (h (PW), M_s and compares it with H_s i.e., (Ms, h(h(PW))= H_s to verify whether sever S is legitimate or not thereby authenticating the server. If both are equal then user computes session key as

SK = $M_c \oplus M_s$ i.e.

SK= $r_c^{h(PW)} \bmod n \oplus r_s^{h(PW)} \bmod n$ and use it to secure the communication else reject the response.

IV. Security Analysis of Proposed Authentication Scheme

In this section, security of proposed SIP authentication scheme with its security features is examined. It resists following possible attacks and provides the essential security. It uses two way handshakes to offer mutual authentication which is highly efficient with respect to systems that demands quick session establishment between two parties for real time implementation of SIP protocol in today's network communications.

A. Stolen Verifier Attack

User's secret information's stored at server are under

extensive threats from attackers. They try to steal user secrets and other useful information. Security of the systems is at stake if an adversary uses *them* maliciously to breakdown the system. In our scheme, server maintains a verification table to store values in encrypted form which are needed to verify user's during logging request. User's password PW is not stored in plaintext format its hash value is embedded in parameter '*V*' calculated using server secret key X_s Even if an attacker captures verification table entries still password of user PW cannot be derived out of it. Hence, the scheme is secure against stolen verifier attack

B. Online and Offline Password Guessing Attacks

In the proposed scheme, parameters of the Request and Response message are Request (ID, N_c, H_c) Response (ID, N_s, H_s)

Let us assume adversary intercepts both Request and Response messages exchanged *between* user and server to create forged login request. Neither of them provide any useful information about values of *h* (PW), r_c and r_s. Computed parameters $M_c = r_c^{h(\mathrm{PW})} \bmod n$ and $M_s = r_s^{h(\mathrm{PW})} \bmod n$ contains h(PW) but the parameter in login message N_c or N_s does not use any *h* (PW) . Even if adversary correctly guesses r_c^* or r_s^* still value of *h* (PW) is needed to modify *hash* and get verified at server and vice-versa. Therefore only legitimate users can use it for authentication purpose. Hence this scheme is secure against online and offline password guessing attack.

C. Forgery Attack (Impersonation Attack)

As *h* (PW) is known only to user and stored in server verification table. Attacker is unable to retrieve *h* (PW) from eavesdropped response message as parameter N_c and N_s does not contain *h* (PW). Let's assume attacker guesses the password PW* and computes *h* (PW*). Still it is not possible to derive the half session key without knowing value of 'r_c' or 'r_s' due to the property of Discrete Logarithm. Moreover it is difficult to guess the correct values of *h* (PW), r_c and r_s simultaneously to get authenticated as a legitimate user. Hence, attacker is unable to create a forged login request.

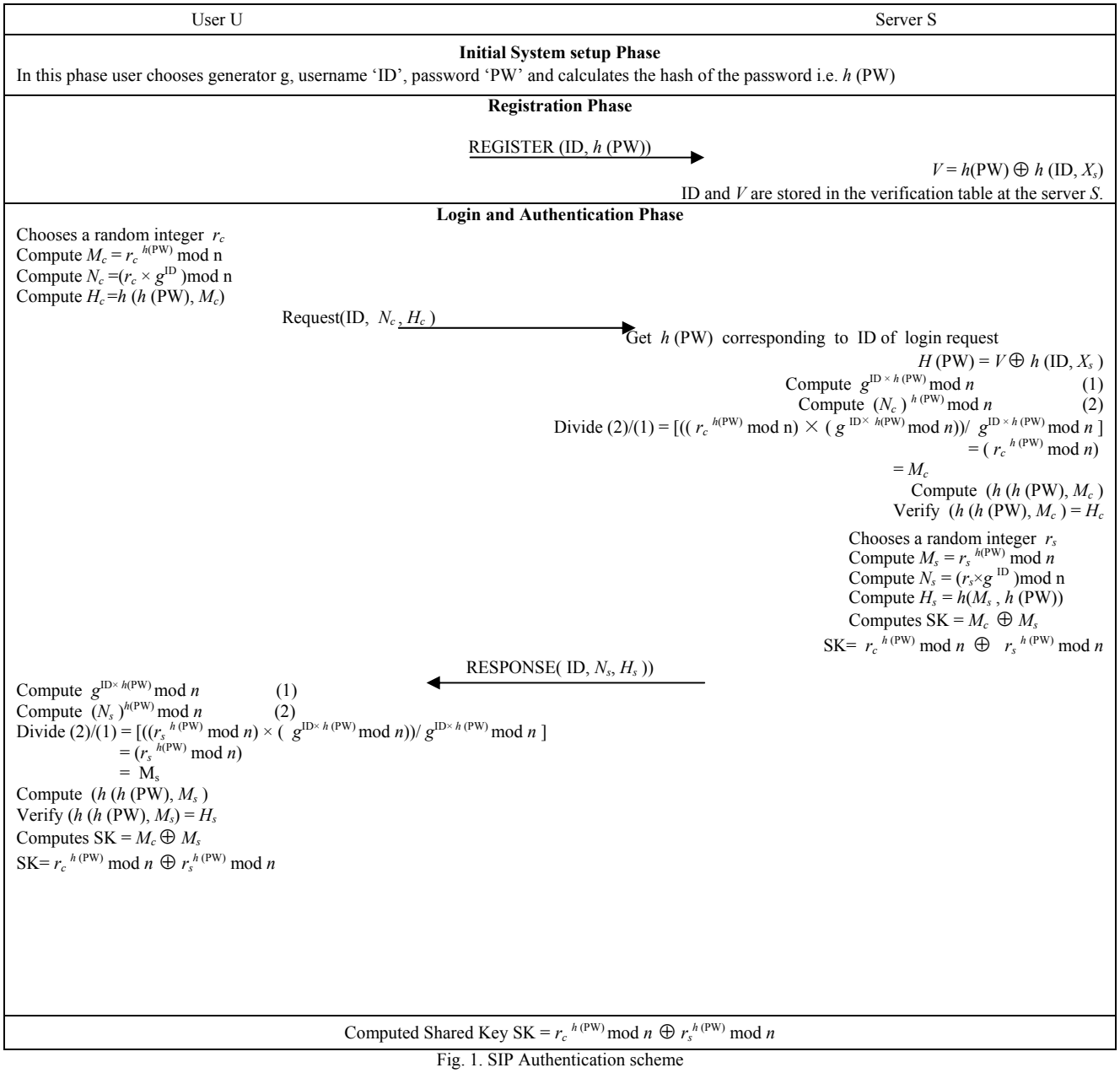

Fig. 1. SIP Authentication scheme

TABLE I: A COMPARISON OF SECURITY FEATURES OF SCHEMES.

Attacks in Schemes	Yangs	Durlanik	Wu	Yoon	Proposed Scheme
Replay Attack	Secure	Secure	Secure	insecure	Secure
Password guessing	Secure	Secure	Insecure	Secure	Secure
Man in Middle Attack	Secure	Secure	Secure	Secure	Secure
Modification Attack	Secure	Secure	Secure	insecure	Secure
Denning-Sacco attack	N/A	Insecure	Secure	Secure	Secure
Stolen-verifier Attack	Insecure	Insecure	Insecure	Secure	Secure
Mutual Authentication	Provided	Provided	Provided	Provided	Provided
Known-key security	N/A	Provided	Provided	Provided	Provided
Session-key security	N/A	Provided	Provided	Provided	Provided
Perfect forward secrecy	Secure	Provided	Provided	Provided	Provided

TABLE II: A COMPARISON OF COMPUTATIONAL COSTS OF SCHEMES

Property Schemes	Yangs	Durlanik	Wu	Yoon's	Proposed scheme
#of exponentiations	4	0	0	0	8
# of ECC compuations	0	4	4	4	0
# of hash functions	8	8	6	5	5
# of exclusive OR operations	4	4	4	3	2
# of rounds	3	3	4	3	2
Security	DLP	ECDLP	ECDLP	ECDLP	DLP

D. Replay Attack

This scheme uses random numbers as 'r_c' and 'r_s' which are different for each session. As password is known only to user, attacker cannot create a forged login request. Moreover, attacker cannot use previously intercepted or eavesdropped messages due to the fact that values of 'r_c' and 'r_s' are different from session to session.

Assume that the intercepted login request is replayed, Request (ID, N_c, H_c)

Attacker is unable to retrieve $r_s^{h(PW)} \bmod n$ correctly from the response message without knowing correct value of h (PW) therefore the session key is not generated at user end.

E. Man-in-the-Middle Attack

Let us assume an attacker intercepts both request and response messages communicated between user and server. Still he is unable to extract any tangible information from eavesdropped request and response messages. This is due to random values of r_c and r_s leading to different values of request and response messages for each session. Moreover, to alter request and challenge message, the correct value of h (PW) is required. Attacker cannot pretend to be U or S to authenticate each other since h (PW) and 'r_c' or 'r_s' are unknown. Hence, the proposed scheme is secure against man-in-the-middle attack.

F. Insider Attack

In this scheme h (PW) is sent to S instead of PW during the registration phase. So any insider of S cannot get user password PW. Hence, scheme withstands insider attack.

G. Attack on Perfect Forward Secrecy

In this scheme, the session key SK = $M_c \oplus M_s$ SK= $r_c^{h(PW)} \bmod n \oplus r_s^{h(PW)} \bmod n$ is computed using randomly generated r_c and r_s (different for each session) which are not a part of any of the previously transmitted messages between U and S. Even if an attacker gets server's secret key X_s, there is no way to derive present or previous session key/s. Hence scheme provides perfect forward secrecy.

H. Denning-Sacco Attack

If an attacker captures a session key still there is no way to derive any information about r_c, r_s or server's secret key X_s. As h (PW) and r_c, r_s are not used directly to compute session key, user's password cannot be derived from the eavesdropped session key.

I. Solves time Synchronization Problem

Proposed scheme uses randomly generated values instead of time-stamps to avoid time synchronization problem.

V. PERFORMANCE COMPARISON

Table I and Table II shows comparative study of previous schemes with the proposed scheme. Our scheme shows an improvement in performance. It performs mutual authentication and session key generation efficiently in less number of operations as compared to previous schemes. Further, it also prevents above mentioned attacks as well. As a significant advantage, it reduces number of rounds for mutual authentication among U and S from three to two. This improvement significantly reduces time to establish the sessions. Thus ensuring as an effective technique for session key generation in SIP and fast growth of VoIP technologies.

VI. CONCLUSION

The security of proposed SIP authentication scheme is examined and found to be secure against known attacks.

Moreover, an attacker can't easily compute session key by using intercepted messages. It is clearly evident from tables I and II that our scheme scores better than the existing schemes. It is also efficient as it uses only two messages between user and server to provide mutual authentication. In today's network environment two way handshake for mutual authentication is very efficient for systems that demands quick session key generation for establishment of session.

REFERENCES

[1] J. Franks, "HTTP Authentication basic and digest access authentication," *IETF RFC2617*, June 1999.

[2] C. C. Yang, R. C. Wang, and W. T. Liu, "Secure authentication scheme for session initiation protocol, "*Computers & Security*, vol. 24, pp. 381-386, 2005.

[3] A. Durlanik and I. Sogukpinar, "SIP authentication scheme using ECDH," World *Academy of Sciece and Technology*, vol. 8, 2005.

[4] 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.

[5] J. L. Tsai, "Effcient nonce-based authentication scheme for session initiation protocol," *International Journal of Network Security*, vol. 9, no. 1, pp. 12–16, July 2009.

[6] E. J. Yoon and K. Y. Yoo, "A new efficient authentication scheme for session initiation protocol," *International Conference on Complex, Inellligent and Software Intensive Systems*, pp. 549-553, 2009.

[7] F. Wang and Y. Zhang, "A new provable secure authentication and key agreement mechanism for SIP using certificate less public key cryptography," *Computer Communications*, vol. 31, pp. 2142-2149, 2008.

[8] E. J. Yoon, K. Y. Yoo, C. Kim, Y. S. Hong, M. Jo, and H. H. Chen, "A secure and efficient SIP authentication scheme for converged VoIP networks," *Computer Communications*, vol. 33, pp. 1674–1681, 2010.

[9] C. C.Yang, R. C. Wang, and W. T. Liu., "Secure authentication scheme for session initiation protocol," *Computers and Security*, vol.1, pp. 74-76, 2005.

[10] H. F. Huang, W. C. Wei, and G. E. Brown, "A new efficient authentication scheme for session initiation protocol," in *Proc. of 9th Joint Conference on Information Sciences*, 2006.

[11] H. Jo, Y. Lee, M. Kim, S. Kim, and D. Won, "Off-line password-guessing attack to yang's and huang's authentication schemes for session initiation protocol," in *Proc. of Fifth International Joint Conference on INC*, pp. 618–621, 2009.

[12] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 286–291, 2009.

[13] D. Butcher, X. Li, and J. Guo, Members IEEE, "Security challenge and defense in VoIP infrastructures," *IEEE Transactions on Systems, Man, and Cybernetics part C: Applications and Reviews*, vol. 37, no. 6, pp. 1152-1162, November 2007.

Mohit Kumar Gokhroo received his B. E. (Hons.) in computer science and engineering from University of Rajasthan, Jaipur in 2008. He has completed M. Tech in advanced networks from Atal Bihari Vajpayee-Indian Institute of Information Technology and Management, Gwalior, India in 2011. His area of interest includes Computer Networks, Information Security and Authentication schemes. He has two years of work experience in IT industry.

Jaidhar C. D. is currently working as an assistant professor in the Department of Computer Engineering, Defense Institute of Advanced Technology, Pune, India. His research interest includes Computer Networks, Information Security, Network Security, Intrusion Detection, Security issues in Cloud Computing and Cryptography.