A new SIP authentication scheme by incorporation of elliptic curve cryptography with ticket server

[1]Farnad Ahangari , [2]Mahsa Hosseinpour Moghaddam, [3]Seyyed Amin Hosseini Seno
Department of Computer Engineering
Ferdowsi University of Mashhad (FUM)
Mashhad, Iran
[1]ahangary@um.ac.ir, [2]mahsa.hosseinpour@stu.um.ac.ir, [3]hosseini@um.ac.ir

Abstract— **Today, Session Initiation Protocol (SIP) is considered as predominant protocol for Voice over IP (VoIP) systems. When the client require to use SIP services, as a demand of accessing proxy server, authentication will be important challenge. SIP protocol presents SIP request authentication through a challenge-response scheme named HTTP Digest Authentication which is inherited from HTTP protocol, but this authentication protocol is vulnerable to different kind of known attacks. In this paper, it has been tried to make the authentication mechanism stronger and to resolve its weaknesses. In this regard, Elliptic Curve Cryptography (ECC) used along with an auxiliary ticket server, in which the results showed an increase in the authentication mechanism security and made it stronger against different kinds of attacks. Gained analysis results represent that the proposed method provides more security and less computational overhead, in compare with other methods.**

Keywords-Session Initiation Protocol, security, authentication, elliptic curve cryptography, ticket server

I. INTRODUCTION

The VoIP (Voice over Internet Protocol) service is used for the transmission of voice, video and multimedia sessions over IP networks. Flexibility in implementation and low cost caused VoIP products to spread quickly into the enterprise and consumer markets. This trend is reinforced by the transition of PSTN networks into VoIP friendly IP networks. To sustain this quick growth and application versatility, VoIP systems need efficient, flexible and secure transmitting and signaling protocols [1]. The Session Initiation Protocol (SIP) [2] is a text based signaling protocol used in order to establish, modify, and terminate sessions among participants. The IP Multimedia Subsystem (IMS) [3], which is an architectural framework to provide IP multimedia services, has adopted SIP as its signaling protocol due to its flexibility and scalability [1]. Although SIP protocol has significant benefits, but it is subjected to various security threats. SIP authentication typically uses HTTP digest authentication, which is vulnerable to many forms of known attacks [4]. HTTP digest authentication protocol noted in RFC2617 [5] for identity authentication. Several studies have proven that HTTP digest authentication cannot resist off-line password guessing attacks or server spoofing attacks using the HTTP protocol [6]. For this reason to solve such problems in 2005 Yang in his paper [7] proposed a Diffie–Hellman key exchange authentication protocol. In the same year Durlanik and Sogukpinar [8] proposed an Elliptic Curve Diffie–Hellman (ECDH) key exchange authentication protocol to resolve these problems. And later [9, 10] found that Yang's protocol was vulnerable to the replay attack and in [11] showed that Durlanik and Sogukpinar's protocol was vulnerable to the stolen-verifier attack and Denning–Sacco attack. In 2006, a better method provided by Ring et al. [9] in that an Agreement Key (AK) protocol for SIP authentication was proposed which used identity-based cryptography (IBC). Proposed method, calculated user's identity with a hash function as the public key. However, this protocol has been found to be vulnerable to the impersonating attack, and the computation cost is heavy on identity-based signature calculation. To solve these problems, Wang and Zhang [12] proposed a new Secure Authentication and Key Agreement (SAKA) mechanism based on Certificate-Less Public Key Cryptography (CL-PKC). Such a protocol can overcome the impersonating attack issue but it suffers from heavy computation cost. In 2009, Tsai [13] proposed a nonce-based authentication protocol for SIP. However, Lee [14] found that Tsai's protocol still suffered from password guessing attacks and insider attacks. In 2009, Wu et al. [15] proposed a SIP authentication scheme based on Elliptic Curve Cryptography (ECC) and proved that the scheme is secure. Yoon et al.'s [16] SIP authentication scheme is also based on ECC and showed that both schemes [8, 15] are prone to offline dictionary attacks, Denning–Sacco attacks, and stolen verifier attacks. In addition, proposed method in [16] suffers from off-line password guessing attacks. Arshad et al. [17] proposed a new ECC based authentication and key agreement scheme for SIP. Nevertheless He et al. [18], and Pu et al. [19], all demonstrated that Arshad et al.'s scheme is insecure against off-line password guessing attacks. Furthermore, they proposed their own schemes to improve the security of Arshad et al.'s scheme. Recently, smart cards have been widely adopted in remote authentication schemes [6]. Wang et al.'s proposed scheme [20] provided two-variant hashing operations on remote user authentication scheme using smart card. Chen et al. [21] proposed an enhancement of Wang et al.'s scheme suffering from impersonation and parallel session attacks. In 2014, Yeh et al. [6] proposed use of smart card for authentication that encrypted information maintained on it, but this method is not much efficient because the members aren't forced to maintain multiple smart card for multiple VoIP system and also in case of theft smart card, thief would access the information or may copy the card, which in the case of copying the card, impersonating attack could be done easily. Since ECC provides a smaller key size than any other cryptosystem and has faster computations than half of the other public key systems at the same security levels, ECC is suitable to be used for higher security authentication [6]. This paper proposes a method of authentication in the SIP protocol by using ECC and ticket server without need of smart card, in order to obtain higher security with less computation.

The rest of paper organizes as follows:

In section 2, number of related works will be discussed and then in section 3 proposed method is presented. Security and performance analysis of proposed method will be represented in section 4 and in section 5 achieved results will be investigated finally.

II. Related works

In this section, Session Initiation Protocol (SIP), operation of HTTP Digest Authentication protocol and Elliptic Curve Cryptosystem (ECC) are reviewed in short.

A. SIP protocol operation

SIP [2] is a text based protocol with similar formatting to HTTP, capable of operating on TCP or UDP and handles all the signaling requirements of a VoIP session, which is analogous to the SS7 protocol in traditional telephony. The role of SIP is to establish streaming connection between hosts. The network entities involved in SIP are composed of user agent, proxy servers, redirect servers and registrar servers. SIP is based on a HTTP-like request/response transaction model. Each transaction consists of a request that invokes a particular method, or function, on the server and at least one response [4, 22]. Fig. 1 shows a typical SIP message exchange scenario between two users Alice and Bob belonging to the domains proxy A and proxy B, respectively [4].

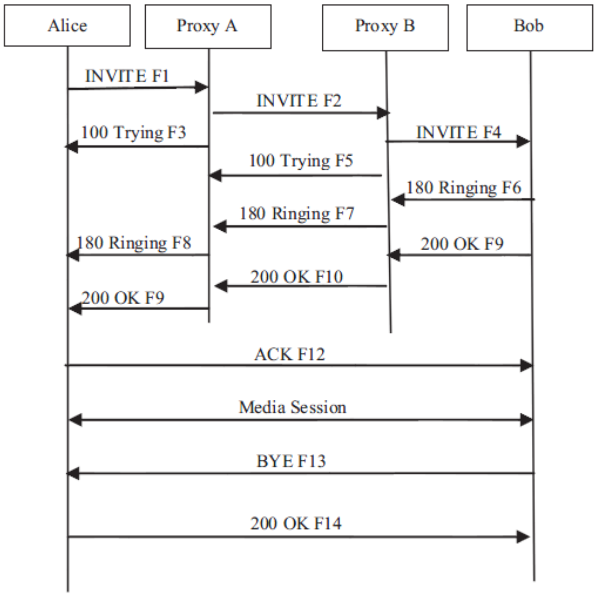

Figure 1. SIP call setup with proxies between two user agents [4]

B. SIP authentication scheme

SIP authentication scheme works similarly to HTTP Digest authentication. Security of this scheme depends on the challenge-response mechanism. The original SIP authentication protocol requires the user and the server pre-sharing a password beforehand. This pre-shared password is used to verify the identity of the user or the server in the authentication procedure [23]. The original procedure performs the following steps as shown in Fig 2.

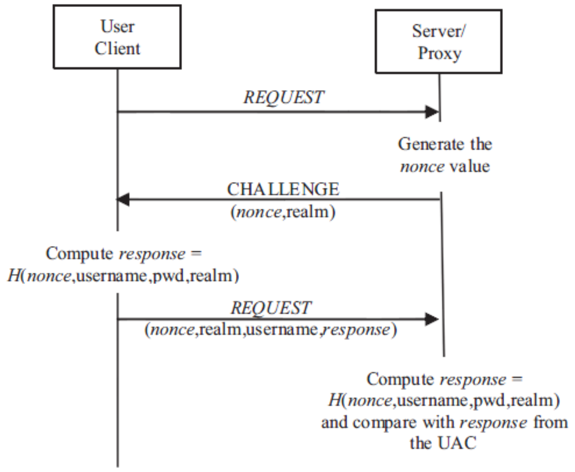
User Client
Server/ Proxy
REQUEST
Generate the nonce value
CHALLENGE
(nonce,realm)
Compute response = H(nonce,username,pwd,realm)
REQUEST
(nonce,realm,username,response)
Compute response = H(nonce,username,pwd,realm) and compare with response from the UAC

Figure 2. SIP Authentication scheme [4]

C. Elliptic curve Cryptography

Victor Miller and Neal Kobiltz proposed a secure and efficient elliptic curve cryptosystem in 1985 [24, 25]. Let $< G_1, +>$ denotes an additive cyclic group of prime order q generated by P. In general, the group G_1 is a subgroup of the additive group of points of an elliptic curve over finite field F_p together with the extra point O living ‘‘at infinity”. We simple define a non-super singular Elliptic curve E over F_p to be an equation of form:

$$E: y^2 = (x^3 + ax + b) mod\ p \neq 0, \qquad (1)$$

with $a, b \in F_p$ satisfying $(4a^3 + 27b) mod\ p \neq 0$, and then we look at the points on E with coordinates in F_p which we denote by:

$$E(F_p) = \{(x, y): x, y \in F_p\ satisfy\ y^2 = x^3 + ax + b\} \cup \{O\}. (2)$$

The curve points on $E(F_p)$ must obey the elliptic curve addition algorithm. In view of shortness, we omit the details and refer to [24, 25].

III. Proposed method

Many techniques have been proposed for SIP authentication which some of them were reviewed in introduction. In yeh et al. paper in 2014 [6], a smart card is used for improving security, but transport of smart card results in decreasing of security itself due to the possibility of card losing or card copying. On one hand, users can’t maintain multiple smart card for multiple SIP system and on the other hand, by card theft, impersonation could be done. In proposed method, by the help of ticket server, there is no need to smart card and more security will be provided. Also, by the help of an auxiliary server, named ticket server, yeh et al.'s storage action will be done and the security problem of smart card will be solved. In this model, ticket server must be related to the main proxy server in a secure channel. At first, for assessing the model, parameters in Table I must be defined.

A. System setup phase

The user and the server setup several system parameters and formula for session key generation. The user and server choose an elliptic curve order *n* over $E_p(a, b)$ generated by *P*, where *n* is a large number for the security considerations. In addition, the eligible server randomly selects $qs\ Z^*p$ as the private key, and then computes the point multiplication as user's authentication key.

B. Registration phase

In this phase, user enter his/her user name and password at first and then following values will be calculated in client user agent:

$$N_r = h(id \parallel PW_x) \tag{3}$$

$$PW_y = h(PW_x \oplus N_r) \tag{4}$$

Table I. The parameters used in the mathematical equations

Parameter	Definition
R_A	A random point on elliptic curve
$E_p(a, b)$	Elliptic curve function on finite field
PW_x	User password
$\oplus$	Exclusive or function
K_B	B user key
K_A	A user key
K	Session key
H(..)	Hash function
T	Time stamp
Nr	Produced string by hash function
K_{ida}	User secret key

Then registration message containing id and PW_y sent to server. In server side, following calculation will be done:

$$B_A = h\big(id \oplus PW_y\big) \tag{5}$$

$$K_{IDA} = qs * H1(id)G_p \tag{6}$$

$$W_A = h\big(PW_y \parallel id\big) \oplus K_{IDA} \tag{7}$$

In the end, server save following parameters in the database and send a copy of that parameters to ticket server by the secure channel and ticket server will saved this parameters:

$$\{B_A, W_A, h(), PWy, H1(), H2(), H3()\}$$

Then ticket server give verification of the action implementation to proxy server and proxy server give it to user. Fig. 3, shows the registration phase completely.

C. Mutual authentication phase

User for beginning communicating with server, starts the mutual authentication phase. At first, user calculated (8) and (9) parameters and send PW_y value to ticket server:

$$N_r = h(id \parallel PW_x) \tag{8}$$

$$PW_y = h(PW_x \oplus N_r) \tag{9}$$

If PW_y found in the ticket server's database, server will send the following parameters to user:

$$\{B_A, W_A, h(), H1(), H2(), H3()\}$$

Now, in user side following calculations must be done:

$$B'_A = h\big(id \oplus PW_y\big) \tag{10}$$

$$PW_y = h(PW_x \oplus N_r) \tag{11}$$

Then user confirm that whether B'_A is equal to B_A or not. If is equal, then user will calculate V and K_{IDA} as follows:

$$V = h\big(PW_y \parallel id\big) \tag{12}$$

$$K_{IDA} = W_A \oplus V \tag{13}$$

Finally, user choose the random point $R_A = \big(R_A^x, R_A^y\big)$ in $E_p(a, b)$. Which R_A^x and R_A^y are x and y points that created after making K_{IDA} authentication key. In T_1 timestamp, user will compute:

$$t1=H2(T1) \tag{14}$$

$$MA=RA+t1*K(IDA) \tag{15}$$

$$R_A^x * P=R_A^* \tag{16}$$

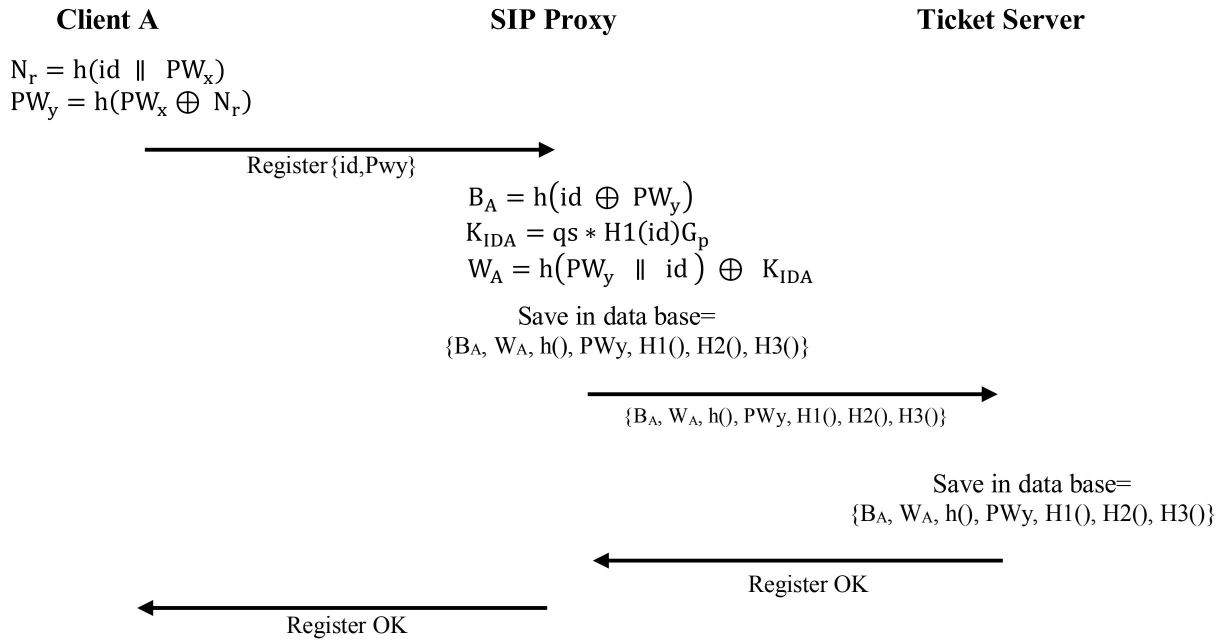
Client A
SIP Proxy
Ticket Server
$N_r = h(id \parallel PW_x)$
$PW_y = h(PW_x \oplus N_r)$
Register{id,Pwy}
$B_A = h(id \oplus PW_y)$
$K_{IDA} = qs * H1(id)G_p$
$W_A = h(PW_y \parallel id) \oplus K_{IDA}$
Save in data base=
{BA, WA, h(), PWy, H1(), H2(), H3()}
{BA, WA, h(), PWy, H1(), H2(), H3()}
Save in data base=
{BA, WA, h(), PWy, H1(), H2(), H3()}
Register OK
Register OK

Figure 3. User registration in main proxy server and ticket server

Then request message sends to proxy server. Following calculations will be done in proxy server:

$$t_1 = H_2(T_1) \tag{17}$$

$$R'_A = M_A - qs * t_1 * U_{IDA} \tag{18}$$

$$U_{IDA} = (U^x, U^y) \tag{19}$$

$$R'_A = (R_A^x, R_A^y) \tag{20}$$

$$R_A^{x'} * P = R_A^* \tag{21}$$

$$R_s = (R_s^x, R_s^y) \quad E_p(a, b) \tag{22}$$

$$t_2 = H_2(T_2) \tag{23}$$

$$M_s = R_s + t_2 * qs * U_{IDA} \tag{24}$$

$$K = H_3(U^x \parallel R_A^x \parallel R_s^x) \tag{25}$$

$$M_k = (K + R_s^x) * p \tag{26}$$

Now, server send CHALLENGE to client. In client side, following values must be calculated and sent to server as response:

$$t_2 = H_2(T_2) \quad , \quad R'_s = M_s - t_2 * K_{IDA} \tag{27}$$

Now for achieving $R'_s = \left(R_s^{x'}, R_s^{y'}\right)$, above values will be used. Finally $U_{IDA} = (U^x, U^y)$ value could gained and user will calculated following values:

$$K^* = H_3\left(U^x \parallel R_A^x \parallel R_s^{x'}\right) \tag{28}$$

$$M_k^* = \left(K^* + R_s^{x'}\right) * P \tag{29}$$

User also checked whether $M_k^* ?= M_k$ or not. If condition is true, user will calculate value of h (userid||realm||K) and made response message and sent it to proxy server. This values will be calculated in server too and results will be compared with entered values. If achieved values was the same, verification will gave to user and session key will be as follows:

$$K = H3(U^x \parallel R_A^x \parallel R_s^x) \tag{30}$$

Fig.4 shows how to function completely.

IV. Proposed Method Analysis

This section provides security and performance analysis of proposed SIP authentication scheme.

A. Security analysis

In this section, the resistance against some kinds of attacks are considered. Studied attacks contains masquerade attack, insider attack, parallel sessions attack, replay attack and password guessing attack.

1) Resistance to masquerade attack

Proof: To successfully complete a masquerade attack, an attacker must know a user's password PW_x to pass verification in the login phase and to interpret the verification message correctly for mutual authentication. But according to the following formulas:

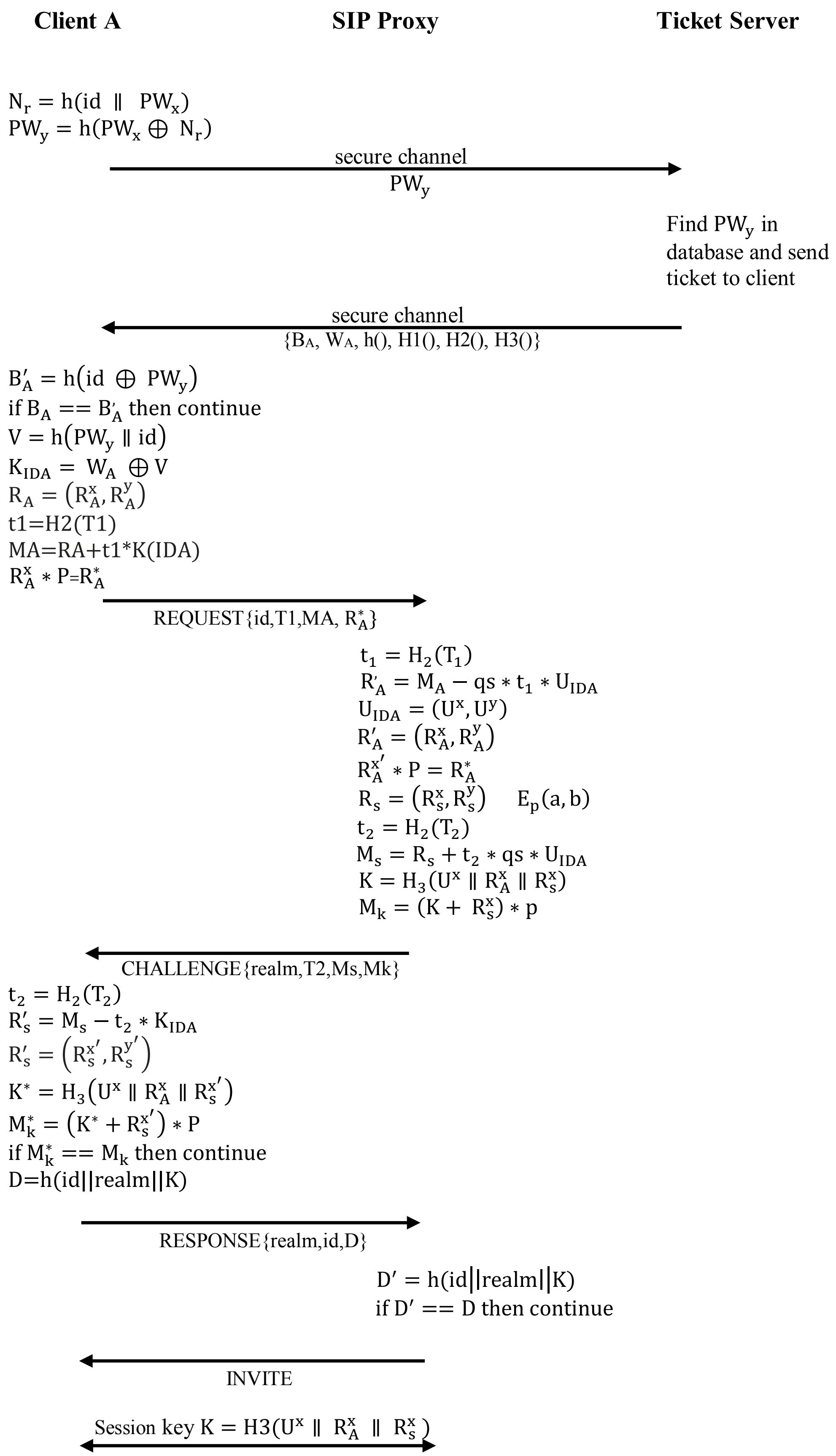
Client A
SIP Proxy
Ticket Server
$N_r = h(id \parallel PW_x)$
$PW_y = h(PW_x \oplus N_r)$
secure channel
PW_y
Find PW_y in database and send ticket to client
secure channel
{B_A, W_A, h(), H1(), H2(), H3()}
$B'_A = h(id \oplus PW_y)$
if $B_A == B'_A$ then continue
$V = h(PW_y \parallel id)$
$K_{IDA} = W_A \oplus V$
$R_A = (R_A^x, R_A^y)$
t1=H2(T1)
MA=RA+t1*K(IDA)
$R_A^x * P$=R_A^*
REQUEST{id,T1,MA, R_A^*}
$t_1 = H_2(T_1)$
$R'_A = M_A - qs * t_1 * U_{IDA}$
$U_{IDA} = (U^x, U^y)$
$R'_A = (R_A^x, R_A^y)$
$R_A^{x'} * P = R_A^*$
$R_s = (R_s^x, R_s^y)$ $E_p(a, b)$
$t_2 = H_2(T_2)$
$M_s = R_s + t_2 * qs * U_{IDA}$
$K = H_3(U^x \parallel R_A^x \parallel R_s^x)$
$M_k = (K + R_s^x) * p$
CHALLENGE{realm,T2,Ms,Mk}
$t_2 = H_2(T_2)$
$R'_s = M_s - t_2 * K_{IDA}$
$R'_s = (R_s^{x'}, R_s^{y'})$
$K^* = H_3(U^x \parallel R_A^x \parallel R_s^{x'})$
$M_k^* = (K^* + R_s^{x'}) * P$
if $M_k^* == M_k$ then continue
D=h(id||realm||K)
RESPONSE{realm,id,D}
$D' = h(id||realm||K)$
if $D' == D$ then continue
INVITE
Session key $K = H3(U^x \parallel R_A^x \parallel R_s^x)$

Figure 4. Proposed authentication scheme for SIP

$$\mathrm{PW_y = h(PW_x \oplus N_r)} \tag{31}$$

$$\mathrm{B_A = h\big(id \oplus PW_y\big)} \tag{32}$$

$$\mathrm{M_A = R_A + t_1 * K_{IDA}} \tag{33}$$

$$\mathrm{R_A^* = R_A^* * P} \tag{34}$$

Data sent by using elliptic curve one way hash function and scalar multiplication and attacker can't show his/her as real user.

2) resistance to insider attack

It is a common practice for users to apply the same password to access different applications for their convenience. If a privileged inside user of a server has the knowledge of a users' password, he/she may try to impersonate the user to access other applications.

Proof: proposed protocol provide user registration through cipher code $\mathrm{PW_y = h(PW_x \oplus N_r)}$ over a secure channel which avoids the risk of stolen passwords because password never saved in system.

3) resistance to parallel sessions attack

Proof: proposed protocol provides the cipher message code, for instance, $\mathrm{M_A}$, $\mathrm{R_A^*}$, etc., which includes the timestamp, random point $\mathrm{R_A = (R_x^A\ , R_y^A\ ) \in EP(a, b)}$. In other words, the parallel session attack is useless in this protocol.

4) resistance to parallel sessions attack

If the attacker wants to replay the same messages of the sender or the receiver, it is clear that user cannot succeed due to the random number MA, $\mathrm{R_A^*}$ in the secret cipher that is different in each authentication session. Furthermore, the server can authenticate the validity of a user (whether $\mathrm{R_A^* = P * R_A^{x'}}$) if the attacker replays the message to impersonate the user. That is, an attacker cannot launch replay attack due to the challenge/response mechanism. Thus, this protocol resists a replay attack.

5) resistance to password guessing attack

Proof: The user can securely change or update his/her password and this registration is also registered in ticket server. In proposed scheme, the password is transformed by a one way hash digest with a random number $\mathrm{N_r}$, and it is stored proxy server and ticket server. Thus, the attacker is unable to guess the password in the transmitting SIP message.

B. Performance analysis

By studying past methods and comparing with proposed method in this paper, performance is present as follows. Proposed protocol were compared with some other protocol in table II.

Also for execution time comparison, parameters in table III, must be defined.

Table III. used parameters in time execution

variable	Task
t_{EC}	Elliptic curve Polynomial make operation time
t_h	One way hash function calculation time
t_{mu}	Elliptic curve scalar Multiplication time

In this case all needed calculations are equal to (35).

$$2t_{EC} + 15t_h + 3t_{mu} \tag{35}$$

If elliptic curve polynomial make operation time, considered equal to elliptic curve scalar multiplication time, table IV is derived.

Table IV. spent time evaluation

Operation	HTTP digest	Wu et al.	Yoon et al.	Arshad et al.	Tsai	Yang et al.	Yeh et al.	Our scheme
Hash	1	6	5	8	7	7	13	15
Exponential	0	0	0	0	0	4	0	0
ECC computation	0	4	4	5	0	0	12	5

V. Conclusions

In this paper, first of all some of most common proposed methods for SIP authentication protocol were reviewed and then a new authentication scheme were proposed, by which without need to smart card, maintaining operation could be done in safe place. Due to using two separate servers, the probability of holding both servers by attacker could be much lower and since data is encrypted in ticket and main proxy server, attacker can't notify the contents. It is worth mentioning that SIP environment is internet network which is too insecure thus the proposed model can do better in comparison with previous models. In future, faster and more complex methods could be designed in order to this protocol become more secure.

Table II. comparing some authentication methods with proposed method

Attack	HTTP digest	Wu et al.	Yoon et al.	Arshad et al.	Tsai	Yang et al.	H_L_Yeh et al.	Our scheme
Crack/miss smart card resistant	Yes	No	No	No	Yes	Yes	No	Yes
Masquerade attack resistant	No	No	No	No	No	Yes	Yes	Yes
Insider attack resistant	No	No	No	No	No	No	Yes	Yes
Parallel session attack resistant	No	No	No	No	No	Yes	Yes	Yes
Replay attack resistant	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Password guessing attack resistant	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Denning-Sacco attack	No	Yes	No	No	No	No	No	No
Known-key security	No	No	No	No	No	No	No	No

References

[1] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *Communications Surveys & Tutorials, IEEE,* vol. 16, pp. 1005-1023, 2014.

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks*, et al.*, "RFC 3261: SIP: Session initiation protocol," IETF, Tech. Rep., 2002.[Online]. Available: www. ietf. org/rfc/rfc3261. txt2002.

[3] G. Camarillo and M.-A. Garcia-Martin, *The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds*: John Wiley & Sons, 2007.

[4] S. Peng, O. Ruan, J. Zhou, and Z. Chen, "A New Identity-Based Authentication Scheme for SIP," in *Information Security (ASIA JCIS), 2014 Ninth Asia Joint Conference on*, 2014, pp. 90-95.

[5] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen*, et al.*, "RFC 2617: HTTP Authentication: Basic and Digest Access Authentication," *Internet RFCs,* 1999.

[6] H.-L. Yeh, T.-H. Chen, and W.-K. Shih, "Robust smart card secured authentication scheme on SIP using elliptic curve cryptography," *Computer Standards & Interfaces,* vol. 36, pp. 397-402, 2014.

[7] 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.

[8] A. Durlanik and I. Sogukpinar, "SIP authentication scheme using ECDH," *World Enformatika Socity Transations on Engineering Computing and Technology,* vol. 8, pp. 350-353, 2005.

[9] J. W. Ring, K.-K. R. Cho, E. Foo, and M. H. Looi, "A new authentication mechanism and key agreement protocol for SIP using identity-based cryptography," 2006.

[10] L. Kong, V. A. Balasubramaniyan, and M. Ahamad, "A lightweight scheme for securely and reliably locating SIP users," in *VoIP Management and Security, 2006. 1st IEEE Workshop on*, 2006, pp. 9-17.

[11] E.-J. Yoon and K.-Y. Yoo, "Cryptanalysis of DS-SIP authentication scheme using ECDH," in *New Trends in Information and Service Science, 2009. NISS'09. International Conference on*, 2009, pp. 642-647.

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

[13] J. L. Tsai, "Efficient Nonce-based Authentication Scheme for Session Initiation Protocol," *IJ Network Security,* vol. 9, pp. 12-16, 2009.

[14] C.-C. Lee, "On Security of An Efficient Nonce-based Authentication Scheme for SIP," *IJ Network Security,* vol. 9, pp. 201-203, 2009.

[15] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," *Computer Standards & Interfaces,* vol. 31, pp. 286-291, 2009.

[16] 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.

[17] R. Arshad and N. Ikram, "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol," *Multimedia tools and applications,* vol. 66, pp. 165-178, 2013.

[18] D. He, J. Chen, and Y. Chen, "A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography," *Security and Communication Networks,* vol. 5, pp. 1423-1429, 2012.

[19] Q. Pu, J. Wang, and S. Wu, "Secure SIP authentication scheme supporting lawful interception," *Security and Communication Networks,* vol. 6, pp. 340-350, 2013.

[20] X.-M. Wang, W.-F. Zhang, J.-S. Zhang, and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," *Computer Standards & Interfaces,* vol. 29, pp. 507-512, 2007.

[21] T.-H. Chen, H.-C. Hsiang, and W.-K. Shih, "Security enhancement on an improvement on two remote user authentication schemes using smart cards," *Future Generation Computer Systems,* vol. 27, pp. 377-380, 2011.

[22] T. Guillet, A. Serhrouchni, and M. Badra, "Mutual Authentication for SIP: A semantic meaning for the SIP opaque values," in *New Technologies, Mobility and Security, 2008. NTMS'08.*, 2008, pp. 1-6.

[23] L. Zhang, S. Tang, and Z. Cai, "Robust and efficient password authenticated key agreement with user anonymity for session initiation protocol-based communications," *Communications, IET,* vol. 8, pp. 83-91, 2014.

[24] V. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO'85 Proceedings*, 1986, pp. 417-426.

[25] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation,* vol. 48, pp. 203-209, 1987.