Cryptanalysis of Tang et al.'s ECC-based mutual authentication scheme for SIP

[1]Samaneh Sadat Mousavi Nik*, [2]Amir Safdari

[1]MSC in department of Engineering, Security in Information Technology, University of Tehran Kish International Campus, Niayesh Blvd., Kish Island, Iran
[2]BA. Of software engineering, Islamic Azad University - Quchan, Iran
*Corresponding author email: samaneh_mousavi@alumni.ut.ac.ir

Abstract: Session Initiation Protocol (SIP) is a powerful signaling protocol that increasingly used for administrating Voice over IP (VoIP) phone calls. SIP authentication mechanism is based on HTTP Digest authentication, which this scheme is insecure; such as off-line password guessing attacks and impersonate other parties and etc. So proposed different schemes to secure the SIP authentication. In the year 2012, Tang et al. proposed a SIP authentication protocol using elliptic curve cryptography (ECC), but their scheme is insecure against off-line password guessing. We proposed an ECC-based authentication scheme for SIP to overcome such security problems and analysis of security of the ECC-based protocol.
[Samaneh Sadat Mousavi Nik, Amir Safdari. **Cryptanalysis of Tang et al.'s ECC-based mutual authentication scheme for SIP.** *Academ Arena* 2018;10(6):40-46]. ISSN 1553-992X (print); ISSN 2158-771X (online). http://www.sciencepub.net/academia. 7. doi:10.7537/marsaaj100618.07.

Keywords: Session Initiation Protocol, Elliptic curve cryptography, Authentication, vulnerability, insecure

Introduction

Session Initiation Protocol (SIP) proposed by Internet Engineering Task Force (IETF) for the IP-based telephony [14,15]. SIP controls communications on the Internet for establishing, maintaining and terminating sessions. SIP is an application –layer control protocol that is a text based protocol and can be used for controlling multimedia communication sessions such as voice and video calls over Internet protocols [17]. SIP is the one important protocol because of the widespread application of the voice over IP (VoIP) in the Internet so the security of SIP is becoming too important [22]. SIP is a request-response protocol when a user wants to access a SIP service, at the first she/he has to authenticate with SIP server but the original authentication scheme for SIP doesn't provide enough security because it's based on HTTP Digest authentication noted in RFC2617 [8]. Different SIP authentication schemes have been proposed especially based on Elliptic curve cryptography (ECC) to provide security for SIP.

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers [17].

In this paper, we investigate SIP Authentication Scheme based on Elliptic Curve Cryptography, Currently, the security of SIP is becoming more and more important. SIP specification does not include any specific security mechanisms. SIP authentication is inherited from HTTP Digest authentication, which is a challenge-response based authentication protocol [8].

1. History and Related Work

In 2005, Yang et al. found that the original SIP authentication scheme was vulnerable to off-line password guessing attack and server-spoofing attack, so they proposed scheme was based on Diffie-Hellman key exchange algorithm [5], which depended on the difficulty of Discrete Logarithm Problem (DLP) [10], but Yang et al.'s scheme was vulnerable to stolen-verifier attack, off-line password guessing attack, and Denning-Sacco attack [4] and Their scheme was high computation cost [6,9,16]. In the same year, Based on Yang et al.'s scheme, Durlanik et al. [6] introduced another SIP authentication by using Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm but this scheme in comparison with Yang et al. [12] scheme reduced the execution time and memory requirements. However, their scheme still vulnerability from off-line dictionary attack and Denning-Sacco attack [12]. In 2008, Tsai [16] proposed SIP authentication scheme based on random nonce. In this scheme all the communication messages were computed with one-way hash function and exclusive-or operation so computation cost reduce highly. But this scheme vulnerable to off-line password guessing, Denning-Sacco and stolen-verifier attacks; furthermore, it did not provide any key agreement, known-key secrecy and perfect forward secrecy (PFS) [2,3,11,20]. In 2009, Wu et al. [23] suggested an SIP authentication scheme based on elliptic curve cryptography (ECC). This scheme achieves authentication and a shared secrecy at the same time. Wu et al.'s scheme provides provable security in the

Canetti–Krawczyk (CK) security model [13] and it's suitable for applications that require low memory and rapid transactions. But Wu et al.'s SIP authentication schemes are still vulnerable to off-line password guessing attacks, Denning-Sacco attacks, and stolen-verifier attacks [10,11]. In 2009, Yoon et al. proposed another authentication for SIP using ECC in [20]. Unfortunately, the scheme was vulnerable to password guessing attack and stolen-verifier attack. The attack method could be referred to [18]. In 2010, Yoon et al. proposed the third and fourth ECC-based authentication scheme for SIP [21,24]. But these schemes were vulnerable to offline password guessing and stolen-verifier attacks [18]. In 2011 Arshad et al. proposed SIP authentication scheme based on ECC [2]. But Arshad et al.'s authentication scheme was vulnerable to off-line password guessing attack [1]. In 2012 Tang et al. proposed a secure and efficient authentication scheme based on Elliptic Curve Discrete Logarithm Problem (ECDLP) for SIP. We demonstrate the Tang et al. authentication scheme vulnerable to off-line password guessing attack in this paper and then propose a secure SIP authentication scheme based on ECC in order to solve those security problems. The proposed SIP authentication scheme can provide high security and executes faster than previously proposed schemes.

The remainder of this paper is outlined as follows. Section 3 reviews the original SIP authentication procedure. Section 4 introduces of Tang et al.'s scheme and discusses attack on it and in Section 5 proposed ECC-based mutual authentication scheme for SIP is presented. In section 6 discuss the security and efficiency of the proposed scheme, In Section 7, evaluates the performance of the proposed scheme. And Section 8 is the conclusion.

SIP authentication procedure

SIP authentication security is based on the challenge-response mechanism, in which a nonce value is used in challenging the target. The common authentication scheme for SIP is Digest Access Authentication (DAA) [8]. DAA security is based on the challenge-response pattern, and this mechanism relies on a shared secret between client and server [19]. So Client pre-shares a password with the server before the authentication procedure starts. Fig. 1 shows procedure of the DAA mechanism in SIP.

(1) Client → Server: REQUEST

The client sends a REQUEST to the server.

(2) Server→ Client: CHALLENGE (nonce, realm)

The server generates a CHALLENGE that includes a nonce and the client's realm. Then the server sends a CHALLENGE to the client.

Review Of SIP Authentication Scheme By Tang Et Al.

This section reviews Tang et al.'s SIP authentication scheme [1]. Then shows that the scheme is vulnerable to off-line password guessing attacks. Tang et al.'s scheme consists of four phases: system setup phase, registration phase, login and authentication phase, and password change phase.

Table 1. Notations and their explanations

Ui , U :	the ith user or user
IDi , username:	the identity of user Ui
PWi:	Password of user
S:	the remote server
Ks:	the secret key of the server
SK:	a session key
Q = Ks.P:	the public key of the server
h(.):	a strong cryptographic one-way hash function
H(.):	a function which makes a point map to another point on elliptic curve
ll:	the string concatenation operation
⊕:	the exclusive-or operation
⇒:	a secure channel
→:	a common channel
A?=B:	compares whether A equals B
D:	a uniformly distributed dictionary of size lDl

(3) Client→Server: RESPONSE (nonce, realm, username, response)

The client computes a response = F (nonce, realm, username, response). Note that F (.) is a one-way hash function. It is used to generate a digest authentication message, and then the client sends the RESPONSE to the server.

(4) According to the username, the server extracts the client's password. Then the SIP server must perform the same digest operation, and compare the result. If the results are identical, the client is authenticated and a 200 OK message is sent.

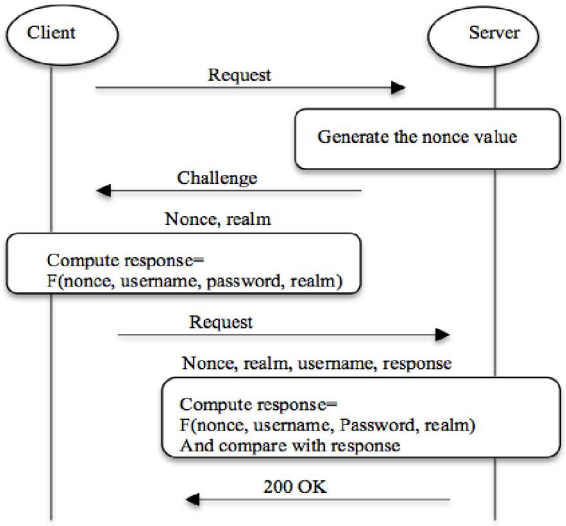

Figure 1. The SIP Digest Access Authentication method during a SIP REGISTER transaction

4.1 Tang et al.'s scheme

Tang et al. propose an enhanced ECC-based SIP authentication scheme in order to strength Arshad et al. scheme. Notations used in this paper are defined in Table 1.

4.1.1 System setup phase

First the members and the server agree on the EC parameters Then server selects a secret key K_S, computes $Q = K_S . P$ and keeps secret K_S and publishes p, a, b, P, n, h, Q [1].

4.1.2 Registration phase

In this phase:

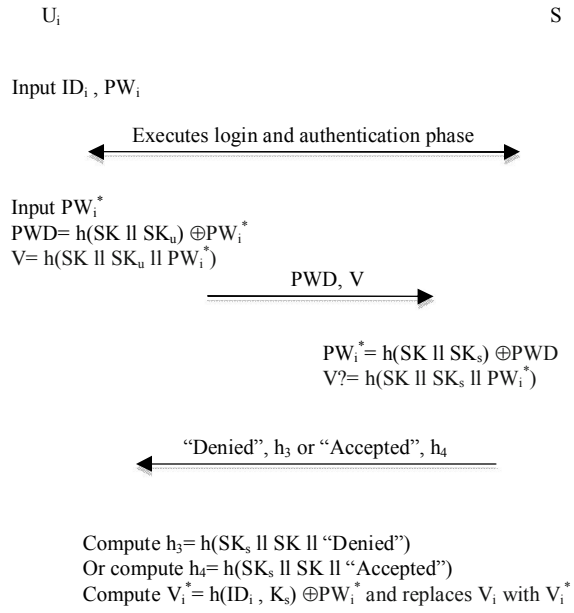

Figure 3. Password change phase

(1) The user chooses his or her identity IDi and password PWi, then through a pre-established secure channel, such as Virtual Private Network (VPN) or Secure Sockets Layer (SSL) sends them to the server.

(2) The server computes Vi = h (IDi ll K_S) ⊕ PWi and stores (IDi, Vi) in its database.

4.1.3 Login and authentication phase

Fig. 2 illustrates Tang et al.'s SIP authentication scheme. When a legal SIP client U wants to login the SIP server S, the authentication scheme between U and S proceeds as follows.

(1) Ui → S: REQUEST (IDi, R1)

Ui selects a random nonce r1 ϵ Z_n^* then computes $R=r_1.P$, $R_1 = R + H (IDi,PWi)$. And then sends message REQUEST (IDi, R_1) To the server S.

(2) S → Ui: CHALLENGE (S, R_2, V_1)

First S checks IDi is exist in database. If yes, S computes PWi = Vi ⊕h (IDi ll KS), $R^{'} = R_1$ - h (IDi, PWi) = r_1. P. And then S selects a random nonce r_2 ϵ Z_n^*, computes $R_2 = r_2$. P, $SK_S = r_2 . R^{'} = r_1 . r_2 . P$, V_1 =h (S ll IDi ll R ll R_2 ll SK_s), and sends CHALLENGE (S, R_2, V_1) to Ui. At the end, S computes the common session key SK = h (IDi ll S ll $R^{'}$ ll R_2 ll SK_s ll PW_i)

(3) Ui → S: RESPONSE (IDi, S, V_2)

Ui computes SKU = r_1. $R_2 = r_1.r_2$. P and checks V_1 is equal to h (S ll IDi ll R ll R_2 ll SK_U). If they are equal, Ui authenticates the server and computes V_2 = h (IDi ll S ll SK_U ll PWi). Then Ui sends message RESPONSE (IDi, S, V_2) To the server. Then Ui computes the session key SK = h (IDi ll S ll R ll R_2 ll SKU ll PWi).

(4) Upon receiving the response message, S checks V_2 is equal to h (IDi ll S ll SK_S ll PWi). If the result is equal S authenticates the identity of Ui and the common session key is: SK= h (IDi ll S ll r_1. P ll r_2. P ll r_1. r_2. P ll PWi)

4.1.4 Password change phase

In this phase user can change his or her password. Figure 3 shows the password change phase.

- Server authenticates Ui with his or her old password PWi.
- After receiving the successful authentication, Ui inputs the new password PW_i^*.
- Finally, the server computes V_i^* and replaces Vi with V_i^*.

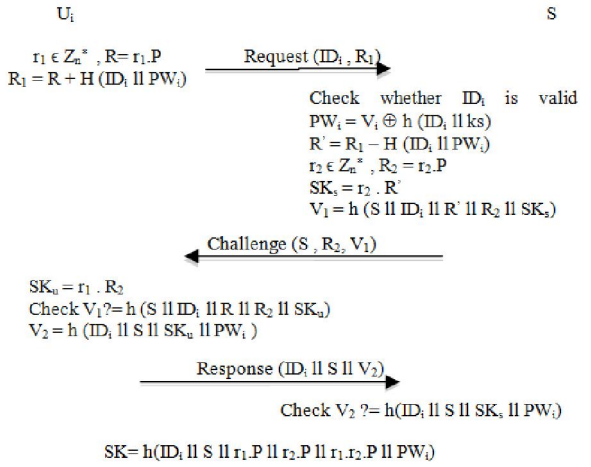

Figure 2. Login and authentication

4.2 Attacks on Tang et al.'s scheme

In this section, we will show that Tang et al.'s scheme is vulnerable to off-line password guessing attack.

4.2.1 Off-line password guessing attack

Off-line password guessing attack works when an attacker tries to find a long-term private key (pw) of Ui. In Tang et al.'s SIP authentication scheme, the off-line password guessing attack is possible.

1) An attacker records Tang et al.'s SIP authentication scheme between the SIP client and the server (use R1, R2 and V2 values).

2) By performing the following can run off-line

password guessing attack.

a) An attacker selects a candidate password PWi* from the password dictionary D.

b) Attacker Calculate H (ID_i ll PW_i^*) then $R_1' = R_1 - H(ID_i \text{ ll } PW_i^*) = R + H(ID_i \text{ ll } PW_i) - H(ID_i \text{ ll } PW_i^*)$ output of this step is R.

c) Attacker computes $Sku^* = r_1.R_2$ and $V_2^* = h(ID_i \text{ ll } S \text{ ll } sk_u^* \text{ ll } pw_i^*)$

d) Finally compares V_2* with V_2. If they are equal, attacker guesses the correct password of U, If not, the attacker repeats the above process until $V_2^* = V_2$.

5 Proposed SIP authentication scheme

We propose a new secure SIP authentication scheme based on elliptic curve cryptography (ECC) to overcome the security problems. This scheme is in order to Tang et al.'s scheme. The proposed scheme exploits speed, and security jointly. The proposed scheme consists of four phases: system setup phase, registration phase, login and authentication phase, and password change phase.

5.1 System setup phase

U and S agree on the EC parameters. The server selects a secret key K_S, computes $Q = K_S.P$, keeps secret K_S and publishes p, a, b, P, n, h, Q.

5.2 Registration phase

In this phase:

(1) The user chooses his or her identity IDi and password PWi, then through a pre-established secure channel, such as Virtual Private Network (VPN) or Secure Sockets Layer (SSL) sends them to the server.

(2) The server computes Vi = h (IDi ll K_S) ⊕ PWi and stores (IDi, Vi) in its database.

This phase is the same Tang et al.'s scheme.

5.3 Login and authentication phase

When a legal SIP client U wants to login the SIP server S, the authentication scheme between U and S proceeds. We indicated that Tang et al.'s scheme is vulnerable to off-line password guessing attack for overcome these security problems, Fig. 4 illustrates the new proposed SIP authentication scheme.

(1) Ui → S: REQUEST (IDi, R1)

Ui selects a random nonce r1 ϵ Z_n^* then computes R=r1.P, R1 = R + H (IDi ll PWi). And then sends message REQUEST (IDi, R1) to the server S.

(2) S → Ui: CHALLENGE (S, $R2^*$, V_1)

First S checks IDi is exist in database. If yes, S computes PWi = Vi ⊕h (IDi ll KS), $R' = R1 - H(IDi \text{ ll } PWi) = r1.P$. And then S selects a random nonce r2 ϵ Z_n^*, computes R2 = r2. P, $R_2^* = (r_2.P) \oplus r_1$, SKS = r2. R = r1. r2. P, $V_1 = h(S \text{ ll } ID_i \text{ ll } R' \text{ ll } R_2 \text{ ll } SKs)$ and sends CHALLENGE (S, R_2^*, V_1) to Ui.

(3) Ui → S: RESPONSE (IDi ll S ll V2)

Ui computes $R_2' = R_2^* \oplus r_1 = (r_2.P) \oplus r_1 \oplus r_1 = r_2.P$, $SK_u = r_1.R_2'$ and Checks V_1 is equal to h (S ll ID_i ll R ll R_2' ll SK_u) If the result is equal Ui authenticates the identity of S. And then computes V_2= h (ID_i ll S ll SK_u) and sends RESPONSE (IDi ll S ll V2) to the server.

(4) Upon receiving the response message, S checks V2 is equal to h (ID_i ll S ll SK_s). If the result is equal S authenticates the identity of Ui.

Shared session key Sk = $r_1.r_2.P$

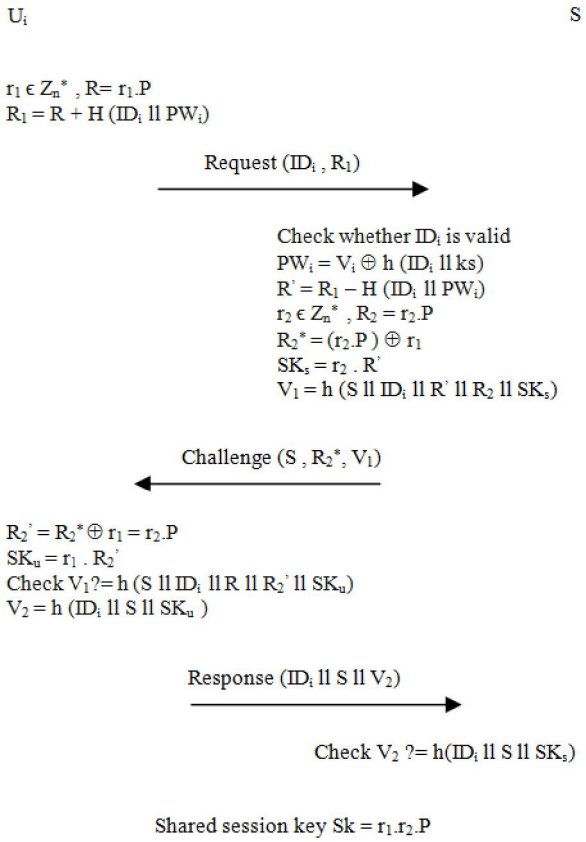

Figure 4 . Proposed Login and authentication phase

5.4 Password change phase

In this phase user can change his or her password. Figure 3 shows the password change phase.

- Ui needs to authenticate with his or her old password PWi. After successful authentication, Ui inputs the new password PW_i^*.
- U_i → S: PWD; V

U_i computes PWD = h (SK ll SK_u) ⊕ PW_i^* and V= h (SK ll SK_u ll PW_i^*) then user sends message PWD, V to the server.

- Then server computes PW_i^* = h (SK ll SK_s) ⊕ PWD and checks if V is equal to h (SK ll SK_s ll PW_i^*) then the server computes h_4 = h (SK_s ll SK ll "Accepted") and sends ("Accepted", h_4) else computes h_3 = h (SK_s ll SK ll "Denied") and sends ("Denied", h_4) to the user. Finally, the server computes V_i^* = h (ID_i ll K_s) ⊕ PW_i^* and replaces V_i with V_i^*. This phase is the same Tang et al.'s scheme.

6. Security analysis

This section analyzes a security of the proposed SIP authentication scheme.

5.5 Define security terms

- Password (pw): is a low entropy value that can be guessed in polynomial time.
- K_s (secret key S): is a high entropy value that cannot be guessed in polynomial time.
- The Elliptic Curve Discrete Logarithm Problem (ECDLP): Given a public key point $Q = \alpha P$, it is hard to compute the secret key α.
- The Elliptic Curve Diffie–Hellman Problem (ECDHP): Given point elements αP and βP, it is hard to find αβP.
- A secure one-way hash function y = F (x): when given x it is easy to compute y and when given y it is hard to compute x.

5.6 Security properties

In this section we analyze the security properties in the proposed SIP authentication scheme.

1. Password guessing attacks

The proposed scheme can resist Password guessing attacks.

Off-line password guessing attack: If Eve try to find a PW by repeatedly guessing possible passwords and verifying the correctness of the guesses based on gain information in an off-line manner cannot success because In our scheme, all knowledge Eve can gain are $R_1 = R + H (ID_i \text{ ll } PW_i)$, $R_2^* = (r_2.P) \oplus r_1$, V_1 and V_2. Therefore if Eve guessing possible password and computes H (ID_i ll PW), it doesn't have any information to compare the guess password is correct or not also in this scheme Eve cannot compute SK because it's difficult Eve breaks the ECDLP and ECDHP, in addition both r_1 and r_2 values are protected too (see R_1 and R_2^*).

On-line password guessing attack: cannot succeed, since S can choose appropriate the secret key K_s that is a high entropy number and cannot be guessed by anyone so Eve cannot make a successful guess of the right password from V_i without the secret key Ks of server. Therefore, the proposed scheme can resist against the password guessing attacks.

2. Replay attacks

The proposed scheme can resist the replay attacks. If an attacker replays REQUEST to impersonate U in Step (1), in Step (3), Eve cannot compute a correct session key sk and deliver it to S.

3. Man-in-the-middle attacks

The proposed scheme can resist against the man-in-the-middle attacks because this scheme based on mutual authentication and shared secret PW between U and S so PWi of Ui and the secret key Ks of S are used to prevent the man-in-middle attack.

4. Stolen-verifier attacks

The proposed scheme can resist against the stolen-verifier attacks because servers are always the targets of attacks but in this scheme the server computes Vi = h (IDi ll KS) ⊕ PWi and stores (IDi, Vi) in its database so if attacker Eve steals verifier from the database of the server, Eve cannot make a successful guess of the right password from Vi.because Eve doesn't have the secret key K_s of server and also K_s is a high entropy number.

5. Impersonation attacks

The proposed scheme can resist against the impersonation attacks. In this scheme attacker Eve cannot masquerade as server because doesn't have K_s and on the other hand Eve cannot masquerade as U because doesn't have knowledge about PW.

6. Oracle attacks

The proposed scheme can resist against the oracle attacks because in our scheme doesn't use decryption oracle.

7. Denning-Sacco attacks

The proposed scheme can resist against Denning-Sacco attacks. Assume that attacker Eve may find fresh session key SK for some reasons. But Eve cannot detect PWi and server's secret key Ks because SK= $r_1.r_2.P$ and it's ECDHP so Eve cannot compute.

8. Known-key security

Our scheme provides Known-key security, means that during authentication between U_i and S, they should produce unique secret session key by random values r_1 and r_2.

9. Session key security

Our scheme provides session key security because of ECDLP, ECDHP and secure one-way hash function therefore just U_i and S can compute the session key at the end of the key exchange.

10. Perfect forward secrecy

Our scheme provides PFS means that, if long-term private keys such as user's password PW_i and secret key K_s of server are compromised, there isn't any effect on the secrecy of previous session keys. Because of ECDHP and attacker Eve cannot compute Sk= αβP from R_1 and R_2^*.

11. Mutual authentication

Our scheme provides mutual authentication means that during authentication mechanism both the user and the server are authenticated each other. Server can authenticate the user by checking whether V_2 is correct and U_i can authenticate the identity of the server if V_1 is correct.

The security properties of the previously reported schemes [1,2,6,16,19,21] and the proposed scheme are summarized in Table 2.

Performance Comparisons

The computation costs of our proposed scheme and the previously schemes [1,2,6,16,19,21] are shown in Table 3. The proposed SIP authentication scheme

requires four PM (elliptic curve scale multiplication), two HP (hash-to-point function), two PA (point addition) and five H (hash function operations) during the protocol execution. Our proposed scheme is efficient authentication schemes for Session Initiation Protocol.

The proposed SIP authentication scheme requires elliptic curve scale multiplication computations and hash-to-point operations to resist the password guessing attack and provide known-key secrecy and PFS.

Conclusions

This paper indicates the vulnerabilities of Tang et al.'s authentication schemes for session initiation protocol (SIP) to off-line password guessing attacks. In order to resolve the shortcomings in their scheme, we proposed a new secure and efficient SIP authentication scheme. Our scheme based on ECC, resists the mentioned attacks and needs to compute four elliptic curve scale multiplications and two hash-to-point function operations during a protocol run. At the end, our scheme maintains high efficiency compared with previous ECC-based authentication schemes.

Table 2. Comparisons of the security properties of different schemes

	Durlanik [6]	Yang [19]	Tsai [16]	Yoon [21]	Arshad [2]	Tang [1]	Ours
Impersonation attack	Insecure	Insecure	Insecure	Secure	Insecure	Secure	Secure
Password guessing attack	Insecure	Insecure	Insecure	Insecure	Insecure	Insecure	Secure
Denning Sacco attack	Insecure	Insecure	Insecure	Secure	Secure	Secure	Secure
Stolen-verifier attack	Not applicable	Insecure	Insecure	Insecure	Secure	Secure	Secure
Mutual authentication	Provided	Provided	Provided	Provided	Provided	Provided	Provided
Session key security	Provided	Not applicable	Provided	Provided	Provided	Provided	Provided
Known key secrecy	Provided	Not applicable	Not provided	Provided	Provided	Provided	Provided
Perfect forward secrecy	Provided	Not applicable	Not provided	Provided	Provided	Provided	Provided

Table 3. Comparison of computation cost

	Durlanik [6]	Yang [19]	Tsai [16]	Yoon [21]	Arshad [2]	Tang [1]	Ours
Exponentiation	**0**	**4**	**0**	**0**	**0**	**0**	**0**
Scale multiplication	**4**	**0**	**0**	**6**	**5**	**4**	**4**
Point addition	**0**	**0**	**0**	**3**	**0**	**2**	**2**
Hash-to-point	**0**	**0**	**0**	**0**	**0**	**2**	**2**
Hash function	**6**	**8**	**7**	**4**	**8**	**7**	**5**
Exclusive or	**4**	**4**	**3**	**0**	**2**	**1**	**3**
Security	ECDLP	DLP	HASH	ECDLP	ECDLP	ECDLP	ECDLP

References:

1. Tang H, Liu X. Cryptanalysis of Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol. (2012); Multimed Tools Appl. DOI 10.1007/s11042-012-1001-8.
2. Arshad R, Ikram N. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. (2011); Multimed Tool Appl. doi:10.1007/s11042-011-0787-0.
3. Chen TH, Yeh HL, Liu PC, Hsiang HC, Shih WK. A secured authentication protocol for SIP using elliptic curves cryptography. (2010); CN, CCIS 119:46–55.
4. Denning D, Sacco G. Timestamps in key distribution systems. (1981); Commun ACM 24:533–536.
5. Diffie W, Hellman ME. New directions in cryptography. (1976); IEEE Transactions on Information Theory IT-22: 644–654.
6. Durlanik A, Sogukpinar I. SIP Authentication Scheme using ECDH. (2005); World Enformatika Socity Transations on Engineering Computing and Technology 8:350–353.
7. Ryu JT, Roh BH, Ryu KY. Detection of SIP flooding attacks based on the upper bound of the possible number of SIP messages, KSII Transactions on Internet and Information Systems. (2009); (TIIS) 3 (5) 507–526.
8. Franks J, Hallam-Baker P, Hostetler J, Lawrence S, Leach P, Luotonen A, Stewart L. HTTP authentication: basic and digest access authentication. (1999); IETF RFC2617.
9. He DB, Chen JH, Zhang R. A more secure authentication scheme for telecare medicine information systems. J Med Syst. (2011); doi:10.1007/s10916-011-9658-5.
10. Menezes AJ, Oorschot PC, Vanstone SA. Handbook of Applied Cryptograph, (1997); CRC Press.
11. Lin CL, Hwang T. A password authentication scheme with secure password updating. (2003); Comput Secur 22(1):68–72.

12. Yoon EJ, Yoo KY. Cryptanalysis of DS-SIP authentication scheme using ECDH, in 2009 International Conference on New Trends in Information and Service Science 642–647.
13. Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels, in: Proc. Eurocrpt 2001, Lecture Notes in Computer Science, 2045, pp. 453–474.
14. Rosenberg J, Schulzrinne H, Camarillo G, Johnstone A, Peterson J, Sparks R (2002) SIP: session initiation protocol. IETF RFC3261.
15. Thomas M. SIP security requirements. (2001); IETF Internet Draft (draftthomas-sip-sec-reg-00.txt).
16. Tsai JL. Efficient nonce-based authentication scheme for session initiation protocol. (2009); Int J Netw Secur 8(3):312–316.
17. Veltri L, Salsano S, Papalilo D. SIP security issues: the SIP authentication procedure and its processing load. (2002); IEEE Netw 16(6):38–44.
18. Xie Q. A new authenticated key agreement for session initiation protocol. (2011); Int J Commun Syst. doi:10.1002/dac.1286.
19. Yang CC, Wang RC, Liu WT. Secure authentication scheme for session initiation protocol. (2005); Comput Secur 24:381–386.
20. Yoon EJ, Yoo KY. A new authentication scheme for session initiation protocol, in 2009 International Conference on Complex, Intelligent and Software Intensive Systems, CISIS '09 549–554.
21. Yoon EJ, Koo KY. Robust mutual authentication with a key agreement scheme for the session initiation protocol. (2010); IETE Tech Rev 27(3):203–213.
22. Geneiatakis D, Dagiuklas T, Kambourakis G, Lambrinoudakis C, Gritzalis S, Ehlert S. Survey of security vulnerabilities in session initiation protocol. (2006); IEEE Commun Surv Tutorials 8(3):68–81.
23. Wu L, Zhang Y, Wang F. A new provably secure authentication and key agreement protocol for SIP using ECC, (2009); Computer Standards and Interfaces 31 (2) 286–291.
24. Yoon EJ, Yoo KY. A three-factor authenticated key agreement scheme for SIP on elliptic curves, in Proceedings of the 2010 Fourth International Conference on Network and System Security 334–339.

6/25/2018