SURVEY OF SIP AUTHENTICATION MECHANISMS

[1]HANANE BELAOUD, [2] JAMAL EL ABBADI , [3]AHMED HABBANI
[1,2]LEC Lab, MIS Team, EMI, University of Mohammed VAGDAL, Rabat, Morocco
3SIME Lab, MIS Team, ENSIAS, University of Mohammed V Souissi, Rabat, Morocco
E-mail: [1]hanane.belaoud@gmail.com, [2]m3s.ride@gmail.com, [3] j.elabbadi@gmail.com

ABSTRACT

In recent years Voice over Internet Protocol (VoIP) has become a popular NGN (Next Generation Network) technology. As this technology is built on internet protocol it is affected by a critical security problems . The Session Initiation Protocol (SIP) is considered as the most used signaling protocol for calls over the Internet for establishing, maintaining and terminating VoIP calls.

The security of SIP is becoming more and more important. The prime security service required by SIP is authentication. This paper focuses on the SIP security mechanisms of authentication. We survey the newly proposed methods of authentication then we proceed to evaluate these methods in view of security efficiency and computational cost.

Keywords: *NGN, VOIP, SIP, authentication*

1. INTRODUCTION

In today's computer networks environment, the security of SIP is becoming more and more important.

Authentication is the most important security service required by Session Initiation protocol. When a user requests to use a SIP service, he needs to be authenticated. To enhance the SIP security, several authentication schemes have been proposed.

This paper is structured as follows: Section II firstly presents the general components of the SIP architecture, then it presents the security attacks against SIP authentication which will be used as evaluation criteria of SIP authentication mechanism, finally it presents the original SIP authentication procedure. Section III reviews briefly the newly SIP security mechanisms of authentication. Meanwhile section IV compare the efficiency of these mechanisms by analyzing them in view of security criteria and computational cost .Finally the conclusion is given.

2. SIP PROTOCOL OVERVIEW

2.1 SIP: Background

SIP [1] proposed by Internet Engineering Task Force (IETF) is a signaling communications protocol, widely used for controlling multimedia communication sessions. SIP defines messages that can be used for establishing, modifying and terminating a session between two endpoints.

SIP is an application-layer protocol. It can be run on UDP [2] or TCP [3]. For voice media, SIP operates with RTP [4].

SIP is a text oriented protocol based on the HTTP protocol which defines two types of messages (SIP requests and SIP responses).

SIP defines four basic classes of network entities:

1)UAC and UAS:UAC runs on the user terminal, generates and sends SIP requests while the UAS receives SIP requests and sends SIP responses.

2) Register server: The register server accepts the registration request for particular user, and manages to add user agent's address to the location server.

3) Proxy server. The proxy server is the element which is responsible for routing messages. It can accept UAC's requests and send them to corresponding server.

4) Redirect server. The redirect server is a logical entity which accepts calls from UA and indicates the redirected destination for UA through querying the location server.

SIP defines the following request messages : INVITE, ACK, CANCEL, BYE and REGISTER.

A user agent, which want to initiate a session, sends an INVITE message. This message is responded by an OK followed by an ACK message. When a UA wants to terminate the session, it sends a BYE. The CANCEL message cancels the INVITE before the OK. REGISTER is used by the

User Agent to be authenticated by the registrar server. A basic SIP session is presented in Fig. 1

For any type of request sent by UA (apart from CANCEL, BYE and ACK), the SIP proxy or registrar server authenticates the User Agent with the mechanism presented in Fig.2

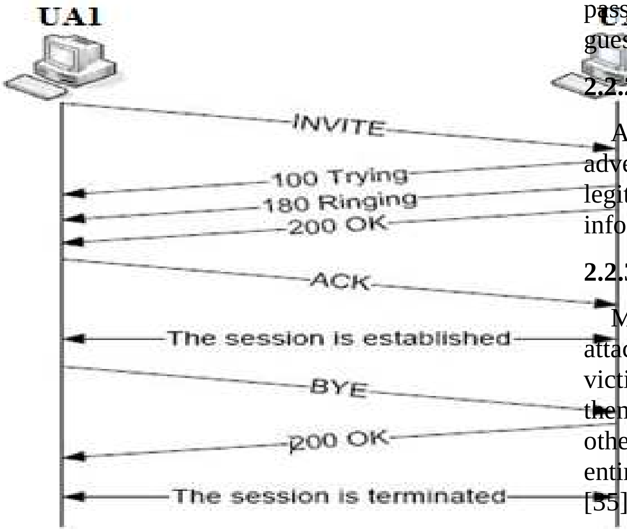

Figure 1. SIP Establishment Session

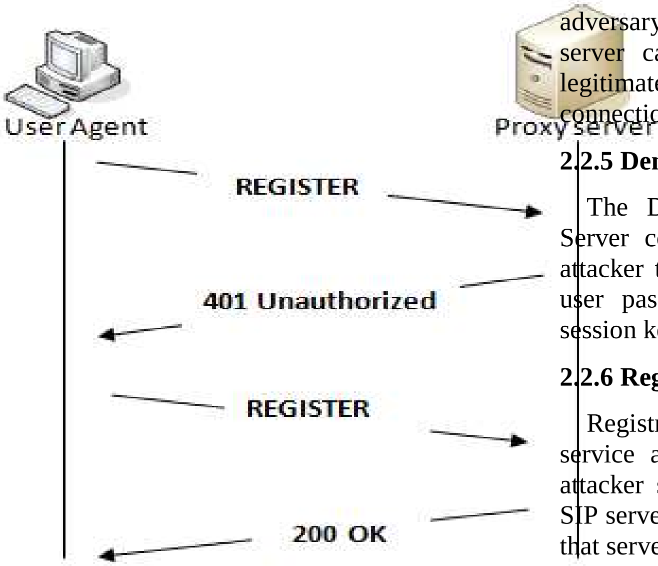

Figure 2. SIP Registration Session

2.2 Security consideration

In this section we will present a set of security attacks; That is, when we analyze the SIP authentication mechanisms, we will analyze them with a view towards how they resist against these attacks or not.

2.2.1 Password guessing attacks

Password guessing attacks means that when an attacker interposes the communication between User and Server then he can guess the correct secret password by repeatedly guessing possible passwords and verifying the correctness of the guesses.[34].

2.2.2 Replay attacks

A replay attack is an offensive action in which an adversary impersonates or deceives another legitimate participant through the reuse of information obtained in a protocol [34].

2.2.3 Man-in-the-middle attacks

Man-in-the-middle attacks means that the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker [35].

2.2.4 Stolen-verifier attacks

The stolen-verifier attack means that an adversary who steals the password-verifier from the server can use it directly to masquerade as a legitimate user in a user authentication connection[34].

2.2.5 Denning-Sacco attacks

The Denning-Sacco attack is when User or Server compromises an old session key and an attacker tries to find a long-term private key (e.g. user password or server private key) or other session keys [35].

2.2.6 Registration attacks

Registration attack is a new kind of a denial of service attack on SIP servers.In this attack, the attacker sends a spoofed unregister message to a SIP server and cancels the registration of the user at that server [35].

2.2.7 Known-key security

Known-key security, means that during authentication between User and Server, they should produce unique secret session key. If one session key is compromised then neither the private keys nor session keys are compromised as a result [35].

2.2.8 Session key security

Session key security means that at the end of the key exchange, the session key is not known by anyone but User and Server [35].

2.2.9 Perfect forward secrecy

Perfect forward secrecy means that if long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities is not affected [35].

2.2.10 Mutual authentication

Mutual authentication means that both the user and server are authenticated to each other within the same protocol [35].

2.3 Review of HTTP Digest authentication scheme for SIP

As mentioned previously SIP is a text oriented protocol based on the HTTP protocol.

REGISTER and INVITE exchanges are the two most used SIP exchanges, respectively used to connect to the network, and establish a call.

The authentication of communicating parties is the most important security service in SIP. When a user requests to use a SIP service, it needs to be authenticated. HTTP digest authentication [5] is the basic authentication mechanism.

HTTP Digest authentication scheme is based on the challenge–Response mechanism, to challenge the target a nonce value is used . Before the scheme starts, the client and the server must pre-share a password.

Figure 3 is an example flow of HTTP Digest authentication mechanism in SIP.

Step 1:

The client sends a REQUEST to the server.

Step 2:

The server generates a nonce and sends a error message requesting for authentication .this message contain the nonce value and a realm.

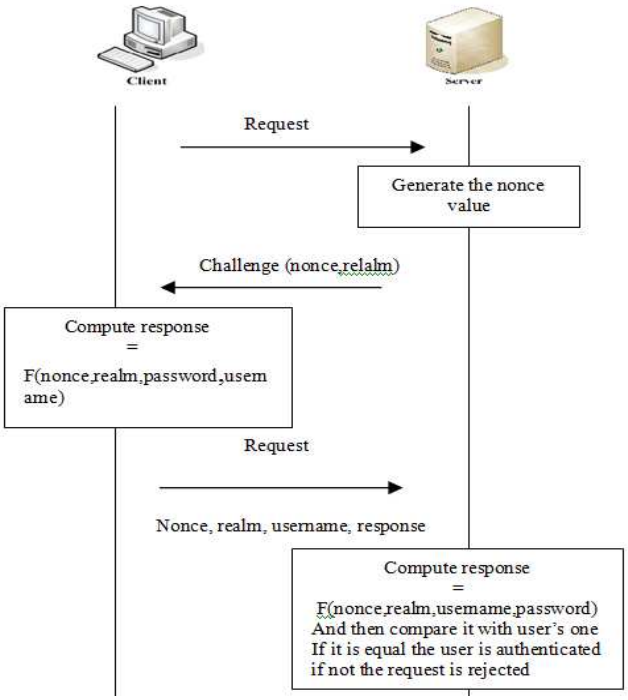
Client
Server
Request
Generate the nonce value
Challenge (nonce,relalm)
Compute response = F(nonce,realm,password,usem ame)
Request
Nonce, realm, username, response
Compute response = F(nonce,realm,usemame,password)
And then compare it with user's one
If it is equal the user is authenticated
if not the request is rejected

Figure3. HTTP Digest Authentication Scheme

Step 3:

The client use a hash function of the nonce value received in challenge, the username and the password pre-shared with the server and the realm to compute the response. Then it sends back the original request message with the computed response value, username, nonce value and realm.

Step 4:

The server extracts the client's password According to the username. Then it verifies whether the nonce is correct or not. If it is correct, it computes a hash function of the nonce, username, password and realm and compares it with the client's response.If they match, the server authenticates the identity of the client.

This mechanism have two important advantages; its easy implementation and its high performance. However it has been proven to be insecure against a number of attacks [11]. For this, more secure authentication mechanisms are needed to deliver a high security of users and servers.

3. SURVEY OF SIP AUTHENTICATION MECHANISMS

In last decade, a number of authentication mechanisms aiming to replace the basic security scheme HTTP Digest Authentication have been proposed, using Diffie-Hellman [6], Elliptic Curve cryptography, nonce, ID-based cryptosystems [9] and others.

In this section we will present several advanced methods of authentication.

3.1 Authentication methods based on Diffie Hellman:

In 2005, Yang et al. [11] show that the basic SIP authentication scheme based on HTTP digest authentication provides only unilateral authentication and it does not resist to the off-line password guessing attacks and the server spoofing attacks. They propose a secure SIP authentication scheme based on the Diffie–Hellman key exchange algorithm [6]. And present a message flow of their method when a user requests to access the server's resources.

They pointed out that their scheme can resist the off-line password guessing attacks, the server spoofing attacks and the replay attack. Regarding the performance of the mechanism, they compare their scheme with the HTTP digest scheme and EKE (Encrypted Key Exchange) scheme and conclude that their scheme is more efficient.

However, Yang et al.'s scheme has still a weaknesses; firstly, it need to maintain preconfigured password table.Secondly, it need an exponential computation, which is not suitable for the user's device with limited computing capability [14].

3.2 Authentication methods based on Elliptic Curve cryptography

In 2005, Durlanik et al. [7] proposed a SIP authentication scheme using elliptic curve cryptosystem (ECC).This protocol provides a small key sizes and a fast computations.

They compare their approach with DH and show that it has a significant advantages; it is faster than DH by means of execution times and memory usage statistics.

However, it is vulnerable to man-in-the middle attack and it is not completely safe with untrusted verifiers (proxy servers) due to the fact that the servers keep user passwords in a plaintext. [16].

In 2008, Wu et al. [16] also proposed a new authentication and key exchange protocol based on elliptic curve cryptography (ECC), They claimed that their scheme can provide a set of security services such as data confidentiality, data integrity, authentication, access control, and perfect forward secrecy .They claimed also that their scheme is secure against man-in-the-middle attacks, replay attacks, off-line password guessing attacks, and server spoofing attacks. Regarding the computation costs Wu et al.'s scheme is more efficient for applications which require low memory and fast computations.

However, Wu's scheme is not completely safe against off-line password guessing attacks [18].

In 2009,Yoon and Yoo [8,18] prove that Tsai's authentication scheme is vulnerable to some attacks like off-line password guessing attacks, stolen-verifier attacks and denning-Sacco attacks , and also it does not provide perfect forward secrecy.They also demonstrate that the new authentication and key exchange protocol proposed by Wu et al. is still vulnerable to off-line password guessing attacks.

They propose a new secure authentication scheme based on the elliptic curve discrete logarithm problem (ECDLP) which can resist to then security properties listed above .

Regarding the computation costs, the proposed scheme is more efficient than the previous related authentication schemes.

However, the scheme was demonstrated unsafe against password guessing attack and stolen-verifier attack and replay attack [33] .

In 2011, R. Arshad et al. [20] show that Tsai's authentication scheme is still unsafe against password guessing attack, stolen-verifier attack and does not provide perfect forward secrecy and known-key secrecy. They propose an efficient and secure authentication scheme based on elliptic curve discrete logarithm problem (ECDLP) which resist to the above attacks.

Regarding the computation costs, they demonstrate that the proposed scheme is faster than any other related authentication method.

Nevertheless, Arshad et al.'s authentication scheme is still vulnerable to off-line password guessing attack [15].

In 2012, Tang et al.[15] proposed a secure authentication scheme based on Elliptic Curve Discrete Logarithm Problem (ECDLP) .

However, the Tang et al.'s authentication scheme is still vulnerable to off-line password guessing attack and registration attack [35].

In 2012, Sadat et al.[35] Demonstrate that the Tang et al.'s SIP authentication schemes is still unsafe against to off-line password guessing attacks and registration attacks.

They proposed a new secure SIP authentication scheme based on ECC. They show that their scheme can resist the set of security services listed above.

Regarding The computation costs, they show that their method can provide high efficiency.

3.3 Authentication methods based on nonces

In 2008, Tsai [19] proposes a secure authentication scheme based on the random nonce. They demonstrate that there scheme provide a low computation cost and so it is very suitable for low computation equipment.

However, Tsai's scheme is still unsafe against some attacks such as off-line password guessing attacks, Denning- Sacco attack and stolen-verifier attacks.Also it does not provide perfect forward secrecy [18, 20].

3.4 Authentication methods based on identity-based encryption

ID authentication mechanism is generally based on a user identification parameters such as an email address, which it forms the public key of the user. The private key is generated from the user's public key by a trusted third party TTP (Trusted Third Party) and is safely imported to the user.

The main advantage of the ID authentication is that it does not suffer from security problems with passwords such as the HTTP Digest Authentication. And it avoids difficulties with PKI certificates. The only disadvantage of this method is long signatures.

In 2006, Ring et al. [21] proposes a SIP authentication scheme based on Identity-based cryptography. This method consist in computing the hash value of user's SIP identity as his public key without the need of concrete certificates.

This new scheme provides mutual authentication. However, it suffers from the heavy computation load [14].

In 2009, H.H. Kilinc [22] propose a new authentication scheme which combine the Elliptic Curve Digital Signature Algorithm (ECDSA) and the ID based authentication schemes of Hess [23] and Cha-Cheon [24] .

They show that there mechanism is significantly faster and resistant to attacks like password guessing attack, spoofing attack. However the disadvantages of this mechanism are seemed to be the large signature size.

In 2012, Rongwei Yu et al. [26] propose a secure identity-based scheme to solve the SIP authentication problem . Their scheme is based on signatures.

This solution can resist kinds of possible attacks .It also satisfies the property of perfect forward secrecy and provide a low computation cost.

3.5 Other authentication methods

In 2008, Cui Tao et al.[29]propose a mutual authentication scheme based on improved HTTP Digest authentication scheme.This solution consist in modifying Several values in digest headers of HTTP Digest authentication method such as the addition of shared key .

The proposed scheme can resist many attacks such as identity spoofing and Denial-of-service (DoS) attacks [30].

This scheme does not incur so much performance because it is based on Advanced Encryption Standard (AES) which provide speed and security at the same time.

In 2008, Geneiatakis and Lambrinoudakis [32] propose an authentication scheme based on improved HTTP Digest authentication. Their scheme introduce a new SIP header, that is the Integrity-Auth header, which can resist to signalling attacks. However, this method is still vulnerable to stolen- verifier attack and to the offline password guessing attack[14].

In 2009, Guillet and et al. [27] propose an authentication mechanism based on the HMAC One-time password authentication called HOTP. Their scheme is based on Challenge-Response model but it permits to reduce the handshakes to one only .this mechanism includes the password generated by HOTP in the user request SIP header.

The HOTP algorithm and the authentication with OTP's is very efficient, fast and resistant to the attack by brute force. The disadvantages of this solution are that authentication is a one way only and so it does not protect users against fraudulent access to the proxy server (the MitM attack). [28]

In 2009,Yi-Pin Liao and Wang [14] present a new secure authentication scheme for SIP using self-certified public keys (SCPKs)[31] on elliptic curves. The proposed scheme is based on the original SIP authentication scheme using SCPKs on elliptic curve for verification instead of password table. the proposed scheme can resist a set of attacks but the main advantages of this method is that it provides mutual authentication .

Regarding the computation cost , Liao and Wang‘s scheme has been demonstrated to be more efficient than the other’s . So it is very suitable to the low computation equipment.

In 2011, Lukas Malina, Vaclav Zeman [28,34] propose a solution for SIP authentication which is composed from an already proposed advanced authentication methods.For the authentication of users in the registeration phase, they have chosen to use Yoon and Yoo’s scheme based on ECDLP because this method provides a protection against the impersonating users and servers, help to avoid the difficulties associated with managing and importing certificates (PKI), and also ensure good security.

In the INVITE phase they have chosen to use the HOTP authentication mechanism presented by Guillet and et al. The combination of HOTP and ECDLP provides high security and good performance in the SIP architecture.

4. COMPARISON OF THE SIP AUTHENTICATION MECHANISMS

While providing the best security mechanisms for users, Quality of Service should also be considered in SIP authentication scheme.

In this section we compare between all the authentication methods presented above. We evaluate them in view of two requirements; security efficiency and computation costs.

This evaluation is summarized in table 1.

5. CONCLUSION

In this paper, We presented a survey of the newly SIP authentication mechanisms .we classified them by the security approach used in each one .then we evaluate theme in view of two requirements; security properties and computational cost.

We noted that all mechanisms presented above didn’t totally cover the two evaluation criteria which we defined; security efficiency and computational cost.

We noted also that some of these mechanisms didn’t take into consideration some other important requirements such as a total interoperability between equipments and also the easy deployment of the mechanism.

Our future work aims to propose a complete SIP authentication approach which covers all evaluation criteria mentioned above.furthermore it guaranties interoperability and easy deployment.

REFERENCES:

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, “SIP: Session Initiation Protocol.” RFC 3261 (Proposed Standard), June 2002. Updated by RFCs 3265, 3853, 4320, 4916, 5393.

[2] J. Postel, “User Datagram Protocol.” RFC 768 (Standard), Aug. 1980.

[3] J. Postel, “Transmission Control Protocol.” RFC 793 (Standard), Sept. 1981. Updated by RFCs 1122, 3168.

[4] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications.” RFC 3550 (Standard), July 2003. Updated by RFC 5506.

[5] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach,A. Luotonen, and L.Stewart, “HTTP Authentication: Basic and Digest Access Authentication.” RFC 2617 (Draft Standard), June 1999.

[6] W. Diffie, and M. Hellman, "New directions in cryptology," IEEE Transaction on Information Theory,vol. 22, no. 6, 1976.

[7] A. Dulanik and I. Sogukpinar, SIP Authentication Scheme using ECDH, in: Proc. Enformatika, vol. 8 (2005) 350 - 353.

[8] Eun-Jun Yoon; Kee-Young Yoo; , "A New Authentication Scheme for Session Initiation Protocol," Complex, Intelligent and Software Intensive Systems, 2009. CISIS '09. International Conference on , vol., no., pp.549-554, 16-19 March 2009

[9] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In Crypto 1984, pages 47–53. Springer-Verlag, 1984. Vol. 196/1985 of LNCS.

[10] D. Geneiatakis, A. Dagiouklas, G. Kambourakis, C.Lambrinoudakis, S. Gritzalis, S. Ehlert, D. Sisalem, “Survey of Security Vulnerabilities in Session Initiation Protocol”,IEEE Communications Surveys and Tutorials, vol. 8 (3), pp.68–81, IEEE Press, 2006.

[11] Chou-Chen Yang, Ren-Chiun Wang and Wei-Ting Liu, "Secure authentication scheme for session initiation protocol," Computers & Security, voL 24, pp. 381-386,2005.

[12] Heasuk Jo; Yunho Lee; Mijin Kim; Seungjoo Kim; Dongho Won; , "Off-Line Password-Guessing Attack to Yang's and Huang's Authentication Schemes for Session Initiation Protocol," INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on , vol., no., pp.618-621, 25-27 Aug. 2009

[13] C.C. Chang, Y.F. Lu, A.C. Pang, and T.W. Kuo, Design and Implementation of SIP Security, in: Proc. ICOIN 2005, Lecture Notes in Computer Science, vol. 3391 (Springer, Berlin, 2005) 669 - 678.

[14] Yi-Pin Liao a,b,*, Shuenn-Shyang Wanga, "A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves" Computer Communications, Volume 33, Issue 3, 26 February 2009, pp 372-380

[15] Tang H, Liu X , " Cryptanalysis of Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol". Multimed Tools Appl. 2012

[16] Liufei Wu a,b, , Yuqing Zhang b, Fengjiao Wang " A new provably secure authentication and key agreement protocol for SIP using ECC".Computer Standards & Interfaces 31 (2009) 286–291

[17] R. Canetti, H. Krawczyk, Analysis of key-exchange protocols and their use for building secure channels, in: P. fitzmann (Ed.), Proceedings of Eurocrpt'01, Lecture Notes in Computer Science 2045, Springer, Berlin, 2001, pp. 453–474.

[18] Eun-Jun Yoon; Kee-Young Yoo; , Cryptanalysis of NAKE Protocol based on ECC for SIP and Its Improvement, Second International Conference on Future Generation Communication and Networking Symposia,2008

[19] J. L. Tsai, Efficient nonce-based authentication scheme for session initiation protocol, International Journal of Network Security, vol. 8, no. 3, pp. 312- 316, May 2009.

[20] Arshad, R.; Ikram, N.; , "A novel mutual authentication scheme for session initiation protocol based on elliptic curve cryptography," Advanced Communication Technology (ICACT), 2011 13th International Conference on , vol., no., pp.705-710, 13-16 Feb. 2011

[21] Jared Ring, Kim-Kwang Raymond Choo, Ernest Foo, Mark Looi, A new authentication mechanism and key agreement protocol for SIP using identitybased cryptography, Proceedings of AusCert R&D Stream (2006) 61–72.

[22] H.H. Kilinc, Y. Allaberdiyev, T. Yanik. Performance Evaluation of ID Based Authentication Methods in the SIP Protocol. Application of Information and Communication Technologies (AICT), 2009.

[23] F. Hess, "Efficient identity based signature schemes based on pairings", Proceedings of the 9thWorkshop on Selected Areas in Cryptography, SAC 2002, LNCS 2595, pages 310-324, Springer-Verlag, 2003.

[24] J. Cha and J. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups", Proc. of PKC 2003, LNCS 2567, pp. 18-30, 2003

[25] "The Open SIP Server," OpenSIPS, 2011 [Online]. Available: http://www.opensip.org

[26] Rongwei Yu; Jie Yuan; Gang Du; Peng Li; , "An identity-based mechanism for enhancing SIP security," Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on , vol., no., pp.447-451, 22-24 June 2012

[27] Guillet, T.; Moalla, R.; Serhrouchni, A.; Obaid, A.; , "SIP authentication based on HOTP," In formation, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on , vol., no., pp.1-4, 8-10 ,Dec. 2009

[28] Lukas Malina, Vaclav Zeman "Comprehensive Security in SIP" elektrorevue ISNN 1213-1539 VOL. 2, NO. 1, APRIL 2011

[29] Cui Tao; Gao Qiang; He Baohong; , "A lightweight authentication scheme for Session Initiation Protocol," Communications, Circuits and Systems, 2008. ICCCAS 2008. International Conference on , vol., no., pp.502-505, 25-27 May 2008

[30] M. Luo, T. Peng, and C. Leckie. CPU-based DoS Attacks Against SIP Servers. In Proceedings of the IEEE Network Operations and Management Symposium (NOMS), pages 41–48, April 2008.

[31] Wang, Fengjiao; Zhang, Yuqing; , "A New Provably Secure Authentication and Key Agreement Mechanisms

Computational Intelligence and Security, 2007 International

Conference on , vol., no., pp.809-814, 15-19 Dec. 2007

[32] D. Geneiatakis, C. Lambrinoudakis, A lightweight protection mechanism against signaling attacks in a SIP-Based VoIP environment, Telecommunication Systems

[33] Xie Q "A new authenticated key agreement for session initiation protocol". Int J Commun Syst,2011

[34] YOON,RYU, YOO "Attacks and Solutions of Yang et al.'s Protected Password Changing Scheme", INFORMATICA, 2005, Vol. 16, No. 2, 285–294

[35] Sadat Yaghmaee- Moghaddam ,Ghaznavi-Ghoushchi, "Proposed SecureSIP Authentication Scheme based on Elliptic Curve Cryptography" International Journal of Computer Applications (0975 – 8887) Volume 58– No.8, November 2012

Table1: Comparison Of The Security Efficiency And Computational Cost Of The Different SIP Authentication Mechanism

Mechanisms	**Diffie-Hellman**	**Elliptic curve cryptography**						**Nonces**	**ID authetication**			**New SIP header**	**HOTP**	**SCPK**
	Yang [11]	**Durlanik[7]**	**Wu[16]**	**Yoon [18]**	**Arshad [20]**	**Tang [15]**	**Sadat [35]**	**Tsai[19]**	**Ring [21]**	**Kilinic [22]**	**Rongwei Yu[26]**	**Geneitakis [10]**	**Guillet [27]**	**Liao [14]**
Password guessing attack	insecure	insecure	Insecure	Insecure	insecure	insecure	secure	Insecure	insecure	secure		insecure	Insecure	secure
Denning sacco attack	insecure	insecure	secure	secure	secure	secure	secure	Insecure				insecure	Secure	
Stolen verifier attack	insecure	insecure	insecure	Insecure	secure	secure	secure	Insecure				insecure	Insecure	
Registration attack	insecure	insecure		insecure	insecure	insecure	secure	insecure			secure		Insecure	
Mutual authetication	provided	Provided	Provided	Provided	Provided	Provided	Provided	Provided	Provided	Provided	Provided	Not Provided	Not Provided	Provided
Session key security	Not applicable	Provided	Provided	Provided	Provided	Provided	Provided	Provided	Provided	Provided		Not Provided	Provided	Provided
Known Key secrecy	Not applicable	Provided	Provided	Provided	Provided	Provided	Provided	Not applicable			Provided		Provided	
Perfect forward secrecy	Not applicable	Provided	Provided	Provided	Provided	Provided	Provided	Not Provided	Not Provided	Not Provided	Provided	Provided	Provided	Provided
Replay attack	secure	secure	secure	secure				secure			secure	Secure	secure	
Man in the Middle	secure	secure	secure	secure							secure	Secure	insecure	
Computation cost	High	low	low	low	low	low	low	low	high	high	low	low	low	low