Authentication Protocol for VoIP based on Elliptic Curve Cryptographic Primitives

Zamudio S. Luis[1], Gallegos-García. Gina[2] and Aguilar T. Gualberto[3]

[1, 2] Instituto Politécnico Nacional. ESIME Culhuacan. México
lzamudios0800@egresado.ipn.mx, ggallegosg@ipn.mx
[3] Comisión Nacional de Seguridad México
autg79y@yahoo.com

Abstract. This article presents the design and development of a new authentication protocol for the Voice over Internet Protocol service, on mobile devices. The proposal is different from the actual ones in four key aspects: uses Elliptic Curve Cryptography primitives; works independently from the SIP protocol messages; authentication is not centralized and is not necessary additional hardware to basic VoIP infrastructure. As a consequence, the advantages of the proposed protocol are the following: lower computational cost, no storage of information related to session keys on any device, the minimum infrastructure is needed and the messages exchanged for authentication are transmitted by a different channel from the signaling one. Due to SIP protocol is conditioned upon verifying digital signature and key exchange, generated independently by mobile devices, the results show that a session is not established unless the devices authenticate each other and that the messages for authentication are recognized as CISCO-CSP by a sniffer.

Keywords: Authentication, Diffie – Hellman, Digital Signature, Elliptic Curve Cryptography, Session Initiation Protocol

1 Introduction

During the last decade, communications have boomed and society is becoming more and more interconnected. At the same time, the growing rate in the use of mobile devices and overlapping services is increasing. This is the case of Voice over Internet Protocol (VoIP), a service that grows fairly rapidly and it is believed that in future, will completely replace the traditional Public Switched Telephone Network service (PSTN) [1].

One of the protocols used in VoIP, for signaling, monitoring and session control, is the Session Initiation Protocol (SIP), which was chosen, by the Third Generation Partnership Project (3GPP) [2], as a multimedia protocol for mobile applications and as a proof of the great use and popularity it has gained. However, due to SIP is a protocol for generic use [3] and not specific to VoIP, it is exposed to a variety of security threats, such as: attacks of fake user authentication and impersonation, two issues that have raised various solutions,

since it is expected that the VoIP service provides the equivalent security and privacy level than the PSTN [4].

The SIP protocol is a protocol that sends messages in plain text and uses Hyper Text Transfer Protocol (HTTP) digest authentication scheme, which on one hand has a very high computational cost and on the other hand, it is also vulnerable to man in the middle attacks and false authentication [5]. Considering the aforementioned it is necessary to develop an efficient and secure way of authentication, applicable in VoIP.

In that sense, many schemes for authentication, based on cryptographic algorithms, have been developed. Most of these schemes [6] use centralized servers for authentication, store pre-configured security and key session information and the messages exchanged to accomplish authentication are transmitted within SIP requests through the same signaling channel.

In this paper, a decentralized protocol, but controlled by mobiles devices, is proposed. It makes use of digital signatures and key exchange algorithms on elliptic curves, subjecting the SIP protocol to the successful key exchange and signature verification.

The reminder of this article is as follows: Section 2 gives an introduction to Elliptic Curve Cryptography and the SIP protocol within the VoIP service. In Section 3, related work that has addressed the problem of SIP authentication using additional infrastructure, pre shared security parameters or authentication messages within the SIP protocol using the same signaling channel, is analyzed. Our proposed protocol is presented in Section 4. In Section 5, the proofs are detailed. In section 6 the analysis and discussion are presented. Finally, Section 7 shows conclusions and future work.

2 Background

In this section, we explain the SIP structure and its original authentication scheme, which is based on the HTTP digest [21]. It is also important to understand the Elliptic Curve Cryptography (ECC); particularly the Elliptic Curve Diffie Hellman (ECDH) and the Elliptic Curve Digital Signature Algorithms (ECDSA).

2.1 SIP Protocol, Structure and Original Authentication Scheme.

The Session Initiation Protocol (SIP) is a signaling protocol designed for handling and managing multimedia sessions between two or more parties in a VoIP call. In 2002, it was improved for last time by the Internet Engineering Task Force (IETF), becoming the current RFC3261 standard [5]. To understand the use of the SIP protocol [9], Figure 1 shows the standard flow of a VoIP call that uses SIP to manage the session.

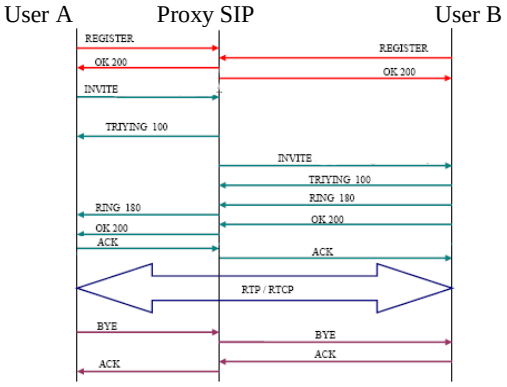

Fig. 1. The flow establishment of VoIP call

The SIP is located in the seventh layer of OSI reference model and runs over TCP transport layer to ensure session establishment [8]. It handles location of users, service quality negotiation for the call, and manages the transfer, modification and completion of sessions [7]. The SIP processing call is based on the client-server architecture and the request-response messages are similar to HTTP or the Simple Mail Transfer Protocol (SMTP) syntax.

Although the original SIP protocol authentication scheme relays on application layer and is based on the HTTP authentication [5], the authentication can be enabled at different layers, including application layer, transport layer and network layer. Along with HTTP, a challenge-response mechanism [5] and Secure/Multi Internet Mail Extensions (S/MIME) protocol are used to provide authentication to SIP Protocol in application layer. Finally there is the Secure Internet Protocol (IPSec) and Transport Layer Security (TLS) that encrypt the messages in transmission layer [9].

2.2 Elliptic Curve Cryptography, ECDH and ECDSA

Elliptic Curve Cryptography (ECC) has extended its use in the past 30 years. Due to its large number of applications, it has been used in mobile devices to meet security requirements in a more robust way. ECC theory is underlined in elliptic curves, defined on finite fields. The main impact of elliptic curves in cryptography is the substantial key size reduction and the lower computational cost due to the operations rely on additive groups [10]. Because of this, the computational benefits, such as reduced memory usage, faster processing and saving bandwidth, ECC fits perfectly in wireless environments and mobile devices. ECC has the versatility to be used in various applications. Figure 2 shows the layers of operation on ECC [11].

The Elliptic Curve Digital Signature Algorithm (ECDSA) [12] is the elliptic curve analogue of the Digital Signature Algorithm (DSA). The Elliptic Curve Diffie Hellman Algorithm (ECDHA) [13] is the adaptation to elliptic curves from the original Diffie Hellman Algorithm.

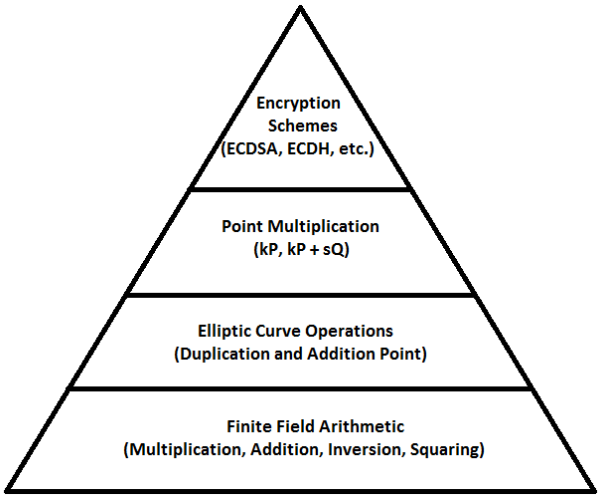

Fig. 2. Branches of Elliptic Curve Cryptography

3 Related Work

The focus of the researches has been divided into four main aspects [14]; proposals based on the Password Authenticated Key Exchange (PAKE); HASH and Symmetric Cipher; Public Key Cryptography (PKC) and ID based schemes. For present work, only the PAKE schemes are subject of study. Within PAKE schemes, there are six main schemes, the first is developed by Yang [15], the second one is proposed by Durlanik and Sogukpinar [16], the third one, proposed by Wu is detailed in [17], the forth scheme is developed by Yoon and Yoo [18], the fifth one is proposed by Qiong Pu and Shuhua Wu in [19] and the last one is shown in [20] and proposed by Shaohui Zhu.

In [15], Yang proposed a scheme with a new way of authentication based on the DH key exchange protocol. This scheme is very close to the original EKE scheme, with the only difference that the encryption part is replaced with an exclusive OR operation and it involves the hash value of the pre-shared password. It means that in step 1 and 2 of EKE in [14], the $Epwd(tx)$ information is replaced with $tx \oplus F(pwd)$. Moreover, in step 2, instead of encrypting a challenge with the session key *K*, the hash value of the session key, together with tx expressed as $F(tx, K)$, is sent by the server.

Authentication is made when the client compare received hash value against a calculated hash value, which the client is capable of calculating after step 2. The advantage of this scheme is the low computational cost in comparison to the EKE scheme. It is due to the encryption and decryption operations are replaced with exclusive OR operations.

Durlanik and Sogukpinar in [16] proposed a new authentication scheme based on ECDH. This is an extension of the EKE and a much closed approach to the Yang´s scheme. The

assumption for this scheme is that both, the server and the client, have a pre-shared password and a public key pair generated by an elliptic curve algorithm. The exclusive OR and classical encryption operations are replaced with elliptic curve encryption operations. The advantage of this scheme is the decreasing total execution time and memory requirement which is good for mobile devices. It is vulnerable to Denning Saco Attack, Offline Guessing Password Attack, Replay Attack and Stolen Verifier Attack.

In [17], Wu proposed the New Authenticated Key Exchange Protocol (NAKE) based on elliptic curve cryptography. The scheme is very similar to Durlanik and Sogukpinar´s scheme, but Wu´s scheme assumes that the client and the server have already agreed upon a password, a hash function and a base point. In step 2 and 3, it uses a random number and two parameters that represent the identities of the server and client. It also uses a session identifier. In addition to that it is vulnerable to Offline Guessing Password Attack and Brute Force attack.

Yoon and Yoo proposed in [18] an authentication scheme based on ECDLP using ECDH. The scheme consists of three phases: system setup, registration and authentication. The assumption for this scheme is that the client and the server have already exchanged messages over a secure channel to establish a shared secret, which is used to compute an elliptic curve point as secret value. This proposal is vulnerable to the Offline Guessing Password Attack.

Qiong Pu´s and Shuhua Wu´s Scheme in [19] show an improvement of [18]. The first two phases are very similar except for there is no shared secret, it is a full domain hash function and also a public parameter. The scheme is vulnerable to Online Guessing Password Attack.

Shaohui Zhu proposes in [20] a scheme that consists of three phases: authentication key agreement, voice data encryption and session key update. The key agreement is made by using a modification of ECDH along with time stamp validation.

4 Proposed Protocol

The proposed protocol differs from the related work in three main aspects: the use of a different channel from the signaling one for authentication messages exchange, there is no necessity of additional infrastructure to basic VoIP infrastructure and the use of a pre shared patron instead of pre shared passwords or configuration tables. All of them are numerated as follows.

4.1 Proposed Protocol Features

1. - The authentication is made independently from the SIP requests inside signaling channel. The exchanged messages for the authentication are transmitted by an UDP socket when the INVITE SIP message is sent by the caller. After this, the SIP requests are blocked and only the required messages for authentication are exchanged. When the authentication is completed, the SIP requests continue the normal flow as in a VoIP call.

2. - There is no need of additional infrastructure. The calculations and operations are made at each end mobile device, which do not storage additional configuration or information for each SIP session. Each session uses a different key. The proposed protocol uses End to End architecture.

3. - The use of a pre shared patron, not a pre shared password or configuration tables. It is used to verify the signature and the validity of the key agreement.

4.2 Protocol Description

The proposed protocol can be divided into three phases: key generation for ECDSA and ECDH, signature generation of ECDH and signature verification.

4.2.1 Key Generation

1) The INVITE SIP message, works as a trigger. Once this message is detected, user A named as the caller catches it and keeps it in stand by while the proposed protocol works. It is important to mention that the initial parameters for the ECDSA and ECDH are defined by the user who initiates the call (user A).

2a) User A executes ECDSA [12] in the following order using the initial domain parameters $D = (q, a, b, P, n)$, pre shared message *m* and the private key d_{A1} randomly selected in the interval [1,*n*−1]. The public key P_{A1} is a point in the elliptic curve equation $Eq(a, b)$ and is computed according to Equation (1).

$$P_{A1} = d_{A1}\, x\, P \tag{1}$$

2b) Initially user A calculates the HASH value of the pre shared message $e = H(m)$ and selects a cryptographically secure random integer $k \in R$ [1,*n*−1], which later, is used for calculation of the curve point kP according to Equation (2).

$$kP = (x1, y1) \text{ and convert } x1 \text{ to an integer } \overline{x1}. \tag{2}$$

2c) Computes the first component, *r* of the signature in Equation (3).If *r* = 0 then select another *k*

$$r = \overline{x1} mod\ n. \tag{3}$$

2d) Computes the second component *s* of the signature according to Equation (4).
If *s = 0* then select another *k*

$$s = k^{-1}(e + d_{A1} r)\ mod\ n. \tag{4}$$

If *s* and$r \neq 0$, then the signature is the pair (r,s)**.** After generation of keys and signature of ECDSA, user A then executes ECDH [13] in the following order using initial domain parameters $D = (q, a, b, P, n)$,. Calculates its private keyd_{A2}, which is an integer less than *n* using the private key d_{A1} as seed.

2e) Calculates the public key P_{A2} as is shown in Equation (5), which is a point in $Eq\ (a, b)$.

$$P_{A2} = d_{A2}\ x\ P \tag{5}$$

4.2.2 Diffie – Hellman Signing

1) User A signs the result of its ECDH calculation according to Equation (6) and sends it to user B named as the callee, along with both public keys $P_{A1,}\ P_{A2.}$

$$S(DH)\ d_{A1} \tag{6}$$

4.2.3 Signature Verification

1) User B receives the messages sent by user A, and verifies the signature using the pre shared message and the public key P_{A1} along with the domain parameters of the curve, but first, user B must verifies that P_{A1} is a valid curve point, by extracting the initial parameters of the curve definition and checking three conditions:

- P_{A1} is not equal to the identity element O , and its coordinates are otherwise valid
- Check that P_{A1} lies on the curve
- Check that *n* $P_{A1} = O$

2) After that, user B computes the Hash value of the message $e = H(m)$ and verifies that *r* and *s* are integers in the interval [1,*n*−1]. If any verification fails then return "Reject the signature"

2a) Calculates the inverse and modular operation *n* of the first component of the signature *s* according to Equation (7)

$$W = s^{-1} mod\ n. \tag{7}$$

2b) Then Computes the *x*-coordinate as seen in Equation (9) using the two components $u1, u2$ from Equation (8), public key P_{A1} and base point .

$$u1 = ew\ mod\ n;\ u2 = rw\ mod\ n. \tag{8}$$

$$X = u1P + u2\ P_{A1}. \tag{9}$$

2c) If X =∞ then return "Reject the signature"; and the VoIP call finishes. Otherwise, convert the *x*-coordinate $x1$ of X to an integer $\overline{x1}$, which is used to calculate the verification *v* of the second component of the signature according to Equation (10)

$$v = \overline{x1}\ mod\ n. \tag{10}$$

2d) If $v = r$ then return "Accept the signature" and the VoIP session continues by User B doing the same actions as User A in steps 1, 2 and 3. If else, return "Reject the signature".

Assuming the valid signature, user B executes Key Generation and Diffie – Hellman Signing phases in the same way as user A. For Key Generation phase (section 4.2.1), executes

ECDSA and ECDH to generate its private keys d_{B1}, d_{B2} and public keys P_{B1}, P_{B2}. At this point, user B has already calculated the Key Agreement.

For Diffie – Helmman Signing phase (section 4.2.2), user B encrypts the pre shared message with the generated key agreement and also signs the DH calculation, then send them to user A along with its public keys P_{B1} and P_{B2}.

Finally, user A receives and verifies the signature of the DH result of user B in the same way user B verified the signature (section 4.2.3). If the signature is not valid, the VoIP call is finished. If the signature is valid, then generates the key agreement and decrypts the pre shared message with its key agreement to validate it is correct.

If the key agreement is correct, the SIP message INVITE, continues the normal flow of a VoIP call. If the key agreement is corrupt the VoIP call finishes.

5 Tests

In order to proof our proposed protocol, a softphone was developed for Android mobile devices, compatible with versions from ICS 4.0 to Kit Kat 4.4.

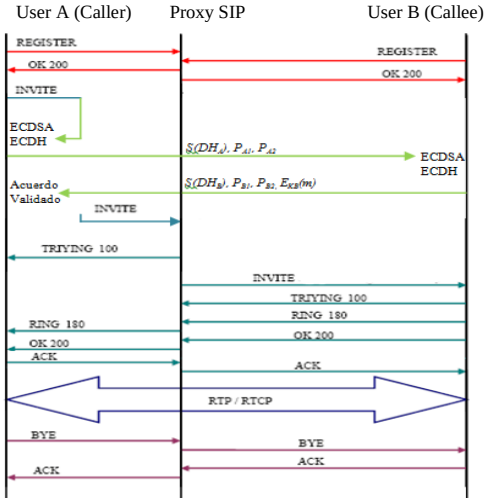

Fig. 3. The flow of the Proposed Protocol for a VoIP call

5.1 Test Scenario

The mobile devices used for testing were: Motorola X, Samsung S5, Sony Xperia SP and HTC One. Figure 4 shows the scenario proposed for the test; it is a self-hosted infrastructure, composed by a PBX server running Elastix, one CISCO router working also as an access point, four mobile devices and one attacker monitoring and eavesdropping the network.

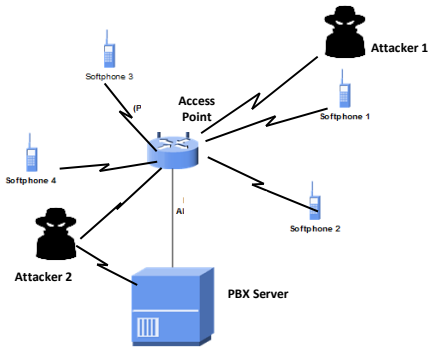

Fig. 4. Self-Hosted Scenario for testing

For the proposed scenario, two mobile devices were installed with a commercial softphone, and two other mobile devices with the developed softphone that includes the proposed protocol. Is assumed that the attacker is able to capture and eavesdrop the traffic.

For the first test, two calls were made. Figure 5 shows the flow of a VoIP call between two devices using our proposed protocol. In this case, due to the users authenticate correctly, the session is established and the VoIP call flows in a normal way. For the second test, it is supposed, that an attacker has already stolen the registration password of another user and try to make a call using its own softphone, as seen in Figure 6, the call is not established. The SIP session is finished after the TRYING and RINGING messages because the authentication protocol is not completed successfully.

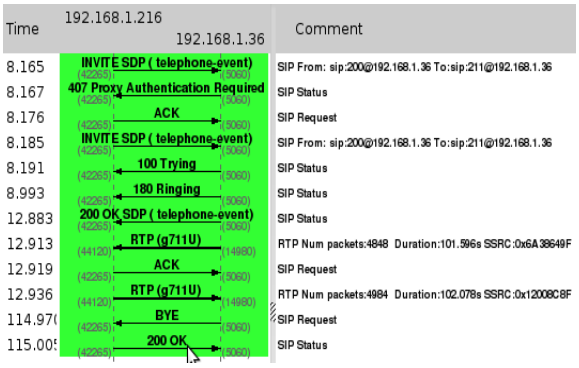

Fig. 5. SIP Session between devices using the proposed protocol

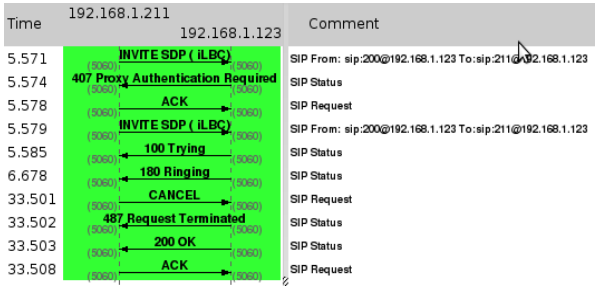

Fig. 6. SIP Session between a device using our proposed protocol and other device using a commercial softphone.

For the third test, the behavior of the two softphones, before, during and after the session was analyzed. Using the Nmap scanner, the following ports and services where identified. In Figure 7, the SIP Ports for the commercial softphone is opened before and during the session establishment. In Figure 8, the ports used for SIP communication, are closed before the session establishment but open only after the session has already been established.

```
# Nmap 6.47 scan initiated Sun Apr 19
14:27:58 2015 as: nmap -vv -sS -p 5060,5061
-oN
/root/Desktop/IdentificaciÃ³nPuertosMIS123T
CPSIP.txt 192.168.1.123
Nmap scan report for 192.168.1.123
Host is up (0.0053s latency).
Scanned at 2015-04-19 14:27:58 CDT for 3s
PORT     STATE    SERVICE
5060/tcp open sip
5061/tcp filtered sip-tls
MAC Address: 00:24:1D:7D:15:67 (Giga-byte
Technology Co.)
Read data files from:
/usr/bin/../share/nmap
# Nmap done at Sun Apr 19 14:28:01 2015 --
1 IP address (1 host up) scanned in 2.44
seconds
```

```
# Nmap 6.47 scan initiated Sun Apr 19
14:37:58 2015 as: nmap -vv -sS -p 5060,5061
-oN
/root/Desktop/IdentificaciÃ³nPuertosMIS123T
CPSIPON.txt 192.168.1.123
Nmap scan report for 192.168.1.123
Host is up (0.0053s latency).
Scanned at 2015-04-19 14:27:58 CDT for 3s
PORT     STATE    SERVICE
5060/tcp open sip
5061/tcp filtered sip-tls
MAC Address: 00:24:1D:7D:15:67 (Giga-byte
Technology Co.)
Read data files from:
/usr/bin/../share/nmap
# Nmap done at Sun Apr 19 14:40:25 2015 --
1 IP address (1 host up) scanned in 147.66
seconds
```

Fig. 7. SIP ports on commercial softphone before/during session establishment

```
# Nmap 6.47 scan initiated Sun Apr 19
14:06:32 2015 as: nmap -vv -sS -p 5060,5061
-oN
/root/Desktop/IdentificaciÃ³nPuertosMIST216
TCPSIP.txt 192.168.1.216
Nmap scan report for 192.168.1.216
Host is up (0.094s latency).
Scanned at 2015-04-19 14:26:48 CDT for 0s
PORT     STATE  SERVICE
5060/tcp closed sip
5061/tcp closed sip-tls
MAC Address: F8:E0:79:5D:8E:54 (Motorola
Mobility)
Read data files from:
/usr/bin/../share/nmap
# Nmap done at Sun Apr 19 14:18:06 2015 --
1 IP address (1 host up) scanned in 694.53
seconds
```

```
# Nmap 6.47 scan initiated Sun Apr 19
14:24:51 2015 as: nmap -vv -sS -p
5060,5061 -oN
/root/Desktop/IdentificaciÃ³nPuertosMIST21
6TCPSIP.txt 192.168.1.216
Nmap scan report for 192.168.1.216
Host is up (0.094s latency).
Scanned at 2015-04-19 CDT14:26:48  for 0s
PORT     STATE  SERVICE
5060/tcp open sip
5061/tcp closed sip-tls
MAC Address: F8:E0:79:5D:8E:54 (Motorola
Mobility)
Read data files from:
/usr/bin/../share/nmap
# Nmap done at Sun Apr 19 14:25:05 2015 --
1 IP address (1 host up) scanned in 15.02
seconds
```

Fig. 8. SIP ports on developed softphone before/during session establishment

6 Discussion

From the proposed protocol we can highlight some key aspects in comparison with Yang [15], Durlanik and Sogukpinar [16], Wu [17], Yoon and Yoo [18], Qiong Pu and Shuhua Wu [19] and Shaohui Zhu [20] schemes.

6.1 Key Aspects of the proposed protocol

Related work use cryptographic algorithms, SIP requests are used for sending and receiving authentication messages. In other words, the information is transmitted within the SIP messages in plain text and is vulnerable for eavesdropping. As a consequence it can be used for guessing the passwords or redirecting the key information. Also, some of these schemes need additional infrastructure like an Authentication Server. This server storages configuration of pre shared passwords or key configuration tables, causing not only false authentication but also adding vulnerabilities like off line passwords attacks or replays attacks. Table 1 summarizes a comparison of these key aspects.

Table 1. Comparison with proposed protocol and actual proposed schemes

Feature	Our Proposed protocol	Related Work
Authentication messages transmission	Independent from SIP. Using an UDP Socket.	Dependent on SIP Using the signaling channel
Authentication Process	Before setting session with SIP protocol.	During session establishment with SIP protocol.
Authentication infrastructure	No needed	Authentication servers
Authentication Information	Not pre-configured or pre shared	Use of configuration and key tables

6.2 Analysis and Discussion

Since authentication and key exchange messages in our proposed protocol are transmitted independently from SIP protocol requests, if an attacker is listening to the channel to capture SIP communication, he will not find relevant information within SIP communication that lets him guess the session key or modify information on digital signatures, on the contrary he would have to analyze all UDP traffic obtained from isolation to SIP.

It is important to mention that method used for authentication and key agreement is known as Signed Diffie – Hellman for multiplicative groups, and according to [22] it is vulnerable to a replay attack. Since user identity is not known, an active attacker could replace the signature of a user with its own signature. In additive groups there is no certainty that this could happen. In [12] is mentioned that even though and attacker be able to obtain signatures of messages from the legitimate signer, if he has not request the new message and obtain the signature he will not be able to produce a valid signature used for fake authentication.

7 Conclusion

We conclude that for an attacker to success on impersonating a valid user, he will need to: analyze all UDP Traffic instead of only SIP, identify the port used for authentication and

request the original signer to send him a new message, so that he could generate a new valid signature. Even if he gets a new valid signature, he would need to get the pre shared patron for verifying the signature, which means hacking the mobile device, not the network traffic. Also, by using only basic VoIP infrastructure and conditioning SIP functionality, the replay and message modification attacks are not feasible.

For future work there is the need of modeling different scenarios of attacking to identify vulnerabilities of the protocol and make the necessary hardening. Also this authentication protocol could also be the base for a secure key establishment and then both parties of the call could encrypt the flow of RTP to provide confidentiality of the call.

Acknowledgments
The authors thank the Instituto Politecnico Nacional and the Consejo Nacional de Ciencia y Tecnologia. The research for this paper was financially supported by Project Grant No. SIP-2014-RE/123, CONACyT 216533.

References

1. ITU. (2010). Measuring the Information Society [Online]
2. IETF. (2005). RFC 4083, Input 3GPP 5 requirements on the SIP. [Online]
3. Pierre Lascuyer, *"Evolved UMTS Architecture" in* Evolved Packet System, the LTE and SAE Evolution of 3G UMTS, 1st Ed, Ed Willey, 2008.
4. Travis Russell, "*Security in a SIP Network" in* Session Initiation Protocol (SIP): Controlling Convergent Networks, 1st Ed, Ed, Mc Graw Hill: 2008.
5. IETF. (2002). RFC 3261, Session Initation Protocol. [Online]
6. H. Hakan Kilinc and Tugrul Yanik, "A Survey of SIP Authentication and Key Agreement Schemes". IEEE. 2013
7. *Specialized Forum on VoIP Telephony*, Foro VoIP: http://voipforo.com/
8. Larry Chaffin, "*SIP Architecture" in* Building a VoIP Network with Nortel´s Multimedia Server 5100, 1st Ed. Ed. Syngress, 2006, pp345 -384.
9. IETF. (2003)RFC 3665, Session Initiation Protocol Basic Call Flow Examples. [Online].
10. Julio Lopez and Ricardo Dahab, "An overview of Elliptic Curve Cryptography", Citeseer, 2000.
11. Lawrence C. Washington. "*Elliptic Curve Crptography*" in Elliptic Curves, Number Theory and Cryptography, 2nd Ed. Ed. CRC – Press. 2008, pp. 169-187.
12. Darrel Henkerson, *"Cryptographic Protocols" in* Guide to Elliptic Curve Cryptography, 1st Ed. Ed. New York: Springer, 2004, pp 153-196.
13. William Stallings, Cryptography and Network Security, 5th Ed. Ed. Prentice Hall, 2011.
14. S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password based Protocols Secure against Dictionary Attacks". IEEE. 1992

15. C.-C. Yang *et al*, "Secure Authentication Scheme for Session Initiation Protocol" Elsevier. 2004.
16. A. Durlanik and I. Sogukpinar, "SIP Authentication Scheme using ECDH" World Academy of Science, Engineering and Technology, 2005.
17. L. Wu, *et al*, "A New Provably Secure Authentication and Key agreement protocol for sip using ecc," National Natural Science Foundation of China, 2007.
18. E.-J. Yoon and K.-Y. Yoo, "A New Authentication Scheme for Session Initiation Protocol" IEEE. 2009.
19. Qiong Pu and Shuhua Wu, "Secure and Efficiente SIP Authentication Scheme for Converged VoIP Networks", The international Arab Journal of Information Technology, 2010
20. Shaohui Zhu, *et al* "ECC-based Authenticated Key Agreement Protocol with Privacy Protection for VoIP Communications", IEEE. 2013
21. IETF (2002). Enhanced Usage of HTTP Digest Authentication for SIP [Online]
22. Hugo Krawczyk, (2003), "SIGMA: The 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols", *Advances in Cryptology: 23rd Annual International Cryptology Conference,* [Online], pp. 400-425.