International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:8, 2007

SIP Authentication Scheme using ECDH

Aytunc Durlanik, and Ibrahim Sogukpinar

***Abstract*—**SIP (Session Initiation Protocol), using HTML based call control messaging which is quite simple and efficient, is being replaced for VoIP networks recently. As for authentication and authorization purposes there are many approaches and considerations for securing SIP to eliminate forgery on the integrity of SIP messages. On the other hand Elliptic Curve Cryptography has significant advantages like smaller key sizes, faster computations on behalf of other Public Key Cryptography (PKC) systems that obtain data transmission more secure and efficient. In this work a new approach is proposed for secure SIP authentication by using a public key exchange mechanism using ECC. Total execution times and memory requirements of proposed scheme have been improved in comparison with non-elliptic approaches by adopting elliptic-based key exchange mechanism.

***Keywords*—**SIP, Elliptic Curve Cryptography, voice over IP.

I. Introduction

DEPLOYMENT of VoIP in data networks brings out the popularity of Remote Distance Telephony Services like pre-select services, ip2ip communications, etc. also for end-users besides commercial companies. Mostly H323 and SIP protocol stacks has been implemented in the rate of %95 over the VoIP networks which have been widely used all over the world. Although the H.323 protocol has been standardized and H.235 security considerations are involved in it, complexity and performance issues needs H.323 protocol stack to be questioned. On the other hand SIP, which is originally developed by the IETF Multi-Party Multimedia Session Control Working Group, known as MMUSIC [1], incorporates elements of two widely used Internet protocols: Hyper Text Transport Protocol (HTTP) used for Web browsing and Simple Mail Transport Protocol (SMTP) used for e-mail which are pretty understandable and plain protocols.

While comparing with the legacy networks like TDM, SIP based next generation networks give the advantages of IP voice, Web enabled control, Open and standard based features and converged network capabilities. On the other hand while comparing SIP with the other VoIP protocols it's seen that simplicity, new developments, intelligent endpoint structure complements SIP with other IP based voice protocols.

Authors are with the Department of Computer Engineering, Gebze Institute of Technology, Istanbul Caddesi No: 101, Gebze, Kocaeli, Turkey (e-mails: aytunc@gmail.com, ispinar@bilmuh.gyte.edu.tr).

As for Security Considerations of SIP; some vulnerabilities like DOS attacks, firewall NAT issue, session teardown, offline-password guessing attacks, replay attacks, server spoofing, registration hijacking are considered and researched in various works. Many applications that are used SIP are robust against to many DOS attacks [2]. It's seen that; by using discrete logarithm problem and Diffie Hellman approach [3], it becomes infeasible to impersonate the UAS and prevention from offline-password guessing and replay attacks are obtained [4].

While providing the best security mechanisms for users, Quality of Service should be considered also for VoIP networks. In this instance; a secure authentication scheme demands faster session initiation, call progress and server/client calculations. On the other hand Elliptic Curve Cryptography (ECC) provides smaller key sizes and faster calculations than legacy public key infrastructures at the same security levels. Smaller key sizes are more advantageous while implementing the applications to hand-held devices by means of memory requirements and storage disquietudes.

In this work a new approach is proposed for Session Initiation protocol to combine these two requirements: Security&QoS for Session Initiation Protocol at one outline. While keeping the same characteristics of public key structure for securing the authentication process, an optimization for memory needs, storage requirements and processing delays shall be examined. Well-known pros of ECC like small-key sizes and faster computations directly meet these criteria's.

II. SIP Architecture and Security Considerations

By the use of Uniform Resource Locators (URL's) and Uniform Resource Identifiers (URI's), SIP has the client-server features of HTTP. On the other hand a text-encoding scheme and header format are proposed as in SMTP. For example, SIP reuses SMTP headers such as To, From, Date, and Subject.

SIP can be introduced by 4 local entities which are User Agent Client (UAC), User Agent Server (UAS), Registrar and Proxy. Generally a SIP enabled device can be expressed as User Agent. This User Agent has a client and server application. A UAC makes requests and a UAS response to these requests. A SIP registrar responds to a message contains registration request and also updates its database to route the requests. As a responder it is seen that a SIP registrar is also a UAS. A SIP proxy same as HTTP proxy just forwards the messages and request but it does not generate or terminate a session.

INVITE, REGISTER, BYE, ACK, CANCEL and OPTIONS messages are the six original SIP messages in the protocol stack. On the other hand REFER, SUBSCRIBE,

NOTIFY, MESSAGE, UPDATE, INFO, and PRACK messages are other optional messages described in other RFC's.

A simple SIP registration and session are presented in the Fig. 1 and Fig. 2.

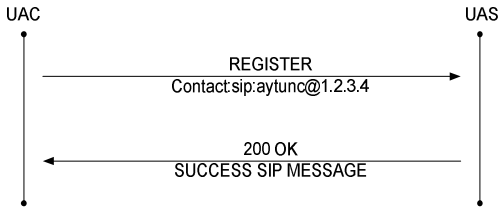

Fig. 1 SIP Registration

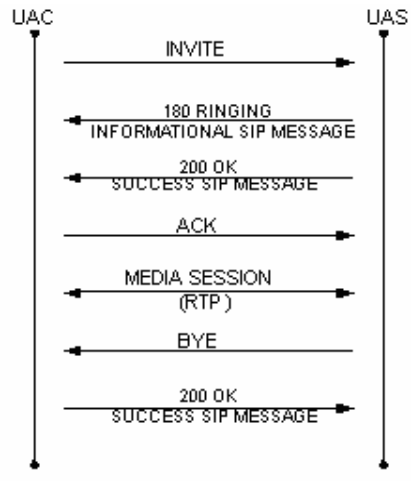

Fig. 2 SIP Session

SIP authentication can be examined in two different forms. In the first form a SIP user agent can authenticate by a proxy, redirect or registrar server. In the other way a SIP user agent can authenticate with another SIP user agent. There are many approaches in SIP authentication but in general there's a lightweight registration depending on a challenge/response mechanism and a more powerful authentication including some cryptographic functions and encryption mechanisms. Encryption based schemes are beyond the scope of this document.

In a proxy required HTTP Digest authentication scheme, [5] call flow can be expressed as follows;

- UAC sends a unauthenticated INVITE
- Proxy responds to this INVITE with a Proxy Authentication required message
- UAC sends An ACK then another INVITE including an authentication header.
- UAS sends back a authorization required message and expect a brand new INVITE including the authorization header.
- UAC again sends a new INVITE including the authorization header.

The whole scheme based on the challenge-response architecture that necessitates a pre-shared password. That scheme can verify the identity of the client. Due to the weaknesses of this scheme including Off-line password guessing attacks, server spoofing and replay attacks, a new security scheme has been proposed to eliminate these features.

In this structure, UAC sends a Request message (1) to UAS including the username, password and a random number r as in statement (1).

$$\text{Request; username, } t_1 \otimes H(\text{passwd}) \quad (1)$$

t_1 value is calculated by using the domain parameters of Diffie Hellman which are p and g. Then the UAS returns a challenge message (2) after Request has received. UAS also calculates a t_2 value same as UAC does. The Challenge message body will be as shown in (2);

$$\text{Challenge; realm, } t_1 \otimes H(\text{password}), H(t_1, K) \quad (2)$$

Challenge message presented in statement (2) has a K value presents a session key and includes both UAC's and UAS's randomly chosen secret value r_i. In normal HTTP Digest Authentication an attacker may try to impersonate the server by getting the realm and guessing the password. But in this Diffie Hellman approach it would be infeasible to calculate session key K because of extreme difficulty of discrete logarithm problem. After the Challenge, UAC make computations to verify the Session key and authenticates the UAS. A response then generated by UAC and transmitted to UAS as statement (3);

$$\text{Response; username, realm, } H(\text{username, realm, K}) \quad (3)$$

After UAS receives the Response message it computes the hashed value of username, realm and K and compares the value as in the transmitted Response message.

Because of the protocol depends on HTTP features, there are some other authentication approaches besides digest authentication. As a least secure solution; basic authentication [6] can be used. In this scheme username and passwords are transmitted as plaintext through the client/server that makes the user disinclined to use this mechanism.

Another approach NTLM (NT LAN Manager) is an authentication protocol used in various Microsoft network protocols for authentication purposes. NTLM uses a challenge/response mechanism different form other protocols [7]. In this scheme a client can prove its identity to the server without sending the password to the server.

In parallel to the HTTP Digest Authentication [8] and secure authentication scheme that has been proposed by Yang et. all. [4], Elliptic Curve Diffie-Hellman (ECDH) key exchange can also be adopted for SIP Authentication purpose.

III. ECDH Approach for Secure SIP Authentication

Today, three main mathematical problems that are Integer Factorization, Discrete Logarithm Problem and Elliptic Curve Discrete Logarithm Problem are constructing cryptographic structures. The main advantage of Elliptic Curve Cryptography (ECC) is the suggestion of smaller and faster public key

systems at the same constrained security levels. These features lead ECC into a position where low bandwidth and low memory criteria's are considerable.

In this proposed scheme, SIP Client and SIP server has a pre-shared "password" for authorization purpose. Both the server and client has an elliptic curve public key pair, while "d" represents the private key and "Q" the public key. "G", base point in the curve, a, b are coefficients, "q", the field, "h", the cofactor, "n" is the order of G for the selected curve; are the global domain parameters for both parties. By using the coefficients a and b; selected elliptic curve should be in the form.

$$y^2 = x^3 + ax + b \quad (4)$$

Equation (4) should be determined and chosen according to the NIST [9] who recommend specific elliptic curves which are robust against attacks.

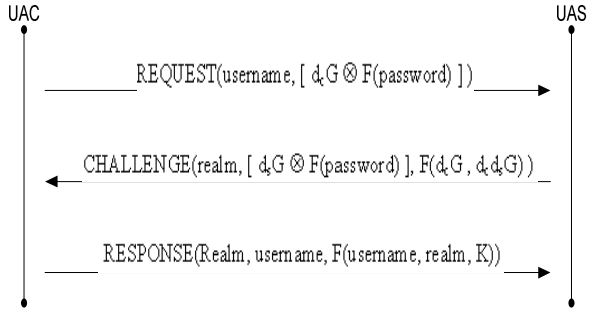

Fig. 3 ECDH approach

At the first step SIP Client sends a REQUEST message including its username and its public key xor'ed by its hashed password. After SIP server receives the REQUEST message, statement (5) is calculated:

$$d_cG = [(d_cG \otimes F(password) \otimes F(password)] \quad (5)$$

and finds out d_cG. UAS creates a session key K (6) by using its private elliptic key together with the result of (4):

$$K = (d_S.d_cG) \quad (6)$$

and sends a CHALLENGE message to client including realm, its public key xor'ed by the pre-shared hashed password, a hashed pair of Clients public key and session key K. At the third step SIP Client calculates;

$$d_SG = [(d_SG \otimes F(password) \otimes F(password)] \quad (7)$$

and finds out the value of d_SG. Session-key K has also been calculated by the client by using its private elliptic key together with the result of (7). By this way client validates the authentication of the SIP Server.

After that SIP Client sends a RESPONSE including username, realm and hashed triple of username, realm and K to the server. Server can easily verify the RESPONSE message by comparing the username, realm, K hash by its own calculation.

IV. Comparisons of DH and ECDH Approaches

At the same security it's widely known the key sizes that is used DH is about 6-7 times larger than EC key sizes. This result brings out the advantage of 171 bits EC keys instead of 1024 bits of DH keys in the transmission medium. Also generation of domain parameters of these two approaches differs in great instances. Test of generating domain parameters is made by using the openssl stack in a Intel Xeon processor 3200MHz box with 1024kb cache and 2048kb RAM. In Table I it's obvious that in the same security levels; there's a significant advantage of ECC besides Diffie-Hellman parameter generation times.

TABLE I
The Comparison of Domain Parameters

EC Domain Parameter		DH Domain Parameter Generation	
Curve prime192v1	0.0475 sec	256 bit	0.0301 sec
Curve prime256v1	0.0676 sec	512 bit	0.5783 sec
Curve sect283k1	0.0931 sec	768 bit	2.4916 sec
Curve sect409k1	0.1784 sec	1024 bit	7.8891 sec
Curve sect571k1	0.3706 sec	2048 bit	14.6603 sec

Besides of key sizes it can be said that ECDH is faster than DH by means of execution times and memory usage statistics according to the comparisons shown in Table II.

TABLE II
The Comparison of Instruction Counts

	Static Instruction Counts	Dynamic Instruction Counts	Loads Dynamic	Stores Dynamic
DH	214/20226	57,229,355	21,312,670	12,908,525
ECDH	306/21217	37,766,470	13,506,830	8,688,365

Table II has been composed and regarding tests has been done in Siena University as for comparisons of various encryption and key exchange schemes [10].

By using Elliptic Curve Cryptography it has seen that low number of dynamic instruction has been executed besides DH approach. Also memory usage is higher in standard cryptographic approach than Elliptic Curve derivative.

On the other hand by increasing the instruction and data caches it's been figured out that; total execution time is approximately %20 lower in elliptic derivate than standard approach.

These features shows that ECDH derivate of Secure SIP authentication is more efficient in embedded devices usage

like smart cards, wireless devices, PDA's due to the memory usage and faster calculations.

V. Conclusion

In this study a new scheme is proposed for security of SIP. Proposed method is based on ECC. Preferred properties of ECC are used for authentication of Session Initiation Protocol. Therefore article covers the basic features of Session Initiation Protocol and security considerations depending on the challenge/response mechanisms. The suggested authentication scheme using Elliptic Curve derived from Diffie Hellman Key Exchange compromises the same robust structure against offline password guessing and server spoofing attacks. Moreover it is more efficient and preferable in the applications/devices requires low memory and rapid transactions. .

References

[1] RFC 3261 – SIP: Session Initiation Protocol, June 2002.
[2] PROTOS - Security Testing of Protocol Implementations". University of Oulu, http://www.ee.oulu.fi/research/ouspg/protos/] ,Jan 2005.
[3] Goh, E.-J., and Jarecki, S. A signature scheme as secure as the Diffie-Hellman problem. In Advances in Cryptology. Proceedings of EUROCRYPT 2003 (2003), vol. 2656 of Lecture Notes in Computer Science, Springer-Verlag, pp. 401-415
[4] Yang C-C., Wang R-C., Liu W-T., Secure Authentication Scheme for Session Initiation Protocol, http://www.sciencedirect.com/science/journal/01674048, Computers&Security (2004).
[5] Johnston, Alan B., SIP: Understanding the Session Initiation Protocol, Second Edition, Artech House, 2004.
[6] RFC 2617 – HTTP Authentication: Basic and Digest Access Authentication, June 1999.
[7] Glass, E., The NTLM Authentication Protocol, http://sourceforge.net/ntlm, 2003.
[8] RFC 3310 – Hypertext Transfer Protocol (HTTP) Digest Authentication and Key Agreement (AKA), September 2002.
[9] NIST, Recommended Elliptic Curves for Federal Government Use, July 1999.
[10] Branovic, I., Giorgi, R., Martinelli, E., A workload Characterization of Elliptic Curve Cryptography Methods in Embedded Environments, ACM SIGARCH Computer Architecture News, Vol.32, No.3, June 2004.