Securing Session Initiation Protocol for VOIP Services

Amina.M.Elmahalwy
Information Technology Dept.
Faculty of Computers and Information, Menoufia University, Egypt

Wail.S.Elkilani
Computer Systems Dept.
Faculty of Computers and Information,Ain Shams University, Cairo, Egypt

Osama.S.Youness
Information Technology Dept.
Faculty of Computers and Information, Menoufia University, Egypt

ABSTRACT

VOIP (voice Over Internet Protocol) has many advantages but at the same time it has security threats not encountered in PSTN (Public Switched Telephone Networks).The paper deals with the security of the widely used protocol for signaling. The Session Initiation protocol (SIP) is considered the most used signaling protocol for calls over the internet. Securing SIP is becoming more and more important. This paper focusing on the SIP security mechanisms of authentication, and proposing an authentication model based on the Kerberos protocol to provide single sign-on, achieving two way authentications, to reduce the computation against authentication checks for each client, and prevent against Session Teardown Attack and Registration Hijacking attack. It acts as a trust third party to allow secure access to VOIP services. In this paper we implemented the SIP-Kerberos system and record the average time that the users need to authenticate at Kerberos and the average time needed to register at SIP server. The measured performance result of the solution is suitable for heavy loads in the SIP architecture.

Keywords

VOIP, PSTN, SIP, Security, Kerberos

1. INTRODUCTION

Public Switched Telephone Networks (PSTN) is closed networks which supporting voice services. It provides high availability, reliability and security.PSTN capabilities are limited services like audio conferences and instant messaging etc. On the other hand, VOIP service gives the opportunity to offer such services to telephony providers. Popular application and devices on the internet tend to become popular targets for attackers (Networking protocols, operating system, web browsers, and other application).SIP is developed to provide telephony services across the internet. It is a flexible and simple tool for establishing connections across the internet. 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, there are several security methods defined within SIP specifications .But, suggested methods cannot solve all the security problems with various system requirement. In The paper we are proposing an authentication model for Session Initiation Protocol based on the Kerberos v5 protocol .It includes many features that are non-existent in other authentication mechanisms, including that No flow of passwords on the network, Mutual authentication, Detection of replay attacks , providing Single sign on solutions that eliminate the need for clients to repeatedly prove their identities to different applications and hold different credentials and prevent Denial Of Service attack that occur due to the CANCEL or BYE attack, This paper is structured as follows section one present the Background of the SIP architecture, section two presents the security attacks against SIP authentication section three present survey of SIP authentication mechanisms and the related work and in section four we describe proposed Kerberos protocol, finally the conclusion is given.

2. BACKGROUND

2.1 SIP Protocol Overview

SIP has been standardized by Internet Engineering Task Force (IETF).It is an application layer signaling protocol for setting up, modifying and terminating multimedia IP sessions including VoIP telephony, video, streaming media, and instant messaging. .SIP is a text based protocol based on the HTTP (Hyper Text Transfer Protocol) protocol which defines two types of messages (SIP requests and SIP responses).

SIP defines basic classes of network entities:

1-UAC and UAS: runs on the user terminal, (User Agent Client) generates and sends SIP requests while the (User Agent Server) receive SIP requests and send SIP responses as depicted in figure 1

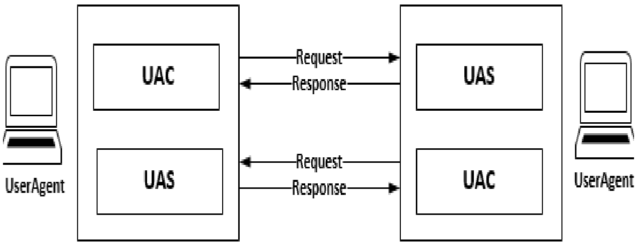


Fig1: Requests and Responses between the UAS and UAC

2-**Register server**: the Register server is responsible for user registration in VOIP services.

3-**Proxyserver**: the proxy server responsible for routing message. It can accept UAC's requests and send them to corresponding server.

4-**Redirect server**: the redirect server is a logical entity which to inform a registered user to connect directly to another proxy or to the register server. SIP messages are defined in RFC 3261 (Request for comments) and they comprise [1]:

REGISTER: used by UA to register with a SIP server.

INVITE: used to invite another UA to communicate and establish a SIP session between two users.

ACK: used to accept a session and confirm message exchanges.

OPTIONS: used to obtain information on the capabilities of another user.

SUSCRIBE: used to request updated presence information.

NOTIFY: used to send updated information on the UA's current status.

CANCEL: used to cancel a pending request and terminating the session.

BYE: used to terminate the session

SIP responses are groups into six categories. Each response has assigned a three digit numerical code. The first digit specifies the category. The categories are, informational responses (1xx) ,success responses(2xx),redirection responses(3xx),client error(4xx),servererror(5xx) and global failure(6xx).SIP addresses are in the form of user@host,where user part can be user name or telephone number and host part is eitherdomain name or network address. When a UA wants to initiate a session, send an INVITE message, thismessage is responded by an OK followed by an ACK message. When a UA wants to terminate the session, it sends a BYE message. The establishment-termination process is depicted Figure 2.

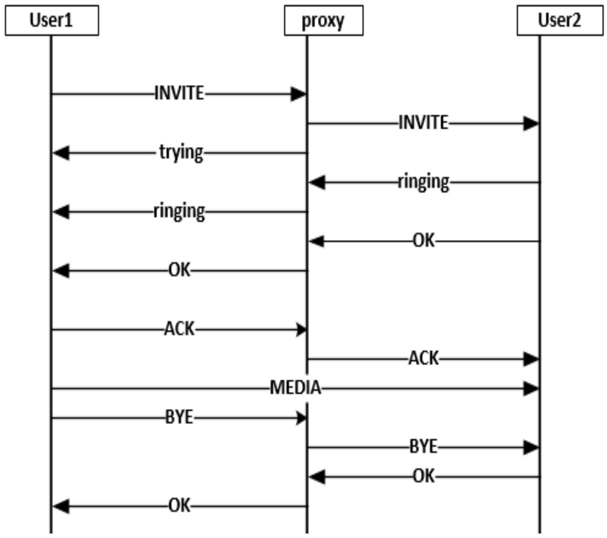


Fig2: SIP establishment and termination procedure

3. SIP SECURITYATTACK

SIP is a text based signaling protocol, this makes SIP more flexible and easy to implement but increases the security risks. Authentication and privacy are most important part of SIP security framework. The following sections describe several vulnerabilities present in most SIP systems.

3.1 Registration Hijacking Attack

Registration Hijacking occurs when an attacker impersonates a valid UA to a registrar and places the legitimate registration with its own address as SIP registration mechanism is based on the From and To headers of the REGISTER requests. When registrar server receiving a REGISTER message from a UAC, it has to verify that the identity in the From header has the permission to change the contacts of the address-of-record specified in the To. So this attack causes all incoming calls to be sent to the UA registered by the attacker.

3.2 Replay Attack

A replay attack is an action in which an attacker impersonates or deceives another legitimate participant through the reuse of information obtained in a protocol.

3.3 Man in the Middle (MITM) Attack

Man in the Middle Attack means that the attacker makes independent connections with the victims, making them believe that they are talking directly to each other over a private connection. An attacker can easily set up a man-in-the-middle attack by using ARP (Address Resolution Protocol) spoofing/poisoning. He just has to spoof the MAC address of the SIP Server. The attacker will receive all the requests and can modify them at will.

3.4 Message Tampering Attack

Message Tampering Attack occurs when an attacker intercepts and modifies packets exchanged between SIP components.

3.5 Proxy Impersonation Attack

Proxy Impersonation Attack occurs when an attacker impersonates your SIP UAS or proxies into communicating with a rogue proxy. If an attacker successfully impersonates a proxy, he has access to all SIP messages and it is in complete control of the call.

3.6 Session Teardown Attack

Session Teardown Attack occurs when an attacker observes the signaling for a call, sniff the traffic and store important dialog information, and then once a Session is established, subsequent requests can be sent to modify or terminate the session. It is sends spoofed SIP BYE message to the participating UAs

3.7 Denial of service (DOS) Attack

DOS can take different forms as malformed packets and flooding such as (REGISTER OR INVITE flood of packets.

4. SURVEY OF SIP AUTHENTICATION MECHANISMS

We could claim that the security mechanisms suggested by RFC 3261 could be employed for protecting SIP based services is depicted in Figure 3. Since there are several limitations associated with these security mechanisms when applied to a SIP environment.

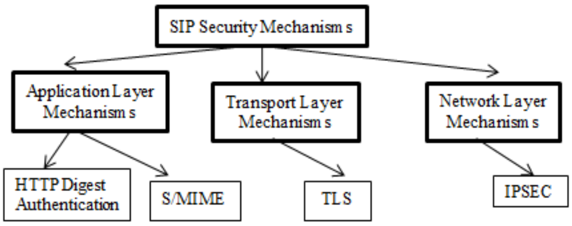

SIP Security Mechanisms
Application Layer Mechanisms
Transport Layer Mechanisms
Network Layer Mechanisms
HTTP Digest Authentication
S/MIME
TLS
IPSEC

Fig. 3: An example of SIP Security Mechanisms

For instance, the utilization of the HTTP Digest Authentication and S/MIME (Secure/Multipurpose Internet Mail Extensions) security mechanism for providing security at SIP system. Both the mechanisms not more secure, as HTTP Digest does not provide message integrity, any protection against signaling attacks and also make SIP messages vulnerable to the Man-In-The-Middle attacks. The limitation concerns the S/MIME since a SIP proxy requires access to specific headers for processing an incoming message. It cannot offer protection against eavesdropping attack. The Transport Level Security (TLS) is the recommended methodology in SIP RFC3261 [1].The TLS provides a mechanism for generating key and provides hop-by-hop transport level security. The cons. Of TLS is that on server side it has to maintain multiple TLS sessions, any break in session or change in address needs a session re-initiation, if using public/private key, the algorithmic procedures are computational heavy, and this makes it less scalable. Since TLS will be a hop-by-hop security mechanism. The IPSEC (Internet Protocol Security), an application security at IP system, need IKE (Internet Key Exchange) management to create and maintain secure tunnels between two clients over the public internet, the complex nature of IKE makes it more difficult within SIP domain. In last decade number of authentication mechanism aiming to replace the basic security scheme HTTP Digest Authentication have been proposed ,using Diffie-Hellman and Elliptic curve cryptography ,ID authentication, and others.

4.1 Related works for SIP authentication schemes

Authentication is an important issue in SIP-based service. for example, when the user agent wants to make a SIP voice call to another user, how can he verify that he is connected exactly to SIP user agent that he want, and not to other client.however,SIP authentication scheme typically uses HTTP Digest authentication protocol and is not providing security at an acceptable level. Although, SIP Over SSL (SIPS) can also provide end-to-end protection on SIP request/response message, but it still requires end user's certificate in place and increase the workload of SIP proxy servers .To guarantee the security of the SIP-based services, several new schemes have been proposed to enhance the security of SIP based services, Yang et al. [2] pointed out that HTTP Digest authentication protocol is subject to the off-line guessing attack and the spoofing attack. Then, they introduced a public key cryptosystem based on Diffie-Hellman key exchange protocol to solve these problems; however this scheme incurs the replay attack. Ring et al.[3] provided a secure authenticated key agreement(AK) protocol for SIP using identity-based cryptography(IBC)[4].It suffers from the heavy computation. Durlanik et al. [5] proposed a SIP authentication scheme using Elliptic Curve cryptosystem (ECC) however, it is vulnerable to Man-In-The-Middle Attack and it is not completely safe with untrusted proxy servers due to the fact that the servers keep user password in a plaintext. Ring et al. 's scheme, Wang and Zhang[6]proposed anew secure authentication and key agreement (SAKA)mechanism using cetificateless public key cryptography(CL-PKC).Wang and Zhang 's scheme suffers from heavy computation load. Also, Geneiatakis and Lambrinoudakis [7] proposed an improved authentication scheme to enhance the security of HTTP Digest authentication for SIP by introducing a new SIP header namely the INTEGRITY-AUTH header, which is aiming at protecting the SIP-based services from signaling attacks while ensuring authenticity and integrity. However, the INTEGRITY-AUTH header cannot be a void the offline password guessing attack .Wu et al. [8] presented a new authenticated key exchange protocol (NAKE) to solve the existing problems in SIP original authentication. Jung-Shian Li et al [9] have proposed to use the Kerberos protocol with VOIP SIP.

5. PROPOSEDKERBEROS AUTHENTICATION PROTOCOL

The main focus of this paper is to enhance the security of SIP, and prevent SIP attack like registration hijacking, Session Teardown Attack that resulting in a form of Denial-Of-Service, and man in the middle attack. Using username and passwords authentication is not enough for security. We will define anew security for SIP domain which provides end-to-end security, this mechanism is based on using Kerberos as key management for authenticating the SIP clients and generating ticket on behalf of server. It is an authentication protocol for network and also provides single sign-on facility to client.

5.1 Background of Kerberos

Kerberos was designed and implemented by the Massachusetts Institute of Technology (MIT) in the mid 1980's as a solution to the network security problems to provide strong authentication for client/server applications using secret key cryptography in project Athena [10].It was named after Cerberus, the Greek three-headed dog that guards the gates of the underworld, thematically indicating the three areas of security that Kerberos provides: Confidentiality, Integrity and Privacy. Kerberos has now reached version 5.12.1 released in January 2014 [11]. It provides mutual authentication (both the client and the server verify each other's identity).

5.2 How Kerberos woks

Kerberos works on the basis of tickets, which serve to prove the identity of users. There are three types of ticket exchange with six message exchange as depicted in Figure 4:

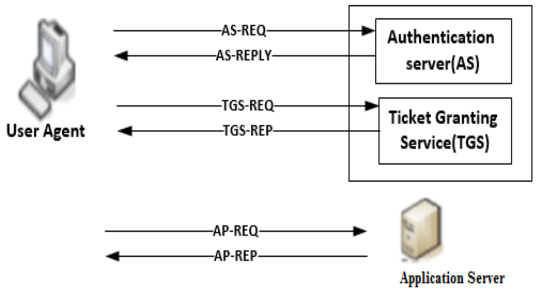


Fig. 4: Overview of how Kerberos work.

Authentication Service (AS) Exchange: AS-REQ and AS-REP.

AS_REQ is the first user authentication request. This message is directed to the Authentication Server (AS).

AS_REP is the reply of the AS to the previous request. It contains the TGT (Ticket granting ticket (encrypted using the TGS secret key) and the session key (encrypted using the secret key of the requesting user).

Ticket-Granting Service (TGS) Exchange: TGS-REQ and TGS-REP.

TGS_REQ is the request from the client to the Ticket Granting Server (TGS) for a service ticket. It contains the TGT obtained from the AS and an authenticator generated by the client and encrypted with the session key.

TGS_REP is the reply of the Ticket Granting Server to the previous request. It contains the requested service ticket (encrypted with the secret key of the service) and a service session key generated by TGS and encrypted using the previous session key generated by the AS.

Client/Server (CS) Exchange: AP-REQ and AP-REP, used by the client to submit a registration to the ticket as registration to a service.

AP_REQ is the request that the client sends to an application server to access a service. It contains the service ticket obtained from TGS with the previous reply and an authenticator again generated by the client, but here encrypted using the service session key (generated by TGS)

AP_REP is the reply that the application server gives to the client to prove it really is the server the client is expecting. The client requests the server for it only when mutual authentication is necessary.

5.3 Kerberos Protocol Messages

Kerberos V5, the details of the messages exchanged in Figure 5 and table 1.

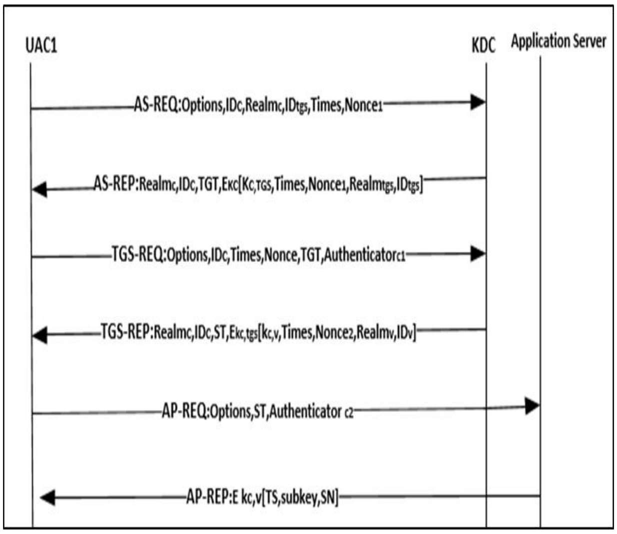

UAC1
KDC
Application Server
AS-REQ:Options,IDc,Realmc,IDtgs,Times,Nonce1
AS-REP:Realmc,IDc,TGT,Ekc[Kc,TGS,Times,Nonce1,Realmtgs,IDtgs]
TGS-REQ:Options,IDc,Times,Nonce,TGT,Authenticatorc1
TGS-REP:Realmc,IDc,ST,Ekc,tgs[kc,v,Times,Nonce2,Realmv,IDv]
AP-REQ:Options,ST,Authenticator c2
AP-REP:E kc,v[TS,subkey,SN]

Fig 5: Kerberos message exchange

TGT = E Ktgs [Flags, Kc,tgs , Realm c, ID c , AD c , Times].

ST = E Kv [Flags, K c,v , Realm c , ID c , AD c , Times]. Authenticator C1 = E Kc, tgs [ID c , Realm c , TS 1].Authenticator C2 = E Kc, v [ID c , Realm c , TS 2 , subkey, SN].

After running the Kerberos, client received a TGT (Ticket Granting Ticket), then get access to the server, and the client request ST (Service Ticket) that can be used to obtain access to the Service.

Table 1: The elements of the Kerberos

V	The application server.
IDc	The name of the client.
ADc	The address of the client.
Realm	The Network
IDtgs	TGS name
Options	Setting of flags for returning ticket
ST	(Service ticket) received from TGS Server to access the service.
TGT	(Ticket Granting Ticket) received from the AS authentication.
Nonce	Used to prevent the use of duplicate messages (Replay Attack).
Times	How long can a TGT or ST.
E Kc	Encrypted with a key derived from the password of the client.
K C, tgs	Session keys used between clients and TGS
E Ktgs	Encrypted with a key known only to AS and TGS.
E Kc, tgs	Encrypted with the session key. Between the client and the TGS
Authenticator C	Verify the requests to use Ticket.
TS	Timestamp (Timestamp).
K c, v	Session keys used between Client and Server.
E Kv	Encrypted with the key of the Server
Subkey	Key selected by the client to protect Session between client and server.
SN	Sequence Number: in order to send a message.

6. SIP-KERBEROS AUTHENTICATION MODEL

6.1 Authentication and access to SIP

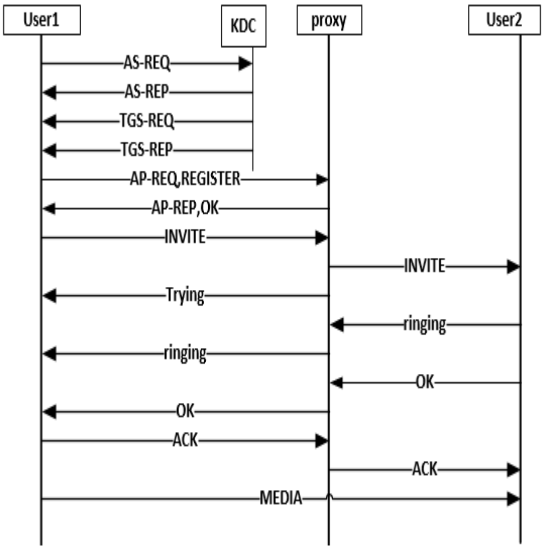


Fig 6: User authentication and access to SIP server

When the user agent access SIP server, as depicted in figure 6.

1. The user agent logs into a workstation by entering the login name before prompting user for the password [11], a message is sent to the AS (Authentication server). The message contains the login name and name of a service (TGS service).

2. The AS responds with a ticket granting ticket (TGT) that is encrypted with a key that is derived from the user's password, which is already stored at the AS.

3. When the user wants access to the SIP server, the workstation sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key.

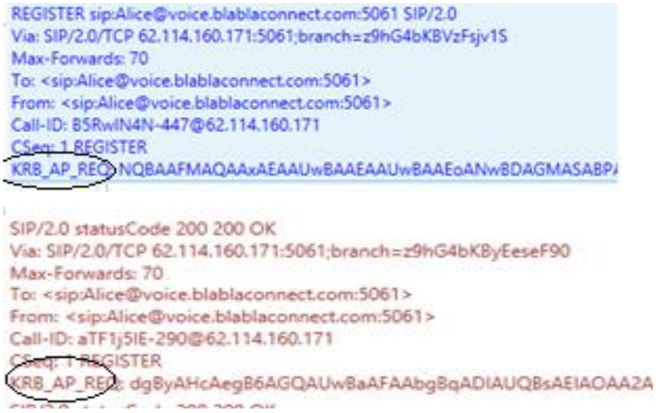
4. The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key – one encrypted with the client password, and one encrypted by the service password.

5. The user application now sends a service request to the server containing the ticket received in Step 4 and an authenticator with the Register Message to the SIP server

6. Server will reply with a server authentication message with the Ok message, as mutual authentication is required.

6.2 SIP -Kerberos Protocol to prevent Registration Hijacking attack.

An attacker send REGISTER message to the SIP server to register in the database. To prevent this attack, any user to register in the SIP server, it must be firstly authenticated at KDC server via AS-REQ/AS-REP, and then acquires a service ticket from the KDC via the TGS-REQ/TGS-REP exchange. A mutual authentication process is then performed between the SIP UA and the SIP server through an AP-REQ/AP-REP exchange. If the Kerberos authentication is successfully completed, the SIP server accepts the SIP REGISTER request, records the user's location information, and then sends the SIP UA a 200 OK message, as depicted in the figures7



```
REGISTER sip:Alice@voice.blablaconnect.com:5061 SIP/2.0
Via: SIP/2.0/TCP 62.114.160.171:5061;branch=z9hG4bKBVzFsjv1S
Max-Forwards: 70
To: <sip:Alice@voice.blablaconnect.com:5061>
From: <sip:Alice@voice.blablaconnect.com:5061>
Call-ID: B5RwIN4N-447@62.114.160.171
CSeq: 1 REGISTER
KRB_AP_REQ: NQBAAFMAQAAxAEAAUwBAAEAAUwBAAEoANwBDAGMASABP
```

```
SIP/2.0 statusCode 200 200 OK
Via: SIP/2.0/TCP 62.114.160.171:5061;branch=z9hG4bKByEeseF90
Max-Forwards: 70
To: <sip:Alice@voice.blablaconnect.com:5061>
From: <sip:Alice@voice.blablaconnect.com:5061>
Call-ID: aTF1j5IE-290@62.114.160.171
CSeq: 1 REGISTER
KRB_AP_REQ: dgByAHcAegB6AGQAUwBaAFAAbgBqADIAUQBsAEIAOAA2A
```

Fig7: An example of Register message in SIP with Kerberos

6.3 SIP -Kerberos Protocol to preventSession teardown attack.

An attacker tears down a conversation between two users by sending his own BYE request to either of the users as depicted in figure 8.

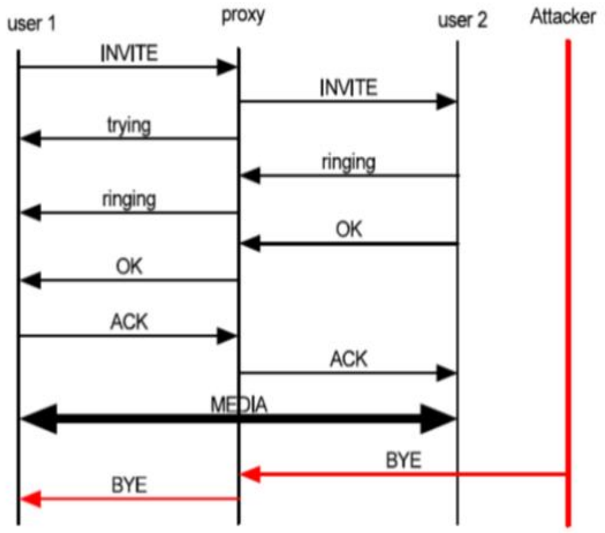


Fig 8: An example of Bye Attack

For SIP Server to prevent Session teardown attacks (BYE attack), it must ensure that the message from the legitimate user as depicted in figures 9, 10.

The user agent used the session key that generated when authenticated using Kerberos. If wants to tear down the Session, it sends the BYE message followed by the Nonce value that generated randomly and the hash value of Nonce and session key between the client and server. Otherwise, the SIP Server can verify that the BYE/CANCEL message of UA that is true or attacked BYE, by computing a hash function h (K c,v , Nonce) and compare it with the message sent, if compatible send OK message, else send bad session key. as depicted in figures 11,12.

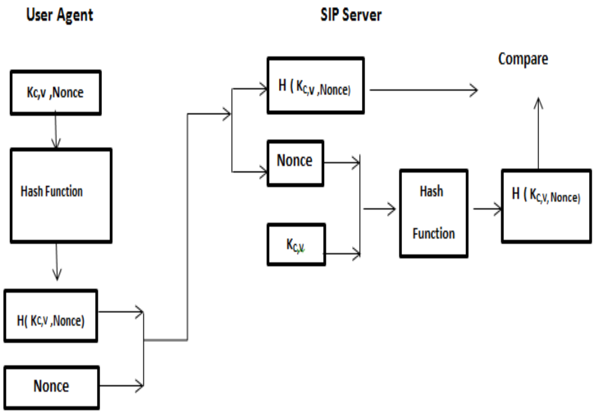


Fig 9: How to prevent session tear down attack.

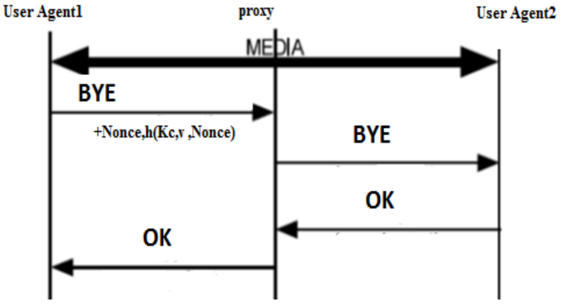
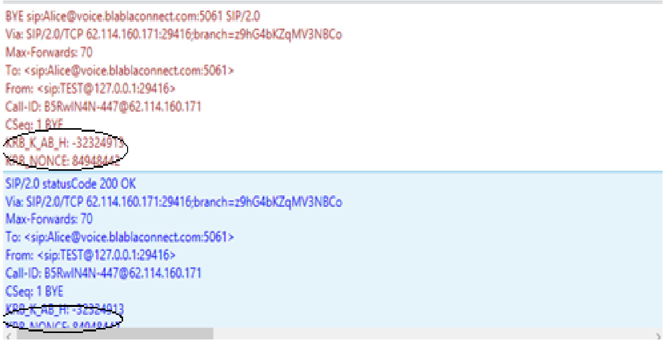


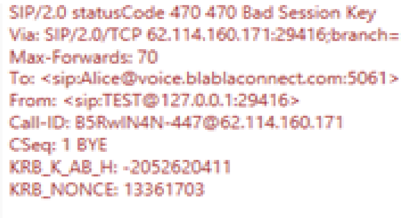
Fig 10: flow of BYE message utilizing the proposed schema



```
BYE sip:Alice@voice.blablaconnect.com:5061 SIP/2.0
Via: SIP/2.0/TCP 62.114.160.171:29416;branch=z9hG4bKZqMV3NBCo
Max-Forwards: 70
To: <sip:Alice@voice.blablaconnect.com:5061>
From: <sip:TEST@127.0.0.1:29416>
Call-ID: B5RwIN4N-447@62.114.160.171
CSeq: 1 BYE
KRB_K_AB_H: -32324913
KRB_NONCE: 84948442
```

```
SIP/2.0 statusCode 200 OK
Via: SIP/2.0/TCP 62.114.160.171:29416;branch=z9hG4bKZqMV3NBCo
Max-Forwards: 70
To: <sip:Alice@voice.blablaconnect.com:5061>
From: <sip:TEST@127.0.0.1:29416>
Call-ID: B5RwIN4N-447@62.114.160.171
CSeq: 1 BYE
KRB_K_AB_H: -32324913
KRB_NONCE: 84948442
```

Fig 11:An example of authentic BYE message and OK message.



```
SIP/2.0 statusCode 470 470 Bad Session Key
Via: SIP/2.0/TCP 62.114.160.171:29416;branch=z9hG4bKcY8qYAqP8
Max-Forwards: 70
To: <sip:Alice@voice.blablaconnect.com:5061>
From: <sip:TEST@127.0.0.1:29416>
Call-ID: B5RwIN4N-447@62.114.160.171
CSeq: 1 BYE
KRB_K_AB_H: -2052620411
KRB_NONCE: 13361703
```

Fig 12: An example of response Fake BYE message.

6.4 SIP -Kerberos Protocol to prevent Man in the Middle Attack

SIP-Kerberos model is safe from Man in the Middle Attack

1-As user's password is never sent over the network, so it is impossible for the attacker to steal passwords by network sniffing. Note also that the Man in the Middle attack is foiled, because if the request is interrupted, the attacker cannot read it because it does not know the encryption key of the service.

2-The Authenticator message includes the sender's ip-address and source port, as well as the destination ip-address and port.

6.5 Experimental Setup

Kerberos authentication required framework to solve SIP Security problems. Kerberos methods can be used to provide hop-to-hop and end-to-end authentication, privacy and integrity for SIP messages. This section details the Kerberos solution. To characterize the performance of a SIP proxy with Kerberos authentication, we implemented an experimental test bed based on the scenario depicted in Fig.13. Experimental measurement has been chosen to evaluate the performance of the proposed algorithm. The faculty of computers and information, Menoufia University. The network consists of two LANs. Each LAN ends with an edge switch. The LANs are connected through a core switch.LAN 1 consists of 10 users, SIP server and SIP server. LAN 2 consists of 20 users.

All PCs are core i5 processor with 3 GB of RAM. The edge switches are cisco catalyst 2960 switch with 24 ports. The core switch is cisco catalyst 4006 switch.

The response time has been chosen to evaluate the performance of the algorithm. The response time to authenticated and accessing SIP server and taking in mind the different parameters affecting the response time values. These measures speed, reliability, and robustness of the algorithm. Hence, it proves the algorithm efficiency.

6.5.1 Research Methodology

In tests our proposal of SIP-Kerberos Security we chose the C # language .we implemented asimple Client was launched in multiple instances according to the number of users in the testedscenario(2,4,8,16,….).besides we implemented Kerberos authentication serverwhich generate the ticketsand apply authentication of the clients ,andimplemented a simple SIP proxy. We measured the performance of the proposed security by measuring the time with the number of simultaneous users 5 times and calculated the average values.

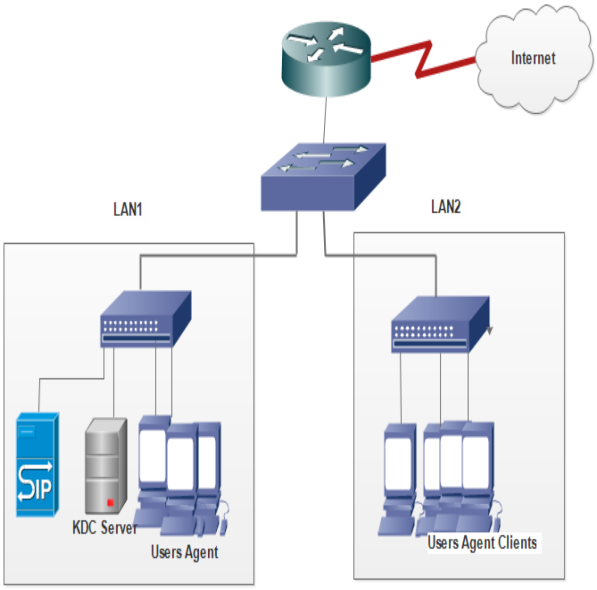


Fig13: Experiment test bed

6.5.1.1 Authentication Time

It represents the amount of time needed to authenticate a trusted user. Fig.14 shows the authentication time values. The X Axis represents the number of simultaneous users trying to authenticate at KDC Server. The Y Axis represents the authentication time values in milliseconds. The different colors represent the number of trials trying to authenticate at the same time.

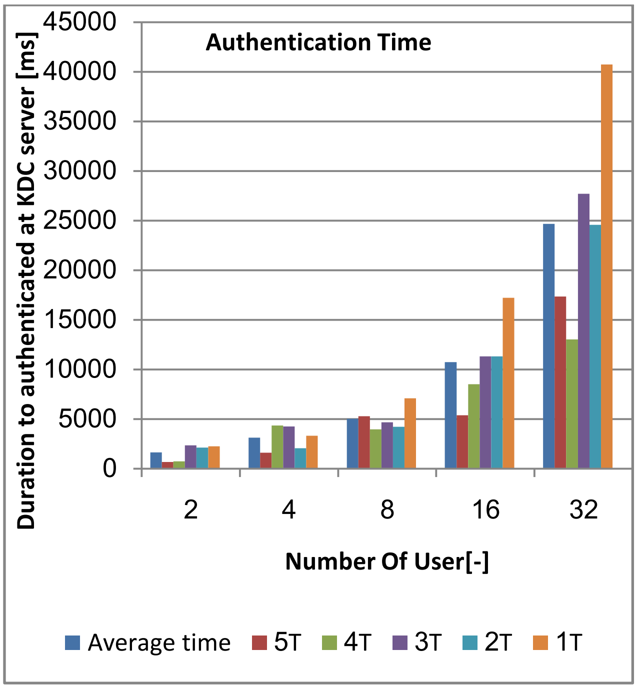


Fig 14: Authentication Time in milliseconds versus number of users

6.5.1.2 Registration time

It represents the time taken by the user to register in the SIP server. Fig.15 shows the registration timeValues. The X-Axis represents the number of simultaneous users trying to register at SIP Server. The Y-Axis represents the registration time values in milliseconds. The different colors represent the number of trials trying to register themselves at the same time.

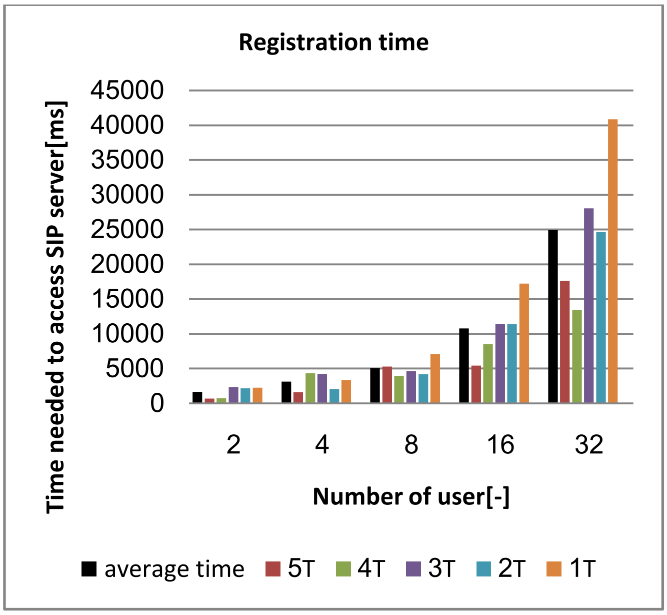


Fig15: Registration Time in milliseconds versus different number of users

These results without a real communication serve only as a demonstration of a secure solution for the SIP system with the

Kerberos strong reliable authentication. The measured performance results of our solution is suitable for heavy loads in the SIP architecture with increasing the numbers of users

7. CONCLUSION

In this paper we have proposed a secure key exchange scheme for use in a SIP system .This scheme is based on reliable Kerberos protocol, Kerberos provides mutual authentication functionality between the SIP clients and servers, and the proposed model is safe from replay attack and Man In The Middle attack, prevent against Session Teardown Attack and Registration Hijacking attack,

8. 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), Internet Engineering Task Force, Jun. 2002, updated by RFCs 3265, 3853, 4320, 4916,5393, 5621, 5626, 5630, 5922, 5954, 6026. [Online].

[2] Chou-Chen Yanga, Ren-Chiun Wangb, Wei-Ting Liuc," Secure authentication scheme for session initiation protocol", Computer& Security (24) (2005) 381–386.

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

[4] A. Shamir, "Identity-based cryptosystem and signature schemes", in: Advance inCryptology-Crypto 1984, LNCS, vol. 196, Springer, Berlin, 1984, pp. 47–53.

[5] A. Dulanik and I. Sogukpinar, "SIP Authentication Scheme using ECDH", in: Proc.Enformatika, vol. 8 (2005) 350 - 353.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989

[6] F. Wang, Y. Zhang, "A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography", Computer Communication 31 (2008) 2142–2149.

[7] D. Geneiatakis, C. Lambrinoudakis, "A lightweight protection mechanism against signaling attacks in a SIP-Based VoIP environment", Telecommunication Systems Springer 36 (4) (2007) 153–159.

[8] L. Wu et al.," A new provably secure authentication and key agreement protocol for SIP using ECC", Computer Standard & Interfaces 31 (2) (2009) 286–291.

[9] Jung-Shian Li, Chuan-Kai Kao and Shiou-Jing Lin, "A Kerberos based Single Sign-On System for VoIP SIP Servers and Clients with a Terminal Mobility Capability ", Computer Communication Control and.Automation (3CA), 2010 International Symposium on, 2010.

[10] Massachusetts Institute of Technology," Kerberos: The Network Authentication Protocol". http://web.mit.edu/kerberos/, Accessed: Apr, 2013.

[11] https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm?turl=WordDocuments%2Fintroductiontokerberosauthentication.htm.

[12] Yudi Prayudi, Tri K Priyambodo , "Study on Cryptography as a Service (CAAS)", International Journal of Advanced Research in Computer Science and Software Engineering 4(10), October - 2014, pp. 150-156