Detection and Prevention Mechanism on Call Hijacking in VoIP System

Amruta Ambre
Department of Computer Engineering
D.J.Sanghavi College of engineering
Mumbai, India

Narendra Shekokar, Ph.D
Department of Computer Engineering
D.J.Sanghavi College of engineering
Mumbai, India

ABSTRACT
VoIP (Voice over Internet Protocol) enables user to make calls through internet. VoIP system is popular because of its rich features. VoIP uses Session Initiation Protocol for initialization, termination and tearing down of a session between two communicating entities. Due to its rich features VoIP has received wide acceptance and becoming one of the mainstreams in communication network, increased use of this includes scams and security concerns. Vulnerabilities in the SIP protocol enable hackers to inject control signals and hijack calls. Hence assuring the identities of the communicating entities is essential. Many authentication schemes were proposed for SIP from time to time. Strong authentication scheme can identify the potential threats. This paper proposes the authentication scheme between two end points in order to overcome the limitations of the existing authentication scheme.

Keywords
VoIP, SIP, Challenge-Response, Authentication, Hash Digest and Sequential Count authentication

1. INTRODUCTION
VoIP is a technology in which there is transportation multimedia over IP network. Instead of being transmitted over circuit switched network, Voice signal is digitized and transmitted over internet [1]. VoIP signaling protocols are divided into two categories media control and session control. Session control protocols are further divided intoH.323 and Session Initiation protocol .Both the protocols play specific role in different services. But SIP is more popular than H.323 because of its simplicity and flexibility [2].

Due to attacker's access to the flow, attacker's ability to exploit and systems susceptibility causes system more vulnerable. Based on some weaknesses in SIP few attacks are observed. This paper focuses on VoIP security by analyzing potential threat and proposed mitigation technique which will not only enhance the security features but also will be helpful in future work.

This paper is organized as below. In section II we have discussed about SIP protocol. Section III represents overview of Literature Survey.Then we have proposed a scheme to avoid Call Hijacking in SIP in section IV.Finally section V concludes the paper.

2. OVERVIEW OF SIP
2.1 SIP components
SIP system consists of four components [5].

1. **User Agent Client (UAC)**: Caller application that initiates and sends SIP requests.
2. **User Agent Server (UAS):** Receives and responds to SIP requests: accepts, redirects, or refuses calls.
3. **Proxy Server:** Contacts one or more clients or next-hop servers and passes the call requests further. It contains UAC and UAS.
4. **Redirect Server:** Does not initiate SIP requests or accept calls. Accepts SIP requests, maps the address into new addresses and returns those addresses to the client.

2.2 SIP Call Flow
In Call flow process, above mentioned components of VoIP plays important role i.e. User Agent can be either UAC or UAS and network server in between for transforming video, voice ,data .Figure 1 shows the basic SIP call flow

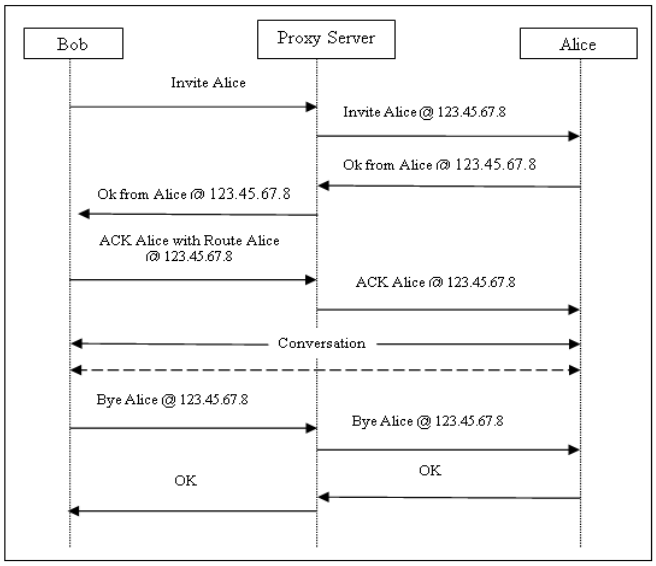


Figure 1: Basic SIP Call flow

2.3 SIP Messages
The messages sent in SIP call flow have a specific format [5].

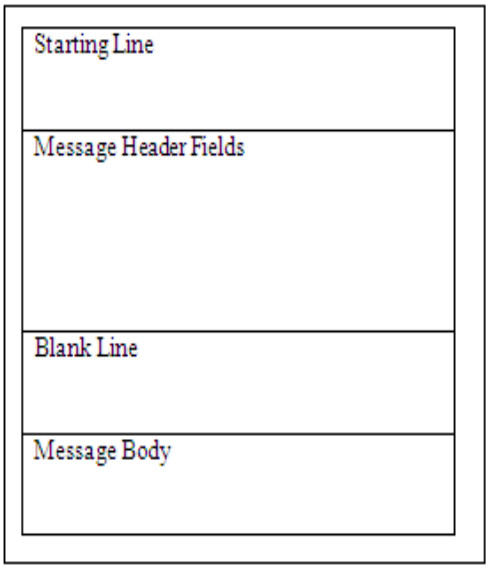


Figure 2: SIP Message Format

Starting line: SIP's first line is called Request-Line in requests and Status-Line in responses. It consists of the method used along with the destination SIP URI.

Message Header fields*:* These fields contain useful information for efficiently routing SIP messages. They also include information about UA's supported capabilities and sequencing of messages. A sample Header field block is provided below.

Message Body: The body of the message may carry session descriptions protocol (SDP) This part of the SIP message is used by UAs during negotiation and settlement of media related information like IP addresses, port numbers and codecs.

2.4 SIP Authentication Techniques

There are currently 2 modes of authentication built into HTTP 1.1 protocol, termed "Basic" and "Digest" Access Authentication [4].

Basic Access Authentication

- Client Requests
- Server Sends HTTP 401 Authorization Required Response Error.
- Browser displays Username/Password prompt displaying host name and authentication realm.
    - If the User hits the cancel-Button
    - If the User enters an Username/Password
- Server compares client information to its user/password list

Digest Access Authentication

- Password won't be sent in clear text
- Password will be sent encrypted
- Normally MD5 is used to encrypt the username-password pair within Digest access. Hence some additional headers are required.
- Server Send Authorization
- Client replies Authorization

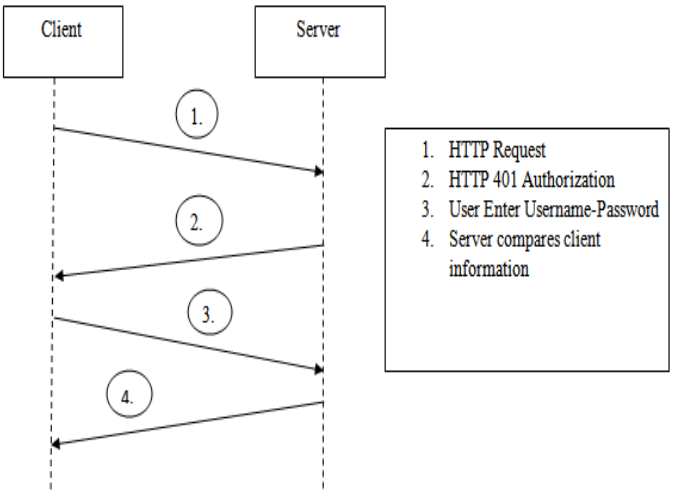


Figure 3: Digest Access Authentication

2.5 SIP vulnerabilities and Attack

Following mentioned are some weakness in the VoIP systems.

1. For security purpose Basic Authentication is used which is vulnerable due passwords which are transformed in clear text format.
2. Next Digest Authentication is a good replacement for basic but to handle modern cryptographic standards, this is also a weak mechanism.
3. User Agent Server is relying only on SIP headers (Contact), which have been changed by attacker.
4. Weakness mentioned above causes intercepting and rerouting the call through a different path before reaching the destination.

Based on above mentioned weaknesses in SIP gives rise to below mentioned attacks [11]

1. **Registration Hijacking:** Registration hijacking happens when an attacker replace the legitimate registration of the victim with his address.
2. **Media Session Hijacking:** Spoofed messages from Attacker may be delivered to either one of the VoIP end points to redirect the media to another end point.
3. **Server Impersonating:** Attacker trick the victim into communicating with the rogue proxy set up by the attacker.

3. LITERATURE SURVEY

The SIP Authentication scheme based on HTTP digest that uses challenge and response message to recognize the communicating parties[3]. However, it is vulnerable because the username and password will be sent in clear text format, which can be stolen by attacker. To overcome this Digest Authentication came into picture in which password will be sent in encrypted format. So even though Digest Authentication is good replacement for basic but still it is weak mechanism for modern cryptographic mechanism. SIP Digest is based on a challenge/response principle [16]. The User Agent (UA) authenticates itself against the server by using its associated credentials (user name, password).In reality, there is no such relationship between two endpoints. The called party cannot hold personal data for any possible caller. But, this would be necessary to verify the origin of an incoming call. Moreover, SIP Digest.

Basic and Digest Authentication vulnerable to offline password guessing attack and server spoofing attack. To overcome these weaknesses, a scheme based on Diffie-Hellman key exchange has been proposed [7]. It maintains preconfigured password used to verify the identity of user or server. Further security depends on Discrete Logarithmic Problem (DLP) which involves exponential computation [8]. However, it is not suitable for user devices have low computation power and computing capability like smart card and mobile. In addition, computation time to generate a key is large which does not meet the requirements of real time implementations of SIP as a protocol for communication.

To meet all these challenges, Elliptic Curve Cryptography (ECC) with key size around 160 bits is an alternative solution because of its security, based on Elliptic Curve Discrete Logarithm problem (ECDL) and operates on group of points on elliptic curve. Moreover, it is faster in computations and provides same security as compared to RSA 1024 bit key [13].Three way handshake nonce based SIP authentication scheme has been proposed [10]. It uses only one-way hash function and exclusive-or operation for all messages exchanged between communicating entities. But it did not provide forward secrecy and modified scheme using ECC proposed to overcome these attacks [14].

David Butcher [15] discusses various security features to be considered while designing new authentication schemes like Denial of Service, Eavesdropping, Alteration of Voice Stream, Toll Fraud, Redirection of Call, Accounting Data Manipulation, Caller ID Impersonation, unwanted Call and Messages. Prominent attacks on SIP include Registration Hijacking, Message Modification, Cancel/Bye Attack, Malformed Command, and Redirection of calls.

This paper proposes the secure mutual authentication scheme agreed by both UAC and UAS, for which we will be using hash function and more XOR computations are for emphasizing the integrity of the authentication process. For that first analysis of prior work with respect to techniques and operations should be known. Hence we have prepared a table for comparison of previous techniques and operations.

Below mentioned two comparison tables, table 1 and table 2.In table 3 notations and their meanings of different techniques and operations are given. table 1 consists of X and Y axis.

X: Axis represents operation, No of Hash and No of XOR

Y: Axis represents Techniques**.**

In table 1 comparison between different techniques and operations dealt by different schemes have been mentioned. table 2 compares possible attacks dealt by different schemes.

Table 1: Comparison table for techniques and operations dealt by different schemes

X / Y	operation	No of Hash	No of XOR
MD	HF	1	--
ECDH	HF,DLP,ECC,XOR	7	2
HF	HF,XOR, Concatenation	7	4
ENCRYPTION	EXP,ENC	--	--
DH	HF,DL,EXP,XOR	7	4

Table 2: Comparison table for possible attacks dealt by different schemes

Attack Types	MD	ECDH	HF	ENCRYPTION	DH
Password Guessing	yes	no	no	no	no
Server Impersonating	yes	no	no	no	no
Man-in-Middle attack	no	--	--	no	no

Table 3: Notations and Meaning of different techniques and operations

Notations	Meaning
MD	Message Digest
ECDH	Elliptical Curve Diffie Hellman
HF	Hash Function
ENC	Encryption
DH	Diffie Hellman
ECC	Elliptic Curve Cryptography
DL	Discrete Logarithmic
EXP	Exponential

4. PROPOSED SCHEME

As discussed previously, we have identified limitations in authentication techniques. To overcome those limitations, we propose mutual authentication scheme so that both UAC and UAS can identify and verify each other. For proposed scheme different parameters need to consider for UAC and UAS which are mentioned below in Table 4.

Table 4: Abbreviations and Meaning for Proposed Scheme

Sr No.	Abbreviation	Meaning
1	PC	UAC Password
2	IPC	Password Index for Client
3	UD	UAC date registration
4	IUD	Date Registration Index
5	SKC	Session Key For Client
6	UID	User Identity Code
7	SID	Server Identity Code
8	PS	UAS Password
9	IPS	Password Index for Server
10	SKS	Session Key For Server
11	SC	Sequence Count
12	⊕	Exclusive–OR operation
13	hf	Hash Function

From above table

For UAC: Abbreviations from no 1 to 6 are required.

For UAS: Abbreviations from no 7 to 10 are required.

Sequence counter (SC) starts its count and continues till it reaches maximum limit. Session keys and Sequence count both are mandatory in every request and response. These Session keys are generated based pre-determined shared formula. Different parameters are XORed and transformed into one way hash function.

Proposed scheme comprises of following 2 phases.

Phase 1: Initial Setup Phase

Phase 2: Verifying Phase

Phase 1: Initial Setup Phase: UAC and UAS agreed on some parameters and session keys prior to this session.

1. UAC, and the UAS chooses its own password and both of these passwords are mutually shared along with their index values namely IPC and IPS respectively to each other.
2. UAC's Identity (UID) and Date of Registration (UD) are intimated to the UAS.
3. UAS intimates SID, IPC, IUD values to the UAC.

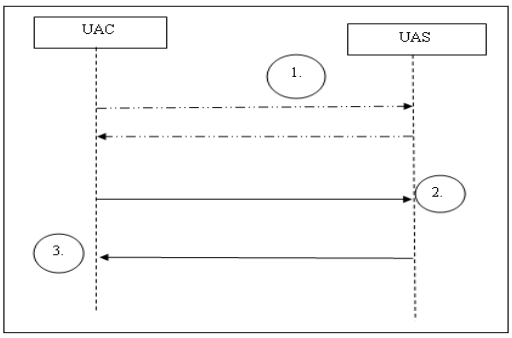


Figure 4: Initial Setup Phase

Phase 2: Verifying Phase:

1) UAC –UAS

Request (UID, hf [(((IPC ⊕ PC) ⊕ SKC) ⊕ SC)])

UAC first will forward UID, Password (PC) with Password Index (IPC) and mandatory Client Session keys (SKC) and Sequence Count (SC). First, the UAC computes the (IPC ⊕ PC) component and then XORed (⊕)with (SKC) and then last XORed (⊕)with SC components to get further component for subsequent communication. Then, these components are transformed into one-way hash digest, and it sends this hash with Client's ID (UID) to the UAS.

2) UAS—UAC

Challenge (Realm, hf[(((IPS ⊕ PS) ⊕ SKS) ⊕ SC)])

After receiving request from UAC,UAS computes hf [(((IPC ⊕ PC) ⊕ SKC) ⊕ SC)].Using SKC key the server could reconstruct the received Request digest for comparison. Then, it compares the computed digest with the received digest, and if the computed value does not agree with the received Request,

2a) then it discards the Request and further steps of authentication are stopped.

2b) If both the values do not match with each other, then, UAS realizes that the Request comes from authorized UAC.

3) UAC receives challenge from UAS

4) UAC—UAS

Response (UID, Realm, hf [(((IUD ⊕ UD) ⊕ SKC) ⊕ SC)])

UAC receives challenge from UAS and computes hf[(((IPS ⊕ PS) ⊕ SKS) ⊕ SC)].Using SKS key, the client could reconstruct the received Challenge for comparison .The computed Challenge is compared with the received hash digest Challenge.

4a) If both the values do not match, then the UAC will decline the Challenge and further steps of authentication between them are stopped

4b) If both the values match, then the UAC computes Response.

5) UAC sends response to UAS

6) UAS—UAC

Authentication (Code, Verifier, hf [(IPC ⊕ PC) ⊕(IPS ⊕ PS) ⊕ (IUD⊕UD) ⊕ (SKS ⊕ SC)])

The UAS receives the Response and it computes.

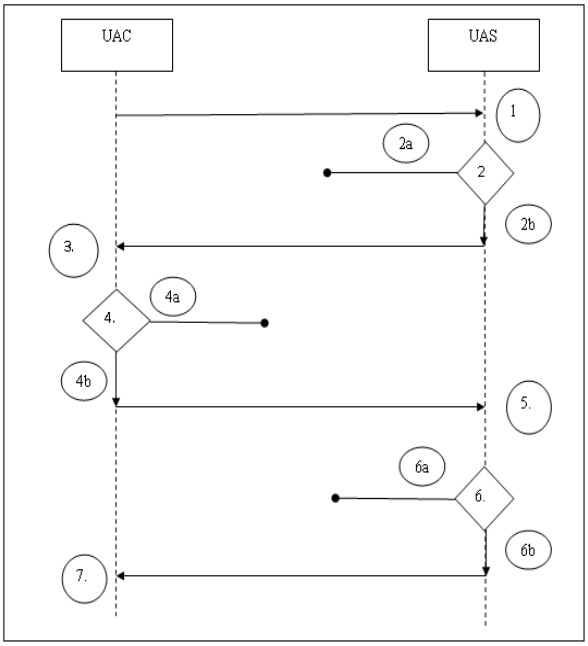
6a) If the computed values do not match with the received Response, then the UAS declines the Response.

6b) If both the values match with each other, then it computes Authentication

7) Verifies the Authentication Code and Authenticates the Server.

Finally both the parties i.e. UAC and UAS will be verified by each other because of predefined shared parameters.

Figure 5 shows above mentioned all 7 verifying phases for mutual authentication.



.

Figure 5: Verifying Phase

After combining both the phases Initial Setup phase (from 1 to 3) and Verifying phase (from 4 to 10) the proposed scheme looks like this.

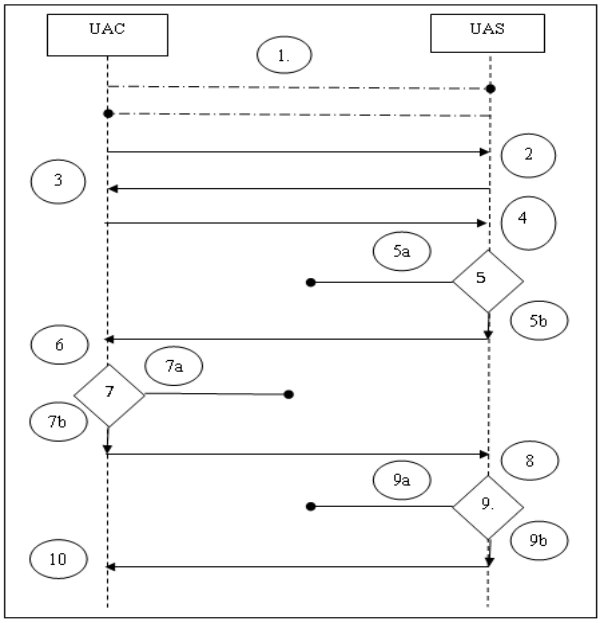


Figure 6: Authentication with Hash Digest and Sequential Count

5. CONCLUSION

In this paper, we have analyzed the different SIP authentication schemes. The attack types dealt by these authentication schemes have been analyzed. The methods, operations, and security features provided by these authentication schemes have also been analyzed. Our proposed authentication scheme has introduced hash digest sequence count challenge-response mechanism to enhance the authentication, efficiency, integrity and reliability for SIP. This authentication scheme prevents the Off-line Password guessing attack, Server spoofing attack, Man-in-Middle attack. The technique of this scheme emphasizes the security features enhancement in authentication process. Thus the proposed scheme enhances the network security in authentication process for Session Initiation Protocol.

6. REFERENCES

[1] Arkko J, et al. Security mechanism agreement for SIP sessions. IETF Internet draft, June 2002.

[2] Rosenberg J., Schulzrinne H., and Camarillo G., Johnston A., Peterson J., Sparks R., Handley M. and Schooler E. SIP: Session Initiation Protocol. RFC 3261, IETF. The Network Working Group, June 2002.

[3] Veltri L, Salsano S, Papalilo D. SIP security issues: the SIP authentication procedure and its processing load. IEEE Network; pp.16 (6):38e44, 2002.

[4] Franks.et al .HTTP Authentication: Basic and Digest Access Authentication.RFC 2617, June 1999.

[5] Jonathan Rosenberg, Henning Schulzrinne, Gonzalo Camarillo, Alan Johnston, Jon Peterson, Robert Sparks, Mark Handley and Eve Schooler. SIP: Session Initiation Protocol. RFC 3261 (Proposed Standard), June 2002. Updated by RFCs 3265, 3853, 4320, 4916, 5393, 5621, 5626, 5630, and 5922

[6] Qi Qui. Study of Digest Authentication, December 2003

[7] Peterson J. Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) FormatRFC 3893, IETF Network Working Group, September 2004.

[8] Yang. C. C., Wang. R. C., Liu. W. T. "Secure authentication scheme for session initiation protocol'', Computers & Security, vol. 24, pp. 381-386, 2005.

[9] Durlanik A, and Sogukpinar I. "SIP authentication scheme using ECDH," World Enformatika Society Transaction on Engineering Computing and Technology, vol. 8, pp. 350-3, 2005

[10] D. *Conference on Complex, Intelligent and Software Intensive Systems*, pp. 549-553, 2009.

[11] Santhosh Baboo. S, and Gokulraj K. "A Secure Dynamic Authentication Scheme for Smart Card based Networks," International Journal of Computer Applications, vol. 11, no.8, pp. 5-12, 2010.

[12] Y. P. Liao and S. S. Wang, "A new secure password authenticated key agreement scheme for SIP using self certified public keys on elliptic curves," *Computer Communications*, vol. 33, pp. 372-380,2010

[13] Bellovin, S. M., Merritt, M (1992). Encrypted key exchange: password-based protocols secure against dictionary attacks, IEEE symposium on research in security and privacy, p.72-84.

[14] Butcher, X. Li, and J. Guo, Members IEEE, "Security challenge and defense in VoIP infrastructures," *IEEE Transactions on Systems, Man, and Cybernetics part C: Applications and Reviews*, vol. 37, no.6, pp. 1152-1162, November 2007.

[15] Prtrik Park "VoIP Threats Taxonomy" CISCO Press, 24 Sept 2008.

[16] Tsai. J. L. "Efficient nonce-based authentication scheme for session initiation protocol, "International Journal of Network Security, vol. 8, no. 3, pp. 312-6, May. 2009.

[17] E. J. Yoon and K. Y. Yoo, "A new efficient authentication scheme for session initiation protocol," *International*