Securing SIP in VoIP Domain

Iyad Alsmairat
Department of Computing
Macquarie University
Sydney, Australia
iyad.al-smairat@students.mq.edu.au

Abstract

Voice service is vulnerable to a number of attacks that can compromise the confidentiality, integrity and authenticity of voice communication. As a result, this paper proposes a security protocol that protects these security aspects of voice service. The proposed security protocol identifies the security roles of the different components within VoIP domain applying SIP as the signalling protocol. The security protocol outlines the exchange of security credentials for two distinct scenarios: intra-domain and inter-domain communications. Moreover, this paper explains the implementation of the proposed security protocol within SIP operations and messages. This includes the insertion of the necessary security credentials, which are specified in the security protocol, in SIP messages, including both the header fields and body of SIP messages.

1 Introduction

VoIP stands for Voice over Internet Protocol. VoIP, as the name implies, relies on the internet, or so-called packet switching network, to deliver the voice service. The main advantages of VoIP include the ease of access, wide use, and low service cost. The infrastructure of VoIP uses several protocols for the signalling purpose such as MGC, MEGACO, H.323 and SIP.[1] SIP represents the de facto protocol in VoIP domains due to its features that facilitate the session signalling operation.

Alternatively, SIP, as the signalling protocol of VoIP domain, has a number of security complications. The attacks that mainly target the SIP and its architecture include that of registration hijacking, server impersonation, message body tampering, session tearing, denial of service, and so forth. Most of the attacks that can compromise VoIP service exploit security holes or one or more of the following security features: integrity, confidentiality, authenticity and availability. An attack can break down the service of VoIP in one of the following main phases of SIP operations: user registration, session setup and termination, and VoIP communication flow.

The paper is essentially structured as follows: Section 2 performs a literature survey on the existing security protocols that can elevate the security of VoIP. Section 3 describes and identifies the architecture of SIP as well as the main operational jobs of each SIP component. Section 4 contains the proposed security framework for SIP. Furthermore section 4 consists of several subsections. The first of these subsections specifies the security roles of SIP components. The second subsection outlines the major security credentials that need to be exchanged among the different SIP components. Moreover the concluding subsection illustrates the implementation of the described security protocol as part of the SIP architecture. Last but not least, section 5 presents both the summary and conclusion of the proposal.

2 Related Work

SIP employs some security measures to protect the communication between its users; however, these security measures are not sufficient to provide the acceptable level of protection to the VoIP service. (For more information regarding SIP security, refer to (Rosenberg et al., 2002), (Geneiatakis et al., 2005), (Thermos and

[1] MGC: Media Gateway Control
SIP: Session Initiation Protocol

Takanen, 2008), (Kultti, 2005), (Kuhn, 2005)). One of the security measures that SIP utilizes is called Digest authentication. Digest Authentication is a challenge-response authentication. One of the limitations of Digest authentication is that it is limited to user-to-user or user-to-proxy communications, but not applicable for server-to-server communication. Another limitation of Digest authentication is its inability to protect the confidentiality and integrity of communication. Digest only protects against re-play and illegal access attacks.

As a result, other auxiliary protocols can be utilized to elevate the security that is offered to VoIP. One of these supportive protocols is so-called S/MIME.[2] S/MIME is a protocol used to secure the confidentiality and integrity of SIP message body that is a MIME type. The deployment of S/MIME requires utilization of certificates along with keys. This operation mandates the presence of a key exchange mechanism in the structure of SIP.

Furthermore, a number of security protocols belong to different layers and can be used in VoIP networks. IPsec protocol, which belongs to layer 3, can be applied to protect the confidentiality and integrity of VoIP communication. However, IPsec has a number of drawbacks, for instance, it is a high-overhead protocol, non-scalable, assumes occurrence of trust among VoIP components, and so on. Another protocol, which is TLS, is a layer 4 protocol.[3] Although TLS protects the confidentiality and integrity of communication, it is applicable only for connection-oriented communications, e.g. TCP and SCTP.[4] This restriction limits the deployment of TLS across the entire VoIP network if UDP is implemented in some parts of the network.

All of the security protocols mentioned above are applicable for session setup, termination, registration. On the contrary, real VoIP communication occurs between two end users and takes precedence over RTP as the application layer protocol.[5] SRTP can also be used to secure RTP traffic, real-time traffic, such as voice.[6] SRTP requires a separate mechanism to manage the key agreement.

3 SIP Architecture

The architecture of the SIP domain mainly consists of a User Agent (UA) and Servers. There are several servers in SIP's domain with diverse functionalities including: Registrar Server, Proxy Server and Redirect Server. Figure 3.1 depicts the architecture of SIP along with the corresponding components.

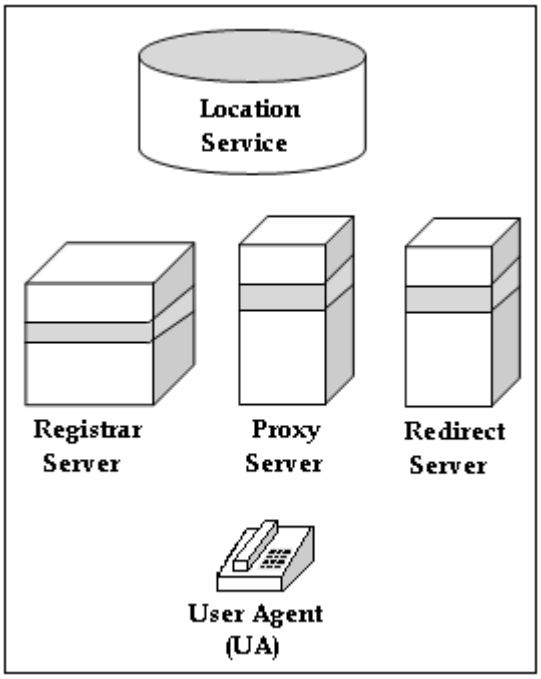

Figure 3.1: The Architecture of SIP Domain

A User Agent is the entity that works on behalf of the user to initiate and receive both SIP messages and VoIP sessions. There are two types of UA, depending on the roles of the UA: User Agent Client (UAC) and User Agent Server (UAS). UAC is the UA that initiates the request to establish VoIP session while UAS is the entity that receives the request and responds to it. The Registrar Server is responsible for registering the user with the domain so that the user can use the domain's services. The registration operation includes associating the user identity with his/her address. If the calling user is not aware of the address of the callee, the user can contact either the Proxy Server or the Redirect Server. The main difference between the Proxy Server and the Redirect Server is that the former takes care of the entire session setup operation; it forwards

[2] S/MIME: Secure Multipurpose Internet Mail Extension
[3] TLS: Transport Layer Protocol
[4] SCTP: Stream Control Transmission Protocol
[5] RTP: Real-Time Protocol
[6] SRTP: Secure Real-time Transport Protocol

the request to the next required entity. However the redirect server returns only the address of the callee to the caller and the caller continues with the remaining steps to establish the session.

4 Proposed Framework

This paper will now centre trapezoid SIP as the main scenario. Trapezoid SIP implies that both the session setup and termination operations are performed through the SIP proxy server, not directly between the end users. The proposal covers the main messages exchanged during the registration and session management stages. The proposal does not describe the additional required operations such as contacting the DNS to get the address of the registrar server, lookup process to obtain the address of the called party and so forth.

4.1 Security Roles

The first step that a user needs to perform before taking advantage of VoIP service is to authenticate with the SIP domain. There are two types of authentication that are required to keep the VoIP service safe, these are user authentication and device authentication. These authentications are necessary for a user to be able to sign onto several devices, and so that a number of users can use the same device. The registrar sever is responsible for the registration operation. This server is the entity that authenticates the different SIP component, e.g. user agent, proxy server, redirect server and so on within a SIP domain. In addition to binding the user identity to his/her address, the registrar provides the user with a token that validates its communications. This token specifies the registration period of that specific entity.

In order for a user to create a connection with another SIP user, even if he/she exists in the same SIP domain, the user needs to contact the proxy server to set up the session. In addition to managing the session, the proxy server acts as key management server. To be exact, the proxy server generates all of the essential security parameters required for the session that it creates between the two users and its key management. These essential parameters include the session key, key refreshment time, and the like. Moreover, the proxy server has the responsibility of checking both the validity and legitimacy of the certificates in inter-domain communications. As for the user agent, it is required to conceal the operational and security parameters of the created session from the user, to prevent from a direct user intervention.

4.2 Security Protocol

The proposed security protocol aims at protecting the security features of voice service. This includes protecting the integrity, confidentiality, authenticity and legitimacy of the communication. Additionally, the security protocol takes the SIP's structure into account whilst defining the sequence of message exchanges. There are two possible types of communication that can take place in a VoIP network, which are the intra-domain and inter-domain communications. As a result, the security protocol identifies the security credentials for both scenarios

4.2.1 Intra-Domain Communication

The notion of intra-domain communication refers to the communication that takes place within a single SIP domain. This means that the two end users, UAC and UAS, both belong to the same SIP domain. Fig 4.2.1 depicts the key security messages and their associated sequence. These messages start with the registration process and continue to cover the session setup. The security credentials that are carried by these messages are described in table 4.2.1.

In order to protect the confidentiality of the communication, the proposal utilizes two Types of keys: public/private and password-derives keys. These keys are symbolized as K_{PU}/K_{PR} and K_{PA}, respectively. Another key defined in the security protocol is the $K_{session,}$ which is generated by the proxy server to be used for the real voice communication between the end users.

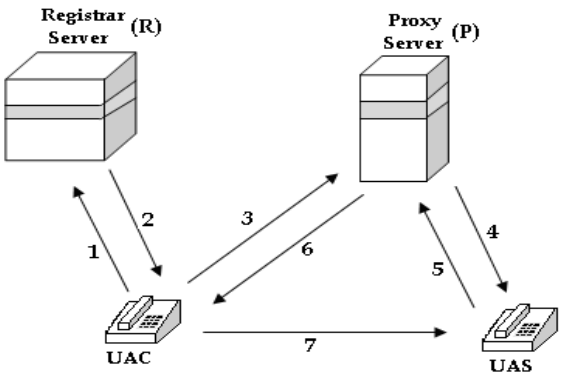

Figure 4.2.1: Security Messages of Intra-Domain Communication

Message	Credentials
1	UAC → R: user1, $CERT_{(UAC)}$, $K_{PA(USER1)}[N_{UAC-R}, UAC, t_{UAC-R}]$
2	R → UAC: $\{K_{PU(P)}\}K_{PR(R)}$, {user1, UAC, $T_{val(UAC)}$, $t_{R-UAC}\}K_{PR(R)}$, $K_{PU(UAC)}[N_{UAC-R}]$, $CERT_{(R)}$
3	UAC → P: {user1, UAC, $T_{val(UAC)}$, $t_{R-UAC}\}K_{PR(R)}$, { user2 , $t_{UAC-P}\}K_{PR(UAC)}$, $K_{PU(P)}[N_{UAC-P}]$, $CERT_{(UAC)}$
4	P → UAS: {user1, $t_{P-UAS}\}K_{PR(P)}$, $K_{PU(UAS)}[N_{P-UAS}, ID_{session(user1, user2)}]$, $CERT_{(p)}$
5	UAS → P: {user2, UAS, $T_{val(UAS)}$, $t_{R-UAS}\}K_{PR(R)}$, $K_{PU(P)}[N_{P-UAS}]$, $CERT_{(UAS)}$
6	P → UAC: $K_{PU(UAC)}[K_{session(user1,user2)}, N_{UAC-P}, ID_{session(user1,user2)}]$, $K_{PU(UAS)}[K_{session(user1, user2)}, t_{P-UAC}, ID_{session(user1, user2)}, N_{P-UAS}]$
7	UAC→UAS: $K_{PR(P)}[K_{session(user1, user2)}, t_{P-UAC}, ID_{session(user1, user2)}, N_{P-UAS}]$

Table 4.2.1: The Credentials of Security Protocol of Intra-Domain Communication

Also, the proposal applies digital signature mechanism to guarantee the integrity of the data. The digital signature mechanism has the notation of: {Data}Key. Similarly, encryption of data is referred to as Key[Data]. Furthermore, the other notations that are used in the protocol messages are as follows: N: nonce, t: timestamp, T_{val}: validity time, CERT: certificate. Lastly, another significant note is that the transmission of an entity's certificate can be used to extract the entity's public key.

The first message is sent by the UAC to the registrar server. In this message, the UAC needs to perform both of the user and device authentications. On one hand, the user authentication is done using the password-derived key. Besides the user, the registrar server should have knowledge of the user's password. On the other hand, the device authentication is performed by checking the validity of the device's certificate. Furthermore, the user attaches nonce and timestamp with the message to defeat any possible re-play attack. The nonce will be used later by the registrar server to prove its authenticity to the UAC.

In turn, the registrar server needs to acknowledge the success of the registration operation. Additionally, the registrar server provides the user with security token that proves the legitimacy of the user. This token, {user1, UAC, $T_{val(UAC)}$, $t_{R-UAC}\}K_{PR(R)}$, specifies the identity of the user and device, the validity time of this token, and the starting time of the registration operation. Moreover, the registrar server informs the user with the public key of the proxy server of this SIP domain.

The UAC then requests the proxy server (P) to create a session with the UAS. In order to validate its request, the UAC submits its own security token as well as its certificate. Besides, it generates a new nonce and transmits this new nonce to the proxy server.

Now, the proxy server forwards the session request to the UAS if the registrar server is aware of the UAS's address. Otherwise, the proxy server queries the location service about the UAS's address. The step of the called party's address lockup is not addressed in this paper. Besides the identity of the caller, the proxy server generates an identity to the session and attaches this session identity with the message. Indeed, the proxy server needs to transmit its certificate to the UAS so that the UAS can verify the legality of the proxy server.

In the fifth message, the proxy server generates a key for the session between the UAC and UAS. Moreover, the proxy server creates two versions of the session security message. The first version is destined to the UAC while the other one is destined to the UAS. Both versions bind the session identity with its associated key. It is important to notice the nonce that is presented in the UAS's version of the session security message. Since the proxy server is the only entity that knows this nonce, in addition to the UAS itself, the UAS makes sure that this message was generated by the proxy server by including this nonce inside the session security message.

Finally, the UAC sends the UAS's version of the session security message to the UAS once it receives it from the proxy server. At the end of this step, the session is securely established because only the involved entities have the knowledge of the session key.

4.2.2 Inter-Domain Communication

Inter-domain communication occurs in case a communication takes place between two end users belonging to two different SIP domains. The security messages that need to be exchanged between the different SIP components in the

inter-domain communication are described in Figure 4.2.2. Also, the corresponding contents of these messages are described in table 4.2.2.

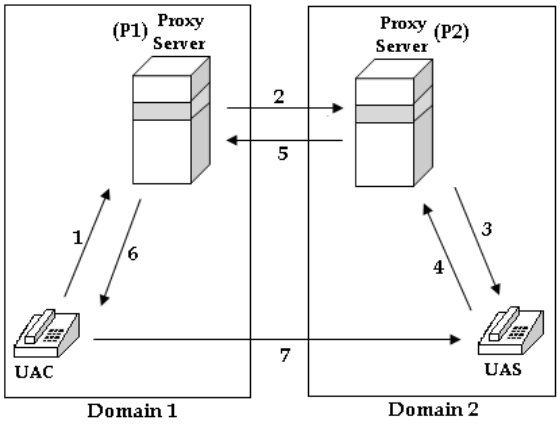

Figure 4.2.2: Security Messages of Inter-Domain Communication

Message	Credentials
1	UAC → P1: {user1, UAC, $T_{val(UAC)}$, t_{R1-UAC}}$K_{PR(R1)}$, {user2, t_{UAC-P1}}$K_{PR(UAC)}$, $K_{PU(P1)}[N_{UAC-P1}]$, $CERT_{(UAC)}$, $ID_{session(user1,user2)}$
2	P1 → P2: {user1, P1, user2, t_{P1-P2}}$K_{PR(P1)}$, $K_{PU(P2)}[N_{P1-P2}, ID_{session(user1,user2)}]$, $CERT_{(P1)}$
3	P2 → UAS: {user1, t_{P2-UAS}}$K_{PR(P2)}$, $K_{PU(UAS)}[N_{P2-UAS}, ID_{session(user1,user2)}]$, $CERT_{(P2)}$
4	UAS → P2: {user2, UAS, $T_{val(UAS)}$, t_{R2-UAS}}$K_{PR(R2)}$, $K_{PU(P2)}[N_{P2-UAS}]$, $CERT_{(UAS)}$
5	P2 → P1: {UAC,UAS}$K_{PR(P2)}$, $K_{PU(P1)}[N_{P1-P2,} ID_{session(user1, user2)}, K_{session(user1, user2)}]$, $K_{PU(UAS)}[N_{P2-UAS,} ID_{session(user1, user2)}, K_{session(user1, user2)}, t_{P2-UAS}]$, $CERT_{(P2)}$
6	P1 → UAC: $K_{PU(UAC)}[K_{session(user1,user2)}, N_{UAC-P1}, ID_{session(user1,user2)}]$, $K_{PU(UAS)}[N_{P2-UAS,} ID_{session(user1, user2)}, K_{session(user1, user2)}, t_{P2-UAS}]$
7	UAC→UAS: $K_{PU(UAS)}[N_{P2-UAS,} ID_{session(user1, user2)}, K_{session(user1, user2)}, t_{P2-UAS}]$

Table 4.2.2: The Credentials of Security Protocol of Inter-Domain Communication

In this scenario, an assumption has been made that the users are already registered with their respective SIP domains. Subsequently, the first message shows the request of the UAC to the proxy server to establish a session with the UAS. This message is similar to the one in the intra-domain communication. However, as the proxy server looks up the address of the destination, it notices that the UAS belongs to another domain. Therefore, the proxy server needs to query the location service about the address of the next hop's address, which is the proxy of domain 2 in this case. The proxy of the domain 1 (P1) sends its own certificate to its counterpart in domain2 (P2) so the latter verifies the validity of P1. This message should clearly tell P2 the destination of the session request. Additionally, P1 transmits a nonce and timestamp along with the session setup request message to P2.

If P2 validates P1 and is wiling to create a communication with domain 1, P2 forwards the session creation to the UAS. Also, P2 sends its certificate to the UAS to confirm its legality as the proxy server of domain 2. Again, the UAS hands in its security token as well as its certificate to P2.

At this point, P2 is sure of the legitimacy of both P1 and the UAS. As a result, it is confident to assign a session key to this specific session between the UAC and UAS. Furthermore, P2 generates two versions of the session security message. One of these two messages is designed to the UAS while the second is tailored to P1. It is necessary to note that the session security message that is designed to the UAS will be forwarded to the UAS through the UAC, not directly by P2. This is because P2 is sure about the legitimacy of P1 but not the other way around. So, if P1 checks and ensures the legality of P2, it forwards the session security messages to the UAC.

Likewise, P1 needs to encrypt the session security message, which is destined to P1, with the public key of the UAC. By receiving message 6, the UAC has the versions of the session security message. Subsequently, the UAC reads the message that is destined to it, and forwards the other version of this message to the UAS.

4.3 SIP Implementation

SIP implementation of the proposed security protocol involves the inclusion of the specified security credentials into SIP architecture. The SIP messages that are needed to transport these credentials contain REGISTER, INVITE, OK and ACK messages. The main structure of SIP messages is as follows: start-line, message-header and body structure. Both the header and body parts of these SIP messages can be used to convey the different security credentials.

The SIP representation of the messages of the proposed security protocol for both the intra-domain and inter-domain communication is depicted in tables 4.3.1 and 4.3.2. These two tables show the specific SIP messages that can be used to carry the security credentials of the security messages, which are shown in both figures 4.2.1 and 4.2.2.

Security message		SIP message
1	UAC → R	REGISTER
2	R → UAC	OK
3	UAC → P	INVITE
4	P → UAS	INVITE
5	UAS → P	OK
6	P → UAC	OK
7	UAC → UAS	ACK

Table 4.3.1: SIP Representation of Security Message of Intra-Domain Communication

Security message		SIP message
1	UAC → P1	INVITE
2	P1 → P2	INVITE
3	P2 → UAS	INVITE
4	UAS → P2	OK
5	P2 → P1	OK
6	P1 → UAC	OK
7	UAC → UAS	ACK

Table 4.3.2: SIP Representation of Security Messages of Inter-Domain Communication

We need to map the different security credentials with the SIP message header fields. The fist parameter that needs to be embedded in SIP messages is the users' identity. The users' identity contains two pieces of information: the caller's identity and the callee's identity. Evidently, the former can be revealed in 'From' header field whilst the latter can be extracted from 'To' header field. As for the device identity, 'Via' header field can be utilized to add the identity of every device forwards the message in the downlink transmission, from the UAC to the UAS. Besides, SIP messages contain timestamp header field which can specifies the time of sending the request from the UAC to the UAS. Furthermore, 'Date' header field is used to indicate the time of creating the request or response.

Although the nonce can be contained in the 'Authorization' header field, it is not appropriate to be included in this header filed because the nonce needs to be encrypted. Accordingly, the nonce needs to be added to the body of the SIP messages. Additionally, the session identity can be indicated in 'Call-ID' header field. The SIP message body can be utilized to rightfully include the following pieces of information: device certificate, session security parameters, e.g. session key, and validity time.

5 Conclusion

The paper specified a number of potential threats can break the security of VoIP service. This paper identified the security roles of the different SIP components. These roles were based on the structure of SIP to protect the integrity, confidentiality and authenticity of the VoIP service. In addition, this paper specified the security credentials that needed to be exchanged between the different entities during both the registration and session setup phases. The proposed security framework covered both scenarios: intra-domain and inter-domain communications. Furthermore, this paper explained a possible implementation for the proposed security framework within the structure of the SIP protocol. This implementation explains the ability of inserting the necessary security parameters, in either the header or body of SIP messages.

References

Geneiatakis, D., Kambourakis, G., Dagiuklas, T., Lambrinoudakis, C. and Gritzalis, S. July 2005. *SIP Security Mechanisms: A state-of-the-art review*, to be presented in the Fifth International Network Conference (INC 2005), Samos, Greece.

Kuhn, D. Richard; Walsh, Thomas J. and Fries, Steffen. 2005. *Security Considerations for Voice Over IP Systems*, Recommendations of the National Institute of Standards and Technology, pages 39 – 46, Special Publication 800-58, Gaithersburg, MD.

Kultti, Johan. 2005. *Secure Text in SIP Based VoIP*, Master of Science Thesis, page 39 – 51, Luleå University of Technology.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler. June 2002. *SIP: Session Initiation Protocol*, RFC 3261, Informative References.

Thermos, Peter and Takanen, Ari. 2008. *Securing VoIP Networks Threats, Vulnerabilities, and Countermeasures*, Key Management Mechanisms, pages 231 – 262, Pearson Education, Inc., Boston, MA.