SIP 프로토콜을 기반으로한 VoIP 네트워크를 위한 Secure Framework

한경헌[1], 최성종[1], 최동유[1*], 배용근[2]

조선대학교

Secure Framework for SIP-based VoIP Network

Kyong-heon Han[1], Sung-jong Choi[1], Dong-you Choi[1*], Yong-guen Bae[2]

[1] Dept. of Information and Communication Engineering, Chosun University

[2] Dept. of Computer Engineering, Chosun University

[1*]Corresponding author(E-mail : dychoi@chosun.ac.kr)

ABSTRACT

Session Initiation Protocol (SIP) has become the call control protocol of choice for Voice over IP (VoIP) networks because of its open and extensible nature. However, the integrity of call signaling between sites is of utmost importance, and SIP is vulnerable to attackers when left unprotected. Currently a hop-by-hop security model is prevalent, wherein intermediaries forward a request towards the destination user agent server (UAS) without a user agent client (UAC) knowing whether or not the intermediary behaved in a trusted manner. This paper presents an integrated security model for SIP-based VoIP network by combining hop-by-hop security and end-to-end security.

Keywords

SIP, protocol, security, communication

1. Introduction

Session Initiation Protocol (SIP) [1] is an application-layer signaling and control protocol for creating, modifying, and terminating sessions including Internet telephone calls, multimedia distribution, and multimedia conferences. Flexible, extensible and open, SIP becomes the most promising candidate as the signaling protocol for IP telephony and it has been chosen by the Third-Generation Partnership Project (3GPP) as the protocol for multimedia application in 3G mobile networks. As the SIP-based service is getting popular, it is facing severe security threats. Significant research and development effort is devoted to the security enhancement to SIP [4].

SIP supports hop-by-hop security using Transport Layer Security (TLS) [6] or by IPSec [5] and end-to-end security using Secure MIME (S/MIME) [7]. Hop-by-hop security assumes that a SIP UA (user agent) trusts all proxy servers along its request path to inspect the message bodies contained in the message while end-to-end security assumes that a SIP UA does not trust any proxy servers to check the message [2]. Hop-by-hop security cannot prevent attacks from malicious intermediaries while end-to-end security provides higher degree of security and better level of performance.

Figure 1 [3] shows four security steps for end-to-end communication within SIP signaling. SIP uses the existing security mechanisms, such as HTTP digest authentication, TLS, IPsec/IKE, S/MIME. There are no specific vulnerabilities in client-server security scheme for registration and in hop-by-hop security scheme (user-to-server and server-to-server security) for setup.

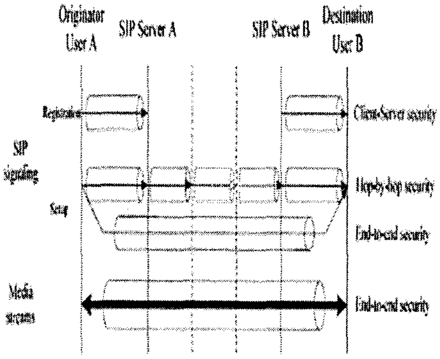

Figure 1: Steps of the end-to-end communication in SIP.

Low-power terminals such as mobile SIP phones have several fundamental limitations. They have very limited CPU power, memory size, and display area. It also requires less power consumption due to battery capacity, and their input device is harder to operate than the typical desktop computers.

Most security mechanisms process key management in SIP signaling takes four steps [3]:

· Negotiate the cipher site,
· Perform mutual authentication using a long term key,
· Set up a secure session to share a session key,
· Exchange the session key in the secure session.

Basically, the specific requirements for low-power terminals in end-to-end security mainly include: lightweight security overhead and dynamic trust.

2. Hybrid Security Model

The hybrid model is proposed based on the assumption that a user trusts the first next-hop server and trusts an opposite-side user via transitive trust. We name the first next-hop server the neighbor servers which here act as security agents to share the security overhead for low-power terminals. We also assume that a hierarchical CA system exist for intermediate servers. In most cases, servers are much stable than UAs so that it is easier for intermediaries to build a hierarchical CA system.

The proposed model is constructed by leveraging the trusted neighbor server to share heavy load in fulfilling security schemes. Its security pattern is a combination of hop-by-hop (user-to-server) and end-to-end (server-to-server) security, shown in Figure 2.

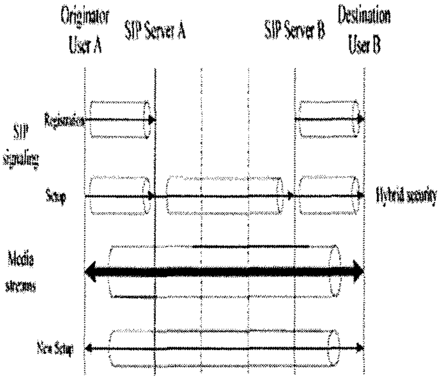

Figure 2: Steps of the hybrid model.

A user and a SIP server authenticate each other when the user registers his own location address. The user requests the server for the help on secure signaling due to its limited capacity. Also powerful users can choose not trusting the neighboring servers and initialize traditional end-to-end secure signaling by themselves.

After the above step, the setup secure session has already been done at registration. The session key exchange can be executed during setup with extended SDP [8]. This allows the encryption of media streams at the application layer.

Considering the dynamic trust, users should authenticate each other not only before the first time signaling but also before a new setup signaling. In this scheme, users use the setup keys to directly authenticate their peers in next setup signaling. The exchange of the setup key can be executed during registration at the first time and be executed during termination afterwards. Setup keys are also dynamic for their limited life time which is determined by the session participants.

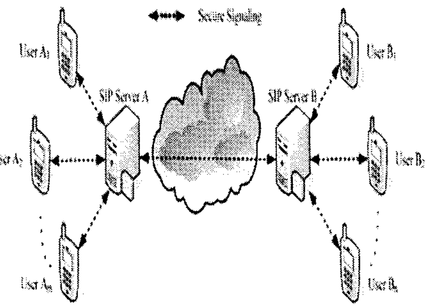

Figure 3 – Application Scenario

Figure 3 defines the application scenario. We consider (m to n) scenario to indicate that there are m originators in domain A and n destinations in domain B. In a direct peer-to-peer (i.e. user-to-user, user-to-server or server-to-server) signaling, caused by mutual agreement and authentication, the additional load and the additional delay.

It can be seen that the hybrid model needs no direct user-to-user security mechanism agreement and no user-to-user authentication. If every originator in domain A goes to setup secure communication with every destination in domain B, they do not need to make secure signaling directly to peers one-by-one. They only need trust the neighbor servers.

3. Conclusion

This paper discusses SIP security requirements for low-power terminals in end-to-end communication and put forward a lightweight secure SIP model by combining the hop-by-hop security and end-to-end security. The trusted neighbor servers in our model provide crucial benefits in terms of key management and security load share. Dynamic trust is achieved by using setup keys to prevent malicious attack towards both low-power terminals and neighbor servers.

In future, we will conduct the simulation of the hybrid security model for VoIP network in order to evaluate performance of such a model with other existing systems.

Reference

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

2. K. Ono and S. Tachimoto, "Requirements for End-to-Middle Security for the Session Initiation Protocol (SIP)," IETF draft-ietf-sipping-e2m-sec-reqs-06, March 2005.

3. K.Ono and S.Tachimoto, "SIPsignalingsecurityforend-to-endcommunication,"Proc.of9thAsia-PacificConferenceonCommunications,APCC2003,Sept.2003.

4. S. Salsano, L. Veltri, and D. Papalilo, "SIP Security Issues: The SIP Authentication Procedure and its Processing Load," IEEE Network, 16(6): 38-44, Nov/Dec 2002.

5. S. Kent,R. Atkinson "Security Architecture for the Internet Protocol", Request for Comments: 2401, November 1998

6. T. Dierks and C. Allen, "The TLS Protocol Version 1.0," IETF RFC 2246, Jan. 1999.

7. B. Ramsdell, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification," IETF RFC 3851, July 2004.

8. M. Handley and V. Jacobson, "SDP: Session Description Protocol," IETF RFC 2327, April 1998.

※ This work was supported by research funds from chosun university, 2008.