Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A dependable privacy protection for end-to-end VoIP via Elliptic-Curve Diffie-Hellman and dynamic key changes

Chia-Hui Wang [a,*], Yu-Shun Liu [b]

[a] *Department of Computer Science and Information Engineering, Ming Chuan University, Tauyuan County 333, Taiwan*
[b] *Lite-On Technology Corporation, Taipei 114, Taiwan*

ARTICLE INFO

Article history:
Received 4 March 2010
Received in revised form
21 August 2010
Accepted 28 October 2010
Available online 4 November 2010

Keywords:
VoIP
AES
SIP
Elliptic-Curve
Diffie-Hellman key negotiation
Key distribution

ABSTRACT

Voice over IP (VoIP) service has been widely deployed over the prevalent Internet due to the advanced technologies of digital voice compression, communication protocols, and wired/wireless networks. VoIP then benefit much lower cost of equipment, operation, and better integration with data applications than voice communications over telephony networks. On the other hand, VoIP further introduce security vulnerability while delivering voice packets over the public Internet, using the transparent IP protocol suite. The most popular solution to secure VoIP voice packets is to apply cost-effective AES encryption with a single key during to a voice call. In this paper, to further enhance the VoIP security to prevent malicious eavesdroppers, we propose a much stronger privacy protection for an end-to-end VoIP. This dependable solution applies not only the Elliptic-Curve Diffie-Hellman (ECDH) algorithm for key negotiation, but also the key generation function (KGF) for changing key dynamically in a VoIP call session. This 2-tier key distribution scheme provides effective and robust security for VoIP voice packets during the end-to-end call session. This proposed scheme has been deployed on an opensource SIP-based phone as our test-bed over the Internet. The performance results from the experiments with the Internet dynamics of packet loss inserted on the test-bed demonstrate that the proposed scheme not only provide more secure VoIP call, but also preserve the quality of voice packet delivery.

1. Introduction

Voice over IP (VoIP) technology converts the analog speech signals to digital voice data, apply voice codec to compress the voice data packets, and transfer the compressed voice data via Internet Protocol (IP) packets over Internet (as shown in Fig. 1). Thanks to the pervasive Internet access via wired/wireless networks, using VoIP can benefit from low cost devices, deployment, operation, and maintenance than conventional telephony. Besides, VoIP can be easily integrated with other applications to foster or furnish more diversified applications, such as videophones, instant message systems, and online games, etc.

The infrastructure of VoIP is generally composed of terminals (i.e. phones), proxy server, gateways, and IP networks. As shown in Fig. 2, the VoIP system communications with VoIP peer using the Intranet and Internet. Through the gateways, VoIP phones can further interact with the telephones in public-switched telephone network (PSTN). To emulate the conventions of telephone calls, VoIP voice channel setup is also done by signaling. The signaling protocol can be applied to initiate and manage VoIP connections or calls between terminals. H.323 (2006) and Session Initiation Protocol (SIP) (Rosenberg et al., 2002; Schulzrinne and Rosenberg, 1999) are widely used signaling standards for VoIP call setup and management (e.g. registration, resource administration, status, capability exchange, etc.)

However, Internet possesses the inherent attributes of applying open technologies and sharing with the public. The voice communication usually preserves privacy and value information. As illustrated in Fig. 1, while the voice packets of VoIP calls are delivered and exposed to the unsecured public Internet, and then the VoIP calls are easier to be threatened by eavesdroppers than conventional telephone calls (Palmieri and Fiore1, 2009; Keromytis, 2010; Butcher et al., 2007; Thermos et al., 2009). In the circuit-switched telephone network, it is quite difficult to tap into a phone call at any place, except the last-mile analog circuit.

Therefore, the aim of our paper is to design and develop an effective solution to provide strong security protection for the prevalent VoIP service. The proposed solution will ensure the confidentiality and integrity of the voice communication over Internet. But, the challenge is the interactive VoIP service preserves more sensitivity to transmission delay than other Internet multimedia applications. Thus, the time-consuming privacy protection for VoIP service must be cost-effective without degradation of the quality of real-time voice communication in interactions.

[*] Corresponding author.
E-mail addresses: wangch@mail.mcu.edu.tw (C.-H. Wang), sky.ys.liu@liteon.com (Y.-S. Liu).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.10.011