ELSEVIER

Computer Communications 26 (2003) 552–565

computer communications

www.elsevier.com/locate/comcom

Performance analysis of secure session initiation protocol based VoIP networks

Mohan Krishna Ranganathan*, Liam Kilmartin

Communication and Signal Processing Research Unit, Department of Electronic Engineering, National University of Ireland, University Road, Galway, Ireland

Received 19 February 2002; revised 18 June 2002; accepted 25 June 2002

Abstract

The commercial deployment of voice over internet protocol (VoIP) networks (and associated packet switching technologies) has gathered pace in the recent years. However, a major concern with such networks is the issue of the security of networks based on such open standards. Little research has been carried out into examining the options for securing VoIP networks and, more specifically, the impact which implementing such security architectures and protocols will have on the performance of such secure networks. This paper describes the research, which has been carried out into the development of a realistic model for carrying out simulations of the performance of secure session initiation protocol based VoIP networks. The results of the performance analysis obtained using this model are presented with a discussion of the implications of these results for designers considering implementation of real secure VoIP networks.

Keywords: Voice over internet protocol; Security; IP Security; Security protocol performance analysis

1. Introduction

> Starting as a hobbyist movement five years ago, "Voice over Internet Protocol" is quietly remaking the telephone system worldwide. It is one of the venerable network's biggest overhauls in decades—but not its last by a long way.

The Economist, March 2001.

The recent years has seen the growth of internet protocol (IP) based networks (e.g. Internet) at a thriving pace. The rapid proliferation and ubiquitous nature of the Internet, for example, has now given rise to strong interest in using IP based networks for carrying non-conventional information like the voice, multimedia, etc. The use of the Internet as a transport network for speech signals is currently in its infancy. The sharing of existing network infrastructure between data applications and voice calls, and the sharing of access and transport services helps in reducing implementation, management and support costs. This also provides an opportunity for new services and applications, which were not feasible with traditional circuit-switched telephony networks, to be developed. Even with all these benefits, wide spread commercial deployment of voice over IP (VoIP) is still restricted [1] due to the challenges posed by the nature of the Internet. However, it is widely accepted that next generation networks will use the Internet Protocol, or some variant thereof, as the networking protocol of choice for supporting multimedia traffic, and voice traffic in particular.

There remains a great deal of research, which still needs to be carried out into the particular problems which need to be solved for VoIP networks to be a technical and commercial success. The non-deterministic nature of the Internet, and the impact, which this specifically has on voice traffic, is one major area of concern. Inherent problems with security due to the 'open' nature of public IP networks are also of equal importance. This paper focuses on the challenges and impact of employing security services into VoIP networks. The security requirement considerations of VoIP networks are highlighted along with the available security service options for the different VoIP architectures. A simulation model of an IPSec secured session initiation protocol (SIP) based VoIP network is presented along with a discussion of the simulated network performance as

* Corresponding author. Tel.: +353-91-750326; fax: +353-91-750511.
E-mail address: mohan.krishna@nuigalway.ie (M.K. Ranganathan).

0140-3664/03/$ - see front matter
PII: S0140-3664(02)00146-9

obtained from this model. A number of implications for real secure network designers and operators arising from this research are highlighted.

2. VoIP architectures

Unlike the circuit-switched PBX scenario, the IP world is dominated by open systems, and hence the need for *standards* to ensure interoperability between devices manufactured by various vendors. Currently, many organisations are in the process of developing standards for session signalling over packet based networks, and the choice for VoIP vendors and manufacturers would be to select the architecture that would support emerging trends.

H.323 [2], adopted in 1996 by the international telecommunications union (ITU), was the first call control standard developed for VoIP. H.323 is an umbrella recommendation suite, which defines audio, video and data communications across local area networks (LANs) that do not guarantee quality of service (QoS).

Even though H.323 was the widely deployed signalling protocol for VoIP, a newer signalling protocol, SIP has gained significant momentum [3] recently as an alternative to H.323, mainly due to its simplicity and efficiency.

The SIP [4,5] is a generic application layer session management protocol, developed by the internet engineering task force (IETF) multi-party multimedia session control (MMUSIC) working group and was standardised in 1999.

SIP provides for advanced signalling and control functionality for a wide variety of multimedia services including VoIP. The syntax and semantics of SIP are heavily borrowed from the popular HTTP and SIP works on the same request–response model as in HTTP. The functionality of SIP is similar to telephony signalling protocols, such as Q.931 [6], but only in an Internet context. SIP also differs from the traditional telephony signalling protocols, in that it does not reserve resources or establish circuits (virtual or real) in the network.

2.1. The VoIP protocol stack big picture

As seen in Fig. 1, there are two main aspects of VoIP (1) the call signalling and call controlling information and (2) the media (speech) information. The protocol stack defines the method of carrying both the signalling and media information.

The well-established VoIP protocol stack can support a variety of underlying network types (typically LAN standards) below the network layer. A VoIP terminal, connected to such networks, has traditionally been a PC equipped with audio peripherals (i.e. speakers and microphones) but many networking manufacturers are now supplying standalone VoIP terminals. The internetworking protocol (IP) networking layer operates above whichever networking technology is in operation. The user datagram protocol (UDP) operates in the transport layer in order to provide a suitable end-to-end protocol for this type of multimedia application. UDP does not, however, adequately support some of the needs of real-time audio being transported over an IP network. Hence, a companion transport layer protocol operates above UDP to provide specific support required by such real-time multimedia applications as VoIP. This additional transport layer protocol suite actually consists of two protocols, namely the real-time transport protocol (RTP) [7] and the real-time transport control protocol (RTCP).

The application layer effectively implements whichever audio or speech codec is in use by the VoIP terminal (e.g. G.711, G.721, G.728, etc.), and uses the RTP layer to transport the media stream. The application layer also implements the call signalling and control protocol to establish, control, and terminate VoIP calls, as well as to invoke any of the multitude of supplementary services that can be supported by a VoIP network (e.g. SIP, H.323).

3. VoIP security requirements

As every VoIP network is essentially an IP network, VoIP network and terminals face the same security threats

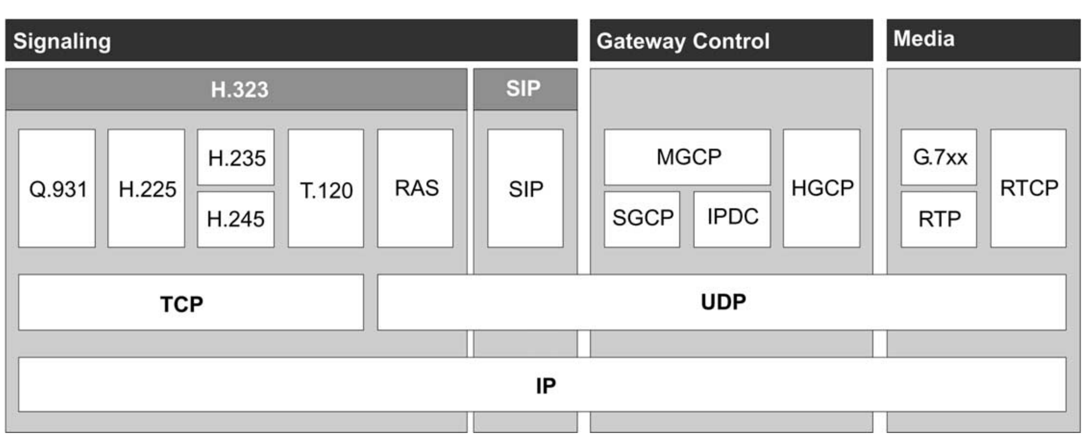

Fig. 1. VoIP protocol stack.