

# 基于 H.323 协议的 VoIP 安全问题探讨

姚玉坤 刘合武

(重庆邮电大学通信学院 重庆 400065)

**摘要** 本文简要介绍了 H.323 协议网络结构、子协议功能及工作流程。分析了 VoIP 网络系统潜在的威胁及安全要求,最后结合 H.323 VoIP 的通信流程,分析了 H.235 建议所采用的安全措施。

**关键词** VoIP H.323 H.235

## 1 引言

VoIP (Voice over IP) 通过对语音信号进行编码数字化,压缩处理成压缩帧,然后转换为 IP 数据包在 IP 网络上传输,从而完成语音通话的业务。VoIP 技术使我们可以基于互联网实现电话业务。这种语音通话业务的实现模式能提供更多的集成功能、更高的通信带宽以及更灵活的管理能力,并能够显著降低成本。近年来,VoIP 得到了迅猛发展和广泛应用。

目前,VoIP 有两种常用的应用层控制(信令)协议:H.323 协议和会话初始协议(SIP, Session Initiation

Protocol)。两者的信令功能基本相同,都是利用实时传输协议(RTP, Real-time Transport Protocol)进行媒体传输。SIP 是由 IETF 提出的一个在基于 IP 网络中实现实时通信应用的一个应用层控制信令协议。H.323 由 ITU-T 提出,它描述了在服务质量无保证的分组网络中提供多媒体通信业务的多媒体通信系统,它继承了通信领域传统的集中、分层控制的设计思想,在传统电信网络向基于 IP 的电信网络过渡的过程中,可以利用原有设备,避免了资源浪费。正是这些方面的特点,使得 H.323 已成为电信运营商、行业部门、企业建设 VoIP 网络广泛采用的协议方案。本文主要以 H.323 为例来分

姚玉坤:副教授,硕士生导师,主要研究方向为数据通信与 IP 网络技术。

---

## Security Analysis of SIP in NGI

Li Feng Tang Baomin

(Nanjing University of Posts & Telecommunications, Nanjing 210003)

**Abstract** In this paper, SIP security threats model is introduced, then the security issues in the application of SIP is studied. There are two aspects (SIP conversation process and the registration process) show a detailed study of the safety in SIP. For the certification process, I proposed a clear authentication mechanism, which safety can be assured from the theoretical study. Thus, the security issues in SIP can be not only an overall but also a micro clear grasp.

**Keywords** SIP, security threats model, registration and authentication

析和探讨 VoIP 网络的安全问题。

2 基于 H.323 的 VoIP 系统简介

H.323 起初并不是为 VoIP 专门提出的,但因为非常适合电话到电话经由网关的这种 VoIP 工作方式,所以被借过来作为 VoIP 的标准。基于 H.323 的 VoIP 网络系统通常包括 H.323 终端(如 PSTN 话机、PC 终端等)、网关、关守 (gatekeeper) 和多点控制单元 (MCU), 如图 1 所示。

图 1 中, H.323 VoIP 网络的各实体的功能如下。

H.323 终端是 IP 网络中能提供实时、双向通信的节点设备,也是一种终端用户设备,可以和网关、多点接入控制单元进行多媒体通信。

网关用于连接 H.323 网络与非 H.323 网络(如 ISDN,POTS),网关通过转换呼叫建立和释放协议,来转换两个网络的不同媒体格式。

关守主要负责电话号码和 IP 地址之间的转换。他们还负责管理带宽并提供终端登记和认证机制。同时关守还提供了诸如呼叫传输、呼叫转发等服务。

MCU 提供对三方终端以上的电话会议的支持。所有参与会议的终端与 MCU 建立一个连接。MCU 管理会议资源,语音(视频)编码算法,还可以管理媒体流。

H.323 协议是一个庞大的协议族,其中又包括许多相关的子协议,形成了一个协议栈,如图 2 所示。

从图 2 可以看到, H.225.0 和 H.245 是 H.323 系统的核心协议。H.225.0 负责呼叫控制,主要包括两部分:呼叫接纳信令(RAS)和呼叫信令协议。RAS 主要用于传送终端登记信息、认证信息和呼叫处理信息;呼叫信令协议基于 Q.931 而制定,主要用于完成呼叫建立过程,也常称为 Q.931 信令。H.245 用于媒体控制,主要实现媒体流通信信道的建立、维护和释放。RTCP 是媒体流实时传输控制协议,RTP 是媒体流实时传输协

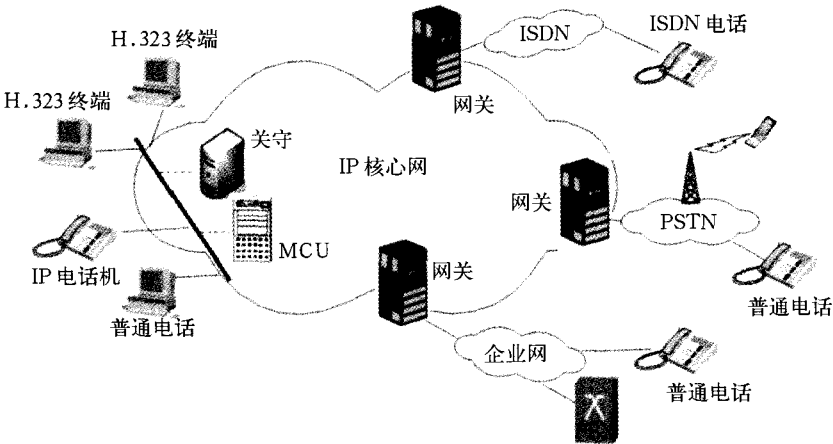


图 1 基于 H.323 VoIP 网络体系示意图

音、视频应用		终端控制与管理				数据应用
音频 G.711 G.722 G.723.1 G.728 G.729	视频 H.261 H.263 H.264	RTCP	H.225.0 RAS 信令	H.225.0 呼叫信令	H.245 控制信令	T.124 T.125
加密						
RTP	认证					
不可靠传输（UDP）				可靠传输（TCP）		T.123
网络层（网络协议）						
链路层						
物理层						

图 2 H.323 协议栈

议。媒体流安全传输将使用 H.245 信道中给出的算法与密钥进行编码。

H.323 终端之间建立通信关系通常执行四个控制过程: RAS, H.225.0 呼叫控制 (Q.931 信令), 连接控制 (H.245) 及媒体 RTP 信道建立的过程。

图 3 简要描述了一个基于 H.323 的 PC2PC 的 VoIP 呼叫的建立过程以及呼叫过程中各相关协议的控制作用。当一个 H.323 终端想要与另一个端点建立呼叫时, 首先, 源端点使用 RAS 信令从一个关守那里获得许可; 然后, 源端点使用 H.225.0 呼叫控制 (Q.931 信令) 来建立与目的端点的通信; 接着, 源端点使用 H.245 连接控制信令与目的端点协商媒体参数并建立 RTP 信道; 最后, 两端点通过 RTP 信道进行媒体传送。

本文共5页，欲获取全文，请点击链接<http://www.cqvip.com/QK/82867X/200709/25722157.html>，并在打开的页面中点击文章题目下面的“下载全文”按钮下载全文，您也可以登录维普官网（<http://www.cqvip.com>）搜索更多相关论文。