VoIP技术及其安全性研究

Research on VoIP and its Security

白芸洁 李娜

Bai Yunjie Li Na

(郑州交通职业学院信息工程系，河南 郑州 450062)

(Department of Information Engineering, Zhengzhou Jiaotong University, Henan Zhengzhou 450062)

摘 要:本文首先介绍了VoIP技术的研究和发展方向,通过分析VoIP的核心协议—SIP协议的安全问题和研究现状,说明VoIP安全性能的研究内容和现实意义,最后给出了本研究的发展方向。

关键词:VoIP; SIP协议; 安全

中图分类号:TP393 **文献标识码**:A **文章编号**:1671-4792-(2010)5-0075-03

Abstract: This paper introduces the research and development of VoIP technology first, and illustrates the research contents and practical significance of VoIP security performance by analyzing the core protocol-SIP's security issues and the current research.In the end,this paper gives the development direction of this study.

Keywords: VoIP; SIP Protocol; Security

0 引言

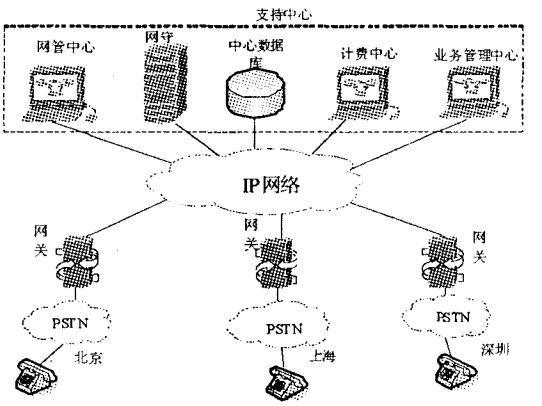
随着IP网络的发展,VoIP技术得到了广泛应用,逐步改变了只有传统电信网络提供语音通信的局面。SIP是实现VoIP连接的主要信令控制协议。由于SIP消息具有基于文本格式的特点,容易遭受注册攻击、伪装服务器、篡改消息体、终止会话和拒绝服务等威胁,影响通信网络的安全性,因此有必要对VoIP的安全性能进行研究。

1 VoIP概述

VoIP(Voice over IP)是一种在传统电路交换网络和IP网络之间传输语音或者直接在IP网络中传输语音的技术。语音信号通过公用电话网络被传输到IP电话网关，然后网关将话音信号进行数字化编码,压缩处理成压缩帧传递进入Internet;而这些数字信号通过遍及全球的成本低廉的网络将信号传递到对方所在地的网关,再由网关将数字信号还原成为模拟信号,输入到当地的公共电话网络,最终将语音信号传给发送方,从而完成语音通话[1]。

图一为一个常见的VoIP网络图。VoIP可以在IP网络上以低成本传送语音、传真、视频和数据业务。和传统的电路交换网络相比,VoIP网络采用分组交换技术,能够更加高效的利用网络资源,并且采用高效的语音编码技术,降低了运营成本。

2 VoIP关键技术



图一 VoIP网络示意图

VoIP的关键技术包括信令技术、编码技术、服务质量(QoS)保证技术以及网络传输技术等。

语音编码技术：包括流行的G.711、G.722、G.728、G.729和G.729A技术，话音压缩编码算法和MPEG-II多媒体压缩技术。

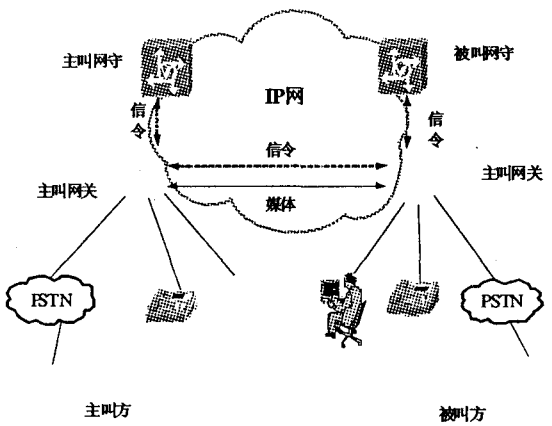
信令技术：包括ITU-T的H.323协议和IETF的会话初始化协议SIP。

QoS保障技术:采用资源预留协议RSVP和用于业务质量监控的实时传输控制协议RTCP来避免网络拥塞，保障通话

质量。

3 VoIP 网络构成

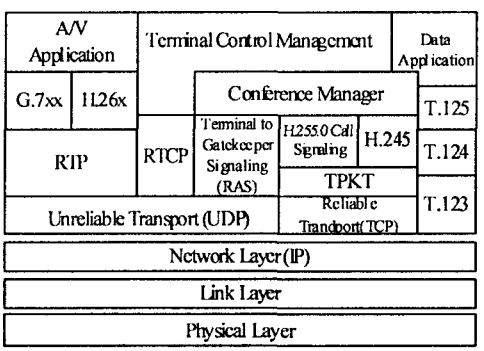
VoIP 系统可以实现 PC 和传统电话之间的通信、PC 间的通信以及传统电话间的通信。总体来说，VoIP 网络主要由主、被叫接入终端；主、被叫网关；主、被叫网守组成，如图二所示。



图二　VoIP 系统结构

目前，存在一些 VoIP 协议类型，主要包括 H.323、SIP 和 MGCP。

H.323 [2] 是 ITU-T 制定的信令标准，最初用于局域网(LAN)上的多媒体会议，后来扩展至覆盖 VoIP。该标准既包括了点对点通信也包括了多点会议。H.323 定义了四种逻辑组成部分：终端、网关、网守以及多点控制单元(MCU)，图三为 H.323 协议栈结构。

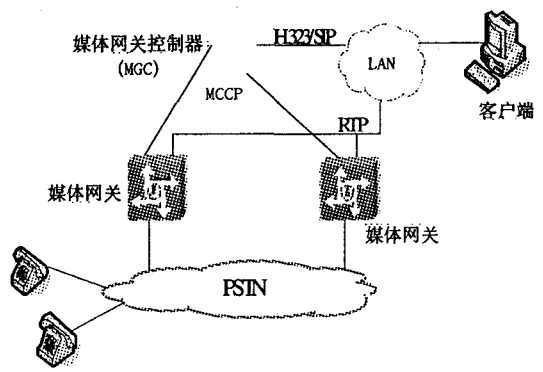


图三　H.323 协议栈

H.323 将可靠的 TCP 用于 H.245 控制信道、T.120 控制信道、呼叫信令信道；视频和音频信息采用不可靠的、面向无连接的传输方式，即利用用户数据协议 UDP。

会话发起协议 SIP(Session Initial Protocol)是建立 VoIP 连接的 IETF 标准。它属于应用层控制协议，用于和一个或多个参与者创建、修改和终止会话。SIP 的结构与 HTTP(客户－服务器协议)相似。客户机发出请求，并发送给服务器，服务器处理这些请求后给客户机发送一个响应，该请求与响应形成一次事件。

媒体网关控制协议(MGCP)定义了呼叫控制单元(呼叫代理或媒体网关)与电话网关之间的通信服务。MGCP 属于控制协议，允许中心控制台监测 IP 电话和网关事件，并通知它们发送内容至指定地址。在 MGCP 结构中，智能呼叫控制置于网关外部并由呼叫控制单元(呼叫代理)来处理。同时呼叫控制单元互相保持同步，发送一致的命令给网关。



图四　媒体网关和媒体网关控制器

图四为媒体网关和媒体网关控制器网络示意图。媒体网关控制协议(Megaco)是 IETF 和 ITU-T 共同努力的结果。它是一种用于控制物理上分开的多媒体网关协议单元的协议，从而可以从媒体转化中分离呼叫控制。Megaco 通知 MG 将来自于数据包或单元数据网络之外的数据流连接到数据包或单元数据流上，如实时传输协议 RTP[3]。

4 SIP 协议安全问题及研究现状

由于 VoIP 是基于 IP 网络的，所以 VoIP 安全性研究变得尤为重要。H.323 协议簇中有 H.325 协议，专门用来保护 H.323 消息的完整性和一致性。但 SIP 协议设计之初，很少注意它的安全机制，而是把重点放在协议的灵活性和扩展其功能方面。随着 SIP 协议的广泛应用，安全性是 SIP 通信过程中的一个关键问题，现在已经有越来越多的人致力于解决 SIP 安全问题。

SIP 的语法格式类似于 SMTP 和 HTTP，并使用 URI(Universal Resource Identifier，统一资源标识符)来表示地址，形如"alice@atlanta.com"。这种以文本形式表示消息的语法容易被攻击者模仿、篡改，加以非法利用。又因为 SIP 用户广泛分布于互联网中，互联网遭受到的各种攻击都可能威胁 SIP 安全。所以 SIP 安全防范的范围很大，并且难以部署各种安全措施[4]。

常见的SIP消息攻击手段有注册攻击、伪装服务器、篡改消息体、终止会话、拒绝服务。SIP允许第三方代表用户注册联系信息，这就使攻击者恶意注册成为可能，攻击者往往利用自己的认证信息对受害者进行注册劫持。

防止SIP攻击的最好方法是保证信息的私密性和完整性，防止重放攻击和信息欺骗，提供会话的验证和信息保密，防止拒绝服务攻击。但是SIP还没有自身的安全协议，主要是依靠现有保护IP网络的各种安全协议来保障SIP安全。具体来说主要有IPSec保护网络层，TLS保护传输层安全，PGP加密、S/MIME和HTTP-Digest摘要认证等。由于这些安全机制并不是专门针对SIP设计的，在SIP终端难以部署这些机制。所以研究合适的针对SIP的安全机制，加强安全支持是今后SIP的研究热点[5-6]。

SIP早期是用于在带宽资源丰富的环境中，但是随着SIP的不断扩展，应用范围日益广泛，现在很多无线环境中已经开始应用SIP作为通话的核心控制协议，这就使得原先的SIP在带宽资源有限的环境中传输时就会显得SIP消息过于庞大。另外现有的安全机制虽然能在一定程度上保证SIP安全，但同时也增加了SIP消息的长度，会占用大量的无线资源，造成的传输延迟不可容忍[7]。如何寻找方法，在安全性和可用性之间找到一个均衡，也是SIP亟待解决的一个问题。

参考文献

[1]张登银，孙精科，等.VoIP技术分析与系统设计[M].北京：人民邮电出版社，2003，(5)：96-99.

[2]ITU-T Recommendation H.323.Packet based multimedia Communication Systems[S].1998.

[3]思科系统(中国)网络技术有限公司.下一代网络安全[M].北京：北京邮电大学出版社，2006，(12)：219-225.

[4]Samer EL SAWDA，Pascal URIEN.SIP Security Attacks and Solutions-A State-of-the-art review[S].IEEE 2006:3181-3191.

[5]Ferenc Leitold，Anna Medve，Levente Kovács.SIP security problems in NGM services [S].IEEE NGMAST 2007.

[6]Kent S.and R.Atkinson.Security Architecture for the Internet Protolol.RFC2401[S].1999，11.

[7]Dierks，T.and C，Allen，The TLS Protocol Version"[S].RFC 2246，January 1999.

作者简介

白芸洁(1981—)，女，汉族，河南平顶山人，硕士研究生，郑州交通职业学院教师；

李娜(1980—)，女，汉族，河南开封人，本科，郑州交通职业学院教师。