VoIP安全问题及对策研究

魏建行　李超　张彬
河北大学网络中心　河北　071002

摘要：作为一种基于IP网络的新兴应用技术，VoIP继承了IP数据网络的若干安全漏洞。通过分析VoIP原理及协议体系，讨论了VoIP系统的安全隐患，并提出相应的防范对策。

关键词：VoIP；语音；安全；SIP协议

0 引言

随着VoIP技术的普及，其安全问题引起了越来越广泛的关注。由于VoIP依赖于IP网络这一高度开放的技术平台，在易于推广普及的同时，也相应存在一定的安全漏洞。因此，分析VoIP技术存在的安全隐患，并探讨相应的安全策略，有利于提高VoIP应用的安全性。

1 VoIP技术及协议标准

1.1 VoIP原理及工作过程

VoIP(Voice over IP，IP电话或网络电话)是一种通过Internet提供话音服务的应用技术。它以IP分组交换网络为传输平台，对模拟的语音信号进行压缩编码、打包分组、分配路由、存储交换、解包解压等处理，从而实现互联网上的语音通信。

典型的VoIP模型基本结构如图1所示。VoIP设备把语音信号转换为IP数据流(数字信号)，并把这些数据流经由IP网络转发到目的地，接收端设备又把它们转换成语音(模拟信号)。VoIP的传输过程分为下列几个阶段：

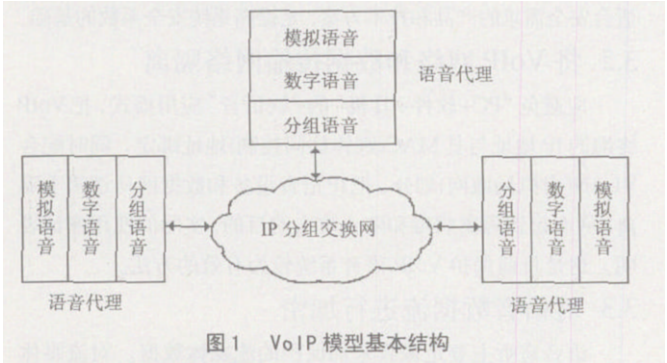

图1　VoIP模型基本结构

(1) 语音-数据转换

语音信号是模拟信号，要通过IP方式来传输，应首先采用特定的编码标准对语音信号进行模数转换。经过转换的数据称为原数据。

(2) 原数据-IP转换

对原数据以特定的帧长进行压缩编码，以便于通过IP网络进行传输。编码后，将4个压缩的帧合成一个压缩的IP数据包送入网络处理器。网络处理器为数据包添加包头、时标等附加信息后通过网络传送到目的地。

(3) 传送

在传送过程中，网络的中间节点检查每个IP数据附带的寻址信息，并使用这个信息把该数据报转发到目的地路径上的下一站直到最终目的地址。

(4) IP包-原数据的转换

目的地VoIP设备接收这个IP数据后，去掉包头、时标等控制信息，保留原始的原数据，并提供给解码器。

(5) 数字语音-模拟语音转换

解码器将得到的原数据还原为模拟信号(语音样点信息)，然后由VoIP设备的播放驱动器取出送入声卡，通过扬声器按预定的频率播出。

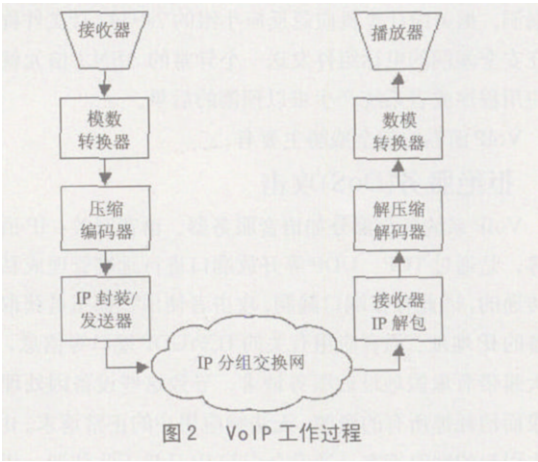

图2　VoIP工作过程

作者简介：魏建行(1970-)，男，河北大学网络中心实验师，主要研究方向：网络信息安全。李超(1979-)，男，河北大学网络中心助理实验师，主要研究方向：网络安全。张彬(1980-)，男，河北大学网络中心助理实验师，主要研究方向：数据安全。

语音信号在IP网络上的传送要经过从模拟信号到数字信号的转换、数字语音封装成IP分组、IP分组通过网络传送、IP分组的解包和数字语音还原到模拟信号等过程。过程示意见图2。

1.2 VoIP使用的主要协议标准

目前较有影响的VoIP协议包括ITU-T提出的H.323协议和IETE提出的SIP协议。

H.323协议是由ITU的第15研究组SG-15提出的多媒体通信协议系列H.32x中的一个，提供了基于IP网络(包括Internet)的传送声音、视频和数据的基本标准，包括在无QoS保证的分组网络中进行多媒体通信所需的技术要求。许多计算机、网络通信公司，如Intel、Microsoft和Netscape都支持H.323标准。

SIP是IETF标准进程的一部分，是在诸如SMTP(简单邮件传送协议)和HTTP(超文本传送协议)基础之上建立起来的协议体系。用来建立、改变和终止基于IP网络的用户间的呼叫。为了提供电话业务，有时还需要结合其他标准和协议，如RTP(实时传送协议)，RSVP(资源预留协议)，LDAP(轻型目录存取协议)，RADIUS(远程身份验证拨号用户服务)等。

SIP协议凭借其简单、易于扩展、便于实现等优点得到业界青睐，正逐步成为NGN(下一代网络)和3G多媒体子系统域中的重要协议，市场上已经出现越来越多的支持SIP的客户端软件和智能多媒体终端，以及用SIP协议实现的服务器和软交换设备。

2 VoIP安全隐患分析

H.323和SIP总体上都是开放的协议体系。在语音通话的实现过程方面，各设备厂家都有独立的组件来承载，并且采用Windows、Linux等操作系统，这些开放的系统本身就容易受到病毒和恶意攻击的影响。同时，作为一种新兴传输协议，SIP尚不完善，它采用类似于FTP、电子邮件或者HTTP服务的形式来发起用户之间的连接，由于不是面向安全连接的协议，容易被黑客用来对VoIP进行攻击。2004年，英国国家基础设施安全协调中心报告称，在许多H.323设施中存在ASN.1协议安全漏洞。据美国计算机应急反应小组的749342号文件称，向存在安全漏洞的电话组件发送一个异常的ASN.1信元就可能使应用程序或者系统产生难以预测的后果。

VoIP面临的安全威胁主要有。

2.1 拒绝服务(DoS)攻击

VoIP系统各个部分如语音服务器、语音网关、IP语音终端等，是通过TCP、UDP等开放端口进行远端管理或私有信息传递的，因此存在端口漏洞，攻击者使用扫描工具获取这些设备的IP地址、语音应用有关的TCP/UDP端口等信息，并发送大量带有虚假地址的服务请求，导致这些设备因处理此类请求而消耗掉所有的资源，无法响应用户的正常请求。由DoS攻击引起的网络拥塞，通常会引起IP话机无法注册、语音网关工作不正常、通话质量严重下降等问题。

2.2 身份和服务窃取

利用SIP协议的安全漏洞，黑客可以攻破IP语音网关，不经过认证随意拨打IP电话，造成运营者的经济损失；或者攻击语音服务器窃取用户身份和密码信息，从而盗用合法用户的身份拨打IP电话，造成用户的话费损失。

2.3 语音窃听

用于VoIP在IP网络上传输等时话音信息的RTP和RTCP也是开放的协议，未加密的语音数据流量在传输时极易被截取或侦听。黑客可以使用伪装欺骗手段突破SIP和IP地址的限制而窃取到整个谈话过程，用户承受着因语音信息泄密而遭受损失的风险。

2.4 对数据网络的安全威胁

与其他数据网络设备一样，以TCP/IP协议栈为基础的IP语音设备面临无孔不入的病毒威胁。随着VoIP的逐步普及，各种IP语音终端和服务器也会成为病毒、蠕虫和木马程序的攻击目标。病毒不仅会严重降低VoIP业务的性能，甚至会传播到数据网络的服务器，使数据网络遭到破坏。

3 VoIP安全对策

VoIP所面临的安全威胁是由其协议和标准的开放特性决定的，也是对原有IP数据网络部分安全漏洞的继承。可以通过采取合理的管理机制和安全配置，减少系统漏洞，最大限度保障VoIP系统的安全。

3.1 选择安全成熟的产品和解决方案

VoIP标准并不统一，尽管有关国际技术组织正在进行VoIP产品的标准化和统一化工作，但各厂家产品的技术特色、产品体系构架和操作平台仍不尽相同。出于自身产品安全性的考虑，不同厂家都有相应的技术保障各自产品免受病毒侵害。如很多厂家采用了将管理网段和IP话音网段隔离的机制，减少端口暴露，以降低安全风险。此外，VoIP安全和数据网络安全是紧密相关的，厂家不仅应提供安全的设备，更要帮助用户设计基于现有数据网络的VoIP安全解决方案。因此，选择适合安全需求的产品和技术方案，是提高系统安全系数的基础。

3.2 将VoIP网络和数据传输网络隔离

应避免“PC+软件+耳机”的“软语音”应用模式，把VoIP终端的IP地址与其MAC(媒体访问控制)地址绑定，同时配合VLAN(虚拟局域网)划分，把IP语音设备和数据网从逻辑上隔离，从而起到隔离病毒和防止攻击的目的。实际的使用测试表明，这是目前保护VoIP语音系统较为有效的方法。

3.3 对语音数据流进行加密

语音窃听主要是截获未加保护的流媒体数据。对流媒体的加密可以有效防止窃听。H.323协议簇中的H.235协议可以提供身份认证、数据加密和完整性功能。目前已经有一些厂家采用私有的加密协议进行音频流的保护，尽管标准还不统一，但仍然在很大程度上提高了IP语音通信的安全。随着IP语音

[下转73页]

理上加强安全措施。希望本文能对计算机用户在计算机网络的安全防范方面有所帮助，并通过我们的共同努力，使计算机网络实现以下安全目标 ：保护网络系统的可用性 ；保护网络系统服务的连续性 ；防范网络资源的非法访问及非授权访问；防范入侵者的恶意攻击与破坏 ；保护学校信息通过网上传输过程中的保密性、完整性；防范病毒的侵害 ；实现网络的安全管理。

参考文献

[1]李圣良.基于校园网的网络安全策略.网络安全技术与应用.2005.
[2]张双喜.防范金融系统计算机网络风险.科技情报开发与经济.2005.
[3]朱明.计算机网络安全.中国科技信息.2005.

The Precaution and Control Against the Safe Risk of the Campus Network

Li Lu
Network center Ocean University of China,Shandong,266003

Abstract:This paper introduces and analyses the safety threat that the campus network be subjected to,and against the Hacker attack,computer virus,the Trojan,back door etc.Then,discuss the risk that the campus network exist,and put forward to correspond on the measure of precaution and control of the technique and managements,the aim is guiding the network customer safety usage network.

Keywords:The campus network;Network safety;precaution and control

[上接58页]

应用的普及，提供通话双方端对端的加密是一个趋势。

3.4 对VoIP系统进行应用程序级保护

从技术角度看，VoIP设备所处地位相当于数据网络中的应用程序和服务器，容易成为攻击目标。因此 应该把VoIP设备作为应用程序来提供保护，主要措施有：

(1) 保护重要端口和应用。将VoIP设备置于网络防火墙保护体系之内，对信令和媒体流两类对外应用和端口提供保护，以有效避免 DoS 攻击。

(2) 关闭不必要的端口和协议。公开的端口和一些协议的未知漏洞经常会被黑客利用，因此应屏蔽无用端口和非必需的协议，尽可能关闭不需要的服务进程。

3.5 强化安全机制管理

建立健全安全管理机制，是保障系统安全的有效措施。包括两个方面：

(1) 及时查找IP语音服务器和IP终端的软件系统漏洞，关注厂家发布的系统漏洞、补丁、升级等信息，及时采取相应措施，如升级软件版本、安装系统补丁、修补安全漏洞等。

(2) 合理制定单位内部VoIP用户的拨号权限。对不同用户设定相应的拨号权限，如内线、市话、长话等，或者针对不同级别的号码(市话或者长途)设置相应的授权码或拨号密码等，可以在很大程度上防止电话盗打现象。

4 结束语

目前，VoIP应用已经有普及化的趋势，对其安全问题的研究日益受到重视。安全性能已经成为决定VoIP能否进入成熟商业应用的关键因素。作为一种基于IP数据网络的应用技术，VoIP的安全问题实际上是IP数据网络安全问题在具体应用领域的反映。因此，应进一步加强IP数据网络安全研究，并结合IP语音通信应用的特点，不断完善VoIP应用安全体系。

参考文献

[1]朱海毅,周春楠.VoIP基本原理[J].信息技术.2003.
[2]http://www.kb.cert.org/vuls/id/749342.
[3]PhilipHunter.VoIPthelatestsecurityconcern:DOSattackthegreatestthreat[J].NetworkSecurity.2002.

Research on Security Problem and Solutions of VoIP

Wei Jianhang,Li Chao,Zhang Bin
Network Center of Hebei University,Hebei,071002

Abstract:As a new network application,VoIP inherits several inherent shortages of IP network.Based on introduction to principium and protocol of VoIP,the paper discusses the security loopholes of VoIP,and gives some relevant countermeasures.

Keywords:VoIP;voice;security;SIP