VoIP 安全问题及解决措施分析

王凌云，陈　薇
（南京邮电大学通信与信息工程学院，江苏省南京市 210003）

摘　要　VoIP 是将传统电信技术与计算机网络技术融合的新型应用，它基于 IP 技术传送语音，得到了迅速发展，但它还存在一些安全问题。文章从 VoIP 的工作原理出发，分析了 VoIP 可能存在的安全问题，提出了一些解决问题的措施。

关键词　VoIP；安全问题；基本原理；解决措施

1　VoIP 技术及协议标准

1.1　VoIP 的工作原理

传统的电话以电路交换的方式传输语音，而 VoIP 是以分组方式传送的，其实现原理如图 1。

VoIP 通过 Internet 传输语音，它以 IP 分组交换网络为传输平台，先将模拟的语音信号经过 A/D 转换器进行量化，转换成数字语音数据，然后通过语音压缩算法对语音数据进行压缩编码处理，压缩成数据帧，按 IP 相关的协议打包分组、分配路由、存储交换，经 IP 网络传输到目的地，再将分组数据串起来，进行解压解码等处理后还原成语音信号，实现互联网上的语音通信。

1.2　VoIP 使用的主要协议标准

VoIP 的主要协议包括 ITU-T 提出的 H.323 协议和 IETF 提出的 SIP 协议，还有与 H.323 协议和 SIP 协议不在同一层面上的 MGCP 协议以及它的演进协议 H.248 协议。

H.323 协议的提出在 VoIP 出现之前，所以它不针对 VoIP，它是一个协议组，包含一系列的子协议，提供了基于 IP 网络的传送声音、视频和数据的基本标准。SIP 是专门针对 VoIP 设计的协议，是在诸如 SMTP（简单邮件传送协议）和 HTTP（超文本传送协议）基础上建立起来的协议，用来建立、改变和终止基于 IP 网络的用户间的呼叫。SIP 协议简单、易于扩展、便于实现，正成为 NGN（下一代网络）的重要协议。

MGCP 协议只涉及网关分解问题，因而它不仅可以用于基于 H.323 的 VoIP 系统，也可以用于基于 SIP 的 VoIP 系统。MGCP 协议包括 SGCP（简单网关控制协议）和 IPDC（IP 设备控制）协议。H.248 协议作为 MGCP 的演进协议，继承了 MGCP 的众多优点，扩展性、安全性和互通性等方面的技术也日臻完善，所提供的功能不仅限于语音，还增加了文本、视频以及许多与 Internet 服务相结合的新功能。

在中国，VoIP 技术于 1999 年被引用到电信运营中，由于其“价廉物美”的特点而深受广大用户和运营商的青睐。到 2002 年底，IP 电话在国内长途和国际长途业务中的应用已经远远超出了传统电话。随着 Internet 的不断发展、语音编码技术的提高以及成本的进一步降低，VoIP 取代传统电话已成为必然趋势。但 VoIP 在发展过程中遇到的安全性问题是一个不能回避和值得探讨的问题。

2　VoIP 可能出现的安全性问题

2.1　VoIP 自身的问题

H.323 和 SIP 总体上都是开放的协议体系，而 VoIP 各个设备厂家都有独立的语音服务器来提供语音网关或 IP 话机的注册和控制功能，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。尤其是某些设备在需要提供基于 Web 的管理界面时，都可能采用 Microsoft IIS 或 Apache 来提供服务，这些应用在出厂时已经安装在设备中，无法保证这些产品能弥补安全漏洞。也就是说 VoIP 网关的自身安全性存在

江苏省高技术研究计划（No.BG2003001；BG2007045）资助项目

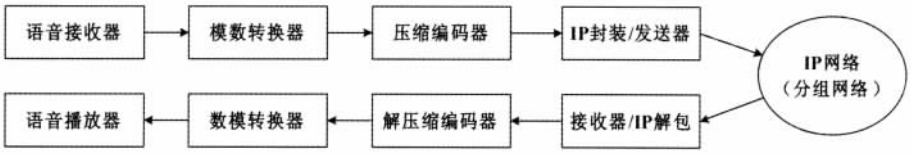

图 1 VoIP 的实现原理

问题，会造成语音服务器存在潜在的安全漏洞。

2.2 DOS 攻击

VoIP 系统各部分（如语音服务器、语音网关、IP 语音终端等）通过 TCP、UDP 等开放端口进行远端管理或私有信息传递，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，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。

2.3 服务窃取

一般在 IP 电话首次登陆到系统时，会要求输入个人的分机号码和密码。很多已经拥有 VoIP 的企业都会在分配给员工一个桌面电话的同时再分配一个 IP 电话，即授予密码和拨号权限。一旦密码被窃取，或被黑客利用 SIP 协议的安全漏洞攻破 IP 语音网关，或攻击语音服务器而获得其登录口令，都会给用户带来一定程度的损失。

2.4 媒体流的窃听

信令和媒体流是建立一个典型 VoIP 呼叫必不可少的，RTP/RTCP 是基于包的网络上传输等时话音信息的协议，这些协议都是开放的，通过网络监听的方式，截取任何一段连续时间的 RTP 报文，就可以恢复出相应的语音，让双方的通话内容暴露无遗，从而对用户的隐私安全构成威胁。

2.5 伪造攻击

SIP 中伪造攻击非常类似于 SMTP。攻击者改变消息的头域和消息体，接收者则认为是非发起者发出的请求。请求伪造就是模仿消息发出者的身份欺骗合法的接收者。

2.6 对数据网络的安全威胁

以 IP 数据网为支撑的 VoIP 技术与互联网同样面临着来自数据网络病毒、木马、恶意程序和代码的威胁。此外，VoIP 账号在数据网络上的安全问题也是一个安全隐患。

2.7 紧急呼叫问题

VoIP 不像 PSTN 那样在用户拨打火警等报警电话时能反应及时，而且 VoIP 也无法准确给出来电的确切物理位置，在这一领域的应用有待进一步研究和发展。

3 VoIP 安全性问题的解决措施

3.1 隔离用于话音和数据传输的网络

这里的隔离不是物理隔离，而是将所有的 IP 话机放到一个独立的 VLAN 当中，不允许无关的终端进入此网段。很多调查都证实了划分 VLAN 是目前最为简单有效的方法，可以隔离病毒和简单的攻击。同时，配合数据网络的 QoS 设定，还有助于提高话音质量。

3.2 对 VoIP 软件运行平台进行管理

对 VoIP 呼叫管理控制软件的运行平台（如 Windows 或 Linux 操作系统或路由器上不同软件平台），应该确保操作系统日常运行的安全性，并且已经安装了最新的安全补丁。

3.3 语音数据的加密

语音窃听主要是截获未加保护的流媒体数据，对语音数据进行加密可以有效防止窃听。H.323 中 H.235 是负责身份认证、数据完整性和媒体流加密的。因此，H.323 协议的 VoIP 终端设备可以提供对音频流的加密保护。

3.4 安全框架

IP 电话终端或其他设备可通过防火墙得到保护。防火墙运行管理员通过对一个点的管理和控制，防止黑客和侵入者等未经授权用户接入 IP。防火墙增强了安全管理，通过防火墙可以保障 IP 的安全。

由于 IP 电话业务是语音与数据基础设施的融合应用，因此，在安全框架内实施 IP 电话安全战略至关重要，而能否提供一个安全 IP 电话实现方案将是决定 IP 电话能否顺利发展的关键环节，只有很好地解决了 IP 电话的安全问题，基于 IP 电话的应用才能稳定发展，并成为解决低话费、高效率、可移动语音通信需求的有效方法。随着 IP 电话所遵循的 SIP 协议不断完善，相关的鉴别、授权、认证及密钥技术将会逐渐引入 IP 电话技术体系，安全通信将会成为 IP 系统的一种增值特性。

3.5 加强安全管理

作为个人用户，就如定期升级自己的杀毒软件

一样，要定期查找 IP 服务器和 IP 终端的漏洞，及时进行修补。而作为企业用户，要合理制订单位内部 VoIP 用户的使用权限。

3.6 利用协议优势提供安全保护

H.323 和 SIP 协议针对 VoIP 的应用也提供了一些相应的安全保护措施。H.323 协议在呼叫通过用户身份验证之后才能进行下一步的操作，这种保护机制无疑加强了对合法用户的监视和管理。此外，它还通过数据包的加密和校验，进一步加强了对数据完整性的保证。H.323 还允许扩展密钥算法和机制来保证密钥传输和验证的安全性和可靠性。SIP 也同样提供了用户鉴别和授权来保证用户的合法性。SIP 网络还引入了 IPSec 来加强安全管理。它还可以在目的地接收数据包时验证数据包的完整性，可以使用 NAT 技术来保障网络安全。

4 结束语

随着 VoIP 使用越来越广泛，对其安全问题的关注将越来越多，必将成为研究人员和工程技术人员研究的热点。本文对 VoIP 的安全性问题进行了分析，提出了一些解决措施，能为相关技术的研究提供参考。随着电信技术和互联网技术的不断发展，VoIP 的安全性问题近期有望得到圆满解决。

参考文献

1 Stefano Salsano，Luca Veltri，Donald Papalilo. SIP Security Issues：The SIP Authentication Procedure and its Processing Load. December 2002.

2 Franklin D Ohrtman，JR 著. 软交换技术[M]. 李晓刚，许刚，译. 北京：电子工业出版社，2003.

3 Daniel Collins 著. VoIP 技术与应用（Carrier Grade Voice over IP)[M]. 舒华英，李　勇，译. 北京：人民邮电出版社，2003.

4 刘伟明，等. VoIP 安全——基于 SIP 协议的深入剖析和解决策略[J]. 计算机应用，2006(6)：167~170.

5 郑　勇，等. 基于软交换的 VoIP 技术在 CRM 呼叫中心中的应用与研究[J]. 邮电设计技术，2008(8)：70~73.

王凌云（1987—），男，主要研究方向为网络通信与网络安全。

收稿日期：2008-11-29

（上接第 43 页）

OTGMonitor：OTG 信息寄存器，格式见表 2。

表 2　OTGMonitor 描述

寄存器名	R/W	位	描述
OTGMonitor	R/W	7	0：ID 信号线为低电平；1：ID 信号线为高电平
		5～6	00b：SE0；01b：J；10b：K；11b：SE1
		4	0：VBUS_SESS_END 无效；1：有效
		3	0：VB_SESS_END 无效；1：有效
		2	0：VB_SESS_VLD 无效；1：有效
		1	0：VA_SESS_VLD 无效；1：有效
		0	0：VA_VBUS_VLD 有效；1：无效

4）实现方法

该模块用状态机实现 OTG 的状态转换，从而实现设备的连接、枚举、SRP 和 HNP 协议，由于该模块涉及到各个状态持续时间的定时，为了让定时更加的灵活和连接的稳定，该模块通过中断向上层的报告，启动上层软件定时。状态切换的状态通过写寄存器 OTGStateCmd 实现。

3 结束语

本文通过对 USB OTG 协议的分析，设计了 USB OTG 的硬件、软件实现方案。当然对于不同芯片的选择、硬件实现的任务有所不同。如果选用功能强大的芯片，那么上层固件会承担较少的任务，反之会承担更多的任务。文中的 OTG 设计方案的验证主要通过 SystemC 进行功能验证。

参考文献

1 王成儒，李英伟. USB2.0 原理与工程开发.北京：国防工业出版社，2004.

2 萧世文. USB2.0 硬件设计.北京：清华大学出版社，2002.

3 肖踞雄，翁铁成，宋中庆. USB 技术及应用设计[M].北京：清华大学出版社，2003.

4 周立功，等. USB 2.0 与 OTG 规范及开发指南[M].北京：北京航空航天大学出版社，2004.

王华强（1982—），男，硕士研究生，主要研究方向为第三代移动通信。

收稿日期：2008-11-13