

安全性问题是否会制约VOIP发展？PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/205/2021_2022__E5_AE_89_E5_85_A8_E6_80_A7_E9_c101_205496.htm

起源于IP的开放性，在获得廉价资费的同时，VOIP网络的安全性一直是其与身俱来的弱点，尽管业界对于其安全性已经有了相当长时间的研究，但是大多成果都仅仅局限在理论和学术性研究，直到在去年中期才有服务提供商开始对其进行实质性的关注，触发动机来源于两个网络诈骗犯盗取了运营商上百万美元的资金。VOIP网络的漏洞很容易被不法的骇客所利用，例如，曾经有骇客非法地利用系统漏洞在Internet和PSTN网络之间免费路由了上千万分钟的呼叫，并且作为非法业务向用户低价出售。这样的技术只需用到一个改进的IP-PBX去伪装企业PBX就可以实现。对于VOIP网络的安全性，部分专家认为并不需要被过分的夸大。例如，著名VOIP公司Vonage的创始人Jeff Pulver就认为，对于VOIP的安全性业界过于强调，其实盗取IP呼叫的行为和偷取商店物品没有本质的区别，这样的事情应该被当作犯罪来看待，而不应该因为其是和IP网络有关而被过分在技术层面被强调。相反，还有大部分专家则认为VOIP网络自身有很多安全性的劣势，如果不被有效地解决，那么在未来商用过程中将会导致系列很严重的问题。例如Core Competence网络和安全公司的总裁David Piscitello就坚持VOIP的安全性应该被重点关注，他强调说，越来越多的VOIP产品的弱点被报告出来，相应业界对于VOIP网络协议（如SIP、RTP等）的安全性漏洞也有了越来越多质疑，这样的网络给人们的感觉是容易被穿透的，因此Piscitello表示，

对于VOIP网络安全性的重点关注是具有很强的商业动机的。此外，媒体广告和安全性总是息息相关的，最典型的例子是让用户听之惶恐手机和移动IM病毒，其大多起源于垃圾广告。同样地，对于VOIP网络，媒体广告也会带来同样的问题，网络电话安全联盟(VOIPSA)的主席David Endler表示，肆意的媒体广告将会是VOIP病毒的一个主要来源，此外，对于VOIP网络和业务，IP数据网络固有的安全隐患例如DOS、蠕虫、病毒等也是值得关注的。因此，VOIP网络在商用的过程中，安全性问题成为了各大服务提供商所共同面临的严重问题。正如很多专家所坚持的，VOIP安全性在技术方面需要很多提升，否则，在未来的全IP业务体系下，这样的安全隐患会被扩展，甚至波及诸如移动通信网络等。例如，先前所提及的垃圾邮件、垃圾广告等入侵行为，则有可能在WLAN热点区域，借助免费VOIP应用入侵移动终端。

Juniper Network亚太地区的解决方案和市场部门负责人Andrew Ma表示，另一个很严重的问题是，在很多情况下用户都无法发现他们正在被攻击，这样对于防御措施要求则更加的苛刻。例如，有种名为VOMIT(Voice over misconfigured Internet telephones)在Unix下运行的工具，能够捕获VOIP数据包，并且能够在计算机上将其还原成音频文件。这样，在公众热点承载的VOIP业务就及其容易受到窃听，因为骇客可以窃取到相关的数据包，并且用VOMIT工具还原声音文件。Andrew表示，应对这样的攻击的方法是对VOIP业务进行端到端加密，从而保证数据包不能被非法还原。VOIP另一个日益增长的安全性问题来源于对SIP协议日益广泛的使用。SIP协议是类似于HTTP的基于文本的协议，用于管理基

于IP网络的会话事务。这种基于文本的协议使得骇客们更加容易窃取，从而控制网络的信令过程。同时，VOIP网络通常都是复用信道，这样更加地容易被窃取。因此，需要防火墙和IDP等组建能够对于VOIP协议有更多的特定效力，从而有效地保护这个服务。除了在教育层的新增隐患（因为VOIP可以看作假设在IP之上的应用，先前所提及安全性问题都可以视作应用层隐患），传统IP层的安全性隐患可能由于VOIP业务自身的特点而加大其严重性。Endler就指出，VOIP业务本身对于IP层的安全性提出了新的挑战，在IP网络上面假设话音服务会使得从前就有的许多IP的问题被暴露得更为明显。例如，传统情况下，一个企业在遭受DOS攻击得时候，可能使得整个公司上网速度减慢，但是并不会彻底影响他们邮件的发送。然而，当他们的IP网络承载话音业务的时候，DOS攻击将可能直接使得一次通话中断（因为话音业务能容忍的时延有限）。因此，在现有IP网络上假设VOIP服务，就意味着对于现有的IP提出了新的挑战。支持VOIP能够加剧IP网络不安全隐患观点的还有阿尔卡特-朗讯亚太地区安全业务主管Keith White，他认为，安全性问题是阻碍VOIP发展的主要问题之一，许多公司和组织都因为这样的顾虑而对其保守地观望，如果解决了这个问题，VOIP市场将会得到一个质的飞跃。这也是他们所希望改善的，然而，VOIP安全性最大的挑战是如何让企业和服务提供商明确分组IP网络固有的特点和传统电路交换网络有所区别，而IP网络由于其尽力而为的设计哲学导致自身就有许多安全性缺陷。White表示，他相信VOIP服务提供商应该也能够提供可信的VOIP服务。谈及安全性问题的时候，他将VOIP服务提供商分为两类，一类是

利用现有Internet基础设施提供VOIP服务的虚拟运营商，例如Skype、Net2Phone、Vonage等，并且将其称为"寄生运营商"。而另一类则是基于自己的基础设施提供VOIP服务的提供商。他表示，这两类服务提供商有着明显的区别，前者是互联网的用户自发架设的端到端应用，具有很低的服务质量保证，而后者是专业网络集成商和运营商所假设的服务，具有可靠的服务质量保证。对于安全性问题，"寄生运营商"显然比起拥有基础设施管控权力的运营商更加的被动，他们只能在终端部署安全性策略而无法涉及到网络内部。 100Test 下载频道开通，各类考试题目直接下载。详细请访问

www.100test.com