层层保护VoIP安全 防止隔墙之耳入侵思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_B1_82_E5_B1_82_E4_BF_9D_E6_c101_644247.htm 即使在VoIP技术广泛应用的今天，VoIP的安全性仍屡遭质疑。英国安全专家、防火墙公司Borderware创办人之一Peter Cox就在近日公开宣称，基于网络的VoIP电话极不安全，容易给黑客造成可乘之机。为了证实这个观点，他研发了可以窃听VoIP网络电话的“概念证实”（ProofofConcept）型软件SIPtap。该软件利用一个安装在公司网络上的特洛伊木马软件，成功对VoIP网络进行监听，并可以生成后缀为“.wav”的文件供黑客随后在互联网上传播使用。 VoIP成为无论专家还是黑客攻击的靶子并非偶然。作为一种在网络上应用的IP技术，与Web和电子邮件等IP应用一样，VoIP技术存在特有的威胁和风险。这些威胁和漏洞包括所有IP网络层面的威胁、VoIP协议和应用的威胁以及与内容有关的威胁等。就如同裸露的皮肤最容易受伤，解决办法就是给你的VoIP多穿几层铠甲采取多层次安全机制，在潜在入侵者的攻击路线上尽可能多地设置各种障碍。 建立一个安全的VoIP网络，首先要将其从数据网络中独立出来。要将虚拟局域网（VLAN）上的VoIP话机设为非路由的地址，然后禁止连接互联网的电脑与VoIP之间有任何交流，还要使用存取控制列表（Access Control Lists）来阻止VLAN之间的通讯。 而且，需要一个特别设计的防火墙，能识别和分析VoIP协议，对VoIP的数据包进行深度检查，并能分析VoIP的有效载荷，以便发现任何与攻击有关的行为。 还要在几个层次上设置障碍，包括保护好VoIP网关，锁闭网络物理层，

用IPSec加密，用TLS锁定会话层和用SRTP来对应用层的介质进行加密。 网关是数据进出VoIP网络的关键点，它会同时连接不同的网络，如IP网络和公共电话交换网（PSTN）。在网关上使用授权机制和存取控制，以便控制可通过VoIP系统拨打和接听的电话，以及设定可以执行管理任务的不同人员权限等。 对一个语音网络而言，限制对介质访问以及对VoIP服务器和端点访问非常重要。 要达到限制对介质访问或对VoIP服务器和端点访问的目的，首先对所有呼叫服务器以及与服务器有关的接触进行控制；然后限制对终端的接触，并将线缆埋设在墙体中的管道里以保证它们自身的安全；最后还要谨慎选择无线AP的位置，限制无线交流，限制信号强度，使用屏蔽材料将无线信号尽量阻挡在建筑物之内。来源：考试大 用IPSec加密来保护网络中的VoIP数据，能保证即使攻击者穿越物理层防护措施截获了VoIP数据包，也无法破译其中的内容。 TLS使用的是数字签名和公共密钥加密，这意味着每一个端点都必须有一个可信任的、由权威CA认证的签名。也可以通过一个内部CA（如一台运行了认证服务的Windows服务器）来进行企业内部的通话，并经由一个公共CA来进行公司之外的通话。 用SRTP来对应用层的介质进行加密，可以提供信息认证、机密性、回放保护等安全机制。 VoIP安全保护偏方 无论VoIP网络防范多么严密，攻击不可避免会发生。因此，有必要通过部署合适的监视工具和入侵检测系统，发现试图攻入VoIP网络的各种尝试。通过仔细观察这些工具所记录下来的日志，有助于及时发现各种数据流量的异常状况，从而发现是否有人通过暴力账号的方式进入网络。 与此同时，及时维护操作系统和VoIP应用系统的补丁，对于防范来自

恶意软件或病毒的威胁是非常重要的。 还有一个点子可能会有帮助，那就是制定一个计划，把你自己假想成一个黑客高手，然后尝试用各种办法来攻击你的VoIP系统。没有找到攻击入口，并不代表你的VoIP系统是安全的。但是如果你能找到入口，那么别人也可以，那就赶快堵住这个漏洞吧！ 编辑特别推荐: 关于思科认证考试的注意事项 Cisco认证总结CCNA重难点 各个方向CCIE认证投资回报分析 CISCO认证和华为3COM认证的区别 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