Broadview
www.broadview.com.cn

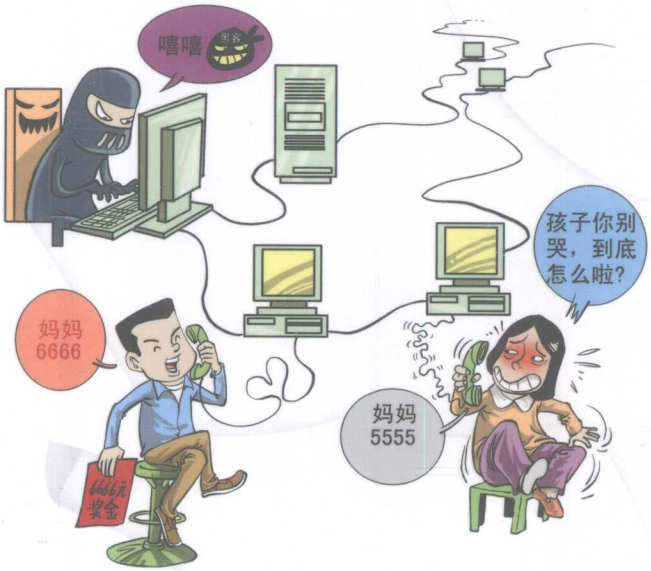
“十一五”国家重点图书出版规划项目

安全技术大系

Hacking Exposed™ VoIP: Voice over IP Security Secrets and Solutions

黑客大曝光：VoIP安全机密与解决方案

【美】David Endler，Mark Collier 著
李祥军 周智 魏冰 译



揭秘VoIP电话应用安全，提供解决方案

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

“十一五”国家重点图书出版规划项目

Hacking Exposed™ VoIP: Voice over IP Security Secrets and Solutions

黑客大曝光：VoIP安全机密与解决方案

【美】David Endler，Mark Collier 著
李祥军 周智 魏冰 译

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

冒用他人的电话号码打电话、窃听他人的通话内容、在他人通话时加入一些背景噪声、在他人通话时恶意强行挂断……所有这些都是很多“黑客”的梦想，然而，在以前的通信网络中，基于一些技术原因，这些都难以实现。随着 VoIP 技术的应用和普及，黑客们终于等到了机会，在 VoIP 时代，特别是端到端的 VoIP 应用时代，在一些安全防护不严的网络中，黑客们的这些梦想就可以成真了。

本书立足于企业 VoIP 通信网络，以大量丰富的实例和各种 VoIP 攻击工具的应用为基础，详细描述了各种针对 VoIP 应用的攻击方式及解决对策，包括号码采集、呼叫模式跟踪与语音窃听、针对服务器和电话的 DoS 攻击、恶意语音的插入与混淆、垃圾语音电话、语音钓鱼，等等。针对企业 VoIP 网络安全攻击与防护，本书绝对是一本安全管理员、安全研究人员等必读的实战型的教材。同时，本书也是了解运营商通信网络（如 IMS 网络）及安全问题的不可多得的入门级教材。

图书在版编目（CIP）数据

黑客大曝光：VoIP 安全机密与解决方案 /（美）恩德勒（Endler,D.），（美）科利尔（Collier,M.）著；李祥军，周智，魏冰译. —北京：电子工业出版社，2010.10
（安全技术大系）
ISBN 978-7-121-11750-3

Ⅰ. ①黑… Ⅱ. ①恩… ②科… ③李… ④周… ⑤魏… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 172984 号

策划编辑：毕 宁 bn@phei.com.cn
责任编辑：贾 莉
印 刷：北京东光印刷厂
装 订：三河市皇庄路通装订厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：29.75 字数：590 千字
印 次：2010 年 10 月第 1 次印刷
定 价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

译者序

出于工作的需要，我经常需要和国内外的各安全厂商进行技术交流，在此过程中我发现，很多安全厂商在IT系统安全、IP网络系统安全，包括操作系统安全、数据库安全、网络设备安全等方面都有着深厚的技术积累，然而在通信网络安全方面，往往了解得较少。许多安全厂家在进行通信网络或者通信业务系统的安全评估、安全加固等工作时，通常不会涉及到通信业务中的安全需求。随着国内安全厂商的不断发展、国内安全从业人员的不断努力，在IT及IP网络系统安全方面，国内外的差距越来越小，然而在通信网络安全方面，国内外的差距还是很明显。许多文献都提到，最早的黑客并不是在计算机领域产生的，如70年代美国的电话飞客（Phreaker），就通常被认为是黑客最早的雏形。通过Blue Box向全世界打电话，是那个时代黑客最酷的行为。直到今天，美国一直都有许多热衷于通信网络安全的研究人员，而在国内，却鲜有精于通信网络安全的专业人员。

VoIP技术已经广泛应用到当前的各种通信网络之中，VoIP技术的应用使得通信网络更加开放，但也同时面临着更大的风险，因此，通信网络安全解决方案将面临更大的挑战。随着VoIP技术应用的进一步普及，很多研究机构都预测VoIP将会成为黑客的下一个乐园。实际上，前几年，美国就曾经发生过利用VoIP网络漏洞窃取价值超过100万美元通话时长的案件，并且美国的几大著名运营商也都曾曝出存在VoIP计费方面的严重安全漏洞。

我曾经阅读过国内外的许多关于VoIP安全的文章和书籍，发现国内的相关文献更多是关注于理论层面，很少有真正讨论安全实战的文献，相比较而言，国外关于VoIP安全实战的书籍更多一些。在安全领域，与那些随手可得的关于IT及IP网络系统安全的书籍和文献相比较，关于通信网络安全或者是说与VoIP安全相关的书籍实在是少得多。本书的原版书在2007年刚出版后不久，我就有幸拜读，获益匪浅。当时，我就认为本书的原版书是市面上介绍VoIP安全最好的书籍之一。时至今日，虽然市面上又出现了大量关于VoIP安全的书籍，但我仍然认为本书是最好的VoIP安全书籍之一。这几年中，我曾经向很多安全界的朋友、很多安全厂商推荐过这本书，为了让国内安全行业的从业人员能够更好地了解VoIP安全，我们特意翻译了此书，并将之献给安全界的朋友。

本书是一本绝佳的关于 VoIP 安全的入门级书籍，作者利用丰富的实例深入浅出地介绍了 VoIP 安全方面涵盖的关键内容。仅从安全的角度来看，VoIP 技术是一把双刃剑，应用得当，可以带来很多安全优势，应用不得当，就有可能带来安全灾难。本书介绍的内容以及攻击场景都基于企业 VoIP 网络应用，而 VoIP 技术在运营商的通信网络应用中的安全性与可靠性方面，与企业应用相比，有着明显的区别：通信网络中的 VoIP 安全水平比企业网络 VoIP 应用的安全水平高出很多。即便如此，本书也是一本上好的了解运营商通信网络安全的入门级书籍。本书在介绍 VoIP 安全时，部分重点内容描述了 SIP 协议的主要安全问题，SIP 协议是现在很多通信网络系统（如 IMS、固网软交换等）或者即时通信系统（如 MSN、飞信等）的基础协议，同时，SIP 协议将越来越多地应用到更多系统之中。因此，本书也有助于读者更好了解 SIP 协议安全以及许多相关系统的安全。

本书的作者是国际上公认的安全专家，是 VoIP 安全方面的权威人物，他们在业界内发起并成立了著名的 VoIP 安全联盟。本书作者不仅仅深入分析了 VoIP 安全问题，还亲自开发了许多安全攻击工具，以便让读者可以更好地理解这些问题。能够分析问题、发现问题并能动手开发工具来验证这些问题，作者的这种务实的精神实在是值得我们学习。

我曾经安装并应用过本书中提到的各种开源的 VoIP 系统，也曾经分析应用过书中的很多安全工具。本书提到的几个开源的 VoIP 系统是国际上很多钟情于 VoIP 安全研究的安全从业人员必备的系统，这些系统可以提供很多扩展，基于此，研究人员能开发出很多应用，同时，还有许多公司专门为这些系统开发与 PSTN 兼容的电路板。这样一来，这些开源的 VoIP 系统在当前就可以应用于家庭及小型企业办公中，是非常好的学习 VoIP、SIP 及通信网络，并进行通信系统 DIY 的参考资料。本书由三位具备多年通信网络安全从业经验的中国移动安全专家李祥军、周智、魏冰翻译，限于水平，译文中的错误和疏漏在所难免，敬请广大读者朋友批评指正。

最后，感谢电子工业出版社博文视点资讯有限公司为本书的出版付出的努力，尤其要感谢毕宁、刘皎以及本书的责任编辑贾莉，感谢他们对通信网络安全及 VoIP 安全领域的关注，他们辛勤细致的工作使本书增色不少。

李祥军

2010 年 2 月

本书赞誉

秘密都被泄露出去了！本书描述的就是安全的禅宗，同样也是攻击 VoIP 系统以及确保其安全的艺术。David 和 Mark 在著书的过程中一直怀着极大的热情，深入分析了如何保障互联网电话的安全。书中描述了大量具体的实例，应用了很多开源工具，其中有许多开源工具是由本书作者开发的。本书是当代通信工程与管理从业人员的必读之书。对于任何好学之人，本书都称得上是一本绝妙的好书，同时，本书也是我近几年推荐的书籍的首选。

——Jonathan Zar

Pingalo 常务理事，VoIP 安全联盟秘书、Outreach 组主席

本书带你进入一段如何发起 VoIP 安全攻击的旅程，从制定计划到发起攻击，所有这一切都是从一个黑客的视角出发。本书洞悉 VoIP 安全问题，让读者可以从黑客的思维角度来测试其网络的安全性。在进行 VoIP 网络体系结构设计及部署之前，这绝对是一本必读之书。

——Brian Tolly

思博伦通信全球服务部客户服务经理

本书作者在解释企业应用 VoIP 系统时可能面临的安全风险方面，做出了极为卓越的工作。同样重要的是，书中还针对这些安全风险提出了可以实施的对策，使得企业将来可以安全地部署和实施 VoIP 系统。

——Gustavo de los Reyes

AT&T 技术顾问

当前，你所应用的 VoIP 系统的语音通信和电话会议并不像你认为的那样安全。本书展开介绍了远程恶意人员如何探测、监听并篡改那些提供 VoIP 服务的电话、语音交换机及网络设备。更重要的是，本书提供了降低或者消除部署 VoIP 系统面临的安全风险的解决方案。

——Ron Gula

Tenable 网络技术总监，Nessus 漏洞扫描器创始人

这确实是一本很危险的书！David 和 Mark 不仅完完全全地描述了那些众所周知的以及那些很难但非常致命的 VoIP 安全攻击，还进一步为读者提供了一些易用的工具，以便读者可以实验这些攻击。如果你是一名安全专业人士，负责保护包括 VoIP 系统在内的基础网络，那么你就一定要阅读本书，否则，你的 VoIP 系统及其他网络系统就将处于危险的境地！

——Dan York

Blue Box：VoIP 安全播客的创始人和主办人

致　谢

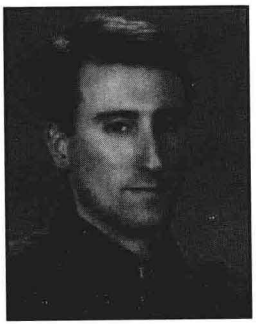
首先，要感谢我们的家人，感谢他们在我们写作和研究过程中始终如一的无私支持。其次，要特别向 TippingPoint 和 SecureLogix 公司中我们各自的同事致谢，感谢他们在整个写作过程中提供的素材、建议以及指导。还要特别感谢 SecureLogix 公司的 Mark O'Brien 的研究工作以及在攻击工具开发方面给予的帮助。同样，也要感谢不断壮大的 VoIP 安全业界进行的那些极为精彩的讨论，这些讨论出现在 VoIP 安全联盟的 VoIPSEC 邮件列表（http://www.voipsa.org/VOIPSEC/）以及 Dan York 和 Jonathan Zar 的 Blue Box 播客系统之中（http://www.blueboxpodcast.com）。

同样要感谢的还有 Skype、Avaya、Cisco 以及 Asterisk 的安全与 VoIP 小组，感谢他们在本书关于具体厂家产品安全相关章节中的工作和支持。

最后，我们要真诚地感谢 McGraw-Hill 出版社的 Jane Brownlow、Jenni Housh、LeeAnn Pickrell、Peter Hancik 以及 Lyssa Wald，正是由于他们的工作才使本书得以出版。

关于作者

David Endler



David Endler 是 3Com（3Com 在 2010 年已经被 HP 公司收购）旗下子公司 TippingPoint 安全研究部门的主管，他负责产品安全测试、VoIP 安全研究中心及漏洞研究小组。在 TippingPoint 工作期间，David Endler 于 2005 年成立了一个业界内的 VoIP 安全组织——VoIP 安全联盟（Voice over IP Security Alliance，VoIPSA）。VoIP 安全联盟的宗旨在于通过提高 VoIP 安全研究、测试方式、最佳实践和相关工具等的现状，来促进 VoIP 技术的应用。目前，David 是 VoIP 安全联盟的主席，该组织有来自 VoIP 设备商、运营商和安全行业的超过 100 个成员，详细情况请

访问 http://www.voipsa.org。

在加入TippingPoint之前，David是新兴的安全服务公司iDefense的技术主管，iDefense后来被 VeriSign 公司收购。除了最新漏洞、蠕虫、病毒的研究之外，iDefense 公司还专业于计算机安全情报分析、计算机犯罪和黑客活动追踪。在 iDefense 公司任职之前，David 作为最前沿的安全研究人员，分别在 Xerox 公司、美国国家安全局、麻省理工学院工作多年。

作为一名国际公认的安全专家，David 经常作为演讲嘉宾出席各主要的业界会议，在许多顶级出版物及媒体上，David 的观点也常被引用或者专门报道，如华尔街日报、今日美国、商业周刊、连线杂志、华盛顿邮报、CNET、欧美科技台、CNN 等。David 发表了大量关于计算机安全的文章和论文，并被《IP 电话杂志》评为 IP 通信领域最具权威的 100 人之一。

David 以最优等的成绩毕业于杜兰大学（Tulane University），并获得了计算机科学学士和硕士学位。

Mark Collier

Mark Collier 是 SecureLogix 公司的技术总监，负责公司 VoIP 安全研究和开发工作。Mark 同时也负责 SecureLogix 公司企业客户 VoIP 安全评估的规划和实施工作。Mark 积极参与美国国防部的研究工作，主要关注 SIP 漏洞评估工具的开发。

在加入 SecureLogix 公司之前，Mark 就职于美国西南研究院（Southwest Research Institute, SwRI），领导一个研究小组进行计算机安全和信息战争方面的研究和开发。

Mark 常常作为演讲嘉宾参加各主要 VoIP 和安全的会议。他发表了大量关于 VoIP 安全方面的文章和论文，同时，他也是 VoIP 安全联盟的创始人之一。

Mark 以最优等的成绩毕业于圣玛丽大学（St. Mary's University），并获得了计算机科学学士学位。

谨以此书献给母亲、父亲、Sally 和 Sarah。 ——Dave

献给我的妻子 Gerri 以及我的两个女儿 Kristen 和 Kerri。 ——Mark

前　言

VoIP（Voice over IP）技术已经成熟，并且在大多数市场上正在替代传统的公用交换电话网络（Public-Switched Telephone Network，PSTN）而得以广泛部署。VoIP 含义广泛，它可以指安装在各种平台（如 Linux、Windows、VxWorks、移动设备、PC 等）之上的各种应用（如硬终端、软终端、代理服务器、IM 终端、P2P 终端等）。这些平台与应用所采用的各种开放的或者私有的协议（如 SIP、RTP、H.323、MGCP、SCCP、Unistim、SRTP、ZRTP 等）在很大程度上取决于已经存在的数据网络的体系结构和服务（如路由器、交换机、DNS、TFTP、DHCP、VPN、VLAN 等）。相应地，由于 VoIP 在用户、企业、电信运营商、中小企业等不同运行环境中的多样性特征，VoIP 安全也成为一个内容广泛的问题。

本书将 VoIP 安全主题做了收敛，我们认定面向的读者主要包括企业网络 IT 从业人员及一些上述列举的常见的部署场景中相关的人员（由于本书的内容大部分是 VoIP 相关技术及基本协议的安全问题，所以同样适用于电信运营商网络及其相关人员——译者注）。因为 VoIP 技术把语音通过分组后承载并传输于传统企业数据网络的路由器之上，相应地，威胁并困扰这些网络的计算机安全问题也将同样适用于 VoIP。这包括拒绝服务攻击（Denial of Service，DoS）攻击、蠕虫、病毒及通用的黑客攻击。打个比方，如果一个企业正在遭受分布式拒绝服务攻击（Distributed Denial of Service，DDoS），那么内部员工进行网页浏览的速度就会比正常时慢，与之类似，一个 VoIP 网络在遭受 DDoS 攻击时，相关的 VoIP 应用就可能会中断，至少那些智能化程度不高的 VoIP 应用会中断。

除了传统的网络安全和可用性等问题之外，对许多新的 VoIP 协议的实现机制进行详细的安全分析以及研究，就会发现 VoIP 还会带来一些其他的安全问题。大多数主流的 VoIP 设备提供商都在其产品中应用了日益重要的会话初始协议（Session Initiation Protocol，SIP）。这样一来，针对 SIP 协议的攻击就开始不断出现，如注册劫持（registration hijacking）、BYE 会话拆除、INVITE 泛洪攻击等，更有甚者，受利益驱动而出现的一些安全问题，如垃圾网络电话（Spam over Internet Telephony，SPIT）、语音钓鱼攻击等，也开始进入到 VoIP 领域。

对于当前和即将出现的 VoIP 安全问题，并没有一个特别有效的方法。相反地，在当前的安全策略中包含规划良好的、深度防御的安全防护体系是减少当前和即将出现的

VoIP 威胁的最好方法。

黑客大曝光系列

本书遵循了黑客大曝光系列图书一贯保持的良好模式。对 VoIP 相关的黑客攻击，目前研究得还不是非常深入和广泛。本书中描述的许多潜在的安全威胁、攻击方法在当前是少为人知的或者是全新的，部分安全问题是在本书写作的过程中才得以发现的。为了验证本书中的安全威胁以及攻击方法，我们搭建了一个小型的测试和研究专用的 VoIP 网络，包括两台 Linux 服务器，其上分别运行着基于 SIP 协议的软件 PBX，其中一台运行 Asterisk 系统，另一台运行 SIP Express Router 系统。我们在这两台 PBX 上尽可能多地连接了我们能够找到的不同 SIP 硬终端，包括 Cisco、Sipura、D-link、Avaya、Polycom 等品牌终端。本书第 2 章详细描述了应用的 SIP 测试网络的拓扑结构。在第 7～10 章中我们还详细描述了针对具体设备商产品的安全问题并搭建了 Cisco、Avaya 的测试网络。

在这些测试网络中，我们用尽各种方法来测试书中描述的攻击方法与技术。另外，本书中公布的一些数据是基于我们作为渗透测试人员、网络安全管理员、VoIP 架构师而获得的第一手资料。

本书对应的网站

我们为本书建设了一个独立的本书专有在线资源的网站：http://www.hackingvoip.com。该网站收集了书中提到的工具以及资料，需要说明的是这些资源是本书独有的。本书中涉及的其他工具，每一个都提供了所在网站的相应 URL 连接。如果书中涉及的工具，其原作者已经不再提供支持，我们在 http://www.hackingvoip.com 中都提供了最新的版本，以避免读者找不到相应的工具。我们计划在本书的网站及相应博客中继续提供相关的研究和发现成果。

本书导读

与黑客大曝光丛书一致，本书内容的基本结构是各章所讨论的攻击手段和相应的对策。

——这个图标代表着一种攻击手段

这个图标表明渗透测试技术和工具，在这个图标后面是攻击方式的名称以及传统的风

险评级表，这与黑客大曝光丛书完全一样。

流行度——表示在实际中，利用这种手段进行攻击的频率，这与简单度是密切相关的，“1”表示最少见，“10”表示最常见。

简单度——表示使用这种攻击手段所需要的技能，“10”表示运用广泛流传的工具就可实施，“1”表示需要编写特定的攻击工具，“5”左右的值表示可以获得相应的命令行工具，但是该工具难于应用，并且需要对目标网络及协议有详细的了解。

影响力——表示攻击成功后可能造成的损失的大小。取值在 1～10 之间，“1”表示仅能获取网络或设备的一些无关的信息，“10”表示能够获取目标的完全权限或者能够重定向、监听、篡改网络流量。

风险率——取值为前三个数值的平均值。

在书中的每一对策后面，我们会根据需要采用“注意”、“提示”和“警告”来强调具体细节以及相应的建议。

——这个图标代表着一种对策

书中在合适的地方，我们会根据不同 VoIP 平台提供不同类型的攻击防护对策。这些对策能够完全解决安全问题（如升级存在漏洞的软件或者采用更加安全的网络协议），或者暂时解决安全问题（如对设备进行再配置来关闭存在漏洞的服务、选项或者协议）。我们一直都推荐采用能够完全解决问题的方法，然而，我们确实发现，由于各种限制，这种方式不是每次都适用。在这种情形下，暂时的或者不完全的对策也强于不采取任何对策。一个不完全的对策仅仅能够起到减缓攻击者步伐的防护作用，并且这些不完全的对策可能被绕过。例如，一个标准的接入控制列表机制可能通过 IP 欺骗、中间人攻击或者会话劫持等方式绕过。

TinyURL

读者可能会注意到，本书中大多数地址比较长的参考网站的 URL 都应用了两种书写方式。一种是完全的 URL 地址，另一种是 TinyURL 的链接。TinyURL 提供一种服务，将原本很长的 URL 地址转换为一种更短的、容易书写的 URL 地址。例如，登录 TinyURL.com 网站，在提交框中输入下列链接：

```
http://maps.google.com/
?ie=UTF8&hl=en&q=10+market+st,+san+francisco&f=q&z=16&om=1&iwloc=addr
```

提交之后，返回如下：

```
http://tinyurl.com/yywp3z
```

这样一来，我们可以通过输入“http://tinyurl.com/yywp3z”来代替原来烦琐的 URL 链接，但却仍能够登录到原来的网站。

本书的组织

本书分为 5 个完全不同的部分。任一部分与其他 4 个部分关联不大，从而都可以独立进行阅读。如果读者只对其中某个部分感兴趣，则可以直接进行选择性的阅读。

第 1 部分　收集情报

第 1 部分是基础介绍，主要描述攻击者如何扫描整个网络并选取特定的目标，以便更准确地进行踩点。在这之后，攻击者可以通过被攻陷的 VoIP 设备进行进一步的更高级的攻击。

第 1 章　VoIP 网络踩点

本书开始部分描述了攻击者如何首先获取一个目标企业的概况信息，这可以通过采用一些工具进行被动侦察的方式来获得，如应用 Google、DNS 和 WHOIS 记录，以及目标企业的门户网站等。

第 2 章　VoIP 网络扫描

本章作为第 1 章的延续，概述了应用不同的远程扫描技术来获取网络中潜在存活的 VoIP 设备的方法。其中，在对 VoIP 设备的扫描中包括了传统的 UDP、TCP、SNMP 和 ICMP 等扫描技术。

第 3 章　VoIP 网络枚举

本章我们展现了主动发现各种独立运行的 VoIP 设备的方法，包括软终端、硬终端、代理服务器，以及其他支持 SIP 的设备。本章提供了大量的例子，其中包括了应用我们开发的 SIP 扫描工具进行的 SIPScan 的演示。

第 2 部分　VoIP 网络攻击

本书中的这一部分主要关注如何攻击 VoIP 应用所依赖的网络设施。我们首先描述了典型的网络拒绝服务攻击，并由此最终引导到 VoIP 会话的监听。由于书中所描述的很多技术都来源于传统的数据网络安全，我们将这些技巧应用到了 VoIP 设备及承载的网络服务。

第 4 章　VoIP 网络设施的 DoS 攻击

本章介绍了服务质量及如何利用各种免费的或者商业工具来客观地测量网络中 VoIP 通话的质量。随后，我们讨论 VoIP 设备及其依赖的各种服务（如 DNS、DHCP 服务等）的泛洪攻击或者拒绝服务攻击。

第 5 章　VoIP 网络侦听

本章重点关注攻击者在有适当的网络接入并能够侦听的前提下，能够进行的各种针对

VoIP 通话隐私的攻击。本章还展示了一些具体的攻击技术，包括号码采集、呼叫模式跟踪、TFTP 文件监听、真实通话监听等。

第 6 章　VoIP 干扰及篡改

本章具体描述了如何实施中间人攻击（MITM），以便对一个活跃的 VoIP 会话及其通话内容进行干扰和篡改。我们展示了应用 ARP 毒化进行中间人攻击的一些方法，并且还演示了 sip_rogue 这个新工具如何在通话的双方之间监视通话、篡改会话或者通话内容。

第 3 部分　针对 VoIP 特定平台的攻击

本书的这一部分，我们把注意力转向攻击一些特定的 VoIP 平台，这些平台一般都有特有的安全弱点和解决对策。我们演示了在本书最后几章中提到的一些攻击方法，并针对这些攻击方法阐述了特定厂商的减少攻击的最佳实践。

第 7 章　Cisco Unified CallManager

我们在全部由 Cisco 的交换机组成的网络环境中安装了 CallManager 4.x、硬终端等设备，进行前面章节描述过的各种攻击。

我们同样也描述了在 Cisco 交换网络中减少第二部分提到的各种安全攻击的最佳实践。

第 8 章　Avaya Communication Manager

类似地，我们搭建了一个包括 Avaya Communication Manager、Avaya 硬终端的环境，在此环境下进行第一部分、第二部分中描述的各种特定的攻击。

第 9 章　Asterisk

在本书的测试网络中我们运行的是 Asterisk，本章中我们进行了第一部分、第二部分描述的各种安全攻击。在我们的测试网络中，我们也通过这些 SIP 终端针对终端平台进行了一些基本的测试。

第 10 章　新兴的软终端技术

在本章中，我们讨论了这些年兴起的一些软终端服务（如 Skype、Gizmo 等）的安全问题。目前而言，这些软终端在企业市场还没有占据主导地位，但是它们在一些合作伙伴的帮助下随时准备着占据企业市场。

第 4 部分　VoIP 会话和应用攻击

本书的这一部分，我们把注意力从网络及设备的攻击转向针对协议的攻击。好的协议攻击就像是一种艺术，它可以在对主机和终端（话机）没有直接接入、无需重新配置的情况下，让入侵者完全控制 VoIP 应用的流量。

第 11 章　VoIP Fuzzing 攻击

Fuzzing 攻击或者称为健壮性测试、协议功能性测试，在安全领域已经应用了很长时间。在实践中已经证明，这种方法在对应用或者设备中的某一协议的自动漏洞发掘过程中是非常有效的。在本章中，我们演示了进行 VoIP 应用 Fuzzing 攻击的一些工具和方法。

第 12 章　基于泛洪攻击的服务中断

本章中，我们描述了通过发起海量的不同类型的 VoIP 协议和会话相关的消息来中断 SIP 代理服务器与 SIP 终端电话的攻击方式。这种攻击在实施时，能够部分或者完全中断 SIP 代理服务器或者 SIP 终端电话，部分攻击能够导致目标退出服务或者重新启动。

第 13 章　信令与媒体信息操纵

本章中我们讲述攻击者通过操纵 SIP 信令或者 RTP 媒体来劫持、结束，以及操纵整个通话的攻击方法。我们通过介绍十多种工具来演示这些攻击方法，与其他介绍的攻击方法相比，这些攻击方法易于实施并且后果严重。

第 5 部分　社交攻击

与传统邮件系统被淹没在垃圾邮件及钓鱼邮件中一样，我们也将在 VoIP 领域中开始看到这一社交骚扰攻击方式的横行。本章讲述了广告人员及诈骗高手如何把 VoIP 用户作为他们的骚扰目标，并提出了如何对付这些骚扰方式的对策。

第 14 章　SPIT（SPAM over Internet Telephony，垃圾网络电话）

语音垃圾信息或者说垃圾网络电话将是一个影响 VoIP 的类似问题。本书中描述的 SPIT 是指大量的、自动进行的、非邀而至的呼叫。SPIT 就像是电话推销界的兴奋剂，屡禁不止。我们大致可以想象 SPIT 会像垃圾邮件那样频繁发生。本章描述了如何利用 Asterisk IP PBX 和一个名叫 spitter 的新工具来产生自己的 SPIT。如何检测和避免 SPIT 在本章中亦有描述。

第 15 章　语音钓鱼

语音钓鱼更容易盛行是因为受害者会比一个在邮件中的网页链接更轻易地相信一个电话号码。另外，不用依靠大量投资，一个攻击者可以通过 VoIP 提供商搭建一个语音交互系统（IVR），而这种系统比起被攻陷的 Web 服务器，将更加难以追溯。VoIP 自身的特点也使得这种类型的攻击更容易实施，因为 VoIP 提供商的服务通常允许客户通过包月话费的形式进行无限制的呼叫。本章详细描述了这些攻击是如何进行的，以及如何在各个阶段检测这些攻击。

致读者

VoIP 的安全问题带来的挑战并不是一个新的话题。历史已经多次证明在 IP 通信领域的许多技术进步及新应用（如 TCP/IP、无线标准 802.11、Web 服务等）在出现之初都曾忽略过真实的安全需求，这些安全需求也是在这些新技术大规模部署之后才得以解决。在安全领域这样的故事演绎了一遍又一遍，希望本书能够让读者立于 VoIP 安全的潮头，帮助读者很好地规划、预算投资、设计、部署相应的保护措施。

目　录

第 1 部分　收集情报