

<<黑客大曝光>>

图书基本信息

书名：<<黑客大曝光>>

13位ISBN编号：9787111372486

10位ISBN编号：7111372484

出版时间：2012-4-20

出版时间：机械工业出版社华章公司

作者：Johnny Cache, Joshua Wright, Vincent Liu

译者：李瑞民, 冯全红, 沈鑫

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<黑客大曝光>>

### 内容概要

普适计算是一种颠覆性技术。

在本书中，施乐PARC研究中心的普适计算开拓者伯·贝戈勒介绍如何成功地将普适计算结合到产品、服务、工艺过程、商业策划之中。

本书介绍了普适计算的技术构成，全面挖掘它的潜能，并论证如何利用普适计算获得实质性的竞争优势。

本书将理论与应用案例相结合，具有较高的学术价值和很好的现实意义。

本书面向商业战略家、技术总监、改革家和企业家，可帮助理解构成普适计算领域的技术集合，理解这些技术带来的机遇和挑战。

## &lt;&lt;黑客大曝光&gt;&gt;

## 作者简介

伯·贝戈勒 (Bo Begole) 担任施乐PARC研究中心的首席科学家。PARC研究中心是著名的信息技术发祥地之一，发明并商业化了多种核心的信息技术，包括激光印刷 (Laser printing)、以太网 (Ethernet)、图形用户界面 (Graphical User Interface, GUI)、便携式计算机 (laptop) 等。贝戈勒负责该中心普适计算领域的研发工作，率领计算机科学技术致力于本书中提到的多种新型技术的发明创造和商业化。在2004年加入施乐PARC研究中心之前，贝戈勒是Sun微系统公司的研发科学家，致力于分布式协同系统和传感器网络的研发工作。他善于与社会学家和其他领域的科学家合作来开展创新性的研究工作，以期实现新的信息系统来帮助人们：远程协同工作，快速便捷地查找信息，高效通信交流，并努力提高信息技术的使用效能。

贝戈勒担任多个国际会议的主席，跨越的领域包括计算机支持的协同工作 (CSCW)、人机交互；担任多个顶级会议的组织委员会和程序委员会的委员，包括ACM普适计算国际会议 (Ubicomp)、智能用户接口、用户界面软件和技术、IEEE普适计算国际会议 (PerCom) 等。他与同事合作发表了数十篇由同行专家评审的学术论文，拥有若干项发明专利。他主持或参与了硅谷的多个商业技术兴趣组，在多个商业和技术的会议上发表了精彩演讲。

贝戈勒于1992年获得弗吉尼亚联邦 (州立) 大学数学专业的学士学位，分别于1994年和1998年获得弗吉尼亚理工大学计算机科学专业的硕士学位和博士学位。1981—1989年在美国陆军部队服兵役，1991年作为阿拉伯语翻译参加海湾战争。现在与他的妻子 (弗洛伦斯) 及3个孩子 (布赖顿、艾登、安娜西) 居住在加利福尼亚州洛斯拉图斯。

## <<黑客大曝光>>

### 书籍目录

译者序  
序言  
前言  
作者简介  
致谢

#### 第一部分 破解802.11无线技术

##### 第1章 802.11协议的攻击介绍

- 1.1802.11标准简介
  - 1.1.1基础知识
  - 1.1.2802.11数据包的寻址
  - 1.1.3802.11安全启蒙
- 1.2网络“服务发现”的基本知识
- 1.3硬件与驱动程序
  - 1.3.1Linux内核简介
  - 1.3.2芯片组和Linux驱动程序
  - 1.3.3现代的芯片组和驱动程序
  - 1.3.4网卡
  - 1.3.5天线
  - 1.3.6蜂窝数据卡
  - 1.3.7GPS
- 1.4本章小结

##### 第2章 扫描和发现802.11网络

- 2.1选择操作系统
  - 2.1.1Windows
  - 2.1.2OSX
  - 2.1.3Linux
- 2.2Windows扫描工具
  - 2.2.1Vistumbler
  - 2.2.2inSSIDer
- 2.3Windows嗅探工具/注入工具
  - 2.3.1NDIS6.0监控模式的支持 ( NetMon )
  - 2.3.2AirPcap
  - 2.3.3WiFi版CommView
- 2.4OSX扫描工具
  - 2.4.1KisMAC
  - 2.4.2OSX上的Kismet
- 2.5Linux扫描工具
- 2.6移动扫描工具
- 2.7在线地图服务 ( WIGLE和Skyhook )
- 2.8本章小结

##### 第3章 攻击802.11无线网络

- 3.1攻击的基本类型

## <<黑客大曝光>>

- 3.2通过隐藏获得安全
- 3.3击败WEP
  - 3.3.1WEP密钥恢复攻击
  - 3.3.2暴力破解由Linux版Nessus  
Datacom算法所创建的40位密钥
  - 3.3.3在Linux的非客户端连接使用Aircrack-ng破解WEP
  - 3.3.4在OSX上的WEP加密攻击
  - 3.3.5在Windows上, PTW对WEP的攻击
- 3.4综合案例: 破解一个隐藏的MAC过滤、WEP加密的网络
- 3.5针对WEP的密钥流恢复攻击
- 3.6攻击无线网络的可用性
- 3.7本章小结

### 第4章 攻击WPA保护下的802.11网络

- 4.1破解身份认证: WPA-PSK
- 4.2破解认证: WPA企业模式
  - 4.2.1获取EAP的握手
  - 4.2.2LEAP
  - 4.2.3PEAP和EAP-TTLS
  - 4.2.4EAP-TLS
  - 4.2.5EAP-FAST
  - 4.2.6EAP-MD5
- 4.3破解加密: TKIP
- 4.4攻击组件
- 4.5本章小结

### 第二部分 攻击802.11的客户端

#### 第5章 攻击802.11的无线客户端

- 5.1攻击应用层
- 5.2使用一个邪恶的DNS服务器攻击客户端
- 5.3Ettercap支持内容修改
- 5.4使用Karmetasploit动态生成非法接入点和恶意服务器
- 5.5客户端的直接注入技术
  - 5.5.1用AirPWN注入数据包
  - 5.5.2用airtun-ng实现通用客户端注入
  - 5.5.3用IPPON更新Munging软件
- 5.6设备驱动程序漏洞
- 5.7网络黑客和Wi-Fi
- 5.8本章小结

#### 第6章 专项解说: 在OSX上架桥过隙

- 6.1制订作战计划
  - 6.1.1准备攻击
  - 6.1.2准备回调
  - 6.1.3初始化recon
  - 6.1.4准备Kismet和Aircrack-ng
  - 6.1.5准备工具包

## <<黑客大曝光>>

- 6.1.6利用WordPress软件来传递Java漏洞
- 6.2让大多数用户级代码能够执行
  - 6.2.1收集802.11Intel
  - 6.2.2通过暴力破解密钥链获得root权限
  - 6.2.3给机器返回胜利
  - 6.2.4管理OSX的防火墙
- 6.3本章小结

### 第7章 专项解说：在Windows上架桥过隙

- 7.1攻击场景
- 7.2为攻击做准备
  - 7.2.1利用热点环境
  - 7.2.2控制客户端
- 7.3本地无线侦察
- 7.4远程无线侦察
  - 7.4.1Windows的监控模式
  - 7.4.2MicrosoftNetMon
- 7.5对无线目标网络进行攻击
- 7.6本章小结

### 第三部分 破解其他无线技术

#### 第8章 蓝牙扫描和侦测

- 8.1蓝牙技术概述
  - 8.1.1设备发现
  - 8.1.2协议概述
  - 8.1.3蓝牙规范
  - 8.1.4加密和认证
- 8.2准备一次攻击
- 8.3侦查
  - 8.3.1主动设备扫描
  - 8.3.2被动设备扫描
  - 8.3.3混杂扫描
  - 8.3.4被动通信数据包分析
- 8.4服务枚举
- 8.5本章小结

#### 第9章 蓝牙窃听

- 9.1商业蓝牙窃听工具
- 9.2开源蓝牙窃听工具
- 9.3本章小结

#### 第10章 蓝牙攻击和漏洞利用

- 10.1PIN攻击
- 10.2身份伪造
  - 10.2.1蓝牙服务和设备类别
  - 10.2.2蓝牙设备名称
- 10.3对蓝牙规范的错误使用

## &lt;&lt;黑客大曝光&gt;&gt;

- 10.3.1测试连接访问
- 10.3.2非授权AT访问
- 10.3.3未授权访问个人局域网
- 10.3.4攻击耳机规范
- 10.3.5文件传输攻击
- 10.4未来展望
- 10.5本章小结

## 第11章 入侵ZigBee

- 11.1ZigBee介绍
  - 11.1.1ZigBee作为无线标准的地位
  - 11.1.2ZigBee应用
  - 11.1.3ZigBee的历史和发展过程
  - 11.1.4ZigBee分层
  - 11.1.5ZigBee规范
- 11.2ZigBee安全
  - 11.2.1ZigBee安全的设计规则
  - 11.2.2ZigBee加密
  - 11.2.3ZigBee可靠性
  - 11.2.4ZigBee认证
- 11.3ZigBee攻击
  - 11.3.1KillerBee介绍
  - 11.3.2网络发现
  - 11.3.3窃听攻击
  - 11.3.4重放攻击
  - 11.3.5加密攻击
- 11.4攻击演练
  - 11.4.1网络发现和定位
  - 11.4.2分析ZigBee硬件
  - 11.4.3RAM数据分析
- 11.5本章小结

## 第12章 入侵DECT

- 12.1DECT简介
    - 12.1.1DECT规范
    - 12.1.2DECT物理层
    - 12.1.3DECT媒体存取层
    - 12.1.4基站选择
  - 12.2DECT安全
    - 12.2.1认证和配对
    - 12.2.2加密服务
  - 12.3DECT攻击
    - 12.3.1DECT硬件
    - 12.3.2DECT窃听
    - 12.3.3DECT音频记录
  - 12.4本章小结
- 附录A无线评估中的范围确定和信息收集





## &lt;&lt;黑客大曝光&gt;&gt;

## 章节摘录

版权页：插图：Makoto过去一直心安理得地做着一份基础设施评估的工作，不过这是她第一次被要求为一个客户完成其无线评估的工作，为此她已经从邻居家“借到”了一台Wi-Fi设备，以及旅行中不会令人产生怀疑的东西。

她知道所选时机不能再糟了，那时正值隆冬时节，她设想要访问的站点应该是一个很远的，并且传说中因为雪暴而闻名的地方。

虽然当她到达那里时，还不算是桃色天气（美国一种表示雪天积雪厚度的说法，桃色表示积雪厚度大约在2.5~5米——译者注），但她还是预先做足了功课，以便找到一种最好的方式以避免困于大雪中。

同时她还计划了需要提前准备的所有设备，并且打包了各种无线仪器。

她觉得她可能需要的设备有：一组无线网卡，远距离的定向天线和一个带有基于Atheros无线网卡的笔记本电脑。

还带了一个GPS装置以备迷路时使用，一个车载点烟器插座的电源适配器可以使笔记本在处于“战争驾驶”（war driving）的时候提供电力。

所有这些设备在她通过机场安检的时候，虽然给她带来了机场安检员无数怀疑的眼光，但她最终没有遇到多少麻烦地通过了安检。

当她在评估前的晚上抵达旅馆后，她向旅馆前台询问次日上午到达目的地需要多少时间，因为她以前从未到过这个地方，也不知道是否有什么交通工具，所以最好提前问清楚，特别是现在正值寒冬，有些路有可能会被封掉。

靠近停车库进行检测像往常一样，Makoto抵达站点时有点儿早。

当她到达那里后，她意识到这是一个庞大的航运和接收设施的大型仓库，卡车进进出出，络绎不绝。

然而，卡车两边的入口处标有不同的名称，因此她得出结论：最有可能的是多个企业共用这个站点。

她做好了心理准备，此时她不得不做出肯定的结论，即她计划中访问的所有无线网络实际上都属于这个客户，而不属于相邻企业中的任何一个。

在进入仓库之前，她决定先看看从仓库外部可以检测到什么。

她把车停在了工厂的车库，打开她的笔记本电脑，首先使用内置在Windows中的无线工具对无线网络进行了第一轮搜索。

她知道主动扫描是非常有限的方式，任何具备无线评估知识的人都知道将无线网卡设置为监控模式。

不过，她也觉得主动扫描这种典型的方式，对于大街上随便哪个人，用来试试看都有哪些无线网络是开着的，也不失为一种方法。

这样也许能获得些有用的信息。

很快，她捕捉到了一些采用出厂默认配置和一些使用WEP和WPA的组合算法进行加密的无线网络名称。

但她不确定这些站点是属于她要找的客户的，还是别的企业的，所以她只是简单地记录了她能看到的内容，然后就继续往前走了。

## <<黑客大曝光>>

### 编辑推荐

《黑客大曝光:无线网络安全(原书第2版)》面向商业战略家、技术总监、改革家和企业家,可帮助理解构成普适计算领域的技术集合,理解这些技术带来的机遇和挑战。

《黑客大曝光:无线网络安全(原书第2版)》将理论与应用案例相结合,具有较高的学术价值和很好的现实意义。

<<黑客大曝光>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>