Fadia道德黑客丛书

ANKIT FADIA 著
孟庆华 译

HACKING MOBILE PHONES

手机黑客攻防

电子科技大学出版社

手机黑客攻防

法迪亚 著

孟庆华 译

电子科技大学出版社

图书在版编目（CIP）数据

手机黑客攻防/（印）法迪亚著；孟庆华译. —成都：电子科技大学出版社，2007.10

ISBN 978-7-81114-652-3

Ⅰ.手… Ⅱ.①法…②孟 … Ⅲ.移动通信—携带电话机—安全技术 Ⅳ.TN929.53

中国版本图书馆 CIP 数据核字（2007）第 153981 号

手机黑客攻防

法迪亚 著

孟庆华 译

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

策划编辑：郭　庆

责任编辑：郭　庆

主　　页：www.uestcp.com.cn

电子邮箱：uestcp@uestcp.com.cn

发　　行：新华书店经销

印　　刷：成都市海翔印务有限公司

成品尺寸：185mm×260mm　　印张　15　　字数　365 千字

版　　次：2007 年 10 月第一版

印　　次：2007 年 10 月第一次印刷

书　　号：ISBN 978-7-81114-652-3

定　　价：38.00 元

前　言

随着计算机与互联网的迅速普及，人类对计算机的依赖达到了前所未有的程度，计算机的安全直接关系到国家、企业、个人乃至人类社会的生存和发展。而对计算机与互联网构成的威胁最严重的，正是防不胜防的网络黑客。纵观当今的互联网业界，病毒木马泛滥、黑客攻击猖獗，各种病毒变体花样百出，恶意攻击手段层出不穷。如何防黑、反黑、制黑，已成为所有互联网用户共同面对的巨大挑战。

上海兴韦教育集团及旗下的上海托普信息技术学院，利用自身的产业背景和专业优势，首度全面引进了国际互联网界资深反恐反黑精英、少年成名的网络安全大师 ANKIT FADIA 的系列专著——“法迪亚道德黑客丛书”。力图从黑客攻防两个角度，将国际最前沿的网络安全技术介绍给国内读者，帮助国内网络用户知黑、防黑、反黑，共同营造和维护健康、安全的互联网世界。

手机黑客攻击是“法迪亚道德黑客丛书”涉足的最新领域，也是移动通信安全天空的一块阴云。此书对手机黑客入侵方面的最新手段彻底曝光，包括各种蓝牙攻击、拒绝服务攻击、手机邮件攻击、木马蠕虫病毒攻击等；对各种防护策略也做了翔实的案例研究；最后深入讨论了现在流行手机的安全使用诀窍。此书内容新颖，视角独特，是安全人士的必备用书。

本书主要由孟庆华博士主持翻译、统稿、审校，李文丽参与了第一章、第二章的翻译，余光柱博士、陆星家博士、扬帆博士、张明艳硕士参与了后续章节的翻译。由于译者水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

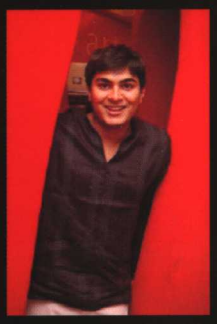
有关全套“法迪亚道德黑客丛书”的出版情况，敬请登录 http://www.e-hacker.info.查阅。

译　者

兴韦—法迪亚网络与信息安全中心（中国）

上海托普信息技术学院

2007 年 9 月



Ankit Fadia 生命中的里程碑

10岁——父母在家给他配置了一台个人电脑。

12 岁——表现出对计算机的超常天赋，成为无师自通的少年黑客。

14岁——出版了第一本个人专著——An Unofficial Guide to Ethical Hacking（良性入侵——道德黑客非官方指导），轰动业界，迅即被翻译成11 种语言，在全球15个国家出版发行，并被亚洲和北美的一些著名高校选作教学用书。

16岁——9·11 事件后，成立了法迪亚道德黑客国际研究院，曾为机密情报机构破译了由本·拉登恐怖分子网络发送的加密的电子邮件。自从那时FADIA就介入了与国际安全和计算机网络有关的多个机密工程，负责处理机密情报机构的亚洲行动。

21岁——成为道德黑客的年轻领袖，出版了11 本畅销书，在25 个国家发表了超过1000 次研讨会,获得了45 个奖励。

22岁——致力于数字智能、安全咨询和培训等方面研究，规划并开发出法迪亚道德黑客培训认证体系，并在新加坡管理大学的信息系统学院、美国圣何塞州立大学得到了成功的应用。

2007年——来到中国。

目　录

第一章 蓝牙攻击

- 你手机上的敏感资料——邮件、银行信息、密码能否有效避免恶意攻击？
- 你的手机是否常收到令人厌烦的、没有安全保障的垃圾信息？
- 你发送的私人短信是否安全躲开了窥视者的眼睛？
- 你手机上储存的照片是否安全避免了在互联网和手机网上传播？

手机已经变得无所不能，手机只是通话工具的日子已经一去不返了。手机已经进化成你的相机，你的电脑，你的互联网联接，你的日历，你的通信录，你的电子邮箱，等等。换句话说，你的手机已经开始掌握极其私密的信息——对个人和企业都很宝贵的信息。这就为一种称为全新的手机破解打开了大门。

现在很多手机都具有内置蓝牙功能。蓝牙是一种无线通信标准。在 10 米的范围之内（大约 33 英尺），电子装置可以通过蓝牙互相通信。也就是说，蓝牙是一种允许蓝牙装置在一定范围内传输文件、照片、通信录和其他数据的协议。与手机相关的攻击在某种程度上涉及蓝牙通信标准。因此，对破解者和潜在的受害者双方来说，都有必要熟悉蓝牙通信标准。

蓝牙通信协议可以连接多种蓝牙设备，并不仅限于两种类似的装置之间（比如两个手机），在两个不相似的装置（如 PDA 和电脑）之间亦可建立连接。该协议还可用于与其他网络协议的连接。例如，蓝牙手机可以连接一台电脑，然后利用电脑连接上互联网。所有的蓝牙通信设置几乎都可划分为两大类：

- 主设备与主设备连接。在这种设置下，通信双方的蓝牙装置都拥有键盘，可以灵活地互相通信。例如，两部手机连接后，两个蓝牙装置都具备了输入设备。因此，这种连接方式被称为主设备与主设备连接。在这种连接方式下，你可以主动键入数据与其他蓝牙设备进行通信。
- 主设备与从设备连接。在这种设置下，设备没有输入装置。例如，手机与蓝牙耳机之间的连接可以称为主设备与从设备连接。因为手机有键盘，你可以主动控制数据的输入与耳机通信。而另一端的蓝牙设备没有输入设备，要依赖程序指示实现通信。

和其他所有协议一样，蓝牙通过预设的程序建立连接。

大部分蓝牙连接步骤如下：

1. 发现：设备扫描目标设备，希望能发现蓝牙。
2. 配对：设备交换配对码及其他信息。
3. 绑定：设备交换密钥绑定连接。

关于蓝牙连接的其他方式将在本章稍后部分的“蓝牙安全模式”一节讲到。

1.1 发现

在两种蓝牙设备互相通信之前，它们必须首先执行被称之为发现的程序。换句话说，蓝牙装置需要先找到对方。通常，一个蓝牙装置在一定范围内扫描以发现其他的蓝牙装置。只有当该蓝牙装置发现正确的目标蓝牙装置后才会开始数据传输。

攻击原理：每个蓝牙手机设备都可以有多种操作模式，如表 1-1 所示。

表 1-1

模　式	状　态
关	蓝牙被关闭。你的手机不能连接任何其他蓝牙设备，其他任何蓝牙设备也不能发现（因而连接上）你的手机
开	一旦你的手机与其他设备建立了蓝牙通信通道，手机的模式就被设定为开
可发现或全部可见	即使当前没有活动的通信通道，也可被 10 米（约 33 英尺）的范围内被任何其他蓝牙设备所发现
隐藏	你的手机不会被不明设备（不能与你的手机配对的设备）发现，只会响应能与之配对的设备

1.1.1 配对

蓝牙设备发现对方后就会进行配对。配对程序之于蓝牙正如 TCP/IP 协议之于互联网上的两台计算机一样。它允许两个蓝牙设备（两者试图建立一个通信通道）互相交换如地址、版本及配对码等重要信息。我们可以把匹配码看成一种类似密码的东西。只有配对程序成功完成之后，两个设备才能取得与对方进行通信的权利。

如果没有输入正确的配对码，设备不会接受蓝牙连接请求。要注意的是，在主设备与主设备蓝牙连接的情况下，双方用户都必须输入配对码。例如，当两部手机试图通过蓝牙连接时，双方用户都必须输入一个配对码。另一方面，在主设备与从设备连接的情况下，主设备用户必须输入配对码，而从设备则按预设程序指示自动读取配对码。例如，一部手机试图与它的耳机连接，手机就需要输入配对码，而耳机自动按预设程序指示读取配对码。

双方用户输入一致的配对码后，就会生成一个链接关键字。然后链接关键字展开了第三步即绑定。要注意的是，有些设备可能不需要配对就可以开始传输数据。也就是说，配对通常是一个可选程序用于绑定固定通信的设备。根据配对码，配对的设备更易被找到、更易识别。

1.1.2 绑定

配对码交换之后，设备自动生成一个密钥并使之共享。正是密钥使每一对蓝牙连接是独立的而且是绑定的。绑定的这种性质意味着两个设备间的连接只能用于这两个设备。其他设备不能干扰或窥视这种连接。也就是说，如果两部手机之间建立了蓝牙连接，那么在该范围内的任意第三部手机均无法窃听数据传输。这只是意味着，在任何一个时间点上从技术上说，一个蓝牙设备应该知道正与之通信的当前设备。从发现开始到绑定阶段，可以说两个蓝牙设备之间的连接建立了。

攻击原理：从底层通信原理看，验证和建立蓝牙连接的不同步骤可以描述如下：

1. 源设备向目标设备发送其地址。

2. 目标设备要求源设备应对随机挑战。源设备使用者输入配对码，计算链接关键值。源设备使用这个链接关键值计算出随机挑战的答案。

3. 目标设备计算出它发送给源设备的随机挑战的答案，源设备将答案发送给目标设备。

4. 目标设备比较它的答案和源设备发来的答案。如果两相符合，蓝牙连接就正式得到授权并启动。

1.1.3 蓝牙安全模式

不是所有的蓝牙通信通道都必须经过发现、配对和绑定三步。要注意的是蓝牙有不同的安全模式，可以在不同的时间启动。每种蓝牙设备都有三种安全模式可供选择：

- 无安全模式。在无安全模式下，蓝牙设备不会运行或跟随任何安全措施。在这种模式下，很多安全措施如验证、配对以及加密都不会使用。例如，你在通过蓝牙发送通信录时，你将忽略所有的安全措施。通常蓝牙设备遭受蓝劫攻击时就会出现这种特别的模式。本章稍后我们将讲到蓝劫。
- 服务级安全模式。启用服务级安全模式的蓝牙设备有一个中心安全经理控制服务设备和服务的使用。在试图连接的过程中，中心安全经理针对不同的申请控制和实行不同的安全程序。这种安全安排有可能使某一用户有权访问某一程序而无权访问另一程序。
- 链路级安全模式。启用链路级安全模式的蓝牙设备在建立通信通道之前就实施了授权和安全程序。这种模式会对设备的链路建立过程实行适当的验证、配对和加密程序。通常情况下，在这种安全模式下，要建立通信通道，就会执行我们之前描述的配对和绑定步骤。

毫无疑问，蓝牙是一种得到广泛支持并广泛应用的革命性的无线通信方式。不幸的是，如同大多数其他协议一样，蓝牙因其不断受到的安全威胁、存在的漏洞和脆弱性而深受其苦。

1.2 案例研究

下面这些真实的案例展示了手机安全受到攻击时可能造成的损害。

1.2.1 美国纽约

在纽约一条繁华的大街上的一个咖啡馆里，一位年轻妇女坐在桌旁，一边啜着她最喜欢的“拿铁”咖啡，一边翻看一本杂志上的最新时尚小招数。突然她的手机屏幕亮了，有一条匿名短信发进来：嗨，美女！看起来很棒。虽然她有一点警觉（而且看到没有发送号码还有点厌恶），但是她还是没有理会，只是觉得自己又做了垃圾短信的牺牲品。没过两分钟，她的手机又亮了，又进来一条匿名短信：你穿着蓝色上衣看起来真的很不错。这条非常私人的信息引起了她的注意，她直起身来。她穿着一件蓝色衬衫。她很快审视了一番坐在她周围的人群，想要找出发送者。摆弄她的手机几分钟后，又收到一条淫秽的短信之

后，年轻妇女快速收起她的东西走了出去。这种公然侵犯她的隐私的行为吓坏了她，她再也不愿踏入这个咖啡馆了。

1.2.2 中国香港

一位成功的香港企业家正在参加一个领导艺术会议。他是那种通过手机运转他的企业的人。从发送敏感的电子邮件到创建计划文件，从发送传真到召开重要的商业电话会议，他习惯于用他的手机做一切事情。他的手机也使他在参加会议时不会漏掉任何与生意相关的工作。会议结束后，这位企业家一回家就发现门下塞了一封信。拆开信以后，他发现里面有好几页他的个人信息资料：电子邮件、照片、电话号码以及其他详细资料。不仅包括敏感的、机密的商业计划，还有他在手机上做的会议记录。他意识到可能有人侵入了他的手机并窃取了手机上的所有数据。

1.2.3 新加坡

一位妇女每周日都带着孩子在新加坡勿洛的一家本地购物中心购物。一天，她的手机收到了一个名片形式的短信。按照以往的惯例，她立即储存了新名片。当她查看名片时，上面写着：哈哈！你的孩子很漂亮。很快她又收到了一条类似的短信。这次她没有储存发进来的名片，而是拒绝了它。接下来的一个小时里，这个妇女不停地收到短信，一条接一条，有些她拒绝了，有些她还是看了。

1.2.4 日本东京

一群青少年搭乘火车到最受欢迎的购物中心去。他们的这个爱好每天要持续几个小时，包括不停地按手机键。这个群体不是由一般的青少年组成的。他们是有经验的蓝劫客，喜欢用手机玩捉弄人的游戏。而且，他们不是唯一的一群骚扰者，不同的骚扰群体之间互相竞争，看谁能向没有戒心的个人发送最多的骚扰信息。

1.2.5 中国北京

我到中国北京时，做了一个蓝牙沿街扫描实验。我走进城里最繁忙的购物中心，在食品区坐下，点了一些北京的小吃。在我吃饭时，我的手提电脑就在寻找蓝牙设备，试图与那些在有效范围内的设备建立未经授权的连接。在一个小时之内，软件在有效范围内找到了令人吃惊的 3 456 部手机，其中 2 982 部设备允许未经授权的连接。而且，我的工具还记录了许多手机话筒传达的敏感数据。

1.2.6 日本大阪

为推进我之前的实验，我在日本大阪的几个战略地点重复了这一程序。结果如表 1-2 所示，相当令人吃惊。

表 1-2 日本大阪，蓝牙沿街扫描实验

地　点	可发现比例	允许连接比例
购物中心	95%	73%
火车站	91%	34%
银行	85%	82%
咖啡店	89%	69%

实验只考虑了那些带有蓝牙功能的手机。

攻击原理：需要非常注意的是，容易被发现的手机的比例非常高。但是，能否未经授权连接上一部手机决定于它的模式和你所花费的时间。

1.2.7 马来西亚吉隆坡

在蓝牙沿街扫描实验的第三部分，我在马来西亚的吉隆坡的一些战略地点重复了上述程序，这次实验的结果同样很有意思，如表 1-3 所示。

记住，只有那些有蓝牙功能的手机才被计算在内。

表 1-3 马来西亚吉隆坡，蓝牙沿街扫描实验

地　点	可发现比例	允许连接比例
购物中心	73%	12%
夜总会	95%	92%
写字楼	85%	73%
机场	84%	23%

1.3 蓝牙攻击的类型

对没有戒心的手机用户可以实行多种蓝牙相关的安全威胁和攻击。

- 蓝劫（蓝牙对象交换（OBEX）信息强推攻击）；
- 修改通信录；
- 蓝牙垃圾短信；
- 蓝窃（OBEX 强拉攻击）；
- 蓝牙后门；
- 蓝牙蠕虫；
- 蓝牙打印；
- 蓝牙扫描；
- 其他攻击；
- 短配对码；
- 缺省配对码；

- 随机挑战答案生成器；
- 中间人；
- 信息广播；
- 强暴攻击；
- 拒绝服务（DOS）；
- 单元密钥；
- 拟人化。

虽然大多数这些与蓝牙有关的攻击方法还比较新，但是这些方法很常用，使用范围也很广。

下面我将逐一介绍每一种类型。

1.3.1 蓝劫攻击

在拥挤的公共场所，你的手机是否曾收到过匿名短信？你是否想过那些短信从何而来而你又是如何收到的呢？答案可能是一种称为蓝劫的技术。

蓝劫就是在 10 米（约 33 英尺）的范围内从一部蓝牙手机向另一部蓝牙手机发送匿名短信的过程。不但接收者不会知道蓝劫短信的发送者，而且，蓝劫允许人们互相发送免费短信。因为蓝劫利用了手机本身的蓝牙技术（不是操作者），所以使用这种技术发送的所有信息都是免费的。人们把蓝劫描述为另外一种通信方式。

蓝劫利用了蓝牙通信协议形成阶段的一个小漏洞。在任何两个蓝牙设备互相通信之前，设备首先通过初始握手阶段交换信息。在这个阶段，初始化的蓝牙设备名字必须要在目标蓝牙设备的屏幕上显示出来。在这一步，初始化设备可以向目标设备发送一个用户确定域。这个域用于在蓝劫时发送匿名短信。这种攻击有时也被称为 OBEX 强推攻击，因为它允许攻击者强行向被害者的手机发送数据。

蓝牙对象交换(OBEX)是大多数无线设备数据交换的事实协议。这一协议超越了 TCP/IP 和蓝牙，在无线设备之间进行文件、图片、名片、日历条目以及各种其他数据的交换。蓝牙通信标准广泛采用 OBEX 通信。因为蓝劫这种攻击方式是强行向受害者的手机设备发送蓝牙短信（确切地说是名片），它有时又被称之为 OBEX 强推攻击。

蓝劫不会移动或修改被害者手机上储存的任何数据。虽然蓝劫不会对手机造成任何永久性损害，但是它会使人非常厌烦。因此，在很多情况下，蓝劫攻击只是为了“找乐”（通常是恐吓或调戏），而非恶意攻击。蓝劫的另一个限制因素是只有双方的蓝牙设备都在距对方 10 米以内，攻击者才可能被抓获。不管怎么说，为了使你更好地了解其他攻击，蓝劫是一个最佳例子。我会在书中稍后部分讲到其他攻击。

匿名免费短信

在世界上大多数城市发送匿名免费短信的方式非常流行。攻击者不仅可以使用蓝牙手机发送匿名短信，还可以使用任何其他蓝牙设备发送短信。传统上来说，每当设备之间进行短信或文件传输时，双方设备都知道对方的身分。这样受害者就非常容易找到其接收的文件或短信的来源。但是，蓝牙的出现使人很难追踪接收到的信息和文件的实际源头。受害者总是试图把其手机上显示的姓名（攻击者可以自定义姓名）与周围的每个人对上号。

只需要一部蓝牙设备，就可以很容易地在拥挤的公共场所实行这种攻击。虽然根据手机型号的不同攻击方式略有不同，但是一个典型的蓝劫攻击发生时，攻击者先要在蓝牙设备上创建新的通信录联系人。匿名短信（如：嗨，你好吗？）是写在通信录的姓名域的。然后在 10 米的范围内扫描受害者手机。这一步通常被称之为发现，用时不超过 10 秒。很快手机的屏幕上就会出现一串名单（虽然你可以更改你手机的名字，但是手机型号的名字是制造商缺省设定的）。从名单中选定受害者手机的名字后，新的通信录联系人就会发送到受害者手机上。受害者手机从以上操作信息接收提示音时就表示受害者收到了这条匿名短信。接通可以看出，发动蓝劫攻击非常简单，只需要一部蓝牙设备和一个拥挤的场所即可。一旦有人收到了一条匿名短信，受害者的手机通常会有短信提示音，同时显示以下信息：蓝牙收到联系人姓名或者是蓝牙收到名片。

很多人都会立即按“查看”键，蓝劫短信就马上显示出来。受害者还可以看到攻击者发送的联系人条目中的所有其他域（如电话号码、姓氏和电子邮箱等）。为了更清楚地说明这一点，我们介绍一下从不同的蓝牙设备上发动蓝劫攻击的步骤。

手提电脑/个人电脑

在下列情况下，可以从手提电脑发动蓝劫攻击：

1．启动电子邮件客户端程序。

如图 1-1 所示的例子用的是 Outlook Express。

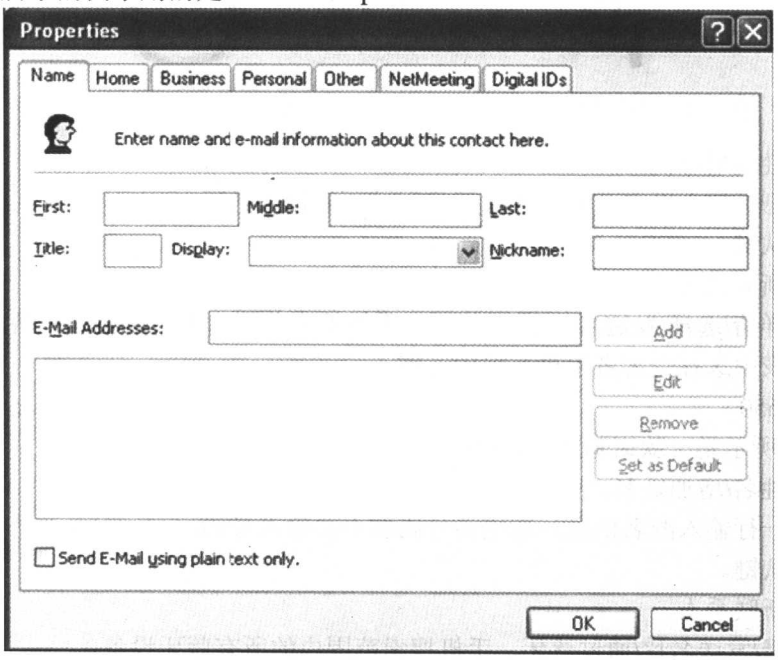


图 1-1　电子邮件客户端 Outlook Express

2．点击地址框。

3．点新建，选择新联系人。

4．在姓名域键入匿名信息并保存新联系人。

5．在新联系人处点击鼠标右键。