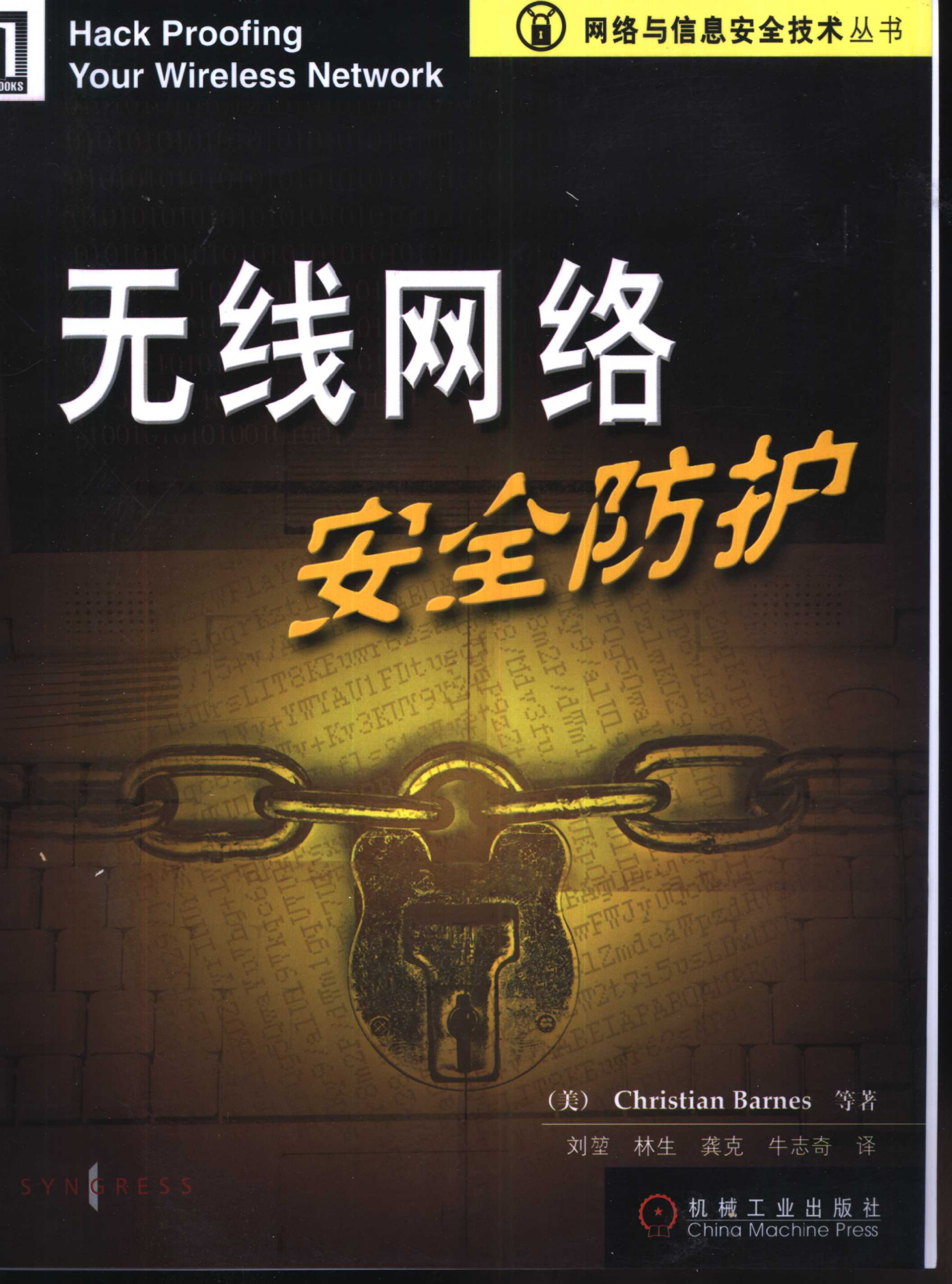
Hack Proofing
Your Wireless Network

网络与信息安全技术丛书

无线网络安全防护



(美) Christian Barnes 等著

刘堃 林生 龚克 牛志奇 译

SYNGRESS

机械工业出版社
China Machine Press

网络与信息安全技术丛书

无线网络安全防护

（美） Christian Barnes 等著

刘堃 林生 龚克 牛志奇 译

机械工业出版社
China Machine Press

本书介绍无线网络所面临的挑战及无线网络的广播特性，涉及监听、截取和窃听技术，以及黑客攻击的工具和设备，入侵检测策略。书中还介绍了如何建立信息分级过程，如何设计和部署安全网络，如何设计和规划成功的审计，如何开发无线网络安全检查表。本书适合网络安全技术人员参考。

本书版权登记号：图字：01-2002-1857

图书在版编目（CIP）数据

无线网络安全防护/（美）巴恩（Barnes, C.）等著；刘望等译. -北京：机械工业出版社，2002.12

（网络与信息安全技术丛书）

书名原文：Hack Proofing Your Wireless Network

ISBN 7-111-11110-9

Ⅰ.无… Ⅱ.①巴…②刘… Ⅲ.无线电通信-接入网-安全技术 Ⅳ.TTN925

中国版本图书馆CIP数据核字（2002）第082990号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：李云静

北京忠信诚胶印厂印刷·新华书店北京发行所发行

2003年1月第1版第1次印刷

787mm × 1092mm1/16 · 18印张

印数：0 001-4 000册

定价：35.00元

序　言

为了让无线通信系统或设备更加安全，一个简单的办法是把它放进法拉第箱（faraday cage）中。不幸的是，这种策略虽然可以使得蓄意攻击者无法接触你的设备，但这样一来，这些设备对你来讲也将会变得毫无用处。

过去，别人必须坐在你的计算机前才能阅读你的文档，偷看你的电子邮件或搞乱你的设置。但是现在，虽然别人可能是坐在隔壁的办公室里、楼上或楼下，或者旁边的一幢建筑物里，但他可以就像是坐在你的计算机面前一样搞破坏。无线通信技术的发展让你极大地提高了工作效率，并且在使用上越来越简单，但同时也给你的系统和使用的信息带来许多意外的危险。

你的计算机上使用了应用802.11或蓝牙技术的设备了吗？你是不是正在使用个人数字助理与其他系统进行通信或者用它连接到因特网？你是不是正在使用移动电话和你的办公室建立网络连接？你是不是为了外出时带着笔记本可以和家里的网络设备通信，就在家里安装了最先进的无线通信网关？你是不是计划在办公室里安装一个无线通信系统？只是做了这么简单的一些事情，信息的安全风险就大大地增加了。这样一来，别人可以更加容易阅读到你的财务数据，看到你保存的文档，或者浏览你的电子邮件。无线通信系统使通信更加方便了，但同时也带来了相应的风险——信息安全技术也要同步发展才行。你必须解决诸如以下这些问题：网络身份识别和加密密钥；别人即使靠得再近也不能让他看出你的无线通信网络；除了你指定的设备、系统或者人，确保没有任何系统和人可以使用你的无线通信资源。

人们在一般情况下是不愿意去考虑安全问题的。安全与成本，或安全与使用的方便性常常是工作中的矛盾问题，并且有许多其他因素在业务上看起来更重要。正是因为这些原因，在你考虑任何新的实施计划的时候，必须要预见到安全问题，制定清晰和明确的业务方案，保证安全保护措施在它们的生命周期内可以被合理和高效地实施。

虽然没有什么办法可以让你的系统百分之百安全，但是你可以了解黑客和解密高手对付你的办法，学会在他们攻击你的计算机或其他无线通信设备的时候将其抓获的办法，了解增加攻击系统难度的办法，让他们望而却步，并转向其他更容易攻击的系统。

本书的目的是为包括业务分析和信息技术方面所有领域的人们提供对无线通信方面的一些看法和相关的信息，无论他们是否正在为无线通信项目准备业务方案；无论他们是不是IS/IT专家，并计划着部署一个新的无线通信网络；也无论他们是不是安全重要性的“忠实信徒”，都应将室内网络扩展成为具有无线通信网络接入的功能、可以反击网络攻击的功能、可以提前部署安全措施的功能。

如果你没有太多的时间阅读和理解所有的章节（它们详细介绍了有关信息安全方面的、被应用到无线通信技术中的各种复杂知识），可以只简单地阅读有关策划和部署无线通信网络方面

的介绍及其安全问题的介绍。你将从本书的实例分析中受益匪浅，因为它们描述了如何使你的无线通信网络和设备变得更加坚固和更加安全。他人若不了解相关的知识将无法危害到你的信息或者利用你的系统，这样一来你就可以高枕无忧了。

——Jeffrey Posluns, CISA，CISSP，SSCP，CCNP

目　录

第1章　无线通信网络的挑战

本章中的解决方案：

- 无线通信网络技术概述。
- 了解无线通信网络的发展前景。
- 了解无线通信网络的优点。
- 面对现在无线通信网络的实际情况。
- 分析无线通信网络的标准。

☑ 总结。

☑ 解决方案简要概括。

☑ 常见问题解答。

1.1　概述

当20多年前无线通信网络的概念第一次被提出来的时候，出于对随时随地都能够漫游连接所带来的便利性和灵活性的渴望，它极大地激发了全球科学家、厂商和用户的想象力。不幸的是，尽管各种无线网络解决方案都出现了，但美好的设想却变成了失望。第一轮解决方案不能满足不断变化的IT环境对网络互连、移动性和安全性方面的需要。

这种情况一直持续着，直到20世纪90年代，基于蜂窝技术的和基于办公室局域网（LAN）的无线网络技术被广泛采用，特别是经过过去两年对基础性问题的研究情况才得到很大的改观。通过研究发现，问题就是绝大多数公司IT部门和小型的办公室对无线通信网络都无法完全接受。

在本章中，你将可以了解到无线数据网络方面现在已有的技术和无线网络技术将来的发展趋势。我们将要介绍办公室局域网解决方案，包括802.11及其他的子组（802.11b、802.11a、802.11g）；HomeRF——蜂窝式无线数据解决方案，包括无线应用协议（Wireless Application Protocol，WAP）和i-Mode，支持它们的网络基础设施（特别是在2G、2.5G和3G中）；最后是802.15个人区域网（Personal Area Network，PAN）解决方案，如蓝牙技术。除此之外，我们将简单分析一些用来构建无线城域网（WMAN）的新标准和其他一些为商业应用而提出来的无线数据传输解决方案。

除了介绍无线通信网络涉及到的一些技术之外，我们还将介绍主要的安全问题，特别是影响到蜂窝式办公室局域网和个人区域网无线设置的问题。通过这种方式，我们将浏览到一些主要的安全问题，这些问题会在以后的章节里为你做详细介绍；另外还将讨论一些可以用来最大限度减少这些影响的措施。

在你阅读完本章之后，将会对无线通信网络技术和相关的安全风险有一个完整的理解。我们希望能够正确评价无线网络互连技术给我们的工作和家庭生活带来的影响，使你认识到安全

问题在使用无线通信网络过程中具有重要意义。让我们开始吧！

1.2　无线通信网络技术概述

现有的无线通信网络技术可以分为几种形式，提供了众多的解决方案，这些解决方案可以应用到主要是以下两种无线网络互连形式：

- 蜂窝式无线数据解决方案。
- 无线局域网（WLAN）解决方案。

1.2.1　定义蜂窝式无线通信网络

蜂窝式无线数据解决方案使用已有的移动电话和寻呼机通信网络来传输数据。数据可以被分成许多种形式来传输，包括传统通信，如电子邮件、目录信息交换和基本信息传输；端对端通信，如报文服务；信息查询，如导航信息、新闻和其他种类。

有一些蜂窝式无线数据网解决方案只支持单向通信。虽然从技术上来说，它们被划分到蜂窝式数据解决方案这一类里，但是它们并不包含在本书的讨论范围之内。我们将集中讨论至少提供双向数据通信的蜂窝式解决方案。而且在本书里，我们只讨论支持包含基本安全措施的解决方案。

1.2.2　定义无线局域网

无线局域网解决方案提供了在有限覆盖区域内的无线连接。覆盖范围通常是指以基站或AP（Access Point）为中心，半径在10米到100米的区域。这些解决方案提供了支持典型办公台式电脑或家用台式电脑与其他网络资源通信的必要功能。

这种情况下的数据流通常由远程应用程序访问和文件传输构成。无线局域网解决方案为无线通信网络节点提供了与有线局域网资源对接的方法。这样一来就出现了有线通信网络节点与无线通信网络节点可以交互的混杂型网络。

1.2.3　无线通信网络技术之间相互交叉发展

在往后不长的一段时间里，通常都可以划分为这两类，但是许多厂商打算在明年将新开发的产品投向市场，这些产品将会使得蜂窝式无线通信网络设备和无线局域网设备之间的界限变得模糊起来。这包括移动电话、高端寻呼机和个人数字助理（Personal Digital Assistant，PDA），它们也提供了与使用像蓝牙这种无线局域网技术的本地设备进行个人区域网互连的能力。

这种趋势将会不断地加速发展。一方面不断开发出功能更强大和体积更小的无线通信网络部件，它们可以支持更高的访问速度和更强大的通信能力；另一方面，PDA和其他便携式信息设备的功能也越来越多。因此消费者不断希望能有集成化更高的的通信环境，它要能够通过有线和无线的信息资源提供无缝的应用支持。

1.2.4　发展趋势与数字统计

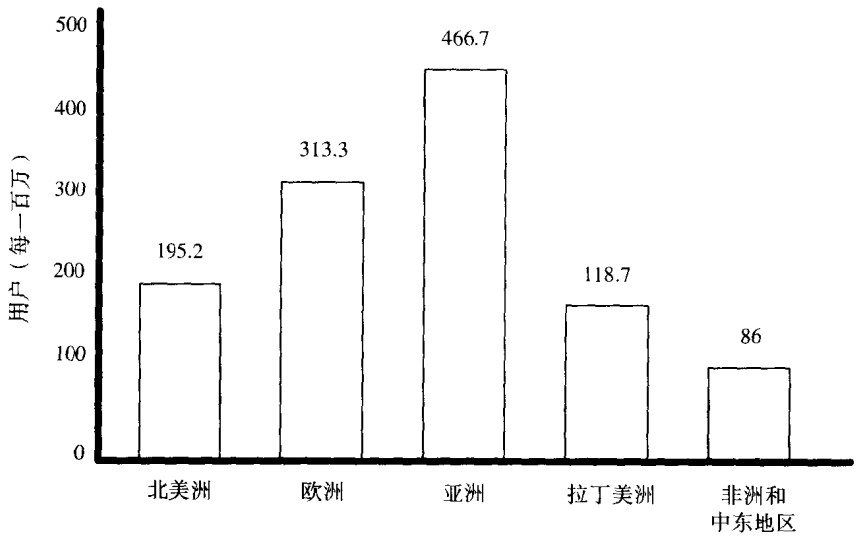
在回顾无线通信网络技术的同时，我们很有必要花一定的时间来关注反映无线通信网络的

数据变化趋势及其使用情况的数字统计。下面的这幅图反映了一些非常有趣的东西。

现在开始有一种非常明显的发展趋势，就是支持网络设备交叉发展将会在两年之后成为标准。虽然现在绝大多数蜂窝式无线通信网络传输的主要都是语音，但据估计到2003年末，蜂窝式无线通信网络将有大约35%到40%的通信量会是数据。

- 在2005年之前，有50%财富排在前100名的公司将部署无线局域网（0.7的可信度，信息来源：Gartner Group）。
- 在2010年之前，绝大多数财富排在前2000名的公司将部署无线局域网（0.6的可信度，信息来源：Gartner Group）。

图1-1说明了预计在2005年无线Internet用户的数量。



（信息来源：Yankee Group）

图1-1 预计在2005年无线Internet用户的数量

1. 信息设备逐渐增多

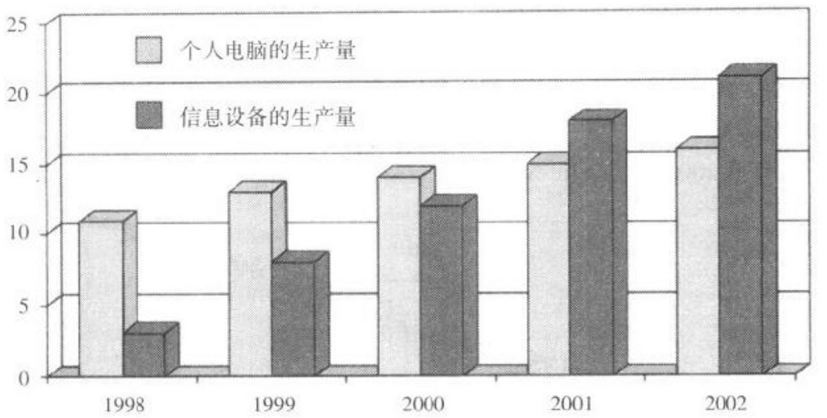
虽然用户对无线设备集成的需求是它们的主要发展动力，但是现有的信息设备（information appliance）最近有一个新的发展趋势，对无线通信行业产生了巨大的影响，并很快将成为无线数据通信的主要平台。

信息设备是指设计目标惟一的设备，要求是方便携带的、易于使用的，并提供与之功能相对应的一套具体的性能指标。现在市场上属于这种设备的有PAD、MP3播放器、电子图书和DVD播放器。今年信息设备的生产量将超过个人电脑（参看图1-2）。

在可以预见的将来，这种趋势将会一直保持着。因为不断有一些新的特征和功能集成到信息设备里，所以将会出现它们分享信息技术市场的情况。最终，只有当无线网络互连功能被完全集成到信息设备里的时候，人们才会完全认识到信息设备的作用。

当信息设备和无线网络互连集成在一起的时候，可以提供给目标用户根据需要来获得并处理信息的能力。这些信息的变化范围包括从已经可以获得的文本信息（如书和新闻）到成熟的

多媒体信息（如音频信息、视频信息和可交互的媒体文件）。使用本地（或基于代理）无线网络互连技术和蜂窝式无线网络互连技术都可以访问信息。这些信息的来源可以是像过去那样从外部资源获取，如分布在因特网（Internet）上的内容服务器和Web服务器；也可以从代理或者可访问的资源获取，如大型购物中心、机场、办公楼和其他公众场合。



（信息来源：IDC Report 1998）

图1-2　预计个人电脑和信息设备的生产量

2. 无线通信网络在大约2005年的发展状况

请你想象一个阳光明媚的早晨。现在是2005年，你正准备踏上去一个国外城市的商务路途。在你的身边，拥有一台你非常信任的和非常普通的集成了双向语音、数据、视频多媒体通信功能的PDA。

旅行社根据存储在你的PDA上的私人数字身份模块，将会为你登记旅行安排，包括你的飞机航班、汽车和在你最喜欢的酒店里预订的一个房间。现在准备工作都做好了，让我们来看看这一天你是怎么过的吧。

你拿出无线PDA调出本地的出租车服务，召唤一辆出租车，叫他来家里接你。出租车来到你家，开车把你送到机场。接着使用集成在PDA上的字迹分析软件，通过了电子支付模块的认证，从你公司的账号里支付这一趟的花费。这次支付交易在出租车、你的PDA和银行之间完成，其间要经过加密和数字签名。支付确认被记录下来，作为以后开支记账和审计评审用。

你来到为航空公司常客设立的自助式登记入口处。在你的PDA附近的无线通信网络开始处于活动状态，你需要使用PDA通过设在入口处的身份验证。于是开始建立一个加密的会话过程。入口处的显示屏上显示有你的航班信息，并提醒你在PDA上签署确认信息。通过登机检查后，会为你打印一张自贴式行李标签。你把标签贴在行李包上，并把它们放在受检行李传输带上。当你的行李被传送到墙壁后面，你的PDA会接到说明你的行李包检查通过的确认信息。当你与登记入口处的会话过程结束了之后，需要再建立一个与机场信息控制台的会话过程。从现在开始到你登上飞机这段时间里，你将可以获得关于航班时刻表的最新信息、机场通道信息、行李信息、机场结构图、住宿信息、购物信息和机场的其他服务信息。

飞机到达目的地后，你要取回行李。又一个与当地的机场信息控制台的会话过程建立起来

了。根据你的机票信息，它告诉行李现在在什么地方和取回行李的估计时间，在哪里将可以取回它们。借助于机场地图，你可以非常方便地了解本地服务信息。

你收拾好行李，跳上当地汽车租用公司的巴士。通过递交一个车辆签号，你可以预先选择你的车，并签署租用协议。接着汽车钥匙就下载到你的PDA上。为了节省时间，你可以预先配置PDA设置，让走到距离汽车还有几米的地方就自动发动汽车并打开车门。你还有一点时间，可以用PDA查阅语音和视频消息。视频消息当中附有一个很大的格式化图形文件。你可以到了酒店之后再仔细浏览这条消息。

你走到车子旁边，发动汽车，打开车门。然后放好行李，选择PDA上的酒店信息。车内的显示屏和GPS指路系统为你提供去往酒店的路径信息。你提前缴税，并把支付确认信息记录下来，以在开支记账和自动缴税时使用。开往酒店时，你可以走高速车道。当你来到高速公路收费亭时，PDA将会负责为你把提前支付的金额转账过去。

你到了酒店，把车交给酒店服务员。他们负责帮你把沉重的行李搬到房间里。在你穿过大厅的时候，PDA帮你通过预订认证，并且告诉你房间号。你想根据情况最终决定要不要住那间房间，房门的钥匙会下载到你的PDA上。当你来到那间房间的门口时，打开房门，走进房间。你检查那间房间觉得满意，然后在PDA上点击“接受房间”。

你用PDA给在那座城市的合作人打了一个视频电话，还向当地的一家饭店预订了四个人的一顿晚餐。PDA提醒你，你还有一条视频消息没有浏览。

现在你完成了所有的登记入住手续并待在你的房间里，你可以有时间阅读那条消息了。你在PDA上打开那条附有很大的格式化图形文件的视频消息，并在房里的电视机上播放它。这条消息是一些学生业余足球联赛的精彩视频片断。你的女儿攻入了制胜一球。

刚开始，你可能觉得我们这篇“一天的生活”描述了许多科幻小说里才能有的东西，但是当你学完本章的时候，就会认识到它们并不像看起来得那么牵强了。让人吃惊的是，现有的技术和标准足以把它变成现实。

让我们来看看无线通信网络技术都为我们提供怎样的发展潜力吧。

1.3 了解无线通信网络的发展前景

在此，我们也许有必要花一定的时间来快速回顾一下数据网络和电话的发展历史，以便清楚地了解到技术的发展方向。

众所周知，在刚开始的时候，计算机都是待在玻璃房里的。那个时候，这些机器更像是因为它们的技术复杂性和处理问题的能力，而不是作为有用的日常生活工具让人钦佩不已的对象。因为它们（甚至现在有一些计算机还是这样的）是人类智慧的结晶，完全弄懂它们需要付出巨大的艰辛，有时要搞懂它们涉及到的知识都非常困难，所以当时局限在只有很少的特殊的人能使用它们。

整个20世纪60年代和70年代绝大多数的时候，计算资源都放在计算中心。那个时候的计算机体积庞大，使用困难。网络刚开始出现，只有很少的协议支持数据共享。

在20世纪70年代末和80年代初，个人电脑取得了革命性的突破，计算资源的普及进入了前所未有的阶段。开发出了商业、通信和娱乐方面新的应用程序。这个时候出现了一个新的趋势：

主动把计算机技术介绍给用户，而不是把用户带到计算机面前，让他们顶礼膜拜。因为这些资源体积变得更小了，功能变得更强了，计算机预言家开始梦想着在将来，人们随时随地都可以访问到一台计算机。

事实上并不是只有计算机人才有那个梦想，在电话行业同样也有相似的渴望。用户开始需要可移动电话服务，希望电话的覆盖范围更广，可以覆盖到偏远地区，或者因为不能安装传统有线电话服务的、访问受到限制的地区。

20世纪80年代末和整个90年代，市场上开始出现了一些无线电话解决方案。在这时候，传统的电脑也开始使用有线电话服务来进行拨号上网、电子布告栏服务（Bulletin Board Services, BBS）和其他一些数据通信活动。开始出现了膝上型电脑，并且与无线通信网络结合在一起，移动计算的时代最终到来了。或者说它将要到来了。

这是一个非常困难的时期。网络标准以惊人的速度发展，以满足办公和科研用户对数据计算不断变化的需求。这个时候开发出了新的功能更强大和复杂的应用程序，它们对网络带宽的要求也不断提高；数据计算的模型由机房集中式计算模型变成了完全的分布式计算模型，适应这种变化的新的安全标准也在这个时候出现了。

这些新的标准当中很少有能够满足无线网络用户需要而被完全采纳的。只要仔细考虑了所有当时制定的数据网络标准和受当时硬件条件限制的因素，我们就会有一点困惑，就是为什么无线通信网络的数量远没有那么多呢。当时有许多便携式数据接收器和便携式电话的体积太大，提供的数据吞吐量太小，它们也因此不能成为高效的远程计算平台。

相对于当时的技术和数据通信标准，无线通信网络概念的提出显得有些过早了。要想实现拥有一个完全不受限制的网络的梦想，我们还需要等待一段时间。

那么我们现在究竟处于无线通信网络发展道路上的什么位置呢？网络互连和网络应用的标准开始相互结合，对无线通信网络比起以前来说也更友好了。为了满足无线通信网络的需要，人们制定了一些特殊的标准。从技术的角度来讲，微电子技术上的突破使得无线通信网络器件的体积变小了，需要的能量消耗也更少了。现实生活中可以使用的无线通信网络解决方案也应运而生了，可以用于大多数的办公和家庭生活场合。

正像当初设想的那样，人们现在对无线通信网络的需求就像10年或者20年前一样，丝毫没有减少。现在的无线通信网络解决方案使得无线通信网络灵活性更强，性能更好，并且被证明像预先估计的那样，可以减少相应网络配置带来的长期的资金消耗和管理成本。

在不久的将来，无线通信网络将会用于几乎所有的场合。目前它将会被人们广泛接受，对它的信任也会不断加强。在许多情况下，集成的无线通信网络技术可以让人与人之间或者人与数据中心之间交互和相互通信，不像过去电报和莫尔斯码那样，只能单向通信。

接下来要做的比起以往通信领域中的任何进步来说，都显得更加了不起。我们要负责让这个“新朋友”能够应付所有的挑战，并提供让它发展和进步的机会，以便能够满足未来很长一段时间内人们的需要。

无线通信网络

在未来不久的几年之后，随着绝大多数地方都可以获得3G蜂窝式无线通信网络、无线局域

网、无线个人区域网和宽带无线通信网络服务，厂家将会开辟出新的应用和服务来满足商务和消费者的网络需求。

1. 无线通信网络在商务上的应用

为了在商务上使用而提供解决方案的无线通信网络应用主要有四大类：

- 办公通信。
- 客户服务。
- 遥感勘测技术。
- 领域服务。

(1) 办公通信

办公环境下的无线通信网络解决方案主要是解决了对数据中心和应用程序服务器进行远程访问的问题。在美国，由于有超过3800万的职员是在家里完成全职或兼职工作的，新的广播通信技术和端对端可交互应用程序开始变得越来越重要了。现有针对无线通信网络的一整套应用解决方案由三个要素构成：

- 移动消息机制。
- 移动办公室/企业组件。
- 远程现场技术。

移动消息机制涉及扩展内部公司消息网络环境，通过无线通信网络向远程用户提供服务。一个典型的应用是，通过使用第三方解决方案来为无线通信网络用户提供电子邮件的功能。通过使用带无线上网功能的PAD、双向寻呼机和精巧的便携式电话，用户可以随时得到他们公司电子邮件收件箱中的最新信息，以便对紧急的事件做出反应。

短消息系统（SMS，Short Message System），被用来即时地发送和接受文本形式的短消息，也是企业用户用来实时跟踪最新新闻和其他事情发展情况的有效途径。虽然这项服务最主要的是用来从文本信息媒体获得信息的，但是它也可以用来和其他用户进行双向的消息传递。

后来，因为世界各地都部署有统一的消息传递系统，这最终使得移动无线通信网络用户真正地拥有了一个远程交互的方式。多媒体功能将来会被集成进来，以满足用户对实时消息传递的需求。

在图1-3中，我们可以看到支持漫游的统一寻址方式将会带来前所未有的移动性。一旦这实现了，企业用户将拥有单联系点。通信信号将会被传送到位置固定的通信点上（无论这个通信点在哪里）。

无线企业通信解决方案集的第二个应用领域就是移动办公室和企业组件。图1-4说明了漫游着的带无线上网功能的台式计算机的概念。基于无线通信网络的移动办公室和企业组件应用通过建立一个无线通信网络连接，为远程用户提供公司内部的网络资源。这个领域中绝大多数的应用包括公司数据库服务器、应用程序服务器、信息与新闻服务器、目录服务、旅游与费用服务、文件同步、企业内部网络服务器浏览和文件传输。

基于无线通信网络的远程现场技术为提高网络之间的相互协作提供了一种途径。图1-5说明了远程现场技术的发展前景，它为远程用户提供了一个本地化位置。双向视频会议和Web广播通信都属于远程现场技术的例子。