新一代信息通信技术书系·无线通信专辑

无线通信安全技术

杨义先　钮心忻　编著

北京邮电大学出版社
·北京·

新一代信息通信技术书系
编委会

内 容 简 介

本书对无线通信各主要领域所涉及的信息网络安全问题进行了全面深入的研究和介绍。书中大部分内容为首次在同类书籍中出现。全书共 7 章，主要内容包括第二代移动通信系统安全技术、第三代移动通信系统安全技术、WAP 安全技术、TETRA 安全技术、WLAN 安全技术、电信网络攻击、手机病毒、SIM 卡攻击、移动多媒体版权管理系统等。此外，本书还系统地介绍了以加密算法、WPKI、签名和认证、密钥管理与协商、伪随机数发生器等为代表的移动通信系统核心安全基础。

本书是为无线通信领域的工程师和电信相关专业的教师和高年级学生（包括本科生和研究生）编写的实用工程书或教学参考书，希望他们通过阅读此书能够了解为其量身订制的必要的安全技术。同时，本书也可作为信息安全领域的相关人员为无线通信领域服务的业务指导书。本书还可作为通信与电子系统、信号与信息处理、密码学、信息安全等专业的本科生和研究生相关课程的教学参考书和培训教材。

图书在版编目（CIP）数据

无线通信安全技术／杨义先，钮心忻编著．—北京：北京邮电大学出版社，2005
ISBN 7-5635-1046-X

Ⅰ．无… Ⅱ．①杨… ②钮… Ⅲ．无线电通信—安全技术 Ⅳ．TN92

中国版本图书馆 CIP 数据核字（2005）第 014994 号

书　　名：无线通信安全技术
编　　著：杨义先　钮心忻
责任编辑：李欣一
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号（100876）
电话传真：010-62282185（发行部）　010-62283578（FAX）
E-mail：　publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：
开　　本：787 mm×1 092 mm　1/16
印　　张：22.25
字　　数：481 千字
印　　数：1—5 000 册
版　　次：2005 年 5 月第 1 版　2005 年 5 月第 1 次印刷

ISBN 7-5635-1046-X／TN·366　　定　价：36.00 元

前　言

无线通信永远是一个让预言家们难堪的领域，因为，他们的每次大胆预言都被事实证明太过保守。移动电话用户数已高达 3.2 亿（截止到 2004 年 11 月），远远超过固定电话用户数，1G、2G、2.5G、3G、Beyond 3G、4G、下一代移动通信系统等等新名词层出不穷，基于移动通信系统的各种新业务（短信、彩信、购物、上网……）日新月异；数字集群系统即将扮演移动政务（或移动警务）的主角；WLAN 大有取代有线局域网络之势，甚至更有人声称 WLAN 将与 3G 争宠；小灵通虽然饱受技术争议，但是其 6 千多万的用户不能不说是无线通信领域的一个奇迹；无论 WAP 能否迅速成为移动商务的主流，移动商务都会走在基于 PC 机的电子商务前面；随着电信网、计算机网和广播电视网“三网融合”进程的加快，无线通信肯定又会再次飞跃。总之，形式多样的无线通信已经深入到千家万户，并正在更快地占领人们工作和生活的各个方面。

无线通信的飞速发展也引来了全世界“黑客”的高度兴趣，虽然，无线通信专家们在设计每种新型无线通信系统时都采取了不少安全措施，但是，事实却常常无情地证明：在“黑客”面前，许多系统不堪一击！

先进的信息安全技术以及无线通信专家与信息安全专家的广泛交流合作是对付“黑客”的最好办法。因此，让更多的人了解为无线通信系统量身订制的信息安全技术是非常有必要的，希望本书能够在这方面起到抛砖引玉的作用。

本书共分 7 章，对无线通信领域中比较活跃的有代表性系统的安全问题进行了全面深入的研究和介绍。

第 1 章是全书安全技术的基础。虽然作者尽量简化一般信息安全书籍中已有的基础知识，但是，由于无线通信系统所涉及的知识领域太多，仍然导致本章成为了全书篇幅最长的一章。在加密算法方面，作者介绍了使用率最高的公钥密码算法 RSA（及其快速实现技术）和官方地位最高的 AES 算法（先进加密标准算法），同时，还介绍了一些新的密码算法设计思路。在公钥基础设施方面，主要从工程角度概述了 PKI 和特别适用于无线通信系统的 WPKI。椭圆曲线密码体系肯定是无线通信系统安全中不可回避的话题，但是，为了精炼篇幅，作者从签名、认证与密钥协商的角度对椭圆曲线基础、基于椭圆曲线的签密方案、移动网络数字签名、基于椭圆曲线密码的可认证密钥协商进行了介绍，希望这种

新型的视角能够既让读者了解椭圆曲线密码的实质，又能使读者体会到椭圆曲线密码的广泛应用。密钥管理与协商是确保信息安全的一个重要环节，由于过去在同类书籍中这方面的内容不多，所以，比较详细地介绍了北京邮电大学信息安全中心在该方面的成果，比如，基于证书公钥的单方签名可认证密钥协商、基于身份公钥的可认证密钥协商、基于自证明公钥的可认证密钥协商等。以伪随机数发生器为基础的序列密码是一种速度快、对存储和计算资源要求低的密码手段，因此，它在存储和计算能力均有限的无线通信终端中将大有作为。这一章主要介绍了一些有代表性的伪随机序列发生器、高速伪随机数发生器、动态并行反馈移位寄存器的实现、伪随机比特发生器等。

第 2 章专注于以 GSM 和 IS-41 为代表的第二代和以 GPRS 为代表的 2.5 代移动通信系统的安全技术。GSM 是用户数最多的现实移动通信网络，这一章简要介绍了 GSM 网络的体系结构，指出了 GSM 的主要安全目标是防止未授权接入、防止假冒用户和保护用户隐私。GSM 已经引入的安全功能包括通过个性化的 SIM 卡和 PIN 码实现访问控制、通过对用户的身份认证和会话密钥来防止非授权接入、通过加密来保护无线链路的信息传输、在无线链路上隐藏用户的身份等。由于 GSM 网络的单向鉴权等缺陷使得它遭受了身份认证攻击、SIM 卡克隆、A5 算法破译、信令网络攻击等一系列网络攻击，这一章在介绍了这些攻击之后，提出了对 GSM 安全协议的改进措施。这一章在介绍 GPRS 系统的安全技术方面比较简单，因为，许多内容都可以借鉴 GSM 系统的相关介绍。关于 IS-41 的安全体系，此章介绍了相关的信任模式和认证场合，IS-41 的接入安全机制与 GSM 相似，因此，只介绍了其中的密钥管理、认证（全局质询/应答认证和惟一质询/应答认证）和保密机制（语音加密、信令加密、用户数据加密）。此章还分析了 IS-41 在接入安全机制方面的漏洞（接入认证漏洞、惟一质询/应答认证漏洞、A-Key 泄漏等），并对其接入安全进行了综合评价。此章还对 GSM 和 IS-41 的接入安全进行了多方比较，提出了一些安全性机制的建议。这一章还有一个重要内容，那就是对 COMP128 算法的详细安全分析，包括中间相遇攻击、半碰撞攻击、旁路攻击、电源分析攻击等，接着介绍了增强 COMP128 算法安全性的办法，比如，密钥筛选、限制 SIM 卡的鉴权次数、攻击性输入检测、鉴权频率检测、行为特征检测等。

第 3 章集中介绍第三代移动通信系统的安全技术。3G 虽然还未大规模使用，但是，由于它不但能够提供传统的语音业务，还将提供多媒体业务、数据业务以及电子商务、电子贸易、互联网服务等多种信息服务，因此，如何在 3G 系统中保证业务信息的安全性以及网络资源使用的安全性已成为 3G 系统中重要而迫切的问题。这一章首先从 3G 的业务分类、业务特征、业务管理、业务实现等方面对 3G 的新业务进行了详细的归纳总结，并介绍了包括业务与用户发展概况、WCDMA 商用情况、CDMA2000 的商用情况以及基于智能卡的 3G 业务开发等方面的现实情况和未来趋势。关于 WCDM 的接入安全，这一章从安全模型、安全原则、安全功能结构、安全目标、安全特征这几个方面介绍了 WCDMA

的接入安全内容。这一章介绍的 WCDMA 网络安全机制包括认证与密钥协商 (认证向量分发、KASUMI 算法)、无线链路数据加密、空中接口数据完整性保护、身份保密等 ;还描述了由加密密钥和完整性密钥设置、加密和完整性模式协商、加密密钥和完整性密钥寿命、加密密钥和完整性密钥识别、安全模式建立等组成的安全链接建立过程 ;为了增强 WCDMA 认证算法的安全性,介绍了一种基于哈希链机制的新型认证与密钥协商机制,该机制的实现简单灵活,能够实现强双向认证和密钥协商,并且具有抗抵赖性。关于 CDMA2000的接入安全,这一章首先简要介绍了 CDMA2000 系统的接入安全内容,接着从无线接入安全和分组网接入安全两个角度介绍了 CDMA2000 的安全特征,通过详细分析采用 OTASP 协商 A-Key 的过程,以及在 CDMA2000 系统中 A-Key 的不同计算方法,研究了该机制的安全性,并提出了可能的改进措施。另外,这一章还从密钥管理、主密钥更新、认证机制、加密算法、完整性算法、分组接入安全等安全机制出发比较了 WCDMA 和 CDMA2000 的接入安全机制,并对 Beyond3G/4G 可能遇到的安全威胁和安全机制进行了预测。3G 系统的安全性比 2G 系统完善还体现在核心网系统中,在 2G 系统中没有考虑核心网的安全威胁。为了介绍核心网中 MAP 协议的安全保护,这一章介绍了 MAPSec 协议的网络模型、MAPSec 提供的安全服务及保护模式、MAPSec 协议的消息流程。为了介绍核心网中 IP 网络层安全,这一章介绍了相关的安全模型、IP 域安全密钥管理、基于 SEG 的 IP 域安全扩展等内容。核心网中的安全认证架构既可以是基于对称密钥的认证框架,又可以是基于 PKI 和 CA 的认证框架。

第 4 章介绍 WAP 安全。WAP 是无线应用的协议模型,它为移动网络提供了类似 TCP/IP 那样层次化的协议支持。WAP 是在 Internet 上成熟的协议标准之上设计出来的。WAP 中涉及安全的模块共有 4 个 :WTLS、WMLSCrypto、WIM 和 WPKI。本章对 WAP 的这 4 个安全模块进行了深入的研究,比较这些安全模块和它们在 Internet 中的原型,分析它们对原型修改的原因,同时还分析了协议本身及其实现和应用方面存在的安全问题 ;最后还介绍了 MeT 框架,它是 WAP 安全模块集中应用的体现。具体地说,关于 WTLS,这一章介绍了它在 Internet 中的原型——TLS 协议,在此基础上列举了它们对于这些原型所做的主要更改,并对这些更改的原因进行了分析 ;同时还分析了 WTLS 实现的一些问题和 WTLS 协议和应用模型存在的一些问题,对于 WTLS 中密钥刷新机制存在的缺陷给出了改进的方法。关于 WMLSCrypto,这一章介绍了它在 Internet 中的原型——JavaScript 中的 Crypto 对象,然后引出 WMLSCrypto 及其应用和发展。关于 WIM,这一章介绍了它在 Internet 中的原型——PKCS # 15,在此基础上介绍 WIM,并提出了 WIM 在 WTLS、WMLSCrypto 和 WPKI 中的应用方式及优点。

第 5 章研究 TETRA 系统的安全技术。标准 TETRA 系统提供的安全措施有空中接口加密、支持用户与网络的双向鉴权。但是标准 TETRA 系统提供的加密功能仅仅局限于空中接口,没有延伸到核心网,并且没有进行消息完整性保护,所以,用户数据在系统内

部仍然是以明文方式传输的。对于那些需要高可靠、高保密、高安全信息传输的高端用户,就需要对标准的 TETRA 系统进行安全改造。在 TETRA 数字集群系统鉴权及空中接口加密方面,这一章系统地分析了 TETRA 系统鉴权的流程,并给出了鉴权算法设计要求和密钥分配、更换方法;详细分析了 TETRA 系统鉴权的安全性,包括协议安全、算法安全和密钥管理安全 3 个方面;分析了 TETRA 系统鉴权的优越性,指出了系统的安全漏洞及危险,并针对安全漏洞给出了改进方法。在 TETRA 数字集群系统的端到端加密研究方面,对 TETRA 系统的端到端保密通信进行了全面分析和设计,提出了在移动通信环境下群组保密通信的密钥分配方案,该方案采用短数据服务 OTAK 消息分发的两级密钥管理方式,该方案可减少信道占用,增加密钥管理效率。针对 OTAK 数据的破坏、修改、重放等攻击以及无线传输过程引起的误码,这一章提出了在 OTAK 消息中加入校验和、序列号、时间戳及带外加载密钥管理中心的 ITSI 等措施;还给出了利用终端所持有的通信密钥进行端到端的语音及短数据保密通信的设计,并给出安全性分析及性能分析;在 TETRA系统的密钥管理中心(KMC)方面,详细分析了 KMC 中的密钥管理流程。根据流程分析,对 KMC 进行总体设计以及功能模块划分,采用消息驱动机制和多线程技术来实现 KMC 系统的各个模块。

第 6 章讨论了 WLAN 安全技术。在此首先描述了 WLAN 的安全机制,包括 802.11 标准规定的安全机制、改进的 WLAN 安全机制(WPA/802.11i/WAPI 等),接着分析了 802.11 标准中安全机制的缺陷,着重考虑了 WEP 算法的安全性,然后介绍了针对上述安全机制缺陷所存在的攻击方法,并提出了改进 WLAN 安全性的一些建议,还介绍了 IPSec 的体系结构和应用领域,阐述了一个基于 IPSec 的 WLAN 安全系统的设计方案,详细讨论了该系统的两个核心功能模块的实现,并对该系统的安全性和性能进行分析,提出了下一步的研究方向。这一章将有线网络中的安全机制应用到无线局域网领域,并结合无线局域网已有的安全机制来提高 WLAN 的安全性。基于 IPSec 的 WLAN 安全技术与已有的 WLAN 的物理层和链路层安全机制无缝连接,对于保证敏感数据的安全性是很有意义的。这一章还介绍了 WLAN 与 3G 互通的安全保护,针对 WLAN 与 3G 互通场景中的一种,分析了基于 802.1x、EAP 协议和 3G AKA 的用户认证机制;最后,以安全嵌入式系统为平台,基于现有的安全协议和密码算法,提出了可行的安全策略。

第 7 章介绍了无线通信系统面临的多种新挑战,所涉及的面较广,但是都比较初浅,希望本这一章内容能引发出许多后继工作。固定电话网中的许多安全问题(包括针对用户终端设备的攻击、针对交换设备的攻击、针对电信数据库的攻击、针对网管系统的攻击、针对信令系统的攻击、针对传输设备的攻击等)肯定会很快在无线通信系统中得到反映。这一章介绍了包括用户终端拒绝服务攻击和交换设备拒绝服务攻击在内的电信网络拒绝服务攻击。手机病毒是无线通信领域中出现的一个值得特别关注的新动向,这一章在介绍了手机操作系统的简况之后,对现行手机的主流病毒进行了一一介绍,包括短信类手机

病毒、炸弹类手机病毒、蠕虫类手机病毒、木马类手机病毒等。SIM 卡攻击对手机造成的威胁非常大,在该方面,这一章介绍了针对手机漏洞的短消息攻击、针对 SIM 卡短消息协议处理漏洞的攻击、利用短消息网站漏洞的拒绝服务攻击、直接拒绝服务攻击、SIM 卡旁路攻击、伪装手机实施 SIM 卡攻击、伪装基站实施 SIM 卡攻击等。以彩信为代表的移动多媒体版权保护是无线通信面临的另一个必须尽快解决的实际问题,这一章最后介绍了基于数字水印技术的版权管理系统,包括数字内容版权的注册封装、数字内容的下载、数字内容的正常转发、数字内容破坏后的转发以及实时性考虑等。另外,这一章还从密钥分配和管理、算法管理两方面对基于数字水印技术的版权保护系统的安全性进行了分析。

无线通信领域中还有许多系统都需要个性化的信息安全技术,但是,限于篇幅和作者能力,不可能在一本书中全部介绍清楚。比如,后起之秀的小灵通确实给普通百姓带来了经济实惠的无线通信手段,但是,从安全角度看,小灵通就完美无缺吗?数量急剧增长的小灵通用户的通信安全问题肯定值得深入研究。

在封闭环境下,无线通信中传统的信令系统和信号系统也许还比较安全,但是,以 VOIP 为代表的新型通信系统打通了电信网与计算机网络之间的连接后,无线通信系统还能经受得住来自计算机网络的强力攻击吗?如何采取有效的预防措施?特别是今后"三网"融合变为现实之后,包括无线通信网络在内的通信网络必须进行全面改造升级,否则,安全问题造成的后果将不堪设想。

由于缺乏必要的资料并且担心作者的权威性不够,本书至少还留有两个遗憾:其一是对我国自己的 3G 标准 TD-SCDMA 的安全技术几乎未作介绍;其二是对我国自己的 WLAN 安全协议 WAPI 研究不够深入。希望有更权威的作者能够弥补我们的这两个缺陷。

在本书的写作过程中,我们一方面注意密切结合我国无线通信的当前具体情况,另一方面也尽量体现国际上的最新动态。本书的各章(甚至各节)都尽量相对独立,以适应各种需求之读者自由组合并阅读相关章节。比如,信息安全专业或无线通信专业的研究生(包括博士生)或高年级本科生可以从头到尾认真阅读此书的全部内容,这样可以使他们对无线通信系统中的信息安全技术有一个比较全面系统的认识,为今后的进一步深造打下基础;需要撰写学位论文的研究生(包括博士生)可以重点参考第 7 章,也许无线通信领域"攻防战"的新进展有助于激发您的创新灵感。

信息安全专家可以忽略第 1 章,而全面浏览其他章节,并根据自己的具体情况锁定目标,为无线通信的某个(或某几个)系统保驾护航。如果有很多信息安全专家全面深入地参与到无线通信系统的设计、建设和维护全过程之中,那么,无线通信领域的安全状态将大为改善。

无线通信专家在阅读完第 1 章之后,可以独立阅读其他任何一章,直接进入自己的兴趣领域。不过,我们建议每位无线通信专家都密切关注第 7 章的内容,因为,无线通信领域正在出现或即将出现的各种新挑战确实值得广泛了解并群策群力想办法避免新的安全

威胁造成重大损失。

希望本书所列的详细章节目录和参考书籍有助于读者迅速了解每一章节的主题，并据此迅速找到自己关心且希望深入研究的内容。如果我们的这些努力能够提高读者的阅读效率，帮助那些有特殊兴趣的读者直接进入自己的专业领域并了解国际上的相关最新动态，那么我们就心满意足了。

本书是北京邮电大学信息安全中心全体成员多年来集体智慧的结晶。在本书写作过程中张文硕士、秦晋硕士、赵义斌硕士、曹华平硕士、傅华硕士、邱志聪硕士、王飞硕士、肖彬硕士、杨轩硕士、邹昊硕士、范晓晖硕士、朱振荣博士、李志江博士、孙宏博士、隋爱芬博士、郭代飞博士、李作为博士、吕慧勤博士、戴元军博士、单广玉博士等为本书提供了丰富的资料，并与作者合作完成了相应的章节（见每章的致谢部分）。特别感谢胡正名教授、罗群教授、李中献副教授、徐国爱副教授、夏光升博士、张振涛博士、李新博士、张茹博士、崔宝江博士、李剑博士、周亚建博士后。他们同心协力，率领北京邮电大学信息安全中心两百余位研究人员在网络信息安全研究领域的丰富成果是本书的营养源泉。本书也是国家“973”项目（编号：G1999035804）和国家自然科学基金项目（批准号：90204017，60372094，60473016）、北京市自然科学基金项目（4042022）成果的总结。

由于作者水平有限，书中难免出现各种失误和不当之处，欢迎大家批评指正。

作　者

2005 年 2 月

序

信息通信日新月异，无线技术前景无限。

为了尽快适应飞速发展的无线通信的需求，北京邮电大学出版社在 2004 年特别组织有关专家撰写了“新一代信息通信技术书系·无线通信专辑”，在这一专辑中为广大专业读者提供了近 10 本图书。在内容上，这些书大致可以分为两大类型：物理层技术与网络层技术。其中：

在物理层技术中，本专辑汇集了“移动通信中多媒体业务基础”、“无线通信中的先进 DSP 技术”等内容，同时还涉及以空域为主体的比较前沿的新技术“智能天线技术”、“无线通信中的多天线技术”。

在网络层技术中，则除了包含“移动通信中的资源管理”、“宽带移动互联网”等内容外，本专辑还包含更为前沿的新技术“无线网络中的信息安全”、“无线重构技术”和“异构网的业务综合”等。

以上内容将分别成书，陆续出版提供给广大的读者，同时，也殷切希望广大读者对本专辑的编写提出宝贵的意见，并提出新的需求，以便我们能进一步充实和改进，为读者提供更好的服务。

2005 年 3 月于北京邮电大学信息学院

总　　序

21 世纪是经济全球化、全球信息化的崭新世纪。

信息化要靠信息系统的支持，通信则是信息系统的核心和桥梁。离开了通信来谈信息化是不可能的。今天，人们越来越倾向于以更为广义的信息通信的丰富内涵来替代相对狭义的通信的概念。

信息通信发展的目标是要实现无论何人在何时何地都能与另一用户（包括网站）进行用各种媒体表达的高质量的信息传输，实现各种信息服务。信息通信是一个巨系统，凡是人类活动之所及都能找到它的踪迹。信息通信同时又是一个整体，任何一种通信方式和通信技术都不可能孤立地存在、单独地发挥作用，各种通信方式和技术只有互相协同、配合和支撑才能构成一个完整的通信过程。当代信息通信系统还有一个特点是与计算机相互交融、相伴相随、密不可分。自 20 世纪以来，计算机与集成电子技术得到了飞速发展，与此相应，信息通信技术也呈现日新月异的发展态势。摩尔定律在信息通信领域同样显示出它的规律。

信息通信既是一个巨大的概念，又是一个巨大的系统，同时还是发展迅速、变幻莫测的领域。我们不敢奢望用一两本书的有限容量来展示它的全貌和魅力。显然，在世纪之初全面地回顾、盘点信息通信技术在近年的发展和现状，展望和评述它的趋势和变化，无疑是有意义的和必要的。基于此，北京邮电大学出版社聘请业界的著名专家、学者组成阵容强大的编委会，全面、深入、系统地分析并探讨当今信息通信最新技术的发展和未来发展的走向，条分缕析，精挑细选，决定策划出版一套反映信息通信技术最新发展及其热点的图书，并向信息通信领域的知名专家组稿。在经过周密而细致地论证、研讨，并得到方方面面的热情支持和鼎立相助之后，初步形成了现在由 4～5 个专辑组成的“新一代信息通信技术书系”。

由于覆盖面宽、内容庞大，该书系按技术基础和应用相近的原则划分为不

同的专辑，基本涵盖了当今信息通信技术发展的大部分前沿领域。每一专辑只介绍信息通信领域中的一种技术门类，包括原理综述，技术进展的评介和作者自己的工作成果。由于该书系的作者都是信息通信领域的知名学者和领军人物，他们撰写的内容无疑具有权威性和前瞻性，相信会得到广大读者的欢迎，并产生积极意义和影响。

在写作方式和篇幅上，书系不追求系统、严格和完善的理论分析，不追求大而无当的鸿篇巨制，而坚持立足于对相关技术的原理阐述、应用开发、趋势评介和引导等原则，尽可能做到深入浅出、规模适当，因此特别适合大多数信息通信和相关领域工程师及高等院校的教师学生以及从业人员阅读和参考。

本书系从一开始就得到许多领导和专家学者的热情支持和帮助，在此一并表示深切的感谢！

信息通信技术的发展变化极快，本书系虽尽可能顾及方方面面，但仍有一些内容没能被纳入，我们会不断地充实，在今后的一段时间内努力完善这一书系。另外，书系中的每一本书也会受种种条件的限制，在内容和行文中可能存在欠缺，对技术发展的评价也会因人而异，我们也并不追求一致。本书系虽经编委会、所有作者和编辑出版者的努力，但疏漏和错误在所难免，我们恳请读者的批评和建议，希望能把这一有意义的工作做得更好！

于 2005 年新春

目　　录