

<<移动互联网之智能终端安全揭秘>>

图书基本信息

书名：<<移动互联网之智能终端安全揭秘>>

13位ISBN编号：9787121148422

10位ISBN编号：7121148420

出版时间：2012-1

出版时间：电子工业出版社

作者：黄晓庆,王梓

页数：356

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<移动互联网之智能终端安全揭秘>>

### 内容概要

本书全面介绍移动互联网中的智能终端安全，涵盖目前主流操作系统，如iOS、Android、Windows Phone

7、MeeGo、Symbian、BlackBerry等，内容包括终端安全的风、现状以及解决思路等，同时阐述了智能终端安全的应对之道。

SIM卡是终端的重要组成部分，本书对SIM卡以及与SIM卡安全息息相关的接入网安全也进行了详细介绍。

本书中讲述的PC终端的安全解决思路对移动终端安全具有借鉴意义。

## 作者简介

王梓，就职于中国移动通信研究院。  
长期从事终端安全、智能卡安全、网络安全等方面的工作。

黄晓庆，现任中国移动通信研究院院长，在信息通信业拥有超过25年的从业经验，在信息通信各个领域都具有丰富的经验和独到的见解，是技术创新的倡导者和践行者。  
带领中国移动研发团队在国际标准化、科技创新、终端平台开放、基础网络架构、融合新业务等方面引领了行业发展。  
发起设立了“中国移动创新系列丛书”出版项目。

书籍目录

- 第1章 密码学和证书基础知识
- 第2章 终端和网络演进趋势
- 第3章 PC终端安全简介
- 第4章 PC终端安全架构
- 第5章 PC终端防御手段
- 第6章 移动终端安全简介
- 第7章 移动终端操作系统安全之Windows Mobile
- 第8章 移动终端操作系统安全之Windows Phone 7
- 第9章 移动终端操作系统安全之Android
- 第10章 移动终端操作系统安全之Symbian
- 第11章 移动终端操作系统安全之MeeGo
- 第12章 移动终端操作系统安全之BlackBerry
- 第13章 移动终端操作系统安全之iOS
- 第14章 移动终端安全解决思路
- 第15章 虚拟化
- 第16章 移动可信计算
- 第17章 SIM卡
- 第18章 移动通信网接入安全
- 参考文献

## 章节摘录

版权页：插图：本书的内容涉及一些密码学相关的知识，因此，本章对密码学的相关知识进行简单介绍。

密码学是对存储和传送的信息加以隐藏和保护的技术。

密码学要做的事情主要就是加密和解密信息，使得授权人员以外的人无法读取信息。

被隐秘的消息称为明文，明文经过加密变换成为另一种隐秘的形式，称为密文。

对明文进行加密操作时所采用的一组规则称为加密算法，对密文进行解密操作时所采用的一组规则称为解密算法。

加密算法和解密算法都依赖于一组秘密参数，分别称为加密密钥和解密密钥。

加密算法和解密算法统称为密码算法。

密码算法可以根据密钥的特点分为对称密码算法和非对称密码算法。

对称密码算法又称为单钥或私钥密码算法，非对称密码算法也称为双钥或公钥密码算法。

在消息传输或处理系统中，除了合法的用户以外，还存在通过各种方法窃取机密信息的攻击者，他们通过分析已经得到的算法信息和截获信息，推断出密钥或明文，这一过程称为密码分析。

所谓密码是不安全的，是指如果攻击者通过一定明文和密文信息能够获得密钥信息。

## <<移动互联网之智能终端安全揭秘>>

### 媒体关注与评论

该书顺应了移动互联网和智能手机的发展热潮，从硬件到网络，终端到系统，全面介绍了各个方面的安全规范和防护措施，快速建立起对移动互联网安全的全貌概览。

尤其难得的是针对各个主流的智能机操作系统，本书都做了深入浅出的讲解，这对于活跃在不同平台的开发者来说，更加具有现实的参考价值。

——周鸿祎该书系统地介绍了终端面临的风险以及应对措施。

难能可贵的是，作者介绍了主流移动操作系统Windows Mobile、Android、iPhone、Symbian、MeeGo、BlackBerry以及WindowsPhone7的安全机制，从系统层面分析了操作系统的安全性，大大提高了本书的指导性和实用性。

——黄晓庆

<<移动互联网之智能终端安全揭秘>>

编辑推荐

《移动互联网之智能终端安全揭秘》深度揭秘主流移动操作系统安全：深度挖掘SIM卡和接入网安全：深度分析终端安全应对措施。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>