

<<移动应用安全>>

图书基本信息

书名：<<移动应用安全>>

13位ISBN编号：9787121154409

10位ISBN编号：7121154404

出版时间：2012-2

出版时间：电子工业出版社

作者：（美）德维威迪，（美）克拉克，（美）蒂尔 著，李祥军，罗熊 译

页数：344

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>

<<移动应用安全>>

内容概要

移动应用不仅仅是下一波技术浪潮，在不远的将来对于很多关键活动而言，它将成为默认的计算方式，如E-mail、在线购物、游戏甚至娱乐等。

本书介绍了手机、PDA等移动设备面临的主要安全挑战以及一些移动应用安全开发中的技巧。

以Android、iPhone、Windows

Mobile、BlackBerry以及Symbian等操作系统为例，详细阐述了这些系统的安全功能以及如何利用这些功能来开发安全的移动应用，如防护缓冲区溢出、SQL注入攻击以及部署私钥与公钥密码技术等。

针对当前的热点应用，本书还介绍了WAP、蓝牙、SMS、MMS、移动地理定位等移动应用面临的安全威胁、自身存在的安全不足以及由此带来的安全风险，并介绍了针对移动平台的企业安全问题，以及不同系统的安全措施和安全防护手段。

<<移动应用安全>>

书籍目录

第1部分 移动平台

第1章 移动应用主要问题及开发策略

- 1.1 移动终端面临的主要问题
 - 1.1.1 物理安全
 - 1.1.2 数据存储安全（磁盘）
 - 1.1.3 应用有限的键盘实现强认证
 - 1.1.4 支持多用户的安全
 - 1.1.5 安全浏览环境
 - 1.1.6 加固操作系统
 - 1.1.7 应用隔离
 - 1.1.8 信息泄露
 - 1.1.9 病毒、蠕虫、后门、间谍软件和恶意软件
 - 1.1.10 艰难的补丁更新/升级过程
 - 1.1.11 严格使用和实施SSL
 - 1.1.12 钓鱼攻击
 - 1.1.13 跨站请求伪造（Cross-Site Request Forgery，CSRF）
 - 1.1.14 位置隐私/安全
 - 1.1.15 不安全的设备驱动
 - 1.1.16 多因素认证
- 1.2 移动应用安全开发中的技巧
 - 1.2.1 应用TLS/SSL
 - 1.2.2 遵循安全编程实践
 - 1.2.3 对输入进行验证
 - 1.2.4 应用OS提供的控制模型
 - 1.2.5 应用系统访问的最小权限模型
 - 1.2.6 恰当地存储敏感信息
 - 1.2.7 对应用代码进行签名
 - 1.2.8 设计安全和健壮的升级过程
 - 1.2.9 理解移动浏览器的安全功能和局限性
 - 1.2.10 清除非威胁因素
 - 1.2.11 应用安全/直观的移动URL
- 1.3 小结

第2章 Android平台安全

- 2.1 Android开发和调试
- 2.2 Android安全的IPC机制
 - 2.2.1 活动（Activity）
 - 2.2.2 广播（Broadcast）
 - 2.2.3 服务（Service）
 - 2.2.4 内容提供者（ContentProvider）
 - 2.2.5 Binder
- 2.3 Android安全模型
- 2.4 Android控制模型小结
- 2.5 创建新的Manifest权限控制文件
- 2.6 Intent
 - 2.6.1 Intent概述

<<移动应用安全>>

- 2.6.2 IntentFilter
- 2.7 Activity
- 2.8 Broadcast
 - 2.8.1 接收广播Intent
 - 2.8.2 安全地发送广播Intent
 - 2.8.3 Sticky Broadcast
- 2.9 Service
- 2.10 ContentProvider
- 2.11 避免SQL注入
- 2.12 Intent Reflection
- 2.13 文件和优先选项
- 2.14 大容量存储
- 2.15 Binder接口
 - 2.15.1 调用者权限或者身份检查实现安全
 - 2.15.2 Binder引用安全
- 2.16 Android 安全工具
 - 2.16.1 Manifest浏览器
 - 2.16.2 Package Play
 - 2.16.3 Intent Sniffer
 - 2.16.4 Intent Fuzzer
- 2.17 小结

第3章 iPhone平台安全

- 3.1 历史
 - 3.1.1 iPhone和OS X
 - 3.1.2 “越狱”与“反越狱”
 - 3.1.3 iPhone SDK
 - 3.1.4 未来发展
- 3.2 开发
 - 3.2.1 反编译和反汇编
 - 3.2.2 避免逆向工程
- 3.3 安全测试
 - 3.3.1 缓冲区溢出
 - 3.3.2 整数溢出
 - 3.3.3 格式化字符串攻击
 - 3.3.4 双重释放 (Double-Free)
 - 3.3.5 静态分析
- 3.4 应用程序格式
 - 3.4.1 编译和打包
 - 3.4.2 分发：Apple Store
 - 3.4.3 代码签名
 - 3.4.4 执行未经签名的代码
- 3.5 权限及用户控制
 - 3.5.1 沙箱
 - 3.5.2 Exploit Mitigation
 - 3.5.3 权限
- 3.6 本地数据存储：文件、权限和加密
 - 3.6.1 SQLite 存储

<<移动应用安全>>

- 3.6.2 iPhone Keychain存储
- 3.6.3 共享Keychain存储
- 3.6.4 向证书存储中添加证书
- 3.6.5 获取Entropy 2
- 3.7 网络
 - 3.7.1 URL装载API
 - 3.7.2 NSStream
 - 3.7.3 P2P
- 3.8 push 通知，复制/粘贴以及其他IPC
 - 3.8.1 push通知
 - 3.8.2 UIPasteboard
- 3.9 小结

第4章 Windows Mobile的安全性

- 4.1 平台介绍
 - 4.1.1 与Windows CE的关系
 - 4.1.2 设备结构
 - 4.1.3 设备存储
- 4.2 内核构架
 - 4.2.1 内存管理
 - 4.2.2 Windows CE进程
 - 4.2.3 服务
 - 4.2.4 对象
 - 4.2.5 内核模式和用户模式
- 4.3 开发及安全测试
 - 4.3.1 编码环境和SDK
 - 4.3.2 模拟器
 - 4.3.3 调试
 - 4.3.4 反汇编
 - 4.3.5 代码安全
 - 4.3.6 应用程序打包和分发
- 4.4 权限与用户控制
 - 4.4.1 特权模式和普通模式
 - 4.4.2 验证码、签名和证书
 - 4.4.3 运行中的应用程序
 - 4.4.4 锁定设备
 - 4.4.5 管理设备安全策略
- 4.5 本地数据存储
 - 4.5.1 文件和权限
 - 4.5.2 设备失窃保护
 - 4.5.3 结构化存储
 - 4.5.4 加密和设备安全存储
- 4.6 组网
 - 4.6.1 连接管理器
 - 4.6.2 WinSock
 - 4.6.3 红外线
 - 4.6.4 蓝牙
 - 4.6.5 HTTP和SSL

<<移动应用安全>>

4.7 小结 2

第5章 黑莓手机的安全性

5.1 平台简介

5.1.1 黑莓企业服务器 (BES)

5.1.2 黑莓的互联网服务 (BIS)

5.2 设备和操作系统结构

5.3 开发及安全测试

5.3.1 编码环境

5.3.2 模拟器

5.3.3 调试

5.3.4 反汇编

5.3.5 代码安全

5.3.6 应用程序打包和分发

5.4 权限与用户控制

5.4.1 RIM的可控API

5.4.2 运营商和MIDlet签名

5.4.3 对MIDP应用程序中的权限错误的处理

5.4.4 锁定设备

5.4.5 应用程序权限管理

5.5 本地数据存储

5.5.1 文件和权限

5.5.2 可编程文件系统访问

5.5.3 结构化存储

5.5.4 加密和设备安全存储

5.6 组网

5.6.1 设备防火墙

5.6.2 SSL和WTLS

5.7 小结

第6章 Java移动版的安全性

6.1 标准开发

6.2 配置、profile和JSR

6.2.1 配置

6.2.2 profile

6.2.3 可选包

6.3 开发和安全测试

6.3.1 配置开发环境并安装新平台

6.3.2 模拟器

6.3.3 逆向工程和调试

6.3.4 代码安全

6.3.5 应用程序打包和分发

6.4 权限和用户控件

6.4.1 数据访问

6.5 小结

第7章 塞班系统 (SymbianOS) 安全性

7.1 平台介绍

7.1.1 设备架构

7.1.2 设备存储器

<<移动应用安全>>

7.2 开发和安全测试

7.2.1 开发环境

7.2.2 软件开发工具

7.2.3 模拟器

7.2.4 调试

7.2.5 IDA Pro

7.3 代码安全

7.3.1 Symbian C++

7.3.2 P.I.P.S和OpenC

7.4 应用程序包

7.4.1 可执行的镜像格式

7.4.2 安装包

7.4.3 签名

7.4.4 塞班签名

7.4.5 安装

7.5 权限和用户控制

7.5.1 功能概述

7.5.2 可执行映像功能

7.5.3 进程功能

7.5.4 进程间的功能

7.6 进程间通信

7.6.1 客户端/服务器会话

7.6.2 共享会话

7.6.3 共享句柄

7.7 永久的数据存储

7.7.1 文件存储

7.7.2 结构化存储

7.7.3 加密存储

7.8 小结

第8章 WebOS安全

8.1 平台简介

8.1.1 WebOS系统结构

8.1.2 模型视图控制器 (MVC)

8.1.3 stag

.....

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>