

<<无线局域网安全实务>>

图书基本信息

书名：<<无线局域网安全实务>>

13位ISBN编号：9787115137982

10位ISBN编号：7115137986

出版时间：2006-2

出版时间：第1版(2006年2月1日)

作者：乔恩·爱德尼

页数：290

字数：462000

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>

<<无线局域网安全实务>>

内容概要

本书详细介绍了Wi-Fi无线局域网安全的基本原理、安全加密的必要性、WPA与802.11i等安全机制的实现方案，论述了TKIP和CCMP等关键的无线局域网安全技术，给出了在制定正确的安全加密决策时所有必要的信息。

本书内容详尽，又不局限于细枝末节，特别适合于无线局域网的产品设计师、网络管理员和即将使用WLAN的家庭用户阅读，也可供那些对无线网络感兴趣的读者参考。

<<无线局域网安全实务>>

作者简介

乔恩·爱德尼是无线网络领域的专家并对IEEE 802.11网络系统的研究与开发作出了突出的贡献。他作为SYMBIONICS NETWORKS公司的技术顾问，率先完成了低成本的IEEE 802.11网络系统的设计。

1996年乔恩·爱德尼作为合伙人成立了世界上首家旨在开发WLAN接入点的INTALK公司。在该公司被诺基亚收购以后，乔恩·爱德尼便专注于WI-FI在公共接入网中的应用。乔恩·爱德尼也是IEEE 802.11网络安全标准工作组的主要成员。

<<无线局域网安全实务>>

书籍目录

- 第一篇 网络安全的基本知识第1章 引言 31.1 背景介绍 31.2 如何阅读本书 41.3 本书说明
- 5第2章 安全性原则 62.1 什么是安全性？
- 62.2 良好的安全性考虑 62.2.1 不要和任何不认识的人交谈 72.2.2 没有担保就不接受任何东西
- 82.2.3 把每个人都当作敌人直到证明他不是敌人为止 92.2.4 不要永远相信你的朋友 92.2.5 使用经试验证明效果良好的方案 102.2.6 审视你应对攻击的立场 122.3 安全性术语 132.4 小结
- 14第3章 为什么Wi-Fi无线局域网容易遭受攻击？
- 153.1 改变安全模式 153.2 敌人都是什么样的？
- 153.2.1 游戏型攻击者 163.2.2 牟利或报复型攻击者 183.2.3 自负型攻击者 193.3 传统的安全架构 193.3.1 选择1：将无线局域网设置在不可信区域 213.3.2 选择2：使Wi-Fi局域网变成可信的 223.4 被动收听的危险 223.5 小结 23第4章 攻击的不同类型 244.1 攻击的分类 244.2 无需密钥的攻击 254.2.1 窃听 254.2.2 中间人攻击(篡改) 264.3 对密钥的攻击 284.3.1 一次性密码 294.3.2 隐藏密钥 294.3.3 无线攻击 304.3.4 使用强力破解攻击密钥 324.3.5 字典攻击 324.3.6 算法攻击 334.4 小结 34第二篇 Wi-Fi安全性设计第5章 IEEE 802.11 协议简介 375.1 层 375.2 无线局域网的结构 385.3 基础结构(infrastructure)模式工作原理 395.3.1 信标 405.3.2 探测 405.3.3 连接到AP 405.3.4 漫游 405.3.5 发送数据 405.4 协议细节 415.4.1 通用帧格式 415.4.2 MAC报头 415.4.3 管理帧 435.5 射频部分 455.6 小结 46第6章 IEEE 802.11 WEP的工作原理及其不足 476.1 引言 476.2 认证 486.3 私密性 506.3.1 使用RC4算法 506.3.2 初始化矢量(IV) 516.3.3 WEP密钥 526.4 WEP机理 576.4.1 分段 576.4.2 完整性校验值(ICV) 586.4.3 帧的传输预处理 586.4.4 RC4加密算法 596.5 WEP为什么不安全 616.5.1 认证 616.5.2 接入控制 636.5.3 重播防护 636.5.4 消息篡改检测 646.5.5 消息私密性 656.5.6 RC4弱密钥 676.5.7 直接密钥攻击 686.6 小结 68第7章 WPA、RSN及IEEE 802.11i 707.1 Wi-Fi与IEEE 802.11i的关系 707.2 IEEE 802.11i 717.3 WPA 717.4 RSN与WPA之间的区别 727.5 安全上下文 727.6 密钥 737.7 安全分层 747.8 标准间的关系 767.8.1 标准列表 767.8.2 图表映射 777.9 小结 78第8章 接入控制：IEEE 802.1X、EAP和RADIUS 798.1 接入控制的重要性 798.2 对拨入用户的认证 818.3 IEEE 802.1X 838.3.1 简单交换式集线器环境下的IEEE 802.1X 838.3.2 Wi-Fi无线局域网中的IEEE 802.1X 868.4 EAP原理 878.5 EAPOL 908.5.1 EAPOL-Start 908.5.2 EAPOL-Key 908.5.3 EAPOL-Packet 918.5.4 EAPOL-Logoff 918.6 IEEE 802.1X中所用的消息 918.7 实现的考虑 938.8 RADIUS 远程接入拨入用户业务 948.8.1 RADIUS工作机制 958.8.2 基于RADIUS的EAP 988.8.3 WPA和RSN中RADIUS的使用 998.9 小结 100
- 第9章 上层认证 1019.1 引言 1019.2 谁来决定采用何种认证方法？
- 1019.3 上层认证中密钥的使用 1029.3.1 对称密钥 1029.3.2 非对称密钥 1029.3.3 验证和验证权威机构 1039.4 上层认证方法详解 1049.5 传输层加密(TLS) 1059.5.1 TLS的功能 1059.5.2 握手交互 1079.5.3 TLS握手和WPA/RSN的关系 1109.5.4 在EAP中使用TLS 1119.5.5 TLS的总结 1139.6 克伯罗斯 1149.6.1 使用票证 1149.6.2 Kerberos票证 1159.6.3 获得票证授权票证 1159.6.4 服务票证 1169.6.5 跨域接入 1189.6.6 票证工作的方法 1189.6.7 在RSN中使用Kerberos 1209.7 思科Light EAP(LEAP) 1249.8 受保护的EAP协议(PEAP) 1269.8.1 第一阶段 1279.8.2 第二阶段 1279.8.3 PEAP的状况 1289.9 蜂窝电话领域的认证：EAP-SIM 1289.9.1 GSM网络中的认证概述 1299.9.2 连接GSM安全与Wi-Fi安全 1309.9.3 EAP-SIM 1309.9.4 GSM-SIM认证的现状 1329.10 小结 132第10章 WPA 和 RSN 密钥层次结构 13410.1 成对密钥和小组密钥 13410.2 成对密钥体层次结构 13510.2.1 创建和交付PMK 13510.2.2 临时密钥的计算 13610.2.3 交换和核实密钥信息 13710.2.4 结束握手 13910.3 组密钥层次结构 13910.4 采用AES-CCMP的密钥分层 14110.5 混合环境 14210.6 密钥分层小结 14210.7 WPA密钥派生细节 14310.7.1 四次握手 14510.7.2 组密钥的握手 14910.8 当前值的选择 15110.9 临时密钥的计算 15110.10 小结 154第11章 TKIP 15511.1 TKIP算法及应用背景 15511.2 TKIP概述 15611.2.1 消息的完整性 15711.2.2 IV的选择和使用 15911.3 每个数据包密钥之混合 16311.4

<<无线局域网安全实务>>

TKIP实现细节 16411.5 消息完整性 Michael 16611.5.1 反措施 16711.5.2 MIC的计算 16911.6
 每个数据包密钥之混合 17011.6.1 替换表或S盒 17111.6.2 阶段1的计算 17211.6.3 阶段2的计
 算 17311.7 小结 174第12章 AES-CCMP 17612.1 引言 17612.2 何谓AES? 17612.3 AES概述
 17812.3.1 操作模式 17812.3.2 码本模式偏移(OCB) 18112.4 在RSN中如何应用CCMP
 18212.4.1 加密传送数据的步骤 18212.4.2 CCMP头部 18312.4.3 实现总论 18412.4.4 加
 密MPDU的步骤 18512.4.5 解密MPDU 18712.5 小结 188第13章 Wi-Fi无线局域网协调: ESS
 和IBSS 18913.1 网络协调 18913.1.1 ESS与IBSS 18913.1.2 加入一个ESS网络 18913.2
 WPA/RSN信息单元 19013.3 应用IEEE 802.1X进行预认证 19113.4 IBSS Ad-hoc网 19213.5 小
 结 195第三篇 Wi-Fi实用安全精要第14章 公共无线热点 19914.1 热点的开发 19914.1.1 公共无
 线接入的定义 19914.1.2 无线接入业务的发展障碍 19914.2 公共无线接入热点的安全问题
 20114.3 如何组织热点 20214.3.1 用户设备 20214.3.2 接入点 20314.3.3 热点控制器
 20414.3.4 认证服务器 20514.4 热点的不同类型 20614.4.1 机场 20614.4.2 宾馆 20614.4.3
 咖啡店 20614.4.4 家里 20714.5 使用热点通信时如何保护自己 20714.5.1 个人防火墙软件
 20814.5.2 虚拟专用网络(VPN) 20814.6 小结 209第15章 已知的攻击: 技术回顾 21115.1 基
 本安全机理的回顾 21115.1.1 保密性 21115.1.2 完整性 21215.2 先前802.11安全机理的回顾
 21415.2.1 保密性 21415.2.2 RC4和WEP 21415.2.3 完整性和认证 21715.3 针对802.11安全机
 理的攻击 21815.3.1 保密性 21815.3.2 接入控制 22415.3.3 认证 22415.4 中间人攻击
 22515.4.1 管理帧 22515.4.2 ARP欺骗 22515.5 由中间人攻击产生的问题 22615.5.1 802.1x
 和EAP 22615.5.2 PEAP 22615.6 拒绝服务攻击 22715.6.1 针对基于Wi-Fi标准的第二层拒绝服务
 攻击 22715.6.2 WPA加密拒绝服务攻击 22815.7 小结 228第16章 实际的攻击工具 22916.1 攻
 击者的目标 22916.2 攻击过程 22916.3 案例分析 23516.3.1 策划 23516.3.2 搜集 23616.3.3
 分析 23716.3.4 执行 23816.4 其他有趣的工具 23916.4.1 Airsnort 23916.4.2 Airjack 23916.5
 小结 240第17章 公共资源实现举例 24117.1 通用架构设计指南 24117.2 保护一个已部署的网络
 24217.2.1 隔离和渠道化 24217.2.2 将设备固件升级为WPA 24217.2.3 如果不能做任何事该怎么
 办 24317.3 计划部署一个WPA网络 24417.4 部署基础设施 24417.4.1 添加支持IEEE 802.1X
 的RADIUS服务组件 24417.4.2 将公共密钥基础结构运用于客户证书中 24417.4.3 安装IEEE 802.1X
 客户端申请者软件 24517.5 基于公开软件资源计划的实际例子 24517.5.1 服务组件基础架构
 24517.5.2 建立一个公共资源接入点 25617.5.3 全部投入使用 25717.6 小结 262附录附录A
 AES的分组密码综述 265A.1 有限域运算 265A.1.1 加法 266A.1.2 减法 266A.1.3 乘法
 267A.1.4 除法 268A.1.5 Galois域 268A.1.6 结论 272A.2 AES编码过程的步骤 272A.2.1 轮
 密钥 273A.2.2 计算轮 274A.2.3 解密 276A.2.4 AES总结 276附录B 消息修改实例 278附录C
 校验下载文件的完整性 280C.1 检查MD5摘要 280C.2 检查GPG签名 280缩略语 284参考文
 献 287

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>