

<<物联网安全技术>>

图书基本信息

书名：<<物联网安全技术>>

13位ISBN编号：9787121160004

10位ISBN编号：7121160005

出版时间：2012-6

出版时间：电子工业出版社

作者：雷吉成

页数：258

字数：341000

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>

<<物联网安全技术>>

内容概要

《物联网安全技术》介绍信息安全的基础知识，概述物联网的基本概念和主要特征，分析物联网所面临的安全挑战，提出物联网安全的体系结构，同时阐述物联网安全主要的关键技术；分别从感知层安全、网络层安全、应用层安全及安全管理等方面对物联网安全进行了介绍，包括传感器网络安全、rfid安全、核心网安全、移动通信接入安全、无线接入安全、数据处理安全、数据存储安全、云安全、安全管理等，并举例说明物联网安全技术的典型应用，最后对物联网安全技术的发展趋势进行了总结。

《物联网安全技术》基本上反映了近几年来物联网安全技术的研究成果，并总结了物联网安全技术的发展趋势。

本书提供了详尽的参考文献，感兴趣的读者可以继续深入研究。

《物联网安全技术》内容丰富，覆盖面广，可作为大专院校师生和广大对物联网安全技术感兴趣的工程技术人员的参考书。

<<物联网安全技术>>

作者简介

雷吉成

研究员、政府特殊津贴获得者，ITU中国专家组成员，中国通信学会高级会员，中国电子学会高级会员，中国GPS行业协会理事，成都物联网产业联盟理事长，中国电子科技集团公司第三十研究所副所长，曾组织和领导了分组无线数据网、高速无线数据网、863无线数据接入技术、数据蜂窝通信系统、GPS / GSM系统、网络入侵检测系统等大量通信保密和信息安全网系列产品的开发、研制和工程建设。

<<物联网安全技术>>

书籍目录

第1章 信息安全概述

1.1 信息安全概念

1.2 信息安全基本属性

1.2.1 机密性

1.2.2 完整性

1.2.3 可用性

1.2.4 可认证性

1.2.5 不可否认性

1.3 信息安全威胁

1.3.1 被动攻击

1.3.2 主动攻击

1.3.3 临近攻击

1.3.4 内部人员攻击

1.3.5 分发攻击

1.4 主要的信息安全技术

1.4.1 身份管理技术

1.4.2 权限管理技术

1.4.3 本地计算环境安全防护技术

1.4.4 防火墙技术

1.4.5 基于网闸的物理隔离技术

1.4.6 网络接入控制技术

1.4.7 入侵检测技术

1.4.8 安全管理技术

1.4.9 密码技术

1.5 信息安全的发展历程

1.5.1 通信保密阶段

1.5.2 计算机安全

1.5.3 信息安全阶段

1.5.4 信息保障阶段

本章小结

问题思考

第2章 物联网安全概述

2.1 物联网简介

2.1.1 物联网的基本概念

2.1.2 物联网概念提出的背景

2.1.3 物联网相关概念及关系

2.1.4 物联网体系结构

2.1.5 物联网技术应用领域

2.2 物联网安全新特征

2.2.1 与互联网安全的关系

2.2.2 与日常生活的关系

2.2.3 物联网安全面临的挑战

2.2.4 物联网安全的特点

2.2.5 物联网安全对密码技术的需求

2.3 物联网安全威胁分析

<<物联网安全技术>>

- 2.3.1 感知层安全威胁分析
- 2.3.2 网络层安全威胁分析
- 2.3.3 应用层安全威胁分析
- 2.4 物联网安全体系结构
 - 2.4.1 感知层安全
 - 2.4.2 网络层安全
 - 2.4.3 应用层安全
- 2.5 物联网安全关键技术
 - 2.5.1 多业务、多层次数据安全传输技术
 - 2.5.2 身份认证技术
 - 2.5.3 基于多网络融合的网络安全接入技术
 - 2.5.4 网络安全防护技术
 - 2.5.5 密码技术
 - 2.5.6 分布式密钥管理技术
 - 2.5.7 分布式安全管控技术
 - 2.5.8 信息完整性保护技术
 - 2.5.9 访问控制技术
 - 2.5.10 隐私保护技术
 - 2.5.11 入侵检测技术
 - 2.5.12 病毒检测技术
 - 2.5.13 叛逆追踪技术
 - 2.5.14 应用安全技术
- 本章小结
- 问题思考
- 第3章 物联网感知层安全
 - 3.1 感知层安全概述
 - 3.2 rfid安全
 - 3.2.1 rfid安全威胁分析
 - 3.2.2 rfid安全关键问题
 - 3.2.3 rfid安全技术有关研究成果
 - 3.3 传感器网络安全
 - 3.3.1 传感器网络技术特点
 - 3.3.2 传感器网络安全威胁分析
 - 3.3.3 传感器网络安全防护主要手段
 - 3.3.4 传感器网络典型安全技术
- 本章小结
- 问题思考
- 第4章 物联网网络层安全
 - 4.1 网络层安全需求
 - 4.1.1 网络层概述
 - 4.1.2 网络层面临的安全问题
 - 4.1.3 网络层安全技术需求
 - 4.1.4 网络层安全框架
 - 4.2 物联网核心网安全
 - 4.2.1 现有核心网典型安全防护系统部署
 - 4.2.2 下一代网络 (ngn) 安全
 - 4.2.3 下一代互联网 (ngi) 的安全

<<物联网安全技术>>

- 4.2.4 网络虚拟化安全
- 4.3 移动通信接入安全
 - 4.3.1 安全接入要求
 - 4.3.2 安全接入系统部署
 - 4.3.3 移动通信物联网终端安全
- 4.4 无线接入安全技术
 - 4.4.1 无线局域网安全协议概述
 - 4.4.2 wapi安全机制
 - 4.4.3 wpa安全机制
 - 4.4.4 ieee 802.1x eap认证机制
 - 4.4.5 ieee 802.11i协议体系
 - 4.4.6 ieee 802.16d的安全机制
 - 4.4.7 ieee 802.16d存在的安全缺陷及其对策

本章小结

问题思考

第5章 物联网应用层安全

- 5.1 应用层安全需求
 - 5.1.1 应用层面临的安全问题
 - 5.1.2 面向应用层的恶意攻击方式
 - 5.1.3 应用层安全技术需求
- 5.2 处理安全
 - 5.2.1 rfid安全中间件
 - 5.2.2 服务安全
- 5.3 数据安全
 - 5.3.1 数据安全的非技术问题
 - 5.3.2 数据加密存储
 - 5.3.3 物理层数据保护
 - 5.3.4 虚拟化数据安全
 - 5.3.5 数据容灾
- 5.4 云安全技术
 - 5.4.1 云安全概述
 - 5.4.2 云计算中的访问控制与认证
 - 5.4.3 云安全关键技术
 - 5.4.4 云计算安全发展现状

本章小结

问题思考

第6章 安全管理支撑系统

- 6.1 物联网安全管理
 - 6.1.1 物联网安全管理需求分析
 - 6.1.2 物联网安全管理框架
 - 6.1.3 基于soa的安全管理系统设计
 - 6.1.4 安全态势量化及可视化
- 6.2 身份和权限管理
 - 6.2.1 统一身份管理及访问控制系统
 - 6.2.2 openid和oauth

本章小结

问题思考

<<物联网安全技术>>

第7章 物联网安全技术应用

7.1 物联网安全技术应用概述

7.2 物联网安全技术典型应用

7.2.1 物联网安全技术在校园门禁管理系统中的应用

7.2.2 贵重物品防伪应用

7.2.3 物联网安全技术在校园安防监控系统中的应用

7.2.4 物联网安全技术在校园智能化数字监狱系统中的应用

本章小结

问题思考

第8章 物联网安全技术发展趋势

8.1 物联网安全技术的未来发展

8.1.1 物联网安全技术的跨学科研究

8.1.2 物联网安全技术的智能化发展

8.1.3 物联网安全技术的融合化趋势

8.1.4 新兴技术在校园物联网安全中的应用

8.1.5 物联网安全技术标准

8.2 物联网安全新观念

8.2.1 从复杂巨系统的角度来认识物联网安全

8.2.2 着眼于物联网整体的强健性和可生存能力

8.2.3 转变安全应对方式

本章小结

问题思考

参考文献

章节摘录

版权页：插图：1.1 信息安全概念在介绍信息安全的概念之前，我们回顾一下生活中发生的信息安全事件。

新闻不时报道，某犯罪团伙利用黑客软件盗取了多个银行卡的网银密码，给人们造成经济损失；前几年互联网上的熊猫烧香病毒，影响广泛。

通俗地说，信息安全就是要保护你的网银密码、秘密短信、悄悄电话等不被别人知道，要保护你的计算机不中病毒，保护公众电话网络不被攻击，保护国家铁路、民航等顺利运行。

抽象地说，信息安全是指信息在产生、传输、使用、存储过程中，对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容或能力被非授权使用、篡改。

一提信息安全，人们就会想到信息加密，密码技术是信息安全的核心技术，但信息安全不仅仅是加密。

比如，对于互联网来说，除了要采用密码技术对网络中的信息进行保护外，还需要实现计算机终端的安全，以及网络设备、通信链路、网络协议、网络应用的安全。

目前，信息安全受到了社会各界的广泛关注。

随着人类社会越来越依赖于各种信息，信息安全的重要性日渐突出。

信息安全正在渗入人们生活的方方面面，随着物联网概念的提出及物联网应用的日渐增多，人们的日常生活将真正地与信息安全紧密联系在一起。

1.2 信息安全基本属性信息的基本属性有机密性、完整性、可用性、可认证性和不可否认性，也就是说，信息安全的目标是要使得信息能保密，保护信息的完整、可用，确保信息的来源和不可否认。

1.2.1 机密性机密性是指信息不泄露给非授权的个人和实体或供其使用的特性。

只有得到授权或许可，才能得到其权限对应的信息。

通常，机密性是信息安全的基本要求，主要包括如下内容。

（1）对传输的信息进行加密保护，防止敌人译读信息并可靠检测出对传输系统的主动攻击和被动攻击。

对不同密级的信息实施相应的保密强度和完善及合理的密钥管理。

<<物联网安全技术>>

编辑推荐

《物联网安全技术》内容丰富，覆盖面广，可作为大专院校师生和广大对物联网安全技术感兴趣的工程技术人员的参考书；是“十二五”国际重点图书出版规划项目之一。

<<物联网安全技术>>

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>