

<<物联网安全>>

图书基本信息

书名：<<物联网安全>>

13位ISBN编号：9787302285038

10位ISBN编号：7302285039

出版时间：2012-6

出版时间：任伟 清华大学出版社 (2012-06出版)

作者：任伟

页数：190

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>>

### 内容概要

《普通高校物联网工程专业规划教材：物联网安全》是国内第一本物联网安全的教材，全面而又系统地论述了物联网安全中的部分关键问题及其典型解决方案。

全书分为3大部分：物联网感知层安全、物联网网络层安全和物联网应用层安全。

物联网感知层安全介绍了RFID安全、无线传感器网络安全、物联网终端系统安全；物联网网络层安全介绍了近距离无线接入安全（无线局域网安全）、远距离无线接入安全（无线移动通信安全）、接入网安全的扩展讨论、物联网核心网安全（6LowPAN安全和RPL安全）、物联网服务端安全（云计算安全）；物联网应用层安全介绍了智能电网安全、EPCglobal网络安全、基于无线体域网的远程医疗安全、M2M安全。

《普通高校物联网工程专业规划教材：物联网安全》可作为物联网工程、信息安全、计算机科学等专业的研究生或本科高年级教材，对物联网安全领域的研究者具有一定参考价值，对物联网领域的工程技术人员亦具有指导价值。

## &lt;&lt;物联网安全&gt;&gt;

## 书籍目录

第1章 物联网安全概述 1.1 物联网安全概述 1.1.1 物联网概念与发展历程 1.1.2 物联网的体系结构 1.1.3 物联网的安全架构 1.2 网络安全问题的一般性讨论 1.2.1 物联网安全与相关学科的关联 1.2.2 一般性安全威胁及其具体表现 \*1.2.3 解决物联网网络安全问题的一般思路 研究与思考 进一步阅读建议 本章参考文献 第1部分 物联网感知层安全 第2章 RFID安全 2.1 RFID系统简介 2.1.1 RFID系统的基本构成 2.1.2 RFID系统的安全需求 2.2 RFID安全的物理机制 2.3 RFID安全密码协议 2.3.1 Hash锁协议 2.3.2 随机化Hash锁协议 2.3.3 Hash链协议 2.3.4 Good Reader协议 2.3.5 David数字图书馆协议 \*2.4 密码算法 2.4.1 轻量级分组加密算法LBlock 2.4.2 密码Hash算法SM3 研究与思考 进一步阅读建议 本章参考文献 第3章 无线传感器网络安全 3.1 无线传感器安全简介 3.1.1 无线传感器网络的体系结构 3.1.2 无线传感器网络的安全需求分析 3.2 无线传感器网络的安全攻击与防御 3.2.1 常见网络攻击方法 3.2.2 常用防御机制 3.3 无线传感器网络的密钥管理 3.3.1 密钥管理的分类与评价指标 3.3.2 确定密钥分配方案Blundo \*3.3.3 随机密钥分配方案EG 3.4 无线传感器网络安全协议SPINS 3.4.1 轻量级安全协议SNEP 3.4.2 广播认证协议uTELSA \*3.4.3 轻量级公钥密码算法NTRU 研究与思考 进一步阅读建议 本章参考文献 第4章 物联网终端系统安全 4.1 嵌入式系统安全 4.1.1 嵌入式系统的安全架构 4.1.2 TinyOS与TinyECC简介 4.2 智能手机系统安全 4.2.1 智能手机病毒简介 4.2.2 Android系统简介 \*4.2.3 OMS平台简介 研究与思考 进一步阅读建议 本章参考文献 第2部分 物联网网络层安全 第5章 近距离无线接入安全——无线局域网安全 5.1 无线局域网的安全威胁 5.1.1 无线局域网的网络结构 5.1.2 无线局域网的安全威胁 5.2 无线局域网的安全机制 5.2.1 WEP加密和认证机制 5.2.2 IEEE 802.1X认证机制 5.2.3 IEEE 802.11i接入协议 \*5.2.4 IEEE 802.11i TKIP和CCMP协议 5.2.5 WAPI协议 \*5.2.6 SMS4对称密码算法 研究与思考 进一步阅读建议 本章参考文献 第6章 远距离无线接入——无线移动通信安全 6.1 无线移动通信安全简介 6.1.1 移动通信系统的体系结构 6.1.2 移动通信网络的一般安全威胁 6.2 2G (GSM) 安全机制 6.2.1 GSM的安全需求 6.2.2 GSM用户认证与密钥协商协议 6.3 3G安全机制 6.3.1 3G安全体系结构 6.3.2 3G (UMTS) 认证与密钥协商协议 6.4 4G安全机制简介 6.4.1 4G国际标准TD—LTE—A \*6.4.2 LTE中的流密码算法ZUC 研究与思考 进一步阅读建议 本章参考文献 第7章 接入网安全的扩展讨论 7.1 近距离无线低速网络安全 7.1.1 Bluetooth安全简介 7.1.2 ZigBee安全简介 7.2 有线网络接入安全 7.2.1 现场总线简介 7.2.2 工业控制系统安全简介 7.3 卫星通信接入安全 7.3.1 CMMB安全广播简介 7.3.2 北斗卫星导航系统简介 研究与思考 进一步阅读建议 本章参考文献 第8章 物联网核心网安全——6LoWPAN和RPL的安全性 8.1 核心IP骨干网的安全 8.1.1 IPsec 8.1.2 SSL/TLS 8.2 6LoWPAN适配层的安全 8.2.1 6LoWPAN协议简介 8.2.2 6LoWPAN要解决的问题 8.2.3 6LoWPAN的安全性讨论 \*8.2.4 RPL和CoAP的安全性讨论 研究与思考 进一步阅读建议 本章参考文献 第9章 物联网服务端安全——云计算安全 9.1 云计算及其安全问题 9.1.1 云计算简介 9.1.2 云计算的安全问题 9.2 云计算的存储安全 9.2.1 云存储的访问控制——基于属性的加密和代理重加密 9.2.2 云存储的数据保密性——同态加密HE \*9.2.3 云存储的数据完整性检验POR和PDP \*9.3 计算虚拟化安全 9.3.1 计算虚拟化简介 9.3.2 计算虚拟化的安全 研究与思考 进一步阅读建议 本章参考文献 第3部分 物联网应用层安全 第10章 智能电网安全 10.1 智能电网概述 10.1.1 智能电网的概念、特征与作用 10.1.2 智能电网的通信与网络架构 10.2 智能电网安全 10.2.1 智能电网的安全架构与安全需求 10.2.2 智能电网的安全问题简介 研究与思考 进一步阅读建议 本章参考文献 第11章 EPCglobal网络安全 11.1 EPCglobal网络概述 11.1.1 EPCglobal网络简介 11.1.2 EPCglobal物联网的网络架构 11.2 EPCglobal网络安全 11.2.1 EPCglobal网络的安全性讨论 11.2.2 EPCglobal网络中的数据清洗 研究与思考 进一步阅读建议 本章参考文献 第12章 基于无线体域网的远程医疗安全 12.1 无线体域网概述 12.1.1 无线体域网的系统架构 12.1.2 无线体域网的特征 12.2 WBAN安全分析 12.2.1 WBAN的安全威胁 12.2.2 WBAN的安全方案简介 研究与思考 进一步阅读建议 本章参考文献 第13章 M2M安全 13.1 M2M概述 13.1.1 M2M的概念、架构与应用 13.1.2 M2M应用实例 13.2 M2M安全 13.2.1 M2M的安全威胁与对策 13.2.2 M2M的安全标准和研究进展简介 研究与思考 进一步阅读建议 本章参考文献 全书参考文献

## 章节摘录

版权页：插图：广义的RFID系统的隐私保护包括两点：一是标签和读写器之间的隐私保护；另一种是服务器中的信息隐私保护，它所关心的是服务器所包含什么样的信息。

本小节主要讨论第一种情况。

隐私问题中的信息泄漏问题是指在获取标签信息之后可对RFID系统进行各种非授权使用，标签可泄漏相关物体和用户信息，如护照、身份证、贵重物品标签持有者可能成为抢劫或者盗窃的目标，个人的药品信息被他人所知导致个人的隐私泄漏等。

隐私问题中的追踪问题是指通过标签的唯一标识符可恶意地追踪用户的位置或者行为。

例如，标识在不同的地方的两次出现，说明用户曾经到达了这两个地方。

攻击者可在任何地点、任何时间追踪识别某个固定标签，从而侵犯了用户隐私。

隐私问题可通过对读写器的认证来解决。

认证问题可通过对标签的认证来解决。

因此，读写器和标签之间的双向认证是RFID系统的主要安全需求。

2.安全威胁 具体而言，一个安全的RFID系统应该对以下攻击加以防范。

(1) 非法读取：非法者通过未授权的读写器读取标签中的数据信息。

(2) 窃听：标签和读写器之间的数据传输容易受到窃听攻击。

(3) 无前向安全性：攻击者在此次通信中截取到了标签的输出，然后通过某种推算可以得出标签以前所发送的信息。

反过来说，如果攻击者不能推算前面发出的信息，则称为前向安全性（Forward Security）。

(4) 位置跟踪：非法者通过标签发出的固定消息来定位标签的位置以达到跟踪的目的。

(5) 伪装：非法者截取到标签信息后，把真实标签信息复制到自己假冒的标签中。

当读写器发送认证消息给标签时，非法者把自己复制的标签信息发给读写器，以伪装成合法标签通过读写器的认证。

(6) 重放：当读写器发出认证信息时，攻击者截取了标签发出的响应信息。

当下一次读写器发出认证请求时，攻击者把截取到的信息发送给读写器，从而通过读写器对它的认证。

(7) 拒绝服务攻击：许多基于挑战—应答方式的协议都要求每次对标签进行访问时，标签都需要提供额外的存储器来存储要产生的随机数，当大量读写器向标签发送询问信息时，标签的存储器就因要存储过多的随机数而停止工作。

3.安全方案设计时的考虑因素 为了设计RFID的安全方案，需要考虑到RFID标签的计算能力，这种计算能力通常限定了可采用的安全方案。

一般可把RFID标签的计算能力分为以下3类。

(1) 基本标签：不能执行加密操作，但可执行XOR操作和简单的逻辑控制的标签。

(2) 对称密码标签：指能够执行对称密钥加密操作的标签。

(3) 公钥密码标签：指能够执行公钥加密操作的标签。

## <<物联网安全>>

### 编辑推荐

《普通高校物联网工程专业规划教材:物联网安全》可作为物联网工程、信息安全、计算机科学等专业的研究生或本科高年级教材，对物联网安全领域的研究者具有一定参考价值，对物联网领域的工程技术人员亦具有指导价值。

《普通高校物联网工程专业规划教材:物联网安全》结构紧密，内容详实。

#### 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>