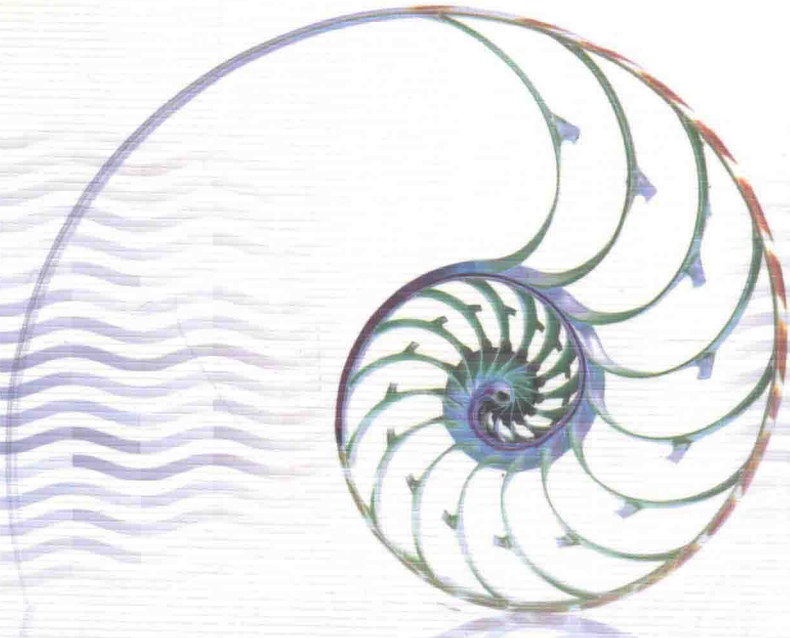
工业和信息化部电子第五研究所　组编



RFID系统安全测评及防护技术

◎主　编　杨　林
◎副主编　刘群兴　朱文立　杨晓明
◎主　审　罗衡峰

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

RFID 系统安全测评及防护技术

工业和信息化部电子第五研究所　组编
主　编　杨　林
副主编　刘群兴　朱文立　杨晓明
主　审　罗衡峰

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书全面、系统地介绍了 RFID 系统的安全、隐私、漏洞及其防护问题。第一篇介绍了 RFID 系统安全的基础知识，分析了 RFID 系统的通用安全需求和可能面临的各种安全威胁。第二篇介绍 RFID 系统安全检测评估标准、方法等，阐述了 RFID 标准体系，RFID 安全的评估指标体系，分两个方面具体阐述 RFID 系统安全评估和 RFID 产品安全检测。第三篇是 RFID 安全防护方法的介绍，提出了 RFID 安全与隐私防护体系，介绍了灾难恢复的相关知识。

本书适合RFID初学者、RFID相关产品设计人员、RFID产品安全测试人员及管理人员、信息安全爱好者，以及物联网相关行业的人士参考阅读。

图书在版编目（CIP）数据

RFID 系统安全测评及防护技术/杨林主编；工业和信息化部电子第五研究所组编.
—北京：电子工业出版社，2015.10
ISBN 978-7-121-27236-3

I. ①R… II. ①杨… ②工… III. ①无线电信号－射频－信号识别－安全技术
IV. ①TN911.23

中国版本图书馆 CIP 数据核字（2015）第 226229 号

策划编辑：张　榕
责任编辑：张　榕
印　　刷：北京天来印务有限公司
装　　订：北京天来印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：720×1 000　1/16　印张：11.75　字数：150 千字
版　　次：2015 年 10 月第 1 版
印　　次：2015 年 10 月第 1 次印刷
定　　价：38.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

<<<<< PREFACE

物联网正在以超越“爆炸”的速度发展，物联网的健康快速发展是两化融合的内在需要，更是我国经济转型升级的强劲动力。RFID 技术作为物联网感知层级核心支撑技术，保障其信息安全显得尤为重要。本书从 RFID 安全技术基础、RFID 安全检测评估体系，以及 RFID 安全防护体系三个方面全面介绍 RFID 安全技术。

第一篇 RFID 安全基础，首先介绍了 RFID 安全技术的基础知识，包括 RFID 系统的组成原理、现代密码技术及公钥基础设施。接着对 RFID 系统进行安全需求分析，最后列举并详细分析了 RFID 系统所面临的安全攻击。

第二篇 RFID 安全检测评估，首先梳理了 RFID 的标准体系，发现标准体系中对射频安全性的保护措施缺乏。然后重点介绍 RFID 系统安全评估技术，再针对 RFID 系统的特点介绍了 RFID 系统安全等级测评的相关知识。最后介绍 RFID 产品安全检测的相关技术，重点介绍了前沿的芯片安全攻击检测技术——边信道攻击技术。

第三篇 RFID 安全防护，介绍了安全防护体系，体系内容包括安全防护策略、安全协议、分级保护以及存储与检索技术。同时，也介绍了 RFID 系统的灾难恢复体系结构，即在系统遇到毁灭性的破坏后，如何最大限度地恢复信息，减少损失。

本书在杨林主任、刘群兴副主任、朱文立副主任及信息安全室主任王颍凯的精心组织和安排下，由罗衡峰负责全书整体策划、设计、协调及审核；曾德智负责全书的统稿；参与人员根据各自的专业擅长分工协作，共同完成，参加本书编写的还有李倩、钟晶、李琳、陈玉明、彭琦、刘锐奇。本书是在这些作者的共同努力下完成的，没有大家的通力合作就没有此书。作为本书的主要策划人，在此对各位作者付出的辛勤劳动表示衷心的感谢！

本书编写过程中得到了电子工业出版社张榕女士及其同事的大力支持、指导和帮助，在此表示衷心的谢意。由于编者水平有限，不当之处，欢迎批评指正。

编　者

目录

CONTENTS

第一篇 RFID 安全基础

第三篇　RFID 安全防护

第一篇　RFID 安全基础

第1章

RFID 安全技术

射频识别技术（Radio Frequency Identification，RFID）利用射频信号通过空间耦合（交变磁场或电磁场）实现无接触信息传递并通过所传递的信息达到自动识别的目的。RFID 作为物联网感知层的核心感知技术，所以研究和发展 RFID 技术前景光明。当前很多 RFID 技术瓶颈正在不断被突破，对于 RFID，人们已经做到“能用”。但在我国，RFID 只是小范围的试点应用，并没有大规模、高质量的应用。究其原因有二：其一，很多 RFID 核心技术没有取得突破，严重影响 RFID 系统的可靠性。其二，RFID 安全形势堪忧，很多黑客能轻易破解 RFID 标签系统和 RFID 后台，轻易地篡改标签信息，达到非法目的。本书是一本全面介绍 RFID 安全的专业书籍，目的就是给 RFID 相关专业技术人员提供参考和借鉴。在介绍核心内容前，在本章首先介绍 RFID 安全技术的几大基础技术。这些基础技术包括：RFID 系统原理及组成、密码技术、公钥基础设施、身份认证、访问控制、入侵检测。

1.1 RFID 系统原理及组成

工业界将 RFID 系统分为阅读器、天线和标签三大组件，其中阅

读器由发送器、接收器和微处理器组成。RFID 技术起源于雷达技术，所以其工作原理和雷达极为相似。其工作流程是：首先阅读器通过自身的天线发送电子信号，标签接收到信号后发射标签内部存储的信息，阅读器再通过天线接收，最后识别标签发来的信息。RFID 系统体系结构如图 1-1 所示。

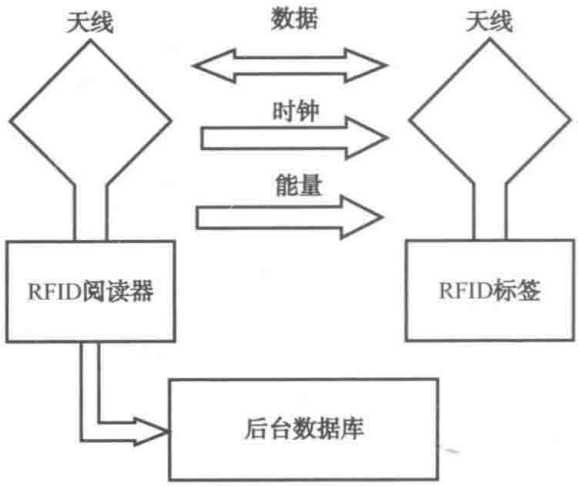


图 1-1　RFID 系统体系结构

1.1.1　阅读器

阅读器是 RFID 系统中最核心的部分，一般都主动向标签询问标示信息。阅读器一般是通过以太网卡、串口、USB 接口和主机相连，通过天线和标签通信。当然在有些场合为了应用方便，阅读器和天线及智能终端设备会集成在一起形成可移动的手持式阅读器。阅读器的外观如图 1-2 所示。

图 1-2　阅读器外观图

1.1.2 天线

天线是用来接收/发射射频信号的，阅读器上可以接 1 个或多个天线，但是每次只能激活一个天线。由于 RFID 工作频段范围很广，从低频到微波，所以天线和标签芯片之间的匹配问题变得很复杂。

1.1.3 标签

RFID 标签（Tag）：由耦合元器件及芯片组成，每个 RFID 标签具有唯一的电子编码，附着在物体上标示目标对象。标签进入磁场后，接收解读器发出的射频信号，凭借感应电流所获得的能量发送出存储在芯片中的产品信息（Passive Tag，无源标签或被动标签），或者主动发送某一频率的信号（Active Tag，有源标签或主动标签）。

RFID 标签可分为三种类型：被动式标签、主动式标签、半主动式标签。被动式标签内部没有电源，又被称为无源标签，被动式标签内部的电路是通过利用 RFID 阅读器发出的电磁波能量驱动。被动标签目前可以采用的通信频率是高频和超高频，高频通信距离最高可达到 1m 左右；超高频标签的通信距离可达到 3～5m，并且支持多标签识别，阅读器可同时识别多个标签。主动式标签内部集成有电源，又称为有源标签，这种标签体积大、成本高，但是通信距离远，可达到上百米。主动标签有两种工作模式，一种是主动模式，在这种模式下标签会主动向四周进行周期性广播。另一种是唤醒模式，在这种模式下，标签只有受到阅读器发出的唤醒命令后才开始广播自己的电子信息编码，这种模式下的标签工作寿命比主动标签长许多年。半主动式标签有着主动和被动的所有优点，内部集成电源，能为标签内部计算提供电源，但是和阅读器的通信是利用阅读器发射的电磁波来获取能量的，而不是利用自身电源供电的。

1.1.4 频率

RFID 的频率是 RFID 系统的一个很重要的参数指标，RFID 的典型工作频率有 125kHz、133kHz、13.56MHz、27.12MHz、433MHz、860～960MHz、2.45GHz、5.8GHz 等。按工作频段，可分为低频、高频、超高频、微波 4 个频段。低频范围：30～300kHz。高频范围：3～3MHz。超高频范围：300MHz～3GHz。微波范围：大于 3GHz。

1.2 密码技术

密码学是信息安全领域的基础学科之一，RFID 系统中的数据存储与传输都会涉及加密技术，所以密码学也是 RFID 系统安全防护的基础技术。密码学是信息安全等相关议题，如认证、访问控制的核心。密码学的首要目的是隐藏信息的涵义，并不是隐藏信息的存在。密码学也促进了计算机科学，特别是对于电脑与网络安全所使用的技术，如访问控制与信息的机密性。密码学已被应用在日常生活，包括自动柜员机的芯片卡、计算机使用者存取密码、电子商务等。

数据加密技术是密码学的核心，原理就是利用加密算法，将明文转换成无意义的密文，确保数据的保密性，明文转换成密文称为加密，密文还原成明文称为解密，加密和解密的规范称为密码算法。在加密和解密过程中，由加密方和解密方使用的加密解密参数称为密钥。加密体制主要有两种：对称密钥（私钥）、非对称密钥（又称为公钥）。对称密钥和非对称密钥的区别如图 1-3 所示。此外，单向哈希函数也是密码学的重要分支，它结合非对称加密机制，可以解决实际应用中身份认证和数据完整性问题。

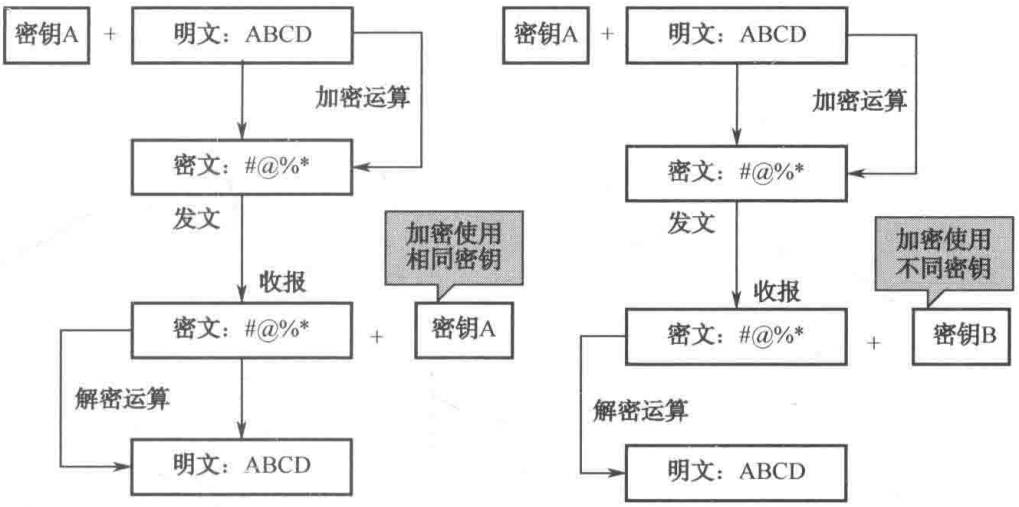


图 1-3　对称密钥和非对称密钥区别

1.2.1　对称密钥

对称密钥加密又称专用密钥加密，即发送和接收数据的双方必须使用相同的密钥对明文进行加密和解密运算。对称密钥加密算法主要包括 DES、3DES、IDEA、FEAL、BLOWFISH 等。

对称密钥是双方使用相同的密钥，必须以绝对安全的形式传送密钥才能保证安全，这点不如非对称密钥。对称加密的要求需要强大的加密算法。算法至少应该满足：即使分析人员知道了算法并能访问一些或更多的密文，也不能译出密文或得出密匙。通常，这个要求以更强硬的形式表达出来，那就是：即使分析人员拥有一些密文和生成密文的明文，也不能译出密文或发现密匙。也就是说，加密算法应足以抵抗已知明文类型的破译。

发送方和接收方必须用安全的方式来获得保密密匙的副本，必须保证密匙的安全。如果有人发现了密匙，并知道了算法，则使用此密匙的所有通信便都是可读取的。