无线射频识别系统安全指南

Frank Thornton　Brad Haines
[美]　Anand M. Das　Hersh Bhargava　著
Anita Campbell

游战清　戴青云　陈　涛　刘春联　等译

RFID Security

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

TN911.23/25
2007

无线射频识别系统安全指南

RFID Security

Frank Thornton　Brad Haines
[美] Anand M. Das　Hersh Bhargava　著
Anita Campbell

游战清　戴青云　陈　涛　刘春联　等译

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

内容简介

无线射频识别（RFID）技术具有非可视识别、距离远、多标签识别、物理环境适应性强、具有唯一的ID号等特点，因此在物流与供应链、小额支付、门禁控制、交通管理等方面得到了十分广泛的应用。也正因为如此，对RFID系统攻击的研究变得十分必要，具有很强的现实意义。本书从RFID系统的角度出发，全面分析了RFID系统常见的攻击方法并提出了相应的安全防护措施。同时，此书在内容安排上还列举了大量RFID系统安全的典型案例。全书分成三个部分，第一部分介绍RFID基本概念与基本应用，第二部分介绍对RFID的常见攻击形式及其危害，第三部分介绍常见的RFID系统安全防护方法。书中还描述了RFID病毒的存在。该书对于RFID应用系统的设计以及系统的开发具有参考作用。附录列举了RFID应用系统中的部分常见问题并简要总结了全书内容。全书始终贯穿沃尔玛公司等典型应用案例，理论结合实际，便于广大读者更好地理解RFID系统安全概念。

本书可作为企业信息化建设特别是RFID应用的行业参考资料，也可以作为准备应用本项技术的企业或机构的参考资料，适合广大信息化工作者、物流工作者、RFID行业技术人员以及应用研究人员阅读。

RFID Security by Frank Thornton, Brad Haines, Anand M. Das, Hersh Bhargava, Anita Campbell.
Original English language edition published by Syngress Publishing, Inc. Copyright © 2005 by Syngress Publishing, Inc. All rights Reserved.

本书中文简体版专有出版权由Syngress Publishing, Inc.授予电子工业出版社，未经许可，不得以任何方式复制或抄袭本书的任何部分。

版权贸易合同登记号　图字：01-2006-7346

图书在版编目（CIP）数据

无线射频识别系统安全指南/（美）桑顿等著；游战清等译. -北京：电子工业出版社，2007.11
书名原文：RFID Security
ISBN 978-7-121-05323-8

Ⅰ.无...　Ⅱ.①桑...　②游...　Ⅲ.无线电信号-射频-信号识别-指南　Ⅳ.TN911.23-62

中国版本图书馆CIP数据核字（2007）第173996号

责任编辑：马　岚　　特约编辑：马爱文
印　刷：北京市顺义兴华印刷厂
装　订：三河市双峰印刷装订有限公司
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：787×980　1/16　　印张：10.25　　字数：201千字
印　次：2007年11月第1次印刷
定　价：25.00元

凡所购买电子工业出版社的图书有缺损问题，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。

译 者 序

无线射频识别（RFID）技术是一项已经存在了数十年的应用技术，但是其在物流与供应链领域的应用才刚刚起步，在其他领域的应用也还处于早期阶段。RFID具有非可视识别、识别距离较远、环境适应性强、具有唯一的ID号、伪造与克隆困难、数据可以现场改写和数据存储量较大等特点，因此RFID可以广泛应用于物流与供应链、小额支付、人员安防识别（包括门禁管理等）、物品防盗与防伪、动物识别、运动计时、疾病追溯以及车辆识别与管理等领域。

与任何一项新技术一样，RFID充满了无穷魅力，给予了人们太多的想象空间，沃尔玛公司和美国国防部（DOD）几年前都宣布将要求其供应商采用RFID进行供货，这两大巨头的这种决定将人们对RFID的应用前景的憧憬推向了极至，以至于掀起了全球范围内对RFID技术的狂热追捧。

任何事物都是矛盾的统一体，RFID技术也不例外。在实际应用中，从对RFID的莫名狂燥中冷静下来时，我们还必须面对另一个非常重要的问题，这就是RFID系统的安全问题。RFID技术的优越特性，如数据可以现场改写等，虽然满足了使用者的工作需要，但是对于系统攻击者来讲，也留下了进行安全攻击的可能，此外，RFID技术对使用者隐私权的侵犯与保护问题也日益受到人们的重视。

RFID系统安全攻击者可以从很多方面对RFID系统进行安全攻击，如标签病毒攻击、标签数据非法改写、应用系统攻击、中间件攻击和后台数据库攻击等，都是RFID系统安全攻击者经常采用的技术手段或技术方法。虽然我们也曾经或多或少地接触到了RFID系统安全的概念，但是很少系统地研究RFID技术的安全性。本书系统地介绍了RFID技术的安全攻击的各种潜在形式，并提出了RFID系统安全保护的基本措施。此外，书中还列举了RFID系统安全的典型应用案例。

我们将此书翻译引进给国内读者，旨在给国内的广大RFID工作者一个关于RFID系统安全的启示，希望本书能对RFID系统安全的建设起到积极的借鉴与参考作用。

本书可以作为企业信息化建设特别是RFID应用的行业参考资料，也可以作为准备应用本项技术的企业或机构的参考资料，还可以作为RFID的普通参考读物。特别地，本书是RFID系统开发人员必备的手册性资料。

该书的读者对象定位于广大信息化工作者、物流工作者和RFID行业技术人员以及应用研究人员。

目前，在国内，甚至在国际上，关于RFID安全的专业图书并不多见，本书的翻译出版，势必对填补国内RFID技术资料的空白，推动RFID技术的应用与发展起到积极的作用。本书具有很好的前瞻性和实用性。

本书由游战清、戴青云、陈涛、刘春联、陈荣、韩国军、徐乐、刘洋、刘海锋等共同翻译。全书由游战清负责审校定稿。

本书特别邀请了中国书法家协会书法家、山东滨化投资公司董事长于江先生为本书题写书名，在此特别表示感谢。

在本书的翻译出版过程中，得到了许多朋友的关爱与支持，在此表示由衷的感谢。由于时间比较紧迫，加上翻译者的水平以及知识面等原因，未必全尽原意，不当或偏差之处，请广大读者予以谅解。

谨以此书献给所有支持和关爱我们的亲人和朋友们！

若有任何问题或者建议，请发邮件至yzq5106@sina.com。

游战清

2007年9月

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

第一部分　RFID 概述

第二部分　RFID 攻击

第三部分　RFID 安全防护

第一部分　RFID 概述

第 1 章　RFID 基本概念

- 本书内容简介
- 无线射频识别技术基础
- 为什么要采用 RFID 技术
- RFID 的基础架构
- RFID 系统的数据通信方式
- 标签的物理形态

1.1　引言

从广义上讲，带有特定识别信息的无线电波的传输都属于无线射频识别技术（Radio Frequency Identification，RFID）的范畴，这就如同出租车司机使用自己的无线呼叫系统与出租汽车管理站进行联系。本章将讨论 RFID 系统的基本构成、主要应用以及 RFID 系统安全的基本概念。

RFID 是对采用无线射频信号来交换识别信息的设备和技术的概括性称呼。一般情况下，RFID 指的是采用一个很小的标签来识别特定的目标对象。识别的过程包括标签接收无线电波信号并解码，然后返回一组数字或其他识别信息。例如，

问：你是什么？

答：我是编号为 12345 的库存货品。

实际上，这个过程首先需要有一个非常复杂的加密编码呼叫与回应的过程，还需要通过数据库进行解码，传输到全球卫星通信系统，最后才能对后台支付系统产生影响。

RFID 技术的应用非常广泛，其中的部分应用列举如下：

- 时点销售（Point of Sale，POS）系统
- 车辆自动识别（Automated Vehicle Identification，AVI）系统
- 建筑物或建筑物内的门禁管制系统
- 家禽识别与管理
- 资产跟踪管理
- 动物识别
- 仓库与物流管理
- 供应链产品跟踪管理

- 产品安全管理
- 工厂原材料跟踪/在制品的厂内跟踪
- 图书馆图书管理系统
- 铁路车辆跟踪管理
- 机场行李管理

1.2 本书内容简介

本书主要研究RFID的技术安全，特别是RFID系统的物理层和数据层（即第1层和第2层）的安全问题。关于RFID应用层的大多数问题，受到特定应用领域的相关规定的影响，也受到相关机构的影响以及哲学或宗教观点的影响。我们对此不做过多的探讨，除非RFID安全决策直接影响某项政策的制定。

我们通常都会以饱满的热忱迎接一项新技术的到来，但是往往会忽略其安全问题。针对企业界的商人对某项技术或产品不负责任地大肆渲染的做法，我们经常会采取批评的态度。即便如此，我们往往也会忽略技术的安全性问题。

对于某项技术来讲，安全问题往往被摆在次要的位置。RFID技术已经在相当广泛的领域得到了应用，但是我们对于RFID系统的安全却没有或者只给予了很少的关注。

RFID虽然是一项较新的应用技术，但是某些RFID应用系统已经暴露出较大的安全隐患。2005年1月，埃克森美孚石油公司（ExxonMobil）的速结卡（SpeedPass）系统和RFID POS系统就被约翰霍普金斯大学进行教学实践的一组学生攻破，其原因就是系统没有采取有效的安全保护手段。

2006年2月，以色列威兹曼大学的计算机科学教授Adi Shamir宣布，他能用一个极化天线和一个示波器来监控RFID系统电磁波的能量水平。他指出，可以根据RFID波瓣场强的变化来确定系统接收和发送加密数据的时间。根据这些信息，RFID系统安全攻击者可以对RFID的散列加密算法1（Secure Hashing Algorithm 1，SHA-1）进行攻击，而这种散列算法在某些RFID系统中是经常使用的。

按照Shamir教授的研究成果，普通的移动电话就会对特定应用场合的RFID系统导致安全危害。就在本书接近脱稿时，荷兰阿姆斯特丹自由大学的一个研究小组研究成功了一种称为概念验证（Proof Of Concept，POC）的RFID蠕虫病毒。这个研究小组在RFID芯片的可写内存中注入了这种病毒程序。当芯片被阅读器唤醒并进行通信时，病毒通过芯片最后到达后台数据库，而感染了病毒的后台数据库又可以感染更多的标签。这个研究课题采用了包括SQL和缓冲区溢出攻击（Buffer Overflow Attack）等在内的常用服务器攻击方法。

由于不能很好地汲取失败的教训，因而经常会出现同样的问题。本书将帮助广大读者采取适当的RFID系统安全措施，不犯或者少犯这种安全错误。

此为试读，需要完整PDF请访问：www.ertongbook.com

因为RFID系统是基于电磁波基础的一种应用技术，因此总是存在潜在着的无意识的信号侦听者。即使RFID系统的电磁波场强很小，电磁波传输的距离也是系统设计的最大阅读距离的很多倍。例如，2005年7月，在美国内华达州拉斯维加斯召开的第13届国际安全会议上，进行了一次演示试验，试验人员在距离RFID阅读器69英尺[①]远的地方，接收到阅读器的电磁波信号，而这个演示系统的最大设计阅读距离不超过10英尺。

此外，电磁波的传播没有固定的方向。电磁波可能会被某些物质所反射，也可能会被另一些物质所吸收。这种不确定性可能会使系统的阅读距离远远大于预期水平，也可能会使信号的正常接收受到影响。

RFID系统的标签数据可在一定距离内传输的特性，为攻击者的侦听（Sniffing）和数据欺骗（Spoofing）提供了方便。

在系统设计的距离之外可以触发RFID标签，使系统拒绝服务，从而产生系统拒绝服务攻击（Denial of Service，DoS）。在这种情况下，电磁信号由于携带大量的数据信息，往往会造成数据堵塞（Radio Jamming）。

在数据堵塞的情形下，杂波信号往往会造成频率拥堵。数据堵塞在现代RFID系统中仍是一种具有很强破坏性的系统安全攻击方式。

近年来，由于如下两个事件的发生，RFID技术越来越引起了人们的普遍关注：

- 2003年6月，沃尔玛（Wal-Mart）公司宣布，到2005年6月，沃尔玛将在其供应链管理体系中逐步推广使用RFID。在沃尔玛的供应链体系中，选择了近100家供货商进行试点。要求这些供货商在包装箱和托盘上使用RFID，因此在收货和发货时就可以采用阅读器进行数据的自动读取。
- 美国国防部（Department of Defense，DoD）做出了采用RFID对所有军用物资进行管理以提高数据质量和管理水平的决定。2003年10月，美国国防部副部长米歇尔宣布了一份备忘录，要求所有军用物资供应商必须使用RFID标签向美军供货。这样做的目的是对军用物资进行实时管理。

美国国防部自从1995年开始就在集装箱货物运输上采用RFID标签进行跟踪。由于美军在全球大约有800亿美元的军用物资，因此对于这些物资的实时跟踪和掌控是非常必要的。

沃尔玛和美国国防部对RFID的推广应用使诸多业外人士、企业和社会团体开始认识到RFID的优势。整个社会对RFID应用的需求将大大推动RFID研发工作的进展，这些工作势必会降低RFID系统的使用成本。

图1.1所示的是不同种类的RFID标签。

① 1英尺 = 0.3048 m——编者注。

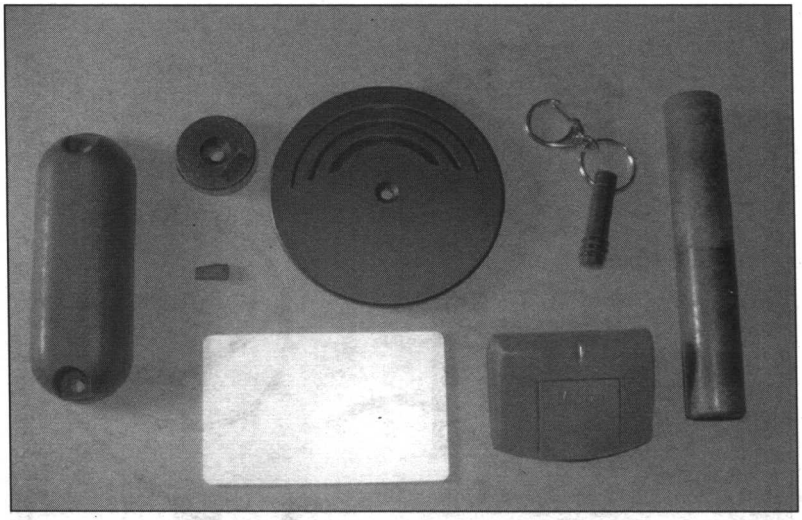

图 1.1 不同形式的RFID标签

随着RFID使用成本的下降，其他大型零售商，如Best Buy和Target等，都开始考虑在托盘级应用上开始使用RFID，或者在规划阶段开始考虑应用RFID。标签的成本下降得足够低时，就可以在更小的包装单元层面上进行应用试点。

图 1.2 所示的是一种RFID阅读器。

小知识

敌我识别（Identification Friend or Foe，IFF）

利用电子标签进行自动识别最早起源于第二次世界大战中对敌机和友机的识别，这就是IFF的由来。当飞机接收到问讯的无线电信号时，友机能反馈回正确的识别信息，而敌机则不能反馈回正确的识别信息。

从原理上讲，IFF类似于现在的RFID。一个经过编码的问讯信号通过特殊的无线设备发射出去，这个信号被标签接收并解码。作为对问讯的回应，标签返回加密的识别信息。每个标签具有唯一的识别号，但飞行员也可以手工设置某些二次信息。

自从第二次世界大战以后，IFF得到了很大的发展。时至今日，在军事领域和民用航空领域仍在应用这项技术进行飞机的识别。此外，还使用IFF技术来传输诸如飞行高度等信息。虽然现在应用于民用航空领域，但是其系统基本上继承了IFF的思想。

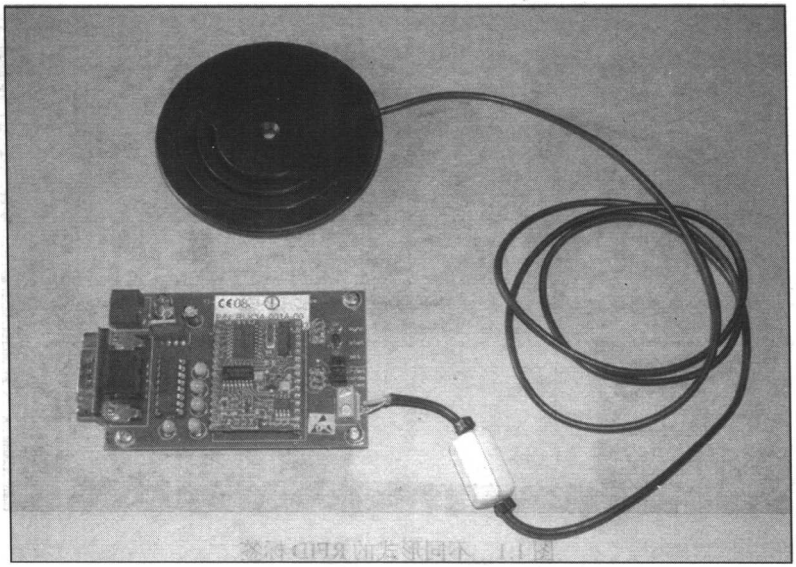

图 1.2　RFID 阅读器（包括天线和阅读器模块）

1.3　RFID 无线电基础

下面简单介绍一些无线电基础知识。如果读者不具备太多的无线电基础知识，那么建议认真阅读这一节。如果读者是个无线电爱好者，那么下面的内容可能简单了些，可以略过。

电磁波是一种很小的电磁波带，覆盖所有频率范围。我们所熟悉的其他电磁波带包括宇宙光子射线、伽马射线、X射线以及可见光等。无线电波谱（Radio Frequency，RF）被分成一系列频段，如甚高频（Very High Frequency，VHF）频段，其频率覆盖30 ~ 300 MHz。在美国，这些频段的使用隶属于联邦通信委员会（Federal Communications Commission，FCC）管理。FCC的职权包括频率的使用授权、无线传输的功率水平以及信号调制方式的管理等。其他大多数国家和地区也设立了类似的管理机构与制度。很多欧盟国家遵从欧洲通信标准委员会（European Telecommunications Standards Institute，ETSI）的管理。

对于RFID来讲，大多数系统都采用了如下三个频段中的一种：低频（Low Frequency，LF，频率范围为125 ~ 134 kHz）、高频（High Frequency，HF，典型频率为13.56 MHz）和超高频（Ultra High Frequency，UHF，频率范围为860 ~ 930 MHz）。对于不同的频段，由于不同国家和地区的具体规定存在差异，在频率的使用上会有所差异。

小工具

赫　　兹

无线电波用赫兹（Hertz，简写为Hz）来进行测量。大多数RFID电磁波的频率在每秒数千周（kHz）、百万千周（MHz）或者十亿千周（GHz）左右。

采用赫兹来对无线电波进行计量是为了纪念德国物理学家海因里希·鲁道夫·赫兹（Heinrich Rudolf Hertz，1857~1894）。赫兹是电子学的鼻祖。赫兹证明了电能可以以电磁波的形式传播，他的证明直接促进了电磁波理论的研究与发展。

很多RFID设备制造商都选择一个特定频率来进行设备的制造，例如可选定在特定应用环境中最适宜工作的频率。频段的电磁特性还影响到阅读器天线的大小以及可用功率水平。反之，特定应用环境中可用设备的物理规格限制也决定了可用频率。

图1.3所示的是两种不同的RFID标签和阅读器。

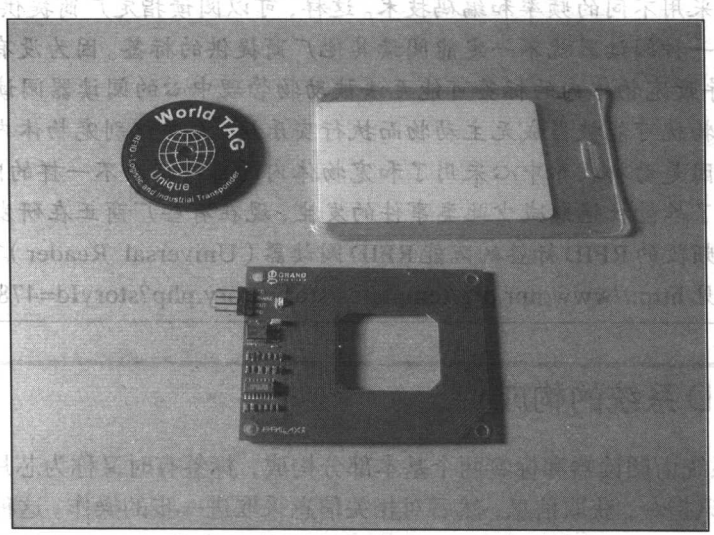

图1.3　两种不同的带有集成天线的RFID标签和阅读器

1.4　为什么要采用RFID

在过去几年里，RFID被广泛地认为可以作为零售业POS系统价格标识的重要技术手段。但是，RFID还远未取代条形码技术，主要是因为单个标签的成本问题。但是，在从制造商到仓储再到零售商的整个零售供应链过程中，RFID技术能够对整个

供应链中的货物进行跟踪，并对整个供应链的经济性产生积极影响，这样，单个标签的价格就变成可接受的了。

小工具

RFID 动物芯片

我们可以将被动 RFID 标签植入动物皮下，称为芯片植入（Chipping）或微芯片植入（Microchipping）。这种方式近年来得到很大发展。将一枚谷粒大小的芯片用注射方式植入猫和狗的两肩之间的某处皮下。这种芯片设计用于替代传统的狗牌进行信息管理。

如果一只宠物丢失，而又被动物管理中心捡到，就可以在动物收养中心进行芯片扫描。如果动物体内存在 RFID 芯片，则工作人员可以通过扫描芯片获取动物主人的信息。这样，就可以及时通知宠物的主人前来认领。

虽然从理论上讲这种方法非常完美，但在实际应用中还存在一些问题。因为目前还没有统一的动物识别 RFID 标签和阅读器标准，不同的制造商可能会采用不同的频率和编码技术。这样，可以阅读指定厂商提供的 RFID 标签的一种阅读器就不一定能阅读其他厂商提供的标签。因为没有统一的标准，导致宠物体内的标签可能无法被动物管理中心的阅读器阅读。这样，这只宠物就可能被当成无主动物而执行安乐死。无法识别宠物体内标签信息的原因是动物收养中心采用了和宠物体内的标签标准不一样的阅读器。

为了尽量杜绝或减少此类事件的发生，现在有些厂商正在研发可以阅读不同频段的 RFID 标签的万能 RFID 阅读器（Universal Reader）。更多信息可参见 http://www.npr.org/templates/story/story.php?storyId=4783788。

1.5　RFID 系统的构成

RFID 系统由阅读器和标签两个基本部分构成，标签有时又称为芯片。阅读器向标签发出问讯指令，获取信息，然后对相关信息采取进一步的操作。这种操作可能会在手持设备上显示相关信息或者向POS系统进行信息分发，也可能会改变库存数据库数据，或者实现数千英里以外的远程支付。

下面讨论典型 RFID 系统的基本构成元素。

1.5.1　标签

RFID单元在传统的无线电设备概念里称为异频雷达收发机（Transponder）。异频雷达收发机是电磁波发射和接收单元的集合体，用来接收特殊的电磁信号并自动进行

信息反馈。在其最基本的应用中，异频雷达收发机侦听无线电信号，并反馈代表其独特标识信息的无线电信号。复杂的系统可以将一串由字母或数字组成的信号传输给信号发射源，也可以传输由数字和字符组成的混合字符串。更高级的系统还可以具有计算和验证过程，包括加密无线电传输，以防止非法侦听者获取传输的信息。

RFID系统中的异频雷达收发机通常称为标签或芯片。虽然芯片指的是很小的无线电单元，而标签由于封装等而具有稍大一些的体积，但是这两种称呼经常是可互换的。本书采用标签这个名称。

作为一般规则，RFID标签主要包含如下组成部分：

- 编码/解码电路
- 记忆体
- 天线
- 电源
- 通信控制电路

标签可以分成两大类：主动标签和被动标签。

1.5.2 主动标签和被动标签

被动（Passive）标签不包含电池或其他电源。这样，标签必须依靠阅读器的信号能量来激活。标签拥有一个可以吸收阅读器天线发射的电磁波能量的共振电路。从电磁场中获得能量的技术也就是所谓的近场（Near Field）技术。顾名思义，为了保证系统的正常工作，标签必须和阅读器天线保持足够近的距离。也就是说，近场必须给标签提供足够的能量，以保证标签可以回传识别信息。

为了保证被动标签的正常工作，天线和标签必须与阅读器保持足够近的距离。因为标签没有内置电源，所以必须从近场中获取能量进行通信。近场具有电磁场的特征，并产生很小的短时电磁脉冲，这种电磁脉冲足够维持标签的正常工作。

与被动标签对应的是主动（Active）标签。主动标签自带电源，通常是内置电池。因为内置电源可以给无线电路供电，因此标签能够主动地发射和接收电磁信号，而不必依靠阅读器天线近场来获取能量。正因为如此，其作用距离不局限于近场范围内。阅读器和标签之间的通信可以跨越近场，达到很远的距离。这样，主动标签系统就具有较远的最小阅读距离。

半被动标签（Semi-passive）内置电池给记忆体电路供电，但是在发射和接收信号时需要依靠近场给无线电路提供能量。

图1.4为主动标签和被动标签系统的工作过程。

此为试读，需要完整PDF请访问：www.ertongbook.com