<<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

<<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。

<<物联网安全>>

书籍目录

章节摘录

 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