软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(4):960−976 [doi: 10.13328/j.cnki.jos.004804]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

射频识别(RFID)隐私保护技术综述*

周世杰, 张文清, 罗嘉庆

(电子科技大学 计算机科学与工程学院,四川 成都 611731)

通讯作者: 周世杰, E-mail: sjzhou@uestc.edu.cn, http://ccse.uestc.edu.cn

摘 要: 随着 RFID(radio frequency identification)技术的广泛应用,引发的隐私威胁问题越来越突出.了解 RFID 隐私的内涵和常见攻击方法,掌握现有的 RFID 隐私保护技术,有助于减少 RFID 隐私信息的泄漏.从 RFID 技术的基本概念入手,全面分析了 RFID 隐私及隐私威胁,给出了 RFID 隐私分类方法;对 RFID 隐私中的跟踪攻击和罗列攻击两种攻击方法进行了深入探讨.在此基础上,对现有典型的 RFID 隐私防御方法进行了详细讨论.全面介绍了 RFID 隐私保护技术发展现状和动态,可作为开展 RFID 隐私保护技术研究工作的参考和借鉴.

关键词: 射频识别;隐私;安全;认证

中图法分类号: TP309

中文引用格式: 周世杰,张文清,罗嘉庆.射频识别(RFID)隐私保护技术综述.软件学报,2015,26(4):960−976. http://www.jos.org.cn/1000-9825/4804.htm

英文引用格式: Zhou SJ, Zhang WQ, Luo JQ. Survey of privacy of radio frequency identification technology. Ruan Jian Xue Bao/Journal of Software, 2015,26(4):960−976 (in Chinese). http://www.jos.org.cn/1000-9825/4804.htm

Survey of Privacy of Radio Frequency Identification Technology

ZHOU Shi-Jie, ZHANG Wen-Qing, LUO Jia-Qing

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract: This survey investigates different approaches proposed in the literature for addressing the privacy issues derived from the radio-frequency identification (RFID) and RFID based applications. The concep of RFID privacy and the vulnerability of privacy in RFID are both discussed. A detail discussion about the classification of RFID privacy is provided. Typical RFID privacy attacks, tracking attack and inventorying attack are also addressed. Finally, concentrating on the existing solutions for RFID privacy, and elaborates how the privacy in RFID and RFID based applications can be assured. The main goal of this survey is to give a concise classification of the most relevant privacy protection solutions applied to RFID privacy. For purpose of brevity and clarity, only the most relevant approaches are selected and addressed.

Key words: RFID (radio frequency identification); privacy; security; authentication

射频识别(radio frequency identification,简称 RFID)技术是一种通信技术,它通过无线电信号识别特定目标,并在无需物理接触下读写相关数据.一个典型的 RFID 系统包括 RFID 标签、RFID 读写器和后端系统[1,2].

RFID 标签(RFID tag 或 tag)包括一个具有一定计算能力和存储能力的芯片和一个耦合部件(如天线).按标签供电方式不同,可以将其分为被动式标签(passive tag)、半被动式标签(semi-passive tag)和主动式标签(active tag).由于受计算能力、存储能力以及成本的影响,RFID 标签(尤其是被动式标签)一般仅能提供简单的安全功能.RFID 读写器(RFID reader 或 reader)包括一个应用处理单元、一个 RF 模块、一个控制逻辑单元和一个用于与标签进行无线射频通信的耦合部件.与标签相比,读写器拥有更好的存储和处理能力,且通常可以提供较好的安

* 基金项目: 国家自然科学基金(60973119, 61170041)
收稿时间: 2013-04-18; 定稿时间: 2014-12-09; jos 在线出版时间: 2015-02-04
CNKI 网络优先出版: 2015-02-04 14:58, http://www.cnki.net/kcms/detail/11.2560.TP.20150204.1458.002.html

全解决方案.后端系统(back-end system)实际上就是 RFID 应用系统的服务器,它一般都包含一个数据库处理系统,用于存储和管理 RFID 标签及其相关信息.

随着物联网技术的发展及其应用的推广,RFID 已经成为极具应用前景的技术之一.然而随着 RFID 应用的普及,其安全问题也日渐突出.其中,用户隐私问题尤为严重.所谓 RFID 隐私问题,是指由于用户因携带有不安全的 RFID 标签导致个人或组织的秘密或敏感信息泄露.比如,如果用户佩戴有 RFID 标签的服饰(如手表)或随身携带有 RFID 标签的药物,攻击者可以用 RFID 阅读器获得标签中的信息,从而不仅获得了用户个人财产的信息,而且还可以据此推断出用户的个人喜好与疾病等私密信息.

目前,关于 RFID 隐私的研究工作已有很多,为了更好地开展该领域的相关研究工作,对现有研究工作进行总结和分析显得极为重要和迫切.为此,本文力图对现有 RFID 隐私技术进行综述.具体来说,对 RFID 隐私威胁及分类、常见的 RFID 隐私解决方案进行了详细的讨论.本文的内容反映了该领域的最新研究成果,对于相关研究人员及开发者具有重要的参考价值.

本文第 1 节分析 RFID 隐私及其威胁.第 2 节对 RFID 隐私保护方法的分类进行讨论.第 3 节重点分析现有 RFID 隐私保护方法和技术,并对各种方法进行比较分析.第 4 节是全文总结.

1 RFID 系统中的隐私及隐私威胁

1.1 隐私及RFID隐私威胁

从概念上来看,隐私(也叫隐私性,privacy)是指个人或组织隐藏自己或与自己相关信息的能力.不同国家、不同个人对隐私有不同的要求和认识.一般来说,因此具有相对性、时效性、专属性、受限性.隐私的相对性是指所有的隐私对于不同的人或者在不同的社会有不同的含义.

RFID 的一个基本特性是自动识别物品.大多数 RFID 隐私威胁来源于具有唯一标示的标签 ID,易于与人的身份相对应.RFID 隐私威胁主要包括关联威胁、偏好威胁、定位威胁、行动威胁、社会关系威胁和垃圾收集威胁等[2−7].

从功能上看,RFID 与传统的其他自动识别技术(如二维条码)相似,因此,RFID 本身并无隐私问题.然而,一旦 RFID 标签与特定目标(如人、商品等)关联起来之后,则可能带来隐私问题.

总之,RFID 技术由于其特殊性,存在较大的隐私泄露风险,需要特殊的方法来确保 RFID 技术以及基于 RFID 技术的各类应用的隐私性.

1.2 RFID隐私性分类

由对 RFID 隐私威胁的分析来看,根据泄露信息性质的不同,射频识别应用领域主要存在两类隐私:信息隐私和位置隐私.根据隐私内容的不同,可分为信息隐私和位置隐私.相关分类如图 1 所示.

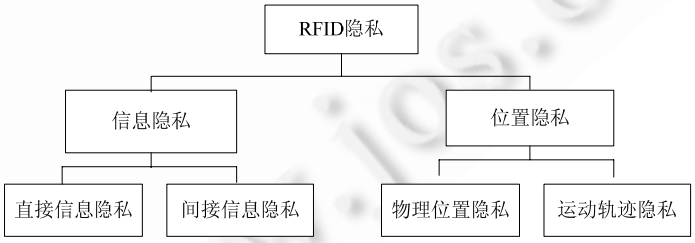


Fig.1 The classification of RFID privacy-according to the features of RFID privacy

图 1 RFID 隐私的分类-按隐私的性质分类

1.2.1 信息隐私

信息隐私(data privacy)是指攻击者通过 RFID 阅读器获得 RFID 标签中的信息,并以此为基础获得个人或组织的其他关联信息.依据隐私侵犯方法,信息隐私包括两类——直接信息隐私和间接信息隐私.

(1) 直接隐私:直接信息隐私是攻击者通过 RFID 标签直接获得隐私信息.例如,在符合电子产品码(electronic production code,简称 EPC)标准的 RFID 标签中,包含产品类别等信息.因此,攻击者通过RFID阅读器扫描用户身上的RFID标签后,通过分析其对象类别编码,就可以直接知晓该标签对应的产品类型.关联威胁、偏好威胁等都属于典型的直接隐私.

(2) 间接隐私:间接信息隐私是指通过对一个或多个标签所对应的产品类型等进行深入分析和推理,并结合社会学等知识,归纳、总结和推导出这些标签所对应的个人的隐私信息.例如,通过分析单个 RFID 标签所对应的药品,可以知道该用户的疾病隐私信息,而攻击者通过手持式阅读器扫描顾客身上的多个 RFID 标签,可获得顾客持有的所有物品信息,从而可以从中推断出顾客的个人喜好或购买偏好.社会关系威胁和垃圾收集威胁等都属于典型的间接隐私.

1.2.2 位置隐私

位置隐私(location privacy)是指攻击者通过采集一个或多个RFID标签的标签特征(tag feature),对该标签特征对应的目标(如人或车)进行位置定位或跟踪.标签特征是指一个 RFID 标签有别于其他 RFID 标签的特殊性质.标签特征可用来唯一识别该标签.标签特征可以是包含在 RFID 标签中的唯一标识符,也可以是标签本身的射频物理特征.包含在 RFID 标签中的唯一标识符(如 96 位的 EPC 编码)是最为重要的标签特征.由于不同厂商对 RFID 物理空中接口的定义不同,RFID 标签的设计、制造和测试工艺不同,甚至所采用的标准也不同,因此某些特殊射频信号特征,如频率、传输调制、数据编码等射频物理特性,也可以作为标签特征.

除了跟踪用户的单个物理位置外,攻击者也有可能根据长期观测结果建立用户的位置移动轨迹,进而推断并预测用户的个人行为.

为了侵犯位置隐私,首先必须建立一个或多个标签特征与个人身份之间的关联关系(mapping relationship).建立该关联关系的方法有很多,例如,通过对个人全身佩戴物的罗列建立个人的 RFID 档案,或者因购买某件贴有 RFID 标签的服饰,而使相关信息被故意或无意泄露等.

根据侵犯隐私的方法的不同,位置隐私可分为物理位置隐私和运动轨迹隐私.

(1) 物理位置隐私:物理位置隐私(physic location privacy)也称为定位隐私,是指通过在特定物理区域部署 RFID 阅读器,对出现在该区域的 RFID 标签进行监控,识别出在该监控区域出现的目标,从而获得目标的物理位置.例如,在知道某个RFID标签(如手表上的RFID标签)的情况下,攻击者若想知道被攻击者是否会在某个珠宝店出现,只需通过手持式 RFID 阅读器对该珠宝店进行扫描.同样,如果攻击者通过手持式 RFID 阅读器在药店某特定药物周围对 RFID 标签扫描,也可以识别出购买该药品的潜在人员.

(2) 运动轨迹隐私:运动轨迹隐私(moving trace privacy)是指通过对一个或多个 RFID 标签进行一段时间的观测和记录,从而建立其运动历史轨迹,并以此预则其未来运动轨迹,进而获得隐私信息.与获得物理位置隐私信息不同,获得运动轨迹隐私信息必须对 RFID 标签进行跟踪观测和记录,因此可能需要在不同的物理地点设置RFID阅读器(或采用移动式RFID阅读器)扫描在该范围内出现的RFID标签.例如,如果商场的商家联合对出现在各自销售区域的 RFID 标签进行记录,并彼此交换信息,则很容易建立顾客在商场的运动轨迹模型,从而推断顾客的个人喜好等隐私.

各类隐私的简要描述、隐私威胁的实施难度以及隐私被侵犯后的威胁总结见表 1.

Table 1 Summary of the classification of RFID privacy

表 1 隐私性分类总结

隐私分类	描述	实施难度	危害
直接信息隐私	通过 RFID 标签直接获得的隐私	容易	大
间接信息隐私	对 RFID 标签数据进行分析获得的隐私	容易	较小
物理位置隐私	通过标签数据获得目标的物理位置信息	较难	大
运动轨迹隐私	通过标签数据的分析获得目标的运动轨迹信息	很难	极大

一般而言,侵犯直接信息技术难度低,而且由于数据准确,因此危害较大.间接隐私由于包含推理和综合分

析的内容,因此准确性难以保证,危害性较小.物理位置隐私需要在指定物理区域部署多个 RFID 阅读器或者借助于手持式阅读器,因此成本较高,技术难度较大.但是由于物理位置隐私可能涉及用户很多敏感内容,因此危害性较大.运动轨迹隐私必须借助于多个物理位置的阅读器数据,因此技术难度最大,其危害性也极大.

此外,信息隐私与位置隐私反映了隐私性的不同方面,二者既有不同点,相互之间也有关联.信息隐私具有静态性,是对攻击目标某一性质的描述;位置隐私是对目标隐私性的动态描述,位置隐私的侵犯一般需要借助于信息隐私来实现.

2 RFID 隐私保护方法分类

2.1 RFID隐私保护对RFID标签的安全性要求

通过以上对 RFID 隐私分类和隐私攻击方法的分析可知,RFID 隐私问题的根源是 RFID 标签的唯一性和标签数据的易获得性.因此 RFID 标签安全需求有如下几方面.

(1) RFID 标签 ID 匿名性.标签匿名性(anonymity)是指标签响应的消息不会暴露出标签身份的任何可用信息.加密是保护标签响应的方法之一,然而尽管标签的数据经过了加密,但如果加密的数据在每轮协议中都固定,攻击者仍然能够通过唯一的标签标识分析出标签的身份,这是因为攻击者可以通过固定的加密数据来确定每一个标签.因此,使标签信息隐蔽是确保标签 ID 匿名的重要方法.

(2) RFID 标签 ID 随机性.正如前面分析,即便对标签 ID 信息加密,因为标签 ID 是固定的,则未授权扫描也将侵害标签持有者定位隐私.如果标签的 ID 为变量,标签每次输出都不同,隐私侵犯者不可能通过固定输出获得同一标签信息,从而可以在一定范围内解决 ID 追踪问题和信息推断的隐私威胁问题.

(3) RFID 标签前向安全性.所谓 RFID 标签的前向安全,是指隐私侵犯者即便获得了标签存储的加密信息,也不能回溯当前信息而获得标签历史事件数据.也就是说,隐私侵犯者不能通过联系当前数据和历史数据对标签进行分析以获得标消费者隐私信息.

(4) RFID 标签访问控制.RFID 标签的访问控制,是指标签可以根据需要确定读取 RFID 标签数据的权限.通过访问控制,可以避免非未授权 RFID 读写器的扫描,并保证只有经过授权的 RFID 读写器才能获得 RFID 标签及相关隐私数据.访问控制对于实现 RFID 标签隐私保护具有重要的作用.

2.2 RFID隐私保护方法分类

根据对 RFID 隐私、隐私攻击方法及技术手段和隐私安全需求的分析,RFID 隐私保护的基本方法包括:

- 改变关联性:改变 RFID 标签与具体目标(如人)的关联性;
- 改变唯一性:改变 RFID 标签输出信息的唯一性;
- 隐藏信息:隐藏 RFID 标签标识符及 RFID 标签中存储的数据.

2.2.1 改变关联性

所谓改变 RFID 标签与具体目标的关联性,就是取消 RFID 标签与其所属依附物品之间的联系.例如,购买粘贴有 RFID 标签的钱包后,该 RFID 标签与钱包之间就建立了某种联系.而改变它们之间的关联,就是采用技术和非技术手段,取消它们之间已经建立的关联(如将 RFID 标签丢弃).

改变 RFID 标签与具体目标的关联性的基本方法包括丢弃、销毁和睡眠.

(1) 丢弃(discarding):丢弃是指将 RFID 标签从物品上取下来后遗弃.例如,购买基于 RFID 标签的依附后,将附带的 RFID 标签丢弃.丢弃不涉及技术手段,因此简单、易行,但是丢弃的方法存在很多问题:首先,采用 RFID 技术的目的不仅仅是销售,它还包含售后、维修等环节,因此,如果简单地丢弃 RFID 标签后,在退货、换货、维修、售后服务等方面都可能面临很多问题;其次,丢弃后的 RFID 标签会面临前面所述的垃圾收集威胁,因此并不能解决隐私问题;最后,如果处理不当,RFID 标签的丢弃也会带来环保等问题.

(2) 销毁(killing):销毁是指让 RFID 标签进入永久失效状态.销毁可以是毁坏 RFID 标签的电路,也可以是

销毁 RFID 标签的数据.例如,如果破坏了 RFID 标签的电路,则不仅该标签无法向 RFID 阅读器返回数据,且即便对其进行物理分析也可能无法获得相关数据.销毁需要借助技术手段,对普通用户而言可能存在一定的困难,一般需要借助于特定的设备来实现,因此实现难度较大.与丢弃相比,由于标签已经无法继续使用,因此不存在垃圾收集等威胁.但在标签被销毁后,也会面临售后服务等问题.

(3) 睡眠(sleeping):睡眠是通过技术或非技术手段让标签进入暂时失效状态,当需要的时候可以重新激活标签.这种方法具有显著的优点:由于可以重新激活,因此避免了售后服务等需要借助于 RFID 标签的问题,而且也不会存在垃圾收集攻击和环保等问题.但与销毁一样,需要借助于专业人员才能实现标签睡眠.

2.2.2 改变唯一性

改变 RFID 标签输出信息的唯一性是指 RFID 标签在每次响应 RFID 读写器的请求时,返回不同的 RFID 序列号.不论是跟踪攻击还是罗列攻击,很大程度上是由于 RFID 标签每次返回的序列号都相同所致.因此,解决 RFID 隐私的另外一个方法是改变序列号的唯一性.改变 RFID 标签数据需要技术手段支持,根据所采用技术的不同,主要方法包括基于标签重命名的方法和基于密码学的方法.

(1) 基于标签重命名的方法:是指改变 RFID 标签响应读写器请求的方式,每次返回一个不同的序列号.例如,在购买商品后,可以去掉商品标签的序列号而保留其他信息(例如产品类别码),也可以为标签重新写入一个序列号.由于序列号发生了改变,因此攻击者无法通过简单的攻击来破坏隐私性.但是,与销毁等隐私保护方法相似,序列号改变后带来的售后服务等问题需要借助于其他技术手段来解决.

(2) 基于密码学的方法:是指加解密等方法,确保 RFID 标签序列号不被非法读取.例如,采用对称加密算法和非对称加密算法对 RFID 标签数据以及 RFID 标签和阅读器之间的通信进行加密,使得一般攻击者由于不知道密钥而难以获得数据.同样,在 RFID 标签和读写器之间进行认证,也可以避免非法读写器获得 RFID 标签数据.

从安全的角度来看,基于密码学的方法可以在根本上解决 RFID 隐私问题,但是由于成本和体积的限制,在普通 RFID 标签上几乎难以实现典型的加密方法(如数据加密标准算法).因此,基于密码学的方法虽然具有较强的安全性,但给成本等带来了巨大的挑战.

2.2.3 隐藏信息

隐藏 RFID 标签是指通过某种保护手段,避免 RFID 标签数据被读写器获得,或者阻扰读写器获取标签数据.隐藏 RFID 标签的基本方法包括基于代理的方法、基于距离测量的方法、基于阻塞的方法等.

(1) 基于代理的 RFID 标签隐藏技术

在基于代理的 RFID 标签隐藏技术中,被保护的 RFID 标签与读写器之间的数据交互不是直接进行的,而是借助于一个第三方代理设备(如 RFID 读写器).因此,当非法读写器试图获得标签的数据时,实际响应是由这个第三方代理设备所发送.由于代理设备功能比一般的标签强大,因此可以实现加密、认证等很多在标签上无法实现的功能,从而增强隐私保护.基于代理的方法可以对 RFID 标签的隐私起到很好的保护作用,但是由于需要额外的设备,因此成本高,实现起来较为复杂.

(2) 基于距离测量的 RFID 标签隐藏技术

基于距离测量的 RFID 标签隐藏技术是 RFID 标签测量自己与读写器之间的距离,依据距离的不同而返回不同的标签数据.一般来说,为了隐藏自己的攻击意图,攻击者与被攻击者之间需要保持一定的距离.而合法用户(如用户自己)获得 RFID 标签数据可以近距离进行.因此,如果标签可以知道自己与读写器之间的距离,则可以认为距离较远的读写器,其具有攻击意图的可能性较大,因此可以返回一些无关紧要的数据;而当收到近距离的读写器的请求时,则返回正常数据.通过这种方法,可以达到隐藏 RFID 标签的目的.

基于距离测量的标签隐藏技术对 RFID 标签有很高的要求,而且要实现距离的精确测量也非常困难.此外,如何选择合适的距离作为评判合法读写器和非法读写器的标准,也是一个非常复杂的问题.

(3) 基于阻塞的 RFID 标签隐藏技术

基于阻塞的 RFID 标签隐藏技术是通过某种技术,妨碍 RFID 读写器对标签 Tag 数据的访问.阻塞的方法可以通过软件实现,也可以通过一个 RFID 设备来实现.此外,通过发送主动干扰信号,也可以阻碍读写器获得 RFID 标签数据.

与基于代理的标签隐藏方法相似,基于阻塞的标签隐藏方法成本高、实现复杂,而且如何识别合法读写器和非法读写器也是一个难题.

各种隐私保护方法的比较分析可见表 2.

Table 2 The comparison of methods of RFID privacy protection

表 2 隐私保护方法比较分析

保护方法	描述	有效性	成本	实用性
丢弃	将 RFID 标签遗弃	低	低	差
销毁	RFID 标签进入永久失效状态	非常高	低	差
睡眠	让 RFID 标签进入暂时失效状态	高	低	强
基于重命名的方法	改变 RFID 标签响应读写器的方式,每次返回不同的数据	高	低	强
基于密码学的方法	采用密码学的方法保证 RFID 标签数据不被非法获取	高	高	差
基于代理的方法	采用第三方设备代替标签响应读写器的请求	高	高	较强
基于距离测量的方法	依据标签与读写器之间的不同距离返回不同的标签数据	高	高	差
基于标签阻塞的方法	采用技术手段干扰非法读写器的攻击	高	高	较强

丢弃的方法不仅无法保护 RFID 隐私,而且还会带来售后服务和环保等问题,因此实用性很差;销毁的方法虽然可以很好地保护 RFID 隐私,而且成本很低,但是由于存在售后服务等问题,因此实用性差;基于睡眠的方法可以较好地保护 RFID 的隐私,成本低,因此实用性强;基于重命名的方法由于改变了序列号的唯一性,因此隐私保护效果好,实用性较强;基于密码学的方法会提高 RFID 标签的成本,因此实用性较差;基于代理的方法、基于距离测量的方法和基于阻塞的方法都需要额外的设备,因此成本高,其实用性取决于应用需求.

3 典型的 RFID 隐私保护方法分析

3.1 基于改变RFID标签与具体目标关联性的隐私保护技术

3.1.1 可移出式标签隐私保护方法

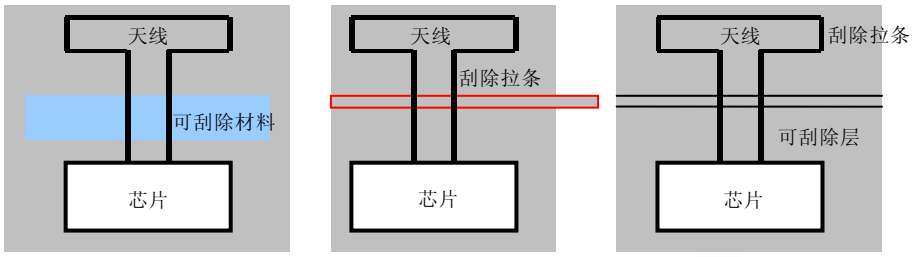
在可移出式标签隐私保护技术中,所采用的 RFID 标签为可移出式(removable tag),当不需要保护隐私时,将标签从产品上取走,从而达到保护的目的[8−10].但是,由于取走了标签即失去了 RFID 的优势,如在产品维修等方面会带来困难.此外,标签移出后如何保存和处理也是一个难题.如果处置不当,可能会带来垃圾收集威胁和环保等问题.因此,从严格意义来说,可移出式标签不是一种隐私保护方法.

3.1.2 可修改式标签

另外一种修改标签信息的方法是在物理上提供修改标签的功能(clipped tag).文献[8]提出:通过从封装等物理特性角度考虑 Tag 的设计,使得用户可以从物理上修改标签状态,从而防止信息泄漏.有两种实现这项功能的 Tag 的设计方法(如图 2 所示).

图 2 中,标签芯片和天线之间有一个隔离层,该隔离层可以是可刮除材料(如图 2(a)所示),或者是一个可去除式窄带(如图 2(b)所示),亦或者是可去除式外层(如图 2(c)所示).当需要避免标签数据被非法读取以提供隐私保护时,只需去掉可刮除材料、窄带或外层,就可以隔断天线和芯片之间的连接,从而使标签从物理上失效.

该方法的优点是用户操作非常简单,不需要额外的工具或 RFID 读卡器.其缺点是设计成本高,一般情况下是对 RFID 标签不可恢复的破坏.当然,采用较高的技术手段,攻击者可以通过重新贴上一层材料,从而恢复天线和芯片之间的连接,重新获得标签上的数据.



(a) 具有可刮除材料的标签 (b) 具有刮除拉条的标签 (c) 具有可刮除层的标签

Fig.2 The RFID privacy protection scheme with physical feature

图 2 具有物理修改功能的标签设计方案

3.1.3 标签支持终止命令的方法

所谓标签支持终止命令的方法,是指 Tag 支持终止(kill)命令,使自己进入永久失效状态[10].所谓永久失效状态(dead),是指通过物理的方法破坏标签的内部结构,使之无法响应任何 RFID 读卡器的读写请求,其内部数据也无法恢复.实现 Kill 命令的方式可以是毁坏电源,也可以是电路短路等方式.许多商用 RFID 标签都支持终止命令.对于支持 Kill 命令的标签,用户只需要使用 Reader 向 Tag 发送 Kill 命令,后者可自动进入失效状态,从而确保隐私信息不会泄露.Kill 协议的示意图如图 3 所示.

条件:Tag 支持 Kill 命令
结果:Tag 执行 Kill 命令后进入永久失效状态
协议:
(1) $R \rightarrow T$: Kill Command
(2) T: 自毁并进入永久失效状态

Fig.3 The Kill protocol

图 3 Kill 协议

该方法的优点是简单,成本低,对 RFID 标签无特殊要求,其缺点是存在安全隐患.由于没有安全保障机制,任何人都可以通过读卡器向标签发送 Kill 命令,从而直接可使 Tag 失效.例如,恶意攻击者可以通过发送 Kill 命令发动攻击,使不应该进入睡眠的标签进入睡眠状态,从而破坏 RFID 系统的可用性.

3.1.4 标签支持口令保护的终止命令方法

支持口令保护的终止命令方法的基本功能与 Kill 命令方式相同,但 Tag 在收到该终止命令后,必须验证发送该 Kill 命令的读卡器的合法性[9,10].验证过程通过验证一个受保护的口令(PIN)来实现.例如,对于 EPC Class-1 和 Gen-2 类型的 Tag,它会在本地存储区存储一个 32 位的唯一标识符(PIN).当读卡器向 Tag 发送 Kill 命令时,必须同时向标签发送 PIN.Tag 收到 Kill 命令及相应的 PIN 之后,与本地存储的 PIN 进行比较:如果相同,则验证通过,Tag 进入失效状态;否则,忽略该 Kill 命令.具有 PIN 保护的 Kill 方法示意图如图 4 所示.

条件:Tag 支持 Kill 命令
每个 Tag 存储一个 PIN
结果:Tag 验证 PIN 后执行 Kill 命令,并进入永久失效状态
协议:
(1) $R \rightarrow T$: Kill Command||PIN
(2) T:与本地 PIN 比较:如果相同,则进入失效状态;否则,忽略

Fig.4 The Kill protocol with PIN

图 4 具有 PIN 保护的 Kill 方法

与简单的终止-睡眠方法相似,该方法的优点是简单,对 RFID 标签要求低,即,RFID 标签只需具备存储 PIN 的能力即可.其缺点是存在前向安全隐患.由于所发送的 PIN 是明文传送,因此易为攻击者截获.获得该 PIN 的信

息后,攻击者可以将该 PIN 和以前的信息关联起来,进而利用该 PIN 获得 Tag 以前的信息,破坏 RFID 的前向保密性.由于需要存储 PIN,对 RFID 成本略有增加.此外,当存在大量 RFID 标签时,RFID 读卡器需要存储所有标签的 PIN,因此,存储和更新 PIN 也是一个极大的问题.

3.1.5 标签支持睡眠命令的方法

标签支持睡眠命令方法的基本思路与支持 PIN 保护的 Tag 相同,只是当验证 PIN 并通过后,Tag 进入睡眠状态(sleeping),而不是进入永久失效状态.当需要唤醒它时,只需要向标签发送一个相同的 PIN 即可.与支持 PIN 保护的 Tag 一样,由于使其进入睡眠状态前所发送的 PIN 可能被攻击者或恶意用户窃听到,因此易被利用发动重放攻击,从而获得 RFID 标签的数据.具有 PIN 保护的 Sleeping 方法示意图如图 5 所示.

条件:Tag 支持 Kill 命令
每个 Tag 存储一个 PIN
结果:Tag 验证 PIN 后执行 Sleeping 命令,并进入睡眠状态或激活状态
协议:
(1) $R \rightarrow T$: Sleeping Command||PIN
(2) T:与本地 PIN 比较,更改当前状态(若当前状态为激活,则进入睡眠;若当前状态为睡眠,则进入激活);否则忽略

Fig.5 The Sleeping protocol with PIN

图 5 具有 PIN 保护的 Sleeping 方法

3.1.6 物理触发开关方法

物理触发开关方法是指:通过在 Tag 上设置物理式开关(physical trigger),以物理接触方式实现睡眠与唤醒.当需要保护隐私时,可以触发物理开关进入睡眠状态[11−15];而当需要利用标签信息进行其他操作(如维修)时,可以触发唤醒开关使标签恢复到正常状态.由于不需要 PIN 保护,因此这种方案简单、易行.但是,如果攻击者获得了该标签,就失去了保护功能.此外,物理开关也会增加标签设计难度和制造成本.

3.2 基于改变标签输出信息唯一性的隐私保护技术

如果 Tag 总是向 RFID Reader 返回固定的标识符信息,就会破坏其隐私性.为此,对于 RFID 读写器的每次查询,标签动态、随机改变返回的标识符信息可起到隐私保护的作用.在本文中,改变标签序列号的方法统称为标签重标示方法.

3.2.1 标签重命名方法

(1) 去掉 Tag 标识符的方法

文献[16,17]提出了一种简单的重标示方法:当用户需要保护个人隐私时(例如当用户购买商品后),去掉商品标签的序列号,但是保留其他信息(例如产品类别码)等.但是,由于产品类别码也有可能会泄漏用户的隐私信息(例如攻击者可以采用罗列攻击),因此这种方法没有提供真正意义的安全保护.

(2) 随机重写标签信息

另外一种更为简单的方法就是完全随机重写标签序列号[18],从而使得标签获得一个全新的随机标识符.重写可以在商品售出时进行,也可以在需要保护隐私时由用户或者制定商家进行.为了提供基于 RFID 标签的商品服务(如维修),商家或者厂商必须提供新旧序列号之间的映射管理,从而在需要时可恢复出原来的 RFID 标识符信息.

随机重写方法的优点是简单,对标签要求低;其缺点是何时进行随机重写不易确定.如果用户需要进行标识符的重写,用户需要拥有相应的 RFID 读卡器.此外,当商品较多时,长期维护标签的历史信息也是一项极为困难的任务.

(3) 标签重用

有两种重用标签序列号的方法:可写式标签(rewritable tag)和标签序列号物理分割(physical ID separation).

(a) 可写式标签

文献[15]提出:每个标签有一个只读存储器(ROM)和一个可写存储器(RAM),ROM 和 RAM 只能互斥使用.即,Tag 存在两个状态:ROM 状态和 RAM 状态.Tag 处于 ROM 状态时,而且仅当 RAM 中没有数据时才能读 ROM 中的内容;当标签处于 RAM 状态时,可以访问 RAM 中的内容.两种状态的切换必须有具有权限的用户才能执行.ROM 中存放标签的永久性 ID,因此其意义是全局的;而 RAM 中存放只对授权用户有意义的临时性 ID.通过在 ROM 和 RAM 两种状态的切换,标签就可以提供无访问限制的永久性 ID 和有访问限制的临时性 ID.当然,授权用户可以擦除 RAM 中的信息而获得标签的永久性 ID.

该方法的优点是既可以保存 RFID 的原始标签,又可以在需要时提供隐私保护.但是,该方法依赖于严格的权限管理,因此不仅需要标签具备较好的安全功能(如认证与加密),也需要一套较为负责的权限管理机制.

(b) 序列号分割

文献[15]提出,将标签序列号分为两个部分:Class ID 和 Pure ID.Class ID 对应标准 RFID Tag 序列号的一部分,因此可以得到产品的某些相关信息;Pure ID 是标签标识符的剩余部分,它由产品序列号等组成.单独的 Class ID 是不具有全局意义的,而只有和 Pure ID 结合后才能成为一个完整的标签标识符.当在产品的某个生命周期阶段需要转让产品的所有权或提供隐私保护(如用户买下该产品)时,利用电子擦除技术去掉 Class ID,而由该产品新的拥有者赋予只对用户有意义的新的 Class ID.新的标识符的含义取决于用户所赋予的 Class ID.

该方法通过修改 Class ID 提供隐私保护功能.但是,由于攻击者通过 Pure ID 也能获得用户的部分信息,因此该方法没有提供完善的隐私保护.此外,与其他重命名方法相似,由于修改了 Tag 的唯一标识号,序列号分割方法也可能失去某些 RFID 固有的优势.

标签重标识方法不能完全解决 RFID 的隐私问题.例如,该类方法如果仅修改唯一标识码,就无法解决罗列攻击;如果没有修改产品类别码,则不能完全解决追踪攻击;虽然赋予新的唯一标识码解决了罗列攻击问题,但却没有解决追踪问题.

3.2.2 基于密码学的方法

(1) 基于最小密码技术的方法

基于以下两个假设,文献[19]提出了所谓最小密码技术(minimalist cryptography):

- 攻击者对 Tag 的轮询攻击是有限的;
- 攻击者发起中间人攻击比较困难.

所谓最小密码技术,就是每个 Tag 存储一个较短的(伪)随机序列(pseudonyms)列表,而读写器(或 Back-End 系统)存储每个标签的整个标识符集合.每次响应 Reader 的询问时,Tag 循环发送该列表中的下一个标识码;当 Reader 收到标签返回的标识码后,通过穷举搜索(枚举)自己所存储的标识符集合从而完成认证,并以此获得 Tag 的其他相关信息.最小密码技术方法的操作过程如图 6 所示.

条件:Tag 存储一个随机序列 $A_i=\{\alpha_1,\alpha_2,\ldots,\alpha_k\}$($k$ 是安全系数)
Back-End 存储所有 Tag 的随机序列 $A=\{A_1,A_2,\ldots,A_n\}$
结果:Tag 随机发送一个自己的随机数,用于表明自己的身份
协议:
(1) Read→Tag: Query
(2) $T\rightarrow R\rightarrow S$: α_i

Fig.6 The minimalist cryptography method for RFID privacy

图 6 Minimalist cryptography 方法

为了抵抗攻击者的枚举攻击,Tag 每次响应时可以有一定的延迟,从而延长攻击者攻击的时间.结合认证技术,可以更新 Tag 的随机标识列表,从而进一步提高安全性.最小密码技术由于要求 Tag 存储随机序列,因此只适合具有一定存储容量的 Tag.此外,这种方法也容易受中间人攻击和重放攻击.而具有认证功能的最小密码技术不仅存储要求高,而且协议复杂,因此在实际应用中很难实现.其他关于 Minimalist Cryptography 的相关研究工作可参见文献[20,21].

(2) 基于加密的方法

RFID 的隐私无法得到保证的原因之一是 Tag 总是输出固定信息,因此,解决方法之一就是对 Tag 进行加密[47].依据所采用的加密技术,主要包括对称密码机制和非对称密码机制.

采用对称密码机制的隐私解决方案的基本流程是:每个 RFID Tag 和 RFID Reader(或后端系统)之间共享一个秘密密钥,Tag 将加密后的信息发送给 Reader 和 Back-End 进行验证和处理.由于攻击者不知道共享秘密,因此无法获得 Tag 所发送信息的真实含义[22].

这里的加密可以是对称加密算法,也可以是非对称加密算法.虽然采用了加密技术,使得攻击者无法获得 Tag 的具体的标识信息,但是由于 Tag 输出依然是唯一的,因此攻击者可以通过其唯一性对用户物理位置进行跟踪.因此,简单的加密技术不能保证其隐私性[23−25].

(3) 基于重加密的方法

解决加密方案中标签输出唯一性问题的方案之一,是采用基于公钥技术的重加密技术(re-encryption technology)[26,27].在重加密方案中,标签具有唯一标识码 T_i 和用读写器的公钥对 T_i 以及一个随机数 r_i 进行加密所得密文 C_i;当响应读写器的请求时,标签返回 C_i;拥有私钥的读写器可以解密 C_i 而获得标签的 T_i,非法读写器由于没有私钥,因此无法得到 T_i.所有的密码操作并非由标签完成,而是由读写器完成,对标签的要求是其存储空间可写.认证完成之后,Reader 对 T_i 以及新的随机数 r_i' 进行再加密,并回传给 RFID Tag.

虽然重加密技术可以解决位置跟踪攻击问题,但是需要密钥对的管理.如果加密操作由 Tag 完成,无疑增加了对 Tag 的要求.如果加密操作由 Reader 完成,那么公钥在传给 Reader 的过程中可能被攻击者窃听和跟踪,从而以此为基础破坏协议的隐私性.此外,如果将重加密技术用于 RFID 支票时,应该对 T_i 的签名进行加密和再加密.

(4) 基于统一重加密的方法

统一重加密 Universal Re-encryption Technology[27,28]基于 ElGamal 密码体制,基本原理与重加密技术相似,但是具有多个私钥/公钥对.该方法具有以下特点:

- 不需要知道公钥,而只需要随机数就可以多次加密;
- 解密时只需要私钥和密文就可以一次解密;
- 具有语义(semantic)安全性:密文不会泄漏明文的信息.

(4) 基于 Hash 的方法

除了上述动态改变 Tag 标识信息的方法之外,也可以采用哈希函数(hash function)或异或运算等方法.由于这些方法均与认证有关,因此在此我们仅作简单介绍[29].

(a) Hash Lock 方法

基于 Hash 的隐私保护的基本思想是:标签存储一个密钥 K 的摘要值:$MetaID=Hash(K)$,其中,K 为标签和读写器之间共享的密钥.当读写器需要读取标签的数据时,向标签发送 K.标签计算并比较 $MetaID$:如果相同,则回应数据;否则,拒绝读写器的请求.Hash Lock 方法存在的问题包括:

- $MetaID$ 是静态的,因此存在追踪攻击隐私问题;
- K 是明文发送的,因此攻击者可截获并伪装成合法标签而欺骗读写器.

(b) 随机化 Hash Lock 方法

Hash Lock 方法的问题之一是可以追踪物体,因此必须周期性改变 $MetaID$.为此,标签需要存储一个哈希函数和一个随机数生成器.当读写器请求时,标签响应$(r,H(ID,r))$.服务器通过搜索所用 ID,计算并比较 $H(ID,r)$;如果找到对应的 ID 使得比较结果相同,则通过认证.该方案的主要问题是:读写器必须穷举所有 ID 空间,计算开销大;读写器可以预先向标签查询一个$(r,H(ID,r))$,进而利用其伪装成合法标签欺骗读写器.

(c) Hash-Chain 方法

在 Hash-Chain 方法中,RFID 标签拥有两个 hash 函数:一个用于更新随机数;另外一个用于响应读写器查询.其响应过程与随机化 Hash Lock 方法相似,即响应$(r,H(ID,r))$(只不过这里的 r 是由另外一个 hash 函数生成).该方案主要问题同样是读写器必须穷举所有 ID 空间,计算开销大.与随机化 Hash Lock 方法不同,虽然读写器可以预先向标签查询一个$(r,H(ID,r))$,进而利用其伪装成合法标签欺骗读写器,但是不存在前向保密威胁问题.

其他有关基于哈希的隐私保护方法参见文献[28,29].

(5) 基于可信计算的隐私保护技术

文献[30]提出在 Reader 中嵌入一个可信模块(trusted platform module,简称 TPM)芯片.TPM 包含该 Reader 特有的安全参数(如密钥等).远程设备(如 Tag、其他 Reader、RFIF Watchdog 和后端系统等)通过远程测试方法查询 Reader 的 TPM 的安全信息,获得对其的可信认证,从而实施正确的安全策略.利用具有可信模块的读写器来确保具有私钥属性的标签的隐私.

方法的假设是:攻击者容易侵入或获得 Reader,但是不能破获或获得 TPM 的有关部门信息.因此,尽管攻击者获得了 Reader,但是由于无法获得其中的安全数据,因此依然无法和 Tag 通信.由于可信模块芯片会增加成本,技术实现难度大,因此,该方法实用性较低.

3.3 基于隐藏RFID标签的隐私保护技术

3.3.1 基于代理访问的方法

RFID 中代理技术(proxy based approach)的基本思路是:RFID 标签对 RFID 读写器的响应不依赖公用读写器,而是通过用户一个专有读写器来读取标签的信息[31].目前,实现代理技术的方法有两种:Watchdog Tag 和 RFID Guardian.

(1) Watchdog 技术

在 Watchdog 技术中,借助一个功能强大的 Watchdog 标签(Watchdog tag)来代替所有的标签响应读写器的访问请求[32].所谓 Watchdog Tag,就是对一般 Tag 的增强.具体来说,与一般的 Tag 不同,Watchdog Tag 具有以下功能:

- 额外的电源(如电池);
- 一个很小的监视屏;
- 较长距离的通信信道.

Watchdog Tag 的主要功能是:解码所有 Reader 对 Tag 的扫描命令,并将相关信息显示在监视屏上,供用户参考.同时,Watchdog 也提供日志和审计功能,以便于事后统计分析.更高级的 Watchdog Tag 甚至具备定位功能,从而可以定位恶意或者伪造的 Reader 读写器对标签的扫描.当然,Watchdog Tag 的功能也可以在 PDA 等移动终端上实现.

(2) RFID Guardian 技术

RFID Guardian 是一个集成的平台,通过它可以实现对用户隐私性和安全性的集中管理[33,34].具体来说,RFID Guardian 是集成在某个 RFID 设备(专用设备或者在 PDA 等移动终端中实现)中的一个监控软件,它负责监控 RFID Reader 对 RFID Tag 的访问.RFID Guardian 的主要功能包括审计(auditing)、密钥管理(key management)、访问控制(access control)和认证(authentication).

审计功能包括 Tag 扫描审计和 Tag 审计:Tag 扫描审计是指记录并分析 Reader 对 Tag 的扫描信息;而 Tag 审计是指对用户周围进行 Tag 扫描,并将存在的 Tag 及其信息进行记录分析.前者可防御非法 Reader 的信息获取,而后者可防御 Tag 植入攻击.所谓 Tag 植入攻击是指攻击者将设计好的 Tag 放置到用户或其物品中,从而实现对用户的位置跟踪.密钥管理是指实现对各种 RFID 功能(如认证、加密等)所需要的密钥的管理.访问控制是指 RFID Guardian 可以控制对 Tag 的访问,从而达到保护 Tag 的目的.认证是指 RFID Guardian 可以代理 Tag,实现与 Reader 等之间的复杂而安全的相互认证(如基于挑战-应答机制的认证协议等).通过 RFID Guardian 的代理认证,可以实现 Tag 的离线式认证(off-tag authentication),从而减少对 Tag 的要求,降低 Tag 成本.

其中,访问控制功能是主要功能,具体来说,RFID Guardian 的访问控制功能包括:

- 安全功能综合协调应用:通过控制使用多种安全手段(如 Hash 方法、对称加密方法等),甚至 GPS 定位、距离分析与控制等技术,实现综合防御策略;
- 上下文感知:通过对不同上下文环境的控制,实现不同的安全策略,从而满足用户的安全和隐私需求;
- Tag-Reader 的代理中介:RFID Guardian 可以代理 Tag 响应 Reader 的查询,从而可以通过代理转发、主

动注入、选择性注入等方法阻止 Reader 对 Tag 的访问.

3.3.2 基于距离测量的隐私保护方法

距离测量方法(distance measuring)[35,36]是 Intel 公司提出的一种方法,在该方法中,标签依据自己与读写器之间的距离,分别发送不同的信息以达到隐私保护的目的.距离测量的方法包括:

- 基于达到时间的三角分析法(triangulation via time-of-arrival analysis);
- 基于信号强度的三角分析法(triangulation via signal strength analysis);
- 噪声分析法(noise analysis).

基于距离测量的隐私保护方法的基本思路是:标签测量自己与 Reader 之间的物理距离,作为读写器可信性的度量值,并依据安全策略向不同距离的读写器发送不同的数据.例如,如果距离近,Tag 就发送更多的信息;相反,如果距离远,则可能发送少量信息.该方法的依据是,攻击者一般只能通过一定的距离实现对 Tag 的数据访问,而 Tag 的拥有者则一般通过短距离访问 Tag.

3.3.3 基于阻塞的隐私保护方法

阻塞方法(blocking approach)就是通过某种技术手段,妨碍 Reader 对 Tag 数据的访问.典型的方法包括阻塞器(blocker)方法、软阻塞(soft blocking)方法和主动干扰(active jamming)方法等[33,36−38].

(1) Blocker 技术

文献[37]提出的阻塞器就是一个类似于主动式 Tag 的设备,它可以模拟多个标签的功能,从而可以代理这些标签执行某些操作或者阻止 Reader 对这些 Tag 的访问.Blocker 方法包括全阻塞(full blocking)方法和选择性阻塞(selective blocking)方法,前者阻止 Reader 对所有 Tag 的访问,而后者可以选择性地阻止 Reader 对某些 Tag 的访问.一般而言,选择性阻塞较为实用.在选择性阻塞方法中,标签有两个状态:公开和私有,只有处于公开状态的标签才会响应读写器的扫描.为此,将需要保护的标签放入一个具有公开状态的标签的保护之下(后者称为阻止器:blocker).当读写器扫描时,Blocker 将向读写器发送相关信息,从而保护其他标签.为了使用受保护的标签,只需去除 Blocker 即可.Blocker 如何阻止读写器对其他标签的访问是一个关键问题,为此,可以将 Blocker 作为主动式标签并放置在 PDA 或智能手机中.

Blocker 方法可以结合二分树算法来进行,即,右边为 1,左边为 0.当 blocker 发现 reader 扫描处于 1 状态的 tag 时,则干扰正常的扫描.该方法存在的问题是,攻击者可以通过信号强弱等过滤掉 blocker.此外,blocker 干扰有可能失效.

(2) Soft Blocking 技术

软阻塞方法[38]的基本原理与阻塞器方式相同,但它采用软件或的方式模拟阻塞器的功能,从而实现控制 Reader 对 Tag 的访问.此外,软阻止方法与阻止方法其他不同之处在于:软阻塞方法可以只发送友好提示信息,告知读写器不可扫描标签.当然,软阻止方法依赖于对读写器扫描的审计.软阻塞技术由于实现简单,对 Tag 和 Reader 的要求低,因此目前来看,它是一种较为实用的解决方案.

(3) Active Jamming 技术

主动干扰方法用一个专用设备主动广播无线电波,从而完全干扰通信信道,防止 RFID 读写器的正常操作,其中最实用的是选择性干扰方法(selective RFID jamming)[33,39−42].主动干扰技术的基本实现过程是:

- RFID Reader 向 Tag 发送询问;
- 一个移动设备(mobile device)捕获并解码该询问,同时依据安全策略确定是否允许该访问;
- 如果该询问不允许访问,则移动设备发送干扰信号,干扰 Tag 的响应,从而破坏 Reader 对 Tag 的访问.

主动干扰技术要求干扰设备处理速度快,而且干扰能力要足够强.此外,还要防止攻击者检测出干扰信号而过滤掉干扰信号.

3.3.4 法拉第笼方法

法拉第笼(Faraday cage)方法是将带有标签的物体放置于用金属筛网或金属片组成的容器中,达到隔离的目的,从而可以放置无线电波穿透.从技术上来看,法拉第笼是一种理想的隐私保护方法.例如,如果用户有一个

附有 RFID 标签的钱包需要保护,则只需将该钱包放到一个具有法拉第信号屏蔽功能的装置中即可.但是,该方法也存在很多缺点.比如,放到具有法拉第笼功能的保护装置中可能影响用户的使用便利性,而且当用户需要保护的产品较多时,装置的便利性也是一个问题.

3.4 其他相关研究工作

RFID 隐私问题的根源之一在于阅读器和标签之间缺少认证.为此,通过提高 RFID 认证协议的安全性来保证 RFID 隐私,也是一种可行办法,相关工作可参见文献[43−50].但是,这种方法取决于认证协议的安全性,因此往往需要使用安全强度较高的密码算法.

文献[51]提出了一种前向隐私安全的 RFID 认证协议 SFP,协议的构造基于一种具有少量存储空间、能够计算伪随机数发生器和比特异或的标签.文献[52]采用部分 ID、CRC 校验以及 ID 动态更新的方法,提出一种新型 RFID 相互认证协议.该协议是一种典型的询问-响应认证协议,具有前向安全性,能够防止位置隐私攻击、重传攻击、窃听攻击和拒绝服务攻击.文献[53]对可扩展 RFID 认证方案、基于 Hash 函数的 RFID 双向认证协议、基于 SLPN 问题 MMR 协议进行了安全性分析.在此基础上,该文作者提出了一个基于 Hash 函数的可扩展双向认证方案,该方案能够满足受限后向隐私安全性,并可以抵御同步攻击.文献[54]分析了几种典型的 RFID 安全隐私保护方法的特点和局限,提出了一种新的方法——Key 值更新随机 Hash 锁.文献[55]以提高隐私保护能力和位置服务效率为目标,对 RFID 追踪系统中的隐私保护问题进行研究,分析了现有的位置隐私保护方法,通过对已有算法加以改进,设计了一种高效的不依赖于可信服务器的 RFID 位置隐私保护算法.文献[56]回顾了已有的各种 RFID 安全机制,重点介绍基于密码技术的 RFID 安全协议.

3.5 RFID隐私保护技术比较分析

现有 RFID 隐私保护技术在实现难易程度、成本、使用范围和隐私保护的有效性等方面各有优缺点,可根据实际需要选择具体的隐私保护方法.各种现有 RFID 隐私保护技术的比较见表 3.

Table 3 The comparions of exsiting technologies for RFID privacy protoction

表 3 各种现有 RFID 隐私保护技术的比较

隐私保护方法	技术难度	成本	实用范围	有效性
可移出式标签	小	低	小	差
可修改式标签	小	低	小	好
终止命令	小	低	小	好
口令保护的终止命令	小	低	小	好
支持睡眠命令	小	低	大	好
物理触发开关	中	中	小	好
去掉Tag标识符	中	中	小	好
随机重写标签信息	中	低	小	中
可写式标签	中	低	小	中
序列号分割	中	低	小	中
最小密码技术	大	高	大	好
加密	大	高	大	好
重加密	大	高	大	好
不可破坏加密	大	高	大	好
Hash Lock	中	中	大	好
随机化Hash Lock	中	中	大	好
Hash-Chain	大	高	大	好
可信计算	大	高	小	好
Watchdog	大	高	小	强
RFID Guardian	大	高	小	强
距离测量	大	高	小	中
阻塞	大	高	小	强
软阻塞	大	高	小	强
主动干扰	大	高	小	强
法拉第笼	中	高	小	强

4 总结与展望

处理能力受限、无线数据读取以及 RFID 标签标识符的唯一性等因素,决定了 RFID 隐私问题的必然性.本文对罗列攻击和跟踪攻击的各种方式进行了简要介绍,目的是明确 RFID 潜在的隐私威胁.虽然目前针对 RFID 隐私的解决方法已有很多,但是从技术实现难度、成本、使用范围以及解决隐私威胁的有效性等方面来看,尚缺少一种行之有效的方法.

从 RFID 隐私及其防御技术的发展来看,在后续研究工作中以下几个问题值得重视.

(1) 研制具有隐私保护功能的低成本标签.

目前,RFID 所面临的隐私威胁的根源在于:RFID 标签低成本和小体积制约了各种安全技术的实现,从而无法提供隐私保护功能.因此,解决 RFID 隐私问题需要首先从提高 RFID 标签的隐私保护入手.比如,如果 RFID 标签能够实现 DES 等对称加密算法,则可以采用目前成熟的隐私保护方法和具有隐私保护功能的安全协议,从而大大减少 RFID 面临的隐私威胁.

因此,研究适合于 RFID 的轻量级加密解密算法和相应的隐私保护协议,并结合超大规模集成电路技术设计和制造具有隐私保护功能的低成本 RFID 标签,是未来开展隐私防御技术研究的重要方向.

(2) 针对特定应用的 RFID 隐私保护技术.

随着 RFID 技术的应用推广,在物流、商品销售、供应链管理等领域都会涉及 RFID 隐私问题.但是,不同领域所采用的 RFID 技术不尽相同,因此其面临的隐私威胁也各有不同.例如:在服装制造业,主要用户是消费者个人,因此主要隐私威胁主要是个人的喜爱偏好等信息;相反,在物流领域,用户主要是企业,因此其隐私威胁主要是关于企业的库存、产品运输过程等敏感信息.显然,针对个人和针对企业的隐私威胁有着本质的不同,因此所采取的隐私防御方法也有所不同.为此,针对应用领域的隐私保护需求,研究不同的隐私保护方法,也是未来 RFID 隐私保护技术研究的重要方向.

(3) RFID 隐私威胁检测设备和工具.

在大规模 RFID 应用中,是否存在 RFID 隐私问题必须依赖可靠的技术检测手段.与攻击威胁检测相似,研究 RFID 隐私威胁检测技术和工具,可以对信息或系统所面临的 RFID 隐私问题进行提前检测.与网络安全领域的隐私检测不同,RFID 隐私检测必须基于 RFID 技术,因此,诸如目前已经出现的 RFID Watchdog 和 RFID Guardian 等综合检测系统,在未来具有广泛的应用前景.当然,考虑到 RFID 标准的不同,未来的 RFID 隐私检测装置应该是多功能、综合性的安全防御平台.

(4) 便携式 RFID 隐私保护装置.

个人隐私威胁是目前和未来很长时间内 RFID 隐私威胁的主要内容.随着成本的不断降低和体积的不断缩小,未来 RFID 技术在服装制造、个人饰品等领域具有广泛的应用前景.个人佩戴和穿戴物采用 RFID 技术后,必将导致个人隐私面临巨大威胁.法拉第笼成本低、便于携带,因此是解决单个 RFID 物品隐私威胁的较好的方法.但是,基于法拉第笼的隐私保护方法不适合大量 RFID 物品.而类似于 RFID Guardian 的隐私保护装置虽然可以同时保护多个 RFID 标签,但是体积大、成本高,不便于携带,不适合于个人隐私保护.因此,研究便携式个人 RFID 隐私保护装置,具有广泛的市场应用前景.

(5) RFID 安全综合解决方法.

本文主要讨论隐私威胁问题,而 RFID 还存在窃听、拒绝服务等安全威胁问题.隐私问题和安全问题是 RFID 中相互关联的问题,因此,研究 RFID 隐私和安全的综合解决技术,是未来 RFID 隐私技术研究的重要内容.

总之,RFID 技术所引发的隐私威胁问题越来越突出,现有方法尚不能很好地解决 RFID 隐私问题,开展 RFID 隐私保护技术研究工作,对于促进 RFID 技术的应用具有重要意义.

References:

[1] Grover A, Berghel H. A survey of RFID deployment and security issues. Journal of Information Processing Systems, 2001,7(4): 561−580.

[2] Rieback MR, Crispo B, Tanenbaum AS. The evolution of RFID security. IEEE Pervasive Computing, 2006,5(1):62−69. [doi: 10.1109/MPRV.2006.17]

[3] Juels A. RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communication, 2006,24(2):381−394. [doi: 10.1109/JSAC.2005.861395]

[4] Langheinrich M. A survey of RFID privacy approaches. Personal and Ubiquitous Computing, 2009,13(6):413−421. [doi: 10.1007/s00779-008-0213-4]

[5] Garcia-Alfaro J, Barbeau M, Kranakis E. Security threat mitigation trends in low-cost RFID systems. Lecture Notes in Computer Science, 2010,5939:193−207. [doi: 10.1007/978-3-642-11207-2_15]

[6] Hermans J, Peeters R, Preneel B. Proper RFID privacy: Model and protocols. IEEE Trans. on Mobile Computing, 2014,13(12):2888−2902. [doi: 10.1109/TMC.2014.2314127]

[7] Klitou D. Human-Implantable microchips: Location-Awareness and the dawn of an “Internet of Persons”. Information Technology and Law Series, 2014,25:157−249. [doi: 10.1007/978-94-6265-026-8_7]

[8] Karjoth G, Moskowitz PA. Disabling RFID tags with visible confirmation: Clipped tags are silenced. In: Proc. of the 2005 ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2005. 27−30. http://doi.acm.org/10.1145/1102199.1102205 [doi: 10.1145/1102199.1102205]

[9] Vahedi E, Shah-Mansouri V, Wong VWS, Blake IF, Ward RK. Probabilistic analysis of blocking attack in RFID systems. IEEE Trans. on Information Forensics and Security, 2011,6(3):803−817. [doi: 10.1109/TIFS.2011.2132129]

[10] Mitrokotsa A, Rieback MR, Tanenbaum AS. Classifying RFID attacks and defenses. Information Systems Frontiers, 2010,12(5):491−505. [doi: 10.1007/s10796-009-9210-z]

[11] Danev B, Heydt-Benjamin TS, Čapkun S. Physical-Layer identification of RFID devices. In: Proc. of the 18th Conf. on USENIX Security Symp. Berkeley: USENIX Association, 2009. 199−214. https://www.usenix.org/legacy/events/sec09/tech/full_papers/danev.pdf

[12] Zanetti D, Sachs P, Capkun S. On the practicality of UHF RFID fingerprinting: How real is the RFID tracking problem? Lecture Notes in Computer Science, 2011,6794:97−116. [doi: 10.1007/978-3-642-22263-4_6]

[13] Danev B, Capkun S, Masti RJ, Benjamin TS. Towards practical identification of HF RFID devices. ACM Trans. on Information and System Security, 2012,15(2):1−24. [doi: 10.1145/2240276.2240278]

[14] Zanetti D, Danev B, Capkun S. Physical-Layer identification of UHF RFID tags. In: Proc. of the 16th Annual Int’l Conf. on Mobile Computing and Networking. New York: ACM Press, 2010. 353−364. http://doi.acm.org/10.1145/1859995.1860035 [doi: 10.1145/1859995.1860035]

[15] Inoue S, Yasuura H. RFID privacy using user-controllable uniqueness. In: Proc. of the RFID Privacy Workshop. MIT, 2003. 1−7.

[16] van Deursen T, Radomirović S. Insider attacks and privacy of RFID protocols. Lecture Notes in Computer Science, 2012,7163:91−105. [doi: 10.1007/978-3-642-29804-2_6]

[17] Kurkovsky S, Syta E, Casano B. Continuous RFID-enabled authentication: Privacy implications. IEEE Technology and Society Magazine, 2011,30(3):34−41. [doi: 10.1109/MTS.2011.942306]

[18] Good N, Han J, Miles E, Molnar D, Mulligan D, Quilter L, Urban J, Wagner D. Radio frequency identification and privacy with information goods. In: di Vimercati SDC, Syverson P, eds. Proc. of the Workshop on Privacy in the Electronic Society. 2004. 41−42. [doi: 10.1145/1029179.1029193]

[19] Juels A. Minimalist cryptography for low-cost RFID tags. Lecture Notes in Computer Science, 2005,3352:149−164. [doi: 10.1007/978-3-540-30598-9_11]

[20] Langheinrich M, Marti R. Practical minimalist cryptography for RFID privacy. IEEE Systems Journal, 2007,1(2):115−128. [doi: 10.1109/JSYST.2007.907683]

[21] Fabian B, Ermakova T, Muller C. SHARDIS: A privacy-enhanced discovery service for RFID-based product information. IEEE Trans. on Industrial Informatics, 2012,8(3):707−718. [doi: 10.1109/TII.2011.2166783]

[22] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. Lecture Notes in Computer Science, 2004,3156:357−370. [doi: 10.1007/978-3-540-28632-5_26]

[23] Hoepman JH, Joosten R. Practical schemes for privacy and security enhanced RFID. Lecture Notes in Computer Science, 2010,6033:138−153. [doi: 10.1007/978-3-642-12368-9_10]

[24] Fishkin KP, Roy S, Jiang B. Some methods for privacy in RFID communication. Lecture Notes in Computer Science, 2005,3313:42−53. [doi: 10.1007/978-3-540-30496-8_5]

[25] Lim CH, Korkishko T. mCrypton—A lightweight block cipher for security of low-cost RFID tags and sensors. Lecture Notes in Computer Science, 2006,3786:243−258. [doi: 10.1007/11604938_19]

[26] Avoine G. Privacy issues in RFID banknote protection schemes. In: Paradinas P, Deswarte Y, Kadam AAE, eds. Proc. of the IFIP Int'l Federation for Information Processing, Vol.153. 2004. 33−48. [doi: 10.1007/1-4020-8147-2_3]

[27] Golle P, Jakobsson M, Juels A, Syverson P. Universal re-encryption for mixnets. Lecture Notes in Computer Science, 2004,2964: 163−178. [doi: 10.1007/978-3-540-24660-2_14]

[28] Saito J, Ryou JC, Sakurai K. Enhancing privacy of universal re-encryption scheme for RFID tags. Lecture Notes in Computer Science, 2004,3207:879−890. [doi: 10.1007/978-3-540-30121-9_84]

[29] Henrici D, Müller P. Hash-Based enhancement of location privacy for radiofrequency identification devices using varying identifiers. In: Sandhu R, Thomas R, eds. Proc. of the 2nd IEEE Annual Conf. on Pervasive Computing and Communications Workshops. IEEE, 2004. 149−153. [doi: 10.1109/PERCOMW.2004.1276922]

[30] Molnar D, Soppera A, Wagner D. Privacy for RFID through trusted computing. In: di Vimercati SDC, Dingledine R, eds. Proc. of the 2005 ACM Workshop on Privacy in the Electronic Society. ACM Press, 2005. 31−34. [doi: 10.1145/1102199.1102206]

[31] Juels A, Syverson P, Bailey D. High-Power proxies for enhancing RFID privacy and utility. In: Danezis G, Martin D, eds. Proc. of the Privacy Enhancing Technologies. Berlin, Heidelberg: Springer-Verlag, 2006. 210−226. [doi: 10.1007/11767831_14]

[32] Metzger C, Flörkemeier C, Bourquin P, Fleisch E. Making radio frequency identification visible—A Watchdog tag. In: Proc. of the Pervasive Computing and Communications Workshops. New York: IEEE, 2007. 352−356. [doi: 10.1109/PERCOMW.2007.63]

[33] Rieback MR, Crispo B, Tanenbaum AS. Keep on blockin' in the free world: Personal access control for low-cost RFID tags. In: Proc. of the 13th Int'l Workshop on Security Protocols. Berlin, Heidelberg: Springer-Verlag, 2007. 51−59. [doi: 10.1007/978-3-540-77156-2_6]

[34] Rieback M, Crispo B, Tanenbaum A. RFID guardian: A battery-powered mobile device for RFID privacy management. In: Proc. of the Australasian Conf. on Information Security and Privacy. Berlin, Heidelberg: Springer-Verlag, 2005. 184−194. [doi: 10.1007/11506157_16]

[35] Liu XL, Qi H, Li KQ, Wu J, Xue WL, Min GY, Xiao B. Efficient detection of cloned attacks for large-scale RFID Systems. Lecture Notes in Computer Science, 2014,8630:85−99. [doi: 10.1007/978-3-319-11197-1_7]

[36] Carluccio D, Kasper T, Paar C. Implementation details of a multi purpose ISO 14443 RFID-tool. In: Proc. of the Workshop on RFID Security. 2006. 1−12. http://citeseerx.ist.psu.edu/showciting?cid=6668645

[37] Juels A, Rivest RL, Szydlo M. The blocker tag: Selective blocking of RFID tags for consumer privacy. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2003. 103−111. [doi: 10.1145/948109.948126]

[38] Juels A, Brainard J. Soft blocking: Flexible blocker tags on the cheap. In: di Vimercati SDC, Syverson P, eds. Proc. of the Workshop on Privacy in the Electronic Society. 2004. 1−7. [doi: 10.1145/1029179.1029181]

[39] Rieback M, Crispo B, Tanenbaum A. Is your cat infected with a computer virus? In: Proc. of the 4th Annual IEEE Int'l Conf. on Pervasive Computing and Communications. New York: IEEE, 2006. 10−20. [doi: 10.1109/PERCOM.2006.32]

[40] Rieback M, Gaydadjiev G, Crispo B, Hofman R, Tanenbaum A. A platform for RFID security and privacy administration. In: Proc. of the 20th Large Installation System Administration Conf. Washington: USENIX Association, 2006. 89−102. https://www.usenix.org/legacy/events/lisa06/tech/rieback/rieback.pdf

[41] Zhang YL, Guo H. An improved RFID privacy protection scheme based on Hash-chain. In: Proc. of the 2010 Int'l Conf. on Logistics Engineering and Intelligent Transportation Systems (LEITS). 2010. 1−4. [doi: 10.1109/LEITS.2010.5665033]

[42] Nithyanand R, Tsudik G, Uzun E. Readers behaving badly: Reader revocation in PKI-based RFID systems. Lecture Notes in Computer Science, 2010,6345:19−36. [doi: 10.1007/978-3-642-15497-3_2]

[43] Alavi SM, Baghery K, Abdolmaleki B. Security and privacy flaws in a recent authentication protocol for EPC C1 G2 RFID tags. Advances in Computer Science: An Int'l Journal, 2014,3(5):44−52.

[44] Li N, Mu Y, Susilo W, Guo FC, Varadharajan V. Privacy-Preserving authorized RFID authentication protocols. Lecture Notes in Computer Science, 2014,8651:108−122. [doi: 10.1007/978-3-319-13066-8_7]

[45] Qian XF, Liu XB, Yang SL, Zuo C. Security and privacy analysis of tree-LSHB+ protocol. Wireless Personal Communications, 2014,77:3125−3141. [doi: 10.1007/s11277-014-1699-x]

[46] Niu B, Zhu XY, Chi HT, Li H. Privacy and authentication protocol for mobile RFID systems. Wireless Personal Communications, 2014,77:713−3131. [doi: 10.1007/s11277-014-1605-6]

[47] Shen J, Zheng WY, Wang J, Xia ZH, Fu ZJ. Study of the privacy models in RFID authentication protocols. Int'l Journal of Security and its Applications, 2013,7(6):346−354.

[48] Avoine G, Bingöl MA, Carpent X, Yalcin SBO. Privacy-Friendly authentication in RFID systems: On sub-linear protocols based on symmetric-key cryptography. IEEE Trans. on Mobile Computing, 2013,12(10):2037−2049. [doi: 10.1109/TMC.2012.174]

[49] Sadikin MF, Kyas M. Security and privacy protocol for emerging smart RFID applications. In: Proc. of the 15th IEEE/ACIS Int'l Conf. on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Atlanta: IEEE Computer Society, 2014. 1−7. [doi: 10.1109/SNPD.2014.6888694]

[50] Luo YJ, Jiang JG, Wang SY, Jing X, Ding C, Zhang ZJ, Zhang YF. Filtering and cleaning for RFID streaming data technology based on finite state machine. Ruan Jian Xue Bao/Journal of Software, 2014,25(8):1713−1728. http://www.jos.org.cn/1000-9825/4666.htm [doi: 10.13328/j.cnki.jos.004666]

[51] Ma CS. Low cost RFID authentication protocol with forword privacy. Chinese Journal of Computers, 2011,34(8):1377−1398 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.01387]

[52] Zhang H, Hou ZH. Wang DH. A new security and privacy on RFID mutual authentication protocol based on partial ID. Journal of Electronics & Information Technology, 2009,31(4):852−856 (in Chinese with English abstract).

[53] Wang SH, Liu SJ, Chen DW. Scalable RFID mutual authentication protocol with backward privacy. Journal of Computer Research and Development, 2013,50(6):1276−1383 (in Chinese with English abstract).

[54] Zeng LH, Xiong Z, Zhang T. Key value renewal random hash lock for security and privacy enhancement of RFID. Computer Engineering, 2007,33(3):152−159 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-3428.2007.03.055]

[55] Wu TT, Li LJ. Study on RFID-oriented location privacy protection algorithm. Computer Technology and Development, 2013,23(1):157−160 (in Chinese with English abstract). [doi: 10.3969/j.issn.1673-629X.2013.01.039]

[56] Zhou YB, Feng DG. Design and analysis of cryptographic protocols for RFID. Chinese Journal of Computers, 2006,29(4):581−589 (in Chinese with English abstract).

附中文参考文献:

[50] 罗元剑,姜建国,王思叶,景翔,丁昶,张珠君,张艳芳.基于有限状态机的 RFID 流数据过滤与清理技术.软件学报,2014,25(8):1713−1728 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4666.htm [doi: 10.13328/j.cnki.jos.004666]

[51] 马昌社.前向隐私安全的低成本 RFID 认证协议.计算机学报,2011,34(8):1377−1398. [doi: 10.3724/SP.J.1016.2011.01387]

[52] 张辉,侯朝焕,王东辉.一种基于部分 ID 的新型 RFID 安全隐私相互认证协议.电子与信息学报,2009,31(4):852−856.

[53] 王少辉,刘素娟,陈丹伟.满足后向隐私的可扩展 RFID 双向认证方案.计算机研究与发展,2013,50(6):1276−1383.

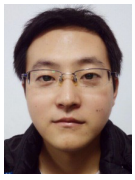
[54] 曾丽华,熊璋,张挺.Key 值更新随机 Hash 锁对 RFID 安全隐私的加强.计算机工程,2007,33(3):152−159. [doi: 10.3969/j.issn.1000-3428.2007.03.055]

[55] 吴婷婷,李玲娟.面向 RFID 的位置隐私保护算法研究.计算机技术与发展,2013,23(1):157−160. [doi: 10.3969/j.issn.1673-629X.2013.01.039]

[56] 周永彬,冯登国.RFID 安全协议的设计与分析.计算机学报,2006,29(4):581−589.

周世杰(1970－),男,四川荣县人,博士,教授,CCF 高级会员,主要研究领域为网络安全,射频识别,分布式计算,交通仿真.

罗嘉庆(1983－),男,博士,副教授,CCF 会员,主要研究领域为 RFID,分布式计算.



张文清(1989－),男,硕士生,CCF 学生会员,主要研究领域为 RFID,网络安全.