密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2015,2(1):40–53

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

物联网安全关键技术与挑战*

武传坤

中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093
通讯作者: 武传坤, E-mail: ckwu@iie.ac.cn

摘 要: 物联网是信息技术发展到一定阶段的产物, 是全球信息产业和技术的又一次飞跃. 物联网的发展非常迅速, 市场潜力巨大. 同时, 物联网的信息安全问题是关系物联网产业能否安全可持续发展的核心技术之一, 必须引起高度重视. 本文首先分析了物联网安全研究的背景和意义, 介绍了国内外在物联网方面的发展情况和重视程度, 阐述了国内的技术短板, 国家对物联网技术和产业的支持等情况, 然后基于大家熟知的物联网三层逻辑架构, 分析了物联网的安全架构, 并侧重感知层安全和应用层安全, 分析了需要研究的一些研究方向和关键技术, 并对这些技术的本质、关键问题进行了分析. 在物联网的感知层, 本文指出轻量级安全是其需求特点, 也是最主要的技术挑战, 轻量级安全技术包括轻量级密码算法和轻量级安全协议. 在物联网的应用层, 本文指出隐私保护、移动终端设备安全、物联网安全基础设施和物联网安全测评体系是关键技术. 对物联网传输层安全和处理层安全的关键技术, 本文将其分别归为网络安全和云计算安全领域, 不属于物联网专有的安全技术, 从而未作深入探讨.

关键词: 物联网; 安全架构; 信息安全
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13686/j.cnki.jcr.000059

中文引用格式: 武传坤. 物联网安全关键技术与挑战[J]. 密码学报, 2015, 2(1): 40–53.
英文引用格式: Wu C K. An overview on the security techniques and challenges of the Internet of things[J]. Journal of Cryptologic Research, 2015, 2(1): 40–53.

An Overview on the Security Techniques and Challenges of the Internet of Things

WU Chuan-Kun

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences Institute of Software Chinese Academy of Sciences, Beijing 100093, China
Corresponding author: WU Chuan-Kun, E-mail: ckwu@iie.ac.cn

Abstract: Internet of Things (IOT) is the outcome of the development of information technology, and is a new scientific, technological, and economical wave of worldwide information technology enterprises. In the meantime, the information security of the IOT is one of the core technologies that will influence the long-term development of the IOT, and much attention should be paid on it. This paper first analyses the background and significance of the security research in IOT, introduces the national development and level of recognition of IOT, analyses the technical shortages we are facing at, and describes the government support to the IOT technology and industry.

* 基金项目: 中国科学院先导专项子课题“海云信息安全体系研究”(XDA06010701); 中科院信息工程所密码专向基金项目“面向物联网终端的轻量级安全认证协议”(Y4Z0061102)
收稿日期: 2014-12-03 定稿日期: 2015-02-01

Then based on the well-known three-layer architecture of IOT, presents a security architecture of IOT, and by focusing on the sensor layer security and application layer security, this paper analyses some research directions and key techniques that need to be further studied, and indicates the essence and key problems of these techniques. This paper indicates that, in the sensor layer of IOT, lightweight security techniques, including lightweight cryptographic algorithms and lightweight security protocols, are what in practical need and are also the main technical challenges. In the application layer of IOT, privacy protection, mobile device security, IOT security infrastructure, as well as IOT security evaluation systems are the key techniques. With respect to the transmission layer security and processing layer security of IOT, this paper treats them as enhanced network security and cloud computing security respectively, and should not be treated as specific security techniques for IOT, hence they are not addressed in depth in this paper.
Key words: Internet of things; security architecture; information security

1 引言

物联网是建立在互联网基础上的泛在网络发展的一个新阶段, 它可以通过各种有线和无线网络与互联网融合, 综合应用海量的传感器、智能处理终端、全球定位系统等, 实现物与物、物与人的随时随地连接, 实现智能管理和控制. 物联网引领了信息产业革命的第三次浪潮, 将成为未来社会经济发展、社会进步和科技创新的最重要的基础设施, 也关系到国家在未来对一些物理设施的安全利用和管控.

在信息技术第一次浪潮, 即电脑时代, 人们的脑力劳动被解放出来, 那时我们国家的技术水平远远落后于欧美发达国家; 在信息技术的第二次浪潮, 即互联网时代, 信息的异地共享成为可能, 那时我们国家的技术水平紧跟欧美发达国家; 今天面临的物联网时代, 将虚拟空间与现实物理空间相结合, 被认为是信息技术发展的第三次浪潮, 我们国家站在与欧美发达国家相同的起点, 只有奋起向前, 才能站在世界前列, 在国际学术技术和产业领域争得更大的话语权.

2012 年 2 月 14 日, 工业和信息化部发布了《物联网“十二五”发展规划》. 该文件显示, 我国物联网在安防、电力、交通、物流、医疗、环保等领域已经得到应用. 易观国际数据表明, 2010 年物联网在安防、交通、电力和物流领域的市场规模分别为 600 亿元、300 亿元、280 亿元和 150 亿元, 预计在今后 5–10 年将出现大规模增长.

虽然物联网发展日趋迅猛, 但物联网的安全问题却日趋突出(特别是当物联网与工业控制将结合时). 一个典型的案例是震网病毒(Stuxnet), 它是第一个专门攻击工业控制中基础设施(如发电站和工厂)的病毒, 震网病毒以蠕虫的形式在互联网扩散, 并重点扩散到 U 盘上, 一旦移动介质放入到工业控制网中, 就寻找西门子的 WINCC 系统并加以感染, 一旦感染, 就可以在 PLC 管理员没有察觉的情况下, 修改发送至 PLC 或从 PLC 返回的数据. 震网病毒攻击了伊朗在纳坦兹的浓缩铀工厂, 造成伊朗约 20%的离心机(1000 多台)失控、报废, 导致发电计划推迟. 2011 年年末发生的一系列网络信息泄露事件表明, 信息安全所面临的威胁比我们许多人想象的要严重得多, 这也是国家近年来大力支持信息安全技术研究的根本原因.

对物联网市场飞速发展和物联网安全问题日益严重的矛盾, 物联网安全将会面临哪些技术问题和挑战, 我们又将如何应对这些挑战? 从物联网的架构可以看到, 典型的物联网系统包括感知层、传输层和处理应用层. 本文将从物联网架构方面讨论物联网安全的关键技术和挑战.

2 物联网安全的研究背景及意义

物联网产业是融合了现有信息化技术广泛应用技术, 需要更多的产学研机构参与. 同时, 物联网产业的发展主要是以应用来推动的, 需要发挥政府各个部门的积极性, 明确产业方向, 引导市场需求, 并从政策上给予扶持, 鼓励各种类型的企业积极投入研发、生产和运营.

我国政府一直高度重视信息化建设, 很早就提出以信息化带动工业化, 通过全面提高我国信息化水

平, 实现产业升级和经济增长方式转变. 早在国家“十一五”规划中, 就已经对宽带无线通信网络、传感网、编码中等物联网涵盖的一些问题做了相关部署. 近年来, 党和国家领导人更充分认识到以物联网为主要内容的新一次信息化浪潮的迅猛发展, 适时果断提出要加快发展我国物联网产业发展, 相关政府部门对有关问题迅速做出部署. 2009年8月7日, 国务院总理温家宝在无锡视察中科院物联网技术研发中心时指出, 要尽快突破核心技术, 将物联网产业发展上升到战略性新兴产业的高度. 2009 年 9 月 11 日, 中国传感网标准工作组正式成立, 该工作组将聚集国内物联网主要技术力量, 制定国家标准, 积极参与国际标准提案工作, 促进国内外物联网业界同行的交流和合作, 通过标准为产业发展奠定坚实基础, 提升中国在物联网领域的国际竞争力. 11 月 3 日, 国务院指出要着力突破传感网、物联网关键技术. 随后在 12 月 11 日, 工信部开始统筹部署宽带普及、三网融合、物联网及下一代互联网发展, 将加快培育物联网产业列为我国信息产业发展的三大重要目标, 制定技术产业发展规划和应用推进计划, 推动发展关键传感器件、装备、系统及服务. 2011 年 11 月 28 日, 工业和信息化部发布了《物联网“十二五”发展规划》, 进一步明确了国家在“十二五”期间在物联网方面的发展目标. 《规划》指出, 要大力攻克核心技术, 加快构建标准体系, 协调推进产业发展, 着力培育骨干企业, 积极开展应用示范, 合理规划区域布局, 加强信息安全保障, 提升公共服务能力. 需要说明的是, 《规划》将信息安全保障作为一个专门任务予以重视, 其内容包括加强物联网安全技术研发, 建立并完善物联网安全保障体系, 加强网络基础设施安全防护建设. 2013 年 9 月, 国家发展改革委、工业和信息化部等 10 多个部门, 以物联网发展部际联席会议的名义印发了顶层设计、标准制定、技术研发、应用推广、产业支撑、商业模式、安全保障、政府扶持措施、法律法规保障、人才培养十个物联网发展专项行动计划, 为后续有计划、有进度、有分工地落实相关工作, 切实促进物联网健康发展明确了方向目标和具体举措.

各部委也积极响应国家号召, 制定相关政策积极推动物联网发展, 通过设立专项资金, 为物联网应用示范工程、技术研发与产业化项目提供大力支持. 发改委自 2011 年起先后启动了 28 项国家物联网重大应用示范工程, 2013 年 10 月份又发布了《国家发展改革委办公厅关于组织开展 2014–2016 年国家物联网重大应用示范工程区域试点工作的通知》. 财政部会同工业和信息化部设立了物联网发展专项资金, 自 2011 年起累计安排物联网专项资金 15 亿元, 陆续支持了 500 多个研发项目, 重点对企业为主体的物联网技术研发和产业化项目进行扶持. 科技部支持组建了物联网产业技术创新战略联盟. 国家标准委联合国家发展改革委支持成立了物联网国家标准基础工作组和 5 个行业应用标准工作组. 公安部、农业部等部门和部分中央企业实施了一批重大应用示范工程. 多个地方政府加大投入力度, 出台地方规划和行动方案, 建立协同推进机制, 积极推广物联网应用, 取得了积极成效.

在中央政府和各部门的大力推动下, 各地方政府积极响应. 无锡、北京、上海、深圳、杭州、南京、广州等东部沿海城市纷纷开始规划自己的物联网城市蓝图, 正在制定或者已经制定了产业发展的推动策略和规划, 大力推进物联网产业发展. 其中, 上海较早在全国成立了 RFID 与物联网产业联盟, 目前上海正在着手物联网产业发展规划制定工作, 初步选定交通、安防、农业、医疗卫生、商贸、物流、环保、电网等八大行业开展示范应用, 以产业园区和社区应用为载体, 分阶段、分领域推进物联网产业发展; 北京提出以传感器、传输网络、集成服务三大领域为核心, 成为产业链和产业支持, 并以应用为先导, 推动物联网在政府、社会和企业三大领域的应用, 打造“感知北京”, 通过物联网的逐步实现与完善, 推进无线城市向智慧北京的演进, 打造以首都为核心得物联网中心, 辐射全国, 逐渐形成系统化, 规模化和产业化, 并成立了物联网产业联盟, 促进物联网协同创新和应用; 江苏省已将物联网列为六大新兴产业之一, 并在无锡成立了物联网国家示范区和技术研发中心, 旨在统一打造物联网技术研发、项目孵化、产业化及商业应用的完整产业链, 促进物联网技术研发和产业化进程, 加快将无锡建成国内首个“感知城市”, 将江苏建成国内首个“智慧之省”; 深圳也在着手物联网产业相关研究和规划, 打造“智慧深圳”. 尽管从整体水平看, 中西部地区由于信息产业基础条件薄弱, 物联网发展相对落后, 但以重庆为代表的中西部城市也在积极打造物联网.

在温总理提出“感知中国”后, 各级政府在抓紧推动在政府管理、社会服务和企业应用等领域的示范工程. 2009 年工业和信息化部信息化推进司就重点推进了基于 TD 的电梯监控、车辆监控和企业安全监控等 M2M 试点应用. 从各地情况看, 智能交通、智能电网、智能物流、智能安防、智能物流、环境监测等领域的示范应用在北京、上海、江苏、浙江、广东等省市已初步展开. 2008 年, 围绕科技奥运, 中关村下一代互联网产业联盟及相关企业在全球首次实现将“物联网”和 IPv6 技术全面服务于奥运会, 城市网格管理、视频监控、智能交通、食品溯源、水质检测、IPV6 奥运网站等方面的成功运用在国内外产生重大影响; 上海已经在世博会和浦东机场布置防入侵传感网, 成为国际上规模较大的物联网应用系统, 世博园还在新能源接入、储能、电动汽车充放电, 以及智能小区等方面建立了综合示范工程; 无锡除了已将传感技术应用在太湖水质监测系统中, 还将在新区的太科园建一个传感网应用体验式主题公园, 并启动建设无锡机场防入侵传感网络系统、机场安检、市民中心、新区综合保税区的应用示范工程, 物联网技术的市场化应用明显加快; 浙江嘉兴已正在试点智能传感网车辆管理系统, 主要用于交通控制; 宁波港也积极开展物联网相关应用, 如给进港汽车贴上电子车牌、在港口和车辆上布置传感器, 以实现“智慧物流”.

物联网系统在建设初期, 由于规模有限, 各个物联网示范区之间相对独立, 还不能构成真正意义的互联互通, 因此面临的信息安全威胁也小. 随着物联网系统数量的增多和规模的增大, 特别是随着这些物联网应用系统的互联互通, 以及服务于这些系统的数据处理平台的集中管理, 物联网安全问题将逐渐显现, 而且会以雪崩效应影响到物联网行业, 到时候“亡羊补牢”将为时太晚, 甚至无法弥补, 就像今天我们的工业控制系统在应对信息安全问题方面的无助局面.

3 国际研究现状及发展趋势

物联网的概念的提出有多种途径, 但最早以物联网为题的年度报告是 ITU2005 年的年度报告[1]. 物联网的概念提出之后, 很多学术研究也很快在该领域开展, 仅在 2008 年, 就出现了物联网专题国际学术会议[2]、专著[3]和系列研究论文[4]等.

随着信息技术日新月异, 特别是信息采集、传输技术及高性能计算机的迅速发展和互联网与移动通信网的广泛应用, 大规模发展传感网及相关产业的时机日趋成熟, 欧美等发达国家将物联网视为未来发展的重要领域. 2009 年以来, 美欧日等发达国家纷纷提出物联网发展的战略、规划、核心技术及产业重点, 促进物联网产业迅速发展, 以在新一轮的信息化浪潮中占得先机. 2008 年, 美国提出“智慧地球”的概念, 随后在 2009 年, 欧盟提出了“物联网行动计划”, 日本提出“i-Japan”计划, 韩国在“ u -Korea”战略的基础上, 提出了“物联网基础设施构建基本规划”. 不难看出, 许多国家在物联网领域的投入和重视程度都是很大的.

在物联网安全相关方面, 也有很多相关的研究成果. 但由于物联网在架构上是一个新的信息技术模式, 物联网安全技术在产业方面的应用还很不够. 我们首先从不同侧面了解一下国际学术研究进展情况.

(1) 物联网安全体系方面

物联网将经济社会活动、战略性基础设施资源和人们的日常生活全面架构在全球互联互通的网络上, 所有活动和设施理论上透明化, 一旦遭受攻击, 安全和隐私将面临巨大威胁, 甚至可能引发电网瘫痪、交通失控、工厂停产等一系列恶性后果. 因此实现信息安全和网络安全是物联网大规模应用的必要条件, 也是物联网应用系统成熟的重要标志.

物联网的安全形态主要体现在其体系结构的各个要素上. 第一是物理安全, 主要是传感器的安全, 包括对传感器的干扰、屏蔽、信号截获等, 是物联网安全特殊性的体现; 第二是运行安全, 存在于各个要素中, 涉及到传感器、传输系统及处理系统的正常运行, 与传统信息系统安全基本相同; 第三是数据安全, 也是存在于各个要素中, 要求在传感器、传输系统、处理系统中的信息不会出现被窃取、被篡改、被伪造、被抵赖等性质. 其中传感器与传感网所面临的安全问题比传统的信息安全更为复杂, 因为传感器与传感网可能会因为能量受限的问题而不能运行过于复杂的保护体系. 因此, 物联网除面临一般信息网络所具有的

安全问题外, 还面临物联网特有的威胁和攻击, 相关威胁如下: 物理俘获、传输威胁、自私性威胁、拒绝服务威胁、感知数据威胁; 相关攻击包括: 阻塞干扰、碰撞攻击、耗尽攻击、非公平攻击、选择转发攻击、陷洞攻击、女巫攻击、洪泛攻击、信息篡改等. 相关安全对策包括: 加密机制和密钥管理、感知层鉴别机制、安全路由机制、访问控制机制、安全数据融合机制、容侵容错机制. 由上可知, 虽然一些工作对物联网的特点、相关威胁与攻击进行了分类, 但是目前还没有支持形式验证的物联网安全体系构架, 显然支持形式验证安全构架是保障安全的重要基础.

国际上, 意大利 Sapienza 大学的 C.M. Medaglia 和 A. Serbanati 在文献[5]中指出物联网在用户隐私和信息安全传输机制中存在诸多不足: 如标签被嵌入任何物品, 用户在没有察觉的情况下其标签被阅读器扫描, 通过对物品的定位可追踪用户的行踪, 使个人隐私遭到破坏; 物品的详细信息在传输过程中易受流量分析、窃取、嗅探等网络攻击, 导致物品信息的泄漏.

瑞士苏黎世大学的 R. H. Weber[6]指出物联网安全体系不仅要满足抵抗攻击, 数据认证, 访问控制及用户隐私等要求, 而且需针对物联网感知节点易遭攻击、计算资源受限导致无法利用高复杂度的加解密算法保证自身安全等物联网安全所面临的特殊问题展开研究, 并指出应该从容忍攻击方面进行研究, 以应对单点故障、数据认证、访问控制和客户端的隐私保护等问题, 建议对企业进行必要的风险评估与风险管理.

英国 Newcastle 大学的 Leusse 中提出了一种面向服务思想的安全架构[7], 利用 Identity Brokerage、Usage&Access Management、SOA (Service-Oriented Architecture) Security Analysis、SOA Security Autonomics 等模块来构建一个具有自组织能力的安全物联网模型.

瑞士苏黎世大学的 Mattern 团队指出了从传统的互联网到物联网的转变过程中可能会面临的一系列安全问题[8], 尤其强调了资源访问控制问题. 德国 Albert-Ludwigs 大学的 C. Struker 提出利用口令管理机制来降低物联网中感知节点(如 RFID 设备)遭受攻击和破坏等威胁的思想[9], 并提出了 RFID 网路中的两种口令生成方法, 以防止非法用户肆意利用 RFID 的 kill 标签来扰乱感知节点正常工作. 德国 Humbold 大学的 Fabian 团队提出 EPC 网络所面临的一系列的安全挑战, 对比了 VPN(virtual private networks)、TLS(transport layer security)、DNSSEC(DNS security extensions)、Private Information Retrieval、Peer-to-Peer Systems 等应对措施的优缺点和有效性[10].

在 RFID 和无线传感网(wireless sensor networks, WSN)等物联网相关领域, 人们也进行了大量的研究工作. 美国丹佛大学的 Ken Traub 等多人在中基于 RFID 和物联网技术提出了全球物联网体系架构[11], 并结合该架构给出了物联网信息服务系统的设计方案, 为实现物联网安全架构、信息服务系统和物联网安全管理协议提供了参考.

在无线传感器认证领域中, R. Watro 等人首次提出了基于低指数级 RSA 的 TinyPK 实体认证方案[12], 并采用分级的思想来执行认证的不同操作部分. TinyPK 较方便地实现了 WSN 的实体认证, 但单一的节点是比较容易被捕获的, 在 TinyPK 中, 如果某个认证节点被捕获了, 那么整个网络都将变得不安全, 因为任意的敌对第三方都可以通过这个被捕获的节点获得合法身份进入 WSN. Z. Benenson 等人提出的强用户认证协议[13]可以在一定程度上解决这个问题. 相对于 TinyPK, 强用户认证协议有两点改进: (1)公钥算法不是采用 RSA, 而是采用密钥长度更短却具有同等安全强度的椭圆曲线加密算法(ECC); (2) 认证方式不是采用传统的单一认证, 而是采用 n 认证. 这个强用户认证协议安全强度较高, 不过其缺点则主要体现在对节点能量的消耗过大. K. Bauer 提出了一种分布式认证协议[14], 采用的是秘密共享和组群同意的密码学概念. 网络由多个子群组成, 每个子群配备一个基站, 子群间通信通过基站进行. 该方案的优点是在认证过程中没有采用任何高消耗的加/解密方案, 而是采用秘密共享和组群同意的方式, 容错性好, 认证强度和计算效率高; 缺点是认证时子群内所有节点均要协同通信, 在发送判定包时容易造成信息碰撞.

由于低成本的 RFID 标签仅有非常有限的计算能力, 所以现有的应用广泛的安全策略无法在其上实现. 西班牙的 P. P. Lopez 等在文献[15]中提出了一种轻量级的互认证协议, 可以提供合适的安全级别并能够应用在大部分资源受限的 RFID 系统上.

国内物联网已经取得了较快的发展, 但其安全领域的研究目前还处于起步阶段.

方滨兴院士指出物联网的安全与传统互联网的安全有一定的异同[16]. 物联网的保护要素仍然是可用性、机密性、可鉴别性与可控性. 从物联网的三个构成要素来看, 物联网的安全体现在传感器、传输系统以及处理系统之中, 特别的, 就物理安全而言, 主要表现在传感器的安全方面, 包括对传感器的干扰、屏蔽、信号截获等, 这是物联网的特殊所在; 至于传输系统与处理系统中的信息安全则更为复杂, 因为传感器与传感网可能会因为能量受限的问题而不能运行过于复杂的保护体系.

作者也曾从感知层、传输层、处理层和应用层等各个层次分析了物联网的安全需求[17], 初步搭建了物联网的安全架构体系, 该文特别指出: 已有的对传感网、互联网、移动网等的安全解决方案在物联网环境中不再适用, 物联网这样大规模的系统在系统整合中会带来新的安全问题.

除此之外, 还有许多关于物联网安全体系架构方面的研究, 分别从不同角度阐述了物联网作为一个大系统的安全问题, 各种架构之间在内涵上基本一致, 但在层次划分的边界方面有所不同.

(2) 物联网感知层的轻量级加密认证技术方面

随着便携式电子设备的普及和 RFID、无线传感器网络等技术的发展, 越来越多的应用需要解决相应的安全问题. 然而, 相比于传统的台式机和高性能计算机, 这些设备的资源环境通常有限, 比如, 计算能力较弱、计算可使用的存储较少、能耗有限, 等等. 而传统密码算法无法很好的适用这种环境, 这就使得受限环境中密码算法的研究成为一个迫切需要解决的热点问题. 适宜资源受限环境使用的密码算法就称为轻量级密码.

轻量级密码算法与经典密码算法相互影响、互相促进. 经典密码算法为轻量级密码算法的设计与安全性分析提供理论支撑和技术指导; 另一方面, 轻量级密码“轻量级”的特点, 将使得一些安全性分析能够更加全面深入展开, 这个过程中可能会衍生出新问题, 从而进一步带动和促进密码算法安全性分析的进展.

源于应用的推动, 近几年轻量级密码的研究非常热. 比利时鲁汶大学的 COSIC 实验室、法国国立计算机及自动化研究院 INRIA、瑞士皇家科技学院 EPFL 中心等国际上著名的密码学实验室, 相继展开了轻量级密码的研究. 欧洲的 ECRYPT II 项目专门设置了轻量级密码研究专题, 轻量级密码逐步走向实用阶段. 轻量级密码算法设计的关键问题是处理安全性、实现代价和性能之间的权衡. 部分学者针对已有的标准分组密码算法如 AES 和 IDEA 等, 进行高度优化并面向硬件平台尝试简洁实现, 期待将实现资源降低到 RFID 所允许范围之内, 但是效果并不理想. 另外, 还有对经典算法稍作修改, 使其符合轻量级环境使用, 如在 DES 基础上对 S 盒加以改进产生 DESL 算法. 还有就是面向专门为低资源环境设计的分组密码算法, 如 HIGHT、mCrypton、TEA、PRESENT、KATAN、KTANTAN 和 PRINT 等. PRESENT[18]分组密码最早发布于 CHES2007, Clefia[19]分组密码最早发布于 FSE2007, 这两个密码算法目前已成为 ISO/IEC 的轻量级分组密码[20]; DES 类轻量级密码[21]最早公布于 2007, 它是在 DES 的基础上进行轻量化的设计; KATAN&KTANTAN[22]是一族轻量级密码, 基于流密码算法 Trivium 设计; LBlock[23]是我国的吴文玲和张蕾设计, 发表于 ACNS2011.

然而, 有很多轻量级密码算法, 还缺乏对它们全面、深入的安全性分析, 比如, Katan/Ktantan 密码在发表后不到两年的时间后就被破译; 此外, 还有一些轻量级密码算法, 其整体结构和算法模块的设计还有进一步轻量化的余地.

认证技术通过服务基础设施的形式将用户身份管理与设备身份管理关联起来, 实现物联网中所有接入设备和人员的数字身份管理、授权、责任追踪, 以及传输消息的完整性保护, 这是整个网络的安全核心和命脉. 在 RFID、无线传感器网络等应用环境中, 节点资源(包括存储容量、计算能力、通信带宽和传输距离等)受到比传统网络更加严格的限制, 资源的严重受限使得传统的计算、存储和通信开销较大的认证技术无法应用, 因此轻量级(lightweight)认证技术成为该领域研究的热点.

消息认证码(message authentication code, MAC)是保证消息完整性和进行数据源认证的基本算法, 它将密钥和任意长度的消息作为输入, 输出一个固定长度的标签, 使验证者可以能够校验消息的发送者是谁,

以及消息传输过程中是否被篡改. MAC 算法主要有三种构造方法, 分别基于分组密码、杂凑函数或者泛杂凑函数族. 为实现安全和效率的平衡, 近几年出现了几种基于分组密码的 MAC 设计新结构. 其中, 以基于约减轮数的高级加密标准 AES 为代表. 2005 年, AES 的设计者 Daemen 和 Rijmen 提出 ALRED 结构及基于 AES 和缩减到 1 轮 AES 的实例 ALPHA-MAC[24], 随后又以 AES 和 4 轮 AES 为主要部件设计了 PELICAN 算法[25]. 由于杂凑函数的普遍性和高效性, 用杂凑函数设计消息认证码的方法也得到了广泛的关注. 1995 年, Preneel 等学者基于 MD 系列杂凑函数设计了 MDx-MAC[26]. 之后, Bellare 等学者提出 NMAC 和 HMAC, 并给出了安全性证明[27]. 近年来, 杂凑函数安全性分析的一系列突破性进展引起了国内外同行对基于杂凑函数的消息认证码安全性的广泛关注. 基于泛杂凑函数族的消息认证码的设计, 其核心是泛杂凑函数族的设计. 由于泛杂凑函数族是满足一定性质的组合结构, 其设计方法和杂凑函数有很大差异, 但在速度上有很大优势. 这类消息认证码如 Poly1305-AES[28]比基于 AES 的 CBC-MAC 和基于 SHA-1 的 HMAC 速度都要快, 但是这类方法的缺陷是对密钥限制过多且占用较多的存储.

基于口令的认证密钥交换协议(PAKE)以其方便易用的独特优势而得到广泛关注. 由于通信双方共享的秘密信息是易于记忆的低熵口令, 这类协议在实际中得到广泛应用. 第一个 PAKE 协议由 Bellovin 和 Merritt 提出[29], 这一工作成为该领域很多研究的基础. 虽然 PAKE 的研究发展有多年的历史, 但 PAKE 的可证明安全性理论研究以及在资源受限网络协议中的应用研究却进展缓慢, 主要原因在于设计从弱口令转化为强的秘密信息的机制是困难的. LEAP 协议(lightweight extensible authentication protocol)[30]是由 Cisco 公司设计的轻量级认证协议, 其目的是填补无线局域网标准 IEEE 802.11 中的 WEP 协议密钥管理的空白, 给出高效的解决方案. LEAP 协议是基于口令的轻量级密钥交换协议, 虽然它提供了无线网络认证密钥交换的一种方式, 但它却受到离线字典攻击(off-line dictionary attack). 如何克服这些困难, 设计高效安全的轻量级鉴别机制, 是一个需要深入研究的问题.

国际标准化组织也正在制订轻量级密码算法的相关标准, 其中包括轻量级的分组密码、流密码、数字签名等. 但是, 目前对于轻量级认证技术并没有统一的衡量和评价的标准体系, 轻量级认证还处于发展阶段. 虽然很多标准化组织已经对消息认证码进行标准化工作, 例如采用 CBC 工作模式构造的 CBC-MAC, 现已是 ANSI X9.9、FIPS PUB 113 和 ISO/IEC 9797 标准[31], 但还没有轻量级的消息认证码的相关标准.

(3) 在感知节点鉴术方面

鉴别机制提供了关于某个实体(用户、节点或设备)身份的保证, 这意味着每当某个实体声称具有一个特定的身份时, 鉴别机制将提供某种方法来证实这一声明是正确的. 目前, 一些轻量级的鉴别机制被提出, 主要思想是以牺牲一方(如让资源丰富的服务器处理大量的计算)为代价, 来节省资源受限节点的计算开销. 最近关于聚合签名(aggregate signature)的研究对于设计轻量级高效鉴别机制有可借鉴之处. 聚合签名的概念最初是由 Boneh 等人提出的[32], 他们引进了一种改进通信效率和计算效率的方法: 把 n 个不同用户对 n 个不同消息做的签名合并成一个有效的签名, 验证者通过对此聚合签名的验证, 即可证实每个用户所做的相应签名的正确性. 如何把这种思想应用到物联网感知层鉴别机制的设计中, 以减少链路所占用的带宽, 缓解通信组成员数量增加所带来的负担, 是物联网安全需要解决的技术挑战之一.

轻量级认证技术是构建物联网信任体系的核心内容, 因此, 轻量级认证关键技术的研究是国家战略需求, 也是互联网演进的必然趋势.

(4) RFID 隐私保护技术方面

关于感知节点隐私保护, 主要涉及到感知节点芯片及存储器物理防护技术, 感知节点数据加密存储技术, 感知节点数据访问控制和双向认证技术, 感知节点周边物理安全防护技术, 感知节点声、光、电磁信号干扰、攻击或隐藏技术. 比较突出的是 RFID 技术感知节点的隐私保护.

RFID 技术应用中因电子标签内容被泄露, 被追踪、定位给人们带来了很多隐私威胁问题. 而随着社会的进步与发展, 安全与隐私得到越来越多的重视. 因此, 针对 RFID 技术应用中的隐私保护问题国内外学者开展了一定的研究.

对于 RFID 技术应用中的隐私保护主要采用两类, 文献[33]提到可从物理方法和逻辑方法两方面来实现. 目前的物理方法有: 破坏标签(Kill 标签)、屏蔽标签(法拉第网罩)、有源干扰法、阻塞标签等. 逻辑方法有: 读取访问控制、标签认证、标签加密等. 本文侧重介绍几种基于 Hash 函数的逻辑方法(读取访问控制). 到目前为止, 已有多种 RFID 系统安全协议提出, 包括 Hash-LOCK 协议、随机化 Hash-LOCK 协议、Hash-CHAIN 协议、各种改进的 Hash 协议.

文献[34]提到 kill 机制. Kill 标签机制由标准化组织 Auto-IDCenter(自动识别中心)提出, 其原理是完全销毁标签可以阻止追踪, 但牺牲了 RFID 电子标签功能. 文献[35]提到静电屏蔽. 静电屏蔽是采用金属屏蔽方式阻止标签被读取. 主动干扰无线电信号是另一种屏蔽标签的方法. 标签用户可以通过一个设备主动广播无线电信号用于阻止或破坏附近的 RFID 阅读器的操作. 文献[36]提到阻止标签方法. 阻止标签方法是通过阻止阅读器读取标签确保消费者隐私.

与基于物理方法的硬件安全机制相比, 基于密码技术的安全认证协议受到人们更多的青睐. 典型的 RFID 安全认证包括 Hopper&Blum 系列协议、噪声标签的密码交换协议、超宽带调制、物理不可克隆函数和基于单时码(One-time Codes)的加密、基于 Hash 函数的安全协议等等.

Hopper 和 Blum 提出了基于 LPN(learning parity with noise)的 HB 协议. HB 协议执行过程简单, 硬件设备易于实现, 存储空间和计算负载较小. 同时, HB+、HB++等一系列 HB 协议基于千位数据二进制向量、千位密钥向量和一些噪声位, 用 1 或 0 来表示向量位元素, 并满足一些限定方程. 但攻击者仍有可能运用标准随机估计理论通过个别数据猜测出可能的函数, 存在一定的安全隐患.

Castelluccia 和 Avoine 提出了基于 RFID 噪声标签的密码交换协议. 其基本思想是在标签响应消息中加入噪声, 这些噪声能够被可信的读写器识别并消除以恢复有用信号. 攻击者因为不能正确地区分出噪声和有用数据, 所以不能窃取有用的信息.

超宽带调制(ultra wide band modulation)方法是基于时分传输时隙来实现的. 它的安全性在于非法攻击者很难得知有用信息是在哪个时隙发送的, 该过程用到了相位调制器, 也用到了跳时码(time hopping codes)伪随机序列生成器.

基于单时码(one-time codes)的加密其主要思想是运用假名标识来增强 RFID 标签的安全性. 一个标签可以携带多个随机标识. 每当标签被查询时, 标签都给出一个不同的标识. 原则上, 只有一个授权的读写器能够识别出两个不同的标识是否是同一个标签, 以实现安全性. 这种方法的缺点是: 攻击者也可以通过反复地向某个标签送查询命令以使这种方法的安全性减弱.

文献[37]中提到基于 Hash 函数的安全协议主要有三种. Hash 锁(hash lock)协议是由 Sarma 等人提出来的. 为了避免信息泄漏和被追踪, 使用 metaID 代替真实的标签 ID. Hash 锁协议中没有 ID 动态刷新机制, 并且 metaID 也保持不变, ID 是以明文的形式通过不安全的信道传送的, 因此, Hash 锁协议非常容易受到假冒攻击和重传攻击, 攻击者也可以很容易地对标签进行追踪. 随机化 Hash 锁(Random Hash-Lock)协议由 Weis 等人提出, 采用了基于随机数的询问-应答机制. 在随机化 Hash 锁协议中, 认证通过后的标签标识 IDk 仍以明文的形式通过不安全信道传送, 因此攻击者可以对标签进行有效的追踪. 同时, 一旦获得了标签的标识 IDk, 攻击者就可以对标签进行假冒, 而该协议无法抵抗重传攻击. Hash 链协议原理如下: 标签最初在存储器设置一个随机的初始化标识符 s, 同时这个标识符也储存在后端数据库. 标签包含两个 Hash 函数 G 和 H. 当阅读器请求访问标签时, 标签返回当前标签标识符 $\mathrm{rk}:G(S)$ 给阅读器, 同时当标签从阅读器电磁场获得能量时自动更新标识符 $s=H(S)$. 该方案具有“前向安全性”, 但是该方法需要后台进行大量的 Hash 运算. 标签加密以后仍具有固定输出, 因此使得标签的追踪成为可能, 存在标签定位隐私问题.

文献[38]提到基于 K-匿名模型安全隐私控制模型, K-匿名的技术上世纪末由 L.sweeney 和 Samarati 在 PODS 上提出. 该技术能够对全部个体敏感属性进行保护, 将其隐藏于 K 规模的群体里. 之后, L.sweeney 又提出了 K-匿名的保护模型, 并给出了应用该技术的隐匿及泛化方法, 有效地提升了保护隐私的力度. K-

匿名的定义是: 若一拥有数据者, 其想将个人数据 $R(D_1,\cdots,D_n,C)$ 进行共享. 数据记录的形式如下: $R(V_1,\cdots,V,\text{cls})$, 其中 V 为属性 D_i 的数值, cls 为一个属性 C 的类别. 如果 R 与外部数据记录 E 共享一些属性, 则将其记录为 $R*E$. 假设 $R*E$ 中值比较特殊, 则依据它就能够在极大概率下, 进行推断一条对应到现实生活中的具体记录. 所以, 针对所有在 $R*E$ 里的值, 持有数据者需确保在 R 中, 均有记录和它进行对应, 该记录的条数可等于或大于某一最小值. 于是, 能够防止利用 $R*E$ 中的值对 R 里数据隐私性的破坏.

文献[39]提到对于使用用户的地点信息, 但是不把地点信息透漏给提供服务的提供者或第三方. 这类位置隐私问题可通过计算几何方法解决. 特别是在物联网的近距离通信中, 由于 RFID 芯片使用者和 RFID 读写器距离太近, 以至于阅读器的地点无法隐藏. 保护使用者地点隐私的方法是使用安全多方计算的临时密码保护并隐藏 RFID 标识.

4 物联网的安全架构

物联网的健康发展少不了信息安全保护技术, 但在物联网这个特殊的领域, 许多传统领域中的信息安全技术不能直接移植过来, 需要重新搭建物联网安全架构和在此架构下裁剪合适的具体方案. 关于物联网安全架构问题已有许多不同观点不同角度的深入讨论, 如文献[16,17,40,41]. 2013 年, 在物联网安全架构体系下, 对物联网安全体系的各个关节进行了深入的分析与讨论[42].

事实上, 到目前为止对什么是物联网没有一个合适定义, 因此对物联网的描述只能从特征和架构上进行描述. 的在介绍物联网安全架构之前, 首先要了解物联网的架构.

物联网的核心可划分为三个逻辑层, 分别为感知层、传输层和处理应用层. 总体上, 感知层的作用是获取原始数据, 传输层的作用是将这些原始数据传输到远程的处理平台进行处理, 而处理应用层的作用无疑是对来自不同感知节点的信息进行存储、处理和应用. 由于对数据的处理和对数据的应用无论从流程上和方法上都有很大区别, 为了更清晰地描述完整的物联网架构, 有时候将物联网的处理应用层又分为处理层和应用层这两个逻辑层, 形成 4 个逻辑层的架构, 如图 1 所示. 从本质上说, 无论三层架构还是四层架构, 其内涵都是一样的, 只是逻辑层划分边界不同.

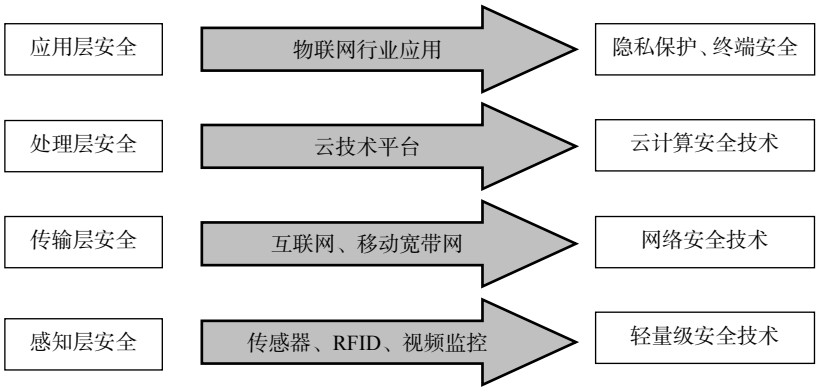

图 1 物联网安全架构和关键技术示意图
Figure 1 An architecture and key techniques of Internet of Things

对物联网系统的架构还有另外一种划分, 即“海-网-云”架构. 在这种架构中, 所有终端设备被化分为一层, 由于物联网系统的终端数量将是巨大的, 可以用海量来形容, 因此将此类设备形象地称为“海”. 数据传输的基础网络设施被称为“网”, 很明显这个“网”不是单一的网, 而是多种异构网络的统称, 包括局域网、互联网、移动网等. 物联网系统的数据将由一个具有很强处理能力的平台进行处理, 用户只需要知道

跟处理平台的逻辑关系, 无需知道自己的数据是在处理平台中的哪个计算机或者处理器处理的, 也无需知道自己的数据存储在哪里, 只关心当自己需要的时候可以从数据处理中心得到数据和处理结果, 这样的数据处理中心被形象地描述成“云”. 这样, 就形成了物联网的“海-网-云”逻辑架构, 如图 2 所示.

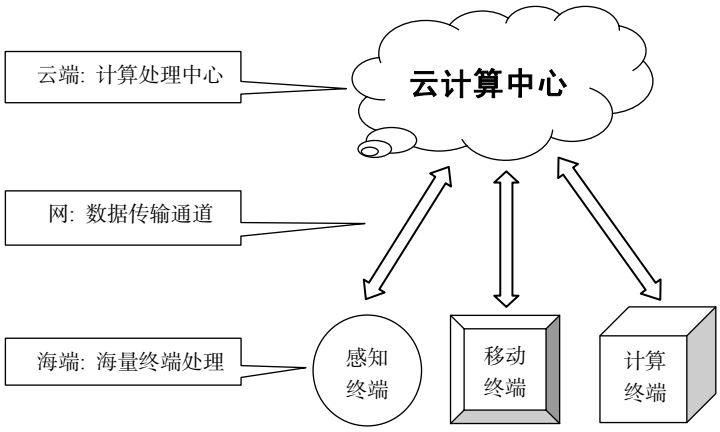

图 2 物联网的“海-网-云”架构图
Figure 2 The “Sea-net-cloud” architecture of Internet of Things

考虑到物联网系统中有两种类型的终端, 一种是用于采集数据的终端, 通常称为感知终端(包括 RFID 标签), 我们称为这种终端为 A 类终端, 一般处理能力小, 但数量庞大; 另一种是用户移动终端, 如手机、平板电脑、笔记本电脑等, 这类终端的目的是获取 A 类终端的数据或对这些数据的处理结果, 并且能控制 A 类终端. 我们称移动终端为 B 类终端. 在物联网的三层架构中, A 类终端在感知层, B 类终端在处理应用层; 在物联网的四层架构中, A 类终端在感知层, B 类终端在应用层; 而在物联网的“海-网-云”架构中, A 类终端与 B 类终端都在“海”端, 因此不同架构的内涵相同, 但划分边界和处理角度不同.

现在我们以物联网的四层架构为基础, 讨论物联网的安全架构. 首先, 物联网的感知层需要安全保护, 我们称这类安全保护为感知层安全; 其次, 物联网的传输层需要安全保护, 我们称为处理层安全; 同样, 物联网的处理层需要安全保护, 我们称为处理层安全; 最后, 物联网的应用层需要安全保护, 我们称为应用层安全. 下面我们针对每个安全层, 讨论相关的关键技术.

5 物联网感知层安全关键技术

物联网感知层主要包括传感器节点、传感网路由节点、感知层网关节点(又称为协调器节点或汇聚节点)、以及连接这些节点的网络, 通常是短距离无线网络, 如 Zigbee、433、Wifi 等. 广义上, 传感器节点也包括 RFID 标签, 感知层网关节点包括 RFID 读写器, 无线网络也包括 RFID 使用的通信协议, 如 EPCglobal.

考虑到许多传感器的特点是资源受限, 因此处理能力有限, 对安全的需求也相对较弱, 但完全没有安全保护会面临很大问题, 因此需要轻量级安全保护. 什么是轻量级? 与物联网的概念一样, 对此没有一个标准的定义. 但我们可以分别以轻量级密码算法和轻量级安全协议进行描述. 由于 RFID 标准中为安全保护预留了 2000 门等价电路的硬件资源, 因此如果一个密码算法能使用不多余 2000 门等价电路来实现的话, 这种算法就可以称为轻量级密码算法. 目前已知的轻量级密码算法包括 PRESENT[18]和 LBLOCK[23]等. 而对轻量级安全协议, 没有一个量化描述, 许多安全协议都声称为轻量级协议, 如文献[15,43].

虽然轻量级密码算法有一个量化描述, 但追求轻量的目标却永无止境. 因此我们这里列出几个轻量级密码算法设计的关键技术和挑战:

(1) 超轻量级密码算法的设计. 这类密码算法包括流密码和分组密码, 设计目标是在硬件实现成本上越小越好, 不考虑数据吞吐率和软件实现成本和运行性能, 使用对象是 RFID 标签和资源非常有限的传感器节点;

(2) 可硬件并行化的轻量级密码算法的设计. 这类密码算法同样包括流密码和分组密码算法, 设计目标是考虑不同场景的应用, 或通信两端的性能折衷, 虽然在轻量化实现方面也许不是最优, 但当不考虑硬件成本时, 可使用并行处理技术实现吞吐率的大幅度提升, 适合协调器端使用;

(3) 可软件并行化的轻量级密码算法的设计. 这类密码算法的设计目标是满足一般硬件轻量级需求, 但软件实现时可以实现较高的吞吐率, 适合在一个服务器管理大量终端感知节点情况下在服务器上软件实现;

(4) 轻量级公钥密码算法的设计. 在许多应用中, 公钥密码具有不可替代的优势, 但公钥密码的轻量化到目前为止是一个没有逾越的技术挑战, 即公开文献中还没有找到一种公钥密码算法可以使用小于 2000 等价门电路实现, 且在当前计算能力下不可实际破解;

(5) 非平衡公钥密码算法的设计. 这其实是轻量级公钥密码算法的折衷措施, 目标是设计一种在加密和解密过程很不平衡的公钥密码算法, 使其加密过程达到轻量级密码算法的要求, 或解密过程达到轻量级密码算法的要求. 考虑到轻量级密码算法的使用很多情况下是在传感器节点与协调器或服务器进行通信, 而后者计算资源不受限制, 因此无需使用轻量级算法, 只要在传感器终端上使用的算法具有轻量级即可.

对于轻量级安全协议, 既没有量化描述, 也没有定性描述. 总体上, 安全协议的轻量化需要交同类协议相比, 减少通信轮数(次数), 减少通信数据量, 减少计算量, 当然这些要求的代价是一定会有所牺牲, 就是可靠性甚至某些安全性方面的牺牲. 可靠性包括对数据传递的确认(是否到达目的地), 对数据处理的确认(是否被正确处理)等, 而安全性包括前向安全性、后向安全性等, 因为这些安全威胁在传感器网络中不太可能发生, 攻击成本高而造成的损失小. 轻量级安全协议包括如下几种:

(1) 轻量级安全认证协议, 即如何认证通信方的身份是否合法;

(2) 轻量级安全认证与密钥协商协议(AKA), 即如何在认证成功后建立会话密钥, 包括同时建立多个会话密钥的情况;

(3) 轻量级认证加密协议, 即无需对通信方的身份进行专门认证, 在传递消息使验证消息来源的合法性即可. 这种协议适合非连接导向的通信;

(4) 轻量级密钥管理协议, 包括轻量级 PKI, 轻量级密钥分发(群组情况), 轻量级密钥更新等.

注意无论轻量级密码算法还是轻量级安全协议, 必须考虑消息的新鲜性, 以防止重放攻击和修改重放攻击. 这是与传统数据网络有着本质区别的地方.

6 物联网传输层安全关键技术

物联网传输层主要包括互联网、移动网络(如 GSM、3G、LTE 等), 也包括一些非主流的专业网络, 如电信网、电力载波等. 但我们研究传输层安全关键技术时一般主要考虑互联网和移动网络.

事实上, 互联网有着许多安全保护技术, 包括物理层, IP 层、传输层、和应用层的各个方面, 而移动网络的安全保护也有自己的国际标准, 因此物联网传输层的安全技术不是物联网安全中的研究重点.

7 物联网处理层安全关键技术

物联网处理层就是数据处理中心, 小的可以是一个普通的处理器, 大的可以是由分布式机群构成的云计算平台. 从信息安全角度考虑, 系统越大, 遭受攻击者关注的可能性就越大, 因此需要的安全保护程度就要越高. 因此物联网处理层安全的关键计算主要是云计算安全的关键技术. 由于云计算作为一个独立的研究课题已经得到广泛关注, 这方面的安全关键技术有许多专门论述和研究, 因此不在本文的讨论范围.

8 物联网应用层安全关键技术

物联网的应用层严格地说不是一个具有普适性的逻辑层, 因为不同的行业应用在数据处理后的应用阶段表现形式相差各异. 综合不同的物联网行业应用可能需要的安全需求, 物联网应用层安全的关键技术可以包括如下几个方面:

(1) 隐私保护技术. 隐私保护包括身份隐私和位置隐私. 身份隐私就是在传递数据时不泄漏发送设备的身份, 而位置隐私则是告诉某个数据中心某个设备在正常运行, 但不泄漏设备的具体位置信息. 事实上, 隐私保护都是相对的, 没有泄漏隐私并不意味着没有泄漏关于隐私的任何信息, 例如位置隐私, 通常要泄漏(有时是公开或容易猜到的信息)某个区域的信息, 要保护的是这个区域内的具体位置, 而身份隐私也常泄漏某个群体的信息, 要保护的是这个群体的具体个体身份.

隐私保护的研究是一个传统的问题, 国际上对这一问题早有研究, 例如文献[5,6,36,44]. 在物联网系统中, 隐私保护包括 RFID 的身份隐私保护、移动终端用户的身份和位置隐私保护、大数据下的隐私保护技术等.

在智能医疗等行业应用中, 传感器采集的数据需要集中处理, 但该数据的来源与特定用户身份没有直接关联, 这就是身份隐私保护. 这种关联的隐藏可以通过第三方管理中心来实现, 也可以通过密码技术来实现. 隐私保护的另一个种类是位置隐私保护, 即用户信息的合法性得到检验, 但该信息来源的地理位置不能确定. 同样位置隐私的保护方法之一是通过密码学的技术手段. 根据我们的经验, 在现实世界中少有不慎, 我们的隐私信息就被暴露于网络上, 有时甚至处处小心还是会泄漏隐私信息. 因此如何在物联网应用系统中不泄漏隐私信息是物联网应用层的关键技术之一.

在物联网行业应用中, 如果隐私保护的目标信息没有被泄漏, 就意味着隐私保护是成功的, 但在学术研究中, 我们需要对隐私的泄漏进行量化描述, 即一个系统也许没有完全泄漏被保护对象的隐私, 但已经泄漏的信息让这个被保护的隐私信息非常脆弱, 再有一点点信息就可以确定, 或者说该隐私信息可以以较大概率被猜测成功. 除此之外, 大数据下的隐私保护如何研究, 是一个值得深入探讨的问题.

(2) 移动终端设备安全. 智能手机和其他移动通信设备的普及为生活带来极大便利的同时, 也带来很多安全问题. 当移动设备失窃时, 设备中数据和信息的价值可能远大于设备本身的价值, 因此如何保护这些数据不丢失、不被窃, 是移动设备安全的重要问题之一. 当移动设备称为物联网系统的控制终端时, 移动设备的失窃所带来的损失可能会远大于设备中数据的价值, 因为对 A 类终端的恶意的控制所造成的损失不可估量. 因此作为物联网 B 类终端的移动设备安全保护是重要的技术挑战.

(3) 物联网安全基础设施. 应该说, 即使保证物联网感知层安全、传输层安全和处理层安全, 也保证终端设备不失窃, 仍然不能保证整个物联网系统的安全. 一个典型的例子是智能家居系统, 假设传感器到家庭汇聚网关的数据传输得到安全保护, 家庭网关到云端数据库的远程传输得到安全保护, 终端设备访问云端也得到安全保护, 但对智能家居用户来说还是没有安全感, 因为感知数据是在别人控制的云端存储. 如何实现端到端安全, 即 A 类终端到 B 类终端以及 B 类终端到 A 类终端的安全, 需要由合理的安全基础设施完成. 对智能家居这一特殊应用来说, 安全基础设施可以非常简单, 例如通过预置共享密钥的方式完成, 但对其他环境, 如智能楼宇和智慧社区, 预置密钥的方式不能被接受, 也不能让用户放心. 如何建立物联网安全基础设施的管理平台, 是安全物联网实际系统建立中不可或缺的组成部分, 也是重要的技术问题.

(4) 物联网安全测评体系. 安全测评不是一种管理, 更重要的是一种技术. 首先要确定测评什么, 即确定并量化测评安全指标体系, 然后给出测评方法, 这些测评方法应该不依赖于使用的设备、或执行的人, 而且具有可重复性. 这一问题必须首先解决好, 才能推动物联网安全技术落实到具体的行业应用中去.

9 结论

物联网是一种新型产业方向, 是信息技术发展的一个新阶段. 物联网系统在物联网概念被提出之前就

已经大量存在, 但物联网的概念会将这类技术和产业推向更重要的位置. 但是, 物联网安全问题还没有引起足够重视, 行业界认为物联网安全问题没有这么严重, 学术界认为物联网研究不能产生许多创新性成果. 事实上, 与物联网相关的许多技术和理论可以具有很高的学术意义和应用价值, 一些已有方法的应用, 即一些技术方法在某种特殊物联网行业中的落地实施也是一种集成创新, 因为在应用中除了考虑功能外, 还要在性能优化方面做许多工作.

本文阐述了物联网安全所涉及的一些安全问题, 其中与传统信息安全中常见问题有所区别的是轻量级安全问题, 特别是非平衡公钥密码的设计问题, 隐私保护问题, 以及物联网安全基础设施问题等.

References

[1] ITU. The Internet of Things[R/OL]. http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf.
[2] Floerkemeier C, Fleisch E, Langheinrich M, et al. The Internet of Things: First International Conference, IOT 2008, Zurich, Switzerland, March 26–28, 2008. Proceedings[M]. Springer Science & Business Media, 2008.
[3] Van Kranenburg R. The Internet of Things[M]. Waag Society, Amsterdam, The Netherlands, 2008.
[4] Yan L, Zhang Y, Yang L T, et al. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems[M]. Auerbach Publications, 2008.
[5] Medaglia C M, Serbanati A. An overview of privacy and security issues in the internet of things[C]. In: The Internet of Things. Springer New York, 2010: 389–395.
[6] Weber R H. Internet of Things—new security and privacy challenges[J]. Computer Law & Security Review, 2010, 26(1): 23–30.
[7] de Leusse P, Periorellis P, Dimitrakos T, et al. Self managed security cell, a security model for the Internet of Things and Services[C]. In: 2009 First International Conference on Future Internet. IEEE, 2009: 47–52.
[8] Mattern F, Floerkemeier C. From the internet of computers to the internet of things[C]. In: From Active Data Management to Event-based Systems and More. Springer Berlin Heidelberg, 2010: 242–259.
[9] Wonnemann C, Struker J. Password management for EPC Class 1 Generation 2 transponders[C]. In: 2008 10th IEEE Conference on E-Commerce Technology and the 5th IEEE Conference on Enterprise Computing, E-Commerce and E-Services,. IEEE, 2008: 29–35.
[10] Fabian B, Günther O. Security challenges of the EPCglobal network[J]. Communications of the ACM, 2009, 52(7): 121–125.
[11] Traub K, Allgair G, Barthel H, et al. The EPCglobal architecture framework[S]. http://www.gs1hk.org/files/document/epc_standards/architecture_1_3-framework-20090319.pdf.
[12] Watro R, Kong D, Cuti S, et al. TinyPK: securing sensor networks with public key technology[C]. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. ACM, 2004: 59–64.
[13] Benenson Z, Gedicke N, Raivio O. Realizing robust user authentication in sensor networks[J]. Real-World Wireless Sensor Networks (REALWSN), 2005, 14: 52.
[14] Bauer K, Lee H. A distributed authentication scheme for a wireless sensing system[J]. ACM Transactions on Information and System Security, 2008, 11(3): 1–35.
[15] Peris-Lopez P. LMAP: a real lightweight mutual authentication protocol for low-cost RFID tags[J]. Journal of Signal Processing Systems, 2010, 59: 95–102.
[16] Fang B X. Security of internet of things[J]. Information and Communications Technologies, 2010, 4(6):4.
方滨兴. 关于物联网的安全[J]. 信息通信技术, 2010, 4(6):4.
[17] Wu C K. A preliminary investigation on the security architecture of the internet of things[J]. Bulletin of Chinese Academy of Sciences, 2010, 25(4): 411–419.
武传坤. 物联网安全架构初探, 中国科学院院刊, 2010, 25(4): 411–419.
[18] Bogdanov A, Knudsen L, Leander G, et al. PRESENT: an ultra-lightweight block cipher[C]. In: Cryptographic Hardware and Embedded Systems—CHES 2007. Springer Berlin Heidelberg 2007: 450–466.
[19] Shirai T, Shibutani K, Akishita T, et al. The 128-bit blockcipher CLEFIA[C]. In: Fast Software Encryption—FSE 2007. Springer Berlin Heidelberg, 2007: 181–195.
[20] ISO. Information technology-Security techniques-Lightweight cryptography-Part 2: Block ciphers[S/OL]. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552
[21] Leander G, Paar C, Poschmann A, et al. New lightweight DES variants[C]. In: Fast Software Encryption—FSE 2007. Springer Berlin Heidelberg, 2007: 196–210.
[22] De Canniere C, Dunkelman O, Knežević M. KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers[C]. In: Cryptographic Hardware and Embedded Systems—CHES 2009. Springer Berlin Heidelberg, 2009: 272–288.
[23] Wu W L, Zhang L. LBlock: a lightweight block cipher[C]. In: Applied Cryptography and Network Security—ACNS 2011. Springer Berlin Heidelberg, 2011: 327–344.

[24] Daemen J, Rijmen V. A new MAC construction ALRED and a specific instance ALPHA-MAC[C]. In: Fast Software Encryption—FSE 2005. Springer Berlin Heidelberg, 2005: 1–17.
[25] Daemen J, Rijmen V. The pelican MAC function[J]. IACR Cryptology ePrint Archive, 2005, 2005: 88.
[26] Preneel B, Van Oorschot P C. MDx-MAC and building fast MACs from hash functions[C]. In: Advances in Cryptology—CRYPT0 '95. Springer Berlin Heidelberg, 1995: 1–14.
[27] Bellare M, Canetti R, Krawczyk H. Keying hash functions for message authentication[C]. In: Advances in Cryptology—CRYPTO '96. Springer Berlin Heidelberg, 1996: 1–15.
[28] Bernstein D J. The Poly1305-AES message-authentication code[C]. In: Fast Software Encryption—FSE 2005. Springer Berlin Heidelberg, 2005: 32–49.
[29] Bellovin S M, Merritt M. Encrypted key exchange: Password-based protocols secure against dictionary attacks[C]. In: 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 1992. IEEE, 1992: 72–84.
[30] MacNally C. Cisco LEAP protocol description[OL]. http://www.missl.cs.umd.edu/wireless/ethereal/leap.txt, September 2001.
[31] ISO/IEC. Information Technology-Security Techniques-Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm[S], 1994.
[32] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]. In: Advances in cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg, 2003: 416–432.
[33] Li H N. Security scheme and strategy for RFID based on Hash protocol[J]. Information and Communications Technologies, 2009, 6: 16–19.
李宏年. 基于 Hash 协议的射频识别系统安全对策[J]. 信息通信技术, 2009, 6: 16–19.
[34] Sarma S E, Weis S A, Engels D W. RFID systems and security and privacy implications[C]. In: Cryptographic Hardware and Embedded Systems—CHES 2002. Springer Berlin Heidelberg, 2003: 454–469.
[35] Sarma S E, Weis S A, Engels D W. Radio-frequency identification: secure risks and challenges[J]. RSA Laboratories Cryptography, 2003, 6(1): 2– 9
[36] Juels A, Rivest R L, Szydlo M. The blocker tag: selective blocking of RFID tags for consumer privacy[C]. In: Proceedings of the 10th ACM Conference on Computer and Communications Security—CCS 2003. ACM, 2003: 103–111.
[37] Chen R X, Zou C Y, Huang J W. RFID cryptographic protocol based on mutual Hash authentication[J]. Microcomputer Information, 2010, 26(11): 149–151.
陈瑞鑫, 邹传云, 黄景武. 一种基于双向 Hash 认证的 RFID 安全协议[J]. 微计算机信息, 2010, 26(11): 149–151.
[38] Hua Y T, Yu B. Protection of privacy on the internet of things[J].China Computer & Communication, 2011, 6(12): 5–6.
华颜涛, 于彪. 物联网信息共享的安全隐私保护研究[J]. 信息与电脑, 2011, 6(12): 5–6.
[39] Bao L, Zhang D Y, Wu J B. Internet of things and privacy preserving technologies[J]. Electronic Science of Technology. 2010, 23(7): 110–112.
暴磊, 张代远, 吴家宝. 物联网与隐私保护技术[J]. 电子科技. 2010, 23(7): 110–112.
[40] Li Z Q. Security architecture and technology in the Internet of things[J]. Microcomputer & Its Applications, 2011, 30(9): 54–56.
李志清. 物联网安全架构与关键技术[J]. 微型机与应用, 2011, 30(9): 54–56.
[41] Zhang B, Ma X X, Qin Z G. Security architecture on the trusting internet of things[J]. Journal of Electronic Science and Technology, 2011, 9(4): 364–367.
[42] Wu C K. Security Fundamentals for Internet of Things[M]. Beijing: Science Press, 2013.
武传坤. 物联网安全基础[M]. 北京: 科学出版社, 2013.
[43] Chakrabarti D, Maitra S, Roy B. A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design[J]. International Journal of Information Security, 2006, 5(2): 105–114.
[44] Beresford A R, Stajano F. Location privacy in pervasive computing[J]. IEEE Pervasive Computing, 2003, 2(1): 46–55.

作者信息

武传坤(1964–), 山东临沂人, 博士, 研究员. 主要研究领域为密码函数、安全协议、物联网安全.
E-mail: ckwu@iie.ac.cn