智能电网隐私保护技术的分析研究

黄秀丽,张 涛,马媛媛,王玉斐,华 晔,陈 璐
(中国电力科学研究院,江苏 南京 210003)

摘 要:融合各种新兴的技术,智能电网的出现给电力系统带来了很大的变革。但和所有新兴事物一样,智能电网也将面临新的风险,尤其是用户侧的风险。面对智能电网用户侧风险,如何保护用户隐私权,是亟待解决的问题,也是文中研究的重点。首先分析了智能电网带来的风险,尤其是用户侧面临的风险;接着,介绍了智能电网隐私保护,对智能电网隐私保护特点进行了详细的解读;最后,结合电力系统,对我国智能电网隐私保护进行了思考,对未来的工作给出了建议。

关键词:智能电网;智能电网安全;隐私保护;分析
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2014)02-0189-04
doi:10.3969/j.issn.1673-629X.2014.02.047

Analysis and Research of Smart Grid Privacy Protection Technology

HUANG Xiu-li,ZHANG Tao,MA Yuan-yuan,WANG Yu-fei,HUA Ye,CHEN Lu
(China Electric Power Research Institute,Nanjing 210003,China)

Abstract:As integration of emerging technology,the emergence of the smart grid has brought great changes to the power system. Smart grid will also face new risks like all something new,especially the risk of the user side. For the risk of the smart grid user side,faced with the problems to be solved that how to protect users' privacy,which is also the focus in this paper. First analyze the privacy risks of the smart grid,especially the risks faced by the user side;then introduce smart grid privacy,and interpret the smart grid privacy features in detail;finally,considering the power system,it makes the thinking to China smart grid privacy,and give suggestions for the future work.

Key words:smart grid;smart grid security;privacy protection;analysis

1 概 述

随着智能电网[1-2]的发展和建设,智能设备、智能表计、智能终端等在智能电网中得到广泛使用。由于大量智能表计、智能家电的接入,网络边界进一步向用户侧延伸,用户侧的安全风险将越来越突出,数据保密性问题,尤其是用户隐私权保护[3-5]成为必须考虑的问题。

欧盟信息保护监督组织日前表示,智能电表等负责监测家庭能耗的高科技设备将给个人隐私[6-8]保护带来巨大威胁。智能电表等技术可以追踪个人信息,而收集到的大量信息可能会给消费者带来严重的后果。国际隐私权组织的安娜菲尔德认为:"如果智能电表对家庭能源信息的收集频率过高,人们的生活习惯将通过这些数据暴露出来,并可能被用于一些非法途径。"

2 智能电网隐私保护问题研究

目前,国际上对智能电网隐私保护问题的研究尚处于起始阶段,对智能电网隐私保护的讨论多集中在智能电网设备暴露个人隐私的风险分析上,其中以美国的研究处于领先地位,并发布有智能电网隐私保护的正式文档。

美国的隐私法律没有明确涉及智能电网及其相关数据,美国现有的国家级智能电网和电力输送法规也没有明确涉及隐私保护[9],现有的法律法规需要被修订,以适用于智能电网。同时,智能电网中的新数据项,以及新的使用现有数据的方式,都需要更多的研究和公众的意见,以适应当前的法律或塑造新的法律。

美国智能电网信息安全非常关注隐私问题,美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)于 2010 年 8 月发布了《Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy

收稿日期:2013-04-16 **修回日期**:2013-07-20 **网络出版时间**:2013-11-29
基金项目:国家电网科技计划项目(ERPIXXKJ[2012]2986)
作者简介:黄秀丽(1979-),女,工程师,硕士,研究方向为信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20131129.1020.060.html

and the Smart Grid》[10],初步剖析了智能电网隐私问题。

NIST 将隐私理解为四个维度,见表 1。

表 1 隐私维度

序号	维度	含义
1	个人信息隐私	任何有关个人的、可确定的、直接或间接的信息,特别是可供参考的身份证号码或特定因素信息,他或她的身体、生理、心理、经济、文化、位置或社会身份
2	个人隐私	控制自己身体完整性的权力,包括:身体需求、健康问题、所需医疗设备等
3	个人行为隐私	选择自己做什么以及保持与其他人相区别的个人行为的权力
4	个人通信隐私	通信不被过分监视、监测和检查的权力

多数智能电网实体解决了第一维的问题,因为大多数数据保护法律法规已经涵盖了对个人信息的隐私保护。但智能电网环境下将产生和传输新类型的能源使用数据,因此第 2、3、4 维的隐私保护问题,也非常重要。例如,可以从个人住宅中获得消费类电子产品、电器等的电子签名以及时间戳的活动报告;充电站的信息可以详细地表述一台电动汽车的下落,而这些数据在智能电网应用前是不存在的。

目前,NIST 隐私小组关注于智能电网以及其中的数据将会在四个隐私维度上给个人隐私带来怎样的侵犯或负面影响,然后寻求方法,协助智能电网组织识别和保护那些信息。智能电网许多数据项类型不是新的,并存在其他组织、实体或个人访问这些数据项的可能性,若对于所收集的数据出现了新的用途,也可能会引起大量的隐私问题。智能电网的应用出现了新的能源数据,这些数据更加具体,并可被更多人所接触,相关的隐私问题的复杂性也随之增高。

隐私小组的任务是认识到智能电网内的隐私问题,并给出解决建议。此外,小组致力于通过以下手段阐明关于智能电网的隐私期望、惯例和权利:

1)确定潜在的隐私问题,并鼓励使用相关的公平信息实践原则。

2)寻求智能电网实体和相关专家代表的意见,然后提供给公众隐私保护的方法,并避免在智能电网中滥用个人信息。

3)在发展隐私政策、惯例提升和保护消费者在智能电网实体中的权益方面,为组织、管理机构和智能电网实体提供建议和信息。

3 智能电网隐私保护技术分析

3.1 智能电网中的隐私问题分析

智能电网中有诸多需要解决的隐私问题,一般将智能电网中的隐私问题分为两大类:

类别一:以前不容易获得的个人信息;

类别二:获得(或操纵)以前不存在的个人信息的机制。

第一种问题包括在特定场所中使用的电器设备的细节信息,包括使用的具体电子设备,指出场所内合法或潜在非法操作中的个人模式和时间安排,计量表中能耗和个人电器设备中的细粒度时间序列数据。

第二种问题包括个人信息来源于哪些其他信息,以及智能电网可能存在一个相同的信息新来源。例如,电动汽车的充电可能提高从新能源数据中获取个体物理位置隐私的可能性。

房屋或建筑内进行的活动的细节描述可由“设备电子签名”和它们的时间模式取得。这些签名和模式可为假设居住着的活动提供基础(如:一个地方包含的个体数目以及何时住所空置)。虽然家电与其他能源消耗元素直接沟通的技术已经存在,但智能电网的实施可能会对它们的使用产生更加广泛的刺激。所有配备的设备可向它们的拥有者或操作者提供更详细的能源消耗信息,同时也可能向外界提供这些信息。

表 2 潜在的隐私问题

隐私问题	情况	分类
欺骗	能耗归咎到其他位置或其他车辆(在电动汽车的情况下)	类别二:虽然欺骗是一个现有的隐私问题,目前的电表读数系统(无论是人工抄表还是远程抄表)在没有与收集数据人员相互勾结的情况下,几乎没有给其他人操作数据的机会
确定个人行为/电器设备的使用	通过智能表计和家庭自动化网络数据可跟踪具体设备的使用。访问数据的使用情况,可揭露在家庭特定区域的电力使用的具体时间和地点,也可以表示活动和/或使用的电器设备的种类。此信息可能的用途包括:家电厂商可以将这一信息用于产品的可靠性和保修的目的;其他实体可以利用这个数据做有针对性的营销	类别一:智能电网的实施产生的数据可能会在一个大范围内更精细和可利用
进行实时远程监控	访问实时能源利用数据,可以揭示人们是否在设施或住所中,他们在做什么,醒着和睡着的模式,他们在建筑物的什么位置,以及有多少人正在建筑物中	类别二:目前存在的许多实时监控方法。与电脑相关的实时或接近实时的能源使用数据的可用性,将创建另一个监控的方式
数据的非电网商业用途	个人能耗数据存储可能揭示对其他实体如众多产品和服务提供商有价值的生活方式信息。供应商可能会为了有针对性的营销活动而购买属性列表	类别二:在现有的计量和计费系统之下,仪表数据在大多数情况下,没有足够的细度透露任何有关活动的细节。然而智能表计,使用时间和需求率和直接负荷控制设备可能会产生可被能源管理分析以及同类比较的细节数据。虽然此信息会给第三方创造有益价值,对消费者进行保护数据的教育有相当大的积极成果

表 2 列出了一些可能出现的隐私问题,并根据之前提出的类型一和类型二提供了一些关于隐私问题的性质分析。

智能电网中关于用户的隐私信息可能“有意”或“无意”的被泄露。任何采集和使用智能电网数据的组织,必须了解到可能对隐私产生的影响,并且为数据管理、安全和使用制定适当的计划。

3.2　智能电网数据分析

智能电网数据包括能源使用量的测量数据、发电数据、家电和设备的能耗报告等,这些数据将成为个人信息的新来源,例如:电力公司收集的个人信息可被用来识别个人身份,包括住址、业主的姓名、生日等。

智能电网数据元素(见表 3)反映能源利用的时间及度量,与传统的个人信息数据相关联时,可以折射出住宅用户的生活方式以及商业和工业用户的业务运作方式,如果没有得到恰当的安全保护,将对隐私产生影响。

表 3　对隐私有影响的智能电网数据元素

数据元素	描述
姓名	账户的所有人
地址	进行服务的位置
账号	该账户唯一的标识符
电表读数	在目前的帐单周期内 15 ~ 60 分钟(或更短)间隔记录千瓦时的能源消耗
实时账单	当前帐户上的数量
账单历史	过去电表的读数及账单,包括支付逾期付款/付款失败的历史(如果有的话)
家庭局域网	电器和设备使用的家庭网络
生活方式	何时房屋有人或无人,何时住户醒着或睡着,有多少电器正被使用
分布式资源	现场发电、存储设备、运行状态、电网的消耗、使用模式的存在
电表 IP	电表的 IP 地址
服务供应商	提供账户的机构的身份(主要与零售市场相关)

3.3　隐私影响评估

隐私影响评估(Privacy Impact Assessment,PIA)是一个确定采集、使用和披露个人信息过程中有关隐私、保密和安全风险问题的过程。隐私影响评估还意味着可用于减轻和尽可能消除所确定的风险的措施。

隐私评估的重点是:

(1)可被收集或创建的,能够揭示有关个人或在特定场所内活动(住宅或商业)的信息类型。

(2)确定这些不同类型的信息如何被利用。

(3)建议业务政策和做法,以减轻所确定的隐私风险。

各种在智能电网中提供、使用、获取数据的实体都能够从隐私影响评估中获益,隐私影响评估能够及时发现隐私风险,并采取措施减轻风险。

在执行隐私影响评估以及后续讨论的过程中,需要确定和解决表 4 中所列的问题。

表 4　隐私影响评估涉及问题

序号	涉及问题
1	智能电网的组件和实体可能会产生、存储、传输或维护哪些个人信息
2	这些个人信息相对其他系统和网络中的个人信息有哪些新颖和不同的地方
3	在智能电网中使用个人信息与在其他系统和网络中使用个人信息相比,有什么新颖的地方
4	智能电网的组件和实体可能带来哪些新的和特别的隐私风险
5	现有的法律法规和标准适用于智能电网中采集、创建和传递的个人信息的可能性
6	在智能电网中有什么建设性的标准化隐私惯例,有助于保护隐私和减少相关风险

对于隐私影响评估,隐私小组给出了一些建议的隐私原则(见表 5),收集或使用智能电网数据的组织可以采用隐私小组隐私影响评估的结论,指导自己的隐私影响评估,制定关于智能电网数据的相应的制度和方法。

表 5　隐私原则

隐私原则	具体内容
管理和问责制	①分配隐私责任 ②建立隐私审计 ③建立执法要求的政策和程序
警告及目的	①提供收集个人信息的警告 ②提供新信息使用目的和收集的警告
选择和同意	提供关于选择的警告
收集和适用范围	①限制收集 ②获取数据
使用和保存	①审查隐私政策和程序 ②限制信息保留
个人访问	①消费者访问 ②争端解决
披露和限制使用	①限制信息使用 ②披露
安全和防护	①只在需要时关联个人能源数据 ②移除标识 ③保护个人信息 ④不要因为研究目的而使用个人信息
准确度和质量	保证信息的准确和完整
开放、监控和具有挑战性的合规	①政策挑战程序 ②定期进行私隐影响评估 ③建立违反通知的做法

3.4 隐私保护建议

对智能电网隐私保护来讲,今后的挑战是创建一个被大家接受的智能电网隐私原则方案,目标是让个人参与智能电网以促进电力部门发展和创新。要实现上述目标,需要有效和透明的隐私惯例在智能电网中被贯彻执行,针对创建这种透明度,并获得智能电网参与者的信任,NIST 提出了关于所有参与智能电网的实体的建议,摘要列表包括:

1)在部署或参与智能电网前,进行隐私影响评估以确定智能电网收集、处理、存储的数据会对个人信息产生的风险,并确定适当的降低风险的方法。智能电网的实体可以参考隐私小组提出的方法,实施 PIA 的模型参考。PIA 应由如下方法执行:

●执行初步的 PIA 以确定存在的隐私风险,建立一个隐私度量的基准线。

●以下情况实施后续的 PIA:当组织、系统或应用程序发生巨大变化时;当提供智能电网数据如何使用要求的新法律法规落实时;其他任何影响智能电网业务实施的事件发生时,如涉及个人信息的信息安全事件等。

2)制定和正式起草隐私保护原则和其他部门的隐私政策、法规和适当的法律全集中的隐私政策和实践。隐私小组的特别建议如表 6。

3)制定一个全面的隐私用例集将帮助电力公司和第三方智能电网供应商严格跟踪数据流和收集、使用信息带来的隐私影响,并帮助组织解决和降低常见技术设计和业务惯例中相关的隐私风险。

4)教育消费者智能电网中的隐私风险以及他们作为消费者如何做才能降低这些风险。

5)与其他智能电网市场的参与者共享共同隐私问题的解决方案信息。

6)智能表计、智能电器和其他智能设备的生产商和经销商应当只收集维持智能设备运转的能源和个人数据。应当建立收集数据的默认值,只让设备在运转需要时使用和共享数据。

4 对我国智能电网隐私保护的思考

我国智能电网是以特高压电网为骨干网架、各级电网协调发展的坚强网架为基础,以信息通信平台为支撑,具有信息化、自动化、互动化特征,包含电力系统的发电、输电、变电、配电、用电和调度各个环节,覆盖所有电压等级,实现“电力流、信息流、业务流”的高度一体化融合的现代电网[11]。

智能电网信息化、自动化、互动化的特征,使得信息技术得以更加广泛、深入的应用,随之信息安全隐患及由此引发的风险也深入到电网生产、管理的各个环节。对于我国智能电网的六个环节而言,信息安全应重点关注的是智能用电[12]环节的安全防护。

表 6 隐私特别建议

隐私原则	特别建议
管理和问责制	组织必须正式任命人事岗位以确保现有的隐私保护政策和惯例被遵循。必须文档化定期培训、不断宣传和交流的要求,并贯彻执行。对所有数据的接入和修改进行审计
警告及目的	组织必须在收集、存储和共享能源使用信息和个人信息之前,给消费者有意义的、明确的、全面的警告。警告必须详细地描述哪个消费者信息将被使用,包括每个分支机构和第三方使用信息的目的。警告还需包括信息将在组织中持续多长时间以及会被分享给哪个第三方组织。在收集数据前进行明确、全面和准确的警告是制定其他原则的前提
选择和同意	组织必须清楚地、全面地、准确地向消费者描述可选项,并在切实可行的范围内,获得收集和使用个人信息的明确批准。消费者有放弃与供应商提供的核心服务不相关的数据收集和服务的选择权
收集和适用范围	只有遵循“警告和目的”中制定目的所需要的个人信息才能被收集。信息的处理应符合这些隐私原则
使用和保存	信息只为收集它们的目的所使用和披露,并只被送交给授权的第三方。个人信息应当被汇总和隐匿以尽可能限制泄露个人信息的可能性。个人信息只能被保存至收集它们的目的所需要的时长范围
个人访问	组织必须提供一个服务,即个人可以要求查看其相应的个人信息并修改错误。个人应当被告知他们的信息被分享给了谁
披露和限制使用	信息只为收集它们的目的所使用。个人信息除了向“警告和目的”中确定的组织或授予方明确同意的组织之外,不应披露给其他人。除非传票、授权令或法院命令强行责令披露,组织应当在向第三方披露信息前得到消费者的认可
安全和防护	各种形式的个人信息都应当被保护,免于遭受丢失、盗取、非授权接入、不当泄露、复制、使用或修改

智能用电环节担负着售电市场运营、需求侧管理、销售电价执行、电能计量管理、客户用电安全、供电服务等方面重要职责,实现与客户间的能量流、信息流、业务流的双向互动,因此,智能用电环节涉及众多的用户用电信息,是用户隐私风险最大的领域,需要重点关注。

目前我国智能电网正处于发展阶段,隐私保护尚处于探索起步阶段,相对于国外稍显迟缓。面对智能电网给用户带来的隐私风险,我国智能电网应加快隐

私保护进程,明确界定隐私保护范围,最大限度地保护用户隐私,同时重视对用户权利保护的细化规定,实行用户权利告知和投诉制度。此外,应加大对侵害用户隐私权的惩罚力度,促进相关机构重视对用户信息隐私权的保护。

5　结束语

文中关于隐私保护的讨论并不是法律意见,而是总结了当前相关机构关于智能电网隐私保护问题的探讨,并提出了自己的见解和解决这些问题的相关建议。

智能电网是一个不断发展新技术、服务与传统的解决方案和组织相结合的实体结构。随着智能电网的发展,必将有新的隐私威胁、脆弱性和相关的风险[13]出现。随着智能电网的扩大和成熟,隐私的冲击和影响将发生改变,关于智能电网隐私的探讨将会进一步加深。

参考文献:

[1] Xiao Shijie. Consideration of technology for constructing Chinese smart grid[J]. Automation of electric power systems, 2009,32(9):1-4.

[2] Li Xinyuan, Wei Wei, Wang Yuhong, et al. Study on the development and technology of strong smart grid[J]. Power system protection and control, 2009,37(17):1-7.

[3] 梅绍组. 网络与隐私[M]. 北京:清华大学出版社,2003.

[4] 周汉华. 个人信息保护前言问题研究[M]. 北京:法律出版社,2006.

[5] 马　特. 英美法中的个人隐私保护[J]. 重庆理工大学学报(社会科学),2010,24(10):92-97.

[6] Warren S D, Brandeis L D. The right to privacy[J]. Harvard law review, 1890,4(5):193-220.

[7] Westin A F. The right to privacy[M]. Cambridge: Cambridge University Press, 1967:25-37.

[8] Schoeman F D. Philosophical dimensions of privacy[M]. Cambridge: Cambridge Univ Press, 1984:33-35.

[9] Rezgui A, Bouguettaya A, Eltoweissy M Y. Privacy on the Web: Facts, challenges, and solutions[J]. IEEE security & privacy, 2003,1(6):40-49.

[10] NIST. Guidelines for smart grid cyber security: Vol. 2, privacy and the smart grid[R/OL]. 2010. http://csrc. nist. gov/publications/nistir/ir7628/nistir-7628_vol2. pdf.

[11] 刘振亚. 智能电网知识读本[M]. 北京:中国电力出版社,2010.

[12] 刘振亚. 智能电网技术[M]. 北京:中国电力出版社,2010.

[13] 高培明,侯新华. 智能化发展给电网带来的风险与防控对策[J]. 能源技术经济,2011,23(7):60-66.

(上接第 188 页)

由研究[J]. 计算机应用研究,2011,28(10):3865-3868.

[3] 向　阳,李腊元,杨利平,等. 基于 Ad Hoc 的 QoS 多播路由协议研究[J]. 计算机工程与应用,2006,27(10):147-150.

[4] 高中山,张晓洁. 多播协议中拥塞控制的可靠性研究[J]. 华北电力大学学报,2006,33(4):88-92.

[5] 张文斌,潘广贞,黄玉飞,等. 基于 ODMRP 的稳定路由协议 LB-ODMRP[J]. 微电子学与计算机,2013,30(4):111-114.

[6] 陆小三,周　颢,赵保华. 基于 MAODV 无线 Mesh 网多播路由协议的优化[J]. 电子技术,2011,38(4):7-9.

[7] Chai-Keong T, Guillermo G, Santithorn B. On-demand associativity-based multicast routing for ad hoc mobile networks (ABAM)[C]//Proc of 52th IEEE VTS vehicular technology conference. [s. l.]:[s. n.],2000:987-993.

[8] Biswas J, Barai M, Nandy S K. Efficient hybrid multicast routing protocol for ad-hoc wireless networks[C]//Proc of 29th annual IEEE international conference on local computer networks. [s. l.]:[s. n.],2004:180-187.

[9] 王婷婷. 基于发布订阅的多播路由协议关键技术研究[D]. 北京:北京邮电大学,2009.

[10] Kaliaperumal B, Ebenezer A, Jeyakumar. Adaptive core based scalable multicasting networks[C]//Proc of INDICON. [s. l.]:[s. n.],2005:198-202.

[11] Li L, Li C. A hierarchical QoS multicast routing protocol for mobile ad-hoc networks[J]. Chinese journal of electronics, 2006,15(4):573-577.

[12] Latiff L, Aliand A, Ooi C. Location-based geocasting and forwarding (LGF) routing protocol in mobile ad-hoc network[C]//Proc of advanced industrial conference on telecommunications/service assurance with partial intermittent resources. [s. l.]:[s. n.],2005:536-541.

[13] Sun B L, Li L Y. A QoS-based multicast routing protocol in ad-hoc networks[J]. Chinese journal of computers, 2004(10):1402-1407.

[14] Lau K S, Pao D. Tree-based versus gossip-based reliable multicast in wireless ad-hoc networks[C]//Proc of 3rd IEEE consumer communications and networking conference. [s. l.]:[s. n.],2006:421-425.

智能电网隐私保护技术的分析研究

作者： 黄秀丽， 张涛， 马媛媛， 王玉斐， 华晔， 陈璐， HUANG Xiu-li， ZHANG Tao， MA Yuan-yuan， WANG Yu-fei， HUA Ye， CHEN Lu

作者单位： 中国电力科学研究院,江苏 南京,210003

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(2)