电网融合泛在网信息平台设计及安全威胁分析

戚 湧 郭诗炜 李千目
(南京理工大学计算机科学与工程学院 南京 210094)

摘 要 随着电力系统信息化的快速发展,电力系统已建立成EMS能量管理系统、SCADA电网调度自动化系统等管理系统。为了解决电力系统众多异构子系统造成的"信息孤岛"问题,提出基于SOA的电网融合泛在网信息平台架构,并针对其体系结构分别从基础设施层、数据层、服务层对安全威胁进行研究。基础设施层的安全威胁研究主要针对终端设备、网络和服务器等物理设施的安全问题,数据层的安全威胁研究主要针对隐私信息泄漏或破坏以及非法访问等安全问题,服务层的安全威胁研究主要针对认证授权措施不当等问题。最后针对各层所面临的安全威胁提出相应的安全措施和建议。

关键词 面向服务,融合泛在网,安全威胁,措施
中图法分类号 TP393.0 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.03.033

Design and Security Threats Analysis for Information Platform of Fusion Ubiquitous Network in Power Grid

QI Yong GUO Shi-wei LI Qian-mu
(School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract With the rapid development of electrical informatization, the electric power system has established EMS (Energy Management System), SCADA(Supervisory Control And Data Acquisition) power grid automatic dispatching system, etc. In order to solve the problem of "information islands" caused by various heterogeneous subsystems in the electric power system, an information platform of the SOA-based fusion ubiquitous network in power grid was proposed. Threats of the infrastructure layer, data layer and service layer were researched on the architecture of the system. The infrastructure layer threats include security threats for terminals, networks and servers. Data layer threats include private information leakage or damage and illegal access. Service layer threats include improper measures of certificate authority. Finally, security measures and recommendations were given for security threats faced by each level.

Keywords Service-oriented, Fusion ubiquitous network, Security threats, Measures

1 引言

早在20世纪60年代,我国电力行业就开始积极进行信息化建设,目前电力系统企业已建成电网调度自动化系统(SCADA)、能量管理系统(EMS)、配电自动化系统(DAS)、配电管理系统(DMS)、地理信息系统(GIS)、企业综合管理信息系统(MIS)、办公自动化系统(OAS)、辅助决策支持系统(DSS)、电力营销管理信息系统(PSMIS)等多个信息系统[1-3]。

虽然电力系统信息化建设已经达到一定的规模,但由于这些信息系统由不同的软件开发商在不同时期分别开发完成,相互之间不能通信,并且这些信息系统归由不同的电力企业或业务部门使用,导致各部门的网络资源没有充分共用,信息不能合理共享以及部分网络和应用系统自成体系,从而造成电力系统中各市县电力公司、各发电厂及省电力公司的信息系统资源相互隔绝,形成大量分散异构的"信息孤岛"。"信息孤岛"的存在严重阻碍了信息资源的有效共享,造成大量的重复建设和资源浪费,使得电力系统信息化的应用受到极大的限制[4]。

自Gartner公司于1996年提出面向服务的体系架构(SOA)[5]之后,这种与平台无关的粗粒度松耦合的系统构建方法就被广泛应用于现代企业集成领域,它将所有资源以及对这些资源的操作都视为服务。在基于SOA的体系架构中有3类角色:服务请求者、服务提供者和服务注册中心[6]。服务提供者通过服务注册中心发布服务,服务请求者从服务注册中心查找需要的服务,这使得服务的接口与实现相分离,服务资源能够灵活组合以适应用户动态变化的需求。

本文针对电力系统的信息化建设现状和特点,将SOA应

到稿日期:2015-11-06 返修日期:2016-03-15 本文受国家自然科学基金项目(61272419),江苏省未来网络前瞻性研究项目(BY2013095-3-02)资助。

戚 湧(1970—),男,博士,教授,博士生导师,CCF高级会员,主要研究方向为网络信息安全,E-mail:790815561@qq.com;郭诗炜(1990—),女,硕士生,主要研究方向为网络信息安全,E-mail:guosw1990@126.com;李千目(1979—),男,博士,教授,博士生导师,主要研究方向为网络信息安全,E-mail:liqianmu@126.com。

用于电力系统的异构网络资源的融合中，设计电网融合泛在网信息平台，并分析其中的安全问题，最后针对各类安全威胁提出相应的安全措施和建议。

2　电网融合泛在网信息平台架构

SOA 是一种注重模块复用及灵活松耦合的软件架构范式，适用于描述 SOA 架构下企业信息系统的内部架构。SOA 参考体系架构如图 1 所示，总共分为 5 个层次。

数据层：各系统的业务数据资源和基础平台构成的后端层，其组成元素包括数据库、操作系统等遗留信息系统；

基本层：将底层数据和平台资源封装为基本服务，它也是独立完成基本功能的最小单元；

组合层：将多个基本服务组合为具有更强大功能的组合服务，以满足业务需求；

流程层：通过业务逻辑将多个服务或组合服务编排为可协作处理某项复杂功能的业务流；

前端层：由服务请求者调用相关服务和业务流程，并返回服务响应。

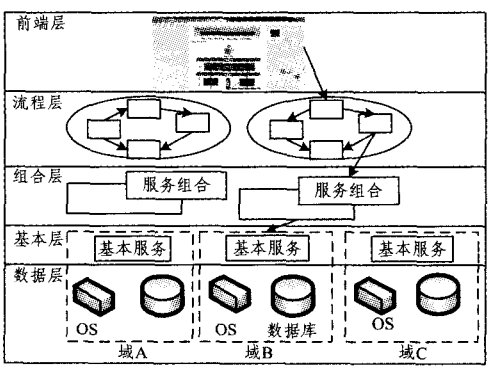

图 1　SOA 参考体系架构

基于 SOA 的电网融合泛在网信息平台是利用 SOA 面向服务的思想解决当前电力系统信息化建设中面临的网络资源和信息资源共享困难、信息孤岛严重、不同的应用系统间难以协作以及应用系统难以支撑业务变化等难题而提出的。平台从应用模式的角度出发，将电力系统中的各种网络和应用子系统包装成独立的标准服务，使各种服务之间能够根据不断变化的业务需求任意组合调用，从而提高软硬件资源的利用率，减少开发和维护成本，为业务系统开发人员提供开发、运行、管理的统一手段，实现业务和技术的统一。电网融合泛在网平台可以使应用系统开发人员将更多注意力放在客户需求分析上，而无需过多关注其他技术细节。

如图 2 所示，该信息平台主要分为三大层次和两个总线：服务层、数据层、基础设施层，企业服务总线和数据总线。在基于 SOA 的电网融合泛在网信息平台体系结构中，可以将电力系统中的上层应用看成是 SOA 体系中的服务请求者，而将底层基础设施看成是服务提供者。

最上层为服务层，业务的实现是以服务的使用为基础的，服务层的概念进一步将系统结构细化，将每个系统的业务细化为若干服务，主要分为两类：应用服务和基础服务。应用服务为各个业务系统提供所必需的服务支持，基础服务是服务层与数据层交互的途径。通过基础服务，应用服务可以访问读取数据，并且实现各服务间数据的交互。安全服务则贯穿于整个服务层，在所有应用服务的基础服务流程中都需要通过安全服务解决存在的安全问题，这也恰好与 SOA 的概念相吻合，即系统的运行基于不同的服务。所有服务都发布在企业服务总线上，所有应用系统都统一通过企业服务总线调用服务接口，实现互联互通。第二层的数据层是系统运行的实际实现形式，它包含系统业务所需的数据以及安全服务的相关数据。第三层是基于 SOA 的电网融合泛在网信息平台最底层的结构层次，基础设施层为整个信息平台提供软硬件资源支撑，并执行系统控制命令。

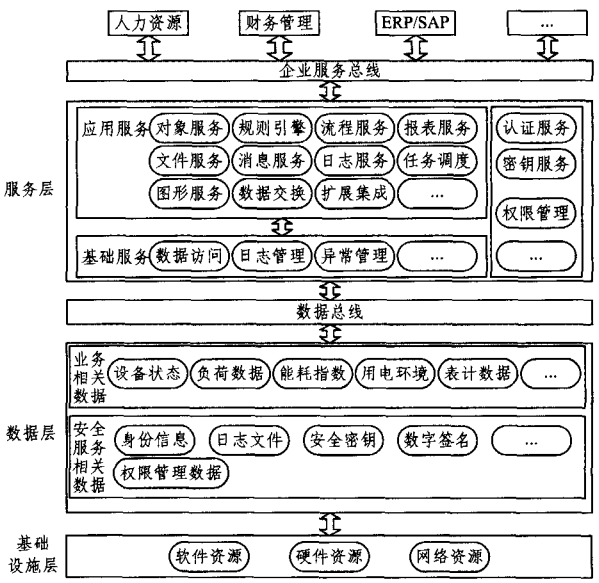

图 2　基于 SOA 的电网融合泛在网信息平台架构

3　电网融合泛在网信息平台的威胁分析

在电网融合泛在网平台的应用环境下，所涉及的安全议题十分广泛，包括：信息网络的安全防护体系研究、安全需求与策略分析、基础支持系统的设计与应用、信息系统与业务系统的安全保障措施、系统的安全评估和容侵能力等。

电网融合泛在网由网络、设备和数据等要素组成，其中每个要素都有各种可能被利用的弱点。网络线路有被窃听的危险；网络中的设备、操作系统以及应用系统所依赖的各种软件在系统设计、协议设计、系统实现和配置等方面都存在大量的安全弱点和漏洞，有被利用和攻击的危险。从服务集成角度看，为了电力企业中的各应用系统之间能实现跨平台的操作，所使用的通信协议的格式就必须是开放的标准文本格式，而不能使用二进制格式。然而以文本形式在网络上传输的消息或协议比二进制格式的消息或协议更容易也更多地遭受安全攻击和威胁。

面对一个日益复杂的网络环境，若要进行安全需求分析，就必须先动态地、发展地认识其中存在的安全隐患和威胁。只有深入了解电网融合泛在网信息平台的发展和应用现状，结合对其网络软硬件设备的基础和原理的专业分析，才能深入了解影响电网融合泛在网信息平台安全的潜在矛盾、威胁

和现实状况，制定出一整套完整的、科学的安全结构体系，从而从根本上解决电网融合泛在网信息平台的整体安全问题。

3.1 基础设施层安全威胁

在电网融合泛在网信息平台的三层架构中，基础设施层是重要的数据来源和控制命令的执行场所。基础设施层的部分设备分布在无人监测的环境中，容易遭受安全威胁。而随着移动智能设备的迅速发展，新的安全隐患也被引入基础设施层。目前针对基础设施层的主要安全威胁如表 1 所列。

表 1 基础设施层安全威胁

威胁名称	威胁描述
物理攻击	对设备本身进行物理破坏，使设备无法正常工作，导致信息缺失等。
设备故障	设备由于环境或老化等原因失去性能，不能正常运行。
拒绝服务攻击	攻击者向网络发送大量无用数据，这些数据使得大量的请求涌向服务器，从而消耗服务器系统资源，并最终导致目标服务器崩溃或使其无法正常工作。
伪装	未经授权的用户假装成合法用户，或特权小的用户假装成特权大的用户访问系统。
数据篡改	攻击者将截获的信息进行修改后传给接收者。
非法访问	计算机或网络资源被未授权的人或以非授权的方式使用。
虚假路由信息	攻击者通过发送一些虚假的路由信息来影响路由协议的工作，如改变路径拓扑、消耗节点资源、形成循环路由等。
海量设备认证问题	基础设施层中包含有海量终端设备，如何对这些设备的身份进行管理和认证，是电网融合泛在网信息平台中亟待解决的安全问题。
重放攻击	攻击者记录下登录服务器过去已经接受过的加密或散列名称或密码，并再次向服务器发送，获取服务器的信任。
信息窃听	攻击者可轻易地截获正在通信链路上传输的信息，从而分析出信息中的敏感数据。另外，通过对信息包的窃听，还可以对网络中的网络流量进行统计分析，推导出终端设备的作用等。

3.2 数据层安全威胁

数据层中保存着大量的用户隐私数据和企业内部信息。这些数据是电网融合泛在网信息平台体系中最重要的信息资源和业务基础，上层的服务需要频繁访问这些数据来完成各种功能。目前数据层面临的主要安全威胁如表 2 所列。

表 2 数据层安全威胁

威胁名称	威胁描述
数据丢失	数据的丢失、窃取或非法移除等。
信息泄漏	机密信息由于数据传输、存储和展现等过程中的不安全因素，被隐私收集者获取而造成的信息泄漏。
恶意篡改	未授权的用户篡改敏感信息，破坏机密信息的完整性。
数据库攻击	攻击者通过口令入侵、特权提升、漏洞入侵、SQL 注入、窃取备份等手段，获取数据库中的信息。
伪装	未经授权的用户假装成合法用户或特权小的用户假装成特权大的用户访问系统。
非法访问	计算机或网络资源被未授权的人或以非授权的方式使用。

3.3 服务层安全威胁

服务层的某些应用服务会收集大量的用户隐私数据和企业内部信息进行数据分析和处理，因此必须对这些数据中的隐私进行特定或通用的保护。同时，由于服务层提供了种类繁多的服务，各个服务的安全需求也不尽相同。如何制定合适的安全策略，如何在用户与各异构系统之间、系统与系统之间建立和维护信任，如何建立和管理用户与各异构系统之间、系统与系统之间的会话关系，成为了服务层的安全难题。目前服务层面临的主要安全威胁如表 3 所列。

表 3 服务层安全威胁

威胁名称	威胁描述
非授权访问	攻击者在未经授权的情况下不合法地访问系统网络数据，包括未授权的用户假冒合法用户进入网络系统进行操作、特权小的合法用户擅自扩大权限以未授权的方式进行操作等。
恶意代码	没有实际作用却可能被利用、攻击的代码。一般而言，系统中不必要的代码都可以看作恶意代码。
数据挖掘中的隐私泄漏	服务层中的服务对海量的数据进行数据挖掘，通过分析结果改善服务，但同时也使得数据中的隐私面临巨大风险。
控制命令伪造攻击	攻击者通过伪造服务层中系统的控制命令进行操作，达到恶意利用系统或破坏系统的目的。
漏洞攻击	攻击者利用程序存在的漏洞对系统进行攻击。
后门	系统开发人员出于恶意或为了维护方便在系统中设置的可以绕过系统安全控制措施的程序方法，可能被攻击者用来控制、破坏系统。
滥用特权	系统管理员故意或错误地使用特权获取专用数据。
病毒、木马	病毒和木马会对系统进行破坏或窃取机密数据，是系统中较为普遍的安全威胁。

4 电网融合泛在网信息平台的防护措施

基于 SOA 的电网融合泛在网信息平台的安全防护必须提供如下保护措施：保证通信过程中数据的完整性(Data Integrity)、数据的机密性(Data Confidentiality)、不可否认性(Non-repudiation)、身份认证(Authentication)、授权和访问控制(Authorization & Access Control)等。这也是保证电网融合泛在网信息平台在集成服务环境下的安全所要解决的重要问题。

4.1 基础设施层的防护措施

基础设施层主要涉及服务器、网络、终端节点等设备的物理安全以及通信安全，包括通信过程中数据的完整性、机密性和一致性等，是电网融合泛在网信息平台安全的基础。以下是针对基础设施层安全威胁的一些防护措施。

(1)技术方面

对终端设备的身份采取一定的管理和保护措施。这可能会造成设备认证的延时，实际应用时需要在系统的安全性和效率中寻求平衡，制定出较合理的设备认证策略。

结合电网融合泛在网信息平台的特点，利用密钥服务、安全路由、安全数据融合等技术保证消息传送过程中的安全性；利用身份认证、密钥协商以及密钥管理等技术保证网络和终端设备的可信接入。

(2)法律方面

加强对破坏电力系统基础设施、威胁系统安全的行为立法，明确违法行为及其代价[7]。

(3)管理机制方面

建立申报审批制度，对设备和介质的使用、维修、报废等操作进行记录；同时加强外部人员管理，对所有维修、服务的外部人员进行登记并全程陪同。

4.2 数据层防护措施

数据层的防护措施的主要目的是保证重要数据的可用性、机密性和完整性。以下是针对数据层安全威胁的一些防护措施。

(1)技术方面

加强数据库的认证授权机制和访问控制机制，根据用户

(下转第 174 页)

[26] GADAT B, VAN N, RIES L. Method Of Decoding A Correcting Code, For Example A Turbo-code, By Analysis Of The Extended Spectrum Of The Words Of The Code: US, US20140351667 [P]. 2014.

[27] El YOUSFI A. Code-based Identification and Signature Schemes [D]. Technische Universitat Darmastadt. 2013.

[28] BERLEKAMP E R, MCELIECE R J, TILBORG H C A V. On The Inherent Intractability Of Certain Coding Problems [J]. IEEE Transactions on Information Theory, 1978, 24(3): 384-386.

[29] 岳殿武. 信息论与编码简明教程[M]. 清华大学出版社, 2015: 166-178.

[30] GABORIT P, ZEMOR G. Asymptotic improvement of the Gilbert Varshamov bound for linear codes[J]. IEEE Transactions on Information Theory, 208, 54(9): 3865-3872.

(上接第 152 页)

的身份和安全等级授予其相应的数据操作权限，有效保障数据的安全性和机密性。

应用安全审计机制记录和分析所有用户对数据的所有相关操作，加强数据溯源能力，数据文件一旦被非法访问，通过日志文件就能快速定位到出现问题的访问端，并可以查看和还原出数据文件被泄漏的原因、时间和访问人，避免否认抵赖等恶意行为。

(2)法律方面

确立数据安全的核心内容，如基本原则、监管模式、等级保护等，在此基础上完善数据保护的相关法律。

(3)管理机制方面

对重要的数据文件进行定期备份，保证数据的可用性。

完善数据管理制度，严格管理存储介质和移动外设的使用，避免信息泄漏。

4.3 服务层防护措施

服务层根据从数据层中获取的信息，通过分析处理为业务系统提供服务，是电网融合泛在网信息平台做出决策的核心部分。以下是针对服务层安全威胁的一些防护措施。

(1)技术方面

使用标准化方式在信任边界的各种认证、授权系统之间共享身份和策略信息。使用联合身份管理，在各目标应用服务之间建立可信关系，并共享身份和策略，确保已通过认证的身份能够被任何一个应用服务识别，从而使该身份相关联的用户能够在不同应用服务之间进行跨域访问，同时避免身份伪造和命令伪造。

加强不同安全环境下和安全域中的服务间的有效安全协作，从而确保整个体系的安全。

对服务进行管控，保证服务的受限受控调用，对服务的调用过程进行认证授权，以防止服务被攻击者或用户非法使用以及服务器的拒绝访问等问题出现。

使用漏洞挖掘技术检测代码漏洞并进行修补，防止攻击者利用代码漏洞对平台进行攻击。

(2)法律方面

对利用电网融合泛在网信息平台威胁用户或者系统安全的行为立法，准确把握和适当增补、完善相关法律条款。

(3)管理机制方面

加强人事安全管理，依据行政上的管理体系建立起自上而下的安全管理机构，并为每一级设立相应的安全策略，明确各级权限职责和操作规范，加强账号安全管理。

结束语 本文分析了 SOA 的参考体系架构，即数据层、基本层、组合层、流程层和前端层，给出了基于 SOA 的电网融合泛在网信息平台架构，其主要包括基础设施层、数据层、服务层、数据总线和企业服务总线。针对给出的信息平台体系架构，详细分析了各层中可能存在的安全威胁，并提出了相应的防护措施。电网融合泛在网信息平台能够解决现阶段电力系统信息化建设中异构网络资源共用和信息共享的难题，但同时又会带来许多信息安全方面的新问题。因此，需要对其进行深入研究和探讨，消除安全隐患和威胁，促进电力系统信息化建设的安全发展。

参 考 文 献

[1] XU W B, SUN Z, CHEN J J. Research on Power System Integration Based on SOA[J]. China Instrumentation, 2007(6): 46-49. (in Chinese)
许卫兵，孙佐，陈继军. 面向服务架构(SOA)的电力系统信息集成研究[J]. 中国仪器仪表，2007(6)：46-49.

[2] BI R H, YANG Z C, WANG Y Z. Studies on Information Integration of MAS-based SOA Model in Power System[J]. Power System Protection and Control, 2010, 38(7): 63-67. (in Chinese)
毕睿华，杨志超，王玉忠. 基于多智能体 SOA 模型的电力系统信息集成的应用研究[J]. 电力系统保护与控制，2010，38(7)：63-67.

[3] LIU G M, SONG Y, TENG X L, et al. Development of Electric Power Information Integration Platform Based on SOA Framework[J]. Electric Power, 2012, 45(6): 96-99. (in Chinese)
刘国民，宋雨，滕晓雷，等. 基于 SOA 架构的电力信息一体化平台开发研究[J]. 中国电力，2012，45(6)：96-99.

[4] XU W B. Research on Information Integration Platform of Power System Based on SOA [D]. Nanjing: Southeast University, 2008. (in Chinese)
许卫兵. 基于 SOA 的电力系统信息集成平台的研究[D]. 南京：东南大学，2008.

[5] HIRSCHHEIM R, WELKE R, SCHWARZ A. Service-Oriented Architecture: Myths, Realities and a Maturity Model[J]. MIS Quarterly, 2010, 9(1): 37-48.

[6] ZHEN F, LIU M, DONG M Y. SOA Message-oriented Middleware Based System Integration Method for Business Process [J]. Computer Integrated Manufacturing Systems, 2009, 15(5): 968-989. (in Chinese)
甄甫，刘民，董明宇. 基于面向服务架构消息中间件的业务流程系统集成方法研究[J]. 计算机集成制造系统，2009，15(5)：968-989.

[7] LI Z, PENG Y, XIE F, et al. Security Threats and Measures for the Cyber-physical System[J]. Journal of Tsinghua University (Science and Technology), 2012, 52(10): 1482-1487. (in Chinese)
李钊，彭勇，谢丰，等. 信息物理系统安全威胁与措施[J]. 清华大学学报(自然科学版)，2012，52(10)：1482-1487.