四川电力信息安全集中监测分析平台研究与应用

刘姗梅，柴继文
（国网四川省电力公司电力科学研究院，四川 成都 610072）

摘 要： 针对四川电力当前信息安全数据较分散、缺乏实时监控问题，提出建立信息安全集中监测分析平台，提取各系统中与安全相关的数据，并利用实时监控手段弥补安全数据短板，对获取到的海量数据进行综合展示分析，全面地分析监测报告，帮助深入掌握系统安全漏洞和信息安全趋势，实现安全技术和管理的结合，同时利用关联分析可以找出安全事件中各种属性之间的相关特性，排除无意义的信息，及时对安全问题进行快速定位，提升了网络信息安全预警防护能力。

关键词： 信息安全；集中监测；预警分析

Abstract: Aiming at the scattered information security data and the lack of real－time monitoring at present in Sichuan power grid, a centralized information security monitoring and analysis platform for Sichuan Electric Power Company is presented. The centralized monitoring and analysis platform can extract the useful data from the existing systems and monitor the security vulnerability on the web or weak passwords etc. The comprehensive analysis report of the mass data stored in the information security monitoring platform can help to know well the system security vulnerabilities and the trend of information security. Meanwhile, the association analysis from the platform can help to find out the related characteristics of security events, which can exclude the meaningless information and rapidly improve the capacity of the early warning.

Key words: information security; centralized monitoring; early warning analysis

中图分类号： TM769 **文献标志码：** A **文章编号：** 1003－6954(2014)01－0023－03

0 引 言

随着国家电网公司信息化的不断建设和完善，八大业务应用整体全面推广、拓展深化应用，信息化效能、效率、效益提升作用明显，信息系统的基础性、全局性、全员性作用日益增强。电网信息安全已经提到与安全生产同样高度，信息系统安全成为电力安全的最重要组成部分之一。目前国家电网公司已建成边界监测系统、桌面终端管理系统等信息安全相关系统，但各系统着重点不同，数据较分散，同时对于内网邮箱弱口令、门户弱口令、网站漏洞等缺乏实时监控手段，不利于信息安全督查工作，也为信息安全埋下了隐患[1]。

针对上述问题，对适合四川电力的信息安全集中监测分析平台进行研究应用，该平台能提取现有系统中与安全相关的数据，并对其进行整合、分析；能对网站漏洞、系统弱口令等进行实时监测；能对数据进行综合展示分析，全面地分析监测报告，帮助深入掌握系统安全漏洞和信息安全趋势，督查人员通过报告能及时定位安全风险，第一时间通知运维单位快速整改。

1 集中监测分析平台总体架构

信息安全集中监测分析平台包括信息安全相关数据抽取规则管理、信息安全相关数据抽取、安全策略配置和下发、系统口令、扫描分析、漏洞扫描分析、安全事件集中管理、安全事件关联分析、安全设备状态实时监控、全景展示等功能模块[2]。图1为系统总体架构图。

系统应用采用满足技术先进性与成熟性相结合的基于J2EE的多层技术构架，以提高系统的灵活性、可扩展性、安全性以及并发处理能力。采用组件技术将界面控制、业务逻辑和数据映射分离，实现系统内部的松耦合，灵活、快速地响应业务变化对系统的需求。系统层次结构总体上划分为客户层、接入表示层、业务逻辑层、数据层（包含数据映射层和数据源），通过各层次系统组件间服务的承载关系，实现系统功能。系统技术架构如图2所示。

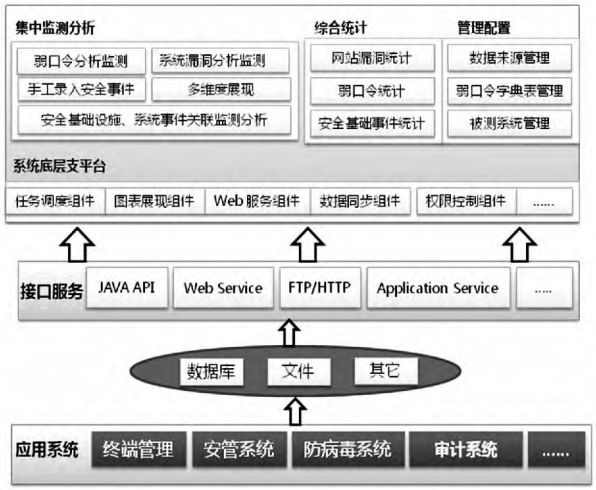

图 1　系统总体架构图

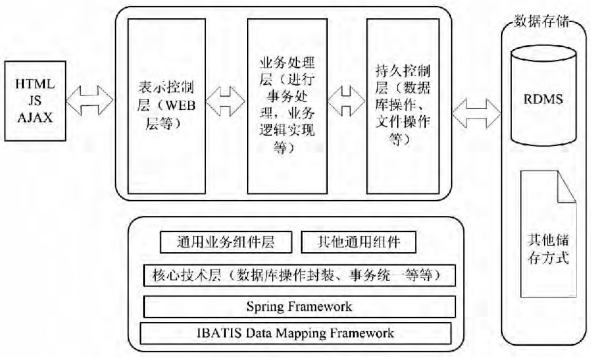

图 2　系统技术架构图

表示控制层对应平台中的控制器，实现画面与后台的数据交换、画面之间的迁移、画面数据的检查等功能；业务处理层对应具体的业务，在此层处理业务逻辑，并通过数据库操作层完成到数据库的交互；持久控制层对应数据库操作，所有的数据库操作都必须且只能集中在该层。控制器依赖于业务处理层，而业务处理层依赖于持久控制层，通过依赖注入功能，可以将这种依赖性通过相关配置进行统一管理，最大限度地降低各层次之间的耦合性[3]。

1.1　现有安全数据整合

现有安全数据整合模块建立信息安全数据表，提取四川电力现有信息系统中与安全相关的数据，进行跨部门、跨平台的安全信息的统一收集、分析、处理。在数据抽取、转换和加载（ETL：Extract，Transact，Load）过程中使用包括直接抽取、文件抽取、WEB 抽取等几种常见形式[4]。对不同应用系统，采用不同抽取方式；甚至对同一应用系统中不同的业务数据，也可以采用不同抽取方式。

直接抽取是指 ETL 服务器直接连接到应用系统后台数据库中直接抽取所需数据的方式，因此必须设置严格的权限控制，保证用户不能访问和修改系统中的其他敏感信息，以免造成安全问题。且由于会对应用系统数据库造成大量负荷，因此必须进行抽取时间窗口控制，协调对外服务时间和抽取时间，以减少数据抽取对正常业务运行造成的影响。基于以上考虑，这里对数据敏感度较小、数据及时性要求不高的 IDS、IPS 入侵数据进行直接抽取。

WEB 抽取是通过 WEB 服务获取系统需要的数据的抽取方式。通过这种方式可以方便获取需要的数据，同时可以对这些数据做校验等操作，是目前一种先进的抽取方式，不便的是在数据量很大时，网络传输速度会很忙，严重影响系统性能。对于数据量较小、系统接口实现较困难的考核指标类数据采用 WEB 抽取完成。

文件交换是指将需要抽取的业务数据保存为有格式的文本文件，ETL 服务器通过读此文件内容来获取业务数据的数据抽取方式。文件交换对原数据库系统造成影响较小。采用此方式时，应用系统将需要抽取的数据按照约定格式保存在文件中，并通过 FTP、文件共享等方式将保存有业务数据的文件传递约定位置。ETL 服务器从约定位置取出数据文件，并通过文件分析引擎对文件进行分析，取出业务数据。这里除 IDS、IPS、小数据外，主要数据均采用文件交换形式传输，且传输时约定文件传输结束标志，标志内容为已传输完毕的数据文件的文件名，以及此文件的 MD5 验证码。ETL 服务器获取传输结束标志文件后，认为对应的数据文件已经传输完毕。然后再通过对数据文件进行 MD5 验证，将验证码与传输结束标志文件内的 MD5 验证码进行对比来验证数据文件是否完整。同时约定文件重传标记，当传递到约定交换位置的数据文件在上传完毕和下传开始期间发生损坏，导致约定位置的数据文件和应用服务器生成的数据文件不一致。这样，ETL 服务器根据约定位置的数据文件计算出的 MD5 验证码就和传输结束标志文件中的 MD5 码不一致，从而发现文件不一致的错误，发现错误后，ETL 服务器需要使用文件重传标志来通知应用系统重新传输相应的数据文件。

数据整合分析模块能帮助安全督查人员在原有系统数据的基础上增强对比分析，对各个信息系统产生的数据进行监测数量、监测位置、监测范围以及

数据的匹配度和数据类比结果进行分析，得出不同系统对相似对象监控的差异，并按时生成信息安全类比分析报告。

1.2 漏洞实时监测

四川电力地域广，所属地市单位、控股、代管单位众多而分散，而专职信息安全督查执行人员有限，无法及时对各单位的终端、网络等情况及时进行督查，而且在工作时间进行漏洞扫描会造成系统访问量增大，影响系统性能。为此，要在集中监测分析平台上实现实时监测功能，对四川电力范围内所有对内、对外服务网站漏洞及应用系统弱口令等进行实时监测与提醒。在实现方式上采用实时调度任务完成，分别设计网站扫描调度任务和弱口令扫描调度任务，扫描时由管理员根据系统实际运行情况配置调度任务执行时间、执行周期、扫描对象等信息，系统根据配置信息调度扫描任务进行自动定时(一般设定在夜间)扫描，自动汇总分析结果[5]。

在进行信息系统弱口令扫描时，对可直接获取口令明文的被测系统，本系统按照系统密码强度规则分析口令明文，判断口令的强度，对不符合规则的

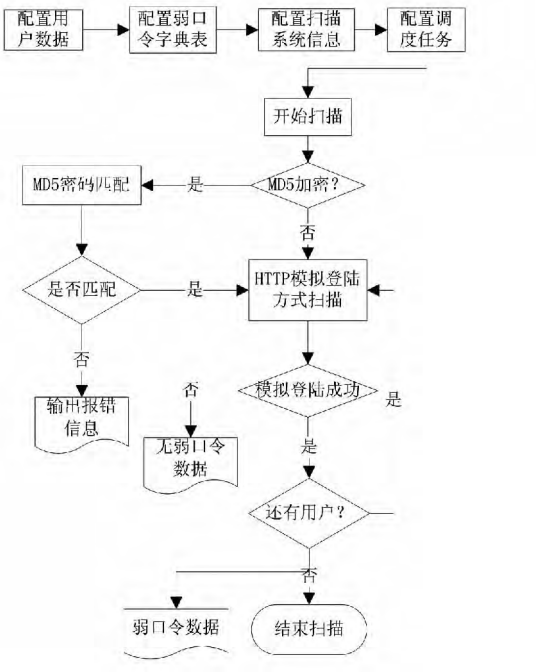

图 3 弱口令监测流程图

系统口令进行记录。对不能直接获取口令明文的被测系统，本系统按照弱口令字典表、ETL 抽取的系统用户账号信息，通过模拟系统登录原理，检查被测系统用户弱口令，记录不符合规则的系统口令，并保留检测分析过程，将发现不符合规则口令的过程、系统现场情况保存为图片作为督查证据。弱口令监测流程图如图 3。

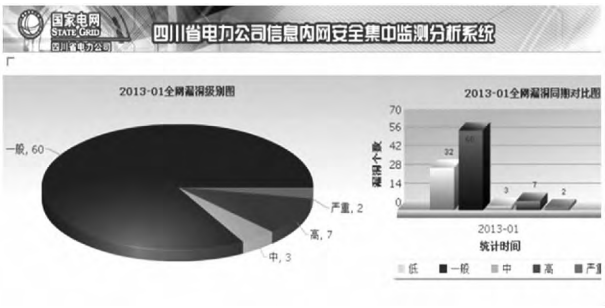

图 4 四川电力全网漏洞图

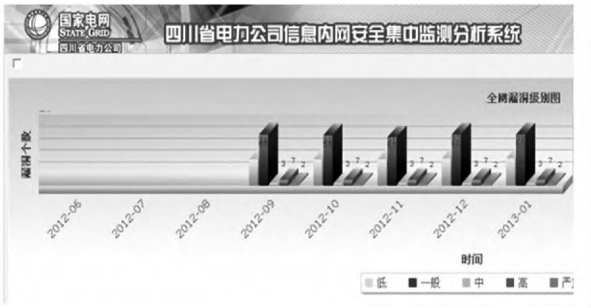

图 5 四川电力全网漏洞环比图

图 6 四川电力当月入侵日志统计

图 7 四川电力各单位告警统计

内、外网网站漏洞自动扫描模块主要扫描 SQL 注入、跨站脚本攻击(XSS)、失效的访问控制、缓存溢出问题、HTTP 响应拆分漏洞、参数篡改、隐式字段处理、目录遍历攻击等由 OWASP(open web application security project，开放式 web 应用程序安全项目)

(下转第 54 页)

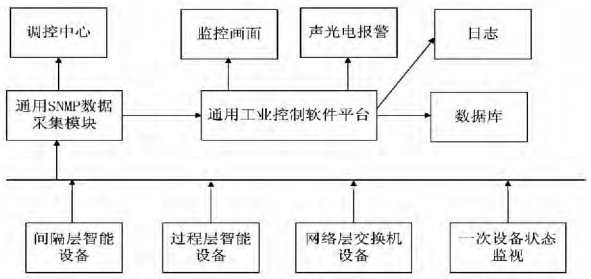

图3 智能变电站状态监测可视系统框架

6 结 论

针对继电保护状态检修工作展开研究，对保护设备缺陷进行分析，建立设备状态检修评估体系，并提出了相应的检修策略，取得了一些创新性成果。最后对智能变电站中二次设备状态检修进行了简要分析。相比传统变电站，智能变电站在实现状态检修方案更有基础以及可操作性，相信随着智能变电站的推广，继电保护设备状态检修将会得到更广泛应用。

参考文献

[1] 陈钢. 变电站电气设备的状态检修和状态监测技术现状及其发展趋势[J]. 贵州电力，2005(1)：15－17.
[2] 黄建华，变电站高压电气设备状态检修的现状及其发展[J]. 电力系统自动化，2008(2)：12－14.
[3] 陈维荣，宋永华，孙锦鑫. 电力系统设备状态监测的概念及现状[J]. 电网技术，2000，24(11)：12－17.
[4] 楼凤丹. 输变电设备状态检修评估分析软件系统[J]. 电力设备，2004(2)：10－12.
[5] 郑圣，赵舫. 故障信息处理系统中继电保护装置的可靠性研究[J]. 继电器，2005，33(11)：37－39.
[6] 李永丽，李致中，杨维. 继电保护装置可靠性及其最佳检修周期的研究[J]. 中国电机工程学报，2001，21(6)：63－65.
[7] 许蜻，王品. 电力设各状态检修技术研究综述[J]. 电网技术，2000(8)：48－52.

作者简介：

何小飞(1986)，硕士研究生，工程师，现从事继电保护二次检修工作。

(收稿日期：2013－09－23)

(上接第25页)

所公布的web应用安全漏洞，并针对出现的漏洞给出指导性建议。

1.3 全景展示

具有安全数据整合及漏洞实时监测功能的集中监测分析平台基本完全挖掘出四川电力当前信息系统运行过程中与安全相关的数据，依托对这些海量数据的综合展示分析，管理者能快速识别当前风险，为信息安全下一步投资提供充分的参考依据。

2 结 论

针对四川电力当前信息安全相关数据较分散，同时对于弱口令、网站漏洞等缺乏实时监控手段问题，不利于信息安全督查工作开展问题，提出建立信息安全集中监测分析平台，提取现有各系统中与安全相关的数据，并对其进行整合、分析，同时对弱口令、网站漏洞等进行实时监测，最后对海量数据进行综合展示分析，全面地分析监测报告，帮助深入掌握系统安全漏洞和信息安全趋势，实现安全技术和管理的结合，同时利用关联分析可以找出安全事件中各种属性之间的相关特性，排除无意义的信息，及时对安全问题进行快速定位，提高安全事件的应急响应处理能力。

值得说明的是，如何利用集中监测分析平台的海量安全事件进行信息安全态势感知，从总体上动态反映网络安全状况，并对网络安全状态的发展趋势进行预测和预警，是安全领域具有挑战性的问题，也是尚需进一步努力的地方[6]。

参考文献

[1] 四川省电力公司. 四川省电力公司“十二五”信息化规划[Z]. 2011.
[2] 沈昌祥，张焕国，冯登国，等. 信息安全综述[J]. 中国科学，E辑：信息科学，2007，37(2)：129－150.
[3] 郭红星. 网络信息安全预警监控系统设计与实现[J]. 计算机安全，2012(2)：48－50.
[4] 王刚军，张学松，郭志忠. 电力信息安全的监控与分析[J]. 电网技术，2004，28(9)：50－53.
[5] 赵衍. 基于网络数据挖掘的信息安全监控体系[J]. 上海管理科学，2010，23(4)：52－55.
[6] 余勇，林为民. 基于等级保护的电力信息安全监控系统的设计[J]. 计算机科学，2012(11)：440－442.

(收稿日期：2013－10－21)