Study on Information Secure Evaluation Framework of Smart Grid Application System

YU YONG, LIN WEI-MIN
State Grid Electric Power Research Institute, Jiangsu Nanjing 210003, China
yuyong@sgepri.sgcc.com.cn

Abstract: Smart Grid has the informaization, automaization, interactive features, which is the future development trend of the modern power grid. With further advancing smart grid construction, the information security problem has been more attention. Secure Evaluation is the key of application system's life cycle, which is important to improve system security measures. This paper describes the information secure evaluation framework of Smart Grid application system, the main purpose of including measurement, standards and criteria, evaluation process, evaluation of content, which content is divided into basic secure evaluation functional requirements and penetration attacks on security requirements, and that information secure evaluation is a measurement, reinforcement, and re-evaluation of the dynamic process, so as to enhance the security level of application system.

Keywords: Information security; Smart grid; Secure evaluation; SQL injection

智能电网业务系统的信息安全测评框架研究

余 勇；林为民
（国网电力科学研究院， 江苏 南京 210003）
yuyong@sgepri.sgcc.com.cn

摘要：智能电网具有信息化、自动化、互动化特征，是未来现代电网的发展趋势。随着智能电网建设的深入推进，其信息安全问题越来越得到重视。安全测评是业务系统生命周期的关键环节，是提高系统安全性的重要措施。本文详细描述了智能电网业务系统的信息安全测评框架，主要包括测评的目的、标准规范、测评的流程、测评的内容等，其中测评内容又分为基本安全功能要求和渗透攻击安全性要求，并指出安全测评是测评、整改、再测评的动态过程，从而提升业务系统的安全水平。

关键词：信息安全；智能电网；安全测评；SQL 注入

1 概述

电力工业是我国的基础产业和公用事业，电力网络和应用系统的安全是电力系统安全运行及对社会可靠供电的保证，直接关系到我国各行各业的发展、社会的安定和人民生活水平。一旦电力系统出现信息安全问题，将危及电网的安全运行，所造成的损失和影响将是无法估量的，电力系统的信息安全已经成为国家安全的重要组成部分。据统计，新发现的安全漏洞每年都要增加一倍，管理人员不断用最新的补丁修补这些漏洞，而且每年都会发现安全漏洞的新类型，入侵者经常能够在厂商修补这些漏洞前发现攻击目标。目前黑客的攻击规模与频繁度越来越高，他们越来越关注业务系统本身的安全漏洞，如 SQL 注入（程序编写者在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患，用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据）、跨站脚本（由于程序对用户输入的字符没有进行严格过滤，导致黑客写入恶意脚本进数据库，当其他用户访问 WEB 网站时，程序从数据库查询出这些恶意脚本并执行）等。许多电力业务系统在设计时安全性未作详细考虑，各种安全隐患较多，需要对这些系统进行详细测评，并对发现的安全问题进行整改，包括在统一安全开发规范下进行开发及进行安全加固。因此，要提高整体安全性，就必须要求各个应用系统本身消除隐患，提高安全性。国家电网公司对信息安全非常重视，已经把信息安全提升到电力生产安全的高度，同时要求各业务系统上线前要进行安全测评，确保上线应用系统的安全性，如国家电网调[2006]1167 号文印发了关于贯彻落实电监会《电力二次系统安全防护总体方案》等安全防护方案的通知，提出各研究、开发单位要按《方案》要求，尽快改进或完善所提供的电力二次系统或设备的安全特性；凡 2008 年 1 月 1 日以后投入运行的调度自动化系统和变电站自动化系统应符合《方案》要求并通过安全测试认证，2009 年 1 月 1 日以后投入运行的电力

978-1-935068-23-5

二次系统或设备都应符合《方案》要求并通过安全测试认证。

智能电网的电力传输系统用于双向传送电力和信息，信息流的宽度和有效深度远远强于传统电网可能涉及的范围，智能电网的建设在为电力企业以及用户带来效益和便利的同时，也带来了如下新的信息安全问题：电力业务系统边界接口增多、系统之间的耦合度更高等复杂度的增加，使得安全防护的难度增大；大量采用 3G、 WIFI、CDMA 等无线通信方式得通信网络环境更加复杂，使得攻击手段更多样化；智能终端、插拔式电动车、高级测量表计 AMI 等用户侧智能设备的安全漏洞加大了被黑客攻击的风险。因此，研究和解决这些问题已成为世界各国的当务之急。美国国家标准技术研究院（NIST）已经建立了一个智能电网网络安全协调任务组（Smart Grid Cyber Security Coordination Task Group，CSCTG），该任务组研究智能电网网络安全战略与需求，2009 年 9 月出版了 NISTIR 7628 第一版草案[1]，2010 年 2 月出版了第二版草案[2]，目的是为智能电网提供足够的安全防护。我国也在研究智能电网的信息安全架构。同时，智能电网业务系统上线前应加强安全测评，对发现的安全问题及时进行加固。

2 智能电网业务系统的安全测评框架

安全测评是指依据有关信息技术标准，对信息系统的完整性、保密性、可用性等安全保障性能进行科学、公正的综合评估的过程。通过全面的系统安全性测评，以期达到以下目的: 1）全面测试电力业务系统的安全机制和安全功能，发现其中存在的安全缺陷和漏洞；2)通过安全整改及验证测试，评估残余风险，确认系统安全状态可以满足安全运行的基本要求。

2.1 安全测评的标准规范

智能电网业务系统安全测评参照如下标准和规范：1）《GB/T 18336.2－2001：信息技术 安全技术 信息技术安全性评估准则 第 2 部分：安全功能要求》；2)《GB／T16260—1996 idt ISO／IEC 9126:1991 信息技术 软件产品评价质量特性及其使用指南》；3）《GA 216.1-1999 计算机信息系统安全产品部件 第一部分：安全功能检测》；《ISO/IEC 14598:2001 软件工程—软件产品评估》；4）《GB/T13423-1992 工业控制用软件评定准则》；《GB/T 17544-1998 信息技术 软件包 质量要求和测试》；5）《GB/T 22239—2008：信息安全技术 信息系统安全等级保护基本要求》；6）国家电力监管委员会《电力二次系统安全防护规定》。

2.2 安全测评的流程

智能电网业务系统安全性测评的工作流程分为系统调研、测试规划、测试实施、测评报告、安全整改和验证测评六个阶段。在具体实施过程中，根据被测系统测评的特定目的或一次测评的结果，有可能省略其中某个阶段。完整的流程图如下：

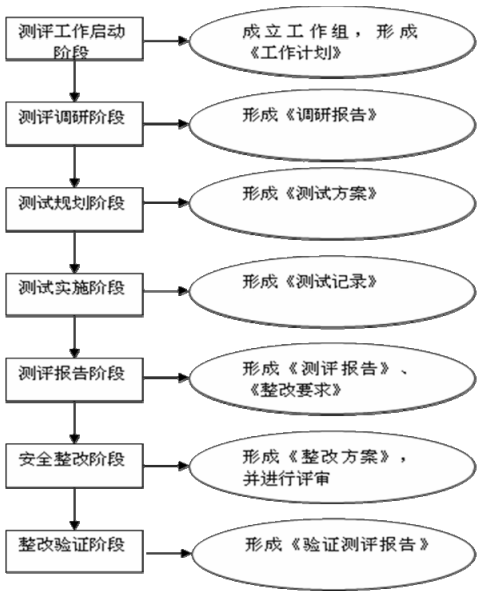

Figure 1 Intelligent Network system security evaluation of operational flow chart

图 1　智能电网业务系统安全性测评流程图

（1）准备和系统调研

此阶段的主要工作是前期协调和资料收集，包括：明确参与测评各方的工作职责和关系，对测评工作目标达共识；通过全面的系统调研，掌握待测系统在安全性上的相关需求及实现程度；确定测评的总体工作框架。

调研主要是由实验室向开发方和使用单位收集相关的文档资料，并整理成调研报告，为下一步测评规划和测试设计提供支持。调研的项目主要包括系统对运行环境的要求、系统的基本情况、系统的安全需求 、系统的安全设计、系统的安全辅助说明文档等五个方面。作为安全测评结论的有效依据，该部分调研内容极为关键，务必真实、详细。权威第三方测评机构的测评报告也可提供，作为本次测评参考或部分结论。调研结束后，形成工作计划和调研报告，指导测试开展。

（2）测试规划

针对前期的调研结果，规划安全测评的细节项目和操作方法，形成指导测评实施的测试大纲和测试方案。

（3）测试实施

测评方和业务系统厂商共同搭建、确认测评环境，实施现场测评工作，收集、记录、确认测试数据，形成记录文件并签字。在智能电网业务系统安全性测试过程中，通过单独使用或组合使用以下方式来执行测试用例，获取测试数据：

操作验证（A）：在系统的界面和工具中，执行、验证和确认系统实现的安全功能。

人工查看（B）：人工查看系统中与安全相关的配置工具和配置信息。

工具查看（C）：使用特定的测试工具对后台数据库、配置文件内容、加密数据等相关安全内容进行确认或验证。

代码检查（D）：人工查看系统源代码，验证是否具备相应的安全功能和安全机制，以及实现是否完善。

攻击测试（E）：利用攻击工具或通过人工操作的方式攻击系统，验证相关安全机制是否可靠。

（4）测评报告

整理、分析测试数据，形成测评报告，经过审核、批准后提出测评委托方，并根据要求提出适当的整改建议。

（5）安全整改

如果有必要，应由业务系统厂商针对系统测评结论中发现的安全缺陷，提出相应的整改方案。经过测评委托方和测评实施方的评审后，实施安全整改。

（6）回归测试或二次测评

在系统完成安全整改之后，再次对系统相关问题的完善情况进行回归测试。

如果系统的基础架构需要进行较大改动，或者整改会影响到已经通过测试的部分指标，可按照完整的测评流程进行二次测评。

2.3 安全测评的内容

智能电网业务系统的应用安全测评内容主要包括两大部分，分别是应用与数据安全要求、渗透与攻击安全要求。应用及数据安全可以参照国家等级保护基本要求和智能电网业务系统有关安全要求，主要测试应用系统的基本安全功能，包括身份鉴别、访问控制、安全审计、软件容错、资源控制、数据完整性、数据保密性等；渗透及攻击安全测试主要包括信息泄露、越权操作、SQL 注入、权限继承、审计安全、溢出测试、重放检测、任意文件上传等。下面重点介绍渗透与攻击安全测试内容：

（1）信息泄露

客户端、服务器和网络上的信息不应有泄露情况，包括任何的配置文件、可执行文件、界面显示、通过网络的操作、机密信息、连接信息等等。

a） 界面信息泄露

应用系统的界面不应在未授权的情况下导致机密信息泄露，包括登录的用户名口令等信息。

b） 文件－本地配置信息泄露

应用系统若将机密信息存储于文件中，应进行加密处理，防止防止未授权人员进行文件分析从而获取机密信息，造成机密信息泄露。此类文件包括存储服务器联接信息的配置文件、用户名口令文件等。

c） 内存－机密信息下载

应用系统若将机密信息下载至内存中进行比对，应进行加密处理，防止未授权人员进行单步调试从而获取机密信息，造成机密信息泄露。

d） 程序－机密信息安全

应用系统若将服务器联接等机密信息写入程序文件中，应做加密处理，防止非法提取机密信息；某些系统若未考虑信息安全因素，造成此类信息无法定期更新，引起安全脆弱性问题，建议采用可更新的方式存储机密信息。

e） 远端－机密信息泄露

应用系统应考虑信息安全因素，不应将服务器联接等机密信息放置在非安全的环境中，如 IIS 等，这些环境导致任何处于相同网络中的用户均能非可控的获取这些信息，导致信息泄露问题。

（2）越权操作

系统应无法使用工具进行的用户提升、越权操作动作，包括绕过界面进行操作。

（3）SQL 注入

系统应防止 SQL 注入攻击，防止非授权人员构造非法 SQL 查询语句，使得原本单一操作的 SQL 语句转变为多句 SQL 操作，达到越过应用系统权限控制，直接操作后台数据库的目的。

（4）界面爆破

系统应对界面进行规范性处理，应无可利用的界面漏洞。系统界面若存在不可用（灰化）的按钮或操作菜单，应进行相应的处理，防止非授权人员突破用户权限执行相应的功能，从而造成界面爆破。

（5）权限继承

系统的权限应有明确的等级划分，高权限的用户对低权限的用户授权应有逻辑依据，不应出现授权漏洞。

（6）审计安全

审计功能应对系统的各种操作提供相应的记录描述，其访问操作应在受控的状态下，且不应有对全局数据的操作功能。

（7）重放检测

系统应通过序列号或时间戳等技术来防止重放攻击，防止攻击者窃听一个正常的通信双方的通信包，然后重新发送这些数据包来欺骗某一方来完成与上次相同的通信流程。

（8）溢出测试

系统应对非安全函数、系统调用和边界进行严格检查，确保系统不存在溢出漏洞。

通过特殊构造的字符串对目标系统进行鲁棒性测试，遍历目标系统或针对目标系统某个方面，检验目标系统存在溢出的可能。

a） 非安全函数

系统不应采用非安全拷贝函数，非安全拷贝函数在处理字符串时不检查 buffer 边界的函数，此类函数包括 gets(),strcpy(), strcat(), sprintf(), fscanf(), scanf(), vsprintf(), realpath(), getopt(), getpass(), streadd(), strecpy(), strtrns()等，使用这类函数前必须进行边界校验，否则会引发数据溢出问题。这类函数完全可以被 fgets(), strncpy(), strncat(), snprintf() 等安全函数替代。

b） 系统调用安全

系统不应使用用户输入的数据作为某些系统调用函数的参数，此类系统调用函数包括 system()、popen()、exec()等，它们会解释 shell 命令，存在类似 SQL 注入的安全问题或其他威胁。

c） 边界检查

系统应考虑信息安全因素，对用户输入的数据进行边界检查，防止数据溢出的发生。

（9）文件上传漏洞

应用系统中的上传附件部分应做严格的限制，防止上传任意文件。

3 结语

随着信息安全技术的快速发展以及智能电网建设的不断推进，对智能电网业务系统本身的安全性要求越来越高，这就需要对业务系统上线前进行详细的安全性测试，发现它们的安全漏洞和存在的安全威胁，并提出安全整改方案，系统整改后再进行回归测试，通过不断反复，最终提高智能电网业务系统的安全水平。

References (参考文献)

[1] Annabelle Lee, Tanya Brewer. NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements [EB/OL]. http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf, September 2009

[2] Cyber Security Working Group. NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements[EB/OL]. http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628_2nd-public-draft.pdf, February 2010