National Conference on Information Technology and Computer Science (CITCS 2012)

Implementation and Design of Security Configuration Check Toolkit for Classified Evaluation of Information System

WANG Tian
Information Center, Guangdong Power Grid Corporation,
Guangzhou 510600, China

XU Hui
Information Center, Guangdong Power Grid Corporation,
Guangzhou 510600, China

ZHU Yi
Information Center, Guangdong
Power Grid Corporation, Guangzhou
510600, China

AI Jieqing
Information Center, Guangdong
Power Grid Corporation, Guangzhou
510600, China

ZHOU Wubing
Information Center, Guangdong
Power Grid Corporation, Guangzhou
510600, China

Abstract —**Through analyzing the indicators of classified protection and risk assessments of information system, a security configuration check specification model of Guangdong Power Grid Corporation is built. Security configuration enumeration library is also designed by reference to SCAP protocol. The architecture, model components and user interface design are given in details. The successful deployment of the security configuration toolkit proves that the design idea is correct.**

Keywords-Grades Evaluation; Security Configuration; Toolkit; Federal Desktop Core Configuration

I. INTRODUCTION

The reliance on information systems is increasing for government departments, financial institutions, enterprises and institutions, and commercial organizations at the present time[1]. Level protection evaluation is an important means to measure the security of information systems. Through implementing information system security classification protection evaluation, it can accurately grasp the security status of information system and help operators and service providers to build, improve and manage the system in accordance with security standards[2][3]. However, in the process of present level evaluation, there are still very obvious limitations in security configuration check, such as: (1) Because the type of evaluation object is large and complex, using manual methods to evaluat objects in security configuration check has relatively high requirements for technicians, which lead to long evaluation cycle and low efficiency; To reduce the number of evaluation object just for high speed will lead to evaluation can not meet the strength requirements, and affect the validity of evaluation results; (2) The uneven level of individual capacities in evaluation organizations has great impact on the accuracy of evaluation results; In addition, big workload, long period of time, high job stress and so on, also lead to low accuracy of survey results; (3) There is still no unified security configuration check standard for evaluation objects, some evaluation departments depend on certain industries custom security configuration specification, and some just follow their experience and feeling in the inspection process, the authenticity of evaluation results is greatly reduced. Consequently, there is an urgent need for a security configuration verification toolkit that is standardized, automated and meet the requirements of classified protection assessment, to assist assessment staff to carry out safety check in the classified protection evaluation process.

II. DESIGN & ANALYSIS OF SECURITY CONFIGURATION VERIFICATION TOOLKIT

In the abroad, Federal Desktop Core Configuration (FDCC), which demands that all government departments to enforce the security standard of baseline configuration, is proposed by Office of Management and Budget (OMB) [4]. FDCC defines the security configuration rule for the operating system of Windows XP and Vista. In order to detect the standardization of FDCC, NIST develop the security content automation protocol (SCAP), which express and use safety data by standardized way, and then evaluate the safety problem. So far there are about a dozen security configuration toolkits which can meet the requirements of FDCC and pass the authentication of NIST SCAP. In China, FDCC as reference, the State Information Center put forward China Government Desktop Core Configuration (CGDCC) in 2008, of which the ultimate goal is to realize the unified planning, unified management of national government office network terminal security protection system, and provide terminal safety nursing services for the government affairs terminal, these services include unified security policy configuration, detection of patch, real-time detection safety monitoring and so on [5]. This program was officially approved in 2010, its related standard, platform and toolkit are still being developed and perfected.

By analysising the development work of security configuration verification toolkit in domestic and foreign, we found that there are still no any toolkits that is suitable for classified protection evaluation work and evaluation characteristics design .

According to the work demand of daily operation and maintenance of information system, we believe that the security configuration verification toolkit should have the following characteristics:

(1) Toolkit with high performance: the objecs of classified protection evaluation are large and complex,and if the evaluation results of those objects need to be obtained quickly and accurately, toolkits must have higher performance, so that it can complete assigned testing tasks quickly and efficiently by ways of concurrent scanning of multi –task and multi-session, matching and checking template with great speed, etc.

(2) Open and flexible check template: classified protection related specification defines five levels for classified protection object. Because different levels have different technical requirements, and different evaluation objects ask for different technical requirements, the number of templates would be very huge. Open check template would encourage the research units of national government and industry departments that have a capacity for work, to improve the template standardization; And, there are some personalized requirements for classified protection evaluation, so inspection template of toolkit that can meet the need of flexible customization is needed, to add or delete inspection parameters and inspection items flexibly for evaluation personnel.

(3) Provide interface for further development: by providing interface for further development, it can form a linkage with other information security products, to achieve functions of more complex information security control, analysis and management, such as centralized management, centralized collection, centralized show, intelligence analysis, automatic repair and so on.

(4) Intelligence inspection process: different operating systems have different standards of safety configuration, and even the same operating system of different versions have different configuration differences of the same security configuration. Therefore, toolkits should be needed to distinguish types and versions of system, which can automatically select the best inspection template for inspection according to the difference, to make sure the quickness and accuracy of inspection results;

(5) Adapt to complex application environment: object environment of classified protection evaluation is complex and changeable, so the toolkit should fully consider the complexity, for example, provide real-time input window for user name and static or dynamic password, provide local script check, provide jump connection check, two log inspection and so on;

(6) Tool easy to operate: the work of classified protection security configuration verification is a cumbersome and complex process and the capacity of testing personnel is uneven. These requires that the interface of configuration evaluation tool should be set reasonably, so that it has the advantages of simple and easy operation;

(7) Easy to analysis examination result, can be preserved and compared for a long time. By providing intuitionistic report, to show individual difference and overall risk evaluation accurately and clearly with the form of pie chart, bar chart, graph and table.

Besides the above requirements, combining with the business needs of Guangdong power grid company, on the basis of the national standard Baseline for Classified Protection of Information System Security, and refer to Technology Specification on IT Mainstream Equipment Security Configuration of China Southern Power Grid to expand the scope of business system, network equipment and information application, to bulid the model of security configuration check standard of Guangdong Power Grid Company. In this model, the allocation requirements of different grade asset and the importance of different configuration grades also should be considered.

III. Security Configuration Check Specification Model

In Baseline for Classified Protection of Information System Security, security level is divided into four grades, each grade has two aspects of request with technique and management. As far as the technique, the main considerations are physical security, network security, host security, application security and data backup & recovery security. Baseline for Classified Protection of Information System Security is the main reference standards to establish security configuration check specification model. Specific requirements of information system security of units belong to Guangdong Power Grid Company, as well as industry standards (IT Security Configuration Baseline of China Southern Power Grid, General Requirements for Information System Safety and so on), are used as reference, and security configuration check standard model of Guangdong Power Grid Company is established finally[6]-[8]. The model includes four layers and three kinds of objects, as shown in figure 1.

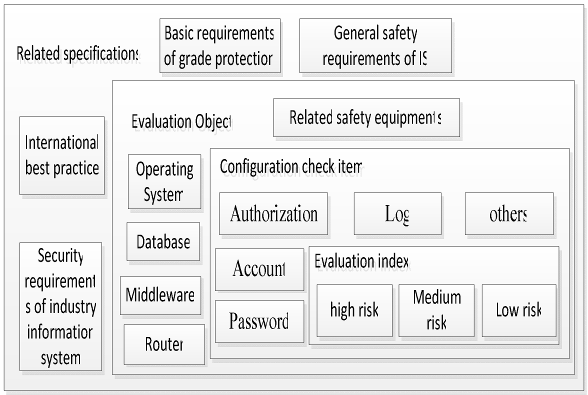

Fig.1 Security Configuration Check Standard Mode

These four factors, evaluation object, evaluation term, evaluation standard and evaluation risk, must be considered when establishing security configuration check specification model. Thorough considering of the future planning and development of information system of Guangdong Power Grid Company, in this study, evaluation objects contain 5 major-categories and 21 sub-categories, as shown in figure 2. Evaluation types contain 5 major-categories and more than 20 sub-categories, as shown in figure 3. For specific evaluation requires of each evaluation item, combining with requirements of classified protection system and using IT Mainstream Equipment Security Configuration Technology Specification of China Southern Power Grid Company as reference, to make reasonable customization, equipment and application. According to different level of system，the evaluation requirements are divided into two-stage and three-stage. For example, in personal identification, there is no specific requirement for two-stage system, but must be two or more than two kinds of combined identification techniques which can support system to realizes the identity authentication of user management for three-stage system. The requirements of security configuration check specification derive from standard layer objects. System layer contains IT system, equipment, application object type which are needed for evaluation, totally 5 major-categories; Check layer, the sub layer of system layer, is the specific type of application object check project, including 5 sub-categories; Evaluation index layer, confirm the impact caused by information assets by evaluating failure results of evaluation object.

Guangdong Power Grid Company has many business systems, and different business systems face different risks. For example: financial system is invaded that will not only cause data theft, but cause key data loss,system paralysis and system can not working properly if the situation is serious, these would have an enormous impact on Guangdong Power Grid Company; But if supplier management system is invaded, even if the data is stolen or the system paralysis, the effects on Guangdong power grid company are very limited. So different business systems have different asset weights, which determines different effects on the same missing security configuration item. These indicators need to be quantitatively measured in previous risk evaluation, but in the classified protection evaluation, the importance and value of assets decide by security level, thus the security configuration check specification model only need to consider the risk value of evaluation. In the actual evaluation, Security Configuration Inspection Specification of Guangdong Power Grid Company includes more than 20 kinds of evaluation objects, and each evaluation object contains more than 20 items. The number of inspection items is very large, and different inspection items have different influences on system, such as: length set requirement of account and password, if not in accordance with the standard, there may directly lead to illegal logging, which can do harm to the system seriously; But if the log storage method is not in accordance with the standard, it just affect the work of analysis and process after security event, has no harm to the system itself. So the risk value on system influence is not the same for different evaluation. According to the requirement analysis of Guangdong Power Grid Company, with the relevant provisions of the classified protection, risk value of evaluation term is set, as shown in table 1.

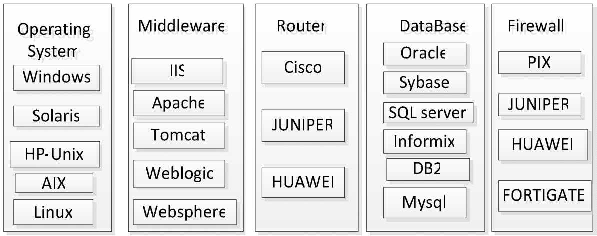

Fig 2 Evaluation object classification

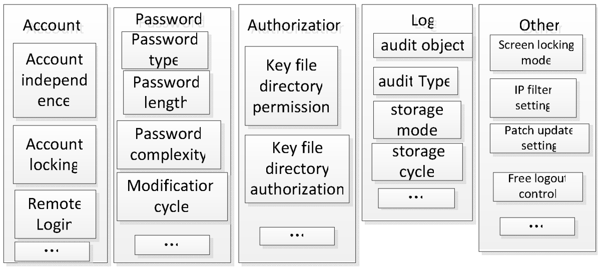

Fig 3 Evaluation type

TABLE 1 EVALUATION RISK VALUE SETTING

Risk Value	Risk Level	Description
8-10	high	System damage cause very serious influence on daily business work of company, the company gets very big loss.
5-7	medium	System damage cause serious influence on daily business work of company, company gets big loss.
0-4	low	System damage cause general influence on daily business work of company, company gets general loss.

IV. IMPLEMENTATION OF SCAP-LIKE UTOMATION VERIFICATION

On the basis of security configuration check specification model, we use SCAP as a reference to implement [9]. The core of security configuration verification tools is all types of security configuration check enumeration library. First of all, in the enumeration library, no matter what kind of information system, at the same security level, security configuration standard of the operating system, applications, routing and security equipments are all the same; Secondly, it should reflect as much as possible that the differences of security configuration between the same type but different version systems; Thirdly, mainstream operation system applications and equipment safety allocation standards should be enumerated as many as possible. So check enumeration library reference SCAP standards to do research, and on this basis, in accordance with the classified protection requirements of related standards, security configuration check enumeration library which is meet the need of classified protection requirements can be formed.This method can greatly reduce the development cycle and development difficulty, we call it SCAP-like implementation.

SCAP contains two main elements. First of all, it is a protocol, a set of standardized formats and open standards. Through it, security software products can exchange software bugs and security configuration informations, the standard is also called SCAP component; Secondly, SCAP includes software bugs and reference data of security configuration standard, and known as SCAP content. According to types, protocol component of SCAP 1.0 are divided into 3 groups: Enumerations Group, defines standard representation symbol and directory for safety and product related information; Vulnerability Measurement and Scoring group, is used for measuring vulnerability characteristics and giving scores according to these characteristics; Expression and Checking Languages group, use XML schema check list , produce check list report, as well as explain for low-level testing process of the check list. Huawei switches as an example, the configuration definition of limit session state and allow access rule reference based on the SCAP is given as the following :

```
<definition class="compliance" id="GPSTL-HUAWEI_FIREWALL-20000" version="1">
      <metadata>
        <title> According to the session state information to provide capabilities of clear allow / deny access for data
stream, and control particle size within the scope of port level;
</title>
        <affected ="HUAWEI_FIREWALL">
          <platform>HUAWEI_FIREWALL</platform>
        </affected>
        <reference ref_id="GPSTL-HUAWEI_FIREWALL-30000" source="CCE" />
        <description> Should check the boundary of network equipment, examine whether it can control data flow,
whether it can control the particle size within the scope of port level port level according to the session state information.
</description>
      </metadata>
      <criteria>
        <criterion test_ref="GPSTL-HUAWEI_FIREWALL-20000" comment=" Limit to use ICMP packets excessively,
prevent DoS attacks, If the firewall has these setting, it is considered to meet the assessment requirements." />
      </criteria>
    </definition>
<definition class="compliance" id="GPSTL-HUAWEI_FIREWALL-20001" version="1">
      <metadata>
        <title> According to allow access rules between user and system to decide whether allow or refuse users to
access the resource of controlled system, to control the particle size for single user;</title>
        <affected ="HUAWEI_FIREWALL">
          <platform>HUAWEI_FIREWALL</platform>
        </affected>
        <reference ref_id="GPSTL-HUAWEI_FIREWALL-30001" source="CCE" />
        <description>Should test the boundary of network equipment, can pass unauthorized resources that attempting to
access.</description>
      </metadata>
      <criteria>
        <criterion test_ref="GPSTL-HUAWEI_FIREWALL-20002" comment=" The rationality of access should control
whithin VLAN " />
      </criteria>
 </definition>
```

V. Design of Security Configuration Check Toolkit Module

The system architecture of the toolkit is shown in Figure 4. There are five major functional modules: (1) Scanning core module, which is the most important module of the system, and is responsible for completing the work of detection evaluation, including determining host survival state, identifying operating system, analysising and matching rules[10]. (2) The template library of security configuration evaluation, contains common configuration enumeration library (CCE) and common platform enumeration library (CPE), contains specific types of checking parameters of the known system, network equipment, application, middleware and database, as well as the related guide parameter check list of security configuration, are the basis of system running. The scanning scheduling module and Web management module are dependent on it to work. (3) Examination results library, contains the information of scanning task results, which is the basis of scanning result report, and is the data sources of results querying and analyzing. (4) Data synchronous module, is responsible for system module version upgrade, and provide data synchronization for external data collection server. (5) Web interface module, is responsible for interaction with user, to complete the management work according to user requests. Web management module includes multiple sub modules, which work together to accomplish user requests.

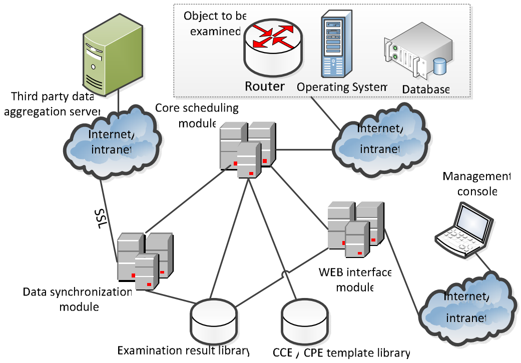

Fig 4 System Structure Diagram

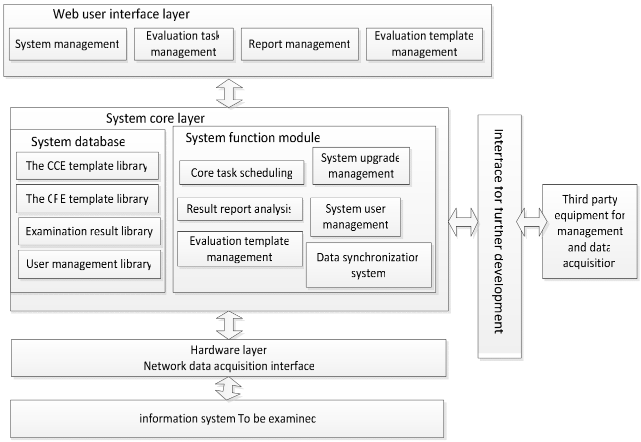
Web user interface layer
System management
Evaluation task management
Report management
Evaluation template management
System core layer
System database
The CCE template library
The CPE template library
Examination result library
User management library
System function module
Core task scheduling
System upgrade management
Result report analysis
System user management
Evaluation template management
Data synchronization system
Interface for further development
Third party equipment for management and data acquisition
Hardware layer
Network data acquisition interface
information system To be examined

Fig 5 System Module

System module is shown in Figure 5, the key functional modules are as follows:

A. *User management interface layer*

User management interface module is responsible for interaction with user, to complete the management work according to user requests. This module includes multiple sub modules, which work together to accomplish user's requests. Its main modules are: (1) Evaluation task management submodule, is responsible to accomplish the management work of user evaluation task. (2) Report management module, reads the assessment results, and generates scanning report according to description information of evaluation and solution. (3) Evaluation template management submodule, provides the functions of query, create, modify, add, delete for evaluation template. (4) System management submodule, provides the functions of query and configuration for all kinds of system control parameters, creation and maintenance for user login and password, download interface of assisted local evaluation script.

B. *System function module*

Intelligent analysis checking module is the most important part of system function modules, which provides intelligent analysis and correlation matching for configuration data acquisition, and put results into the examination result library. Core task scheduling module is responsible for reading the evaluation task information, to complete the work of target detection evaluation, including the determination of target survival state, log target, operating system identification, target configuration data acquisition. Result report analysis module provides the functions of data query, analysis and report generation. System upgrade management module can complete the update of platform enumeration library and evaluation template library, and each function module of the system can be upgraded through the upgrade module.

C. *System built-in library*

There are 4 built-in librarys in the system, and security configuration evaluation template library consists of CCE and CPE template library. CCE library contains various types of specific requirement list of safety equipment configuration, is the operation foundation of tools. CPE library contains all kinds of lists of operating system, application software and hardware. Safety configuration evaluation template library illustrates the discovery of defect configuration platform by correlating platform enumeration library. Examination result library contains the result information of scanning task, which is the basis of scanning result report, and the data sources of result querying and analyzing. User management library has login username, authority, password, audit and other relevant information of login tool.

D. *Interface for further development*

By Providing interface, it can form a linkage with other information security products and management platforms, to realize the decentralized data for unified data platform management.

VI. Implementation

The management mode of the security configuration verification tool of Guangdong Power Grid Company is based on WEB, users can interact by using the browser through SSL encrypted channel and system's WEB interface modules. When logining into system, user can create evaluation task, view task information, check task results, output statements, download check script of configuration specification, use commonly used tools, set upgrade settings, view task information, check task results, output report and so on.

VII. Conclusion

Security configuration verification toolkit has come into use in Guangdong Power Grid Company, which makes classified protection configuration evaluation work to obey a common unified standard. By using security configuration toolkit, we can set up different levels of technical requirement, take into account the risk level of each configuration item and make sure to the corresponding risk score by evaluation result according to classified protection requirements. During routine inspection, this automated security configuration verification toolkit can improve the efficiency of examination and follow-up by avoiding the inefficient shortcomings of manual examination. Security configuration verification toolkit can effectively improve the level of standardization and automation of the work, and ensure it is in accordance with the classified protection specification by monitoring the system effectively and continuously. In general, any large and medium-sized government departments, enterprises & institutionsthe can design and implement the security configuration verification toolkit, which is suitable for their own departments referring to our design idea.

REFERENCES

[1] XIAO Guo-yu. Information Systems Classified Security Protection Customer Evaluation [J]. Netinfo Security，2011, (7)：34-35

[2] Cai PengCheng, Feng FangHui. Classified Protection and Government Terminal Security [J]. Netinfo Security. 2010, (08):11-13

[3] Hu Zhe-qian Yang Lu. United Endpoint Management Research and Application [J]. Information Security and Technology. 2011, (01):27-30

[4] WANG Yi-shen. Terminal Security Protection New Ideas from FDCC [J]. Network & Computer Security, 2011, (10):45-46

[5] Xu Tao, Wu Yafei, Liu Bei, Li XinYou. Research on Core Configuration Standard of China's E-government Security Desktop [J]. Network & Computer Security, 2010, (11):74-76

[6] GUI Yong-hong. Study and Applications of Operation System Security Baseline [J]. Network & Computer Security, 2011, (10): 77-80

[7] Sun Tie. To Create Security BaselineTechnology System for Independent Controllable Service System [J]. Netinfo Security. 2009, (05):77-78

[8] WANG Yu-ping,DUAN Yong-hong,HONG Ke. Security Baseline in Banking Practices and Applications [J]. Network &Computer Security, 2011, (8):47-49

[9] Zhang Li. The Introduction of SCAP Standard to Improve the Safety System Configuration [J]. Information Security and Technology, 2010, (10):44-46

[10] Zhang Lijuan. MASS NETWORK MONITORING DATA AUTOMATIC FUSION AND CORRELATION ANALYSIS [J]. Computer Applications and Software. 2011, (08):21-23