A Derivation of Evaluation Item about Enterprise Security Management

Sun-Joo Kim, In-June Jo, *Member, KIMICS*

***Abstract*— The Enterprise Security Management system is a centralized control system based on predefined security policies by organizations. In Korea, there is a Common Criteria security certification according to the strict standards for various features. As the needs of information security product are increasing, the ESM system should be evaluated with quality characteristics. In this paper, we propose evaluation items for functionality and performance of Enterprise Security Management system, and the best practices for evaluation.**

***Index Terms*— Enterprise Security Management, ESM, Evaluation Item.**

I. INTRODUCTION

In the past, most network traffic was packets for web, ftp, and e-mail. So, simple security solution as Firewall, IDS (Intrusion Detection System), IPS (Intrusion Protection System), Anti-Virus System was enough to protect the threat. As online game, online banking, and, streaming services become popular recently, simple security solution can not satisfy the security requirement. And, as the size of IT services becomes bigger, the numbers of systems for IT services are increasing. These systems should be operated efficiently, and be controlled according to the security policies. So many companies adopt ESM (Enterprise Security Management) system to manage IT systems for services. The ESM system is an important system for central controls various systems in a company [1].

In 2009, the domestic market size of information security in Korea was 807.2 billion won, and the market share of ESM was 33.9 billion won(4.2%), which grew 36.8% from 2008. Mostly, public institution, and financial institution introduced the system, and the major suppliers were Igloo security (SPIDER TM), INZEN (SecuPlat ESM), JCom information (e-Pentagon ESM), Internet Security Systems (SAFEsuite), and CheckPoint (OPSEC).

Manuscript received August 18, 2010; revised September 28, 2010; accepted October 1, 2010.

Sun-Kim is with the Department of Computer Engineering, Paichai University, Daejeon 302-735, Korea (Email: uneedme@paran.com)

In Korea, KISA (Korea Internet & Security Agency) certificates security products according to the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), but there is no research on the certification of security software from the quality point of view.

In this paper, we propose evaluation items according to the quality characteristics, based on the international standards (ISO/IEC 9126, ISO/IEC 12119), and provide a applied case.

II. ESM

The ESM can be divided into several stages: threat and risk assessment, business process analysis, security policy definition, security policy interpretation, security policy enforcement, security audit and monitoring. So the ESM system links multiple heterogeneous equipments, and applies the defined security policies for each level, operates these equipments. The ESM system is a totally integrated security system, and is needed various functions and high performance.

A. system structure of ESM

Every ESM system is not the same because security policies and equipments of companies are different. But the general ESM system consists of 3 parts: console, server, and agent. (Fig 1)

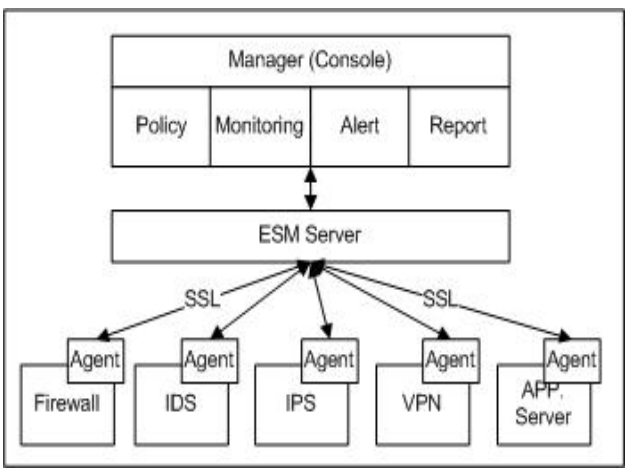

Fig. 1. System structure of ESM

The console program set the rules and policy, and monitors all events according to the predefined rule. It analyzes collected events in the ESM server, and causes alarm to a system operator by SMS, or e-mail,

The server program collects events from every agent according to the predefined collecting rule, and stores them.

The agent program is installed on servers, which are used for IDS, IPS, VPN control system, and application. Each agent collects all events on the system, and reports them to the ESM server.

Usually, the connection among console, server, and agent is based on SSL (Secure Socket Layer) in order to keep data safety.

B. Requirement of ESM System

To find out common functional and performance requirement of ESM, we analyze major function of 3 products in Korea, which have the highest market share.

TABLE I
PRODUCT FEATURES AND COMPARISON TABLE

Company /product	IGLOO Security SPiDER v2.5	INZEN SecuPlat ESM v3.0	J Com e-Pentagon ESM V4.0
Structure	- 3-Tier (Console, Server, Agent)		
Common	- Asset management - Policy management according to risk level - Alarm(popup, sound, e-mail) - User/Group management - Agent register/start-up management - Host information and log management - Event collection and classification - Correlation analysis - Monitoring(event, equipment, log, resource, performance) - Statistics and reporting - User authentication, access control, remote control		
Difference	- Monitor server file manipulation - Trace IP and URL route - SSL encoded communication - Backup policy management - Black list management	- API for agent creation	- Critical point setup - Black list management

According to the analysis, the common functional requirement of ESM system are the follow:

- Function
  - Equipments management
  - Policy management
  - Operator and user management
  - Agent management
  - Security level management
  - Correlation analyses
  - Monitoring rule set
  - Alarm management
  - Server and agent observation

- Performance
  - Resource usage for event process
  - Response of event collection
  - Search time of events
  - Time for mass data processing

III. RELATED STANDARDS

A. ISO/IEC 9126(Information Technology Software Quality Characteristics and Metrics)

There are 6 software quality characteristics, and 27 sub-characteristics defined in ISO/IEC 9126 (Fig 2)[2].

- Functionality: The capability of the software product to provide functions which meet stated and implied needs when the software is used under specified conditions.
- Reliability: The capability of the software product to maintain a specified level of performance when used under specified conditions
- Usability: The capability of the software product to be understood learned, used and attractive to the user, when used under specified conditions.
- Efficiency: The capability of the software product to of resources used, under stated conditions.
- Maintainability: The capability of the software product to be modified. Modifications may include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications.
- Portability: The capability of the software product to be transferred from one environment to another.

B. ISO/IEC 12119(Information Technology Software Packages Quality Requirements and Testing)

This standard is applicable to software packages. Examples are text processors, spreadsheet, database programs, graphics packages, programs for technical or scientific functions, and utility programs [3]. It establishes

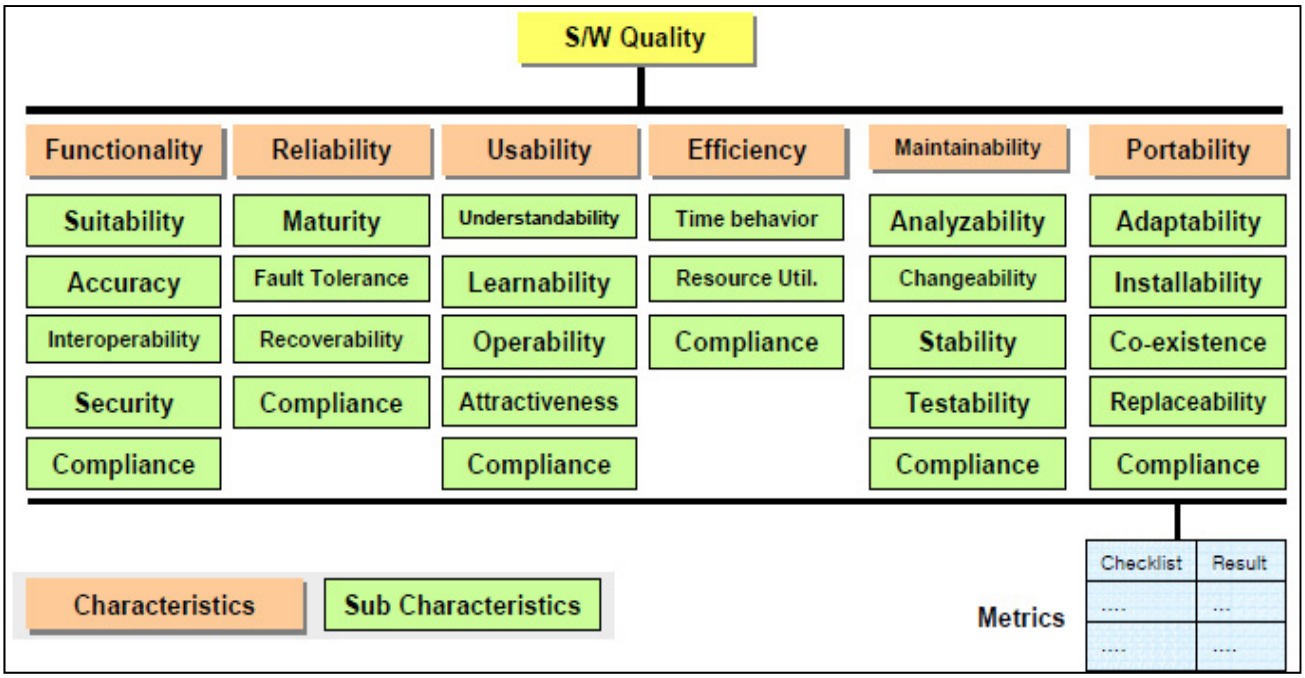

Fig. 2. Software product qualities

- requirements for software packages (quality requirements)
- instructions on how to test a software package against these requirements (instructions for testing, in particular for third party testing)

According to the standard, software package should have the following:

- Product description: It is a part of the package documentation of the product. It provides information on the user documentation, the programs and if any, the data. The main purposes are to help the user or potential buyer in their evaluation of the suitability of the product for themselves.
- User documentation: The user documentation shall contain the information necessary for the use of the product. All the functions stated in the product description and all user-callable functions in the program shall be completely described in the user documentation.
- Programs and data: All functions mentioned in the user documentation shall be executable in the form given in the user documentation with the corresponding facilities, properties and data, and within the boundary values given there. If installation can be carried out by the user, it shall be possible to install the programs successfully by following the information in the installation manual.

Ⅳ. DERIVED EVALUATION ITEMS

When we derive evaluation items about ESM system, we consider the general requirement of ESM system, and software quality related standards [4].

- Functionality: Suitability, Accuracy
  - Add/update/delete devices
  - Set the policy for each device
  - Backup/recover the policy
  - IDS
  - Manage operator, and user
  - Manage the work log by operator, and user
  - Monitor the device failure

- Set the critical point for each device
  - Set and analyze the correlated rules
  - Set the event monitoring rule
  - Manage the event level
  - Alarm by the type of events
  - Status report

- Functionality: Interoperability
  - Collect all events in the target device without the agent installation
  - Export reports in various file format (e.g. hwp, doc, ocx, ppt, xls, etc)

- Functionality: Security
  - Authenticate operator, and user
  - Access control by user authorities
  - Log events

- Ensure secure communication between the server and the agent
- Support secure access by operator and user
- Prevent fabrication of collected event file

- Reliability: Fault tolerance
  - System fault/halt when the server or the agent is down
  - Effect when fault occurs (e.g. OS down)

- Reliability: Recoverability
  - Re-establish the system when the server or the agent is down
  - Data corruption after system recovery
  - Retry when the network is down

- Usability: Understandability
  - Procedure for fault occurrence and device management

- Usability: Learn ability
  - Support on-line help
  - Easiness of messages for various events

- Usability: Operability
  - Operate and control the server and the agent
  - Classified by functional categories

- Efficiency: Time behavior
  - Detect intrusion by attack types
  - Processing time when the server or the agent is under heavy load
  - Response time for event search with certain condition

- Efficiency: Resource utilization
  - Resource usage when the server or the agent is under heavy load
  - Resource usage when detecting intrusion by attack types

- Maintainability: Analyzability
  - Identify events from target devices recorded in the server(occurrence time, event type, event content, etc)
  - Analyze the possibility of fixing

- Maintainability: Changeability
  - Enable modification
  - Check the system after modification
  - Upgrade the server and the agent program

- Portability: Install ability
  - Install/uninstall the console programs
  - Install/uninstall the agent program on various device (UNIX server, Windows server, network equipment, etc)

- Portability: Co-existence
  - Co-exist with the other independent software in common environment
  - Proper execution with the other programs for security

In the listed evaluation items, the evaluation items for 'Reliability', which is for safe operation even when the failure happens, are the follow: <Table II>

TABLE II
EVALUATION ITEMS FOR QUALITY CHARACTERISTICS "RELIABILITY"

Quality Characteristics	Evaluation item
Fault tolerance	- System fault/halt when the server or the agent is down - Data communication with normal agents when a agent process is down - Execution of the server and agents after network failure between the server and agents
Recoverability	- Data communication between the server and agents after server reboot - Transmit accumulated events when the server is down or rebooting - Transmit accumulated event after the agent is rebooted - Transmit events network failure between the server and agents

V. APPLIED CASE FOR EVALUATION

According to evaluation items, which were described in chapter IV, test cases were developed. Fig. 3. is the tested system.

A. Evaluating case

As classify the errors according to the quality characteristics, errors in functionality were 32(e.g. asset registration function error, event type detection function error, etc), errors in usability were 17(e.g. asset display error, input field display error, etc).

For efficiency, CPU usage was 52%, and memory usage was 23% ~ 73%, and the detection rate was 99%, when the system load was under 6,000 events/sec.

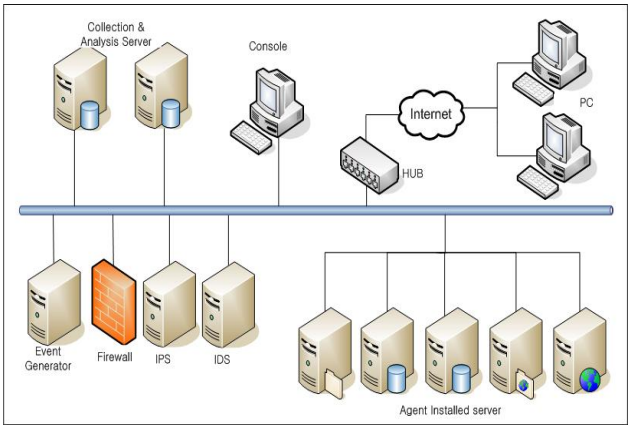

Fig. 3. Tested system

The average processing for detecting attacks was 3 sec/event, and the average processing for events 2sec ~ 28sec when the searched results were 500 ~ 10,000 in total 1,200,000 events

B. Comparison of evaluating methods

ISO/IEC 9126 Software engineering — Product quality is an international standard for the evaluation of software quality, so it is useful for evaluation of general package software. But it is difficult to apply it because the requirement will be changed according to the IT environment for using software in a company.

<Table IIII> is the comparison among proposed method, method based on ISO standards, CC evaluation method. [4]

TABLE III
COMPARISION TABLE AMONG PROPOSED METHOD

Method	Advantage	Disadvantage
Method based on ISO standards	Evaluate S/W quality based on ISO standards	Can't apply requirement of IT environment
CC evaluation method	Evaluate S/W quality in security	Can't evaluate non-functional item
Proposed method	Evaluate S/W quality in 6 quality characteristics	Need continuous improvement for various IT environment

VI. CONCLUSIONS

In this paper, we propose evaluation items for ESM system, and provide the applied case. Some evaluation item can be added according to the system environment. As a new feature of ESM can be developed, corresponding evaluation item should be added too. Even though we used international standards as a guideline, every ESM system has different functions and security policies. Recently some research of enterprise security management is spread over many fields including autonomous and mobile agent, policy languages, business process analysis, remote configuration protocols, access control system and system management.

Efficiency and portability is the most important because an agent should be installed and it must be supported by a small bandwidth on the target system when evaluating ESM system. Also the ESM should be stable and efficient when processing massive data. Therefore, efficiency and reliability should be weighted more, when evaluating ESM system

For accurate evaluation, we need more research on the method of weighting evaluation items which are consisted with a purpose of ESM system adaptation.

REFERENCES

[1] TTA Dictionary of Information and Telecommunication
[2] ISO/IEC 9126: Software Engineering- Software Product Quality
[3] ISO/IEC 12119: Information Technology Software Packages Quality Requirements and Testing
[4] Ministry of Public Administration and Security, Notice 2008-26, "Common Criteria for Information Technology Security Evaluation ", 2008.7.16
[5] 2010 White paper on national information security, KISA, 2010.4

Sun-Joo Kim received the B.S. and M.S. degrees in computer engineering from Paichai University, Daejeon, Korea, in 1999 and 2001. He is currently an research engineer in the S/W Quality Evaluation center at the Telecommunications Technology Association. His current research interests include security testing and Common Criteria.

In-June Jo received the B.S. and M.S. degrees in computer engineering from ChonNam University, Gwangju, Korea, in 1982 and 1985, respectively, and the Ph. D. degree in computer engineering from Ajou University, Suwon, Korea in 1998. He is currently a professor in the computer engineering at Paichai University. His current research interests include security of mobile and network