Study on Automatic Classified Protection Testing and Evaluating System

Yuanjing[1, a]

[1]MPS Information Classified Security Protection Evaluation Center, The Third Research Institute Of Ministry Of Public Security, Beijing, 100142, China

[a]email: yuanj1101@163.com

Keywords: Classified Protection of Information; Classified Protection Testing and Evaluating; Automatic Evaluating System; Knowledge Base; Rule

Abstract. Technology report of classified protection testing and evaluating is consulted in supervision and inspection of classified protection of information. The paper brings forward a system for automatically evaluating information system's security. The system analyses knowledge during classified security testing and evaluation, and classifies them, thus knowledge base come into being. Furthermore, it put forward a method of building topology of networks and application flow chart. Finally, it explains in detail how to automatically evaluate protection ability of information system using knowledge base. The method makes up man-made flaw, and synthesizes correlative factors including testing and evaluation results of one item, controls and penetration, to a truer and repeatable and impersonal conclusion.

Study Background

Classified protection of information orders that organization should be supervised, inspected and instructed. And the report of classified protection testing and evaluating is must. So the process of classified protection testing and evaluating must be normative, the conclusion must be exact, fair and returnable.

The automatic classified protection testing and evaluating system in the paper forwards evaluation process based on the evaluation knowledge base. With the knowledge base, it automatically judges the result of individual item. And it judges the combination result of individual item or individual control by combining business flows and penetrability test outcomes. And then the conclusion is coming into being.

Technology Difficulty

First, classified protection testing and evaluating indexes includes not only secret, integrity and usability technology indexes, but also security government indexes. There's correlation between the indexes. How to find the correlations and define them scientifically is the difficulty.

Secondly, the target of classified protection testing and evaluating is judging that if system has the security protection capability of correspond class. Proofs of individual item gathered by testing and evaluating are point, multi data. How to synthesize the proofs and automatically deduce the conclusion is the other difficulty.

Design and Realization of System

Framework of system

The basic principle of system is to confirm testing objects, topology, business flows based on inquiry results, and implement testing and evaluating on each item of the object to gathering proofs. And then based on the proofs, applying kinds of fact knowledge, process knowledge and rule knowledge in knowledge base，deducing testing results of security control and risk analysis. Furthermore, testing and evaluating conclusion is reached. Figure1 shows the framework of system.

Synthesis database is the data exchange platform. Program basic information, basic survey

results, testing and evaluating proofs of each individual item, and risk information are formalized as fact. These fact are the initial data. Under the action of the inference engine, the fact, process and rules are also loaded into the synthesis database. The inference engine completes inference analysis by pattern matching.

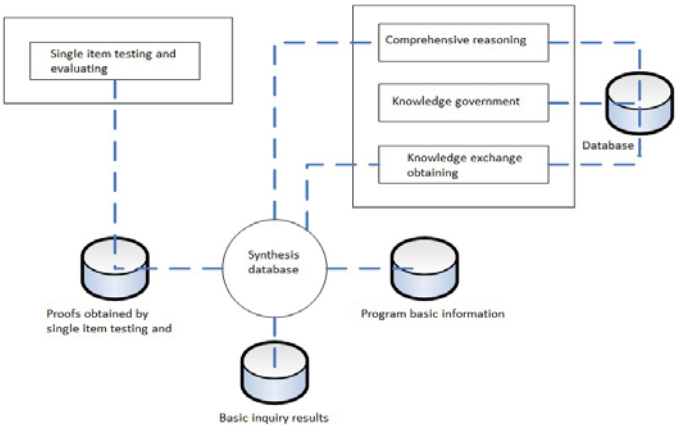

Figure1 The framework of system

Synthesis database is a comprehensive database which facts and the inference result (including the intermediate results) are resident in.

Comprehensive reasoning is triggered by the event, and the rules and the order of precedence are obtained by the matching rules and the facts. After deduction of the results, the conclusion is given.

Knowledge base is used to set up storage fact knowledge, rules knowledge, process knowledge based on classified protection testing and evaluating index system and vulnerability database. Knowledge base is the basis of automatic comprehensive evaluation, its completeness and accuracy directly determines the evaluation conclusions objectivity and credibility.

Knowledge base build

The knowledge in this paper refers specifically to the knowledge that is necessary for classified protection testing and evaluating and auto-evaluation, including not only fact knowledge that are the inquiry form, evaluation implementation manual, associate evaluation item relationships, the relationship between evaluation item and vulnerability, the relationship between vulnerability and penetration methods, procedural knowledge that are automatic evaluation step or sequence, but also including rule knowledge needed by an automatic evaluation system that are device connection rules, business flows correlation rules, correlation analysis rules.

Classified protection testing and evaluating knowledge analysis

Classified protection testing and evaluating knowledge can be analyzed using object-oriented approach to sort assessment evaluation processes and tasks. The assessment process consists of four phases of the systems inquiry, evaluation preparation, on-site evaluation and report preparation. Knowledge related to the systems inquiry phase are: inquiry form, information system components. Knowledge related to the evaluation preparation phase are: threats, security objectives, evaluation implementation manuals, safety controls, evaluation items, evaluation plan template. Knowledge related to the on-site evaluation stage are: vulnerability, relationship of vulnerability and penetration methods, device connection rules, business flows rules. Knowledge related to the report preparation stage are: evaluation report template, the rules determined individual item evaluation, associated evaluation items, relationships between evaluation items, the rules determined security control evaluation, evaluation item associated vulnerabilities, risk value associated vulnerability, correlation analysis rules, vulnerabilities and suggestions, classified protection testing and evaluating conclusions determination rules.

Classified protection testing and evaluating knowledge database

According to the analysis of knowledge, classified protection testing and evaluating knowledge database as follows:

- Threat knowledge: the threat situation faced by information systems, including description, corresponding security objectives.

- The security objectives knowledge: security objectives that information systems should achieve.
- Evaluation index knowledge: information systems should meet the baseline, including security controls, evaluation items, related evaluation items, relationship between evaluation items, security goals to achieve.
- Vulnerability knowledge: CVE number, description, related security controls, related penetration methods, related risk value.
- Information system component knowledge: network device, safety device, operating system, database systems, application software platform.
- Evaluation implementation manual knowledge: kinds of technical and government checklist，including evaluation item, evaluation implementation and expected results.
- Template knowledge: inquiry form, evaluation plan, evaluation report.
- Rules knowledge: including the rules determined individual item evaluation, correlation analysis rules, the rules determined security control, and classified protection testing and evaluating conclusions determination rules.

Synthesis Reasoning

Reasoning process and related knowledge

Classified protection testing and evaluating include testing individual evaluation item and correlation analysis. The latter is based on the former. The system builds information system network topology and business flows based on knowledge database. And then reasoning with facts and rules knowledge in database to automatic evaluating protection ability of information system. Reasoning includes determining outcome of individual item evaluation, correlation analysis, determining outcome of security control, determining conclusion of classified protection testing and evaluating.

Relationship between synthesis reasoning process and knowledge is shown in Figure 2.

System mainly uses knowledge representation based rules, that is, "if ... then ..." form. Formalized in the form of: if a then b, that is a->b.

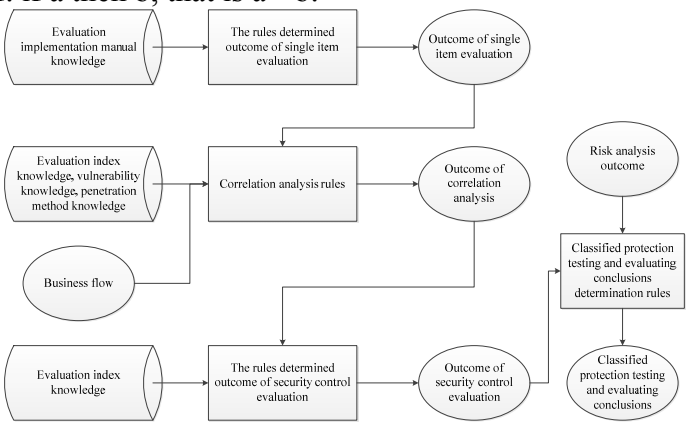

Figure2 synthesis reasoning process

The rules determined outcome of individual item evaluation

Individual item evaluation uses different methods to implement several steps for each assessment item, whereby gathering a plurality of proofs. The related rules are:

Rule1：If all proofs are as same as expect outcomes shown in evaluation manual, then the outcome meet;

Rule2：If not all proofs are as same as expect outcomes shown in evaluation manual, then the outcome doesn’t meet;

Rule3：If all outcomes meet, then the outcome of individual item evaluation meet;

Rule4：If all outcomes don’t meet, then the outcome of individual item evaluation doesn’t meet;

Rule5：If not all outcomes meet or don’t meet, then the outcome of individual item evaluation partially meet.

Correlation analysis rules

Correlation analysis is further evaluation based on individual item evaluation, which mainly include evaluation between security controls, between layers, and between security controls and penetration outcomes. Correlation analysis is divided into two steps:

1) According to the knowledge of the evaluation items related evaluation indexes, evaluation items relationship, and associated with different levels of evaluation items, and the topology and business flows diagram, analyzing the influence to individual item evaluation outcome result of the same level between different evaluation items, the same business flow between different evaluation objects and relationship of items in different levels. Consequently all related intermediate results of evaluation items.

2) According to the knowledge of vulnerabilities, related evaluation items, permeation methods, the penetration results are associated with evaluation items. Then analyzing the influence to related intermediate results of evaluation items as step 1) with the penetration test outcome. Consequently the correlation analysis results are obtained.

To get the related intermediate results of evaluation items as step 1), function $f(a, b, r)$ is used. Wherein, a is outcome of the evaluation item $c1$, b is outcome of the evaluation item $c2$, $c1$ and $c2$ have relationships, the impact to a result of the relationships between $c1$ and $c2$ is r. r maybe enhance or weaken.

The function $f(a, b, r)$ represents the correlation analysis of intermediate outcome of $c1$ because of the impact result of b. $f(a, b, r) \in \{1,0, -1\}$ (representing meet, partially meet and non-meet), where, $a, b \in \{1,0, -1\}$ (representing meet, partially meet and non-meet), $r \in \{0, 1\}$ (representing weaken and enhance). $f(a, b, r)$ is defined as follows:

$$f(a, b, r) = \begin{cases} -1 & ((a=-1 \wedge r=0) \vee (a=-1 \wedge b=-1 \wedge r=1)) \\ 0 & ((a=0 \wedge r=0) \vee (a=1 \wedge b=-1 \wedge r=0) \vee (a=1 \wedge b=0 \wedge r=0) \vee (a=-1 \wedge b=1 \wedge r=1) \vee (a=-1 \wedge b=0 \wedge r=1) \vee (a=0 \wedge b=-1 \wedge r=1) \vee (a=0 \wedge b=0 \wedge r=1)) \\ 1 & ((a=1 \wedge b=1 \wedge r=0) \vee (a=1 \wedge r=1) \vee (a=0 \wedge b=1 \wedge r=1)) \end{cases}$$

The reasoning rule of step 2) is:

Rule1：If all intermediate results of evaluation item meet, and penetration outcome does not meet, then the correlation analysis outcome meets;

Rule2：If not all intermediate results of evaluation item meet, and penetration outcome does not meet, then the correlation analysis outcome partially meets;

Rule3：If penetration outcome meets, then the correlation analysis outcome does not meets.

Security control determined rules

Each security control includes several evaluation items. The outcome of security control is obtained based on the correlation analysis outcome. The determining rules are:

Rule1：If correlation analysis outcomes of all items of some security control meet, then the security control evaluation outcome meets;

Rule2：If correlation analysis outcome of all items of some security control do not meet, then the security control evaluation outcome does not meet;

Rule3：Otherwise, the security control evaluation outcome partially meet.

Testing and evaluating conclusion determining rules

Testing and evaluating conclusion is determined according to security controls evaluation outcomes and risk analysis outcomes. Risk analysis is implemented against those security controls which outcomes partially meet or non-meet. According to the related vulnerabilities of these security controls and its risk value, the risk analysis outcome is obtained.

Testing and evaluating conclusion determining rules are:

Rule1：If all security controls evaluation outcomes meet, then the testing and evaluating conclusion meets;

Rule2：If not all security controls evaluation outcomes meet, and all risk analysis outcome are

not high, then the testing and evaluating conclusion partially meets;

Rule3：If not all security controls evaluation outcomes meet, and some risk analysis outcome is high, then the testing and evaluating conclusion does not meets.

Conclusion

Automatic classified protection testing and evaluating system is built here according to practical experience and theoretical research. And from the view of general business flows of classified protection testing and evaluating, all related knowledges are analyzed and be divided into eight categories. That's the base of reasoning. And then the reasoning process and basic rules are forward. From comprehensive several aspects of individual item evaluation proofs, penetration outcomes, relevant knowledge to evaluate the ability of information systems security.

References

[1] Li yuexin, Hu jie, Qin li, Knowledge Engineering Fundamentals and Applications, Beijing: Science Press [M], 2006.

[2] Xu jiepan, Ma yushu, Fan ming, Introduction to Knowledge Systems, Beijing: Science Press [M], 2000.

[3] The General Office of the Central Committee of the Party, the General Office of the State Council. Requirement about the work of enhancing information security assurance. (GOCCP[2003]27). 2003.8. (in Chinese)

[4] MPS, Protection of State Secrets Bureau, State Bureau of Cryptologic Admistration, State Office of Informatization, Regular for information security classified protection management. (MPS[2007]43). 2007.6.

[5] GB/T 22239-2008 Information security Technology - Baseline for classified protection of information system. [S]