# Research on the security of information system integration based on percolation test

Jingbo Guo, Qi Cai

Pingdingshan Institute of Education, 467000, Pingdingshan Henan China

**Keyword:** Information Security, percolation test, system integration

**Abstract:** This paper analyzed the safety problem of integrated system from hardware integration, data integration, interface integration and other aspects by using the method of percolation test. It focuses on security issues which newly created in the process of information system integration, namely the use of a data warehouse, middleware, XML and other models for security issues which may arise in information systems integration. And the results of penetration test were used as the data material of risk assessment, improving the accuracy in the results of risk evaluation. The experiment proved that this method reflected a real and effective security level of target system.

## Introduction

In recent years, with the rapid development of computer technology and network technology, more and more enterprises have entered the era of information and intelligence, integrated business systems are widely used in various areas such as government, bank, military and other areas. With the rapid development of various types of business, information system with single functions unable to meet the business requirements for many companies. More and more companies adopt methods of system integration to integrate different functions, different language and different architectures of multiple applications of single function together to achieve data sharing, and improve convenience and efficiency in business. However, integrated system can also bring potential security problem that may not happened to single system at the same time.The security risk assessment for integrated information system, identification for security risks and provide security reinforcement plan, enhancement for overall security in integrated information systems are need in order to ensure security after the operation of information system integration. However, now commonly used assessment method of information systems in construction algorithm and security model is largely dependent on the personal experience of experts which cannot provide a specific security reinforcement plan after giving the security valuation for target system. This paper will introduce the concept of penetration test by using its methods to accurately locate and point out the security risk and vulnerabilities in integrated information system and provide more intuitive, real data and more accurate assessment of the security level of the target system for experts when calculating the risk value of the target system. And after giving the safety assessment of whole target system, each specific security risk points and vulnerabilities were given a specific security reinforcement program based on the results of penetration test, to better enhance the security level of the integrated system.

## Correlation theories of information system integration in percolation test

**Theories of integration of information system.** 1.Framework of information system integration. With the development of computer technology, the single-function information system has been unable to meet the work needs for many companies. More and more companies using the methods of information systems integration to integrate to integrate various systems. These single system or different function or different languages for development or different architectures was by way of system integration to improve the convenience and efficiency of business. There are some steps for the process of system integration: requirements analysis, program design, project management, environment construction, installation and configuration for selection of software, development of applications system, etc., in which not only many management factors need to be considered but also various technical factors need to be considered. The paper will divided the system integration work into different levels and establishing the systematic framework.

2. Definition of information system integration. The concept of system integration was given different definitions by different organizations and different people. American International Data Corporation (IDC, International Data Corporation) attributed system integration to a conceptual business, and this business logic is to combine software and hardware with information technology, and then the ultimate goal is to solve the problem of information data in business for users. American large system integrators INPUT companies further expand the concept of system integration. They believe that system integration is based on a company's own design philosophy and customer needs for the user's information system to carry on program, in which various software and hardware technology and project management processes of resource document class were covered.

3. Classification of Information system integration. The essential methodology of system integration approach is sharing resources and information. According to different kinds of information, the system integration can be integrated into the following three categories: first, the data integration: means integrated sharing of isomerous data information. Second, control integration: means effective sharing and reuse for different software and hardware logic. Third, the performance integration: refers to integrate and redesign the presentation layer of multiple different systems, providing a interface for external services.

**Ways of information system integration and its security risk.** In the aspect of integrate deepness, system integration can be divided into presentation integration, business logic integration, application interface integration and data integration.

1. Ways of network integration and its security risk. Network integration was located at the bottom of the system, here mainly refers to hardware and software environment, providing a unified support environment for normal operation of application system. On the one hand, network integration involved in technical problem, while on the other hand it also relates to the internal management of the unit, especially for the large-scale network system which is a very complex issue. Information security risks on the network level are the first portal of information systems, but also be the preferred path to hacker attacks.

2.Ways of data integration and its security risk. The difficulty of information systems integration lies in data integration. Data integration not only physically integrates in the different formats of data, more importantly in the logic of data, thus providing a comprehensive data sharing for companies. At the present stage, common data integration has three ways: data warehouse schema, middleware mode, XML mode. Data warehouse is to organize and manage data, and cannot consider this question from the angle of application, so it is difficult to design its security directly. Data warehouse is located on a very abstract level, ranging between applications and databases, and difficult to control its security. If the used of middleware in data integration system has significant security vulnerabilities, which might be a breakthrough for hacker to breach the integrated system completely. However, as the mechanisms of XML itself which result in the XML file appears injection vulnerability in the process of being parsed, according to the injection method, the vulnerability can be divided into: XML injection vulnerabilities and XML external injection vulnerability.

### Integrated system carrying out in the percolation test

Percolation testing is the use of security tools and personal experience of penetration specialists in the network core servers and critical network devices which including servers, switches, firewalls to process non-destructive simulate attacks by hacker. The purpose is to discover vulnerabilities, intrusion system or obtain confidential information and the specific processes and details of invasion are reported to the users.

The traditional penetration testing method is generally artificial investigation. This process requires a lot of manpower and the requirements for manpower are very high. Only the tester who masters reliable knowledge can work out high quality penetration test, ensuring the accuracy and correctness of results. More logical and deeper system vulnerability and technical defects can be found in this way. Usually, the scanning tool is not that smart and often feels powerless to those more complex and deeper system vulnerabilities though its scanning speed is high, and it still has certain false positive rate. Therefore, it is generally combined the penetration test with scanning tool in practical operation, in order to achieve better test results.

The difference between penetration test and hacker attack is that the penetration test needs to obtain delegation authorization from customer and it generally involves five steps: information collection, vulnerability discovery, exploitation of vulnerability, elevation of privileges and finish penetration test report.

**Information collection.** Information collection is the first step of percolation test which is the process of preparing, sorting and analyzing for relevant information and this is the basis of the entire penetration test. The object of information collection can be any information that helpful to invasion system. in general, the object of information collection includes four categories: the first is target system information, including operating system type, domain information, situation of open ports, IP information, operational service, etc. The second is the administrator information, including various materials about the administrator, which is helpful to social worker’s attack and common password cracking in the future. The third is sub-station information. In general, many systems have been processed with strong network protection in its major parts, and it is more difficult to invade. However, the safety protection of sub-module does not adequate and has no much defense and test, thus the sub-station can be attacked first, then the sub-station can be set as a springboard for further attack primary station. The fourth is topological information, and the understanding of internet topological information can know the internet architecture of the whole system from overall context. This kind of information includes other relate conditions of application system in a small network segment. Through collecting the information from above four aspects, tester can has a whole overview of target system in order to set out subsequent test steps.

**Vulnerability search**. After finishing the collection of information, the system is going to have a penetration test for overall understanding and then the vulnerability can be searched. The process of looking for vulnerability can be divided into two ways: manually search and scan tool.

**Vulnerability utilization**. Vulnerability utilization is the use of above system vulnerability to process system intrusion. The first step is to obtain some permission from target system. Only the permission obtained from system can further collecting the information from system. The method of vulnerability utilization can be generally divided into two types: manual type and instrument type. Generally speaking, sql injection vulnerability is manual, while overflow vulnerability is instrument type.

**Privilege escalation.** In general, certain privilege should have been obtained from destination host after last step, but this privilege still very low. There is no use for percolation tester to obtain a low-privileged common user, maybe just can check the system data, and just can check insignificant unimportant information. The process of privilege escalation needs to obtain higher system privileges by this time. Escalation here means local privilege which generally finished by the vulnerability of internet applications on target system.

**Completing percolation test report.** For customers, the true value of penetration test is the penetration test report provided by tester. Penetration test report must be clear and easy to understand, as the results of penetration test may provide to business worker as a reference who has no related professional knowledge, reflecting the value of the entire penetration testing. Test report should identify the process of test, risk analysis and assessment of vulnerability. The most important thing is to propose a solution to this kind of risk.

**Hierarchical analysis.** Hierarchical analysis was selected as a method in this paper. The basic approach of this analysis was that decision problem was a large system. This system was affected by many factors. Those interactional factors were arranged in accordance with a certain relationship, and then the results after arranging will be the final result of logical analysis. Considering that the various factors affected security risk of information system has hierarchical relationship, so the use of analytic hierarchy process to analyze and evaluate security risk of information system is more scientific.

1.Structural model Establishment. The purpose of establishing structural model is on the basis of in-depth analysis practical problems to build the evaluation index system based on essential characteristic of system. Figure 2 shows hierarchy structure model in which three basic levels were included. From bottom to top are measure layer, criterion layer and the target layer. The lowest level is the measure layer, which is the behavior means to achieve the objectives. Criterion layer is rules and standard that needs to be following in the whole procedure. The target level is the highest level of the model which is the ultimate goal to be achieved.

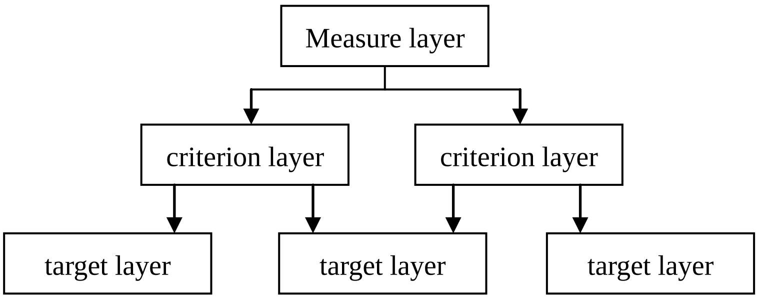

Figure2.1 hierarchy structure model

2. Judgment matrix construction. After the establishment of low-level hierarchical model, it cannot directly draw any useful information. The intention of judgment matrix was to compare the importance of different elements on the same levels. And the method was nine quantile. Significance scale value was shown in Table 2.1.

Table2.1 Matrix of significance scale value

| Significance scale | Connotation |
|---|---|
| 1 | It has the same importance when comparing with 2 elements |
| 3 | Comparing with 2 elements, the former more important than the later |
| 5 | Comparing with 2 elements, the former more obviously important than the later |
| 7 | Comparing with 2 elements, the former more intensely important than the later |
| 9 | Comparing with 2 elements, the former more extremely important than the later |
| 2、4、6、8 | Intermediate value from above judgment |
| Reciprocal | If the ratio of the importance between elemen ti and j, then the ratio of the importance between elemen ta$_{ij}$ and i was a$_{ij}$=1/ a$_{ij}$ |

Numerical value was obtained from the comparison of different elements based on Table 2.1, farmable matrix: A:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1j} \\ \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{ij} \end{pmatrix}$$

Among this, element aij(i, j = 1,2,... ) means the specific value of superiority of elements i and j. Matrix composed of these elements was considered as judgment matrix. Judgment matrix can be found through the comparison of elements between layers from the hierarchical structural model.

## The application of percolation test in integrated system

**Experimental environment.** There are four application servers in the experimental environment and one database server. Four application system was used the method of single sign on to identify the visited users through the same proxy server. OA application system and mail system were used the way of middleware for data integration, while financial system and portal system used XML. The strategy of access control was set into the server zone firewall to strict control common user visiting sensitive ports such as port 3389 and port 21.

**Percolation test in the experimental network.** Some vulnerability in verification, firewall, server and system were found in the experiment network and the vulnerability details were shown in Table 3.1

Table 3.1 Vulnerability list

| device name | Vulnerability description | Results of utilization |
|---|---|---|
| firewall of server zone | SNMP group name | Obtaining privileges form firewall administrator |
| database server | ms08-067 | Arbitrary remote code execution |
| Single sign-on server | Apache Struts2 vulnerability | Arbitrary command remote execution |
| OA application server | Open port 3389 | Remote blasting password |
| portal system | SQL Injection | Obtaining privileges from portal system administrator |

Analyzing the connected relation in each vulnerability, and based on the expert evaluation mark, structuring oriented-edge values in each vulnerability node, namely P12=0.45，P13=0.47，P24=0.54，P34=0.43，P35=0.43，P45=0.55. And the attack map of experiment network can be made according to the oriented-edge values.

Taking the firmware bug as an example, the matrix of game profits in each node can be constructed via the analysis of historical data and advisory consultant

$$(M_a \quad M_d) = \begin{bmatrix} (2\ ,\ 8) & (4\ ,\ 6) & (8\ ,\ 2) & (5\ ,\ 5) \\ (7\ ,\ 3) & (5\ ,\ 5) & (6\ ,\ 4) & (1\ ,\ 9) \\ (4\ ,\ 6) & (9\ ,\ 1) & (8\ ,\ 2) & (2\ ,\ 8) \end{bmatrix}$$

Adjacent matrix of attack map:

$$M_0 = \begin{bmatrix} 0 & 0.45 & 0.47 & 0.445 & 0.447 \\ 0 & 0 & 0 & 0.54 & 0.297 \\ 0 & 0 & 0 & 0.43 & 0.667 \\ 0 & 0 & 0 & 0 & 0.55 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Risk vector quantity of vulnerability:

U =[ 7.25 2.88 6.33 3.6 5.45]

Risk vector quantity and propagation vector of vulnerability itself

V（Rs）=[0 1.3 2.98 5.09 10.69]

V（Ra）=[8.31 3.56 5.18 2.99 0 ]

The whole risk vector quantity of experiment network:

M（Ra） =[ 8.31 4.86 8.16 8.08 10.69]

According to the whole risk vectors you can see that the most serious flaw is the value of 8.31 and 10.69, viz. default group name of SNMP and portal system SQL injection.

According to the algorithm of attack map, endanger degree of vulnerability and optimal attack path, an optimal attack path can be found as follow:

1. Using the vulnerability of default group name of SNMP to obtain the privilege from firewall administrator and modify firewall configuration so that the ordinary users can access some sensitive server port.

2. Using the vulnerability of SQL injection to obtain the privilege from portal system administrator and further obtain the privilege from server administrator.

3. Using the portal system server as a springboard to blast administrator password of OA application server via port 3389.

4. Using single-point to login the vulnerability of Apache Struts2 and execute malicious code. Using administrator account of portal system to login other systems and obtain privilege from other system

administrator.

5. Using the vulnerability of database server ms08-067 to gain privilege from database server administrator and obtain a lot of business data.

6. Seeking whether the XML injection vulnerability exist in the financial system and portal system when using XML for data integration, if exist, then using the XML injection vulnerability to obtain business data from financial system

7.So far, penetration testers basically achieved all the permissions form the test network.

**Assessment of hierarchical analysis in experiment network.** After inviting experts to check the penetration test results, the relative influence on the sorting of comparison matrix in each layer was given, which relative affected the sorting, according to the danger level of vulnerability and utilization of difficulty in the process of penetration test. Proportional scaling method was used to construct the judgement matrices and the matrix was shown as follows:

$$\mathbf{A} = \begin{pmatrix} 1 & 3.25 & 1.57 & 2.09 \\ 0.31 & 1 & 0.53 & 0.68 \\ 0.64 & 1.89 & 1 & 1.35 \\ 0.48 & 1.47 & 0.74 & 1 \end{pmatrix}$$

After calculation the maximum eigenvalue was λ = 4.0009 in this matrix. And this eigenvalue corresponds to normalized vector was W=[0.4142, 0.1323, 0.2587, 0.1948], calculating concordance index(4.0009-4) / (4-1)= 0.000 3CI when order n=4, RI=0.9, this moment consistency ratio: CR=CI/RI = 0.00033＜0.1, while the maximum eigenvalue of matrix A corresponds to the planning vector can be used as the weight of criterion layer to target layer.

The weight of index level to target layer was calculated via the same algorithm, and expert was invited to judge the weight.

Table 3.2 weight of index level and expert statistics

| Index level | Weight of risk value | Sorting | High | Higher | Medium | Lower | Low |
|---|---|---|---|---|---|---|---|
| Confidentiality | 0.1412 | 3 | 0 | 2 | 6 | 9 | 3 |
| Integrity | 0.0939 | 7 | 3 | 4 | 3 | 5 | 5 |
| Availability | 0.1791 | 1 | 2 | 2 | 10 | 2 | 4 |
| Environmental factor | 0.0540 | 9 | 1 | 2 | 3 | 8 | 6 |
| Human factor | 0.0783 | 8 | 2 | 1 | 3 | 9 | 5 |
| Technology vulnerability | 0.1564 | 2 | 1 | 5 | 9 | 3 | 2 |
| Management vulnerability | 0.1023 | 4 | 2 | 3 | 6 | 7 | 2 |
| Security precautions | 0.0974 | 5 | 0 | 2 | 5 | 11 | 2 |
| Security measurement | 0.0974 | 6 | 1 | 3 | 4 | 9 | 3 |

The total evaluation result was B=W×R=[0.11, 0.14, 0.31, 0.41, 0.17], and the biggest data in five value was 0.41. According to the expert's judgment, security level in experiment network was "medium"

## The advantages of hierarchical analysis based on the results of percolation test

In the process of using hierarchical analysis to evaluate the risk in experiment network was based on the results of percolation test. It can be found that hierarchical analysis has more advantages than general fuzzy hierarchical analysis, as it not only considered more comprehensive security risk for the target system, and finally the safety evaluation was given by the target system when hierarchical analysis processing risks evaluation. And the advantages were shown as follow:

Before establishing judgment matrix, expert was provided with the results of percolation test and has a directly understanding to the number of vulnerability in the internet and the utilization difficulty of vulnerability, constructing more suitable judgment matrix in experiment network.

After giving the whole level of security risk in experiment network, the operations manager was provided with a detail vulnerability list according to the results of percolation test and the reinforcement scheme of internet on every security risk point was provided by operations manager according to the results of percolation test.

## Reference

[1] Wen Quan, Wu MingJie, Wang ZeYu. A method of security and automation information systems of penetration test: CN, CN103532793 A. 2014.

[2]Liu Yang. Analysis of information systems security risks and vulnerabilities based on penetration test[C].Chinese News Technological Staff Federation of the Sixth Congress on2014 Academic Annual Conference. 2014.

[3]Jiang Yang. Research of key technology based on penetration test[D]. Xidian Electronic Engineering University, 2014.

[4]Pu FuLian. Technical research of autonomous collaborative network penetration test[D]. University of Electronic Science and Technology of China, 2014.

[5]Tian LiJun. Research on thetechnology and method of penetration test[D]. Railway Computer Application. 2015; 2:8-12.

[6]Zhuang Z S. Research on the Security Model Design of Accounting Information System Based on the B/S Model[J]. Applied Mechanics & Materials, 2014, 687-691:1840-1843.

[7]Fang S L. Vulnerability Analysis and Research of IPv6 Network Based on Penetration Testing[J]. Journal of Hunan Institute of Science & Technology, 2013.

[8]Engebretson P. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy[J]. Syngress, 2014.

[9]Finke K A, Mayne P W, Klopp R A. Piezocone Penetration Testing in Atlantic Piedmont Residuum[J]. Journal of Geotechnical & Geoenvironmental Engineering, 2014, 127:48-54.

[10]Engebretson P. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy[J]. Syngress, 2014.

[11]Huang WeiJun. Assessment process of information security risk based on penetration test[J]. China Management Informationization. 2015; 15(15):99-102.

[12]Wei Xing. Research on Web penetration test based on manual SQL injection[d]. North University of China; 2015.