Computer Information System Construction Based on Information System Security Level and Structure Model

Lei Gao *

1 School of Computer and Information Engineering, Beijing Technology and Business University, 100048, China
2 School of Engineering and Advanced Technology, Chengdu, Sichuan, China
3 Advanced Technology, ABC University, Nanjing, Jiangsu, China

Abstract — Objective: with the development of information technology, computer information system has become the lifeblood of the national institutions and the pillar of the social activities, so the information security is particularly important. Methods: in this paper, according to the level and structure of information security model, it is proposed based on the host, network, facilities, and methods such as the security policy of security events. Process : design a system of information system security model and empirically validate the practicability of this model. Analysis : use the method of risk analysis technology forms and advantages of system security threat. Conclusion: building a set of perfect security system for information system from the system angle.

Keywords - Information System; Security System; Security Tactic; Security Service ponent; format; style; styling; insert

I. INTRODUCTION

Though having a wide application, information technology has also made our information security situation very grim. According to the statistics by 2010, there were more than 420 million Internet users across the country, but the basic safety knowledge was known by less than 40% of Internet users, e-commerce transactions reached more than $4 trillion in 2010 and the network shopping amounts more than $400 billion (Liu, 2001). It is just because of a huge benefit in the network that domain name hijacking, web tampering and hacking events appear more and more according to the national computer virus emergency response center statistics, China's access to the Internet computer implanted Trojans reached 91.47%, namely, nine out of ten computer access to the Internet in our country, (Hutchison, 2016) there are eight units under control which have a lot to do with the black economy industrial development. It is estimated according to the national computer network emergency center that the current "hackers" industry output value has more than 238 million Yuan, the damage reaches to 7.6 billion Yuan. Hackers industry refers to the training and professional hackers, hackers training threshold is very low, which doesn’t need a degree or any experience, and no need to understand English, only need to pay hundreds of Yuan that the hacking tutorials and attack tools or even the method how to make use of the hacker technology to make money can be provided. Because convenient hacker training exists, all kinds of network attack such as Trojan virus are increasing (Langer, 2016).
government organizations really get a wide range of applications. For its growing dependence information system and the information system on operation risk, benefits and opportunities of the business, many organizations make the information security management as a part of enterprise management which is more and more critical. Top management needs to ensure that the information technology adapts to the enterprise strategy, enterprise strategy and appropriate use of the advantages of information technology. But any system in the real world is a series of complex link, security measures must be penetrated into all parts of the system, some of which even don't know the system designers, implementers, and users. Therefore, insecurity is always present (Sambri, 2016; Lafuente, 2016). No system is perfect and no technology is a panacea. At present, the industry generally believes that government and enterprises must work together to face the information security problem (Muhammad, 2016; Cho, 2016). Government and enterprise management has a responsibility to ensure that providing a safe environment information system for all users, moreover, the government departments and enterprises should be in the awareness of the information system security benefits at the same time (Li, 2016; Sunil, 2016).

II. METHODS PRINCIPLE

A. Information System Security Level

Open systems interconnection reference model of Open System Interconnect (OSI) is the international organization for standardization (ISO) and the international telegraph and telephone consultative committee (CCITT) jointly formulated by the Open systems interconnection reference model, for the Open System interconnection information provides a function of the structure of the framework. Each layer of the OSI seven layer models has clear characteristics (Stroer, 2016). Basically, in the seventh to the fourth layer handles the end-to-end communication between data sources and data destination, and the third to the first layer handles communication between network devices. In addition, the seven layers of the OSI model can also be divided into two groups: the upper (layer layer 7, 6, and 5) and the lower layer (layer 4, 3, 1) layer 2 and layer o OSI upper processing application of the model problem, and usually only used in the software. At the highest levels, that is, the application layer is the closest with end users. The lower of the OSI model is to process data transmission. The physical layer and data link layer application on hardware and software. With bottom, that is, the physical layer is the physical network media (wire), for example, the most close to, and be responsible for sending data on the media. As shown in figure 2:

![Structure layer of the OSI model figure.](image)

A detailed description of each layer are shown in table I.

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>The main function</th>
<th>Functions overview</th>
<th>The sample application</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Applicator layer</td>
<td>Provide web service interface</td>
<td>Provide (OSI) user services, such as file transfer email, network management, etc</td>
<td>Telnet, HTTP</td>
</tr>
<tr>
<td>6</td>
<td>Presentation layer</td>
<td>To transform the upper data or information</td>
<td>The exchange between different formats and coding</td>
<td>ASCII, JPEG, EBCDIC</td>
</tr>
<tr>
<td>5</td>
<td>Session layer</td>
<td>Session management between hosts</td>
<td>In between the two application process establishment and management with communication in the form of dialogue. The data stream side there are three kinds of control mode, namely the simplex, half duplex, duplex</td>
<td>The operating system/application access plan</td>
</tr>
<tr>
<td>4</td>
<td>Transport layer</td>
<td>The upper data transmission</td>
<td>Multiple use provide transfer way, to realize data exchange between the endpoints to the endpoint, provide the session layer entity with transparent and reliable data transmission service</td>
<td>TCP, UDP, SPX</td>
</tr>
</tbody>
</table>
LEI GAO: COMPUTER INFORMATION SYSTEM…

<table>
<thead>
<tr>
<th>3</th>
<th>Network layer</th>
<th>For routing packets between subnets</th>
<th>With packet switching and routing for entities to provide end-to-end transport layer exchange of network data, transport function makes the transport layer to get rid of routing and congestion control, network transmission, exchange way details, for data transmission</th>
<th>IP, IPX</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Link layer</td>
<td>On the physical media of unreliable provide reliable transmission</td>
<td>To transmit binary data blocks, and carry on error detection and data flow control. It is divided into two layers, namely the media access control protocol and the logical link control protocol.</td>
<td>802.3/802.2, HDLC</td>
</tr>
<tr>
<td>1</td>
<td>Physical layer</td>
<td>Provides a data transmission of physical media</td>
<td>Through mechanical and electrical interconnection way to connect the entities, used to get data flow</td>
<td>EIS/TIA-232 V.35, 10BASE5, 10BASE2, 10BASET</td>
</tr>
</tbody>
</table>

B. The Security Policy

In today's information technology rapid development, solve the problem of information security, not only depends on good information security management system, (Lin, 2016) and more to information security requirements into specific information system management. And the security policy formulation and implementation of information system is the necessary technical measures to implement the information security requirements. Information system security policy is divided into six classes, as shown in figure 3.

![Security policy diagram](image)

Figure 3. Information system security strategy.

Designed to protect the computer server, data storage, system terminals, hardware facilities, such as network exchange from natural disasters, man-made destruction, ensure use safety. Physical security strategy focuses on storing computer servers, data storage devices, security of core network switching equipment room. Its site selection and planning and construction should follow GB 9361 computer site safety requirements and GB2887 computer technology site condition, ensure constant temperature, constant humidity, lightning protection, waterproof, fire prevention, rat, antimagnetic, antistatic, equipped with anti-theft alarm device, provides a good grounding and power supply environment, matching as the core device configuration and its power to voltage stability and UPS uninterruptible power supply.

Resist network resources could be aimed at preventing and attack, ensure no illegal use of and access to network resources, the flow of data within a protection network security. Access control is an important means of maintaining network security, protection of network resources, is one of the core network security strategies. Access control including access authorization control, access control, network directory level security control, properties, safety control, network server security control, network monitoring and locking control, network port and node firewall security control and control. Security (authentication), content inspection is also an effective measure to protect the safety of network. Network encryption methods including link encryption, endpoint encryption, encryption and node link encryption is to protect the network node link between data security, end-to-end encryption is to from the source end users to the transmission of data between end users to provide protection, node encryption is between the source node and destination node transmission link to provide protection. In addition, the digital certification in a certain extent to ensure the safety of online trades information.

To prevent data is accidental or intentional illegal disclosure, alteration, destruction, or illegally identification and control, to ensure data integrity, confidentiality, available. Storage security and data security include data transmission security. Data storage security system of security index according to the storage conditions, including whether they were illegal calls, etc., can use different data disaster backup, storage of cipher text, set access permissions, identification, such as local isolation strategy to improve safety level.

Aimed at preventing due to software quality defects or vulnerabilities were illegally control information system, or performance degradation, denial of service, stop. Software security policy can be divided into system software security policy and application security policy. Of general application software, it can be reference to the practice of the preceding paragraph, by strengthening the communication with the software provider, discovery, plug up loopholes in safety in a timely manner. Application of tailored software, can consider optimization through quality control system authentication, rich industry software development and marketing.
experience, a software company, to strengthen quality control in software development, strengthen the fault-tolerant design, arrange the trial run for a long time such as strategy to avoid risk, improve the level of security.

System management strategy is to strengthen operation and management of computer information system, and improve the system security and reliability. To ensure the system stable operation, reduce the malicious attacks and bring the negative effects of all kinds of fault, it is necessary to establish effective mechanism of system operation maintenance and related systems. For example, establish and improve the center machine room management system, information equipment operation procedures, system maintenance information system, network communication management system, emergency response system, and so on. According to the division of labor, we need to implement the system running and maintenance work responsibility system. To strengthen the training of relevant personnel and safety education, reduce because of wrong operation to the impact of the system safety. To keep the system operation, maintenance data, completes the related records, should organize emergency drills regularly, for a rainy day.

Designed to take advantage of this system are still in the running, a disaster recovery plan, will reduce disaster losses to minimum, and improves the security of the system security strategy. Should be mainly based on the actual situation of this unit and information system, study the influence of the system meet the business after the disaster; design business switching method after a disaster, such as the backup data regularly, depending on the type of disaster and make disaster recovery process, establish disaster early warning, trigger, response mechanism, organize related training and practice, timely update and maintain a disaster recovery plan, etc.

III. THE PROCESS OF SECURITY MODEL DESIGN

P2DR model is the ISS on behalf of the model of dynamic network security system is put forward, and the prototype of the dynamic security model P2DR model includes four main parts: Security Policy, Protection, testing and response. As shown in figure 4.

![Figure 4. P2DR model.](image)

P2DR model can use the safety of some typical mathematical formula 1 to express: R system in order to protect the security goal setting various protections after the protective time; or understand for under such protection way, the hacker attacks (intruder) safety target time. Dt representatives from invaders invasion began, the system can detect the time it takes to invasion behavior. Rt representative since found intrusion behavior, the response of the system is able to make enough to adjust the system to normal time.

\[ P > D + R \]

(1)

For the safety of the need to protect target, if the above mathematical formula 2 meet the protection time is greater than the detection time and response time, which is before the invaders harm security goals can be detected and processed in a timely manner. Formula is the premise of protection time 0 o Dt representative from invaders destroyed the safety target system, system can detect the time spent on damage behavior. Rt representative since found damaged, the response of the system is able to make enough to adjust the system to normal time. For example, to Web Server: to restore damaged page. And so, Dt and Rt is the exposure time Et safety target system. For the safety of the need to protect target, if the smaller Et system more security.

\[ E = D + R \]

(2)

In trust domain entity elements, there are two kinds of security policy attributes, namely trust entity in the domain elements Shared by the limited security policy attribute set, the entity itself has, not to violate the Sa special security policy attribute of Sp. Thus we can launch formula 3.

\[ S = S + \sum S_p \]

(3)

P2DR model is the overall security strategy of control and guidance, the integrated use of protective tools (such as firewalls, operating system authentication, encryption, etc.) at the same time, using the detection tools to understand and evaluate system security status, adjust the system by the reaction of appropriate security and the state of the lowest risk. This model has a total of four levels, from inside to outside, respectively is the security policy, management, technology, and training layers. Can be seen from the diagram is in the service of the upper bottom, the top of the "strategy" is on behalf of the security policy layer, the layer is the core of the entire model, by which guidance on the implementation of the other three levels. Strategy layer is composed of three parts of security policy system revision, implementation and evaluation. The second layer is management, it is according to the requirements of security policies formulated the corresponding management system, to regulate a variety of workflow. It includes management system for improvement, implementation and evaluation of three phase arg. The third layer is the technology layer, mainly from the perspective of security technology and product dynamic network information system security, it includes three stages of safety inspection, safety response and safety protection. Training is the most outer layer of the model, and the layer is the main component of the model. Added to the model focusing on technology to ignore the
lack of management, will be added to the model of management and training two aspects, the whole model in network security management and technology two aspects have been reflected, as shown in figure 5:

A. Security Policy Formulation Selecting a Template

In the information security management strategy, we need to strictly abide by the following main principles. (1) Purpose. Strategies for the organization of information security mission, strategy should reflect the organization's overall interests and the requirements of sustainable development. (2) Feasibility. Strategy should be practical and feasible, the goal should be able to achieve, and easy to measure and review. No feasibility of policy is not only a waste of time also can cause confusion. (3) Applicability. Strategy should reflect the reality of the organizational environment, reflecting the development level of information security. (4) Integrity. It can reflect all the business process securities' needs of the organization. (5) Economy. Strategy should be economic and reasonable, too complex and summary are not desirable. (6) Consistency. The consistency of strategy includes the following three levels: ① Consistent with national and local laws and regulations; ② Organization has some strategy, policy consistent; ③ Consistent with the overall security policy, to reflect the enterprise to the general point of view of information security, ensure that users do not see this strategy as unreasonable, even for one person. (7) Elastic. Strategy should not only meet the requirement of the current organization, and also satisfy the organization and the environment for the development of a period of time in the future.

B. Security Policy Assessment Phase

In the security strategy formulation to review them, after the completion of mainly from the perspective of organizational needs to develop security policy whether can meet the needs of the current organization and assess whether conform to the organization's future development direction. In addition, after the security policy is applied according to the three aspects from the management, technology and training to get the feedback of whether need to modify the organization's security policy, all levels of the whole system are closely combined, form a strict security system to meet organization needs.

C. Security Policy Execution Phase

Security policy execution is the security policy of mainly running state, its execution is rely on management, technology and training level of dynamic cycle do together. Three levels of common benign role to make the security policy is executed effectively. With the continuous development of technology, management level, when some previously established security policy is not to meet the needs of the development of the enterprise, will re-enter the assessment phase, the relevant personnel to confirm evaluation result and the security policies are revised, and will enter the next round of strategy execution phase.

D. Information Security Risk Assessment Method

In 1979, the《Federal Information Processing Standards》published by the National Bureau of Standards put forward ALE-based risk assessment method based on probability statistics. It is a quantitative assessment method based on probability statistics. Risks are expressed as an ordered set.

\[
\text{RISK} = \{(L_1,O_1),(L_2,O_2),\ldots,(L_n,O_n)\}
\]

(4)

\[L_i (i=1,2,\ldots,n)\] is the possibility of unexpected event. \(O_i (i=1,2,\ldots,n)\) is the consequence of unexpected event. Metrics of measuring risk is the expected annual loss.

\[
\text{ALE} = \sum_i L_i O_i F_i
\]

(5)

\(I(O_i)\) is the amount of annual loss caused by the event. \(F_i\) is the frequency of events.

E. Value Calculation of Information Assets

In different industries, because of the business, requirements of safety assurance and purpose of information security are different. To solve this problem, in the calculation of the value of assets, different weights are introduced to it.

\[
\text{AssetValue} = \text{Round1}\left\{\log_2\left[\left(A \times 2^{\text{conf}} + B \times 2^{\text{int}} + C \times 2^{\text{avail}}\right)/3\right]\right\}
\]

(6)

In this equation, conf represents the value of confidentiality, Int represents assignment of completeness, Avail represents assignment of usability. Round1 represents half adjust which reserves a decimal fraction. A is the weights of privacy, B is the weights of completeness, C is the weights of usability. A, B, C are constant between 0 and 3, and A+B+C=3.
Int = f(X_{int}, Y_{int}) \tag{7}

Function f can be represented by a matrix as shown in Tab.3.

### Table II: Matrix of Function f

<table>
<thead>
<tr>
<th>Value</th>
<th>X=4</th>
<th>X=3</th>
<th>X=2</th>
<th>X=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y=4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Y=3</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Y=2</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Y=1</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

IV. ASSESSMENTS AND ANALYSIS

In the information system security, the system risk assessment and analysis is very important. Information system risk analysis for the system is the purpose of the relevant personnel to provide a based on the protected information, computer network and system operation mode analysis method and the technical details: object is a system of risk analysis from each component to their function and management of a series of links: risk analysis approach is to analyze technology form of threat to system security, as well as within the system can be in the form of exploitation and utilization of the fragility of existence. There are two types of risk calculation method, as shown in figure 6:

A. Risk Analysis Matrix Method

Matrix method is mainly applied to the value of the two factors determine a factor worth. In risk calculation, often two elements to determine another element values to calculate. For example by the threat and vulnerability to determine the possibility of a security incident, the assets and vulnerability to determine the loss value of security incidents, etc. At the same time need to overall grasp the determination of value at risk so matrix method is widely used in risk analysis. Formula 4 shows the formula of the matrix method. Function f adopts the form of a matrix, with element factors of x and y values to build a two-dimensional matrix, matrix in m * n value is the element of Z values, table such as table II.

\[ z = f(x, y) \tag{7} \]

### Table III: Value Table

<table>
<thead>
<tr>
<th>x</th>
<th>y1</th>
<th>y2</th>
<th>...</th>
<th>yj</th>
<th>...</th>
<th>yn</th>
</tr>
</thead>
<tbody>
<tr>
<td>x1</td>
<td>z11</td>
<td>z12</td>
<td>...</td>
<td>zj</td>
<td>...</td>
<td>zin</td>
</tr>
<tr>
<td>x2</td>
<td>z21</td>
<td>z22</td>
<td>...</td>
<td>z2j</td>
<td>...</td>
<td>z2n</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td>...</td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>xi</td>
<td>z11</td>
<td>z12</td>
<td>...</td>
<td>zj</td>
<td>...</td>
<td>zim</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td>...</td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>x m</td>
<td>zm1</td>
<td>zm2</td>
<td>...</td>
<td>zmj</td>
<td>...</td>
<td>zmn</td>
</tr>
</tbody>
</table>

B. Risk Multiplication Calculation

Risk multiplication phase as follows: the characteristics of simple and clear, direct, in accordance with the unified formula, can get the result. Phase method using range: in risk terms usually set to two elements of another element values calculated, so the phase method is widely used in risk analysis. Formula 5 shows multiplication formula. When f as the incremental function, \( x \) can be directly multiplied, will be able to multiply after modulus, etc.

\[ z = f(x, y) = x \circ X y \tag{8} \]

V. CONCLUSION

The security system for information system is a multi-dimensional, multi-level, multi-factor and multi-objective system whose final goal is to guarantee information confidentiality, integrity, availability, controllability and reliability anywhere in the system at any time and any condition. Because of the large scale, complicated structure
and wide range of research of computer information system, this article only researched the security system model, security technology, security policy and risk assessment, so there are many aspects need to improve, which also need to be constantly explored and researched in the future. A network security model was proposed in this paper on the P2DR model, which will be the security policy, management and safety technology and safety training aspects in the dynamic model at the same time and can even reflect the industry consensus "three points, seven points management". In the application of the dynamic model to large enterprises, every aspect of the gradual refinement in this model made readers have a deeper understanding of the model. At the same time, for any organization or department, absolute security is difficult to achieve and there is no necessary. The modern information system security planning, strategy implementation system view and method view, have certain operability and help to develop information system security planning and implementation of the information system security policy to provide a basis and reference. Therefore, any organization or department in the concrete implementation of the safety planning and strategy, should follow two principles:

(1) adhere to the principle of combining technology strategy and management strategy and safe enough principle
(2) With the information system achieved, it is fair that the cost is taken for its security and a risk appears to the system which may be caused by the loss, and the security level is enough.

These are all subject to continue to study and promote model perfect place. At the same time, because my level is limited, in this paper, there must be many hold no place. Here, please all experts and scholars give more valuable opinions and suggestions to push the future research work to the next level.

REFERENCES