Journal of Theoretical and Applied Information Technology
10th March 2013. Vol. 49 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EVALUATING METHODS OF TELECOM DATA NETWORK BASED ON THE SCORE OF INDEX SYSTEM

[1]HUANG WENHUA

[1] Lecturer, School of Telecommunications and Information Engineering, Xi'an University of Posts and Telecommunications,
E-mail: [1]hwh_cara@yahoo.com.cn

ABSTRACT

Evaluation is a basic requirement to protect telecom data networks. How to carry out a usable evaluation is a main problem to solve in this paper. The index system is the basis of the analysis. The general framework is combined with the structure of China telecom data network to get the index system. The evaluation method is established based on the score of index system. The score is obtained through grading every index parameter and weighted sum. The feasibility of the method is verified by an example. The theoretical basis is given for security evaluation of telecom data networks in this research.

Keywords: *Telecom Data Networks; Security Evaluation; Index System; Score*

1. INTRODUCTION

The telecommunications network is the national information infrastructure. The telecom data network is an important part of telecom network. And the security problem of them is becoming increasingly serious with the growing of users and information flow. To solve the security problem, the security evaluation and the construction of security system must be strengthened [1]. Although there are a variety of specific practical ways for security evaluation at home and abroad， most of them such as ISO 17799, ISO 15408 focus on some aspects of the security technology, function and mechanisms based on concepts of security risk. The evaluating process relies mainly on the technological level and understanding level of tester of the network system. Just as the lack of unified system of security assessment framework, it is difficult to quantify a lot of the evaluation criteria and indexes.

The China telecom data network is a big complicated system. Building a unified security framework is necessary for security evaluation [2]. Over the years, ITU-T has been actively involved in telecommunications and information technology security research. In its proposal of X.805, a unified glossary has been established to discuss various aspects of security issues and provide a general communication system security framework model. Combining the general model with the reality of China telecom data network, the effective evaluation index system can be established. And the security level of system can be determined by estimating these parameters of evaluation.

2. THE SECURITY FRAMEWORK OF DATA NETWORKS BASED ON ITU-T X.805

2.1 The model of security framework based on ITU-T X.805

To strengthen the design, construction and operation in the process of safety protection, ITU-T defined a model of security framework for a distributed end-to-end application system aiming at threats and vulnerabilities of telecommunication network in the proposal of X.805, as shown in figure 1. The framework is defined based on three axes of dimension, layer and plane [3].

A Security Dimension is a set of security measures designed to address a particular aspect of the network security. These dimensions are not limited to the network, but extend to applications and end user information as well. The Security Dimensions are: (1) Access Control, (2) Authentication, (3) Non-repudiation, (4) Data Confidentiality, (5) Communication Security, (6) Data Integrity, (7) Availability, and (8) Privacy.

In order to provide an end-to-end security solution, the Security Dimensions described in the previous section must be applied to a hierarchy of network equipment and facility groupings, which are referred to as Security Layers. There are three layers: The Infrastructure Layer represents the fundamental building blocks of networks, their

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

services and applications. Examples of components that belong to this layer are individual routers, switches and servers as well as the communication links between individual routers, switches and servers. The Services Security Layer addresses security of services that Service Providers provide to their customers. These services range from basic transport and connectivity to service enablers like those that are necessary for providing Internet access (e.g. AAA services, etc.) to value-added services such as VPN etc. The Applications Security Layer focuses on security of the network-based applications accessed by Service Provider customers. These applications are enabled by network services and include basic file transport (e.g., FTP) and web browsing applications, fundamental applications such as network-based voice messaging, email, as well as high-end applications such as electronic/mobile-commerce, video collaboration, etc.

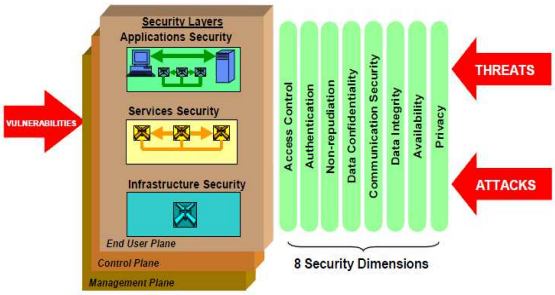

Figure1. *The Architecture Of Security System In Communication System*

A Security Plane is a certain type of network activity protected by Security Dimensions. There are three Security Planes to represent the three types of protected activities that take place on a network: (1) the Management Plane, (2) the Control Plane, and (3) the End-User Plane. The Management Security Plane is concerned with the protection of OAM&P functions of the network elements, transmission facilities, back-office systems, and Data Centers. The Control Security Plane is concerned with protection of the activities that enable the efficient delivery of information, services and applications across the network. This type of information is sometimes referred to as control or signaling information. The End-User Security Plane addresses security of access and use of the Service Provider's network by customers. This plane also represents actual end-user data flows.

The model of security framework covers the communications system security problems in many aspects. It provides the foundation for establishing security evaluation framework and index system of China telecom data network.

2.2 The Security Framework Of China Telecom Data Networks

In order to solve security issues of the telecom data network, security objectives and requirements must be clear from the inside to the outside of the telecom data network. It must be based on its own structure characteristics and the operating environment, which is the internal and external data network. Then it should be evaluated whether the protection to asset can meet to the realistic security requirements or not [4]. Telecom data network security evaluation framework is organized based on all of above requirements.

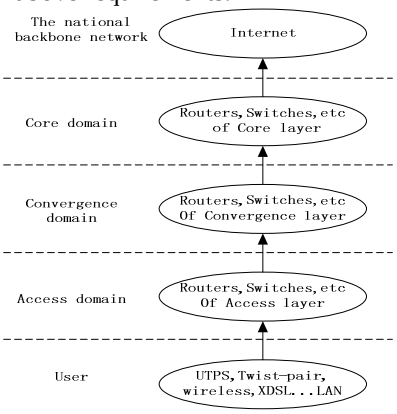

Figure 2. *The Layer Frame Of Telecom Data Networks In China*

At present our country telecommunication data network is divided into three layers structure. They are respectively the core layer, convergence layer and access layer, as shown in Figure 2. The specific functions of each layer are as follows: 1. Core layer: the core switching equipments are placed in this area, mainly used in converging data flow and connecting with backbone, or exchanging conditionally information in the local area network; 2. Convergence layer: the converging equipments and switching equipments are placed in this area, mainly used in converging data flow and connecting information in the local area network; 3. Access layer: the accessing equipments and switching equipments are placed in this area, mainly used in converging data flow and connecting the convergence layer network, or exchanging conditionally information in the local area network.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

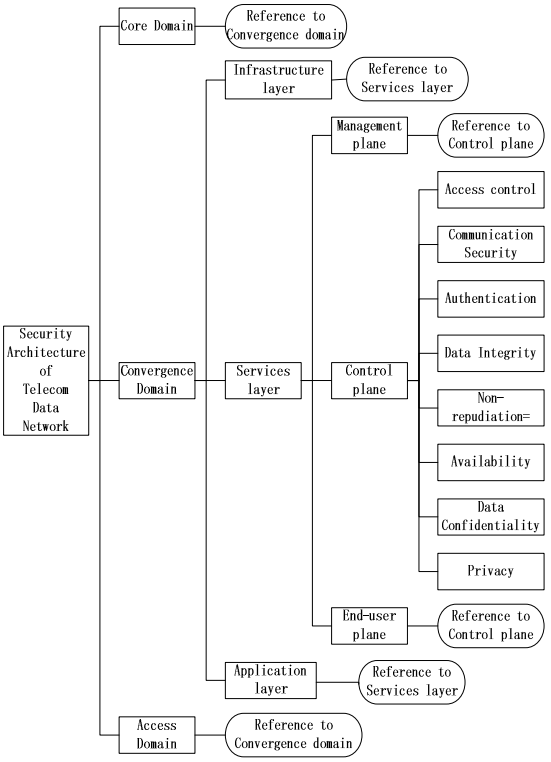

Figure3. *The Security Architecture Of Telecom Data Networks*

Therefore, from our country current hierarchical framework of telecom data network, the sub-framework of each layer firstly can be established for different security domains, with reference to the security framework model of ITU-T X.805. Then a whole security framework of China telecom data network can be established, as shown in figure 3.

3. TELECOM DATA NETWORK SECURITY GRADING BASED ON THE SCORE OF INDEX SYSTEM

3.1 The Index System Based On The Security Framework Of Data Networks

The security evaluation index system of telecom data network is the basis of collecting data and information about an evaluated object. The system is a group of related indexes established on the objectives and requirements of security assessment [5]. These indexes can reflect the basic appearance, quality and level of a security evaluation object. The system is a tool of security evaluation [6]. As one of the key to implement the assessment, the establishment of index system should be based on the security framework of China telecom data network. Combined with the analysis of specific assets and the security requirements, those indexes which reflect security properties of the evaluation objects can be obtained. A concrete method for index extracting based on the security framework of data networks is mentioned in reference [7]. It is through determining key assets of the evaluation objects and locating the assets to get the index system for security evaluation of telecom data networks. The index system is shown in table 1.

Table 1. *Index Parameters For Security Evaluation Of Telecom Data Networks*

Security Domain	*Security Layer*	*Security Plane*		*Level 1*	*Level 2*
Core Domain	Infrastructure Security	Management Security	Asset A1	Data Confidentiality Indexes	PR11PR12PR13…
				Availability Indexes	PR21PR22 R23…
				Data Integrity Indexes	PR31PR32 R33…
				Communication Security Indexes	PR41PR42 R43…
				Privacy Indexes	PR51PR52 R53…
				Non-repudiation Indexes	PR61PR62 R63…
				Authentication Indexes	PR71PR72 R73…
				Access Control Indexes	PR81PR82 R83…
			Asset A2	Reference to Asset A1	
			…	…	
			Asset AM	Reference to Asset A1	
		Control Security	Reference to Management Security		
		End User Security	Reference to Management Security		
	Services Security	Reference to Infrastructure Security			
	Application Security	Reference to Infrastructure Security			
Convergence Domain	Reference to Core Domain				
Access Domain	Reference to Core Domain				

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.2 The Concrete Index Parameter Based On Common Criteria

Table 2. *Index Parameters Based On CC (Part)*

Security dimension	***Index parameter***	***Remark***
Access control	Security audit automatic response	Make security warning
	Security audit analysis	Monitor and audit events and point out the potential damage
	Security audit review	Query audit data and provide audit tools for authorized user
	Security audit event selection	Selective audit on centralized audit events
	Security audit event storage	Protect stored audit records to avoid unauthorized removal
	Access flags	Display to the user about the appropriate use of advice and warning information
	Access history	Display an access history of the user account for the successful and unsuccessful access
	Information flow control	Ask the server to perform appropriate access control when the user data is output to the outside the server
	Session establishment	Provide user to access server request based on attribute
	Multiple concurrent session control	The concurrent session limit to the same user
	Session locking	Lock an interactive session after a certain time interval

The concrete index parameters can be got by some related standard such as Common Criteria. The CC is useful as a guide for the development of products or systems with IT security functions. The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation and for the procurement of commercial products and systems with such functions [8]. According to security functional requirements classes, subclasses and components of CC, the index parameters for a security dimension can be obtained in each plane. A part of the parameters for dimension of access control is shown in table 2.

3.3 The Evaluation Method Based On The Score Of Index System

Obtained the detailed evaluation indexes, it become an important problem for the security evaluation of telecom data network how to obtain the numerical value of parameters and by which means to operate these values to determine the security level.

A method for telecom data network security grading is given in this paper that is based on the score of index system. The security level of system can be determined by this means, which includes through the investigation to those parameters of different assets corresponding with each layer of the plane in the domain of data network, inspect the security of system and mark the points, and then calculate the security scores of the telecom data network according to certain rules. The grading method is carried out as the following steps:

1. Due to the different importance to three domains of telecom data network, the first thing necessarily is to identify the weight value of the three domains, which are denoted as x_1, x_2, x_3. In the same domain i, the importance level of different layer is not same, so the weight value of the three layers in each domain needs also to be identified, which are denoted as y_{i1}, y_{i2}, y_{i3}. For the different plane on the same layer j in domain i, the importance level is not the same either, so it also needs to consider the weight value of three planes, which are denoted by $z_{ij1}, z_{ij2}, z_{ij3}$.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. Before points are marked to different asset plane k on the same layer j in domain i, making use of the index parameters corresponding to eight dimensions, first of all need to be considered is the important degree of these assets in the system. The weight is assigned to every asset based on the divided level of assets. Considering all assets of plane k on layer j in domain i, their weight values are denoted as $\alpha_{ijk1},\alpha_{ijk2},\cdots,\alpha_{ijkm},\cdots,\alpha_{ijkM}$, which M is the total number of assets locating at domain i layer j plane k.

3. The study on assets gives security scores of all the assets corresponding to those parameters based on the evaluation detailed indexes of eight dimensions. It is supposed there are L detailed parameters, denoted as $C_1, C_2, \cdots C_L$. Mark a specific asset m in domain i layer j plane k according to the actual situation of the asset. If it has a index then the value is 1; if the device does not have the index, then the value is 0. Therefore, the score is marked as:

$$u_{ijkml} = \delta, \delta = \{0,1\} \ (l = 1,2,\cdots L) \quad (1)$$

4. Due to the differences of specific equipment model, function, performance and the security technical, the degree is different that different equipments complete an index parameter. Because the completed degree of the parameters has an impact on the security of data network, it is necessary to consider the weight of the degree. A completed degree of equipment m to index C_l is denote by β_{ijkml}.

5. All of indexes will affect the security, but the degree of influence is different, that is the degree of importance is different. Therefore the weight of each index also needs to be considered. For the asset located at plane k on layer j in domain i, the weights of index C_l are denoted as $s_{ijkm1}, s_{ijkm2}, \cdots s_{ijkmL}$. The comprehensive score of an asset m, recorded as X_{ijkm}, is got when using the following formula combined with a index parameter score, completed degree and index weights:

$$X_{ijkm} = \sum_{l=1}^{L} s_{ijkml}\beta_{ijkml}u_{ijkml} \quad (2)$$

6. All of assets in domain i layer j plane k are marked as steps 3, 4, 5, and combined with the weight in step 2. Then the total scores of all assets in domain i layer j plane k can be obtained:

$$V_{ijk} = \sum_{m=1}^{M} \alpha_{ijkm} X_{ijkm} \quad (3)$$

7. At last, the security of whole telecom data network is marked. Get a security score of the data network system, considered all of three domains, three layers of each domain and three planes of each layer with respective weights, and combined with step 6. The score is a mean F:

$$F = \sum_{i=1}^{3}\sum_{j=1}^{3}\sum_{k=1}^{3} x_i y_{ij} z_{ijk} V_{ijk} \quad (4)$$

Using the above method, the range of value of F can be obtained, that is $[Min, Max]$. According to the sequence from small to large, this interval is divided into five subintervals. Then five security levels of data network system are listed, as shown table 3. For example, a final score obtained according to the above method is f for a data network system. If $f \in (X_2, X_3]$, then the security grade of this system is level 3.

Table 3. *Hierarchy Partition Of Telecom Data Networks*

Level of telecom data network	***Range of value***
1	$[Min, X_1]$
2	$(X_1, X_2]$
3	$(X_2, X_3]$
4	$(X_3, X_4]$
5	$(X_4, Max]$

Though the index system evaluation method, the security level become a specific quantified value. It is necessary to pay attention that, here, weights of each domain, plane and layer are obtained from experience or experiments and range boundary of subintervals is also reached by the experiment. At the same time, each index parameter is related to specific operational issues, that is how to get numerical values of parameters for different assets and what is the operation. Some quantitative values can be obtained through consulting running logs of network equipments. Some can through the survey to network user. Some need network test and so on. The choice needs to be flexible according to specific assets, indexes and the state of network on the basis of protecting the data network security.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. AN EXAMPLE FOR EVALUATION METHOD

4.1 Experimental Environment And Topology Of Network

The experiment environment is shown as figure 4. A LAN is made up of 40 hosts, 3 servers, 3 routers and 1 switch. Three servers which are the web server, mail server and access authentication server, access network through the router. To simplify the problem, the asset level is considered to be the same for the same type of equipment.

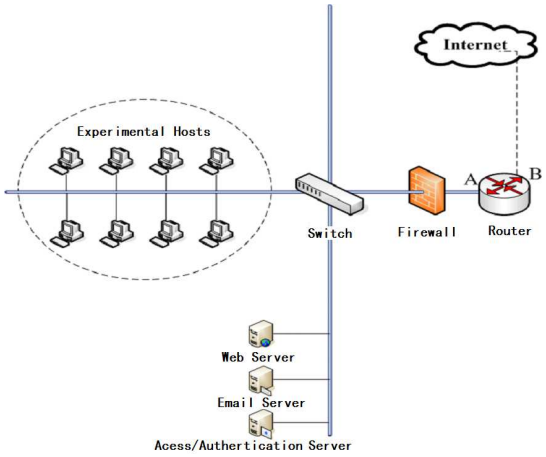

Figure 4. *Topology Of Experimental Network*

4.2 Asset Index Survey

Detect each index value of experiment network using the following auxiliary tools: Snort SuperScan and Whisker/Libwhisker[9]. And combined with questionnaire, the major assets in experimental environment are scored. A part of related parameters are listed as shown in table 4.

4.3 Scores Of Index System

According to the evaluating algorithm, the scoring process is executed as follows:

1) By normalization method, set $[Min, Max]$ to $[0,1]$. The first necessary thing is to identify the weight value of the three domains. The values of weight x_1, x_2, x_3 are taken as {0.4, 0.3, 0.3} for the core domain, convergence domain and access domain in this experiment.

2) The weight value of the three layers in each domain needs also to be identified. The experiment network is in access domain, the values of y_{31}, y_{32}, y_{33} are taken as {0.4,0.3,0.3} to the infrastructure layer, the services layer and applications layer of access domain.

3) The experiment network is in infrastructure layer of access domain, the values of $z_{331}, z_{332}, z_{333}$ are taken as {0.3,0.4,0.3} to the management plane, the control plane and the end-user plane.

Table 4. *Scores Of Index Parameters For Assets (Part)*

Security dimension	*Index parameters*	*Switch*		*Router*		*Server*		*Host*	
		Score	*C.D*	*Score*	*C.D*	*Score*	*C.D.*	*Score*	*C.D.*
Access control	Security audit automatic response	1	0.6	1	0.7	1	0.6	0	0
	Security audit analysis	0	0	0	0	0	0	0	0
	Security audit review	0	0	0	0	0	0	1	1
	Security audit event selection	0	0	0	0	0	0	0	0
	Security audit event storage	0	0	0	0	1	0.9	1	0.9
	Access flags	0	0	0	0	0	0	0	0
	Access history	0	0	0	0	0	0	1	1
	Information flow control	0	0	0	0	0	0	1	0
	Session establishment	1	0.1	1	0.2	1	0.2	0	0
	Multiple concurrent session control	1	0.8	1	0.8	0	0	0	0
	Session locking	0	0	0	0	0	0	0	0

(C.D. is completed degree in the table.)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4) Get the level and weight of asset according to the method in reference [10][11] which is used to classify assets. The level of host is medium. The level of servers is important. And those of switches and routers are very important. The weight of host is 0.006. The weight of servers is 0.078. That of switches is 0.085 and that of routers is 0.271.

That is

$\alpha_{3311},\alpha_{3312},\cdots,\alpha_{33140}$ =0.006, $\alpha_{33141},\alpha_{33142},\alpha_{33143}$ =0.078, α_{33144}, α_{33145}, α_{33146} =0.085, α_{33147} =0.271.

5) In order to simplify the model, the importance degree of each index parameter is considered as the same in the experiment environment. A s_{ijkml} is 0.02 from the formula of $\sum_{l=1}^{50} s_{ijkml}=1$. A u_{ijkml} of asset m and β_{ijkml} are obtained after the asset index survey. Work out the weighted sum of these numbers. The score of asset m can be got. The result of V_{ijk} is calculated by using $V_{ijk}=\sum_{m=1}^{M}\alpha_{ijkm}X_{ijkm}$, in which $X_{3311},X_{3312}\cdots,X_{33140}=0.314$, $X_{33141},X_{33142},X_{33143}=0.308$, $X_{33144},X_{33145},X_{33146}=0.302$, $X_{33147}=0.306$. The result is V_{331} =0.307368.

6) The environment lies in the terminal user plane of infrastructure layer of access domain. The other planes of this layer and all of those in the other two domains are considered as safe. For this reason, the value is 1 for the completed degree and each index. The security means of experiment system can be obtained by $F=\sum_{i=1}^{3}\sum_{j=1}^{3}\sum_{k=1}^{3}x_i y_{ij} z_{ijk} V_{ijk}\approx 0.98$ in the end.

The scores and grades are compared. Because that 0.98 is very close to the maximum value (1), the whole system is with high security. In fact, as the other planes and layers of each domain are considered very safe, the experimental network almost has not an effect on the entire data network security.

The case study is in a smaller network environment. All of values of weight are based on the results of the investigation or expert experience. Although many of those assets indexes are not be related to this experiment and the result is a relatively ideal numerical value, these does not affect the validation of the proposed index extraction and evaluation method.

On the other hand, there is seldom a method especially for the security evaluation of telecom data network in other researches at present. So it provides a new direction to researchers to improve that.

5. CONCLUSIONS

The security evaluation of telecom data network is a huge and complicated engineering. A set of indexes for evaluation is a basic requirement for carrying out the evaluation successfully to protect telecom data network. An method for evaluation is given in this paper. The main idea of this method is that the security evaluation index system needs to be set up based on the security framework, and then the evaluation can be finished by security grading based on the index scores. The conclusions are as follows:

1. A general security framework of communication system is combined with hierarchy structure of China telecom data network. Then the security framework of China telecom data network is put forward, which lay the foundation for security evaluation;

2. Safety grade is an important result that needs to be obtained in the security evaluation of telecom data network. The security evaluation index system provides a basis to solve the security problem of grading.

3. The evaluation method is established based on the score of index system. The concrete index parameters can be obtained by evaluation standard such as Common Criteria.

4. The security level of telecom data network is determined by the score of index system. The score is obtained through grading every index parameter and weighted sum. The feasibility of the method is verified by an example. The theoretical basis is given for security evaluation of telecom data networks in this research.

ACKNOWLEDGEMENT

This work has been partially supported by the project of the natural science fund of Shaanxi Province called 2009MJ8002-3 and by the project of Youth Research fund of Xi'an University of posts & telecommunications called ZL 2010-15 and by the project of Special Scientific Research plan of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the department of education Shaanxi Province called 11JK0920.

REFRENCES:

[1] Wei wei, "Study on Risk Evaluation of Telecom Networks", *Telecommunications Network Technology*, vol 259, pp. 7-11, September 2009.

[2] Hojaji, Fazilat, Shirazi, Mohammad Reza Ayatollahzadeh"A framework for evaluating SOA governance frameworks" *Journal of Theoretical and Applied Information Technology*, v40, n2, pp.120-130, June 2012

[3] ITU-T X.805. Part 6: Security dimension. Swiss,2008

[4] Abbas, Rabab A. ; Mokhtar, Mohd Rosmadi; Sulaiman, Rossilawati; Othman, Zulaiha Ali; Zin, Abdullah Mohd "Impact of disasters in Southeast Asia on Malaysian computer networks" *Journal of Theoretical and Applied Information Technology*, v37, n2, pp.188-198, March 2012

[5] Liao hui, Ling jie, "Research on network terminal security assessment index system", *Computer Engineering and Design*, vol 65, pp. 47-51, 2010.

[6] Sunitha, R. ; Sreerama, R. Kumar; Mathew, Abraham T. "A composite security index for on-line steady-state security evaluation" *Electric Power Components and Systems*, v39, n1, pp.1-14, January 2011

[7] Huang Wenhua , "Research on Extracting Method of Evaluation Index System for Telecom Data Network based on ITU-T X.805", *In Proceedings of the International Conference on Computer Science and Service System, IEEE Press*, pp.181-185, 2012

[8] ISO15408. Part 1: Introduction and general model. 1999.

[9] Stiawan, Deris ; Shakhatreh, Ala' Yaseen Ibrahim; Idris, Mohd. Yazid; Kamarulnizam, Abu Bakar; Abdul, Hanan Abdullah "Intrusion prevention system: A survey " *Journal of Theoretical and Applied Information Technology*, v40, n1, pp.44-54, June2012

[10] Lei Bo, Liu Jianhua, "The Principle of Telecom Data Network Equipment Classification Based on the Fuzzy Comprehensive Decision ", *In Proceedings of China Institute of Computer Information Security Professional Committee (Conference)*, pp.370-377, 2006Fu, Maoming

[11] "Application of fuzzy comprehensive analysis to information security evaluation" *Xinan Jiaotong Daxue Xuebao/Journal of Southwest Jiaotong University*, v45, n3, pp.440-444, June 2010