ISSN : 0974 - 7435 Volume 10 Issue 11

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(11), 2014 [5377-5386]

The research of computer network security and the protective measures

Huifen Jiang

First Affiliated Hospital of Soochow University, Suzhou, Jiangsu, (CHINA)

ABSTRACT

There are many manifestations in the problem of computer network security. Such as the individual's privacy disclosure, the database file is stolen; the computer system is damaged, etc. To some extent, these conditions make certain losses to people and bring some trouble in life. Some vicious damage and attack can do harm to national security, social stability and economic construction. It also caused an adverse impact on the lives of the lives of people. This paper analyzed the vulnerability of the network through traverse modes. Stable and safe operation of the computer network center is very important. Strengthen the management software is mainly for the prevention of system security vulnerabilities. A series of stages is needed to establish a computer network security protection. Such as specific research, exploitation and design, system analysis, the selection of equipment, software installation, commissioning and acceptance.

KEYWORDS

Computer network; Traverse matching algorithm; Protective measures; Safety protection.

INTRODUCTION

With the progress of the society, we are gradually entering the network age; the computer network at the same time also has brought a lot of convenience to people's learning work and life. Such as people can understand world affairs in home, learn to shop on the internet, and see a doctor, make friends, and so on. With the gradually strong of the function of computer network, the corresponding problems in network security also become the focus of attention, and it faced with new opportunities and challenges constantly.

Strengthen the management software is mainly for the prevention of system security vulnerabilities. A series of stages is needed to establish a computer network security protection. Such as specific research, exploitation and design, system analysis, the selection of equipment, software installation, commissioning and acceptance. Since the late 80s, the Morris worm destruction network security events occurred. All kinds of network security threaten and the news about the network intrusion appeared in the country like the mushroom. China didn't avoid the big trend. Network security problems also occurred in China, and produced some bad social impact. For example, the king of worm virus which was all the rage, this network virus is powerful; it can make the influence of the poisoning of the network center in the world lost processing ability of computer data. When the king worm virus occurred in our country there are more than 80 percent of the Internet as affected by this virus attacks and forced to interrupt the network, making the corresponding computer is in a state of paralysis. According to the related reports, the average increase of new computer viruses every day is over thirty-five kinds. Within the scope of the country, the virus is almost once every ten seconds will invade a computer network system.

Network security risks not only the junk software and viruses in the traditional sense, but also contains some dangerous index relatively high fishing software ads implanted spy ware, and so on. These are serious threats to the security of the Internet. Among these threaten the security of a network virus, spy ware hazards is one of the most prominent, It is recognized as a plug-in that the harm to the network operation. Network scholars and relevant experts agreed that, in the next few years. The number of spy plug-in will grow rapidly and become the greatest harm to the network security risks.

Network security can be divided into the following sections. First, the data security: First, It requires a computer network to ensure that users' data confidentiality, consistency, integrity, protection of data against unauthorized access to other people. Second, the security software: the operating system is not protecting the network software and application software illegal intrusion; the system can't be illegally copied and tampered with, from virus damage. Third, the physical security network: the physical environment, including computer room and physical condition as well as the necessary facilities comply with national safety standards, installation and configuration of computer hardware and network transmission lines to meet certain safety standards. Fourth, the safety management system: If the incident occurred when running the network, you can then get the appropriate emergency treatment the first time, which includes the establishment of safety management systems and existing safety audits and risk analysis.

MODELING

The computer network security research can be roughly divided into the following several kinds of research methods

(1) System analysis: On the basis of our current computer network running on the security situation and found problems in network operations, and the causes of these phenomena are analyzed through systems analysis approach to the various elements causing these comprehensive network security analysis, and find appropriate solutions.

(2) The instance study method: Questionnaires for some network users, these users understand the perception of the current situation in the construction of network security, for the security of the status quo were to take cases of computer network analysis and demonstration, to find universality in one case, to make the right theory for the construction of network security guidance

(3) Literature research method: clearance to collect, review and collate the relevant national requirements for the construction of computer network security and related laws and regulations and literature, can be a good grasp of cutting-edge research status and dynamics related to computer network security in China.

For computer network security can be roughly divided into the following several methods of complementary relationship between them, their research relationship as shown in Figure 1:

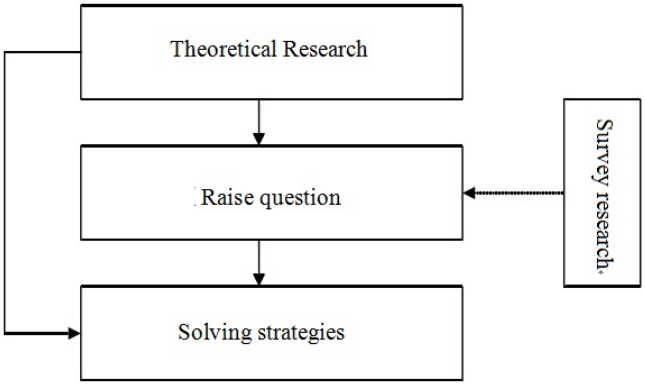

Figure 1 : Network security research

Preparation before a model

For computer network security, the existing protective measures are: virus detection tools, antivirus software, firewalls, virus intrusion detection systems, virus protection system, these protective measures in a certain extent, although made to protect computer network security purposes, But for computer network security incidents affecting the obvious limitations. These limitations in the following three aspects:

First, the appropriate virus detection these existing safeguards are generated after a virus attack, the security means a passive way to increase the time in the network era of rapid development of modern, network attack sharp, To face these sorts of attacks necessarily need to spend huge security cost, so the safe operation of this passive defense software can't effectively protect computer networks.

Second, the current security measures for these new unknown attacks lack of effective monitoring and means of defense, protective measures are now using their computer network is based on the basic principles of rule matching works, for some new positions to attack them will be helpless, unable to find the appropriate matching rules, so these new viruses is the lack of appropriate responses to attacks.

Third, these protective measures are used for internal network attacks are caused by the lack of appropriate protective effect, especially for a protective measure by intrusion detection systems and firewalls, they are located at the network edge, for the computer internal network attacks is no way.

Situation of computer network development

With the development of the times, among microcomputer gradually into people's lives, and now people in their daily life and work are inseparable from the study of computer networks, the share of modern information exchange between people and resources of these urgent requirements are promote

the rapid development of computer networks. In recent years, along with the expanding of internet, the membrane and the increase in the number of Internet users. According to statistical data in this Internet decency association, such as the number of hosts shown in Figure 2 Internet access.

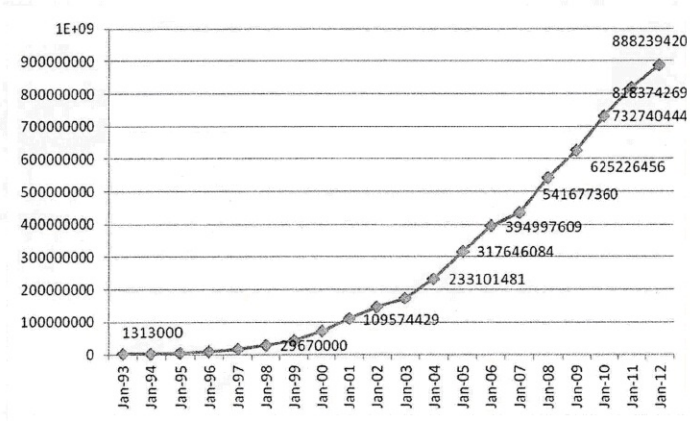

Figure 2 : Internet access to the number of hosts

As can be seen from the number of hosts shown in Figure 2 Internet access, and in 1993 the number of hosts Internet access is 1.313 million units, and an upward trend year by year, from the data is to look at as of New Year's Day 2012, access to the Internet The number of hosts has reached nearly 900 million units, an increase of about 700 times multiples.

The number of domestic mainframe computer connected to the Internet have the same trend, according to the China Internet Network Information Center (CNNIC) released data (Twenty-ninth report of China Internet network development statistics status) results are shown in TABLE 1.

TABLE 1 : domestic popularity of the Internet

Census year	Internet users (million)	Internet penetration	Percentage
June 2006	12300	0.03	9.40%
June 2006	13700	0.04	10.50%
June 2006	16200	0.04	12.30%
June 2006	21000	0.06	16.00%
June 2006	25300	0.07	19.10%
June 2006	29800	0.08	22.60%
June 2006	33800	0.09	25.50%
June 2006	38400	0.10	28.90%
June 2006	42000	0.11	31.80%
June 2006	45700	0.12	34.30%
June 2006	48500	0.13	36.20%
June 2006	51300	0.14	38.30%

(Source: Report of the twenty-ninth of Statistics China Internet Network Information Center (CNNIC) China Internet network development situation)

The data corresponding to the above "two axes - column chart, " as shown in Figure 3

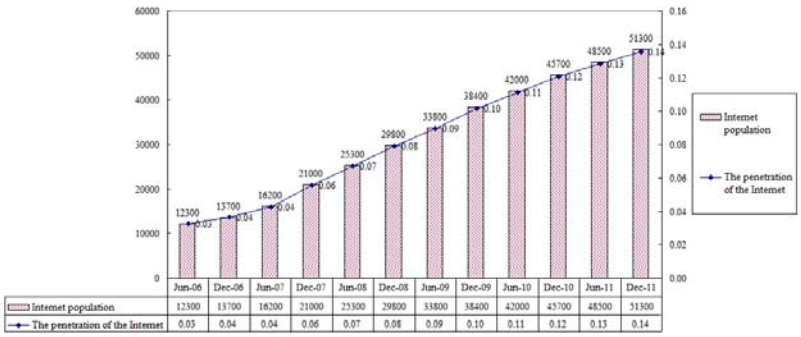

Figure 3 : The of the Internet popularity in China

As can be seen from the above analysis, the overall scale of China's Internet users are increasing year by year, until the end of 2011, the overall number of Internet users in China has reached more than 500 million, compared with the end of the previous year increased by nearly 60 million people. Internet penetration increased to 38.3% in our country by the end of 2010 compared to the increase of 4 percentage points.

Computer network security problems

The growing popularity of the Internet, a sharp increase in the number of Internet users, in order to meet the growing needs of the majority of Internet users applications, application software for computer network industry, more and more, such as various aspects of e-commerce, communications, entertainment, e-government, finance, etc. there is a computer network that figure. While computer networks function is very powerful, but these rich applications and variety of users in a variety of computer applications and operating systems in the design, development, management, there is a more or less when using defect, causing them to these applications the existence of vulnerability, with the increase in a variety of network applications, the number of vulnerabilities are constantly rising, according to the National Institute of Standards and Technology (The national institute of standards and technology; NIST) international Vulnerability Database (International vulnerability database; NVD) vulnerability data released over the years are summarized as follows Table in Figure 2.

TABLE 2 : The vulnerability of computer networks over the years the number of

Year	Number of fragility	The proportion of
1997	252	0.01
1998	246	0.01
1999	894	0.02
2000	1020	0.02
2001	1677	0.03
2002	2156	0.04
2003	1527	0.03
2004	2451	0.05
2005	4932	0.10
2006	6608	0.14
2007	6514	0.13
2008	5632	0.12
2009	5733	0.12
2010	4639	0.10
2011	4145	0.09
The total number of	48426	1.00

(Data source: U.S. National Institute of Standards and Technology (The national institute of standards and technology; NIST) international Vulnerability Database (International vulnerability database; NVD) vulnerability data released over the years)

Make "black and white histogram" According to TABLE 2 data, as shown in Figure 4.

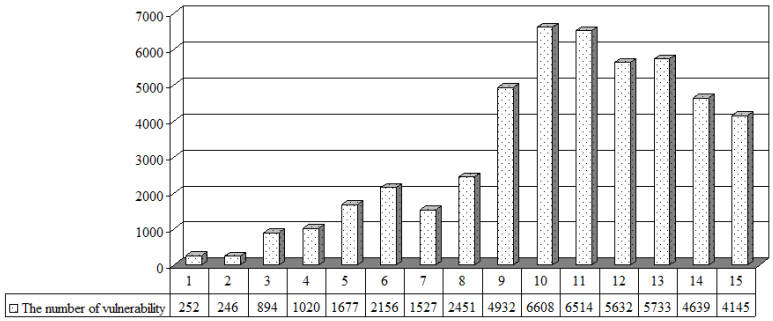

Figure 4 : The number of computer network vulnerability calendar year

The risks exist in computer network development

For the development of computer network vulnerabilities are in each year upward trend, for some virus program to target these vulnerabilities to attack aspects, there are some scholars use to attack the tree in the form of system security analysis to be intuitive. Based Attack Tree network security assessment and fault model is an extension of the way, attack the tree also provides a formal and structured way to describe v clear security threats facing computer network systems and may be subject to attack cases, it is one kind of tree structure to represent the system faces attacks. It is also a top-down structure to represent; Figure 5 is a schematic diagram of a simple attack tree.

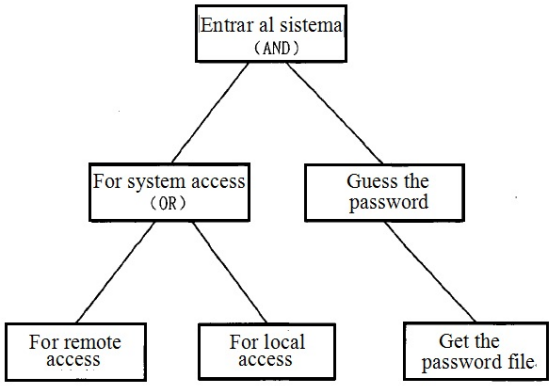

Figure 5 : Attack tree diagram

From the above analysis we can see that: Attack the root of the tree is an attacker's target, attack the tree in the middle of the leaf nodes are represented by the different ways to attack the target. The child nodes of each node are representative of a method of the multi-node.

An attack against the attack tree nodes in turn can be divided into two structures, one AND type structure (The structure of the AND type), and the other is the structure of type OR (The structure of the OR type), a schematic view thereof, two structures as shown in 6 Figure Schematic

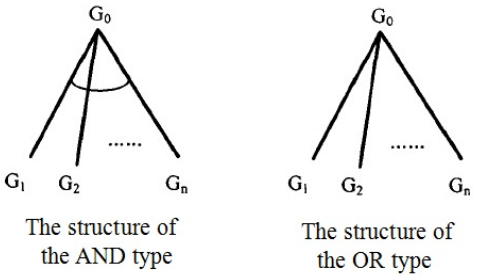

Figure 6 : Two kinds of diagram structure

In the AND type structure, each target from G_1 to G_n must be satisfied in order to achieve the attack to the target G_0, each one is indispensable. In the OR type structure, any target from to must be satisfied in order to achieve the attack to the target.

Some scholars have proposed the use of privileged diagram to describe intruder privilege escalation process. In the different process intruder attacks, the use of privileged map constructed attack state diagram, in order to describe the intruder can reach a particular target (e.g.: the host file tampering) have different paths and can be Through mathematical formula to calculate the cost of these vulnerabilities potential attackers want to take advantage of paid quantify standards, it's the process as shown in Figure 7.

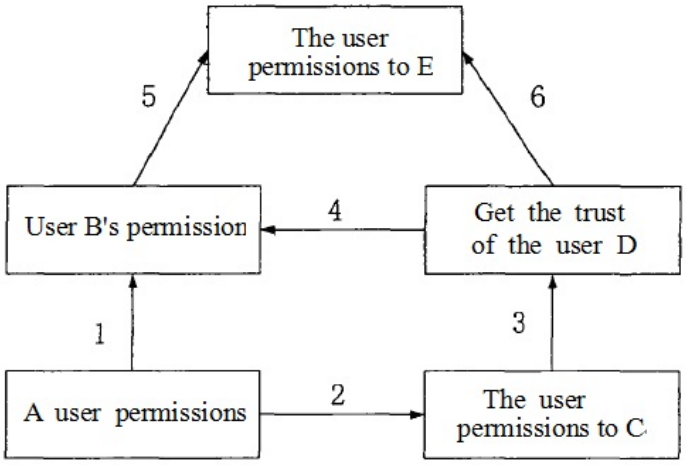

Figure 7 : The privilege of a simple graph instance

Each connected attack meaning as shown in TABLE 3.

TABLE 3 : Meaning of connections attack

Number of connections	Meaning
1	user A can become wherein a user of group B
2	user C can be A used to guess
3	rhosts files of user D can be rewritten by user C, user C can be trusted by user D
4	User B can run the program belong to the relevant user group D
5	User B can modify the tcshrc file of user E.
6	User D can modify the setuid program of user F

Establishing and solving the model

For computer network security risks exist, the first elements of the network model of information processing, its processing relationship as shown TABLE 4:

TABLE 4 : Model information network elements

Information Type	Description	Remarks
Host Information	Network hosts, servers, hardware components correspond	Including the operating system on the host, applications, services, and vulnerability information
Connectivity relations	Rules and topology of the network, access control policy, the corresponding firewall	Description of the network components between physical and logical connectivity
Trusts	Special Access network of relationships that exist between the host and the corresponding	As a special vulnerability of the network information system has
Vulnerability information	With the host operating network vulnerability and likely to cause corresponding changes in the security situation	And trust relationship model simulated attack together as transition condition
Attack information	And the attacker using a network host connectivity relationships, trust relationships No. vulnerability to complete the process corresponds to aggressive behavior	Including relevant definitions attack model, attack paths, vulnerability attack graph representation of a model, such as

Analysis based on traversal matching algorithm nodes

In the process of looking for a computer network vulnerability node, the application of this traversal algorithm matching analysis. In the Traverse the matching algorithms, V_C means the project's vulnerability to the current node; V_G means the attacker's target node ; VS means the attacker to gain system to attack targets set, It constantly attacks the tree node metastasis motivating factor.

The main idea of the of the algorithm is to facilitate the matching of nodes for each vulnerability checks performed in the order V_x.

Whether the main frame of vulnerability V_x is connected with that of the vulnerability V_C.

Whether the prerequisites of vulnerability V_x in accordance with the attack consequences of the vulnerability V_C.

If the conditions are matched attack and then communicates with the host, Then V_C is the parent phase node, and V_x is the phase of the child node.

Specific ideas for arithmetic operations:

Input:

V_C :The vulnerability of the current node

V_G :Target vulnerability node (default targets)

VS :Collection of network vulnerability

$Path(V)$:Before connecting path node V

V_host :Vulnerability V are from the host

$a(V)$:Attack using the vulnerability V

output:

V_C After adding notes:

In order to prevent the attack, we carried out in this monotony assumptions vulnerability utilization. That is based on the assumption of non-retrogression attack, the attacker the ability to attack once again will not get. So node traversal of algorithms specifically determine the third line to increase the vulnerability of the new node is in the previous section, there have been, that is to avoid an attack is to appear the same path twice vulnerability.

Protective measures of computer networks

However, between respects for strengthening management is mainly for system security vulnerabilities precautions. In building integrated security systems engineering is a strong need to go through specific research, development and design chosen to analyze the system, equipment, construction bidding, software installation, commissioning and acceptance phase to be completed to establish a computer network security protection. For the specific content of the various stages of implementation as shown in TABLE 5:

TABLE 5 : The establishment of computer network security

Complete steps	Specific content
Research phase	Relevant person in charge of network management would like to know the actual situation of a region, learn the advantages of other network under construction, is designed to correct shortcomings, serious study, combined with local reality is actually provided specifically reference
Development phase	Construction leading group set up a network, hiring related to leadership and technical staff, in conjunction with local realities, to develop the planning and implementation of specific programs.
Systems Analysis	For planning and design scheme, the relevant experts in the field technicians analyze the feasibility of capital, technology, specific implementation.
Device selected	Solutions for network planning, combined with the actual school, select the appropriate network equipment and instruments
Construction Bidding	Construction leading group of the network, designed to publicly announce the tender and contracting companies have completed their training and related technical personnel to install equipment
Software Installation	Related network software installation, installation-related network management operating system and teaching management software applications.
Commissioning and acceptance	Testing phases in the construction, commissioning and acceptance during the last full network.

CONCLUSION

For security in computer networks, there are many forms of expression, such as the individual's privacy disclosure, the database file is stolen, the computer system is damaged, these cases were to some extent, to let people suffer some losses in life bring some trouble. For some vicious damage national security networks and attacks severe cases can be hazardous, stability and economic construction and social development, on the lives of the masses caused an adverse impact.

For the development of the vulnerability of computer networks are part of the upward trend in the year, for some virus program targeting these vulnerabilities link attack. Safe operation of the computer network is directly related to information security and increasing a country's Internet users personal data and safety information, is now the most important computer development of the times, for a computer network is safe and reliable operation is directly related to a country The overall level of operation, so that the stable and secure operation of computer network center is very important.

REFERENCES

[1] Zhong Shizhi Advanced Computer Network [M] Beijing: Electronic Industry Press, 230-235 **(2002)**.
[2] Zhang Ran; The study of firewalls and intrusion detection technology [J] The study of computer applications, **18(1)**, 4-7 **(2001)**.
[3] Feng Guodeng; Computer communication and network security [M] First Edition, Beijing: Tsinghua University Press, 195-204 **(2001)**.
[4] Jiang Jianchun; Other network security intrusion detection: Research Summary [J] Journal of Software, **11(11)**, 1460-1466 **(2000)**.
[5] Duan Haixin; CERNET Analysis of campus network security issues. Countermeasures of China Education Network, **(2005)**.

[6] Jiang Dongxing; The situation and solution of countermeasures network teaching in universities [J]. Informatization, **7**, **(2007)**.
[7] Elite Technology system security and hacker prevention [J]. China Electric Power Press, **(2002)**.
[8] Li Tao; Network Security Introduction [M] Beijing: Electronic Industry Press, 3-250 **(2004)**.