Proposed Guidelines for Effective Management of Universities Network; University of Karachi – A Case Study

M. Sadiq Ali Khan*

Department of Computer Science, University of Karachi, Karachi, Pakistan

Abstract: Without networks life would be very much less convenient and many actions would be unfeasible. Network Security has become significant due to the inter-connection of nodes and the rise of the internet. This paper discusses some of the popular network security threats like spoofing; masquerade; phishing attacks; session hijacking; man-in-the-middle attack; website defacement; message confidentiality threats. This paper gives an explanation of several important security concepts and gives security policies guidelines for the educational network specifically. The network security policy is anticipated to keep the integrity of campus networks and to alleviate the risks and losses associated with security threats to campus networks and network resources. Security incidents and threats make up a risk to the University's academic mission. Failure to use due to diligence may lead to fiscal accountability for damage, done by persons accessing the campus network. This paper gives guidelines that allow the universities to manage network security effectively and identifies some key concerns and issues faced by the University community.

Key Words: Network Security, Security Threats, Intrusion Detection, Reliability, Congestion.

INTRODUCTION

Network is formed by combining two or more than two computers. When we talk about the term networking, network security should also be discussed. Many computers that are connected with insecure host create complexity among others. It can be modified by other. The original message can be changed. If there is a poor service then security on large scale can be useless. Such security can be firewall, intrusion detection and other measures in advancement of security. To protect systems from hackers is a big task from system administrators. To avoid such disaster, technology is not only the way for any removal of attacks. The system should be maintained and to have such network security, the technology must be implemented and it should be updated with the latest technology. To keep the updates, the training must be given to the administrator and he should follow all the rules and regulations. By applying such security to the system will create complexity. The data will be protected but it will be very hard to configure, maintain and manage. Only the person who will implement can handle it and for others it will be a complex situation. Every system has been created or built to utilize itself at a maximum. Firewalls and ID mechanisms are useless if your main servers offer easily compromised services. If a hacker finds any kind of loop hole in your network it will penetrate on your network and creates problems for you as an administrator and for your entire network. Security can not be achieved by simply adopting the technology and by installing new technological accessories, but its an active process that must be constantly followed and renewed. Many people believe that there is an inherent tradeoff between security and usability. We should finding a ways to maximize both the usability of a system and the security of the system has been a long standing problem.

BACKGROUND

To build any machine, it is always kept in mind that it can be handled by human. The machine is made to use at its maximum life. The programs are installed in it so that it can easily interact with the humans and also to minimize human error [1].

Passwords

Password are a mechanisms designed to authenticate a user i.e to bind the identity of the user to an entity on the computer. A password is a sequence of characters that confirm the user's identity [2]. To avoid a system from any distortion by human, a password is kept on the system. The administrator knows only the password, as he operates the system. When the password is on the system, no one can modify data on the system. The information on the system is kept secure. A password contains characters A-Z, a-z, 0-9 or special characters. It can be of any length. Software having passwords has different requirements of passwords. An attacker can attack only a system, when the password is known to him. Users set passwords that are easily memorable to them. Passwords can be easy and complex that depends on the user. Experiments shown that user able to guess user password for between 25% and 80%. The user usually use dictionary words, names, and other common words [3] [4].

*Address correspondence to this author at the Department of Computer Science, University of Karachi, Karachi, Pakistan;
E-mail: msakhan@uok.edu.pk

0250-5363/07

Patching

When the technology is applied to the system, it is needed to be updated. This concept is called patching. Patch updates the technology with its functionality to solve a problem. A patch updates the capabilities of the technology that is applied for the protection purpose. The process of patching is same to as updating the virus definitions to the antivirus. The patch is copied and then it is executed. Patching is not required as the system is protected with the software [5]. It is providing all the security requirements but as the environment changes it is necessary to keep the security up-to-date so patching is done at the minimal level [6].

Configuration

To operate a system, installation must be done without the installation it may not work correctly. Secure installation is completed by configuration and the system operates well. Configuration is the setting of the system. The process will run in such a way that the configurations are set. Different system has different configurations. All configurations are not same and all do not have the same result. Most of software provides the ability to users to write their definitions to replace the standard functions. Attackers write their own computer languages in a file that is called worms and viruses. When that file is opened, the virus attacks the system. The solution is set the configuration in such a way that a warning is displayed before every worm or virus when it is opened. e.g; Microsoft word allows the user to take appropriate actions upon opening a file. These actions are programmed using a powerful macro language. But intruders have written computer viruses and embedded them in documents. Among other actions, the virus infected a commonly used template file, so any other file referencing that template would also be infected [2]. We should have some sort of acceptable security mechanism that depends upon the context in which those mechanisms are to be used. We should have an alternate authentication mechanisms.

Evaluating Authentication Mechanisms

There are three steps of security that keeps the unauthorized people out:

Identification

It is important to identify the person who is using the system.

Authentication

It is important to give the access to the right person.

Authorization

The right person has the right to make changes in the system.

Applying the Strategies to Everyday Security Problems

Email viruses: Self- propagating email attachments have caused widespread havoc in the last few years. Some exploit software bugs in the operating system or mail program, but bugs are not the whole story. Many email viruses, such as MyDoom, Netsky and sobig, rely on humans to activate them by opening executable attachments, and would continue to spread even with bug free software. By using internet, there are several security problems using the system. A user checking the e-mail box can face several viruses while downloading their documents. They must use the e-mail scans before downloading the documents.

Other viruses and spy ware: There are certain antiviruses which indicate that sites which are infected with viruses. AVG antivirus provides such facilities. It scans the files before opening or downloading the file. It shows the warning when there is any virus [7].

Securing File Access: To perform security by designation, we would stop providing applications with all the user's authority to access the disk; applications would start with access only to their own program files and a limited snatch space. By installing antivirus on the system, everything is secure. Secure access to file is provided. Antivirus contains virus definitions that must be updated after every 15 days.

Cookie Management: Cookies are small data records that web sites ask browsers to retain and present in order to identify users when they return to the same site. When we search on internet, the whole record of our data is saved that is called cookies. It keeps the records of the pages that are visited. Cookies can be personalized with the book marks [8].

Phishing Attacks: Such websites that are designed to crack the password of any software are called phishing attacks. It is the most common method of stealing password. Some information is provided to user to protect from such attacks. A better solution is to give the user control over the name used to identify the site.In a typical so called phishing attack, a user receives an email message that appears to be from a bank, asking the user to click on a link and verify account information [9].

RELIABILITY

If a device is providing services without breakdown, it is called reliability. If there is no protection against any failure in the system, then there is a great risk. The biggest task of network is to keep working no matter how much is the load at the system. It is important to note that the network must be more reliable than any device attached to it. It is important to have the best server because it will provide the network keep working [10].

Fault tolerance is one of the important component of reliability. This means that devices can breakdown without

affecting services. In practice, we might never see any failures in our key network devices. But if there is no inherent fault tolerance to protect against such failures, then the network is taking a great risk at the business expense. Secondly the network must meet its peak load requirements sufficiently to support the business requirements. As its heaviest times, the network still has to work. So peak load performance must be included in the concept of network reliability. It is important to note that the network must be more reliable than any device attached to it. In our university network there are many servers supporting many applications. They are still connected to the user workstations by a redundant network, though if you have a backup redundant server in your environment than the failure of server will not effect. But if you have a single network and the network fails, than several servers may become inaccessible.

Mean Time between Failures

Mean time between failure is a half of all equipment of this type will no longer be functioning after this length of time. Failure can happen at any time. If the MTBF for active components is 5 yrs, then you will expect to see 2.5% of your devices fail every year, on average if the MTBF is 20 years, then the value drops to 1.25%. In our network with hundreds or thousands of devices. At 2.5% per year, out of a network of 1440 devices, you will expect to see 36 failures per year. This implies, the more devices you have, the greater the chances are that one of them will fail. So, the more single points of failure in the network, the greater the probability of a catastrophic failure, so we have redundancy in our network model.

Multiple Simultaneous Failures

MTBF gives a probability of failures per unit time. To find the probability for simultaneous failures, you need a way of combining these probabilities. If the MTBF per day value by the letter M so the probability of one particular device failing in a given day is P= 1/2M.

$$kP_n = n!.\ (2m-1)^{n-k} / k!(n-k)!.(2m),$$ where m = M/ 1 day.

This implies in a network of n devices, each with an MTBF value of M, there will be k failures in one day. But for a network in our university of about 2000 nodes, MTBF is very low. In our network most of the problems that occurs were of TCP/IP configurations like IP not works, subnet mask errors and gateway addresses problems. As per statistics daily 5 complains received of about virus, IP's and connector problems, any device failure problem noticed on average once in a year and ratio of problem related to passive equipments is two or three times in a year. Some problem may occur in a data centre due to the malfunctioning of SDH module but its very few may be once in a year. Frequently internet bandwidth problems noticed but that is from the HEC part, may be a delay in the data transmission, rate of downloading files from the internet etc. Generally we want to work out these probabilities for our whole network. You should plan your network for a level of redundancy that the organization can handle.

Congestion

In most cases congestion problems occurs in a network. In dealing with congestion, it is important to understand your traffic flows. In our network traffic flows through the core VLANS, we have about 60 VLANS in our campus network. We divided each department in separate VLANs in order to achieve the maximum security and administration benefits. We divided each department in a 10../16 networks. We have core switch of 6506 catalyst, 3845 series router, about 8 distribution switches of 3550 series and about 40 2950 series with fiber port and rest of 20 without fiber port. Congestion is what happens when traffic hits a bottleneck in the network. Before dropping the packets, most network equipment will attempt to buffer them, in our network devices have good buffering capacity.

OBSERVATIONS

In a multivendor environment MTBF values for every components of a particular device differs accordingly. In such situations we have to combine different MTBF values to find the suitable number for our network. As we can see with a simple example below in Table which shows typical component MTBF values

Component	Hours
Chassis	3,000,000
Power Supply	150,000
Processor	200,000
Network Card	100,000

The percentage of chassis fails is very rare and if it happens its due to swapping card aggressively or due to heating problem at the back plane. Network card's problem however are frequently occurs and they are less reliable specially in a campus networks. See below the Table for failure probabilities of typical components.

Component	Probability
Chassis	0.0004%
Power Supply	0.0080%
Processor	0.0060%
Network Card	0.0120%

If we have a redundant solution having backup devices so therefore if one fails the other will take over for it. First of all these MTBF values have to be converted to probabilities of

failure per day. Any of the remaining components fail independently and count as a device failure, so we can just add these probabilities to get the net probability.

The trouble with this is that it completely neglects the fact that there are several elements here, any of which can fail. The more components we have in our network, the more likely something will fail. Many hardware vendors offer the capability of redundant processor modules. So, duplicating the processor module has improved the net MTBF for the device.

DISCUSSION & CONCLUSIONS

Attacks and security incidents make up a risk to the University's academic mission. The loss of data or unauthorized disclosure of information on research, student records, and financial systems could greatly hinder the lawful activities of University staff, faculty and students. Failure to implement due diligence may lead to financial liability for damage done by persons accessing the network from or through the University. Within this Policy, information technology resources include information assets, software assets and physical assets. The information security policy includes access management, Identification, Authorization, Authentication, Account Management, Student Accounts and Privileged Users Access. Main Communication Network, University of Karachi, MCN System Administrator must regularly review their schedule of delegated authority, to determine who is authorized to use the system and their level of authorization. Only those users who have valid for accessing the University's systems. All network users are assigned a unique ID to use in accessing the University's systems and applications. All users of the University network resources must be authorized to access the appropriate systems and their resources. In our university network student's accounts are generated automatically when a student is enrolled and MCN department get the list of enrolled students from the admission/enrollment section.

MCN computing resources are shared by all network users on a fair and equitable basis. It is the responsibility of network staff not only to provide these computing resources, but to ensure that the rights of users are not infringed upon by the abuse of another. Therefore, administrator utilizes every means available to detect, restrict and/or take legal action against individuals responsible for the abuse of computing resources. This serves to provide specific examples of the types of abuse not tolerated.

REFERENCES

[1] Shuo Yang & et al., (2006), "A Fair, Secure and Trustworthy Peer-to-Peer Based Cycle-Sharing System", J Grid Computing 4: 265–286, Springer.

[2] Matt Bishop, (2003), "Computer Security: Art and Science", Reading, MA: Addison Wesley Professional.

[3] Robbert Moris & Ken Thompson, "Password Security: A Case History", Communications ACM 22:11.

[4] Angelo Ciaramella & et al., (2006), "Neural Network Techniques for Proactive Password Checking", IEEE Transactions on Dependable and Secure Computing, Issue: 4, pp. 327 – 339.

[5] Robert Ball & et al., (2004), "Home-Centric Visualization of Network Traffic for Security Administration", VizSEC/DMSEC'04, ACM 1-58113-974-8/04/0010.

[6] Peter Mell & Miles C. Tracy, (2002), "Procedures for Handling Security Patches", NIST Special Publication 800-40.

[7] Petr Aubrecht & Petr Miksovsky, (2003), "Sumatra TT: a Generic Data Pre-processing System", Proc. of the 14th International workshop on Database and Expert Systems Applications (DEXA-2003), 1529-4 188/03 IEEE.

[8] R. Baumgartner & G. Ledermiiller, (2005), "DeepWeb Navigation in Web Data Extraction", Computational Intelligence for Modelling, Control and Automation & International Conference on Intelligent Agents, Web Technologies and Internet Commerce, Vol 2, pp. 698 - 703.

[9] Tadeusz Pietraszek & Chris Vanden Berghe, (2006), "Defending Against Injection attacks Through Context-Sensitive String Evaluation", LNCS 3858, pp. 124-145, Springer-Verlag Berlin Heidelberg.

[10] S. M. Aqil Burney & M. Sadiq Ali Khan, (2005), "Algorithms for Data Security in Wireless Networks", Karachi University Journal of Science Vol 33 (1 & 2), pp. 53-56.