ISSN 2278-7763

Insight on Protection of Universities Networks Information Security: The Problems and the Solutions

Ahmed Dheyaa Basha[1*], Satar Habib Mnaathr[2], Irfan Naufal Umar[3], Rozinah Jamaludin[4]

[1]Center for Instructional Technology and Multimedia (CITM), Universiti Sains Malaysia, Penang, 11800
ahmed2009shh@yahoo.com

Abstract

In the current age of information and progress technology, network education has been boosted and leap toward develop m casionally especially in its applications of IT and ICT technology as well as enhancing and increasing the talents in le learning and training , which makes learning in education more of privatization and of opening up. In order to better enable learners to go beyond the constraints of space and time to attain the knowledge; to provide an effective learning environment for greater freedom and greater multi choice of learning activity space, the project to build university network high security become the basis of all university building work. The university network has a number of tasks such as teaching, learning, training, research, management, and communication with each other and outside of universities. Therefore, the related issue of network security has become a priority to each university network administration. Unquestionably and obviously, the current internet is very convenient, but at the same time it is unsafe. As part of the internet and unparalleled attributes of university network, it is liable to more easily attacked when exploring and enjoying the service provided by the internet. This study begins from the current security status of the university network, threatens to analyzing university network security and strategies to continue maintenance of network security systems. In addition to establish a suitable university network security system, to explain and introduce and highlight on some current public problems and university network information security solutions.

Keywords: Universities networks; Security technology,; Firewall, the Solutions,; the problems.

1 INTRODACTION

In the current era and with continuing the development of society, network information became indispensable and used by learners more and more and its importance is becoming notable and occupied different sectors undisputed especially in education sector , the networks has also the most critical thing of interesting about country 'political, economic, education, and military resources. Currently there are a lot of network applications which are not secure; it's mainly in information tampering and leakage, weakness and illegal use of network resources, illegal information breaching by penetration via network, scam, fake etc... . As the dissemination of several computer network security hazards, then attempting to prevent "hackers, spies" is weak and corporate and government web sites still have been "attacked" increasingly and frequently, these have caused many economic losses. Therefore, the network information system security and hindering and its secrecy seems urgent request and important upwardly. With the rapid extension of the universities networks through connectivity and collaboration, the network applications have increased rapidly, moreover and the same time, the university network information security has caused more interesting and attention today. In the current network and broad application systems, there are often no security norms has been taken, and of application system are also without any plans for processing, meanwhile there are a lot of problems within system management, all of these addressed and formed a main serious security problem, as with serious and ongoing threatening the safety of the universities network. Of later networks monitoring systems and the hosts were found to attempt to be overrun by others, a big number of security weaknesses exist in the system, and also there are a lot of security vulnerabilities which are very difficult to avoid and eradicate; Also, many of a virus transmitted via the network badly affected the ordinary running of the university network [1].

2 WIDESPREAD PROBLEMS IN UNIVERSITIES NETWORK

Usually faculty and University are provided with a computer laboratory; there are a number of computers which can direct access to the university computer network in this laboratory, learners and the college are usually allowed and available to use these computers to connect to the internet to get information and learn through online. In this respect, the lack of united management software and system for observation and logging, these computer laboratories can't be major in the management case. Moreover, most laboratories have serious defects in registration and management system, in this case the internet user's identity very difficult to be recognized.

Security weaknesses in the host operating system and majority

ISSN 2278-7763

Meanwhile, it's very convenient for us to use multi functions provided by the university network, but it in the same way has become very a quick way to transfer a lot of the virus. Network virus flows can lead incredible and directly to the user's privacy and very important data leaks. Arrant the network virus is a great consuming of network resources, the situation resulting in a shape incline and impairment in network performance even can hardly bring down the network performance [2].

As with the university network, attacks, intervention the machines, attempts to theft of another account, keep on the illegal use of the network, intrusion via illegal access to forbidden files, practice harassment through mail and other events often occur, and so on, referring into the users' safety awareness in the university network are so unimpressive. The majority of serious main problems which facing college or campus are the acute shortage of funds for the network construction and infrastructure; therefore limited funds which often mainly invest in network devices, organized input for construction and constitute management of network security has not been bearing in mind seriously. Because of lack of the consciousness in core universities, management institutions are inadequate, administration system is incomplete, management technology is more often not advance ; these factors which mentioned make the university's network management center can't take any norm and precautionary measure for information security. In addition, Countries do not have well-sophisticated and strict network security system, There are no rigorous applications of standards for the university network security management; this is a key element and an important reason for the augmentation of network security figure 1 is showing the public types of network security threats.

As we mentioned the analysis above, the university network security issues are classified mainly in the following areas: password detection resulted in data loss. Diversity of database systems in implementing online in a university network, such as teaching management system, learner's achievements management system, university card management system, test bank system and so on. In addition the user personal' role in using and lack experience and indifference for many users in pertaining safety measures can lead to these database passwords be lost, the using of data may be illegally removed or cloned, which led to reveal of information, in actual circumstance and serious, this situation may result in serious problems and illegal case this has caused in deletion of data. Therefore, private setting related password is secure and very important [3].

University networks start connecting with the internet with routers; and internet users usually can interest and enjoy by suitable way of very fast with diverse and unlimited resources for this platform in one hand, but also have to face the hazard of an attack in other hands. There is security hazards must take into account within university network, unquestionable internal users are relatively understood well about the using and network structure as well as the applications of models than the external users, therefore, the threats to internal security consider the main threats and real risk. In current time, hacking tools and spy flooded in the internet, hackers use and focus on network protocols, server and breaching the operating system security weaknesses and observation management to breaking into the network by illegally way to access to network resources to deleting of data and damage the system, these attacks usually have caused destructive effects of the university network of mislead and defamation of college.

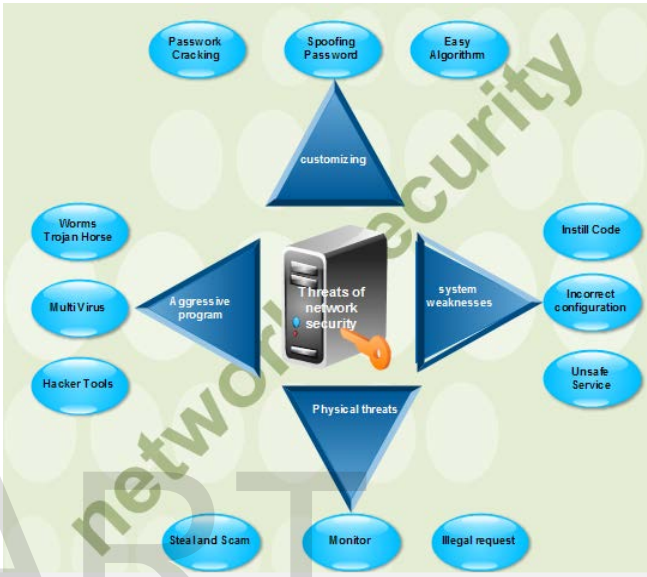

Figure 1. Public types of network security threats

There are many security weaknesses within advancing and genuine operating system, these security weaknesses mannerism a lot of serious threats such as the information security, using of the system without protections, operations of the network, and weaknesses of algorithm and so on. Therefore to the lack of consciousness of copyright, exists of piracy soft ware, dissemination films and television resources is also used in general in the university network, as well as the spread of the different software taken up many network bandwidth; on the other hand it helps to brings a lot of network security hazards and threats .For instance Microsoft's XP operating systems corporation has some constraints in updating the new software; if the users wanted to install Microsoft's XP operating system with forger one, in this case the computer system will left a big number of security weaknesses[4].

On the other hand, frequent of downloading from the internet software which may contain many viruses hidden like Trojans horse virus, backdoors and other some malicious code, because a lot of systems have invaded and used already by which the attackers .The applications in the field of computer have gradually broadened at the university, also access points to the university network have boosted largely, but the majority of these nodes is the new and some of precautionary measures have not been adopted or improving. This case may

ISSN 2278-7763

allow the virus flooding frequently at any time, and cause information loss, destroy or corruption of data, network attacks , eventually lead to system collapse and subsequently to serious consequences [9].

A lot of the spies and hackers start their attack by distributing their messages and send spam for purpose dissemination harmful information using to disinformation and not managed university server as a crossing station, this situation has brought a serious threat and influence and affect to the network and brought the disastrous influence on the college's reputation. In outline, the security case of the university network is very necessary, in order to solve these security hazards and weaknesses, according to many of the structural features of the university network and many security issues which the university network faced, security solves should be taken into account the university network and it should be also implemented as soon as possible to protect university network.

4 THE SOLUTIONS FOR PROTECTION OF UNIVERSITY NETWORK INFORMATION SECURITY

For the university network, at first, we should highlight on vulnerabilities and have integrated plan and take deep consideration based on security hazard analysis of the university network. Secondly in addition to plan , we should effectively adopt diverse advanced technologies such as adapting virtual exchange network (VLAN) is a technique in computer networking contains many switch ports that are be restricted which called "private port" , different encryption technology, virtual private network (VPN) is technology which connection via internet is technically (WAN) link between the sites to enables a host computer to send and receive data through shared or public network,PKI technology, firewall technology, and contributes in a achieve centralized configuration, observation , management, eventually, we also should strengthen relevance for formulating of system and enhancing specifications about the network security secrecy for information, and accurately implement it. In this respect ensuring the physical security of suitable and diverse equipments for this purpose of computer information system is consider corner stone and premise to adopt and protect the security of the whole network system. It includes three aspects mainly: preparedness to environmental safety, provision of equipment safety, ensuring lines security. Preparedness environmental safety more often includes the security protection to the available system environment, the instance the sectional protection and calamity protection [5]. While provision equipment safety includes of anti- theft of different devices, anti- break and crash, anti or prevent -electromagnetic caused information radiation leak, to abolish any delay or stopping, as well as prevent – electromagnetic intervention and prevision protection for power supply. Usually university generally includes of two parts. First part of the internal network consisting LAN, LAN for office automation, library LAN, etc.; the second part is external network, including many of public servers. From point of view a network security, they represent different domains of network security, so the internet firewall in this case should be installed at the border, meanwhile the security policy control should be corresponding and taken into account the implementation as a condition. To provide protection for the internal network, it is very important regarding main switcher on the main segment must provided with the plumb-line which has the task of snooping detection system, snooping detection system is very important to provide protection for network access control [7,13].

While the operation system (OS) considers is a basis for workstations, all computer terminals, servers to implement correctly, also operating system security is most important. In this respect the server version is one of the real operating systems should be contribute and used in the critical servers and workstations which include (proxy server, database server, email server, backup server, www server and network management stations, etc.).In addition into the advantage of operating system there are a lot of security weaknesses in operating system, because of the problems of design version; the incorrect use of security setting will also boost the security weaknesses, consider cause a security hazard. In case of absence of higher security level commercial OS of choice, OS security management and sophistication of improving security measures is the key elements, Moreover, OS's security problems has come from multi of virus threats and spies, hackers or attackers penetrated the network to damage the data .However network many anti-virus tools must be shielded able to protect and prevent all various virus entry from the internet. Whereas all anti-virus programs should be installed from many online virus programs revealed the virus cleanup or chase [6, 11].

The main aim of attacks by hackers is to grab on data and update the system illegally. Risk evaluation tools for system must be used to help system in dedicate administrators identify, also the user privileges command must be installed or reduce. Moreover, real time snooping detection system can follow trace of the user's activity, testing of overrun, also can control and prevent internal employers from to destruct intranet. Once the violations detected, the system will promptly notify the administrator, then the administrator can register the corresponding test results data to track the stranger, to dedicate whether it endanger and threats the safety of the system and installation and take effective precautionary measure to insure the system's important information and important data from damage. Students in their computer laboratory are connected with the university network for different purposes bearing mind the needs of students will inevitably use many of USB the storage device on the equipments in the computer laboratory, and more often download a lot of software from internet on these devices, which causes a hidden danger of the spread of the various viruses [10]. Therefore, to attain overall university network anti-virus, unified solutions must taken by using instance a strong server antivirus, stand alone antivirus and gateway antivirus to avoid any attack [8] .Over setting for allowing and password of the

ISSN 2278-7763

network resources for students and users, network manager can control and save the user name and password, transfer and equips an integral student record in encrypted manner and the suitable analysis way can insure the system security. Managers of the network also need some procedures to establish and maintain an integral database of network users, rigorous administration of the system log is also will be inevitable. To evaluate and review the security solving organized on the university network system, focus on to the dynamic network security anxiety and update the pertinent security settings for hindering snooping, emergency repair system.

Suitable control strategy CS can be used to investigate the security of the university network, like applying access control (AC) policy, Operation AC, guide security CS, network observation and lock control. As well as, there is some information encryption strategy. Applying suitable encryption algorithms to encrypt critical information, you can block illegal persons illegally to steal any information. There is a lot of encryption software which can encrypt any message; files et al. Applying encryption software can influentially protect data, password, files, and control the data transfer safely via the network. In addition you can also apply backup and imaging technology to improving the safety of the university network. Moreover backup technology is the best common measures to enhance data safety; the way is to protect the information in another location to make a backup as a precautionary measure, when information is lost, we can retrieve the data from a backup of the original information.

During embarking on in construction the university network, network security needs plan of a united security system has high specifications that must joint with the real case in university network, in addition into united security system specifications must performed fist before any implementations of many network techniques integral and safety, the construction of the security planning system is urgent request, today specialists must lead the construction plan of the security system completed in the security applications process with the relevant company of other departments; in addition they must lead the all departments to constantly enhance the system security level. To attain high security of the university network information system, in spite of technical norms and ways is very important; we should be link importance to the construction and enhancing of the administration system [15]. The university network security weaknesses are clear, as well as to design the network to boost operations for the security services , enhance system security norms, we should make large efforts to strengthen the relevance with the network security administration , evolve a safety administration system and implement a suitable safety administration principles, data network security is a very organized work, just once the network security administration and the network security technology are managed together, then they can build a universal information network security system INSS [14,12].

5 CONCLUSION

Like many universities and faculties construct their own university network, and the implementations of the university networks becomes an information security increasingly as an urgent request and inevitable factor to ensure the network implementations smoothly and integral in its functions. Provision a very well informed educational environment is the robust backup of paradigm education jobs and disseminates the suitable information technique education and university network is the hardware insuring of the environment. The aim is to how to make the university network applications with high quality and qualifications is the key issue. The paper introduces and analyzes many factors and possible factors which threat the security of university networks to be avoided with suitable solutions for high protection, and gives many advices and a lot of ways on how to set up the systems of university networks from the administration and techniques.

REFERENCES

[1] Bishop, M. (2003). What is computer security? Security & Privacy, IEEE, 1(1), 67-69.

[2] Brownlie, M., Hillier, S., & Van Oorschot, P. C. (2001). U.S. Patent No. 6,202,157.

[3] Washington, DC: U.S. Patent and Trademark Office.

[4] Burns, J., Cheng, A., Gurung, P., Rajagopalan, S., Rao, P., Rosenbluth, D., & Martin Jr, D.

[5] M. (2001). Automatic management of network security policy. In DARPA Information
Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings (Vol. 2, pp. 12- 26). IEEE.

[6] Chen, J., Wang, Y., & Wang, X. (2012). On-demand security architecture for cloud computing. Computer, 45 (7), 73-78.

[7] Cuppens, F., Cuppens-Boulahia, N., Sans, T., & Miege, A. (2005). A formal approach to specify and deploy a network security policy. In Formal As pects in Security and Trust (pp. 203-218). Springer US.

[8] Hsiao, W. H., Su, H. K., Wei, Y. S., Ho, W. S., & Chen, K. J. (2012). A Study of SLA-Based Defense Resource Management Strategy in Network Security De fense System. In Network and Parallel Computing (pp. 336-348). Springer Berlin Heidelberg.

[9] Irvine, C. E. (2012). A note on mapping user-oriented security policies to com plex mechanisms and services.

[10] Kaeo, M. (1999). Designing network security. Cisco Press.

[11] Keromytis, A. D., & Wright, J. L. (2000, June). Transparent network security policy enforcement. In Proceedings of the Annual USENIX Technical Conference (pp. 215-226).

[12] Liu, S., & Fang, Y. (2012, August). Application research in computer network security evaluation based on genetic algorithm. In Instrumentation & Measurement, Sensor Network and Automation (IMSNA), 2012 International Symposium on (Vol. 2, pp. 468-470). IEEE.

[13] Viduto, V., Maple, C., Huang, W., & Lopez Perez, D. (2012). A novel risk assessment and optimization model for a multi-objective network security countermeasure selection problem. Decision Support Systems.

[14] William, S. (2006). Cryptography and Network Security, 4/E. Pearson Educa tion India.

[15] Williams, B. L. (2013). Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2. 0, and AUP V5. 0. Auerbach Pub.
You, Y. (2012). Network Security Policy Study in the New Era.

