Strategy of Campus WLAN Network Security Based on University Management & Auditing.

Nethun Kawitha Madanayake, Sri Lanka Institute of Information Technology Department of Information Technology, Information Technology, IT18107692

Abstract --- In the study and management of school`s everyday activities, the campus network is critical with the growing growth and popularity of the campus network security concerns have grown more significant. How to make the campus network secure and efficient, while giving full play to its teaching, Administration, and services roles, has become a problem that cannot be overlooked. Because of the study of the features and frequent risk to campus network security management, network security techniques such as firewalls VLan and others were used to create a set of security policies for the campus network characteristics. Network security and services have never been more important in higher education institutions than they are now. users and organizations are requesting an increasing number of networks services as well as the flow of potentially sensitive data inside these services. To begin with, there is a clear demand for network connectivity on campus. The project to construct a campus network has become the foundation of all university construction work to enable learners to gain information beyond the restrictions of place and time in order to create an outstanding learning environment for more flexibility and greater choice of learning activities space, the project to establish a campus network has become the basis of all university building work. Auditing information system security is tough, but it is becoming increasingly important to assure business day to day operations as well as stimulate competitiveness and develop new business prospects. it is presented and explored a conceptual security framework for managing and auditing information system security the suggested framework is based on a conceptual mode approach, which is based on the ISO/IEC JCT1 standards and is intended to help enterprise better manage their information system security.

Keywords – Campus network security threats strategy, Campus network, Network security, Security technology, security threat, Firewalls, security audit management,

I. INTRODUCTION

The campus network combines teaching, Research, Administrative, and general management tasks into a single network with an inbuilt waiyin function to satisfy a variety of needs such as internet access, remote education, electronic bulletin boards ,video conferencing , and off – campus data communications services .with the fast growth and wider us of computer technology ,network technology and campus network technology in the school teaching and administration , the campus network is set to replace traditional teaching and management models for instructors and students work , study , and living . Security challenges, on the other hand ,a re becoming increasingly prominent computer viruses, Hacker assaults ,data manipulation and network security threats posed a serous danger to university network . once these security concerns are breached, they will have a significant negative impact and may result in major repercussions. As a result the core design of campus network to operate correctly by understanding and analyzing security threats and implementing the appropriate strategy to counter the threat.

Established security standard ISO / IEC_JTCI1[1]

The following is how the paper is organized the suggested conceptual model , which contains the semantic ideas defined in the information security domain , and their relationships , hierarchically organized in an ontology ,will be described in section ii; section iii will offer the suggested conceptual model , which contains the semantic concepts described in the information security domain , and their relationships , hierarchically constructed in technology; the suggested frame work for managing and auditing information system security is presented which is based on technology structure . the section concludes with recommendations for further work.

II. The Campus Network Security Threats & problems

The reasons for the campus network and other networks posing a danger to the campus network `s safety and the presence of security threats are not the same when compared to their own features. Because of the unique nature of the campus network, college network security vulnerabilities are primarily caused by internal and external factors. Many internal resources are available to a firm user. There may be no way to get beyond firewalls or other security measures the prohibit untrusted sources, such as internet users, from gaining access to the internal network. Internal users with hacking expertise may be able to effectively infiltrate and get remote administrative network rights. in reality, a large percentage of network rights. In reality a large percentage of network threats begin inside the firewall. Poor network security implies theta if an external hacker gains access to a machine on the network, they will have a much easier time accessing the remainder of the internal network. This would allow the attacker to access and perhaps leak secret emails and documents as well as trash machines, resulting in data loss. the network at the university must be kept safe. Protection of critical data files, host machines and the network itself are all security problems. it's a never - ending process to keep track of virus's infections, hacked machines and collaborate with other sites to identify problem. when a problem arises, the most common solution is to isolate the offending computer from the rest of the university network by shutting its network port. During viral epidemics, the happens on the regular basis and often may times a day. Clearly a single – port strategy reduces service disruption in the event of a security breach with network authentication, it will be possible to call the computer`s owner to notify him or her that the device has been quarantined, saving the user time and confusion. The network on campus is in a critical state of security. the college network on campus is in a critical state of security. the college network has attracted a swarm of hackers. this is due to the fact that viruses and hacking tools are on the rise, and most users are unconcerned about security. Furthermore, college students are vicious and eager to learn about new things.

They are intelligent and passionate, yet they are not responsible for the consequences of their actions. Internal network assaults are the source of malicious assaults on the university network. The wireless link makes the network more vulnerable to assaults ranging from passive eavesdropping to aggressive interface. Because wireless networks send data viva electromagnetic waves in the air, all wireless networks within the transmitters service area are connected.

These data are accessible to network users on campus as long as the message is received on the same frequency by the same receiver. The danger that can be experienced in the campus WLAN is mostly in the following Ares; information disclosure, integrity destruction, denial of service, and unauthorized usage. Because network traffic is typically sent in an unencrypted manner. Attackers may simply monitor and decrypt wireless network communication packets. Intruders do not need to physically access the network to capture eavesdropping or analytical devices hence the danger has become one of the most serous issues with wireless local area network.

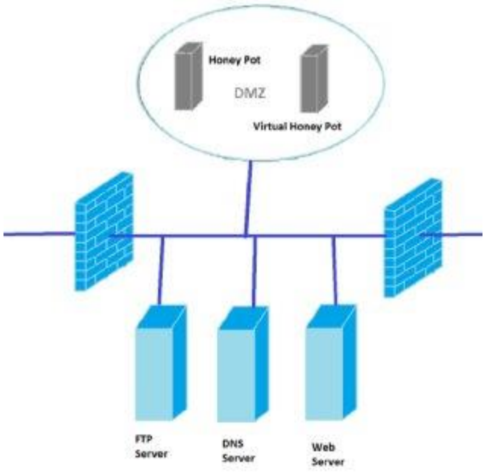

Figure. 01 Security problems in campus network

III. Campus Network defects and physical security threats

There are various security hazards in addition to the attacks from inside and outside the system, the campus network; Vulnerabilities in the system this is one of the causes behind the campus network`s flaws. Because of the large amount of operating system code, there are serval security flaws, some of the most commonly used operating systems, such as Windows 2000/ xp security flaws, plus the systems and their own security measures do not know enough , inappropriate setup , resulting in a security risk .

Threats to physical security the networks `s surrounding environment and physical qualities of network equipment and writing are unavailable, for example , if a device is stolen, damaged or if a connection ages , leading in information leakage due to electron irradiation equipment unforeseen failures , power outages , or natural catastrophes. Physical issues such as the annihilation of toxic gases , for example will also pose a threat to the campus network `s proper function .

IV. *Campus Network Security Building Strategy*

The existence of security risks assault will have unanticipated consequences. And network or to prepare for a faculty network at any moment may be vulnerable to threats, the existence of security risks attack will have unanticipated consequences, a significant case of system crashes, and network paralysis. As a result , it is critical to adopt appropriate steps to protect network security. To maintain the safety of the campus network, you must invest in internal staff management education and technological fortification, depending on the features of the campus network.

V. *The proper use of the password the encryption means.*

Make a password for yourself to make frequent changes to the system administrator account and establish random password, ensure that the password is long enough and has anti-cracking capabilities so that the attacker finds it difficult to identify the account number and password and uses a software application to crack the code. the password you create should be complicated, using letters, numbers and special characters and it should not leave a trace on the computer you may also create a “Administrator” trap account that has no right and has a super difficult password, as a result even if the password is cracked, the attacker has nothing to work with.

The encryption and decryption algorithms Amy be reloaded by users to create their own encryption and decryption modules, you may also use the “encrypt files and folders” Functionality to prevent people from looking at your computer.

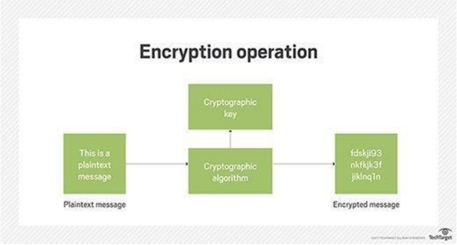

Figure .02 Encryption operation

VI. The use of anti-virus techniques adheres to the preventive detection.

Strengthen management because of its ideological significance. Any data copied from an external Hard disk to the machine should be saved on Hard disk. For virus scanning, if the virus has to be removed so your computer does not get infected again in addition because latent viruses can hide old viruses they can attack when the time comes so we should always check the disk if a virus is discovered. Rising, Jiangmin.jinshan , and international Norton, Mcafee, and Trend are the most widely used anti-viruses software, though they are most costly than domestic versions.

VII. Proposed Security Framework To Manage and Audit Information System Security

The introduction of ISO/IEC JTC1 standards paved the way for the standardization of information security semantic concepts. the right understanding and identification of those ideas are the most information system `s security semantic concepts. the right understanding and identification of those ideas are most important factors to consider when conducting a good evaluation of an information system `s security efficacy.as well as when identifying and characterizing a security event and estimating its consequences. The suggested conceptual framework aims to assist the organization in determining what should be safeguarded (assets) and what weaknesses (Vulnerabilities) should be safeguarded (vulnerabilities) in their everyday activities. Second, determine the vulnerabilities that may be exploited by an attack, as well as the risks that may materialize as a result of an assault. Finally, assess the efficiency and effectiveness of the policies and controls in place to see if they are being applied appropriately or if they need to be tweaked depicts the suggested conceptual framework, which includes three nuclear concepts: assault, threat, and assets. The auditor might choose the idea from which to begin the auditing process and then proceed to the guided audit. Each concept has a list of elements that are related to other ideas, in accordance with the ontology's hierarchical structure for semantic ideas. Due to the nature of the audit activity that the auditor plans to execute, these three ideas were put at the front-end of the framework rather than the others. A security audit is often performed after an event (reactive followed by a corrective audit), or after an asset has been hacked. In this scenario, an audit is required to discover the source of the assault and how the event occurred, as well as to implement appropriate corrective measures. A security audit, on the other hand, is not only about detecting security breaches; it's also about mitigating known dangers to ensure: (1) security compliance; (2) the security of important assets; and (3) the proper controls are in the appropriate places. In this last approach, a security audit is conducted as part of the security risk management process with the goal of developing or evaluating a security policy. The suggested framework, which is guided by the major ideas and their relationships as specified by an ontology, aims to help businesses understand, prepare, and conduct security audits on their own. This framework imposes policies and policies to aid businesses in maintaining continuously high levels of usable and excellent quality information concerning their information security systems, rather than focusing just on technological controls related to information security. Each notion in the ontology is linked to a real-world subject. A malicious code assault, for example, is related to the impacted assets, the vulnerability it exploits, and the compromised security properties.

VIII. Proposed *Solution For Campus Network Information Security Problem*

To create a more secure campus network, we must first assess security risks and then develop a coordinated action plan based on those findings. We should use more modern technology in our networks, such as firewalls, virtual Local Area Networks (VLANs), encryption, and Virtual Private Networks (VPNs).

Issue 100 of the International Journal of Advanced Engineering and Application was published in January 2011. VPN (Virtual Private Network), numerous operating systems on the server, and so on We can employ virtual private network (VPN) technology on the campus network, which employs special software (i.e. VPN client) on each computer to encrypt network traffic from that machine to a VPN concentrator on the institution's network. We don't utilize VPN in school very much because the functionality that VPN provides is already available on campus. On the other hand, on a wireless network, it would be more theft and abuse resistant. It can also be used to connect to a virtual private network (VPN). Members of the university computer network can connect safely via VPN. WLAN (Wireless Local Area Network) technology has played a key part in the advancement of campus information technology and is an important component of the campus network. The effort of network cabling is reduced by using WLAN. It becomes incredibly straightforward for users to access the network from any point on campus once it is done. Using PKI technology, centralized configuration, monitoring, and administration may be achieved. Finally, we should improve the formulation of network security systems and standards. If a user, user group, or department wishes to create their local area network or link to external data communications networks, they must choose a member of their group or department to cooperate with Network Services and gain clearance. Within the campus network, colleges and administrative entities can form subdomains. Multiple departments with a requirement to communicate information are frequently divided into subdomains. If a security problem is found, the system should automatically warn the user, and the user should be isolated to the recovery area or data flows should be blocked based on the user ID. Computer viruses and worms are the most prevalent security issues on campus networks, and these viruses are built to exploit security processes on any operating system. Viruses are developed for certain operating systems and can only execute on that particular operating system (For example Linux-Unix, Microsoft Window, MAC OS etc.) check by the week lastly any operating system Available, If there re any update immediately stop all the other works and take update. If any pc has trouble indicate make the pc recovery point after that start to troubleshoot its good practices.

As a result, rather than enforcing the security strength of single local points, security measures in some crucial areas such as outlets should be extended across the entire network to make a huge leap beyond equipment level security.

IX. Conclusions

Campus Network Security is a systems engineering problem that requires careful consideration of the systems `s security needs targeted internal education and management, cryptography, virus prevention, detection, system bug fixes, firewall technology , physical security awareness , and security technology advances , the tools and procedures for maintaining campus network will also play a more important role in schools .

X. References

[1 Saadat M. Network Security Principles and Practices (CCIE Professional Development) (CCIE Professional Development) (Hardcover) [M].Cisco Press, 2007: 52-78.]

[2 William S. Network Security Essentials: Applications and Standards (3rd Edition) (Paperback) [M]. Oxford:Blackwell business, 2006: 15- 47]

[3] Wang Zhixian. Computer virus and its prevention in the modern network environment. "Computer network" 2005.3,4.

[4] Sun Ao, Huang Yan, Wu Ping. MVC mode. NET Framework and Implementation. Technology Square, 2006 (1): 69 - 71.

[5] Da Veiga, A. and Eloff, J.H.P, An information security governance framework. Information Systems Management 24, 361-372, 2007.

[6] [ISO/IEC FDIS 27000 Information technology Security techniques Information security management systems Overview and vocabulary, ISO copyright office. Geneva, Switzerland (2009).

[7] Onwubiko, C., 2009. A Security Audit Framework for Security Management in the Enterprise. In Global Security, Safety, and Sustainability. In 5th International Conference, ICGS3 2009, London, UK, September 1-2, 2009.