Network Usage Security Policies for Academic Institutions

S.M.Aqil Burney
Meritorious Prof Dept of Computer Science
University of Karachi

M.Sadiq Ali Khan
Asst Prof. Dept of Computer Science
University of Karachi

ABSTRACT
In any universities operation its managerial administration play an important characteristics. Universities have their Management Based System (MBS) but most of them are vulnerable to malicious activities such as virus attacks, spoofing attacks, and unauthorized access from outside network. We have to build a stable system of administration which guarantees us the operation of all academic affairs and monitor the real time traffic and detect possible attacks generated by hackers which basically want to destroy the important resources and information contents of the university. We also proposed a security policy especially for the universities networks. Furthest most, we can constitute an apt and accomplished system to secure the educational administration and bestow useful suggestions for university's educational administration information security. The rapid increase of information technology usage demands the high level of security in order to protect the data assets and equipments of the user. This paper will give guidelines that allow the universities to manage network security effectively.

Keywords: *malicious activities, management based system, security, intrusion detection system, risk, information contents.*

1. INTRODUCTION

For the appropriate performance of universities operations, instructive direction is considered to be an essential and important part (or component). For the promotion of information creation and logical operation of teaching, design of a valuable and secure system is necessary. However, in the present era of internet, academic institutions specially faced lots of threats like viruses and hacking etc. Some intruders may be tried to access your campus network from inside and outside and may create vulnerability in the system. Due to an attack in the universities network, operations of the MIS are effected badly. It will cause an information loss related to student's information bank, course management system, record management, library management system and overall learning. Therefore, the security in the universities network is essential and key component. To detect penetrators in the network through various means and techniques, an IDS for campus management is necessary. When network discussed, network security also is in discussion. 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 for 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 network security policy architecture in which we should be updated with the latest technology. To keep the updates, the training must be given to the administrator/ manager networks in order to maintain the networks and to reduce the complexity [1]. Only authorized users have access to retrieve the data. Every system has been created or built to utilize itself at a maximum. Firewalls and ID mechanisms are useless if your main servers compromised. 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 cannot be achieved by simply adopting the technology and by installing new technological accessories, but it's 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 find a ways to maximize both the usability of a system and the security of the system has been a long standing problem [2].

2. BACKGROUND

The events that occurred and that are processed which are monitored in a computer system are called intrusion detection [3]. When there is a step to attempt to stop detected possible incidents. Logging information, stopping them and then informing to the system administrator are the possible incidents. IDPS is sued for keeping the records of threats, solving the problems with security policies and giving information to the individual from violating security policies. Incidents for protection form a risk to the educational academic assignment [4]. The failure of data or illegal revelation of research oriented information, client's records, and financial systems could greatly hinder the legitimate activities of University staff, faculty and students. Failure to work out due diligence may direct to financial accountability for damage done by users retrieving the network from or through the University. We have to build IDS based solution in our network to protect proposed Management Based System that monitor the network traffic and detects the abnormal activities. MBS comprises of some crucial systems like Time Table Management System, Student Record Maintenance System, Audit System, Enrollment System,

Payroll System, Decision Support System, Library Management System and Semester Examination System.

2.1 Goals

The objective of this network usage security policy are to protect the universities networks and system resources form misuse, to identify the security breaches or any kind of abnormality in the network, to establish a mechanism that help in responding user complaints and queries about the real and perceived abuses, to create a mechanism that will save the university's academic reputation and will permit the institution to keep its lawful and moral responsibilities. As per this policy, information technology resources comprise information assets, software assets and physical assets. We have to propose such a system that is actually secured not only theoretically secure, this needs to combine both theoretical and practical.

2.1 Passwords

It is considered as a mechanism for the verification of the network user. It is a series of characters comprising of alphabets, digits and may have some special characters that validate the individual identity [5]. Intruder may try to gain access your password if it is easy breakable and your network not having the proper guidelines for password assigning. By guessing the password a malicious user may be penetrated into your university's network. You should not use the default administrative password and the password set by the vendor but always tries to enable the password option and assigned the password at its maximum difficulty level and we need to change our password on frequent basis. University network user in generally who have some limited access to the network resources like browsing internet, exchange emails, some word processing and avail the printing facility are unaware that how much intelligent an attacker be, so therefore it is solely dependent upon the network policy. Similarly we should not leave the wireless network access points on its factory settings that may allow everyone to use your network without a password. Passwords can be easy and complex that depends on the user. Experiments have shown that user able to guess user password for between 25% and 80% [6].

2.2 Patching

Any kind of update that increase the functionality and solving a problem for a program or system designed refer as patching [7]. It may refer as a mechanism to solve any kind of security problem by updating the system. Administrator need to validate the identity of the source that generated patch before running it. It should be verified by the vendor public key. Especially for the university network environment it is the role of the system manager / administrator to update the patches of antivirus software on regular basis.

2.3 Configuration

The system we deployed need to operate properly, configuration covers a vital part in installing and operation of the system [8]. It depicts what user and the processes can do in the concerned domain where the system deployed. Safe installation is done by the configuration and the system functions well. All Among other actions, the virus infected a commonly used template file, so any other file referencing that template would also be infected [9]. 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 verification mechanism.

2.4 Congestion

Congestion problem arises in most cases at the campus network. In dealing with congestion, it is important to understand your traffic flows [3]. Like in our university's network by VLANS traffic of the network flows, about 60 VLANS in our campus network. In order to achieve the security and to reduce the broadcast traffic we separated each department into a VLAN. 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 [10]. Before dropping the packets, most network equipment will attempt to buffer them; in our network devices have good buffering capacity.

3. ARCHITECTURE

The security architecture for network systems with the internet access is completely different as far as earlier concerned. Information is easily available and widely accessible from anywhere else by using the technology and people demands that they have the basic resources of network in their intranet but due to this spread of information, it may contains some malicious information during the transmission across the internet. Before connecting to the internet we should check our system for security. Security policies reinforce the procedures to prevent from attacks and give guidelines for the network usage and respond if some incidents occur. It may consider as the foundation because it notifies which assets needs to be secure. A complete security framework required a well established network security policy. In order to implement the network security policy a risk analysis should be evaluated. Our policy implementation in such a way that the cost of protecting assets is not greater than the cost of assets.

3.1 Proposed Model for MBS

Every university should have the Information management type system as proposed in figure 1 in this section for achieving their goals but needs to be secure because university core administration sometimes depending on this type of proposed management based system.

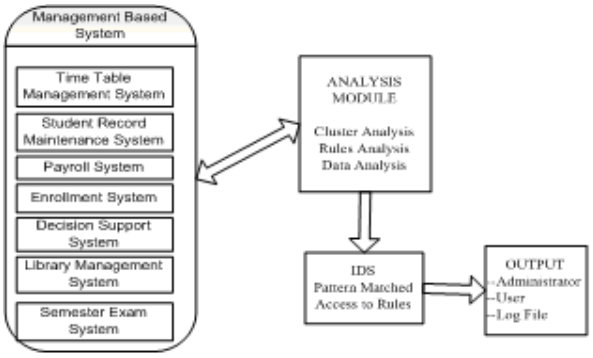

Figure 1. Proposed IDS Model for MBS.

- Time Table Management System (TTMS):

TTMS responsible for managing the course planning and Semester Time Table. All the queries related to classroom conflict, teachers course load and labs conflict, handled by TTMS. If this compromise by the intruder, causes mismanagement of scheduling, calashes occurs that creates problems in Semester Management. Some intruders have intensity to break the availability of the resources.

- Student Record Maintenance System(SRMS):

In SRMS all the records related to students stored in a database. Their Fee structures and profile records managed by SRMS. In university's system we need to secure it by strong intrusion detection system.

- Payroll System(PS):

Employees' salaries managed by the payroll system. All the financial issues handled by PS including the audit system. It's a complete ledger system, if it compromised by the hacker it causes major auditing problem and disturb the accounts management activities.

- Enrollment System(ES):

As student gets admitted in the university it first got the enrollment from the enrollment section, their ES works effectively. Highly sophisticated database record related to students stored in ES. It contains strong verification mechanism and major attackers want to generate the security threats in order to penetrate in the enrollment section and tampered the record.

- Decision Support system(DSS):

Sort of a system that helps the university's administration to take decisions for running the top level affairs of the university. Intruders focused on this subsystem of MBS and puts efforts to figure out which type of traffic flows.

- Library Management System(LMS):

It deals with the complete issues related to library Information system contains all records related to the books, journals, periodicals etc. and have the excellent searching techniques. Student may use this facility online by the help of web portal system. If authenticity, secrecy and integrity get compromised, attacker has the room to easily penetrate in the system.

- Semester Examination System(SES):

Semester related activities like student semester record, student grade point calculation, and student's promotion issues are the part of SES. It contains highly confidential information and needs restricted access through strong authentication methods. Most of the hacker just wants to concentrate on such activities by which they find the solution to access SES in academic environment.

4. OBSERVATIONS

4.1 Proposed Risk Model for Universities Networks

Different categories of risks shown in the below mentioned model in figure 2. The possible impact of these risks are compromise on one of the security requirements causes the damage of universities confidential data, financial loses and destroy the image of academic institution.

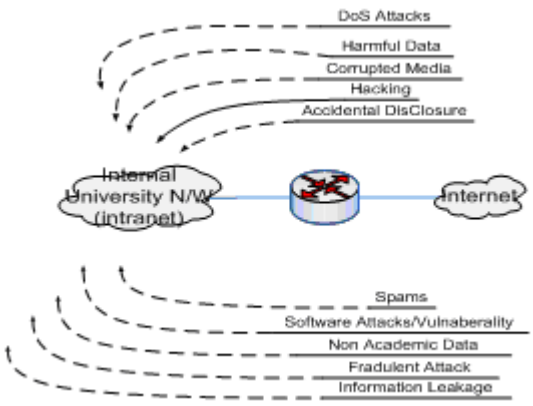

Figure 2. Internet Risk Model for University Network

Users of the internet may generate flooding with unwanted traffic causes DoS attacks like Ping of Death and teardrop attacks [11]. Administrators need to install some software fixes that can limit the deficiencies caused by known attacks. New viruses developed day by day by the hackers to effect the working of the system. Some emails can be misdirected during transition, messages may become corrupted. Undesirable data may enter into the network system through the internet. On the internet we have some laws to access or to retrieve the information but unfortunately our internet user not bother such kind of issues and may deliberately download someone data by illegal means. We have to obey rules and regulations for downloading our relevant information.

Hackers try to access the network system by unauthorized means. Their point of concern is to cause damage including forging of emails. Many attackers find the secret password by using some illegitimate. When using internet we just exchange different data and incaution while communicating our secret information. It may cause the induction of secret information with our emails and websites. Network user may receive unauthorized emails which may causes harmful activities in the system. People generally disable the spam filtering. So junk of emails bombarded into the folder. We have to spam such kind of emails in order to reduce these kinds of attacks.

Much attractive software contains the malicious code may causes viruses attacks, system failures and memory loses etc. We should aware while using such kind of untrusted software's. Information secrecy is one of the ultimate goals of security measures. Disclosure of confidential information may cause the harmful academic activities. Some users are using the internet just for the entertainment purposes. For this they connected many unsecure sites and joined different untrusted internet groups. We should restrict our network users by applying security policies that limit such kind of usage and try to focus them on their research activities. In order to maximize the benefits of the university internet usage should be aligned with your objectives. However, we may modify the above proposed risk model for internal threats/attacks and there is need for precautionary measures to mitigate these risks.

4.2 University Academic Policy

This paper provides you guidelines to use machines and network resources on the Karachi University campus. It will also give a usage outline for network users and connected systems. The MCN is an inter-network of local area networks (LANs) located in various departments on the Karachi University. MCN (Main Communication Network) is connected to the PERN network which is connected to the worldwide Internet. The usage policy for the network is proposed to keep the reliability of university's network and to alleviate the threats linked with defensive threats to educational intranet and its assets. In creating policies that apply to all people who use these resources, MCN system and network administrator need to show how global policies benefit everyone who relies on computing at MCN.

In a heavily networked environment like our university network, having a point of view that gets the whole university structure into account formulates it mainly that result will not permit one piece of the network to accidentally have a harmful impact on different portion. In the end, thoughtfully skilled educational network policies will assist to produce a computational atmosphere that replicates the requirements of its network clients and facilitates set up the most reliable group of policies for the extensive group of people that depends on PCs and intranet at MCN.

The effective intranet usage of university of Karachi network is possible by this policy document. MCN network usage policy revised on regular basis in order to incorporate the experiences learned by using the network. Technical Committee of the Main Communication Network is responsible for all major reviews and updates. Usage guidelines and rules linked with this policy will be available online on the official site of the University. The target of this MCN policy document is to make general policies for the whole academic institution in order to prevent it from misuse and different malicious attacks and to set up some methods that will help in the recognition and prevention of misuse of University networks and its resources. Also to establish useful system for reacting to outside objections and inquiries about genuine misuses of educational intranet and its resources, and will permit the institution to fulfill its satisfy its official tasks with regard to its intranet and PCs connectivity to the public network.

The University of Karachi provides network assets to its academic departments. Majorly this policy used to prevent the network from threats/ dangers and to reduce the number of security events on the university's intranet without impacting the educational work or the reliability of the University's computational societies. The goal of this MCN policy guideline is to make sure the constant availability of the major services provided by university network, the validity and integrity of the data, skills to recover successfully from disorder if any and the security of all resources.

Reporting Problems are one the widest problem that this policy faces. Organizational safety mainly concern about the physical security and if client PC stole than there is no means of electronic security. Theft should be reported immediately to the University Campus Security Office as well as to MCN office. In case of any security violate client promptly report to the MCN office. Any remote system policies violation must notify to the system administrator. PCs which are out of order and other troubles related to lab equipments must be immediately informed to lab staff available in the department or otherwise report to the MCN complaint office.

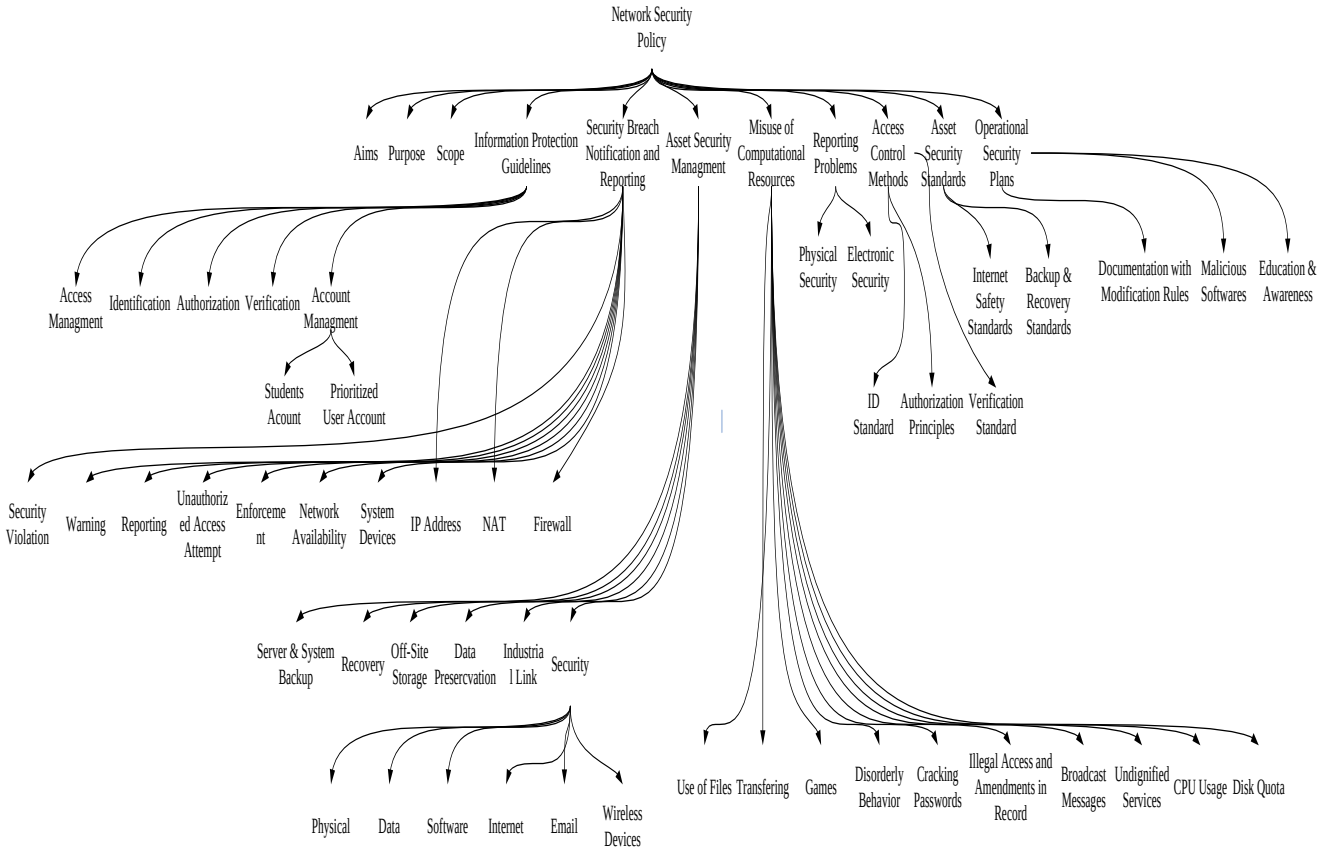

Figure 3. Framework for Internet Usage Policy

5. DISCUSSION & CONCLUSIONS

University's academic mission may be affected by the threats and security incidents occur in a network. The loss of data or unauthorized disclosure of information on MBS could greatly hinder the legalized procedures of the University employee, teachers and students. The academic institution has its own responsibility to maintain the secrecy in their network system, for this a proper network support department like MCN should exist. IT resources include information resources, hardware and software resources.

The complete frame work model for the network security policy as proposed in fig. 3 should be existed in your network to proper utilize the benefits of the network resources. MCN System Administrator has to frequently evaluate their assigned rights, to verify who is certified to utilize the PC system and its authorization level. To utilize the network resources efficiently a user is assigned a username and password keeping the integrity concerns. Network users must be verified to access the appropriate systems and their resources. When students gets admitted and got the enrollment its account is generated by system procedures automatically and MCN department get the list of enrolled students from the admission/enrollment section.

To prevent the system from the different categories of risks as proposed in the risk model in fig. 2, strong policy infrastructure developed as per guidelines proposed in this paper. In order to keep the university critical mission secure and for proper working of the academic affairs one should follow the system based on the proposed model as mentioned in fig.1.We are also developing the statistical model for risk management and network security decision support systems.

6. REFERENCES

[1] JA Gutiérrez, Donald P Sheridan and R. Radhakrishna Pillai. 2000; "A Framework and Lightweight Protocol for Multimedia Network Management"; Journal of Network and Systems; Springer.

[2] Peter Folger. 2009; "Geospatial Information and Geographic Information Systems (GIS): Current Issues and Future Challenges"; CRS Report for Congress.

[3] Syed Muhammad Aqil Burney and M. Sadiq Ali Khan. 2010; "Feature Deduction and Ensemble Design of Parallel Neural Networks for Intrusion Detection System"; IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010

[4] Ki-Yoon Kim and Ken Surendran. 2003; "Information Security Management Curriculum Design: A Joint Industry and Academic Effort"; Journal of Information Systems Education, Vol. 13(3).

[5] Adrianne Jefrries. 2010; "Debate Around Password Security Overlooks Universal Logins" .

[6] Sandra. Steinbrecher, Groß. Stephan, Meichau. Markus. 2009; "Jason: A Scalable Reputation System for the Semantic Web"; IFIP Advances in Information and Communication Technology, Volume 297, Emerging Challenges for Security, Privacy and Trust, Pages 421-431.

[7] Jeffrey Brian Arnold. 2008; "Ksplice: An automatic system for Rebootless Kernel Security Updates"; MIT.

[8] Parsa Mirhaji, S. Ward Casscells, Arunkumar Srinivasan, Narendra Kunapareddy, Sean Byrne, David Richards, and Raouf Arafat. 2006;" Services Oriented Architectures and Rapid Deployment of Ad-Hoc Health Surveillance Systems"; AMIA Annu Symp Proc. 2006; 2006: 569–573.

[9] Matt Bishop. 2003, "Computer Security: Art and Science"; Reading, MA: Addison Wesley Professional .

[10] Akhter Raza,S.M.Aqil Burney,Major Saleemi. 2010, " Forecasting Network Traffic Load using Wavelet Filters and Seasonal Autoregressive Moving Average model", Submitted for publication in International Journal of Computer and Electrical Engineering (IJCEE) will be published in Dec.

[11] Amit P. Jardosh, Krishna N Ramachandran,Kevin C Almeroth and Elizebeth M. Belding Royer. 2005; "Understanding Link-Layer Behavior in Highly Congested IEEE 802.11b Wireless Networks"; *SIGCOMM'05 Workshops,* Philadelphia, PA, USA. ACM 1-59593-026-4/05/0008.

Dr.S.M.Aqil Burney is the Meritorious Professor and approved Supervisor in Computer Science and Statistics by the Higher Education Commission, Govt of Pakistan. He is also the Director & Chairman of Computer Science Department, University of Karachi. Additionally he is also a Director of Main Communication Network University of Karachi. He is also member of various higher academic boards of different universities of Pakistan. His research interest includes AI, Soft Computing, Neural Network, Fuzzy Logic, Data Mining, Statistics, Simulation and Stochastic Modeling of Mobile Communication system and Networks, Network Security and MIS in health services. Dr.Burney is also referee of various journals and conferences proceedings, nationally & internationally. He is member of IEEE(USA), ACM(USA) and fellow of Royal Statistical Society, United Kingdom. He has vast education management experience at the university level. Dr.Burney have been awarded best IT academician in the country in 2003 by NCR (Pak).

M.Sadiq Ali Khan received his BS & MS Degree in Computer Engineering from SSUET in 1998 and 2003 respectively. Since 2003 he is serving Computer Science Department, University of Karachi as an Assistant Professor. He has about 12 years of teaching experience and his research areas includes Data Communication & Networks, Network Security, Cryptography issues and Security in Wireless Networks. He is member of CSI, PEC and NSP. He is also working as a System Administrator Main Communication Network University of Karachi.