Enhanced Methods of Ensuring Network Security in Campus Networks

Aman Ullah[1]

[1]Department of Computer Science, Alpha College of Science, Pakistan

Summary

The Internet was built in university campuses by academics for academics. They never thought to use it for new kinds of commerce, cybercrimes, espionage and social activities. As the internet became popular outside university campuses among corporations and governments as well as a target for criminal minds and terrorists, the security industry appeared to develop new controls and defenses to ensure protection against every threat imposed by criminals. The academia which developed the Internet, has not accepted thriving industry of security tools and tactics. A secretive government agency or a company may have a highly secured network that closely monitors and controls new devices, users and online traffic. But it does not make sense for universities and higher education institutions where intellectuals come for study from all over the world having their own devices, to have strictly monitored network. In this paper, I have proposed new techniques to ensure network security in campus network. This model can also be used in large scale enterprises as well as users and online traffic. But it does not make sense for universities and higher education institutions where intellectuals come for study from all over the world having their own devices, to have strictly monitored network. In this paper, I have proposed new techniques to ensure network security in campus network. This model can also be used in large scale enterprises as well.

Keywords:

campus network, security, applications, awareness

1. Introduction

In a college or university nobody desires having a computing environment where selected groups of users, their data and their infected laptops and smartphones are protected. At the same time everyone wants to ensure safety and integrity of personal information and intellectual property of the staff and students. We also want to ensure the network resources are not used for illegal activities or used to attack or infiltrate another network for malicious activities. So it is difficult for administrators, academics, IT staff and students to find out how to balance their research and educational mission.

With the development in the field of science and technology, peoples depend upon network resources a lot. Definitely, the network has become the backbone of any country's political, economic, military and scientific resources as information about them are stored over the network [16]. The security breaches, which have become very common these days, are constant danger to the information security, integrity and availability for any private or public organization. As we see cyber-criminals have attacked on public and private organizations like Sony, Adobe, MIT etc frequently. As a result, these organizations have paid heavy price in the form of great economic and scientific data breaches and lost credibility. Therefore, each public or private organization requires appropriate measures, controls, procedures etc in place to thwart such attacks to ensure its network resources are safe. These days campus networks are connected which has led to increased number of applications and users and more attention to the network security. Most of the campus networks don't have specific security tools, applications, procedures etc in place as they mostly depend upon installation of anti-viruses and to some extent firewalls. They never have mechanism to identify vulnerabilities and bugs in applications and host operating systems thus threatening the security of the entire network [2].

Network technology is key to many applications. Network security is the most important requirement in modern networks, but information about implementation of security methods needs more research. Network security means the entire network, resources, applications, hardware, software etc must be secured. It does not mean security in workstation at the user end. The communication channel must be free of any vulnerability because any experienced hacker could hack communication channel resulting in data capturing, data decryption and injecting spoofed information. A successful network security plan is developed by giving importance to security issues, possible attacks, social and cultural factors which could make the network vulnerable.

Manuscript received September 5, 2025

Manuscript revised September 20, 2025

https://doi.org/10.22937/IJCSNS.2025.25.9.19

Various methods are available to ensure the network is less vulnerable to the malicious users. For example, authentication mechanism, firewalls, encryption and intrusion detection system can be applied. Large scale enterprises combine multiple methods for their network security [7]. To understand what types of security measures can be taken to guarantee network security, we need to understand the Internet in detail which itself leads to vulnerabilities. So the Internet has great influence over the development of new security strategies, approaches, technologies etc.

2. Network Partitioning

The network partitioning and segmentation are quite popular techniques in universities network security. The most sensitive and administrative information can be protected satisfactorily by granting access to selected group of users [4]. On the other hand, open parts of the network keep on supporting educational and research activities. Individual departments and research groups manage their own data which makes difficult for university administration to identify and select suitable place for storing sensitive information and what types of activities are going on in other parts of the network. The universities are appealing targets to the hackers because they contain very valuable information which includes personal information, R & D data about their basis science or grant related projects of enormous interest to national state groups. The universities are not competitors to financial services, oil and gas and aviation sectors on the infrastructure side.

3. Anomaly Monitoring

A new view has become spread through universities and large scale enterprises that is monitoring network behaviour for anomalies. In this approach universities, companies and organizations assume themselves under constant attack with the notion that perpetrator is inside the network. On the basis of the analysis of the network behaviour new set of controls and defenses can be implemented [15]. It should be clear that no set of controls, defenses, procedures and methods is sufficient to completely bar a determined adversary from the network. The companies watch the behaviour of the network more closely rather than just making perimeter of defense around it. The companies and organizations tend to make a new security system or patch it necessary for its users, but in an academic institute users are given the option that will fulfill their needs rather than forcing them to take up those changes. The University of Idaho gives its users two choices: long password and short password. The long password must be 15 characters long and it does not expire before 400 days. The shorter passwords are changed after every 90 days. The majority of the users prefer shorter passwords. In order to support collaboration, innovation, and research where collaborators work globally, the universities have to ensure they don't put barriers in place which could make it more difficult for users.

4. Strict Security Policies

Security incidents are reported at many educational institutes. In the past many campus networks were used as launch points for attacks on third parties, but in the past few years, this trend has changed dramatically. As number of schools have been target of breaches and run off their intellectual property. Why academic institutes are reluctant to formulate stricter security measures is the conception that security equals constraint which is against the spirit of open exchange of information.

Two schools of thoughts on computer security in educational institutes are popular. According to one, universities are much behind tan companies in their security efforts so they need to introduce more locked-down, corporate approach to network security. The other says that companies are embracing educational institutions perspective that emphasis should be given on network monitoring activity rather than forcing them to accept security policies. Even some researchers consider academic institutions as models to deal with security threats raised by BYOD environments [14]. Academic institutes always supposed that security is much easier for corporations because they can lock-down their staff and devices which cannot be done in universities.

5. Network Security Awareness

Information security awareness among users is one of the building block for information security strategy for any organization. The research community and information security practitioners do recognize human factor in network and information security because attitude and behaviour of the users do reflect whether they are aware of network security [1]. However, socio-cultural factor must be analyzed and understood to make sure diverse users' commitment and adherence to network security regulations, policies, procedures etc. On the other hand, we see that scientific studies about network security in developed countries in higher education is not so common. We find only a few good research articles which do not reveal complete status of network security. In developing countries, the situation is even worse where socio-cultural environment joined with lack of resources and knowledge create even more obstacles to promote network security.

6. Effective Network Security Strategy

Each university has thousands of students, employees, endpoints and diverse applications connected to the network at any given time. Installing firewalls, anti-virus software, single step authentication etc are not enough to guarantee network security in the face of rising cyber threats every day. Layered protection, web and email gate filtering, two layered authentication and scalable security solution are simple answers to mounting security threats but there is no surety they will protect network resources under attack. Threat intelligence and defense measures should be incorporated in each vendor's network resources to continuously gather and analyze new threats. Centralized and simple management having automatic monitoring and reporting capabilities must be implemented [17]. Traditional security strategies used in network cannot provide peace of mind for organizations. As we saw in cyber-attacks on Sony Corporation, the intruders destroyed the network although Sony had placed sophisticated security mechanism in place. The intruders thwarted that mechanism and robbed every piece of valuable information. This incident is an example for future security mechanism and strategies development to show how intruders can foil current security mechanisms.

7. Next Generation Network Security Platform

Next generation networks provide complete protection than so-called next generation firewalls [6]. Due to higher data rates and traffic volumes enterprises and service providers switch to multi-protocol network architectures which demand highly flexible, scalable and evolving platforms. Next generation firewalls which do not provide traditional and advanced threat protection cannot ensure protection of such high-performance environments. Thus, organizations require next generation security platforms and related devices which can guarantee protection against known and unknown threats. These platforms are not only flexible but also scalable to adapt to variable business growth and services. A platform of scalable and field-proven core security technologies and next generation security capabilities is compulsory to keep enterprise network safe from any attacks.

8. Next Generation Network Security Technologies

It's been evident that traditional security mechanism consisting of firewall, intrusion detection system and host-based antivirus are not satisfactory to protect against modern sophisticated threats. Every year, data breaches and damage to the corporate networks are rapidly growing as criminal minded persons discover new techniques to infiltrate corporate networks. Corporate executives and IT staff members are more concerned about their employees' actions as new regulations and legal requirements hold them accountable for any data breaches in corporate networks [6]. That's why they monitor the activities of their employees for what they view and download from the Internet. Few next-generation network security technologies are shown below.

9. Applications Control

Application control is primary requirement for next-generation firewalls adoption. Organizations must have the ability to effectively control both legacy applications and modern Internet based application to make certain data loss prevention and new threats mitigation. Regardless of ports and protocols in use, next-generation application control must ensure detection, monitoring and usage control of such applications and related files at both gateways and endpoints [11]. Before giving proper access rights to end users, an association must be established between the application and its users.

10. Integrated Intrusion Prevention System

Installation of updates and patches is by itself a complex and time-consuming process in complex next-generation networks. All effected systems require long time like weeks or even months to install a fix in their networks. In this situation, networks must be protected from known and zero-day vulnerabilities and access must be blocked for all requests that may threaten to exploit unpatched systems. Malicious network activities such as

Manuscript received September 5, 2025
Manuscript revised September 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.9.19

predefined and custom signatures, protocol decoders, packet logging, and IPS sensors must be monitored and blocked appropriately to ensure network security [8].

11. Data Loss Prevention

Some employees transmit data into untrusted Zones due to negligence. Various communication protocols like HTTP, HTTPS, FTP, FTPS, POP3, POP3S, IMAP, IMPAPS, SMTP, SMTPS etc must be monitored for sensitive data transmission. DLP can be used to avoid unnecessary data transfer to untrusted receivers. Its features are fingerprinting of document files and their sources, proxy and flow based inspection modes, data archiving and enhanced pattern matching [10].

12. Dual Stack IPV4 And IPV6 Support

Many organizations prefer migrating to IPV6 due to the exhaustion of the IPV4 address space. The IPV6 is next generation Internet communication protocol which provides trillions of IP addresses for future use. It also provides many new features such as better security, improved addressing, routing efficiency and much better QoS. Its architecture will respond to future requirements for global end to end communication efficiently [5].

The organization are running to deploy such network security devices that can deliver better content protection for IPV6. At present, two methods, dual-stack and tunneling, are most commonly used. Dual-stack technique is preferred because it processes each packet in IPV4 or IPV6 depending upon the network whereas the tunneling wraps IPV6 packet into IPV4 header. The drawback of latter mechanism is that a device can forward a packet but cannot inspect it regardless of the contents which may be even malicious. This limited support will result in unwanted traffic traversing the entire network.

13. GOVERNANCE

Governance means those considerations taken into account at the time of design and implementation of a campus network security plan which includes ownership, oversight to policy and practice. These considerations must be given priority to make sure selected users exploit network resources in line with university policies [9]. The senior leadership must lead from the front to face a problem and ensure institution level engagement of various users and policies to enhance network security. The governance is driven by accountability, organizational structure and appropriate monetary resources.

14. Ownership and Accountability

The ownership and accountability for network security depends upon a formal person having large measure of authority to create and disseminate network security policy. Such person is necessary to cut through departmental boundaries and conflicting agendas of various users. Recovery efforts can be fully focused if clear lines of authority and accountability are defined [3].

15. Staff and Organizations

For network security, operation responsibility is a major issue when defining network security policies. Most of the universities are always in uncomfortable position when enforcing network security policy without appropriate power [12]. Although staff members have necessary knowledge and skills to make certain network security, still there is no guarantee that each application and system on campus can be secured especially when different applications are administered by different departments.

16. Monetary Resources

A structured funding model is essential for ongoing network security governance. Network security never comes free especially when we come across rising data breaches on everyday basis [13]. The staff must have the latest tools, applications, hardware etc at their disposal to prevent unexpected issues generated intentionally or intentionally. It is crucial to recognize proper funding resources for an effective network security plan.

17. Conclusion

This paper simply identifies various techniques and technologies to safeguard campus network against modern threats which cannot be mitigated by traditional technologies. Cost and lost business value continue to rise every year in large scale enterprises and universities worldwide which shows criminals will try their best to steal valuable scientific data wherever it exists. Therefore, universities and technological institutes are prime targets for criminals. To cope with modern threats, the universities need to implement such security platform which can safeguard known and future threats. It requires field-proven and scalable platform which consists of both core security technologies and next generation security capabilities. As we know the next-generation network provides much more beyond traditional security. A next generation network must be developed to utilize both today's requirement and future technology disruptions. It must be a dynamic network that must support mobility and cloud computing trends and variable threat landscape. Above all, security awareness among students, faculty members and IT staff is mandatory to ensure they utilize network resources in accordance with policies set up by the management.

References

[1] Abraham S, Nair, S (2015). A Novel Architecture for Predictive CyberSecurity Using Non-homogenous Markov Models . *In Trustcom/BigDataSE/ 2015*, Helsinki, 20-22 Aug. 2015. Finland: IEEE 774-781

[2] Anon. (2015). *How Secure is Your Campus Network?*. Available: http://vectorusa.com/how-secure-is-your-campus-network/. Last accessed 27th Jul 2016.

[3] Cohen, F. (2005). Security governance for the enterprise. (Vol.1). Burton Group, Retrieved July 26,2016,fromhttp://www.burtongroup.com/content/doc.aspx?cid=660

[4] Deepa, T and Jeyaawinothini, R (2015). An efficient approach to reduce network partitioning using AMMNETS . In Electronics and Communication Systems (ICECS), 2015 2nd International Conference Madras, Feb 26. India: IEEE Conference Publications. 474 - 478.

[5] Faria, B, Suoto, E. (2014) 'Performance analysis of +Mobile IPv6 support for Dual Stack hosts'. In *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*. Doha, Qatar, pp. 92-100.

[6] Garcia,W,B, Calderon,C,A. (2011). Experiences in Planning and Implantation of Security at Next Generation Networks. *IEEE Latin America Transactions*. 8 (6), 703-707.

[7] Huang, C, Ziong,J (2014). Study of campus network security based on SAPPDRR model. In Information Sacience, International Conference on Electronics and Electrical Engineering (ISEEE), 2014. Sapporo, 26-28 April 2014. Sapporo: IEEE. 1122-1127.

[8] Koch, R (2011). Towards Next-Generation Intrusion Detection. In 2011 3rd International Conference on Cyber Conflict, Tallinn, IEEE, 1-18.

[9] Kvavik,R.B., & Voloudakis,J.(2003). *Information technology security: Governance, strategy, and practice in higher education.* Boulder, CO: EDUCAUSE Center for Applied Research, Available from http://www.educause.edu/ecar/

[10] Liu, S, Kuhn, R. (2010). Data Loss Prevention. *IT Professional*. 12 (2), 10-13

[11] Mueller, J, Magedanz, T (2012). Towards a generic application aware network resource control function for Next-Generation-Networks and beyond. *In Communications and Information Technologies (ISCIT), 2012 International Symposium*, Gold Coast, QLD, 2-5 Oct. 2012. IEEE. 877-882

[12] Oblinger, D. (2003). *Computer and network security and higher education's core values*. Boulder, CO:EDUCAUSE Center for Applied Research. Available from http://www.educause.edu/ecar/

[13] Salomon, K.D., Cassat, P.C., & Thibeau, B, E. (2003), IT Security for higher education: A legal perspective. Boulder, CO:EDUCAUSE. Retrieved July 26, 2016, from http://www.educause.edu/ir/library/pdf/CSD2746.pdf

[14] Vukalović, J, Delija, D (2015). Advanced Persistent Threats - detection and defense. In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention Opatija, 25-29 May 2015. Croatia: IEEE. 1324 – 1330

Manuscript received September 5, 2025
Manuscript revised September 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.9.19

[15] Wang, L, Wu, X. (2015). Distributed prevention mechanism for network partitioning in wireless sensor networks. *Journal of Communications and Networks.* 16 (1), p667 - 676.

[16] Wolf, J. (2015). *Can Campus Networks Ever Be Secure?.* Available:http://www.theatlantic.com/technology/archive/2015/10/can-campus-networks-ever-be-secure/409813/. Last accessed 25th Jul 2016.

[17] Zhou, H, Wu, C, Jiang, M, Zhou, B, Gao, W, Pan, T, Hunag, M (2015). Evolving defense mechanism for future network security.*IEEE Communications Magazine*. 53(4), p45-51.

Aman Ullah received M.Sc. degrees in Applied Computing from Dublin Institute of Technology in 2010. He has vast teaching experience in Pakistan and abroad. His interests include information security, network security, wireless networks, data communication and reliable software development.