Managing Security Risks and Vulnerabilities in University's IT Threats Landscape

Chanchala Joshi
Institute of Computer Science
Vikram University Ujjain, M.P. India

Umesh Kumar Singh
School of Engineering and Technology
Vikram University Ujjain, M.P. India

ABSTRACT
The large and open networks of Universities are particularly vulnerable because they often have multiple overlapping public and private networks. The staff, faculty members or students with infected devices might connect with the Universities networks. Many labs also have devices into their networks that were never intended to be there, which opens up new avenues of attack. This paper analyzed the security threats evolve specifically in University's computing environment, and proposes risk management framework to guide security and risk executives through the process of network security management. The framework follows three phase activities: the first phase concentrates on the identification of the weak point in University's networks; the second phase quantitatively measures the security risk level of the University's networks; the third phase suggests plans for enhancing the security level of University's network environments. The proposed framework focuses on critical assets that are truly at risk.

Keywords
CVSS; security risk; security threats; university campus network; vulnerability

1. INTRODUCTION
University campuses are proving themselves to be some of the most technologically advanced places in the world by providing facilities like extensive Wi-Fi support, online learning using lecture capture software, digital library, classroom virtualization, web conferencing etc. All these advancement makes University's computing environment particularly vulnerable because in contrast to hacking targets like banks, college and university computing environments are often large open networks. Protecting open large university campus against constantly evolving threats and vulnerabilities presents major challenges. On the other hand, the open computing university environment also supports diverse users; mainly the three distinct types of users of university are students, faculty and administration. Each of the user accesses university computing environment with varying level of university resources. Therefore, University campus network must not only provide the secure access to users but also defend them from vulnerabilities and security breaches. In the large University campus network there is need of improving risk posture and security effectiveness. It requires identification of operationally critical threats, assessment of vulnerabilities for measurement of risk level by continuous network monitoring of University campus network.

This paper proposes Quantitative Information Security Risk Assessment Model designed specifically for University computing environment, with the consideration of security dangers presents in large open campus network of University. The proposed model quantitatively measures the security risks by identifying potential threats and information processes within Universities network configuration. This model can be used by risk analyst and security manager of University to perform reliable and repeatable risk analysis in realistic and affordable manner.

2. SECURITY DANGERS IN UNIVERSITY NETWORK
An open and diverse environment is a standard requirement in higher education. University computing environment is setup by academics for academics, not aware of security challenges and dangers. Therefore under most circumstances, universities computing environment are strapped for resources to manage the equilibrium between openness and security against malware and sensitive data exfiltration. Some major issues while managing University campus security are:

- Open Campus: An infection originating in just a single computer can propagate a worm or virus through the entire campus network within minutes [1]. E.g., the "Slammer" worm was able to infect 90 percent of vulnerable hosts in most networks within 10 minutes. If such attacks do not destroy or steal data, they often cause storms of excess traffic and seriously impair an institution's ability to function, resulting in downtime and lost classroom time. In addition, IT administrators in education are challenged to provide robust protection of critical IP applications, while preserving an inherently open network demanded in a college or university environment.
- Large Network Environment: Universities have large campus span ranging from few kilometer to acres, securing such a huge network is challenging task. Along with the large network environment constantly changing technologies increases the data protection pressures.
- Diverse Users: Universities mainly have three distinct types of users of university are students, faculty and administration. Each of the user accesses university computing environment with varying level of university resources. The unique ways students, professors and administrators use the Internet that jeopardizes Universities networks.
- Decentralized Network: University computing environment is typically integration of dozens networks run by colleges and departments. Different department have their own IT department manage by their faculties and students- non IT professional not having knowledge of implementing secure network. This integrated network comprises various types of devices, which results in higher potential risks.
- Social Media Security Risks: Universities students are known to be among the most avid users of social networking sites. The social networking frequently leads to the sharing of personal information. Phishers have

recognized this and attempt to exploit these factors, making for an alarming risk when students surf Facebook or Twitter.

- P2P Dangers in Higher Ed: One critical security problem, unique to University networks is the use of P2P software. P2P file sharing software provide facility to exchange music, movies, videos, and other files over the Internet; and are mostly used by student populations. But malicious software like viruses, worms and Trojans are regularly distributed using these P2P applications.

The above analysis of Universities computing environment concluded that assessment of security risk is crucial in order to ensure organization's security; and security solutions should be implemented according to the structural features of the campus network and security issues which the campus network faced.

3. RELATED WORK

There are various risk assessment models available, some of which are qualitative while others are quantitative in nature; having a common goal of estimating the overall risk value. [2] OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), developed by CERT is a model for risk-based infosec strategic assessment and planning. OCTAVE defines assets as including people, hardware, software, information and systems. One of the major drawbacks of OCTAVATE is its complexity and it doesn't allow organizations to quantitatively model risk.

In order to improve security organization system some standard principles are needed, Joshi et. al [3] analyzed the prominent taxonomies of attacks and vulnerability of computer system and network to improve vulnerability categorization and proposed novel approach towards Standardization of Network and Computer [4]. One another prominent risk assessment model is [5] FAIR (Factor Analysis of Information Risk), provides framework for understanding, analyzing and measuring information risk. FAIR is built to address security concern weaknesses. The framework allows organizations to standardize the risk, apply risk assessment, view in total organizational risk, defend risk determination using advanced analysis and understand how time and money will affect the organization's security profile. The main shortcoming of FAIR is the lack of information about methodology and examples of how the methodology is applied.

[6] NIST RMF (National Institute of Standards and Technology's Risk Management Framework) covers a series of activities related to managing organizational risk. [7]TARA (Threat Agent Risk Assessment) is a risk assessment framework created by Intel that helps companies to manage risk by distilling the possible information about security attacks. The major drawback is to be prohibitively expensive and impractical to defend possible vulnerability. One of the primary tasks of risk assessment process is vulnerability scanning; Joshi et al. [8-9] evaluated the efficiency of web application vulnerability scanners by designing a vulnerable web application. This evaluation assists in choosing vulnerability scanner during first phase of proposed model.

There are numerous risk assessment models; however, there is no mechanism to assist organizations in determining which model is the best to be employed within an organization; also these models considered the security challenges identified in hacking target organizations like banks. Although security risk assessment is crucial for these organizations but these organizations have secure and close network environment. On the other hand, higher educational institutions like Universities where information security risk assessment is major and high priority job are having large and open computing environment. The next section describes the typical scenario of University network environment comprises of diverse small network.

4. UNIVERSITY CAMPUS NETWORK SETUP

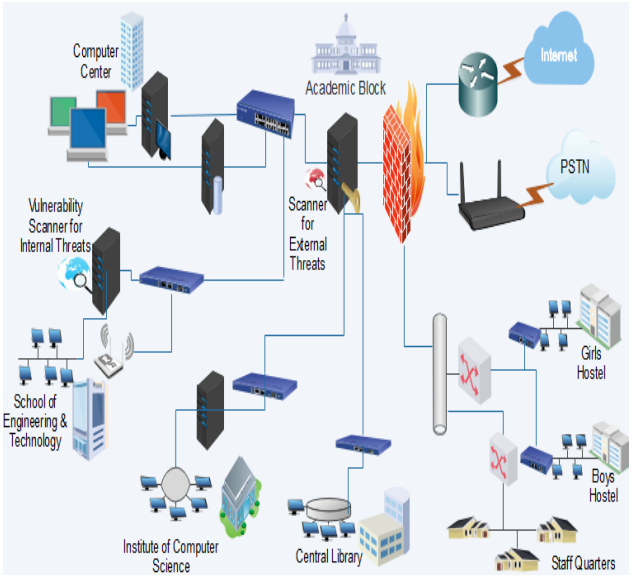

Figure1: Network Setup for University Computing Environment

Figure1 shows the large and open, University campus network setup, comprises of diverse small networks. With the rapid development of technology, universities strive to develop a convenient and valuable learning environment through IT technologies. University large computing environment includes diverse network devices, various software applications and many servers.

5. PROPOSED QUANTITATIVE INFORMATION SECURITY RISK ASSESSMENT MODEL

The main objective behind designing a security risk assessment framework is, "security controls should be selected based on real risks to an organization's assets and operations". Numerous of security risks assessment models are available but University computing environment is differ from other organizations as it is large, open and consists of several small diverse network with various users.

Selecting risk assessment model without analysis, results in implementation of security controls in the wrong places, wasting of resources and leaving an organization vulnerable to unanticipated threats. The proposed risk assessment model initially analyses what is to be assessed, who needs to be involved and the criteria for quantifying, qualifying, and comparing severity of risks.

The assessment results must be documented properly. The goal of proposed framework is to measure risk level quantitatively that will allow higher educational institutes to understand security risks.

The proposed model is based on the most popular risk frameworks in use today, OCTAVE(Operationally Critical Threat, Asset, and Vulnerability Evaluation), developed at Carnegie Mellon University.

The proposed framework performs three phase activities to make standard model more absolute, and provides a practical approach which can be used in real educational environment.

Figure2 shows the abstract three phase view of the proposed model:

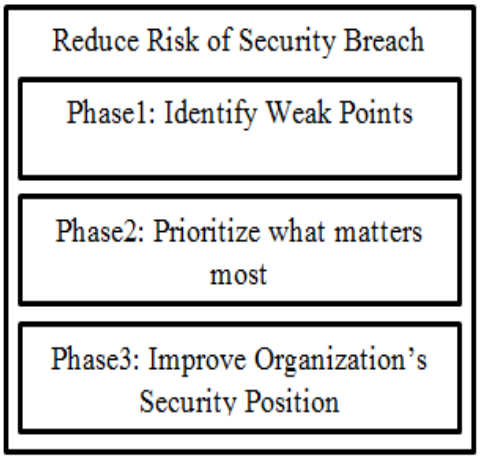

Figure 2: Three Phase Quantitative Information Security Risk Assessment Model

The goal of proposed model is to reduce risks of security breach, this means understanding the cause that makes system vulnerable. The first phase focuses on knowing weak points, even in constantly changing and challenging University's environment.

Then the second phase concentrates on understanding which areas are having the highest risks, based on reliable and granular real risk scoring. The proposed framework uses Common Vulnerability Scoring System (CVSS) [10] to validate which vulnerability can be actively exploited.

The third phase pivot along the creation of actionable remediation plan over with University environment's unique factor to and finally generate powerful reporting to track recursive risk measurement activities.

The central of the proposed risk assessment framework is an objective of assessing University's campus network, recursive mechanism that collects input regarding vulnerabilities and threats and produces quantitative risk level that can be measured and treated.

General steps for the proposed framework are: identifying assets and stakeholders, understanding security requirements, assessing vulnerabilities, analyzing the effectiveness of controls, evaluation of risks by estimating frequency and impact of exploit, designing remediation plans and finally drive decisions using powerful reporting.

Figure3 shows the proposed framework for Quantitative Information Security Risk Assessment:

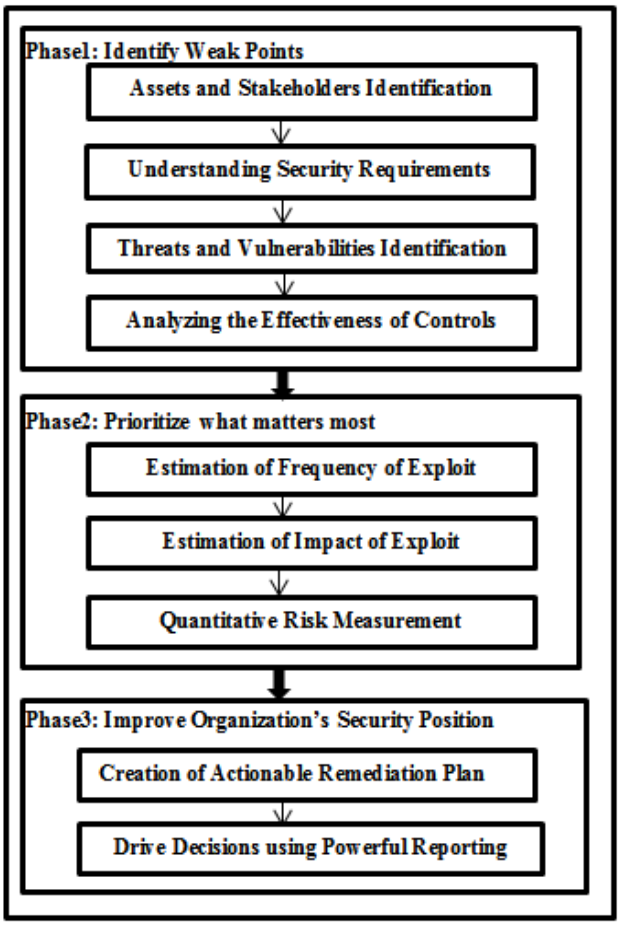

Figure3: Framework for Quantitative Information Security Risk Assessment

5.1 Assets and Stakeholders Identification

The risk assessment techniques require to clearly specifying the assets. This step of proposed model defines the boundaries and contents of the asset to be assessed. In proposed framework information is taken as an asset.

5.2 Understanding Security Requirements

In this step, along with the resources and the information that constitute the system, the boundaries of the IT system will be identified. This step defines the scope of the risk assessment effort and provides information essential to defining the risk. The input for this step is information about hardware, software, data and information, network connections and system interfaces; and the output is a document that describes system mission, system boundary, system functions and information about criticality and sensitivity of data.

5.3 Threats and Vulnerabilities Identification

In this step, threat scenarios will be created, by listing the most common combinations of attack paths, attack goals and attack actor (attackers or hackers), that might lead to the compromise an asset.

5.4 Analysis of Effectiveness of Controls

In this step of assessment technical controls like authentication and authorization, intrusion detection, network filtering and routing, and encryption are considered and a document is prepared as an output which describes the

effectiveness of system in defending against the particular threats.

5.5 Estimation of Frequency of Exploit

In this step, the likelihood that a vulnerability can be exploited by the attacker is determined. Frequency of exploit will be calculated using mathematical formula and will be used in determining the quantitative security risk magnitude.

5.6 Estimation of Impact of Exploit

The impact can be measured by using Confidentiality Impact, Integrity Impact, and Availability Impact metrics of the CVSS [12]. The impact estimates how exploitation of a configuration issue could directly affect a targeted system and reflects the degree of loss of confidentiality, integrity, and availability. This step measures the impact of exploit onto the system.

5.7 Quantitative Risk Measurement

By the convergence of frequency and impact of exploit, quantitative security risk level can be measured. With the calculated risk magnitude the qualitative risk level can be determined in the range low to high. This risk level will be further used in creation of remediation plans.

5.8 Creation of Actionable Remediation Plan

Risk magnitude calculated in previous step prioritize the vulnerabilities which assists in defining remediation plans to validate identified vulnerabilities in order to improve system's security level. Second phase of the proposed identifies the areas are having the highest risks using Common Vulnerability Scoring System (CVSS) [10]. This risk magnitude can be used to estimate which vulnerability can be actively exploited and remediation plans will be designed using this information.

5.9 Drive Decisions using Powerful Reporting

After completion of risk assessment procedure the results should be documented in an official report format. This report will help senior management, the mission owners in making decisions on policy, procedural, budget, and system operational and management changes. As risk assessment is recursive procedure, this final generated report will be used as an input of phase1 of proposed framework in the next cycle of risk assessment procedure.

6. EVALUATION OF PROPOSED QUANTITATIVE INFORMATION SECURITY RISK ASSESSMENT MODEL

In this section, the proposed model is evaluated for University computing environment. University's network environment is continually expanded and updated, its components changed, and its software applications replaced or updated with newer versions [16]. These changes indicate that new risks will emerge and the previously mitigated risks may again become an issue. Thus, the risk management is ongoing and evolving process. This section emphasizes the good practice and need for an ongoing risk evaluation and assessment.

The first phase of the proposed framework identifies the weak point of the system, which already discussed briefly in section II of the paper. The next phase prioritizes the security vulnerabilities according to the risk magnitude. The first step in quantitative risk level measurement is identification and assessment of vulnerabilities. The next subsection describes the vulnerability scanning method in University computing environment (network setup shown in Figure1).

6.1 Network Vulnerability Scanning

Proactive network security finds the holes in network before the attackers do. Vulnerability scanning helps to protect system against both internal threats such as malicious users within the network and external threats like attackers and worms [12]. A network scanner identifies vulnerabilities which are present in the system. The scan results will depend on the placement of the scanner in organization's network. Vulnerability can only be detected if the scanning host has access to the vulnerable service [13]. Since scanning through a router or firewall could hide internal vulnerabilities, it is best to place the scanner inside the firewall so it can scan for both internal and external vulnerabilities, as shown in the placement of the blue scanner in the diagram below. The red scanner in the Figure1 can only scan for external vulnerabilities. Vulnerability scanning method involves the creation of attack scenario by listing the most common combinations of attack paths, attack goals and attack actor (attackers or hackers), that might lead to the compromise an asset.

In the next step of the second phase frequency and impact of identified vulnerabilities are calculated using mathematical formula. Risk magnitude depends on the likelihood of the exploit, as the more frequent occurrences of vulnerability make system riskier; also, the Frequency of vulnerability depends on the date of emergence of vulnerability in the system [14]. The frequency and quantitative risk level of vulnerabilities determined by using the mathematical equations of Quantitative Security Risk Level Estimation Model [15], that computed temporal and environmental metrics to augment base CVSS scores and then derived a final risk value. The quantitative risk level score is ranging from 0 to 10; this numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

During the third phase of the proposed model, risk magnitude is measured by convergence of calculated likelihood of exploit and impact of exploit onto the system. Determined risk magnitude further used in the creation of remediation plans to validate identified vulnerabilities in order to improve system's security level. And finally, the risk assessment results are documented in an official report format which help senior management, the mission owners in making decisions on policy, procedural, budget, and system operational and management changes. As risk assessment is recursive procedure, this final generated report will be used as an input of phase1 of proposed framework in the next cycle of risk assessment procedure.

7. CONCLUSION

This paper proposed Quantitative Information Security Risk Assessment framework for University's Computing Environment. The goal of proposed model is to reduce risks of security breach, this means understanding the cause that makes system vulnerable. The proposed framework consists of three phases; in the first phase weak points of the system are identified and the threats and vulnerabilities are assessed by designing attack scenario specifically for higher educational institution's environments; in the second phase, risks are prioritized in order to create actionable remediation plan; the third phase of risk assessment model recognized the

vulnerability management compliance requirement in order to improve organization's security position. The proposed model quantitatively measured the risk magnitude for University's network configuration and can be used by risk analyst and security manager of University to perform reliable and repeatable risk analysis in realistic and affordable manner.

8. ACKNOWLEDGMENT

The authors are highly thankful to Madhya Pradesh Council of Science and Technology, Bhopal for providing financial grant and support for this research project.

9. REFERENCES

[1] Cisco Adaptive Threat Defense for Education Networks, whitepaper, Available : http://www.cisco.com/c/dam/en_us/solutions/industries/docs/higher_CampusSecure_defense_WP.pdf

[2] C. Alberts, and A. Dorofee, "An Introduction to the OCTAVE Method. Software Engineering Institute", Carnegie Mellon University, USA, 2010.

[3] C. Joshi and U. Singh, "A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System". International Journal of Advanced Research in Computer Science and Software Engineering (IJRCSSE) Volume 5, Issue 1, January 2015, pp 742-747.

[4] C. Joshi C. and U. Singh, "ADMIT- A Five Dimensional Approach towards Standardization of Network and Computer Attack Taxonomies". International Journal of Computer Application (IJCA, 0975 – 8887), Volume 100, Issue 5, August 2014, pp 30-36.

[5] B. Dixon, "Understanding the FAIR Risk Assessment", Nebraska CERT Conference 2009.

[6] Guide for Applying the Risk Management Framework to Federal Information Systems, U.S. Department of Commerce, February 2010.

[7] Prioritizing Information Security Risks with Threat Agent Risk Assessment, whitepaper, February 2010.

[8] C. Joshi and U. Singh, "Analysis of Vulnerability Scanners in Quest of Current Information Security Landscape" International Journal of Computer Application (IJCA, 0975 – 8887), Volume 145 No 2, July 2016, pp. 1-7.

[9] C. Joshi, and U. K Singh, "Performance Evaluation of Web Application Security Scanners for More Effective Defense" International Journal of Scientific and Research Publications (IJSRP), Volume 6, Issue 6, June 2016, ISSN 2250-3153, pp 660-667.

[10] CVSS v3.0 specification document, Available: https://www.first.org/cvss/specification-document.

[11] P. Mell, K. Scarfone, and S. Romanosky, "CVSS: A complete Guide to the Common Vulnerability Scoring System Version 2.0", Forum of Incident Response and Security Teams (FIRST), 2007.

[12] R. Marchany, "Higher Education: Open and Secure", A SANS Analyst Survey, June 2014.

[13] Overview of Vulnerability Scanners, whitepaper, Available: http://www.infosec.gov.hk/english/technical/files/vulnerability.pdf.

[14] U. K. Singh and C. Joshi, "A Framework for Security Risk Level Measures Using CVSS for Vulnerability Categories", accepted in ICCCNS 2016: 18th International Conference on Computer Communications and Networks Security.

[15] U. K. Singh and C. Joshi, "Quantitative Security Risk Evaluation using CVSS Metrics by Estimation of Frequency and Maturity of Exploit", The World Congress on Engineering and Computer Science (WCECS 2016) San Francisco, USA.

[16] U. K. Singh, and C. Joshi, "Measurement of Security Dangers in University Network", International Journal of Computer Applications, Volume 155, Issue1, pp.6-10, December 2016.