International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 02 - Issue 08 || August 2016 || PP. 06-14

A Review of Security Vulnerabilities, Controls and Models in Networked Environments

Samuel W. Ndichu[1], Dr Okoth Sylvester J McOyowo[2], Dr Cyrus Wekesa Wabuge[3]

[1]*PhD Student, School of Computing & Informatics, Maseno University, Maseno, Kenya*
[2]*School of Computing &Informatics, MasenoUniversity, Maseno, Kenya*
[3]*Department of Electrical and Information Engineering, University of Nairobi, Nairobi, Kenya*

ABSTRACT: The availability of information and communication technologies (ICTs) and network-based services offer a number of advantages in today's society, for example e-government, e-commerce, e-education etc. These ICTs and networks are used for storage and transmission of highly sensitive data which is a subject of interest to both authorized and unauthorized users. Hence security is necessary to ensure only authorized users get access to this data. Technological, configuration and policy vulnerabilities are experienced due to the rapid development and complexity of these networks, evolving technology and usage patterns, and changing hacking tactics. Despite the existence of various security mechanisms to secure the networked environments, unauthorized users still find their way into networked environments by exploiting vulnerabilities in networked environments causing serious damages and data loss. This paper performs a review of various networked environments, vulnerabilities, security controls and models with an objective of finding their gaps and suggests taking vulnerability management approach to secure networked environments.

KEYWORDS - control, ICTs, model, network, vulnerability

1. INTRODUCTION

The availability of Information and Communication Technologies (ICTs) and network-based services offer a number of advantages in today's society [1] in general, with ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment. These applications are considered as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. Low cost and reliable communication services have given boost to their widespread use in various walks of life. This has led to emergence of modern societies characterized by ubiquitous ICT and networked environments [2]. The significant spillovers and positive externalities associated with the proliferation of ICTs potentially influence all aspects of development through its effects on governance, markets, media, and public services [3]. ICTs and networked environments are increasingly playing an important role in organizations and in society's ability to produce, access, adapt and apply information. They are being seen as the tools for the post-industrial age, and the foundations for a knowledge economy, due to their ability to facilitate the transfer and acquisition of knowledge [4].

Security of ICTs, network infrastructures and data cannot be ignored in today's networked environments because of the untold number of security risks it has begun to create. Information security threats and cyber-attacks have become a recurrent phenomenon with governmental, nongovernmental, private, public, financial, academic and many other institutions being susceptible to cyber-crimes due to infrastructural, technological, policy, legal and configuration vulnerabilities. Threats are becoming more and more sophisticated and complex. Rapidly changing and evolving usage patterns that include increasing use of the cloud services, preference and use of tablets and mobile devices and introduction of terms like Bring Your Own Device (BYOD) into the modern work environments make it very challenging to understand both the modern threats and the modern threat landscape.

Network security problems can be divided roughly into five intertwined areas: confidentiality, authentication, integrity, availability, and nonrepudiation [5][6][7][8]. Many organizations are faced with various and recurrent security threats and cyber-attacks to their networked environments for political, financial or other malicious purposes. These lead to data loss, financial loss, down times and loss of business. Data Breaches continue to rank as a top threat to networked environments as more and more attackers successfully find their way into the networks.

Operational definition of terms:

- **Confidentiality** is also called secrecy; it is keeping information in networked environments out of the hands of unauthorized users.

- **Authentication** is determining whom you are talking to before revealing sensitive information in networked environments, ascertaining that the handler of information is who s/he claims to be.
- **Integrity** is ensuring that information in networked environments has not been modified by third parties and ensuring its correctness and completeness.
- **Availability** refers to being able to access information in networked environments whenever necessary, hence guaranteeing that the services offered can be used when needed.
- **Nonrepudiation** deals with signatures, it is being able to prove that someone made a request or a transaction in networked environments, which the person claims he never did.
- **Vulnerability** is a weakness that can potentially be exploited to gain access in networked environments [9][10].
- **Networked environment** refers to a system of interconnected computers [11].
- **ICTs** refer to information and the technologies that facilitate its exchange in networked environments; includes technologies, equipment and services that facilitate the electronic capture, processing, display, and transmission [12].
- **A Threat** indicates the potential for a violation of security in networked environments [11].
- **An attack** is an attempted violation, attackers use a set of rules and applications to break the security and create the weak points in networked environments [10].
- **E-Government** is the automation or use of ICTs to improve the activities and services of government where government services are delivered on-line to citizens using networked environments [13][14][15].

This paper presents a review of the vulnerabilities, security controls and models and a highlight of the weaknesses in the individual models. This paper also suggests vulnerability management approach as the way forward to securing networked environments. This can be implemented by means of vulnerability management model which can result with a more effective and economical approach to securing the networked environments.

2. NETWORKED ENVIRONMENTS VULNERABILITIES

These are weaknesses inherent in networks, networking devices or the networking controls. These weaknesses can either be technological, configuration or policy weaknesses. Some examples of these weaknesses include programing errors, configuration errors, compatibility errors and operation errors. Vulnerabilities can also result from actions of trusted employees defrauding a system, outside hackers or from careless data entry clerks. These vulnerabilities can be exploited by both internal and external sources [13][16][17]. This exploitation may be by means of ethical hacking, Trojan attacks, web hijacking, or logical bombing [10] inflicting various types of damage resulting in significant losses. The damage can range from errors harming database integrity, fires destroying entire computer centers, bad publicity to loss of business. Precision in estimating computer security related losses is not possible because many losses are never discovered and others are never reported or brought to the public domain to avoid unfavorable publicity. The effects of these vulnerabilities vary considerably; some affect the confidentiality or integrity of data while others affect the availability of a system [18].

This paper covers the following areas as shown in figure 1.

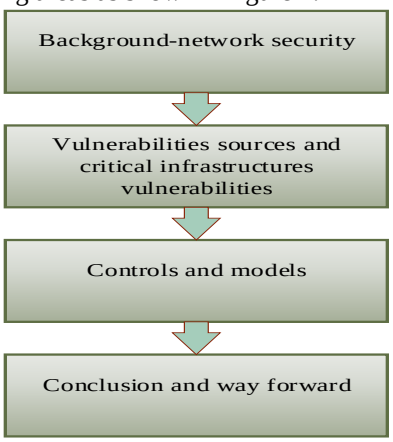

Figure 1: Areas covered by this paper

2.1 Sources of vulnerabilities

Vulnerabilities are experienced due to the rapid development and complexity of networks, evolving technology and usage patterns, and changing hacking tactics. Most ICTs and networks are developed in the private sector where security is not a priority during system design. Due to competition, manufactures or developers try as much as possible to reduce the time it takes to release these technologies to the market. This leads to ICTs and networks with in-built weakness or vulnerabilities and critical points of failure [19]. Therefore, ICTs and network vulnerabilities are to be expected. Technology is changing quickly resulting to less time between discovery of new vulnerabilities and the development or emergence of new tools or techniques to exploit these vulnerabilities. These tools and techniques used in exploiting these vulnerabilities are simple to use, inexpensive and widely available. Modern networked environments adopt multilayer network architectures and heterogeneous server environments in order to efficiently fulfill each organization's goals and objectives in their day to day operations. This complexity in ICTs and networked environments have resulted in increased demands for information security.

2.2 Vulnerabilities in critical infrastructures

Critical infrastructures include electrical power grid, telecommunications, financial services, networking services and the internet. Some of the countries with evolved ICTs and networked environments have experienced vulnerabilities and initiated suitable counter measures to deal with the vulnerabilities [2]. Examples of such vulnerabilities include prolonged disruption of electrical power during disaster leading to degradation or collapse of information infrastructure, communication overload during disaster leading to unacceptable delay or collapse of communication service, vulnerability to use of Radio Frequency Weapons (RFW) by terrorists or other disgruntled persons, vulnerability to information warfare and cyber terrorism through electronic media and physical damage by accidental, natural hazards or intentional sabotage. It has been well documented about the vulnerability of ICTs and networked environments to tools of information warfare or cyber terrorism [2][6][11]. Terrorists could use cyber-attacks to hurt the economy and political will severely as demonstrated by participants in a war game called Digital Pearl Harbor sponsored by Gartner and the U.S. Naval War College [20]. The players were drawn primarily from Gartner's client base and included people who manage the IT systems that are part of the critical infrastructure. The conclusions reached by the participants suggest that vulnerabilities in critical infrastructures stems from the vulnerability of software in use and from the availability of information on the Internet. Addressing vulnerabilities requires a comprehensive and collaborative approach. Security of ICTs and networked environments is a major technology concern [2].

3. NETWORKED ENVIRONMENTS SECURITY CONTROLS AND MODELS

3.1 A summary of the various networked environment security controls and models is discussed here:

3.1.1 Networked Environment Security Controls

According to [11], networked environments security controls include antivirus software's, secure network infrastructure, encryption, backup, regular Operating System (OS) updates, web browser updates, firewalls, IDS, IPS, passwords, security policies, proper configurations, etc. All these controls aim to safeguard the networked environments from the technological, configuration or policy vulnerabilities. Network security controls have proven be ineffective if applied as standalone controls. Hence the emergence of frameworks, standards and models which combines two or more of the security controls.

3.1.2 A General Model for Network Security [8]

For plain-text message to be sent across a network from one person to another, the two parties must cooperate. A communication channel is established. The communication channel is not secure since there is an eavesdropper (opponent) who presents a threat. To provide security, information to be sent is transformed for example by encryption and some secret information (encryption key) is shared by the two parties. A trusted third party responsible for distributing the encryption key and arbitrate disputes between the two parties will be important for security to be achieved. To design a security service, one needs to design an algorithm for performing the security related transformation, generate the encryption key to be used with the algorithm, come up with methods for the distribution and sharing and specify a protocol to be used. This model is meant for plain-text messages sent across a network from one person to another. The model is weak in that it concentrates only on one security mechanism; encryption, as a network security mechanism.

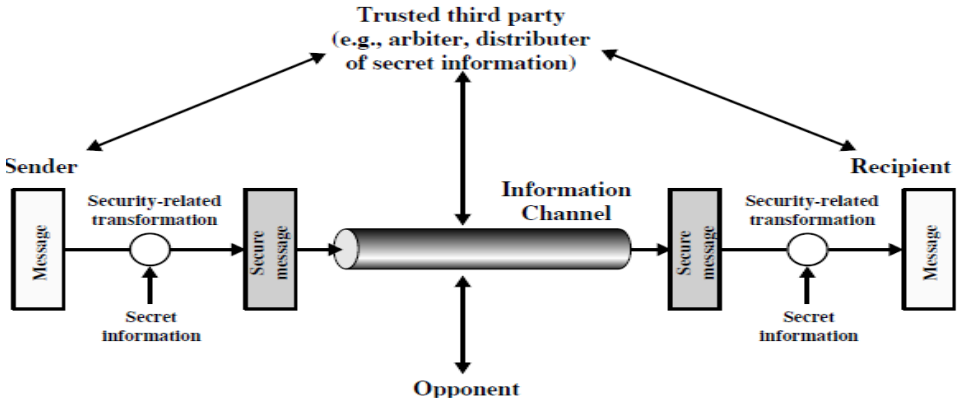

Figure 2: A general model for network security [8]

3.1.3 Network Security Model [21]

This is a seven layer model that divides the task of securing a network infrastructure into seven sections; (i) Physical (ii) Virtual Local Area Network (VLAN) (iii) Access Control List (ACL) (iv) Software (v) User (vi) Administrative (vii) IT Department. It works from top down to determine which layer may have failed and once the failure is found, it can be determined that all the layers above that particular layer have also failed. This will enable a network security professional to quickly determine if other possible hosts have been compromised with the breach of the layer and how to secure that layer against that particular attack in the future. This model provides a way to implement basic network security mechanisms, devices and locate underlying issues that may allow an attack to succeed, however, it fails to include Intrusion Detection System/Intrusion Prevention System (IDS/IPS) as part of the model and it is also more technologically oriented as a model for network security.

1) Physical
2) VLAN
3) ACL
4) Software
5) User
6) Administrative
7) IT Department

Figure 3: Network security model [21]

3.1.4 Security Model Based on Network Business Security [22]

The security defense of information system network of an enterprise includes the network of the information system and data security and the security of business running on the network of information system. These include confidentiality, integrity, continuity and real-time of network business [22]. It divides protection object of information security into three; data security; network security; network business security. New information security concept considers network business security as an important protection object in enterprise information network. In this model, network security is considered as a combination of security protocol, security service and security mechanism. This model describes a network business security theoretical study and research concept on information security, however, it concentrates only on the security of network process sets and data sets; the security of network processes running and writing operation on data sets. It does not put into consideration other aspects of network security.

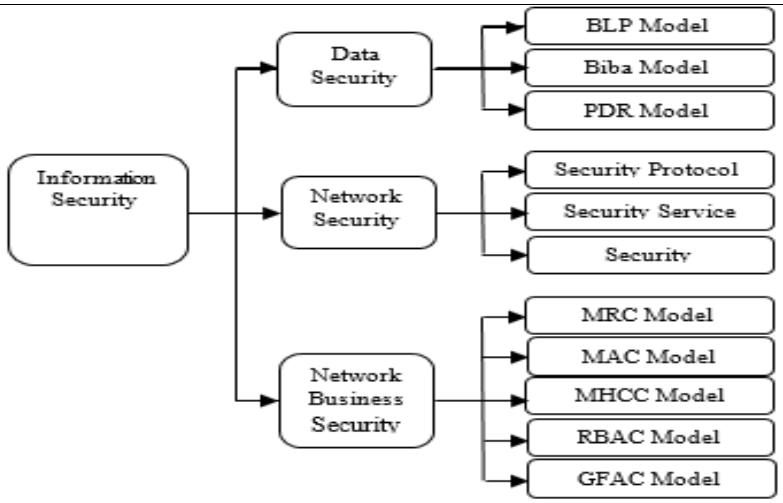

Figure 4: The information security system based on data, network and network business [22]

3.1.5 Evaluation of Vulnerability Assessment Model [10]

This model uses criteria for evaluating the web application infrastructure in cyber security with a lower password model which represents the intruder attempts. It adapts a method that requires security analysts to identify the bottlenecks of the system and the controls or mechanisms that are most effective to be implemented in the system. The method combines firewalls, Intrusion Detection System (IDS) and policy based rules. It also uses network monitoring IDS that is able to check port numbers and IP address when they access the network. This model explains the attacks from inside and outside and the effective counter mechanisms, but it has drawbacks in that the low level model may result in a user account lockout due to typographical errors from authorized users. Firewall, IDS and network monitoring based rules have been used widely in many systems but vulnerabilities are still being experienced which implies that this approach is still lacking.

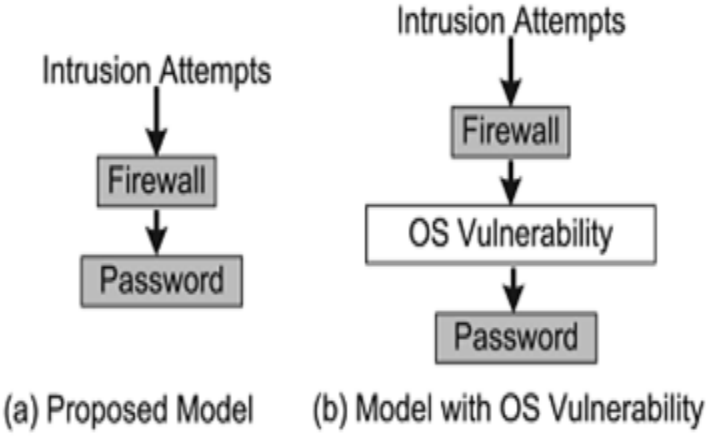

Figure5: Evaluation of vulnerability assessment model [10]

3.1.6 Network Security-A Layered Approach [23]

This approach is a technical strategy requiring adequate measures to be put in place at different levels within network infrastructures. The layered approach centers on maintaining appropriate security mechanisms and procedures at five different levels within IT department. These levels include perimeter, network, host, application and data. This approach however fails to put into consideration other aspects of network security such as configuration and policy management and concentrates only on the technological aspects of network security.

Security level	Applicable security measures
1. Perimeter	• Firewall • Network-based anti-virus • VPN encryption
2. Network	• Intrusion detection/prevention system (IDS/IPS) • Vulnerability management system • Network access control • Access control/user authentication
3. Host	• Host IDS • Host vulnerability assessment (VA) • Network access control • Anti-virus • Access control/user authentication
4. Application	• Application shield • Access control/user authentication • Input validation
5. Data	• Encryption • Access control/user authentication

Figure 6: The layered approach and the technologies that function on each [23]

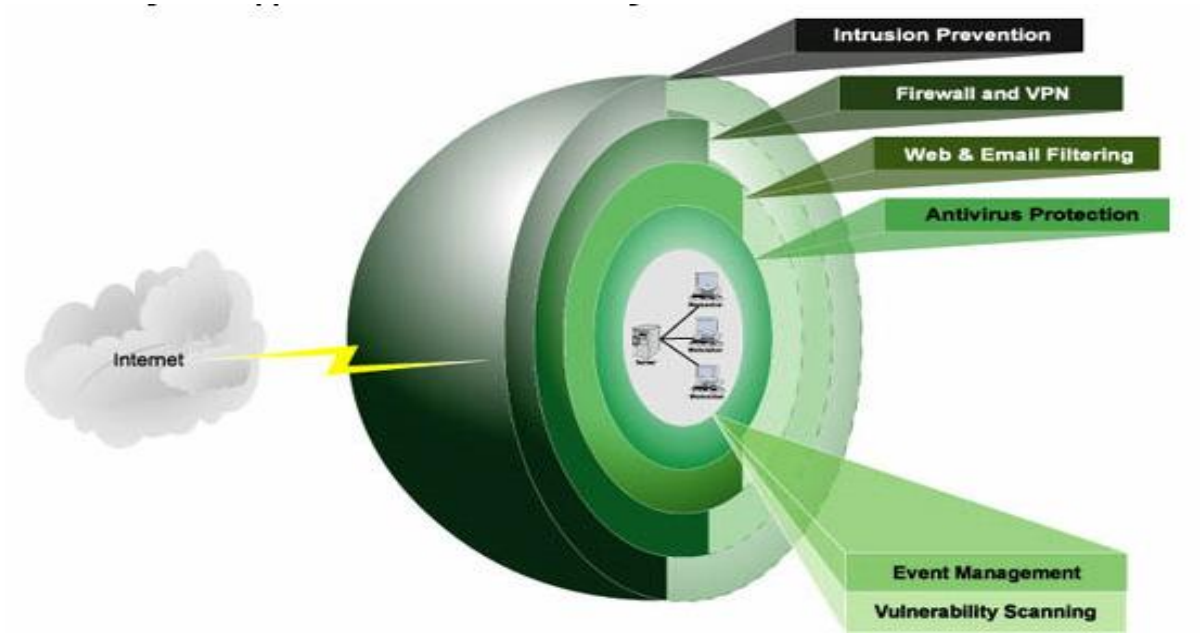

Figure 7: Network security-a layered approach [23]

3.1.7 Combined Security Model Tool for Adhoc Networks [24]

This model addresses security issues in an environment where devices remain in contact with each other for longer duration. The joining of a device is to be authenticated by a server owned by the organization. The objective is to define and categorize types of data transfer pertaining to general and role specific use respectively for sake of easiness and simplicity. The universal description, discovery, and integration (UDDI) channel is proposed to include registry information about the groups, given by the central server and propagated by the coordinator device. Each entry in the UDDI channel is identified by Keyi, and information within the channel is customized to fit wireless environments. The session channel contains the description of each session, and information within the session channel is indexed with a service key to enable better access performance. The data channel is used to transfer data among network devices. Whenever a device enters an ad hoc network, it downloads UDDI channels content to its device and stores it for later use. Caching the UDDI channels content

avoids frequent access to the channel and minimizes power consumption of the devices as well. Ad hoc network architecture with multi channels consists of a group of devices forming an ad hoc network through an authentication server for accessing services and information interchange among users. This model proposes a fully distributed approach to secure long term communities of devices. It however helps in providing security at only two levels:

- Authentication based on role
- XML embedded data transfer, which are independent levels and can be merged within one server or application hence simplifying security and secured data transfer within networks.

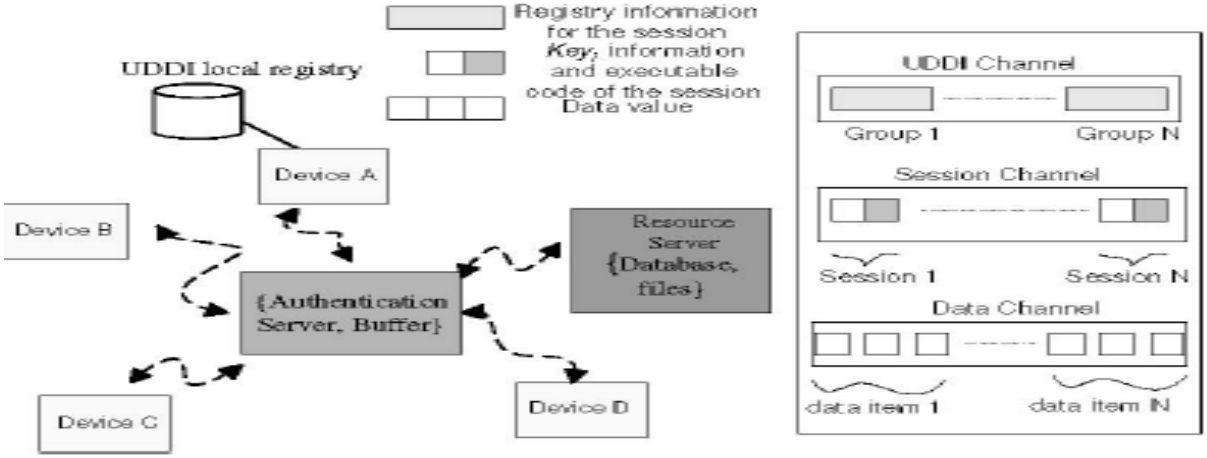

Figure 8: Adhoc network architecture with multi channels [24]

3.1.8 Security Model for Computer Network Based on Cluster Computing [11]

A cluster is a type of parallel or distributed processing system, which consists of a collection of interconnected stand-alone computers working together as a single integrated computer resource. The model identifies for different levels; end user external level; coherent rational level; in-house hardware level; and system connection level. It identifies these levels as the different security features needed to make cluster computing architecture secure.This model applies various security tools available in TCP/IP model on the different defined levels of cluster computing architecture for various types of security features. Every tool has its own security features. Applying these security tools with their security features on the different levels of cluster computing architecture makes a secure high performance computing system, however, this model is a scheme for specifying and enforcing security policies. Every security tool has its own constraints which are also inherent to the model.

TCP/IP Model	Security Tools	Security Features	Cluster Computing Architecture Levels
Application Layer	Kerberos S/MIME PGP SET	User Validation Access Permission System Discretion	End User External Level
Transport Layer	SSL/TLS	Packet Seclusion Message Integrity Channel Reliability Single User Access Firewall Prevention	Coherent Rational Level
Internet Layer	IPSec	Secure Network Signing Internet Protocol Addressing	In-House Hardware Level
Network Interface Layer	CheckSum	Network Authentication Server & Client Authorization	System Connection Level

Figure 9: Security model for computer network based on cluster computing [11]

3.2 Other Security Mechanisms, Standards and Approaches

Many security mechanisms, standards and approaches have been developed due to requirements in networked environments security [5]. Security standards and certifications which do not cater for the current ICT complexities and threats are still being used by some organizations (e.g. ISO/IEC 17799). Standards such as BS 7799, COBIT [25], ISM3 [26], ISO/IEC27001 [27], ITIL [28],PCIDSS developed by international organizations exist. ISO/IEC 27001 [27] being the latest standard introduces security policy life-cycle. Use of firewalls to eliminate the various attacks, filtering algorithm to secure against email bombing and server system security to avoid hacking [10] is common, but attacks are still finding their way into networks. Regular updates are necessary but mis-configurations and design flaws cannot be located and patched making the whole network vulnerable to attackers. Security regulations, privacy and data protection policies impose a number of obligations and are important to organizations [29]. Attacks cannot be controlled by use of technology and scientific solutions alone, the right synergy of people, process and technology would create well prepared attack resistant systems [2]. The protection of data in transit and or in storage is important in networked environments. Information security is much more than implementation of usernames and passwords and up to date software and hardware [30][31]. Networked environments today are dynamic with various emerging threats. Technology today is changing radically which calls for equally dynamic security mechanisms and methods to safeguard today's networked environments [5][7].

4. CONCLUSION

The security controls and models reviewed here have been developed to secure ICTs and networked environments.The security controls reviewed include antivirus software's, secure network infrastructure, encryption, backup, regular Operating System (OS) updates, web browser updates, firewalls, IDS, IPS, passwords, security policies, proper configurations, etc. the models reviewed adopt either one or a combination of security controls. These security controls and models all aim to achieve confidentiality, integrity and availability in networked environments. However, despite the fact that these controls are in existence and being used, unauthorized users still find their way into networked environments by exploiting vulnerabilities in networked environments thereby causing serious damages and data loss. This paper suggests taking vulnerability management approach to secure networked environments and point's towards development of a vulnerability management model that addresses remote data access vulnerabilities inherent in networked environments.This approach will be more effective and economical compared to existing approaches. Also, a vulnerability management model will ensure protection of confidentiality, ensuring integrity and maintaining availability in networked environments.

REFERENCES

[1] Mellado, D., Blanco, C., Sanchez, L. E. and Medina, E. F. (2010). A Systematic Review of Security Requirements Engineering. Computer Standards and Interfaces, Volume 32, Issue 4, June 2010, ISSN: 0920-5489, Pp.153-165.

[2] Chaturvedi, M. M., Gupta, M. P. and Bhattacharya, J. (2006). Analysis of Information and Communication Technology Infrastructure (ICT) Vulnerabilities in Indian Context, Towards Next Generation E-Government, Privacy and Security. Computer Society of India, Pp.192-202.

[3] Maximo, T. C. and Joachim, V. B. (2006). Information and Communication Technologies for Development and Poverty Reduction. The Potential of Telecommunications, International Food Policy Research Institute (IFPRI), ISBN 0-8018-8041-6, ISBN 0-8018-8226-5.

[4] Morales-Gomez, D. and Melesse, M. (1998). Utilizing Information and Communication Technologies for. Development: The Social Dimensions, Information Technology for Development, 8(1), Pp.3-14

[5] Alghazzawi, D. M., Syed, H. H. and Trigui, M. S. (2014). Information Systems Threats and Vulnerabilities. International Journal of Computer Applications (0975-8887), Volume 89, № 3, March 2014.

[6] Krishnan, K. (2004). Computer Networks and Compute Security. SFWR 4C03, March 2004, Pp.19-21.

[7] Mellado, D. and Rosado, D. G. (2012). An Overview of Current Information Systems Security Challenges and Innovations, JUCS Special Issue. Journal of Universal Computer Science, Volume 18, № 12, 2012, Pp.1598-1607.

[8] Stallings, W. (2003). Cryptography and Network Security. Principles and Practices, 3rd edition, Prentice Hall, NJ, 2003.

[9] Cheng, L. S. B. (2009). Cyber Attacks, Why, What, Who and How. IT Pro, May-June 2009.

[10] Suma, C. M. (2010). Evaluation of Vulnerability Assessment in System from Hackers in cyber security. International Journal of Engineering Science and Technology, Volume 2(7), 2010, Pp.3213-3217.
[11] Thalod, S. K. and Niwas, R. (2013). Security Model for Computer Network Based on Cluster Computing. International Journal of Engineering and Computer Science, ISSN: 2319-7242, Volume 2, Issue 6, June 2013, Pp.1920-1927.
[12] Maximo, T. C. and Joachim, V. B. (2006). Information and Communication Technologies for Development and Poverty Reduction. The Potential of Telecommunications, International Food Policy Research Institute (IFPRI), ISBN 0-8018-8041-6, ISBN 0-8018-8226-5.
[13] Heeks, R. (2004). E-Government for Development as a Carrier of Context. Institute for Development and Policy Management, University of Manchester, UK 2004, ISBN: 1-904-143-46-6, 978-1904143-56-8, P.15.
[14] InfoDev, (2002). The E-Government Handbook for Developing Countries, A project of InfoDev and the Centre for Democracy and Technology, November, Washington, D.C. 2002.
[15] Zaied, A. N. H., Khairalla, F. A. and Al-Rashid, W. (2007). Assessing e-Readiness in the Arab Countries: Perceptions Towards ICT Environment in Public Organizations in the State of Kuwait. The Electronic Journal of e-Government, Volume 5, Issue 1, Pp.77 – 86.
[16] McNamara, R. (1998). Networks, Where does the real threat lie? Information Security Technical Report, 3(4), Pp.65-74.
[17] Yeh, Q. and Chang, A. J. (2007). Threats and Countermeasures for information system security, A cross-industry study. Information and Management, 44, Pp.480-491.
[18] The NIST Handbook. An Introduction to Computer Security, National Institute of Standards and Technology, Technology Administration. U.S. Department of Commerce. Special Publication, 800-12.
[19] Naf, M. (2001). Ubiquitous Insecurity, How to Hack IT Systems. Information and Security: An International Journal, № 7, Pp.104-118.
[20] Purchase, E. and Caldwell, F. (2002). Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack, Guarding Your Business. A Management Approach to Security, Part II, 2004, ISBN 978-0-306-48494-0, 978-0-306-48638-8, Pp.47-64.
[21] Backfield, J. (2008). Network Security Model. SANS Institute 2008.
[22] Kehe, W., Zhang, T., Wei, L. and Gang, M. (2009). Security Model Based on Network Business Security. Computer Technology and Development, ICCTD '09. IEEE International Conference, Volume1, Nov. 2009, Pp.577-580.
[23] Bala, K., Barjeena, L. and Surinder, P. G. (2010). Network Security-A Layered Approach, Advanced Network Technologies. Proceedings of ISCET 2010, ISBN: 978-81-910304-0-2.
[24] Maturi, K. K., Mukiri, R., Rao P. S. and Shaik, B. (2011). Combined Security Model Tool for Adhoc Networks. International Journal of Computer Science and Information Technologies, Volume 2(3), 2011, Pp.987-991.
[25] COBITv4.0, (2006). Information Security Audit and Control Association. Cobit Guidelines.
[26] ISM3, (2007). Information Security Management Maturity model, v.2.0. ISM3 Consortium, Handbook.
[27] ISO/IEC, 27001. (2005). Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC JTC 1/SC 27.
[28] ITILv3.0, (2007). Information Technology Infrastructure Library-ITIL.
[29] Heru, S. and Fahad, M. (2010). Multimedia Information Security Architecture Framework. Future Information Technology-FutureTech. 2010 5th International Conference, May 2010, Pp.1-6.
[30] Bechtsoudis, A. and Sklavos, N. (2012). Aiming at Higher Network Security through Extensive Penetration Tests. Latin America Transactions, IEEE (Revista IEEE America Latina), Volume 10, №3, April 2012, Pp.1752-1756.
[31] Solms, B. and Solms, R. (2004). The 10 Deadly Sins of Information Security Management. Computers & Security, Volume 23, Issue 5, July 2004, Pp.371–376.