Securing Wireless Networks in African Universities: A Case Study of Universities in Kenya

Samson Otieno Ooko
University of Eastern Africa, Baraton

Securing Wireless Networks in African Universities: A Case Study of Universities in Kenya

Otieno Samson Ooko
Department of Information Systems and Computing, School of Business,
University of Eastern Africa, Baraton
Eldoret, Kenya
Email: ookosoft@gmail.com

Metto Shadrack
Department of Information Technology, School of Information Sciences, Moi University
Eldoret, Kenya.
Email: ksmetto@gmail.com

Ataro Edwin O
Department of Electrical Engineering, School of Technology, Moi University,
Eldoret, Kenya.
Email: edwin.o.ataro@gmail.com

Abstract - Many learning institutions are increasing deploying wirelesses networks due to its advantages. Securing wireless networks is always a challenge, there is therefore a need to come up with lasting solutions towards ensuring that these networks are secured. This study focused on finding out underlying insecurity issues with the aim of proposing the best solutions for mitigating the threats. From the review of literature relating to security of wireless networks it was evident that this problem cuts across all industries necessitating the need for the study. The objectives of the study were: To investigate security threats associated wireless networks in universities and to propose measure that can be put in place to ensure secure university networks. The study was based on the Game Theory that was pioneered by Princeton mathematician John Von Neumann. A qualitative research design was used with data being collected using interviews, observation and analysis of documentations and related researches. A review of data collected from different universities in Kenya was analyzed to find out the vulnerabilities identified and thereafter solutions to mitigating the network security problems proposed.

Keywords: Networks, Wireless, Network Security, Africa

I. INTRODUCTION

The use of wireless networks is becoming popular among users today including in universities and other learning institutions. Chloi et al, 2008 notes that there are increasing threats and attacks to wireless networks a factor that led to stunted wireless deployment rate in enterprise environments in the past few years. According to Tobana, 2010 the increasing cases of wireless security is a result of laziness and sometimes due lack of knowledge among those installing and using the networks. Since most users may not understand the security risks that come with an insecure wireless network but are more concerned with getting connections to resources, security is usually considered last by many.

According to cybersecurity reports from different regions there have been increasing reports of cybercrime from many African countries. The criminals are not only targeting computers but are also targeting the information stored and transmitted over the networks. Whether the source of an attack is an insider, a hacker, or a terrorist, the consequences are often the same—loss of revenue, loss of sensitive information, erosion of consumer and constituent confidence, interruption or denial of business operations (Kigen, Kisutsa et'al. 2014).

The use of mobile computer devices has been on the rise and, as a result, traditional ways of networking have proven inadequate to meet the challenges posed by the new lifestyles and professional interactions. If users must be connected to a network by physical cables, their movement is drastically reduced. Wireless connectivity, however, poses no such restrictions and allows a great deal of more free movement on the part of a network user (Gast, 2010). According to Wi-Fi Alliance (2013), 87% of U.S. youth aged between 18 and 29 years polled said they needed to have access to wireless networks in institutions.

Wireless campus networks are like any other public Wi-Fi network that's full of strangers. But students in many parts of the world are often unaware that some of the college wireless networks they connect to are not secure. Cyber criminals are not only focusing on wireless networks. They are also targeting college and university databases, one of the richest sources of information for identity theft. Between 2008 and 2010, dozens of higher education institutions like the University of Florida, Purdue University and UC Berkeley experienced 158 data breaches that compromised 2.3 million records (Legnitto, 2011).

In March 2014, a student at Florida State University Panama City was facing felony charges after he hacked the university's wireless network and rerouted users to a porn site to expose flaws in the school's security system (Roberts, 2014). According to a report by Cyberoam with presence in more than 125 countries, placed Kenya among African countries leading in cyber-attacks with some of the attacks attributed to wireless networks, after Egypt, Morocco and South Africa, with two Kenyan universities topping the list.

The objectives of the study were: To investigate security threats associated wireless networks in universities and to propose measure that can be put in place to ensure secure university networks.

The result of this study will help universities towards ensuring the wireless networks.

II. METHODOLOGY

This study was conducted using qualitative research design so as to get an in-depth data and information about the security of networks in the participating institutions.

The population sample size from a target population of 30 and 17 public and private universities respectively was generated using the Slovin's formulae as indicated below:

n=30/(1+30(0.21)2   and n=17/(1+17(0.25)2

n= 13 for public universities and n=8 for private universities

The universities were selected to participate in the research based on their firsthand experience of the phenomenon of interest. For the purpose of the study the based on data from the Kenya Education Network the participants were selected because they had installed functioning wireless networks.

The main data collection tools included Interview schedules, observation, practical experiments and document analysis guide

The qualitative data generated from the interviews and observation and practicals was transcribed and grouped. It was then analyzed based on the research questions and developed themes. Content and thematic analysis was used to analyze the data and make inferences by objectively and systematically identifying characteristics of responses.

III. Results

The main findings some of the noted security concerns included but were not limited to the following:

- Many institutions are not aware of the specific risks that they face during the day to day operation of the networks.
- Evidence of upgraded wireless software and uninstalled patches were noted.
- Many institutions had not conducted security assessments and were therefore not able to identify the corrective actions on time and thus are not able to maintain an acceptable level of security.
- Even though the universities had inventory of the wireless devices, evidence of rogue access points were noted in the networks
- The methods of disposals used e.g keeping in storage and donations pose a security risk for the universities
- Management of guest user accounts did not adhere to industry standards
- Many user in the universities lacked security awareness and training, this may imply that the users were not able to establish good security practices to prevent inadvertent or malicious intrusions into universities network and information systems.
- It was noted that some institutions did not have any network monitoring mechanisms. Without the insight that good monitoring tools and techniques provide, the universities cannot understand the effects that changes will make.
- Authentication methods used in some of the universities are not very secure and are not combined with any encryption methods. It was also interesting to note that the universities put more emphasis on access to the network; once the users are authenticated there were limited measures in place to ensure security of the connected users and systems.
- On different devices there were many ports that were open but not in use providing backdoors for possible breach in security of the network.
- Some universities also used a common and/or default password for multiple Aps making them vulnerable.
- The estimated usable range of each AP extended beyond the physical boundaries of the facility where installed with channels were overlapping for different APs
- Some universities were Broadcasting SSID with leading name such as office and department names that are likely to attract attention of potential hackers.
- Most universities used insecure and nonessential management protocols which are potential methods that an adversary can use when attempting to compromise an AP.

IV. Conclusion

From the findings of the study it was evident that the security of wireless networks in the universities is wanting. There has however been some effort that have been put in place by different universities to ensure security of the networks.

To mention but a few, the security concerns included: Limited risk assessments, Installing patches and upgrades without testing, limited security assessments, Poor disposal practices, inadequate security and access policies, Inadequate user awareness and training on wireless network security, Insufficient monitoring strategies, Insecure authentication methods, Open unused ports, use of one off passwords, overlapping channels, broadcasting beyond boundaries, insecure management protocols and broadcasting leading SSIDs.

This therefore calls for network administrators to do extra work to ensure security of the networks. The results of this study will come a long way towards ensuring secure networks.

V. Recommendations

To ensure university networks are secured the researchers recommends the use of a Wireless Network Security Model. The specific recommendations from the findings of the study have been classified into the layers of the WNSM in which they should be implemented.

A. The Physical Layer

From the findings of the study many universities had physically secured there networks however the researcher recommends the following:

Aps should be configured in different channels to avoid overlaps and located in appropriate places to prevent broadcasting beyond boundaries.

SSIDs should be hidden and when broadcast they should not reflect the institutions and departments they serve

B. Network Layer

The researcher recommends that wireless networks should be on separate VLANs for specific group of users.

C. Authentication Layer

The researcher recommends the following:

The Universities should undertake a risk assessment to enable them find out the risks that they face during the day to day operation of the networks

Secure authentication methods should be integrated with secure encryption methods to ensure improved security

Adequate firewalls that will ensure all ports not in use are blocked should be put in place

D. Software Layer

The researcher recommends that all devices should be frequently upgraded and before installing any patches and upgrades the universities should conduct tests to ensure all bugs are eliminated.

E. User Layer

The researcher recommends that universities should conduct frequent trainings and introduce awareness programs on network security from time to time

F. Management Layer

The researcher recommends that universities should train the staff on regular basis to keep up with the changing technologies.

G. Administrative Layer

Based on the findings of the study the researcher recommends the following:

1) The universities should conduct frequent security assessments to be able to identify the corrective actions on time

2) Appropriate policies should be formulated by the universities. These should include Security Policies, Access Policies, Acceptable use policies, Disposal Policies, Password Policies, Guest Access Policies

3) The universities should use the online tool to the assess the security of their networks so as to find recommendations specific to each university

4) Universities should put in place efficient monitoring techniques and review from time to time

5) Universities should use secure management protocols

REFERENCES

1. Aubuchon, K. (2011, August 29). Infosec Island. Retrieved July 15, 2014, from Universities Account for a Higher Number of Breaches: http://www.infosecisland.com/blogview/16161-Universities-Account-for-a-Higher-Number-of-Breaches.html

2. CUE. (2017, December). Commission for University Education. Retrieved 15 October, 2017, from Universities Authorized to Operate in Kenya, 2017: http://www.cue.or.ke/services/accreditation/status-of-universities

3. Flickenger, R. (2002). Building Wireless Community Networks. Sebaspotal.

4. Fogie, S. (2003, May 23). Security Reference Guide. Retrieved May 22, 2014, from InformIT: http://www.informit.com/guides/content.aspx?g=security&seqNum=162

5. Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007). Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Gaithersburg: National Institute of Standards and Technology.

6. Gast, M. (2010). 802.11 Wireless Networks: The Definitive Guide.

7. Hamilton, S. N., Miller, W. L., Ott, A., & Saydjari, O. S. (2002). The role of game theory in information warfare. Proceedings of the 4 th information survivability workshop. ISW-2001/2002.

8. Karygiannis, T., & Owens, L. (2002). Wireless Network Security 802.11, Bluetooth and Handheld Devices. Gaithersburg: National Institute of Standards and Technology.

9. Kashorda, M., & Waema, T. (2014). E-Readiness Survey of Kenyan Universities (2013) Report. Nairobi: Kenya Education Network.

10. Kigen, P., Kisutsa, C., Muchai, C., Kimani, K., & Mwangi, M. (2014). Kenya Cyber Security Report 2014: Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring.". Nairobi: Serianu Ltd.

11. Kornkaew, A. (2012). Management Information System Implementation Challenges Sucess Key Issues, Effects and Consequences. Jonkoping University.

12. Liang, X., & Xiao, Y. (2013, January). Game Theory for Network Security. IEEE Communications Surveys & Tutorials.

13. Masai, J. (2016, December 10). Campus Wireless Security. (S. Ooko, Interviewer)

14. Nanda, S. (2013, 2 17). Wireless Insecurity. Retrieved 8 12, 2014, from How Johnny can hack your WEP protected 802.11b Network!

15. Oblinger, D. (2003). Computer and Network Security in Higher Education. Jossey-Bass Inc.

16. Osborne, M. (2003). An Introduction to Game Theory. New York: Oxford University Press.

17. Polit, & Hungler. (2003). Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. Sweden: Elsevier Inc.

18. Republic of Kenya. (2013). Kenya Gazette Supplement No. 192 (Acts No. 42). In R. o. Kenya, The Universities Act, 2012 (p. 1891). Nairobi: Republic of Kenya.

19. Ross, D. (2005). The Security of Wireless Computing Technolgies. AusCERT Conference.

20. Scarfone, K., & Dicoi, D. (2007). Wireless Network Security for IEEE802.11a/b/g and Bluetooth. NIST Special Publication 800-48 Revision 1.

21. Sindhuh, E. S. (2013). Analysis of the Effect of Wireless Campus Networks on Internet Usage in Kenyan Universities. Nairobi: Unpublished.

22. Tabona, A. (2010). An Overview of Wireless Network Security. New York: NIST.

23. Wack, J., Tracy, M., & Souppaya, M. (2003). Guideline on Network Security Testing. Gaithersburg: National Institute of Standards and Technology.

24. Weiss, J. (2002). Wireles Networks: Security, Problems and Solutions. SANS Institute.