SJIF IMPACT FACTOR: 2.92 CRDEEP Journals
International Journal of Research in Engineering and Management Ooko et. al., Vol. 2. No. 1 ISSN: 2456-1029
*International Journal of Research in Engg. & Mgmt. Vol. 2 No. 1. 2017. Pp. 1-10*


*Full Length Research Paper*

# Security of Wireless Campus Networks in Selected Public and Private Universities in Kenya

**Otieno Samson Ooko[1*], Ataro Edwin O[2] and Metto Shadrack[3]**
[1]*Department of Information Systems and Computing, School of Business, University of Eastern Africa, Baraton, Kenya.*
[2]*Department of Electrical Engineering, School of Technology, Moi University, Kenya.*
[3]*Department of Information Technology, School of Information Sciences, Moi University, Kenya.*

**Article history**
*Received: 02-11-2017*
*Revised: 07-11-2017*
*Accepted: 20-11-2017*

**Corresponding Author:**
**Otieno Samson Ooko**
*Department of Information Systems and Computing, School of Business, University of Eastern Africa, Baraton, Kenya.*

***Abstract***
*Because of the uncontrolled medium of wireless networks there have been increasing cases of hacking and unauthorized access of wireless campus networks thus investigating into wireless campus network security is an essential step to ensuring wireless network security. This study therefore focused on identifying if there were vulnerabilities so that lasting solutions could be found to secure organizational data and communication. The aim of this study was to investigate the security of wireless campus networks in selected universities in Kenya and thereafter proposed solutions for ensuring improved security of the networks. A review of related literature showed that there were many attacks that had been targeting wireless networks in all sectors, However, no studies had been conducted specifically on security of wireless campus networks thus the need for this study. A qualitative research design was used in this study, with qualitative data being collected using interview schedules, observation, practical experiments and document analysis. Data was collected from twelve public and eight private universities that were purposively selected based on their investment on wireless networks. The findings of the study showed that the campus wireless networks were insecure and recommendations to improve on the security given.*

***Keywords:*** *Networks, Wireless, Network Security, University*

**Cite this article as:** Otieno S. O, Ataro E. O and Metto S .(2017). Security of Wireless Campus Networks in Selected Public and Private Universities in Kenya. *International Journal of Research in Engineering and Management, 2*(1), 1-10. Retrieved , from www.crdeepjournal.org/ijrem

## Introduction

Wireless networks are gaining popularity to its peak today, as the users want connectivity in terms of wireless medium irrespective of their geographic position. There is an increasing threat and various attacks on the Wireless Network (Choi et. al, 2008). Security of wireless networks ensures that the same level of data integrity and confidentiality as a wired network is maintained. Without properly implemented security measures, malicious users may gain access to network resources and data. Widely reported and easily exploited holes in the standard security system have stunted wireless deployment rate in enterprise environments (Singh et. al, 2014). The current wireless access points present a larger security problem than the early internet connections. This amount of insecurity in wireless networks may be rounded down to laziness and lack of knowledge; people are not aware of these things (Tabona, 2010). Overlooking wireless security is like leaving the front door to one's house permanently open with little or no security. Insecure wireless networks can allow anyone in range to sniff network packets, read someone's e-mails, use internet for free, and even gain access to another's files.

Every day there are new wireless networks installed in campuses. Unfortunately for most of wireless networks, security is an afterthought. The reason for this is that most wireless users do not understand the risks associated with using or setting up an insecure and open network (Fogie, 2003). In the recent past a huge rise in cyber-criminal activity targeting both public and private organizations in Kenya has been witnessed. Criminals are not just targeting computers, they are targeting the information that the networks store and transmit. 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 et'al. 2014).

With the continued use of portable information technology devices, such as laptops and smartphones, in Kenyan universities and the growing popularity of the internet, online and mobile applications, wireless networks are becoming more popular as a means of accessing different services, applications and academic materials over the internet. So there is an increasing need to ensure the networks are secure.

With the increasing use of ICT in management, universities store an increasing volume of sensitive information relating to students, employees and research activities. These information resources used to be accessed directly on work stations before, but with the growing use of the internet, most universities in Kenya use wireless networks to access the internet and online applications used in the institutions (Kashorda & Waema, 2014). However, a number of problems have resulted from insecure wireless campus networks
For example, in the recent past a number of cases of people hacking into university networks to access student online account details have been reported in many universities, including in universities in Kenya. Security researcher Kurt Aubuchon did a search of publicly reported breaches that happened between 2009 and 2011, and even when excluding inside jobs (namely staff or students hacking the network), universities are hacked 357 times more than would be expected, if breaches were distributed evenly among US firms (Aubuchon, 2011).

A report by Cyberoam, a global Network Security appliances provider, with presence in more than 125 countries, placed Kenya among African countries leading in cyber-attacks, after Egypt, Morocco and South Africa, with two Kenyan universities topping the list. The report noted that hackers tamper with school systems to adjust grades and fee balances and that hacking had become a booming business in schools, especially towards the end of semester and during the graduation period (Letoo, 2015).
A compromise in security may not only lead to loss of personal data but also loss of confidentiality of an institutions' data. Cyber security is one of the areas that need to be looked into with proper solutions, including identifying the minimum level of security for any learning institution (Letoo, 2015). Therefore, there was a need for an investigation on how secure the wireless networks in the universities in Kenya are so as to mitigate the security threats in future to ensure privacy of network users, confidentiality, and integrity of institutional databases and availability network services.

The aim of this study was to investigate the security of wireless campus networks in selected universities in Kenya thereafter proposed solutions for ensuring improved security of the networks.

*The objectives of the study were:*

1. *To identify the security risks associated wireless campus networks in the selected universities in Kenya;*
2. *To assess the security measures in place for wireless campus networks in the selected universities in Kenya;*
3. *To determine the vulnerabilities of wireless campus networks in the selected universities in Kenya; and*
4. *To propose measures and for ensuring improved security of wireless campus networks in the universities.*

The result of this study will not only be used by different universities towards ensuring the wireless campus networks are well secured but also by other organization as a guide towards improving wireless network security. With network security in place, Universities will experience many benefits. The University is protected against business disruption by ensuring availability. Network security helps protect universities and students data, it reduces the risk of legal action from data theft. Ultimately, network security helps protect a universities' reputation.

**Research Methodology**
A qualitative research design was used given the fact that little is known about the security of wireless campus networks in Kenyan universities. The target population comprised of the 23 chartered public universities and 16 chartered private universities in Kenya.
The sample size was generated by applying Slovin's formula (1843) was used as follows:
*n = N / (1+Ne2).*
*n = no. of samples*
*N = total population*
*e = error margin / margin of error*

The population sample size for the population of 23 and 16 public and private universities respectively is therefore:
*n=23/(1+23(0.21)2 and n=16/(1+16(0.25)2*

n= 12 for public universities and n=8 for private universities
Purposive sampling, a procedure that involves the selection of universities that represent the desired population, was used. This is a non-probability sampling method which involved the conscious selection of certain subjects to be included in the study. For the purpose of the study the participants were selected because they had installed operational wireless campus networks based on data

obtained from the Kenya Education Network. Interview schedules, observation, practical experiments and document analysis guide were used as the main tools for collecting data. The selection of these tools was guided by the nature of the data to be collected, the time available as well as by the objectives of the study. For quality control, the research instruments were piloted in one institution and modified to improve their validity and reliability. The qualitative data generated from the interviews and observation 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.

**Results**

Data was collected from all the selected thirteen public universities and of the eight selected private universities data was collected from seven. It was noted that most private universities we reluctant in sharing information on their wireless network security.

*Risk Assessment*

It was found out that many universities had not performed any risk assessments but only rely on the published risks associated with wireless networks. Some of the major risks identified included; Data interception, cracking transmission and denial of service attacks

*Patches and Upgrades*

There was evidence of upgrades that had not been done in some institutions while others had patched their software to the latest versions as shown in the diagrams below.

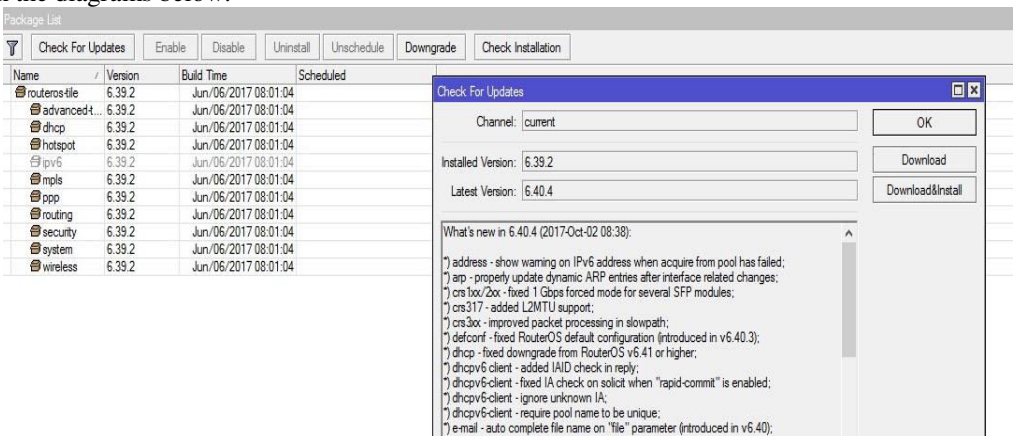


**Fig 1:** Wireless router upgrade status

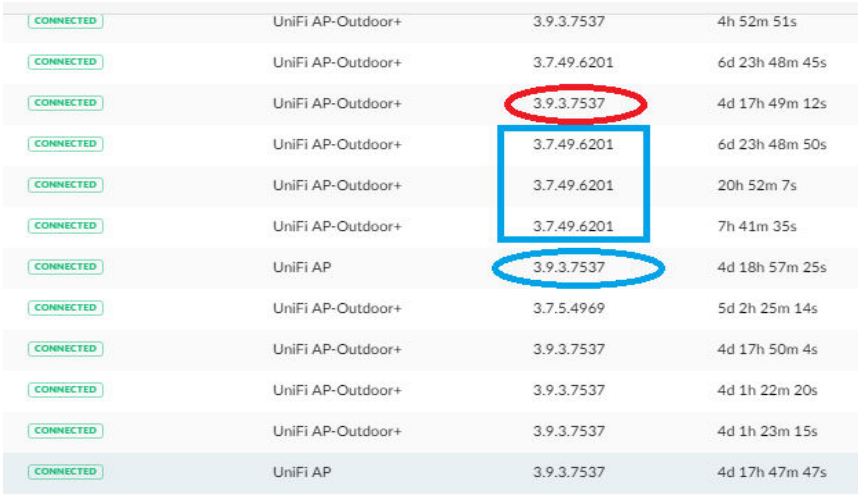


**Fig 2:** Wireless Access Points upgrade status

*Security assessment*

Many institutions had not conducted any security assessments for the wireless networks. This was attributed to lack of a specific tool to carry out a comprehensive assessment.

*Inventory*

From the practical tests the researcher was able to identify rogue Aps in some institutions. For example, in the image below the AP with SSID Josephine was a rogue AP installed by a student in the halls of residence.

| SSID | MAC Address | RSSI | Chan | 802.11 |
|---|---|---|---|---|
| MarriedQuaters_Hc | 00:27:22:32:58:ED | -86 | 6 | b, g |
| Married Quarters1 | 00:27:22:32:58:EF | -83 | 6 | b, g |
| AndroidAP | 88:AD:D2:32:03:C0 | -88 | 1 | b, g, n |
| Josephine | A4:2B:B0:B9:CA:9C | -89 | 4 | b, g |

**Fig 3:** Rogue Access Points

*Disposal*

On disposal of devices no longer in use the responses were: they are kept in storage, forwarded to the procurement department or donate to other institutions and organizations.

*System logs*

Many institutions reviewed their security logs, this enabled the security and support staff to identify potential security issues and respond accordingly as shown below.

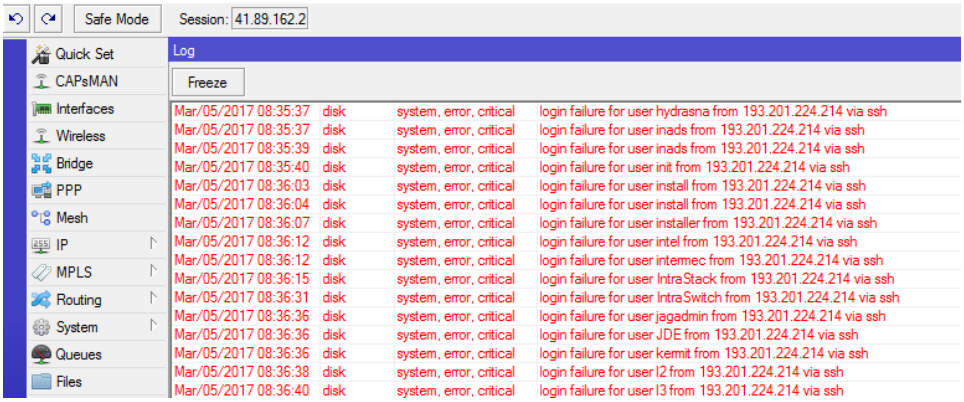


**Fig 4:** Wireless Router System Log

Some universities used automated logging tools to assist with log review and send real-time alerts in response to critical events. Events tracked included failed authentication attempts and MIC failures as shown below.

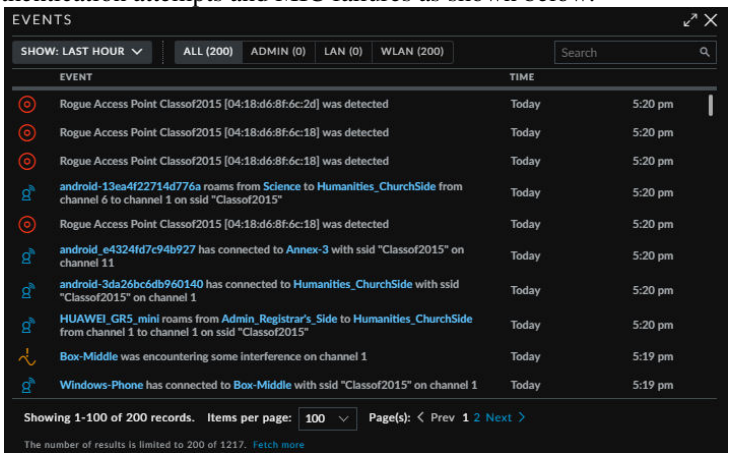


**Fig 5:** Automated system logging

*Network separation*

A majority of the universities used dedicated VLANs which facilitated the use of network access control lists, which identified the protocols and services that were allowed to pass from WLANs to the DS. Different VLANs were defined within the wireless connections to further separate varying security policies.

*Guest access*

Most universities did not have the best solutions thus may be faced with challenges of hacking from guest accounts. As a guest user, the researcher was able to use *nmap* to scan an organizations network and get more information as shown below:

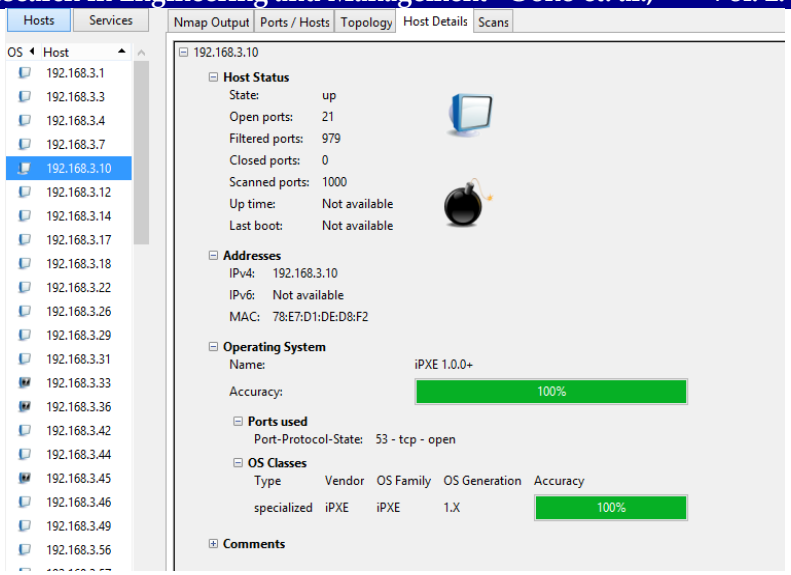


**Fig 6:** Nmap Guest scan out put

*IP Addressing*
Most universities used dynamic addressing with dynamic addresses assigned to users while the network devices had static addresses.

*Policy*
Some of the universities have acceptable user policies. However, to ensure compliance with the university security policies users indicated that: they complied with policies during configurations, deployment and implementation of different authentication mechanisms. Most institutions do not have a well-defined WLAN security policy.

*User training*
A majority of the users had not undergone security awareness and training.

*Physical security*
To ensure physical security of the devices the respondents indicated that; they had placed them in secure places away from easy reach, Put under lock and key or secured cabinets and also sometimes put in undisclosed places. This was also observed when the researcher visited the institutions as shown below.

**Fig 7:** Outdoor AP physical location

*Use of reset function*
Many institutions indicated that only the network administrators and approved support staff could use the reset function. It was however noted that in some universities where the physical devices were within easy reach anyone could use the reset function.

*Network Monitoring*
For the purposes of network monitoring the universities indicated that they used; Simple Network Management Protocol (SNMP) which is a protocol for network management. Others use open NMS which is an open source enterprise network management tool. They also use Cacti, a complete network graphing solution designed, Smokping that keeps track of network latency and use of inbuilt router monitoring functionalities. It was however noted that some institutions did not have any network monitoring mechanisms.

*Authentication*
For authentication the institutions use; Radius servers, MAC address access control, captive portal, passwords, WPA2, 802.1x

authentication with DES and 3DES, 802.1x EAP, PEAP-MSCHAP v2. There was an institution that had no authentication enabled for users, allowing anybody on campus and neighboring community to access their network.

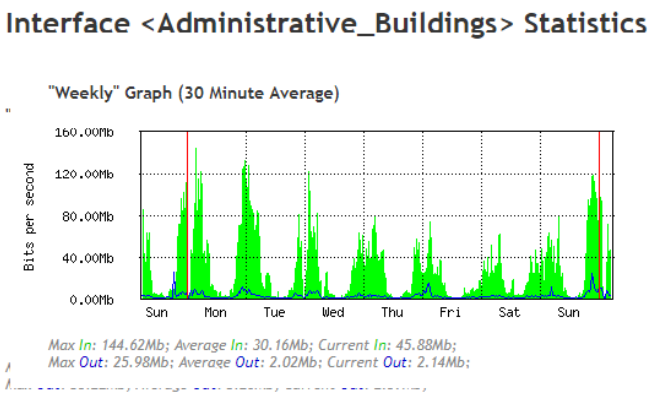


**Fig 8.** Router traffic statistics

*Firewalls*
Many of the universities are at a risk because they did not have personal firewall and anti-virus software for all STA platforms for which such security products are commercially available. It was also noted that remote connectivity to the devices (e.g., file sharing, open network ports) was not limited as recommended. There were many ports that were open but not in use providing backdoors for possible breach in security of the network. For example in the diagram below 3 ports were open for a router while only 1 was in use:

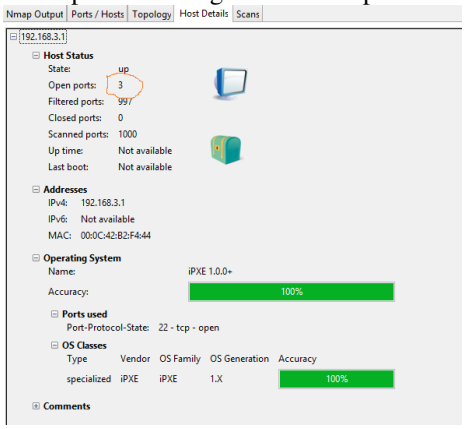


**Fig 9.** Nmap Host details

*Passwords*
Many of the respondents had never changed the passwords for the access points since installation.

*Intrusion detection*
Most universities had intrusion detection systems deployed on the wireless network.

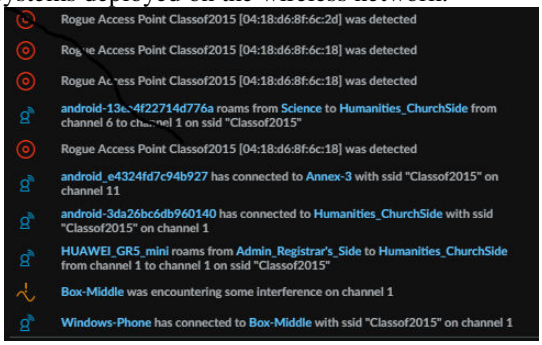


**Fig 10.** Intrusion detection logs

*Site survey and AP range*
Most universities had conducted a site survey to establish AP coverage and tested AP range boundaries to determine the extent of wireless coverage. However, from the practical survey the researcher found out that some of the APs broadcasted further than the

boundaries indicated by the respondents as shown below.

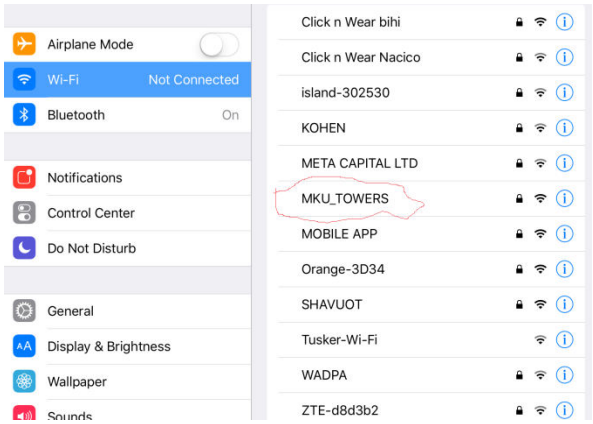


**Fig 11.** AP broadcast beyond boundary

It was also found out that channels were overlapping for different APs especially in towns and around student hostels broadcast causing interference in the networks. All the respondents stated that the APs run all day and night even if they are in use or not.

| MAC Address | RSSI | Chan | 802.11 | Max Speed | Vendor | First | Last |
|---|---|---|---|---|---|---|---|
| 44:D9:E7:21:1B:94 | -91 | 1 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:16 | 00:00:07 |
| D4:CA:6D:CE:4C:45 | -37 | 3+7 | b, g, n | 300 Mbps | Routerboard.com | 16:35:17 | now |
| 44:D9:E7:21:1C:7D | -88 | 6 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:18 | now |
| E4:8D:8C:6D:68:7B | -91 | 3+7 | b, g, n | 300 Mbps | Routerboard.com | 16:35:26 | now |
| 44:D9:E7:21:1B:E1 | -91 | 6 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:26 | now |
| D4:CA:6D:FC:92:89 | -88 | 6+10 | b, g, n | 300 Mbps | Routerboard.com | 16:35:28 | 00:00:49 |
| 44:D9:E7:21:1B:ED | -90 | 1 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:44 | 00:00:06 |
| 04:18:D6:8F:6C:18 | -91 | 1 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:59 | 00:00:05 |

**Fig 12:** Overlapping AP channels

*SSID broadcast*
All the institutions broadcast their SSIDs. The SSIDs include university names, location names, students, staff, lectures, Department names, School names, Eduroam and in some cases customized naming.

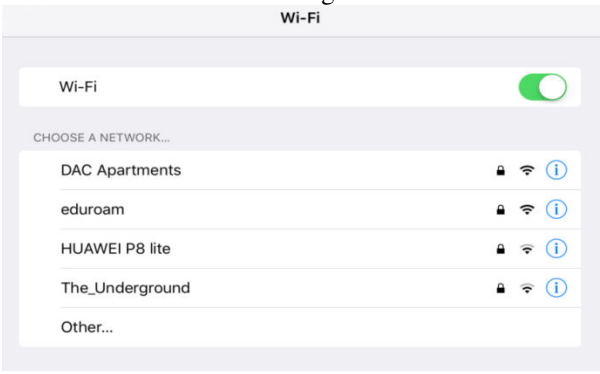


**Fig 13:** AP SSID broadcast

*SNMP version*
Most of the universities use SNMP to manage the devices. Most universities used insecure and nonessential management protocols which are potential methods that an adversary can use when attempting to compromise an AP. Examples of insecure management protocols include SNMPv1 and SNMPv2. Universities that used SNMPv3 did not configure it for least privilege (i.e., read only) even when write access was not required creating security loop holes.

*Measures and tools for ensuring improved security of wireless networks*
To ensure improved security of campus wireless network the respondents proposed; Use WPA2 Enterprise for authentication and use of separate VLANs, User management and authentication, Mac Lockdown, all campus unified monitoring, frequent device monitoring and re-configuration, RADIUS authentication of users, Deploy of authenticated and encrypted wireless networks. Use of an online

tool for measuring wireless security parameters against university settings will be helpful in ensuring maximum protection of the campus networks

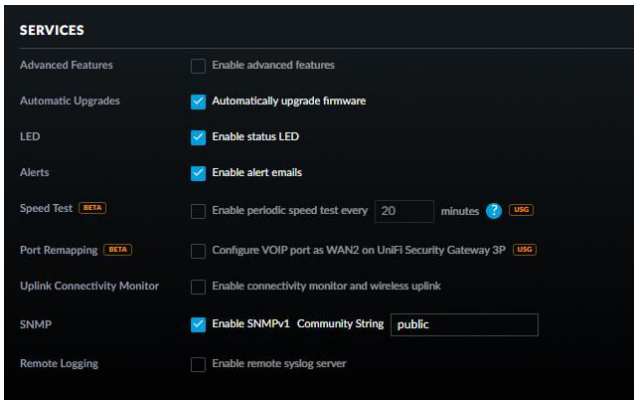


**Fig 14:** SNMP settings window

**Discussion**

From the findings above the researchers noted the following;

Like any other aspect of security, wireless security is a game of risk (Hiltunen, 2004). By knowing the risks involved in the network and making informed decisions about security measures, the wireless network operator has a better chance to protect itself, its assets, and users (Hiltunen, 2004). Given the fact that most universities in Kenya do not know the risks the face they are not likely to make informed decisions on how to protect themselves and even user from the threats they face.

According to Weiss (2000), newly discovered security vulnerabilities of vendor products should be patched to prevent inadvertent and malicious exploits. From the data collected it shows that many institutions have implemented this even though some install the patches without testing, this can lead to security problems in case the patches have bugs. Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and identifying corrective actions necessary to maintain acceptable levels of security (Frankel et al, 2007). Many institutions are therefore not able to identify the corrective actions on time and thus are not able to maintain an acceptable level of security.

A complete inventory of an organization's authorized APs is the basis for identifying rogue APs during security audits and can be helpful for a variety of support tasks. Motorola (2012), states that Information contained in the audit records may be needed even after the WLAN component is discarded (e.g., for an investigation of a subsequently discovered security breach). The methods of disposals pose a security risk for the universities thus they should identify the legal requirements to retain records that apply to their operations and copy the same before they are transferred to other departments. When donating they should ensure all the devices are reset so as to conceal organizational settings, something most institutions indicated they do not do.

You need a good solution or network access control solution that adjusts depending on what device is being used, where it's being used and who is using it while at the same time deploying reliable policy management that can automatically enforce those rules (Masai, 2016). Most universities did not have the best solutions thus may be faced with challenges of hacking from guest accounts
Even though many universities prefer to use dynamic addressing due to convenience, this method makes it difficult to track and control access based on IP addresses creating a security management challenge to the administrators.

Security policy is the foundation on which subsequent security controls are based (Frankel et al, 20017). This leaves the institutions at a vulnerable situation given the fact that without a policy it is easy to overlook important security requirements. A majority of the users had not undergone 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. This means some of the users may unintentionally perform actions that can create security risk to the universities. Without the insight that good monitoring tools and techniques provide, the universities cannot understand the effects that changes will make. Any change is likely to cause unintended damage to the network. Monitoring also helps the administrators to constantly know how the network is performing and whether there are any security problems (Nanda, 2013).

WLAN-capable devices typically are at greater risk of a security breach than wired-only devices and may require additional security controls beyond those already present (Gant, 2010). Many of the universities are at a risk because they did not have personal firewall and anti-virus software for all STA platforms for which such security products are commercially available. It was also noted that remote connectivity to the devices (e.g., file sharing, open network ports) was not limited as recommended. There were many ports that were open but not in use providing backdoors for possible breach in security of the network. Many universities are exposed to

dictionary attacks, administrator passwords on APs should be hard to guess and should be changed often. The estimated usable range of each AP should not extend beyond the physical boundaries of the facility whenever possible to ensure security of the networks. In addition, Broadcasting SSID with leading name such as office and department names are likely to attract attention of potential hackers.

**Conclusion**

From the findings of the study it is evident that wireless campus networks in most universities in Kenya are not secure. Efforts, even though not comprehensive, have been put in place by different universities to ensure security of the networks.

Some of the major concerns are: Limited risk assessments, Installing patches and upgrades without testing, limited security assessments, Poor disposal practices, inadequate security and access policies, Dynamic IP Adressing, 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

It was found out that the universities have however managed to; frequently review system logs, keep an inventory of network devices, Separate networks based on users, physically secure networks devices and deploy intrusion detection systems.

Network administrators play a major role in ensuring security of university networks. Most of the time they make use of recommended security measures that are not unique to the individual institutions and in the process ignore important elements of ensuring wireless security. The recommendations below have been made to help organizations improve their wireless security posture of all campus wireless networks.

**Recommendations**

*1.* 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
2. Before installing any patches and upgrades the universities should conduct tests to ensure all bugs are eliminated.
*3.* The universities should conduct frequent security assessments to be able to identify the corrective actions on time
4. 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
5. Universities should conduct frequent trainings and introduce awareness programs on network security from time to time
6. Universities should put in place efficient monitoring techniques and review from time to time
7. Secure authentication methods should be integrated with secure encryption methods to ensure improved security
8. Adequate firewalls that will ensure all ports not in use are blocked should be put in place
9. Aps should be configured in different channels to avoid overlaps and located in appropriate places to prevent broadcasting beyond boundaries.
10. SSIDs should be hidden and when broadcast they should not reflect the institutions and departments they serve
11. Universities should use secure management protocols

**References**

Alazzawe, et al. (2006). *Game theory and intrusion detection systems.* Retrieved 7 26, 2014, from http://theory.stanford.edu/.

AN-MSI, (. N.-S. (2002). *Developing Network Security at Minority-Serving Institutions: Building Upon the Title V Collaborative Effort Model.".* Unpublished.

Aspinwall, J. (2003). *Installing, Troubleshooting, and Repairing Wireless Networks.* John Wiley & Sons Inc.

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

Barnes, & Noble. (2008). Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs. *Proceedings of the 2nd ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots.* ACM.

Carnaghi, B. (2004). What is PHP server side scripting? www. webpointmopheus.combines.

CCK. (2012). *3rd Quater Report 2011/2012.* Nairobi: Communication Commision of Kenya.

Chappie, M. (2014, May 22). Are wireless networks inherently insecure? Atlanta.

CHE. (2004). *Reforming Higher Education.* Nairobi: Commission for Higher Education.

Corner, D. E. (2009). *Computer Networks and Internets* (5th Edition ed.). Prentice Hall.

CUE. (2013, December). *Commission for University Education*. Retrieved 22 August, 2014, from Universities Authorized to Operate in Kenya, 2013: http://www.cue.or.ke/services/accreditation/status-of-universities

Frankel, et al (2007). *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.* Gaithersburg: National Institute of Standards and Technology.

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

Floyd, C. (1984) A Systematic Look at Prototyping, in: Budde, R., Kuhlenkamp, K., Mathiassen, L. and Zullighoven, H. (Eds.) Approaches to Prototyping, Springer-Verlag: Heidelberg, 1-17.

Fowler, M. and Scott, K. (2000). Uml distilled.

Fogie, S. (2003, May 23). *Security Reference Guide*. Retrieved May 22, 2014, from Inform IT: http://www.informit.com/guides/content.aspx?g=security&seqNum=162
Gast, M. (2010). *802.11 Wireless Networks: The Definitive Guide.*
Gast, M. S. ( 2005). *802.11 Wireless Networks: The Definitive Guide* (2nd Edition ed.). O'Reilly Media.
Government of West Australia. (2007). *Wireless Network Security Position Paper.* Department of Finance.
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.
Hart, C. (1998). *Doing a Literature Review.* London: Sage Publications.
Hiltunen, K. (2004). WLAN Attacks and Risks.
Juma, P. (2011, December 1). *Kenya: Hackers Blamed in KU Exam Row*. Retrieved 22 May, 2014, from allafrica: http://allafrica.com/stories/201112020126.html
Kahn, R. E. (2009, August 20). *Network World*. Retrieved May 16, 2014, from LAN Services Set to Go Wireless.
Karygiannis, T., & Owens, L. (2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices.* Gaithersburg: National Institute of Standards and Technology.
Karygiannis, T., & Owens, L. (2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices.* Gaithersburg: National Institute of Standards and Technology.
Kashorda, M., & Waema, T. (2014). *E-Readiness Survey of Kenyan Universities (2013) Report.* Nairobi: Kenya Education Network.
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.
Kornkaew, A. (2012). *Management Information System Implementation Challenges Sucess Key Issues, Effects and Consequences.* Jonkoping University.
Legnitto, J. (2011, May 4). *Private Wifi.* Retrieved May 20, 2014, from Have You Been Hacked Using On Campus Wifi?: http://www.privatewifi.com/have-you-been-hacked-using-on-campus-wifi/
Macharia, K. (2013, November 27). *Kenyans being conned through hacked Facebook accounts*. Retrieved May 21, 2014, from Business Tech: http://www.capitalfm.co.ke/business/2013/11/kenyans-being-conned-through-hacked-facebook-accounts/
Masai, J. (2016, December 10). Wireless campus Security. (S. Ooko, Interviewer)
Motorolla. (2012). *Wireless Security: Ensuring Compliance with HIPAA, PCI,GLBA, SOX, DoD 8100.2 & Enterprise Policy.*
Nanda, S. (2013, 2 17). *Wireless Insecurity.* Retrieved 8 12, 2014, from How Johnny can hack your WEP protected 802.11b Network!
Neumann, J. v., & Morgenstern, O. (1947). *Theory of Games and Economic Behavior.* Princeton: Princeton University Press.
Oblinger, D. (2003). *Computer and Network Security in Higher Education.* Jossey-Bass Inc.
Obsborne, M., & Rubinstein, A. (1994). *A course in game theory.* MIT Press.
Obura, F. (2012, November 6). Kenyan universities lead region in ICT investment. Nairobi, Kenya.
Osborne, M. (2003). *An Introduction to Game Theory.* New York: Oxford University Press.
Pender, T. (2003). UML 2 Bible. Wiley Publishing Inc, USA.
Polit, & Hungler. (2003). *Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness.* Sweden: Elsevier Inc.
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.
Roberts, C. (2014, March 12). *Student hacks Florida University's wireless network*. Retrieved May 21, 2014, from New York Daily News: http://www.nydailynews.com/news/national/student-hacks-school-wireless-network-redirects-users-porn-site-article-1.1286260
Ross, D. (2005). The Security of Wireless Computing Technolgies. *AusCERT Conference.*
Samuel, S. (2009). *Big Challenges: Wireless Networks and Services.* Alcatel.
Scarfone, K., & Dicoi, D. (2007). Wireless Network Security for IEEE802.11a/b/g and Bluetooth. *NIST Special Publication 800-48 Revision 1*.
Sindhuh, E. S. (2013). *Analysis of the Effect of Wireless Campus Networks on Internet Usage in Kenyan Universities.* Nairobi: Unpublished.
Tabona, A. (2010). *An Overview of Wireless Network Security.* New York: NIST.
Wack, J., Tracy, M., & Souppaya, M. (2003). *Guideline on Network Security Testing.* Gaithersburg: National Institute of Standards and Technology.
Weiss, J. (2002). *Wireles Networks: Security, Problems and Solutions.* SANS Institute.
Welling, L. and Thompson, L. (2009). Php and MySQL web development. Sams Publications, 4th edition.