ATTACK SUSCEPTIBILITY OF KNOWN ATTACKS ON IEEE 802.11 PUBLIC WLAN

Mwathi, D.G.[1], Opiyo, E.[2] and Odongo, O.[2]
[1]Chuka University, P. O. Box 109-60400, Chuka; [2]University of Nairobi, P. O. Box 30197-00100, Nairobi
Email: dgmwathi@chuka.ac.ke, Tel.: 0722395597

Citation: Mwathi, D.G., Opiyo, E., & Odongo, O. (2016). Attack susceptibility of known attacks on IEEE 802.11 public WLAN. In: Isutsa, D.K. and Githae, E.W. *Proceedings of the Second Chuka University International Research Conference held in Chuka University, Chuka, Kenya from 28th to 30th October, 2015. 318-325 pp.*

ABSTRACT
Besides WLAN networks popularity in many places, they have security concerns. Whereas efforts have been made to address the security concerns, design flaws in the security mechanisms of IEEE 802.11 standard such as support for vulnerable authentication methods, and poor configurations give rise to a number of potential attacks. Consequently, readily available WLAN attack software tools make exploitation of these weaknesses relatively easy. This paper describes various WLAN attacks together with the vulnerabilities exploited and analyzes the attack susceptibility based on availability of attack tools and ease of their usage in the context of developing countries. The researcher analyzed attack susceptibility of 30 attack tools. Findings revealed that there are many tools that can be used to exploit WLAN vulnerabilities to launch attacks. The attack susceptibility of denial of service, man in the middle and cipher suite attacks were high. Many of the attack tools were open source, multi-platform and downloadable from the vendor website which made their usage level high. The high attack susceptibility suggested that the risk of attack is quite high in developing countries where institutions allocate low budgets on computer and network security design and implementation. Although all risks in using a WLAN network cannot be mitigated, keeping up-to date and implementing all reasonable measures should make WLAN reasonably safe from attack. Institutions need to prioritise and allocate reasonable resources to protecting WLANs against attacks.
Keywords: WLAN attack susceptibility, Cipher suite attacks, Man in the middle attacks, Denial of service attacks, WLAN vulnerabilities; Attack tools

INTRODUCTION
WLAN networks are everywhere; university campuses, coffee shops, hotels, airports, homes, fast-food restaurants and municipalities/cities(Wei-Lin and Quincy, 2010). Whereas wireless networking is emerging as a significant aspect of internetworking, it presents a set of unique issues based on the fact that the only limit to a wireless network is the radio signal strength. There is no wiring to define membership in a network. There is no physical method to restrict a system in radio range to be a member of a wireless

network. WLANs when deployed in public places are susceptible to certain inherent security issues found in all WLANs; such issues include known vulnerabilities such as the following:

- The WLAN broadcasts the access point name and location beyond the boundaries of the institution they are deployed. This allows external malicious users to see and recognize the institutional network.
- WLAN is vulnerable to spoofing i.e. rogue networks mimicking a real access point and establishing connections to intercept data and files.
- Data transmitted via WLAN can be vulnerable to interception and monitoring, creating risks to users.

How basic wireless LAN technology works

The general architecture used by WLAN, whether they are using the 802.11a, b, g or n technology, is to allow client devices e.g laptops, tablets, smart-phones and workstations to establish a connection with the WLAN through a wireless access point. Each IEEE 802.11 a/b/g/n device can operate in one of four possible modes; master mode, managed mode, adhoc mode or monitor mode. When operating in master mode, the device is a service provider operating with a specific SSID and channel. When in managed mode, the device is a client and joins a network created by a master and will change the channel to match that of the master. When in adhoc mode, the device creates peer to peer connections with other devices creating a multipoint to multipoint network. When in monitor mode, the device does not transmit any data but passively listens to all radio traffic on a given channel.

Association is the name given to the process of connecting a station (laptop, tablet, smartphone or workstation) to the WLAN. The station must have a wireless network interface card (NIC) installed and have its wireless protocols running. The station will periodically scan the environment looking for an access point. The station will use either active scanning or passive scanning. If the station is using active scanning, it will transmit a probe frame on all available frequency channels. When an access point receives the probe frame, it will respond with a probe response. The probe response contains all the information needed by the station to associate itself with the access point. If the station then agrees to associate with the given access point, communication has been established. In passive scanning, the station listens on all available channels for a beacon frame from the access point. The beacon frame, like the probe response, contains all the information needed by the station to associate itself with the access point. Once the station detects a beacon frame, it may choose to associate itself with the access point that transmitted the beacon frame. The type of information required to associate a station with an access point includes the Service Set Identifier (SSID) and the wireless network's transmission rate.

The IEEE 802.11 Media Access Control protocol supplies the functionality in WLANs that is required to provide reliable delivery of user data over the potentially noisy unreliable wireless media (Sheila et al., 2007). The 802.11 finite state machine of a WLAN client or Accesspoint is shown in Figure 1.

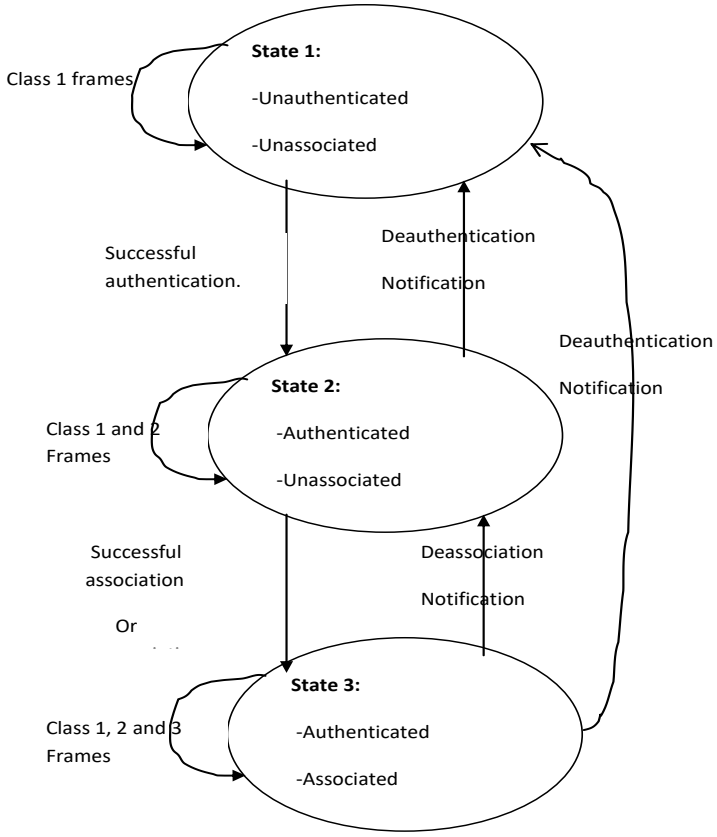
The 802.11 finite state machine consists of three kinds of states:
• State 1: initial state, not authenticated, not associated;
• State 2: authenticated, not associated;
• State 3: authenticated, associated.

For 802.11 wireless communications, the authentication, association, deassociation and deauthentication procedures enable wireless client and access point to be synchronized regarding finite state machines. De-authentication and deassociation procedures are in charge in keeping the state machines synchronized.

From client-side, we have:

- State 1 is the initial state where the client device probes for access points,
- State 2 is the authenticated state where it is authenticated to the access point,

- State 3 is the associated state where it is authorized to send (and receive) data communication frames to and from the wired network through the wireless access point. All state transitions are processed by 802.11 management frames.



Source: Laurent and Tinnès, 2007

Figure 1. 802.11 finite state machine of a WLAN client or Accesspoint .

Analysis of vulnerabilities exploited to attack a WLAN

Attacks associated with WLANs can generally be grouped into three; Denial of service, man in the middle and cipher suite attacks. Denial of service attacks include disassociate flooding (John et al, 2002), deauthentication, authentication flooding, EAP and TKIP countermeasure attacks (Scott, 2011) and WPA 196. Denial of service attacks may exploit use of a cipher suite (integrity and confidentiality protocols) that does not support encryption of management frames to cause disassociate flooding and deauthentication attacks on a WLAN. Additionally, inability of IEEE 802.11i to provide a guideline on how to choose an EAP method and cipher suite blending leads to choice of weak EAP methods and cipher suite combinations which can be exploited to cause EAP authentication flooding and TKIP countermeasure attacks. Support for features such as virtual WLANs by operating systems such as windows 7 creates a vulnerability that can be exploited to make it easy for WPA 196 denial of service attack to be realized.(Airtight networks,2010).Man in the middle attacks on the other hand may exploit the following vulnerabilities on a WLAN; Lack of secure Mutual authentications, use of a cipher suite that does not encrypt management frames during authentication, access point secret being rarely changed in pre-shared implementations, lack of automatic checking of the certificate provided by authentication server, use of Virtual Wi-Fi Soft access points, incorrect client configuration e.g. allowing self signed certificates. These vulnerabilities can lead to attacks such as resource stealing (John et al, 2002), captive Portal evil twin, Traffic re-direction and RADIUS certificate attacks.Cipher suite attacks may exploit use of Wired Equivalent Privacy (WEP) cipher

suite during authentication.WEP is relatively trivial to defeat and numerous attacks exist which can either decrypt WEP protected packets or recover the WEP key (Scott, 2011). Choosing a Weak passphrase in pre-shared WPA implementations can be exploited to cause WPA-PSK dictionary attack of the WPA key.WPA2 can also be broken by capturing a handshake that provides Snonce, Anonce and little more info knowledge of IPV4 address range of WLAN provided the passphrase is weak. Use of LEAP as upper layer authentication protocol can be exploited to cause LEAP attacks.

WLAN attack tools

WLAN attack tools can be broadly classified into three:

Cipher suite attack tools

You can use Wi-Fi stumblers to detect nearby access points and their details, like the signal level, security type and media access control address.You might find access points set with weak wired equivalent privacy security, which can be easily cracked, or possibly rogue access points setup by employees or others that could be opening your network up to attack. If there are access points set with a hidden or non-broadcasted SSID, Wi-Fi stumblers can quickly reveal it.You can use wireless sniffers to capture raw network packets sent over the air. You could import the captured traffic into other tools, such wireshark so as to crack encryption. Or if you're connected to the network (or if it's not encrypted), you could manually look for email and website passwords sent in clear-text. For eavesdropping, a commonly used tool is Wireshark, formally Ethereal. It is a basic sniffing program that will display all network traffic both wired and wireless. It is a multi-platform, multi-protocol analyzer with hundreds of protocols supported. It includes support for 802.11 and Bluetooth and also includes decryption support for many popular wireless security protocols including IPsec, Internet Security Association and Key Management Protocol (ISAKMP), Kerberos, Secure Sockets Layer, Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA)/WPA2.The sniffing programs work well for information that is sent in the clear. For encrypted information, an encryption key cracker is necessary (Anh and Shorey, 2005).For 802.11, WPA2 is the latest wireless encryption standard that has not been broken yet. WPA and WEP are two previous encryption schemes with many tools available that will crack their encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. Aircrack-ng is a 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as all-new PTW attack, thus making the tool much faster compared to other WEP cracking tools (Anh and Shorey, 2005). Aircrack-ng is a set of tools for auditing wireless networks.AirSnort is well known for WEP and AirCrack../../../../../../Documents and Settings/coordinator ict/Desktop/Wireless Hacking Tools.htm - 7 is an attack tool for WPA. Kismet is a 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. It shows the access point details, including the SSID of "hidden" networks. It can also capture the raw wireless packets, which you can then import into Wireshark, TCP dump, and other tools. In Windows, Kismet only works with CACE AirPcap wireless adapters due to the limitation of Windows drivers. It does, however, support a variety of wireless adapters in Mac OS X and Linux. Vistumbler is open source Windows application that displays the basic access point details, including the exact authentication and encryption methods, and can even speak the SSID and RSSI. It also displays graphs of signal levels. It's highly customizable and offers flexible configuration options. It supports access point names to help distinguish them, also helping to detect rogue access points. It also supports GPS logging and live tracking within the application using Google Earth **(**Michael, 2007).

Tools such as Hotspotter, APsniff, APhunter, and KNSGEM will scan for wireless AP beacon signals. Although they are not necessarily attack tools, they can be used to find the wireless APs. KNSGEM will even place the APs on a Google Earth map. Attackers will then setup their “Evil Twin” AP near these legitimate ones. OpenWRT and HyperWRT are two open source projects that replace the factory firmware for Linksys's popular WRT line of APs. Attackers can use these distributions to create fake APs. Wifi

Analyzer is a free Android app you can use for finding access points on your Android-based smartphone or tablet. It lists the basic details for access points on the 2.4-GHz band, and on supported devices on the 5-GHz band as well. You can export the access point list (in XML format) by sending it to email or another app or take snapshot of the screens. It also features graphs showing signals by channel, history, and usage rating and also has a signal meter feature to help find access points.Cain and Abe is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources, however it also ships some "non standard" utilities for Microsoft Windows users. Cloud is a commercial online password cracking service. In addition to WPA/WAP2 PSKs, it can also be used to attempt cracking of password hashes and password-protected documents. They use huge dictionaries of 300 million words to perform the cracking and have the computing power to do it quick. You just simply upload the handshake file for WPA/WPA2 or PWDUMP file for the hashes or documents. Reaver is a Linux program that performs brute force attacks against wireless routers to reveal their WPS PIN and WPA/WPA2 PSK within four to 10 hours. They also offer an easy-to-use hardware solution, Reaver Pro, with a graphical web interface can be used to test your wireless routers against the WPS PIN weakness:

Man in the middle attack tools

Data integrity ensures that the transmitted data arrives at the destination unchanged. HermesAP and OpenAP are two Linux based tools that allow the user to setup phony APs. Frame injection and frame replay tools can be used to attack the integrity of the data. The attack tools focus on frame manipulation, so that an attacker can cause the user to receive the information it chooses.Ettercap and dsniff are two popular men in the middle attack tools. They both provide sniffing capabilities similar to Wireshark, but go beyond that with the ability to modify the data in transmission (Jiang and Garuba, 2008). Dsniff can be used in auditing and penetration testing.Ettercap features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols (even ciphered ones) and includes many features for network and host analysis. Again these are available for many platforms. Ettercap even has a tutorial on how to write your own plugin. Airpwn is a wireless attack tool for 802.11 packet injection. It listens for specific patterns of the incoming packets. If there is a match with what is specified in the config file, then custom spoofed packets are injected from the AP.

The valid packet that the spoofed packet replaced will be intercepted by airpwn and not allowed to reach the user. File2air is a similar injection tools except it allows the user to specify a file that will be used for the payload of the injected packets. It uses another tool called AirJack to perform the actual frame injection. File2air runs on top of AirJack and reads in a binary file and transmits its contents onto a wireless network. Simple-replay is an attack tool that does exactly as the name implies. It allows for 802.11 packets that were previously captured to be injected back into the network. FreeRadius-WPE is a patch for the open source FreeRADIUS server designed to perform man-in-the-middle attacks against users of wireless networks using 802.1x authentication. It modifies the server to accept all network-attached storage devices and EAP types and logs the username and challenge/response from the unsuspecting users that connect to the fake wireless network. Then the challenge/response can be inputted into another Linux program, asleap, to crack the encrypted password.

WiFish Finder is an open source Linux program that passively captures wireless traffic and performs active probing to help identify wireless clients vulnerable to attacks, like evil twin access points, honey pots, or man-in-the-middle attacks. It builds a list of network names that wireless clients are sending probe requests for and detects the security type of that desired network. Thus you can identify clients probing for unencrypted networks, which would be easily susceptible to evil twins or honey pots attacks, or those

probing for a WPA/WPA2-Enterprise network that could be susceptible to man-in-the-middle attacks. Jasager (based on KARMA) is Linux-based firmware offering a set of Linux tools to identify vulnerable wireless clients, like WiFish Finder, but can also perform evil twin or honey pot attacks. It can run on FON or WiFi Pineapple routers. It can create a soft access point set with the SSIDs nearby wireless adapters are probing for and run a DHCP, DNS, and HTTP server so clients can connect. The HTTP server can then redirect all requests to a web site. It can also capture and display any clear-text POP, FTP, or HTTP login performed by the victim. Jasager features a web-based and command-line interface.WiFiDEnum (WiFi Driver Enumerator) is a Windows program that helps identify vulnerable wireless network drivers that are risk to wireless driver exploit attacks. It scans the wired or wireless network for Windows workstations, collects details about their wireless network adapter drivers, and identifies possible vulnerabilities.

Denial of service attack tools

To execute an authentication flooding attack, you could use frame injection to inject many authentication frames from different MAC addresses. This will fill up the authentication table of the AP and make it difficult for a legitimate user to connect(Scott, 2011). FakeAP tool generates thousands of 802.11 APs.Specifically it generates thousands of 802.11 beacon signals that can be used for the beacon signal flooding attack. Void11 is another flooding attack tool. It has the ability to implement three different flooding attacks: deauthenticate clients, authentication flood, and association flood. The deauthenticate attack floods the WLAN with deauthenticate packets for random MACs. Those legitimate users connected with matching MAC address will close their connection upon receiving the deauthenticate packet. The authentication attack again floods the network with authentication packets so legitimate user cannot connect. The same is with the association packets.

METHODOLOGY

The following procedure was used by the researchers to determine the attack susceptibility of WLAN attacks. The researcher analyzed attack susceptibility of eighteen (18) cipher suite attack tools, ten (10) man in the middle attack tools and two (2)denial of service attack tools collected from internet sources and characterized them as follows:

(i) If the tool is open source and is downloadable directly at the developers' official website, then availability is 'free'**.**

(ii) If the tool is open source and does not have an official download site and so must be obtained by using alternative methods such as peer-to-peer transferences or visiting hackers communities then availability is 'limited'.

(iii) If the tool is commercial, then availability is 'Not available'

In the context of developing countries where many hackers may have financial constrains there is a limit on how much one can spend to acquire a WLAN attack tool. Therefore:

(i) If the tool is free, then the probability of it being used to attack is considered high. Therefore the associated attacks/vulnerabilities are easy to be exploited and their attack susceptibility is high.

(ii) If availability is limited, then the probability of it being used to attack is considered medium. Therefore the associated attacks/vulnerabilities are considered relatively difficult to be exploited and therefore their attack susceptibility is medium.

(iii) If availability is 'Not available', then the probability of it being used to attack is considered Low.Therefore the associated attacks/vulnerabilities are considered difficult to be exploited and therefore their attack susceptibility is low.

FINDINGS

Table 1 analysis the attack susceptibility of cipher suite, man in the middle and denial of service attacks to wireless local area networks (WLANs) commonly referred as WIFI.The table shows the attack tool, description of specific attack it carries, availability of the tool and the attack susceptibility of the particular attack performed by the tool.

Table 1: Analysis of attack susceptibility of cipher suite, man in the middle and denial of service attacks

Tools	Description	Availabilityof the tools	Attack susceptibility
Cipher suite attacks			
AirSnort	Brute force WEP Encryption cracker	http://airsnort.shmoo.com/**[free]**	High
AirCrack	WPA Encryption cracker	http://www.aircrack-ng.org/ **[free]**	High
Ettercap, dsniff, and Wireshark	Packet sniffers with traffic analysis. These also include tools to break encryption.	http://www.wireshark.org/download.html http://www.monkey.org/~dugsong/dsniff/ http://ettercap.github.io/ettercap/downloads.html**[free]**	High
Hotspotter, APsniff, APhunter, and KNSGEM	Access Point locators that discover WLANs by listening for beacon signals transmitted from APs.	http://www.wirelessdefence.org/Contents/hotspotter.htm http://www.monolith81.de/apsniff.html http://www.math.ucla.edu/~jimc/mathnet_d/download.html http://www.wirelessdefence.org/Contents/knsgem_main.htm**[free]**	High
Kismet	A 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.	http://www.kismetwireless.net/download.shtml[Free]	High
Wifi Analyzer	A free Android app you can use for finding access points on your Android-based smartphone or tablet.	http://download.cnet.com/Wifi-Analyzer/3000-2094_4-75029583.html[free]	High
Vistumbler	Open source Windows app that displays basic access point details.	http://www.vistumbler.net/downloads.html[Free]	High
Reaver	A Linux program that performs brute force attacks against wireless routers to reveal their WPS PIN and WPA/WPA2 PSK	http://code.google.com/p/reaver-wps/[Not available]	
CloudCracker	An online WPA password cracking service for penetration testers.	https://www.cloudcracker.com/[Not available]	Low
OpenWRT and HyperWRT	Replacement firmware so APs can be programmed to execute attacks e.g Fake AP creation	https://openwrt.org/ http://www.polarcloud.com/tofu[free]	High
Cain and Abel	A password recovery tool for Microsoft Operating Systems.	http://www.oxid.it/cain.htm[free]	High
THC-RUT	Freeware wireless LAN discovery tool that uses “brute force” to identify low traffic access points.	http://www.thehackerschoice.com(free)	High
Man in the middle attacks			
HermesAP and OpenAP	Used to setup a rogue Access Point causing Evil Twin	http://linux.softpedia.com/progDownload/HermesAP-Download-13871.html http://www.1mobile.com/openwifi---open-ap-connector-966964.html**[free]**	High
Airpwn	Allows for generic 802.11 packet injection	http://airpwn.sourceforge.net/Airpwn.html**[free]**	High
File2air	Allow the specified file be used as packet payload. 802.11 replay attack	http://www.willhackforsushi.com/?page_id=19**[free]**	High
AirJack and Simple-replay	Allows previously captured packets to be injected back into the network. 802.11 replay	http://sourceforge.net/projects/airjack/ "Simple-replay", http://www.802.11mercenary.net/simple-replay/ **[Limited]**	Medium
WiFiDEnum	Identify vulnerable wireless network drivers that are risk to wireless driver exploit attacks	http://ihackers.co/wifidenum-wi-fi-vulnerability-scanning-tool/**[Limited]**	Medium
Jasager	Linux-based firmware offering a set of Linux tools to identify vulnerable wireless clients, but can perform evil twin or honey pot attacks.	http://www.digininja.org/jasager/download.php[**free]**	High
WiFish Finder	An open source Linux app passively captures wireless traffic & performs active probing to identify wireless clients vulnerable to attacks.	http://www.airtightnetworks.com/home/resources/knowledge-center/wifish-finder.html http://sourceforge.net/projects/wifishfinder/files/latest/download**[free]**	High
FreeRADIUS -WPE	A patch for FreeRADIUS server designed to perform man-in-the-middle attacks against users of IEEE 802.1x authentication.	http://www.willhackforsushi.com/?page_id=37**[free]**	High

Denial of service attack			
FakeAP	Generate thousands of 802.11 beacon signals	http://www.blackalchemy.to/project/fakeap/ http://www.wirelessdefence.org/Contents/FakeAPMain.htm**[free]**	High
Void11	Can be used to execute deauthenticate, authenticate, and association flooding attack	http://www.wirelessdefence.org/Contents/Void11Main.htm**[Limited]**	Medium

The findings reveal that there are many available tools that can be used to exploit WLAN vulnerabilities to launch attacks. The attack susceptibility of denial of service, man in the middle and cipher suite attacks is high. Many of the attack tools are open source and downloadable from vendor website.

CONCLUSIONS AND RECOMMENDATION

WLAN implementations are susceptible to many attacks due their inherent vulnerabilities and readily available software attack tools. Many WLAN attack tools are multi-platform which makes their usage level high. The risk of attack is quite high in developing countries where institutions allocate low budgets on Computer and network Security design and implementation. Despite the fact that everyone gains by using WLAN and considering the increasing development of software attack tools there is no truly workable security solution to date that has been proposed to completely manage the security risks of WLAN networks. Although all risks in using a WLAN network cannot be mitigated, keeping up-to date and implementing measures should make WLAN reasonably safe from attack. Additionally institutions need to prioritise and allocate reasonable budgets to protecting WLANs against attacks discussed.

REFERENCES

AirTight Networks. 2010.Windows 7 Virtual Wi-Fi: The Easiest Way to Install a Rogue AP on Your Corporate Network, AirTight Networks, CA www.airtightnetworks.com.

Anh, N. and Shorey, R. 2005. Network sniffing tools for WLANs: merits and limitations, Personal Wireless Communications, IEEE International Conference.

Jiang , L. and Garuba, M. 2008. Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities, Information Technology: New Generations: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=4492539andabstractAccess=noanduserType=inst.

John, V., Ann, A. and Robert, M. 2002. 802.11b Wireless Networking and Why It Needs Authentication, Interlink Networks, www.interlinknetworks.com.

Laurent, B. and Julien, T. 2007. Discovering and exploiting 802.11 wireless driver vulnerabilities,Journal in Computer virology Vol 4 Issue 1,PP 25-37Publisher:Springer –Verlag, 1/2/2008 http://link.springer.com/article/10.1007%2Fs11416-007-0065-x#page-1,viewed 27th Sep., 2014.

Martin, B. and Erik, T. 2008. Practical attacks against WEP and WPA, TU-Dresden, Germany, TU-Darmstadt, Germany.

Michael, R. 2007. Wireless Hacking Tools, http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking.pdf Viewed on 30th June, 2013.

Scott, A. 2011. Known Wireless Attacks. Loughborough University.

Sheila, F., Bernard, E., Les, O. and Karen, S. 2007. Establishing Wireless Robust security Networks: A Guide to IEEE 802.11i NIST.US

Wei-Lin C. and Quincy Wu, A. 2010. Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal: Proceedings of Asian-Pacific Advanced Network 2010 v.30 p. 66-69. http://dx.doi.org/10.7125/APAN.30.10,Taiwan Viewed March 2014.

******