Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The Challenges of Mobile Unauthorized Access Point

Modesta. E. Ezema
Department of Computer Science,
University of Nigeria, Nsukka

Chikaodili Helen Ugwuishiwu
Department of Computer Science,
University of Nigeria, Nsukka

Paul .U. Chine
UNICEF Field Office
Enugu State, Nigeria

Abstract: ***The introduction of wireless access in the computer world changed the order of events. Wireless networking provided many advantages such as productivity improvement due to increased accessibility to information resources, network configuration/reconfigurations made easier, convenience, mobility, expandability, faster, and less expensive network accesses etc, but it also brought a new order of security threats and challenges as its ills, which altered the organizational overall information security risk profile. For example, because communications, occurred "through the air" using radio frequencies as in the case of wireless access, made the risk of interception to be greater than when it was with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can easily access and read through into the network, thereby compromising confidentiality and network integrity. Since implementation of technological solutions is the usual response to wireless security threats and vulnerabilities, wireless security then becomes primarily a management issue. Effective management of the threats such as mobile Unauthorized Access Points, broadcasted SSIDs, unknown stations, spoofed MAC addresses associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a network plan to mitigate identified threats. In this paper, we strove to present a framework that would help the management team understand, evaluate and assess the various security threats of mobile unauthorized access points, associated with the use of wireless technology within their own peculiar network and thereafter consider the recommendations listed, as a tool for safe networking environment.***

Keyword: wireless access point (WAP), wireless network ,wireless security , wireless threats, hot spot ,media access, control address, wireless Intrusion detection system node,Firewall.

I. INTRODUCTION

Access Point is a base station that transmits and receives data (sometimes referred to as a transceiver) within a wireless local area network (WLAN). It can also be defined as a as a stand alonedevice that plug into an Ethernet switch, wireless router or hub connecting users to other users within the network and also can serve as the point of of interconnection between the WLAN and a fixed wire network. Each access pointcan serve multiple users within a defined networkarea; as people moved beyond the range of one access point, they are automatically handed over to the next one. A small WLAN thatcan only require a single access point, the the number required increases as a function of the number of network users and the physical size of the network.[1] Access points used in home or small business networks are generally small, dedicated hardware devices featuring a built-in network adapter, antenna, and radio transmitter. Access points support Wi-Fi wireless communication standards. See figures1 below;

Fig 1 wireless Access Point

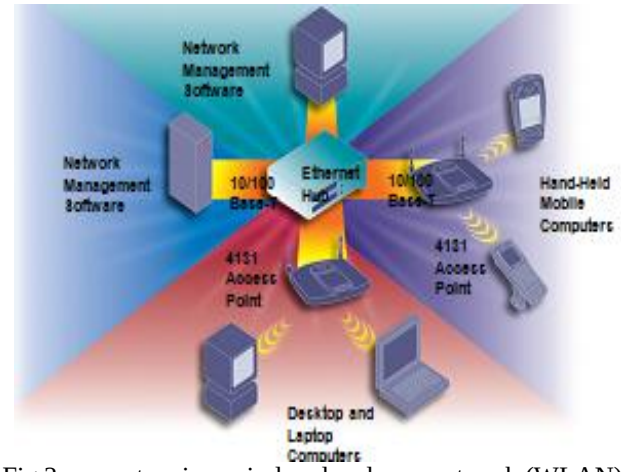

Fig 2 computers in a wireless local area network (WLAN)

Fig3 Linksys Mobile "WAP54G" 802.11g wireless Access Point

In computer networking, prior to introduction of wireless access (i.e. non-mobile access), setting up a computer network in a business, home or school often required running many cables through the walls and ceilings in order to deliver network access to all of the network-enabled devices in the building. This structural design were cumbersome, time-consuming, resource consuming, untidy and limited. With the creation of the Wireless Access Point (WAP) later, network users breathed sign of relief in which they can now be able to add devices that access the network with few or no cables, using radio frequencies rather than cabling; and supporting a standard for sending and receiving data defined by the IEEE 802.11 standards. These Wireless Access Points (WAPs) which are network equipment(s) that provide mobile devices, access to the network; usually are managed by WLAN Controllers, handling the automatic adjustments to RF power, channels, authentication, and security. They (i.e. WLAN Controllers) were also made to be part of a mobility domain in other to allow clients access, through large or regional officelocations conveniently. Mobile Access Points were later introduced, to enhance the capabilities of the Wireless Access Points using Operating Systems (e.g. Symbian O.S., Palm O.S., Tiny O.S) that ran on mobile devices. As the usefulness were growing, just like in any other system, the ills were also growing such asprowling of the company's network for stealing or fraud, filesandInternet accesses, printers and fax machines unauthorized printings of jargons, injecting of Trojans, viruses, malicious malware, congesting your bandwidth with malicious software, sniffing for your Bank details and credit card pins, damaging of vital data, Interference just to mention but a few.

All of these attributes above, necessitated the introduction of security system on the Mobile Access Point(s) to authenticate and authorize Access points (i.e. Authorized Mobile Access Point), before access is granted onto the network.[2] Wireless technology is becoming ever more popular, both in the business world and with consumers. The ease with which wireless access points can be installed and the risk of unauthorized access they present means that users need to apply security skills to safeguard their wireless networks. A measure instituted to regiment the unauthorized access points causing havok in general; Certain security techniques have since then been developed while more are still under construction; Organizations are now very serious and business minded in deploring these security tools such as: WEP, WPA, WPA2, WPA-PSK, activated 802.11 encryption, non broadcast of SSID, strong firewalls & passwords, SmartCards etc, in protecting their organizational data and resources from the mobile unauthorized access Points and hackers, having suffered it themselves or seen neighboring organization who have been victim undergoing the terrible experiences of rebuilding the entire organizational network. Hotspot were also introduced to further limit unauthorized Access Point/users from gaining easy access to the network.

II. MOBILE UNAUTHORIZED ACCESS POINT

It is a mobile wireless network device that has been
installed (either via cabling, Bluetooth, Wi-Fi or any related standard means) within an organization/enterprise without the explicit authorization from the host or the owner who has the capabilities of influencing the network of the organization negatively [3] The trouble is that a rogue access points often don't conform to wireless LAN (WLAN) security policies, which enables an open, insecure interface to the corporate network from outside the physically controlled facility.

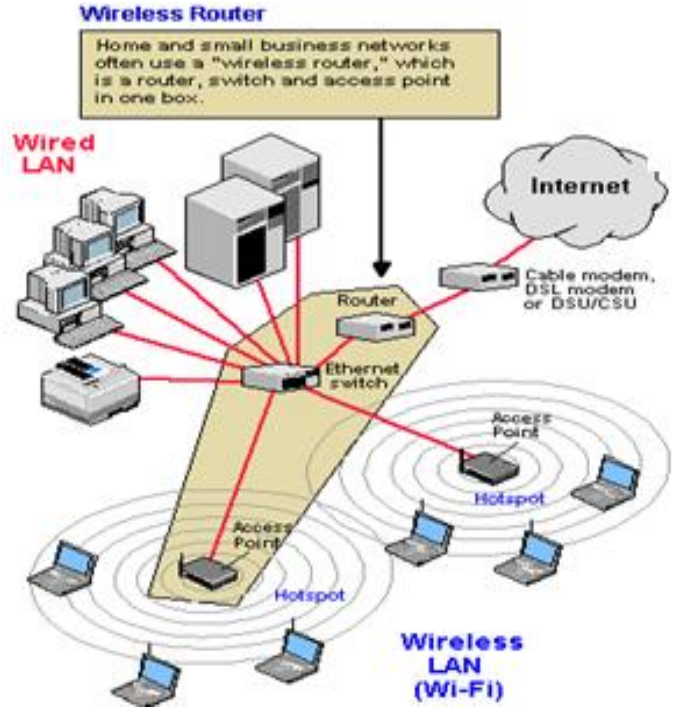

Fig 4:Systems in wireless LAN connections showing access points

There are terms one has to be familiar while discussing unauthorized access points .they include the following;

A. Hotspot

A hotspot is a common public application of WAPs, where wireless clients can connect to the Internet without regard for the particular networks to which they have attached for the moment using authenticated ID),

B. Service Set Identifier (SSID)

Service Set Identifier (SSID) [5] Service Set Identifier, is the network name. It is a sequence of characters that uniquely names a wireless local area network (WLAN) and its sometimes referred to as a "network name." [6] Because multiple WLANs can coexist in one airspace, each WLAN needs a uniqueNamethis name is the service set ID(SSID)ofthe network. Your wireless device can see the SSIDs for all available networks. Therefore, when you click a wireless icon, the SSIDs recognized by device are listed . For example, suppose your wireless list consists of three SSIDs named Student,Faculty, and Voice. This means that an administrator hascreated threeWLAN Service profilesand, as part of each WLAN service profile, provided the SSID nameStudent, Faculty, or and Voice. Service Set
Identifier (SSID) issimply the 1-32 byte alphanumeric
name given to each ESS identifier.This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area; e.g. a departmental WLAN (ESS) may consist of several access points (APs) and dozens of stations, all using the same SSID. Another organization in the same building may operate on its own departmental WLAN, composed of APs and stations using a different SSID. The purpose of SSID is to help stations in department A find and connect to APs in in department A, ignoring APs belonging to department B.Each set of wireless devices communicating directly with each other is called a Basic Service Set (BSS) identifier. Several BSSs can be joined together to form one logical WLAN segment, referred to as an Extended Service Set (ESS) identifier.

III. CAUSES OF MOBILE UNAUTHORIZED ACCESS POINTS

[4] The simplest cause of unauthorized access point
is that 802.11x wireless access points and network cards have been available for some time, however ,their use is ever more common among the populous of home users and non IT employees at the companies. Due to popularity and explosive growth of the use 802,11x wireless products , prices have dropped , causing the technology to become commonly used and understood across the computing community . Unlike before it is very simple for a user to go to the local computer outlet pick up an access point and wireless card at a cheap rate and plug it into a wired Ethernet jack at home or office . a major problem being faced by many enterprises network today.

Also in some offices staff bring all manner of unauthorized Access Points into their working place environment; because most times while at work there is poor or no network coverage from their server and certain network features are required for them to work. What they need to work are often times lacking or incomplete; most times the network link to which they are connected unto, run slowly for the type of work they are required to do; sometimes perhaps due to congestion on that Access Point; sometimes they will be around at off-office hours to complete their left-overs and with utmost dismay discovered that the Access Points are switched-off by the Network Administrators who are not on sit at that moment, so the only option is simply to connect their Access Point to neighboring office WAP broadcasting their SSID etc*".*

The above appeared honest and truthful to necessitate a legitimate employee to come along with their own Access points to work, What about the hackers who stay at the car parks inside their cars near an organization fence to hack-through**?** What about the 419's who stay on their laptops, iPhones, iPads, Smartphone's etc 24hours hacking into the organizational networks**?** What about the unauthorized visitors thatsmuggle their Access Points into an organization by any means available to them in-disguise, of seeing their friends (that are legitimate employees) and
staying in their offices to hack into the organizations
hence the intense need for a strongly defended
network security system installed and put in place.,

A. How mobile unauthorized accesspoint work

A fake access point can be set up by a malicious attacker as seen in the fig 5 below, to masquerade as an authorized Access Point by spoofing the authorized Access Point's Medium/Media Access Control (MAC) address. This fake Access Point is used to fool a wireless node in the WLAN, into accessing the network through the fake Access Point instead of the authorized one. The fake Access Point can then launch a variety of attacks thereby compromising the security of the wireless communication.

B. Setting up a fake Access Point

Setting up fake Access Point's is not hard. Public domain programs including raw glueapplications (i.e. raw glue access point is a proof-of-concept tool that tries to catch wireless stations that are searching for preferred SSIDs using wireless raw injection in monitor mode) sniffs 802.11x probe request frames to find out the default Access Point of the probing wireless node and then impersonate the default AcessPoint. [7]Raw Fake AcessPoint isa program that emulates IEEE 802.11 access points thanks to wireless raw injection.It aims at creating/injecting both beacon and probe response frames in order to emulate valid IEEE 802.11 access points.It is a program that catches wireless stations searching for preferred SSIDs.Therefore, detecting unauthorized Access Point's is a very important task of WLAN Intrusion Detection Systems (WIDS node). See fig 5 below;

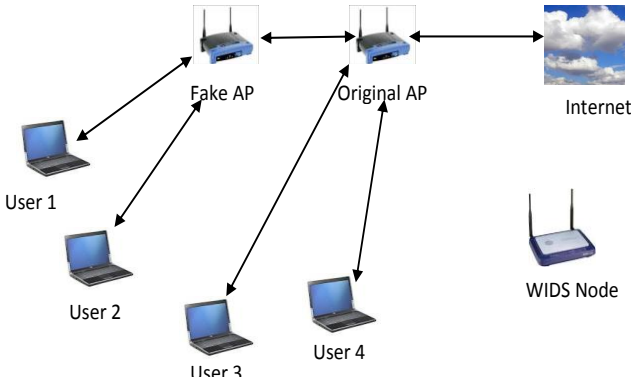

Fig5 wireless LAN showing fake AP

The new wireless security enhancement 802.11i *RSNA (Robust Security Network Association)* uses
traditional cryptographic methods (i.e., digital certificates) to provide strong mutual authentication between wireless clients and the Access Point's. Although this solution, if
implemented properly, will make the fake Access Point
attack less likely, the following practical issues can still
make wireless networks using 802.11i RSNA vulnerable.
First, management and verification of digital certificates
across different domains is known to be cumbersome. Secondly, as the current Access Point selection algorithms use signal strength as the only criteria for Access Point selection, users can be fooled to connect tothe fake Access Point that has a higher signal strength compared to the original one but does not support any security measures such as RSNA.1
Thirdly, an attacker can also set up fake Access Point's having the same identifiers (MAC address, Basic Service Set Identifier (BSS) and Service Set Identifier (SSID)) as the original Access Point and evade detection by using different physical channel characteristics (by using short/longpreambles, operating in a different channel etc).
These facts motivate us to find a viable non cryptographic solution to the fake Access Point attack. We emphasize that this solution is not meant to replace existing cryptographic methods. Rather, it should be used in conjunction with the cryptographic methods to achieve a higher level of security in WLANs.

IV. PROBLEMS CREATED BY MOBILE UNAUTHORIZED ACESS POINT

The concept behind wireless technology is to give people the freedom to roam around and still be connected to their network resources conveniently. The lure of this freedom has metamorphosed into strange unimaginable scenarios' today.Because a simple WLAN can easily be installed by attaching a WAP (often for less than N20000) to a wired network and a N5000 WLAN card to a laptop, all bought for a token; employees like never before, are coming to work well-equipped with an array of network-compatible wireless gadgets such as iPhones, iPads, laptops, media players, wireless Access Points etc and are all deploying all of these unauthorized WLANs anyhow, while IT departments (System Administrators/Engineers) are slow to adopting to the new technology trends.

You might ask, "What is the harm in doing that?" The harm is unlimitedly increasing daily, as more threats/harms are being discovered.[8] By installing an unauthorized access point, for example, you have succeeded in extending/opening up an invitation to everyone, including hackers within a 500-foot radius of the Access Point, to accomplishing their selfish activities; including prowling your company's network for stealing files, Internet access, printers, fax machines, injecting Trojans horse
viruses, malicious malware, congesting
your bandwidth with malicious software, sniffing
for your bank details/credit card pins, damaging
vital data, Denial of ofService etc. and any
other devices currently connected
to this network is already vulnerable to the
same consequences and challenges.This unwelcome by
product of unsanctioned wireless activity, is that offend
ing employees/authorized visitors unwittingly make
the enterprise's wireless network traffic, vulnerable to interception by unauthorized Access Points/hackers,
exposing the organization's confidential data, critical
assets andintellectual property - to the outside world.
There's also the possibility that these users/ hackers
/unauthorized Access Points could introduce
malware, viruses, trojansetc either intentionally or or unintentionally, into the company's network .

V. DETECTION AND REMOVAL OF MOBILE UNAUTHORIZED ACCESS POINTS

The best way to detect the presence of unauthorized mobile wireless devices was to routinely analyze the company's network by plugging in a laptop into the network system and running a detection tool utility, provided by the vendors often times, such as: Airmagnet Inc. andAruba Networks Inc., These mechanism allows the network administrators/other authorized personnel to quickly pinpoint the existence of any rogue (unauthorized) device(s). Physically moving around the organization's premises with detection devices have again also proven to be among the best detection techniques
There are two types of detection tools: those that
classify rogues (unauthorized) and those that do not.
Systems that classify it, can automatically determine
if an access point or other devices are actually connected to tothe network. Less sophisticated products flag
everything detected in the general vicinity as "rogue"
and leave it to the administrator to determine whether
the device is a genuine threat or just a harmless signal
leaking over from a nearby office.

Once you've located an unauthorized access point, working directly to the end user(s) to remove it, is the fir first step, but If the end-users education doesn't address the issue, options then exist to blocking the Access Point device from the network inside. One solution available in achievingthis is to implement a system that shields unauthorized radio frequencies. Another option, is to go back through the wired infrastructure, and find where the device is plugged into the network, and disable that port; Miller says. "That doesn't kill the RF signal, but at least the security hole is plugged, because people can't access the network through it any more", yet another option which may be among the simplest way to avoid rogue (unauthorized) Access Points is to deploy a corporate-sanctioned wireless network. Cost and support issues might often be cited as obstacles towards this approach, but the organization that balks should consider the consequences at long run.

A. Solutions Recommended

Today, certain recommendations which can help keep/maintain safe computing environments, have been envisaged in recent times, and may include the following:-

Think security : Always imagine what happens when any unauthorized hacker gains access to your data, what would become of the data later

1.) *use safe strong long passwords*: this implies ensuring that your files/folders, drives, accesses to your system are properly inhibited by unauthorized Access Points/hackers. Never reuse any password anywhere. disable all network management features of the access point such as simple-network-management-protocol (SNMP) ,Hyper Text transport protocol (HTTP) Telnet etc. USE FIREWALL enforced policy to thoroughly filter/checkmate accesses into your system/Access Point.

2.) *use strong authentication*; such as the one provided for by 802.1x protocol to authenticate all devices plugged into the network, which would uncover the identity of each wireless device (mobile or otherwise) attempting to access the network before assigning them IP addresses, it easily eliminates unauthorized access point.

3.) *hide and change the SSID often* ;(Service Set Identifier) which is a sequence of characters that uniquely names a WLAN, thus not allowing hackers, intruders or unauthorized Access Points connecting into the broadcasted Access Point of the organization via the SSID (or network name).

4.) *Turn-off access point;* Turn-off access point system whenever you arenot doing any useful work on them, since no hacker can gain access into a switched-off system/Access point etc.

5.) *Get more training*: Add more knowledge to Yourself by reading vast. Know that newer products of Access Point devices should have better facilities to offer. Study their manuals to know how to personally configure them away from their default settings which is accessible to anyone with the same device. Read about hackers and their activities, viruses, malwares, threats, Trojans etc. Go for Seminars, Conferences and other form of Improving ones knowledge and skills. This implies reduced threat and exposure to unauthorized mobile Access Point hackers into your organizational network.

6.) *Avoid sharing*: Detest Peer-to-Peer file sharing software such E-mule, eDonkey, Gnutella, Kazaa, BitTorrent, LimeWire, WinMX etc. Also avoid the sharing of files, printers or other form of resources whilst on the network. These activities can open the network to the outside world, accesses to e-mail, bank pin numbers, introduce viruses, malware and even Denial of Service (DoS) attacks that floodthe network with data and incapacitate the computers/Access Points.

7.) *Use of radio frequencyShielding* : It's practical in some cases to apply specialized wall paint, window film, or the use of walls/opaque objects, to significantly attenuate wireless signals, (since these wireless signals are usually radio signals often times that can be inhibited by these substances/ instruments) which keeps the signals from propagating outside a facility. This can significantly improve wireless security because it's difficult for hackers to receive the signals beyond the controlled area of an enterprise, such as within parking lots. It is not the best option but can contribute immensely also.

8.) *use of smart cards, usb tokens, and software tokens*: This is a very strong form of security. When combined with some server software, the hardware or software card or token will use its internal identity code combined with a user entered PIN to create a powerful algorithm that will very frequently generate a new encryption code. The server will be time synced to the card or token. This is a very secure way to conduct wireless transmissions. Companies in this area make USB tokens, software tokens, and smart cards. They even make hardware versions that double as an employee picture badge. Currently the safest security measures are the smart cards / USB tokens. However, these are expensive.

9.) *careful site surveying :*This measure when done well, can identify locations where radio signals from other Access Point devices hanging around the organization exist/concentrate; the resulting output of such surveys could enhance the decision making of where the organizational wireless access points should be located/installed.

10.)*Use of directional antennas*: Although this is more costly method for reducing or hiding radio signals from unauthorized Access Points/hackers, it easily offerse better solution by directing/constraining radio signal emanations from the organizational network Access Point within desired areas of coverage only.

VI. CONCLUSION

The advent of Wireless networking technology suddenly sprouted in many opportunities in computer industry which sporadically increased productivity, efficiency, throughput and with great costs cutting. On the other-hand, it altered the entire organizational computer security risk profile. This again became a deep concern because of the havocs it created which led to diverse measures of securities, installed and deplored consequently. Although it wasn't possible to totally eliminate all the risks associated with wireless networking, but yet a reasonable level of overall security was achieved by adopting a systematic approach to assessing and managing the risk.

With a well secured wireless infrastructure such as those using (WPA2, WPA-PSK, activated 802.11iRSNA, non broadcast of SSID carelessly, strong firewalls & passwords, Smart Card, USB and software tokens etc.) in place, businesses can actually encourage their employees, authorized guests/visitors to bring-in their favorite wireless devices to work officially. Rather than attempting to enforce a blanket "i.e. no-wireless policy," which will do little or nothing, to enhancing the security of the organization and much more rather, sapping their employee's morale; sales representatives, supervisors and other personalities , should be allowed to use their wireless devices they feel most comfortable with, during official hours thus enabling them to work at maximum productivity for increased throughput of the organization, without fear of any mobile Unauthorized Access Point/hackers breaking through the security.

REFERENCES

[1] http://compnetworking.about.com/cs/wireless/g/bldef_ap.htm
[2] http://www.computerweekly.com/feature/Securing-your-networks-against-the-risk-of-rogue-wireless-access-is-no-longer-optional.
[3] http://www.wifiplanet.com/tutorials/article.php/1564431
[4] http://www.giac.org/paper/gsec/4060/rogue-wireless-access-point-detection-remediation/106460
[5] http://compnetworking.about.com/cs/wireless/g/bldef_ssid.htm
[6] http://www.juniper.net/techpubs/en_US/junos-space-apps12.3/network-director/topics/concept/wireless-ssid-bssid-essid.html
[7] http://rfakeap.tuxfamily.org/#Raw_Fake_AP
[8] http://searchnetworking.techtarget.com/tutorial/Network-Security-First-step-Wireless-threats

