Available online at www.pelagiaresearchlibrary.com

Pelagia Research Library

Pelagia Research Library

Advances in Applied Science Research, 2014, 5(4): 113-116

Pelagia Research Library

ISSN: 0976-8610
CODEN (USA): AASRFC

Threats and security measures on wireless local area networks

Inyiama H. Chibueze[1], Achi I. Ifeanyi[*2] and Agwu O. Chukwuemeka[3]

[1]*Department of Electronic and Computer Engineering, Nnamdi Azikwe University-Awka, Nigeria*
[2]*Department of Computer Science, Our Saviour Institute of Science and Technology, Nigeria*
[3]*Department of Computer Science, Ebonyi State University-Abakaliki, Nigeria*

ABSTRACT

The demands on Wireless Local Area Networks (WLANs) are growing due to the ever increasing proliferation of network devices and applications [14]. The number of devices and connections per user is rapidly on the increase. It is common for most flexible mobile users to have not only primary computing devices but also at least one or more smart devices. However, advent of Information and Communication Technology (ICT) and its adoption has made the wireless networking readily available, affordable, and easy to use. Many users use wireless technology for domestic as well as commercial purposes. This use has to take care of certain security threats that may be encountered. This paper analyses those threats and suggests the necessary measures so that both home based and publically situated wireless networks can be well guarded.

Keywords: Wireless Local Area Networks (WLANs), Information Communication Technology (ICT), Crackers, Encryption.

INTRODUCTION

The advancement in science and technology has empowered us with tremendous power to deal with various segments of human life. These advancements have, however, also given rise to certain deviances and criminal tendencies. The same equally applies in the present era of ICT. The ICT has conferred tremendous control over the information we generate and disseminate. So much is the benefit of ICT that the traditional means and modes of human interactions have been substituted by ICT. The same has resulted in use of e-governance, e-commerce, etc that have drastically reduced the face to face human interaction. The instrument or tool that made all this possible is a computer connected to the Internet. Initially, the Internet was used for computers connected through cables and routers.[1] Routers in a home network are generally connected to a broadband cable or DSL[2] modem. But with the advancement of technology even wireless communication and interaction is possible. Wireless routers perform the same job as wired routers, only they convert network traffic to a radio signal. This convenience has to be enjoyed with caution otherwise it may be a costly affair in every sense. The use of Internet has changed the entire platform of crime and criminal perpetuating the same. Crimes like hacking, pornography, privacy violations, spamming, phishing, pharming, identity theft, cyber terrorisms, etc are increasing day by day. The modus operendi[3] adopted for these cyber crimes and contraventions is different from the traditional crimes that make it very difficult to trace the culprits. This is because of the anonymous nature of Internet. The Internet is boundary less and that makes the investigation and punishment of crime very difficult. This is more so if an unsecured wireless connection is involved in any transaction. The need of the hour is to set priority for a secure and safe electronic environment so that its

benefits can be reaped to the maximum possible extent.[4] The wireless security must be accepted and adopted for both home based and publicly placed wireless networks.

2. NETWORKS TO BE PROTECTED

Wireless networks are very common, both for organisations and individuals. Many laptop computers have wireless cards pre-installed for the buyer. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into non-wireless networks. Network administrators must be aware of these risks, and stay up-to-date on any new risks that arise. Also, users of wireless equipment must be aware of these risks, so as to take personal protective measures.[5]

A. HOME WIRELESS THREATS

The need to secure traditional wired Internet connections was felt long before. However, there is a growing trend of shifting to a wireless connection at homes. This involves a process where the user connects a device to his DSL or cable modem that broadcasts the Internet connection through the air over a radio signal to his computer. If traditional wired connections are susceptible to security tribulations, there is a great risk of security breach that may arise when a user opens his Internet connection to the airwaves. An unsecured wireless network coupled with unsecured file sharing can be disastrous. There are, however, steps one can take to protect the wireless network. The following are some of the possible security steps:

(i) Make the wireless network invisible by disabling identifier broadcasting,
(ii) Rename the wireless network and change the default name.
(iii) Encrypt the network traffic,
(iv) Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network,
(v) Use file sharing with caution. If the user does not need to share directories and files over his network, he should disable file sharing on his computers.
(vi) Keep the access point[6] software patched and up to date,
(vii) Check internet provider's wireless security options as it may provide information about securing your home wireless network,
(viii) Do not auto-connect to open Wi-Fi (wireless fidelity) networks
(ix) Turn off the network during extended periods of non-use, etc.

B. PUBLIC WIRELESS THREATS

The risks to users of wireless technology have increased exponentially as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Currently, however; there are a great number of security risks associated with wireless technology. Some issues are obvious and some are not. At a corporate level, it is the responsibility of the Information Technology (IT) department to keep up to date with the types of threats and appropriate counter measures to deploy. Security threats are growing in the wireless arena. Crackers have learned that there is much vulnerability in the current wireless protocols, encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has become much easier and more accessible with easy-to-use Windows-based and Linux-based tools being made available on the web at no charge. IT personnel should be somewhat familiar with what these tools can do and how to counteract the cracking that stems from them.[7] Accessing the internet via a public wireless access point involves serious security threats. These threats are compounded by the inability to control the security setup of the wireless network. The following steps can be taken to protect oneself at public places:

(i) Be careful while dealing in an online environment if the network is not properly secured. Avoid online banking, shopping, entering credit card details, etc,
(ii) Connect using a virtual private network (VPN) as it allows connecting securely. VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted,
(iii) Disable file sharing in public wireless spaces as it is more dangerous than it is on your home wireless network,
(iv) Be aware of your surroundings while using a public wireless access point. If an internet connection is not essential, disable wireless networking altogether.

C. CORPORATE SECURITY

The network of companies are equally vulnerable to various cyber attacks and if not properly secured may cost the company tremendous loss of information and money. The following are the types of unauthorised access generally found at companies networks:

(i) Accidental Association: Unauthorised access to company wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as "accidental association". This is when a user turns on their computer and it latches on to a wireless access point from a neighboring company's overlapping network. The user may not even know that this has occurred. However, this is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

(ii) Malicious Association: "Malicious associations" are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops are known as "soft APs" and are created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point. Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans.

(iii) Ad-Hoc Networks: Ad-hoc networks[8] can pose a security threat. Ad-hoc networks are defined as peer to peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little security, encryption methods can be used to provide security.

(iv) Non-Traditional Networks: Non-traditional networks such as personal Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even bar code scanners, handheld PDAs,[9] and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel that have narrowly focused on laptops.

(v) Identity Theft (MAC Spoofing): Identity theft occurs when a cracker is able to listen in on network traffic and identify the MAC[10] address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorised computers with specific MAC IDs to gain access and utilize the network. However, a number of programs exist that have network "sniffing" capabilities. Combine these programs with capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

(vi) Man-In-The-Middle Attacks: A man-in-the-middle attack is one of the more sophisticated attacks that have been cleverly thought up by crackers. This attack revolves around the attacker enticing computers to log into his/her computer which is set up as a soft AP. Once this is done, the cracker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent cracking computer to the real network. The cracker can then sniff the traffic for user names, passwords, credit card numbers...etc. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols. It is called a "de-authentication attack". This attack forces AP-connected computers to drop their connections and reconnect with the cracker's soft AP. Man-in-the-middle attacks are getting easier to pull off due to freeware such as LANjack and AirJack automating multiple steps of the process. What was once done by cutting edge crackers can now be done by less knowledgeable and skilled crackers sitting around public and private hotspots.[11] Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

(vii) Denial of Service: A Denial-of-service attack occurs when an attacker continually bombards a targeted AP or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

(viii) Network Injection: The final attack to be covered is the network injection attack. A cracker can make use of AP points that are exposed to non-filtered network traffic. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.[12]

CONCLUSION

The growing penetration of Internet in the day to day affairs of Nigeria society has both positive and negative effects. Recently, Nigeria is ranked first in Africa in the rating of countries with the highest Internet Users [15]. The positive side of this is the advent of e-governance, e-payment and e-commerce in Nigeria. The use of e-governance will provide a transparent, accountable and hassle free citizen and Government interaction. Similarly, e-commerce is also facilitated with the use of ICT while e-payment is defining the way payments are made in e-commerce platform. The e-commerce is a well known phenomenon of the global trade that is gaining momentum in Nigeria

with the recent adoption of cashless economy. However, neither e-governance nor e-commerce or e-payment can be a success in Nigeria until we secure these infrastructures. This will further militate against the widespread adoption of the proposed cashless economy as contained in the vision 2020 agenda. Any ICT infrastructure is ineffective till we are capable of securing and protecting it. It must be appreciated that the ICT infrastructure of a nation can exist only to the extent it can be protected from internal and external online attacks. This "need" becomes a "compulsion" due to the provisions of IT Act, 2000 that fixes both civil and criminal liability for failure to act diligently. Both the citizens and companies are required to establish a sound and secure ICT infrastructure to escape the accusation of lack of "due diligence".[13] The need of the hour is to secure both home based and publically situated wireless networks.

REFERENCES

[1] D. Ngo, (2013), Home Networking Explained, Part 5: Setting up a Home Router, Online at: http://www.cnet.com/how-to/home-networking-explained-part-5-setting-up-a-home-router/
[2] M. Rouse, (2010), Fast Guide to DSL (Digital Subscriber Line), Online at: http://whatis.techtarget.com/reference/Fast-Guide-to-DSL-Digital-Subscriber-Line
[3] G. Karame, I. Christou and T. Dimitriou, (2008) "A Secure Hybrid Reputation Management System for Super-Peer Networks", In Proceedings of IEEE CCNC.
[4] P. Dalal, (2006), "Cyber security in India: An ignored world", Online at: http://cyberforensicsinindia.blogspot.com/2006/08/cyber-security-in-india-ignored-world.html
[5] R. Acharya, V. Vityanathan and R. Pether, (2009), "Wireless LAN Security – Challages and Solutions", International Journal of Computer and Electrical Engineering, Vol 1, No 3.
[6] K. Konstantinos, (2006), "Ten Steps to a Secure Wireless Network".
[7] R. Scotland, (2013), "Unsecure or Secure: The Network Security Challenge for Small and Mid-size Businesses".
[8] J. Bola, (2002), "Wireless LANs Demystified".
[9] R. Wiggins, (2004), "Personal Digital Assistant", Online at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3043961/.
[10] B. Mitchell, (2010), Medium Access Control(MAC), Online at: http://compnetworking.about.com/od/networkprotocolsip/g/bldef_mac.htm.
[11] K. Sanka,S. Sundaralingam,A. Balinsky, and D. Miller "Cisco Wireless LAN Security",Cisco system inc,2005.
[12] Wikipedia, (2013), Wireless Network Security, Online at: http://en.wikipedia.org/wiki/Wireless_security
[13] P. Dalal, (2006) "The need of techno-legal compliance in India", http://perry4law.blogspot.com/2006/06/need-of-techno-legal-compliance-in.html
[14] Cisco Systems Inc., (2011), Wireless LAN Design Guide for High Density Client Environments in Higher Education.
[15] Wikipedia, (2012), List of Countries by number of Internet Users, Online at: http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users