

Wi-Fi: Unknown risks to enterprise Networks in Lagos Metropolis (A basic advisory on Wi-Fi threats)

By Anu Odusami (CCWP, MCSA, MCSE)

X-wireless Project

aodusami@x-wireless.lexium.net

<http://x-wireless.lexium.net>

No doubt, wireless technologies have made life worth living by providing consumers of ICT products with mobility and flexibility. Wi-Fi (Wireless Fidelity) is no exception, as this technology has contributed immensely to the deployment and implementation of cost effective enterprise networks. It's interesting the rate at which enterprise IT departments are fast adopting the Wi-Fi technology as an integral part of their IT infrastructure.

This technology is quite convenient as compared to deployment of hard wired networks but believe me it has horrifying downsides if enterprise security is compromised. The issue of vulnerability poses a major threat to enterprise security if adequate security measures and policies are not implemented.

Moving around Lagos metropolis in search of free public hotspots, I came across several access points (APs) with little or no security implementation. It's alarming to know the numbers of organisations found on the compromised list.

Do these people actually run information driven organisations? , that's a question am yet to find the answer and if it happens to be yes, information security should be one of the key priorities of such organisations. Clients' information or company's records should be kept away from preying eyes. It was possible to gain access to some of these unsecured networks and this is all a malicious hacker needs to launch a Denial of Service (DOS) attack.

Wi-Fi risks to Enterprise Wired Network

You might be pondering what kind of threats will Wi-Fi pose to an enterprise wired network which does not have Wi-Fi as a part of its network infrastructure. A lot of network administrator have the presumption or rather misconception that there network is completely safe from Wi-Fi threats which is absolutely wrong. Your enterprise maybe connected to Wi-Fi through Wireless NICs in client's laptops to another laptop or to a rogue access point without the knowledge of the network administrator.

Most Laptops today comes with built in Wireless NICs and this cards work in two different modes namely;

- a) Infrastructure mode: Infrastructure mode is when you connect to an access point, perhaps in your office, at home, or at a public hotspot
- b) Ad-Hoc mode: allows you to configure your laptop to act like an access point and also have others connect to you through a peer-to-peer wireless connection.

Most wireless laptops by default from the manufacturer are set in ad-hoc mode. This brings us to the vulnerability posed by **Wired & Wireless Dual Homing**. Modern laptops have two NICs - one for a wired connection (Ethernet) and one for Wi-Fi connection (Wireless). This enables the laptop to be dual homed, or connected to two networks at the same time. If the Wi-Fi card is set to ad hoc mode, and the user logs on to the wired network, an attacker can easily connect to the laptop via the ad hoc connection and gain access to the wired portion of the enterprise network using the dual homed laptop as a conduit (*Bingo!*).

Network Administrators should ensure that network security policies are adhered to by network users and also take adequate preventive measures. User complacency is major problem but with proper user awareness this will be drastically minimized.

Rogue & Unsecured Access points

Hackers are known to set up APs with default SSIDs, hotspot SSIDs, and even corporate SSIDs outside of buildings and watch a large number of clients automatically connect to the AP. These APs can then inflict a variety of attacks on the client or attempt password stealing by presenting a login page to the client over the mis-associated wireless connection. Examples include The Promiscuous Client and the so much talked about "*Evil Twin*" which captures network and computer data from some unsuspecting users, unfortunately the only way to prevent this attack is to avoid unsecured APs.

Wireless network viruses

I guess everyone is quite familiar with the word Virus, at the mention of the word what comes up on your mind is Malicious, disastrous, destroyer etc. You know how horrifying it could be when you are infected I could go on and on but there's no point crying over spilled milk instead learn not to spill it again so is the scenario we have here. There are viruses, and then there are wireless viruses. For example, "MVW-WiFi" is powerful Virus worm which has the ability replicate and propagate its bores into a laptop through a wireless network, sends out wireless probe request packets to find other local wireless networks and then forwards itself to adjacent wireless networks. To prevent such an attack one should have a reliable antivirus installed with regular updates.

Conclusion

Whether you're using a Wi-Fi enabled Personal Digital Assistant (PDA) or a Laptop, you can steer clear of these threats by double checking your security settings. Nearly two-thirds of all wireless users are on an unsecured network, according to several surveys. So it imperative for us to change our perception to the way we use unsecured connections because it could be a connection to catastrophe.