Investigating the Effectiveness and Performance of WPA_PSK (Pre-Shared Key) and WPA_RADIUS Server in Wireless Network Security

Musibau A. Ibrahim

Department of Information and Communication Technology, Osun State University, Osogbo Campus, Osun State, Nigeria

Abstract

In this research paper, Wireless local area (WLAN) connections and access security were investigated in terms of roaming between access points, setting up an ad-hoc Network and sharing internet access via ADSL router. Finally, the WLAN packets were captured and analyzed with the wire shack analyzer. The paper demonstrates the effectiveness and performance of WPA-PSK and WPA_RADIUS in terms of access security in wireless networks.

Keywords: *Wire shark, Encryption, Pre shared key, Radius, ADSL, Packets*

1. Introduction

Wireless networking is causing a revolution in computing and Internet access. Wireless Local Area Networking (WLAN) frees users from the constraints of cables in the office or home environment. Ideal for notebook PC users wanting mobility and for desktop users requiring access to networks where the traditional wired method is impractical or prohibited such as in listed buildings or across public highways. The arrival of the IEEE 802.11b Wi-Fi standards meant that most vendors could provide a low cost compatible solution for wireless communication over the local area, at speeds on a par with basic wired Ethernet technology. Prior to IEEE 802.11 brand x radio would not work with brandy access point. The WLAN standard continues to evolve to provide higher speeds, greater range and better security than the earlier systems. Both radio and optical (laser or infrared light) transmission methods are used for the wireless connectivity of computer systems, but radio systems are by far the most popular as they have greater range and don't require line of sight. Wireless versions of the *Network Interface Card* (NIC) are employed to transmit and receive the signals and *Access Points*, are used to concentrate and repeat these transmissions or bridge to wired network equipment such as hubs or switches (Figure 1) **(White, R 2010)**

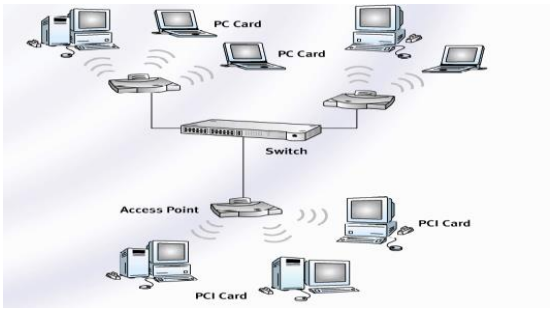


Fig. 1: Wireless access points

1.1 Security issues with WLAN and IEEE 802.11i

Security is a major concern in any wireless network because any computer or PDA equipped with a WLAN card can pick up the signals. Also the WEP (Wired or Wi-Fi Equivalent Privacy) layer2 encryption method used by IEEE 802.11b is seen as insecure (easily cracked). There are, however, many ways to make WLANs as secure as wired networks. The more effective WPA (Wi-Fi Protected access) technology is now being used in by most IEEE 802.11g technology, which is a subset of the new IEEE 802.11i standard designed to be used with the IEEE 802.1X extensible authentication protocols to stronger data link encryption and then the fixed key method of WEP and improved access security. WPA2 provides authentication support via IEEE 802.1X and **PSK** (Pre Shared Keys) for the following applications:

- **Personal Mode** is a term given to products tested to be interoperable in the PSK-only mode of operation for authentication. It requires manual configuration of a pre-shared key on the access point and clients. PSK authenticates users via a password, or identifying code, on both the client station and the access point. No authentication server is needed and Personal Mode is targeted to SOHO environments.
- **Enterprise Mode** is a term given to products that are tested to be interoperable in both PSK and

IEEE 802.1X/EAP modes of operation for authentication. When IEEE 802.1X is used, an authentication, authorization, and accounting (AAA) server (the RADIUS protocol for authentication and key management and centralized management of user credentials) is required. Enterprise Mode is targeted to enterprise environments (Figure 2) (**Holroyd c., 2009).**

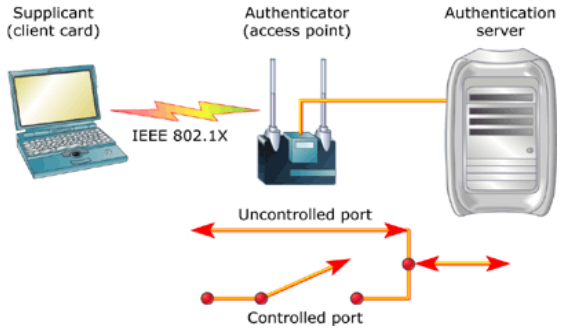


Fig. 2: Access Control in Enterprise mode

2. Other Access Control methods

Data link access control via the access point identifiers (SSIDs) offer some degree of protection against unauthorised access – if a station does not know this value then it is not allowed to associate. Turning off SSID broadcasting, which is on by default on some access points, is only a mild deterrent to hackers as packet sniffing will easily reveal the name of the access point when an authorized node transmits a frame. Access control lists of MAC addresses can also be included in the Access Point used to restrict access to known users entered into a table, but again hackers can easily spoof (or clone) MAC addresses (pretend to be a valid user) to gain access. If security is a major concern**,** however, users are being advised to implement higher layer authentication methods or use Virtual Private Network (VPN) or VLAN techniques. For mid to large networks, WLAN switches can simplify administration and Enterprise Wireless gateways (EWGs) can ease the authentication and connectivity issues. **(Schaefer, S 2003)**

3. Association, Inter-Cell Communication and Roaming

The process of connecting a node to an access point is called 'Association' This occurs when a node moves within range and tunes its radio channel to what the access point is set to.

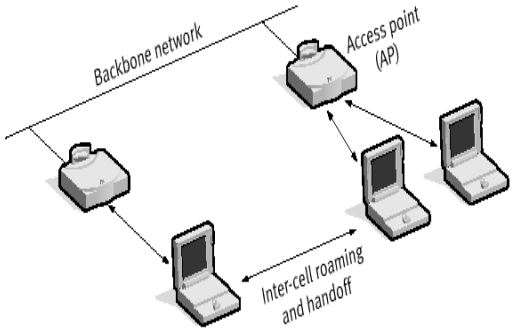


Fig. 3: Inter-cell Communications and Roaming

Inter-cell communication of nodes connected to different access points by a distribution system or backbone network as in Figure 3 is accommodated by a frame structure which contain four MAC addresses. How these addresses are interpreted depends on the setting of the DS bits in the control field. In the simplest case, two addresses identify the source and target wireless nodes (DS=00) but in the most complex (DS=11) two additional intermediate addresses are needed. Addr1 is the destination node, Addr2 is source node, and Addr3 is the local access point that forwards the frame to the destination access point Addr3.

Roaming, the ability of a mobile computer to move between access points is an important feature of larger WLANs. Roaming provides a continuous network service for mobile workers by a technique called 'scanning' and 're-association'. The wireless node assesses the received signal level from each access point within range and then resynchronises (adjusts channel settings) to the stronger as the user moves between service areas using either active or passive scanning. Active scanning employs four steps involving an interchange of frames: (1) node sends a probe frame, (2) all APs within range reply with a probe response, (3) node selects an AP by sending an association request and (4) the AP replies with an association response. In passive scanning the APs send out Beacon frames periodically and nodes wishing to change AP send back an association request. Beaconing is also used to awaken nodes in power save polling mode and advertise other access point services. The process of dynamically associating and re-associating with access points allows network managers to set up WLANs with a very broad coverage by creating a series of overlapping cells as in Figure 10, but care must be taken to ensure that channels do not overlap. The wireless node assesses the received signal level from each access point within range and then resynchronises (adjusts channel settings) to the stronger as the user moves between service areas using either active or passive scanning. Active scanning employs four steps

involving an interchange of frames: (1) node sends a probe frame, (2) all APs within range reply with a probe response, (3) node selects an AP by sending an association request and (4) the AP replies with an association response. In passive scanning the APs send out Beacon frames periodically and nodes wishing to change AP send back an association request. Beaconing is also used to awaken nodes in power save polling mode and advertise other access point services. **(Bauman, Z 2007)**

The process of dynamically associating and re-associating with access points allows network managers to set up WLANs with a very broad coverage by creating a series of overlapping cells as in Figure 4, but care must be taken to ensure that channels do not overlap.

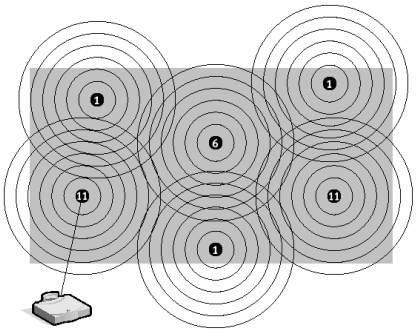


Fig. 4: IEEE 802.11b DSSS cell overlap

In IEEE 802.11b there are only three of the 14 channels that do not overlap at all so these should be used if at all possible. If two partially overlapping channels are used they may cause interference for one another, leading to reduced bandwidth in the overlapping area. Not all channels are available in some regions, ***(Kizza, JM 2011).*** WPA–PSK is the technique recommended for home use and small business networks without a RADIUS server. WPA is more secure than WEP, but can still be compromised. Here the EAP authentication packets would be captured on the client PC with Wire shark as it is authenticated by the AP. WPA supports two modes of operation. WPA Enterprise is for environments with a RADIUS infrastructure and uses an EAP authentication method. WPA Personal is for environments without a RADIUS infrastructure and uses a pre-shared key for authentication. For a home or small business WPA (Wi Fi Protected Access) provides a pre-shared key authentication method for infrastructure mode wireless networks. The pre-shared key is configured on the wireless AP and each wireless client. We consider some experimental analysis to demonstrate the effectiveness of the AP using WPA-PSK. The procedures for the experimental setup are as follows;

- Configure the AP to use WPA-PSK and enter a pre-shared network key (passphrase) to generate the key.
- Create a new profile for your WLAN connection called wpa1 and configure it to match the new AP security settings, and then test access as before.
- Test connections between PCs by Pinging another client as before and determine if the data is now encrypted. Analyse the packets to see that WPA is now being used and see that the IEEE 802.1X EAP authentication packets are as in Figure 5.

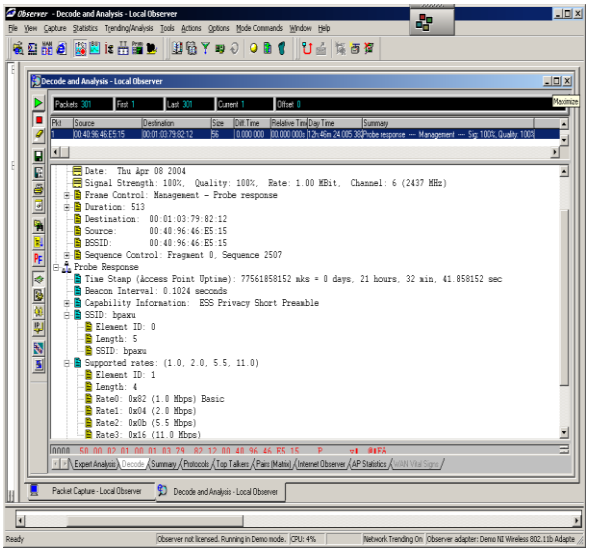


Fig. 5: Local observer for a four way handshake

From figure 5, the initial WPA encryption key is derived from the authentication process, which verifies that both the wireless client and the wireless AP are configured with the same pre-shared key. Each initial WPA encryption key is unique and 4 way handshake is done by EAP packets.

4. IEEE 802.1X - WPA with Radius: This is the recommended method for enterprise wireless networks. It makes use of IEEE802.1X and a Radius server for authentication and key distribution. In this exercise we will use the standard method for Microsoft enterprise WLAN installations called PEAP. This overcomes security issues for wireless connections where EAP occurs during the IEEE 802.1X authentication process, before wireless frames are encrypted. The IEEE 802.1X standard defines port-based, network access control used to provide authenticated network access for Ethernet networks. Although this standard was designed for wired Ethernet, it

has been adapted for use by 802.11. IEEE 802.1X uses the Extensible Authentication Protocol (EAP) and specific authentication methods known as EAP types to authenticate the network node. The IEEE 802.1X standard enforces authentication of a network node before it can begin to exchange data with the network. Exchanging frames with the network is denied if the authentication process fails. IEEE 802.1X provides much stronger authentication than open system or shared key and the recommended solution for large networks requiring better security is an issue ***(Fenna, A 2010).*** This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. Although this standard was designed for wired Ethernet networks, it has been adapted for use on 802.11 wireless LANs as shown in Figure 6.

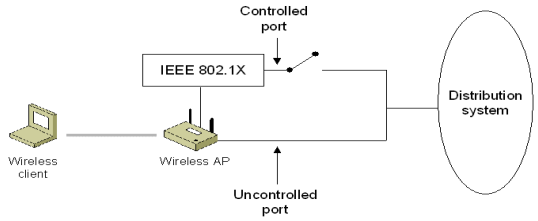


Fig. 6: Wireless Network Access Control

In the second experiment, the authenticator's port-based access control defines the following different types of logical ports that access the wired LAN via a single physical LAN port:

- Reconfigure the AP to use WPA-with Radius and specify the Radius server details as shown in Figure 6. Review the Radius server settings to show how it is configured in conjunction with the AP.
- Create a new profile for your WLAN connection called WPArad1 and configure it to match the new AP settings. Supply login details when requested.
- Test connections between PCs using Ping as before and determine if the data is now encrypted.
- Analyse the packets to see the authentication procedure shown in Figure 6 is now being used. To do this you will need to capture EAP packets on the client and Radius PCs using Wire shark while authentication takes place.

Radius Server Settings

Primary Authentication Server

IP Address 192 . 168 . 0 . 123

Port Number 1812

Shared Secret richard123

Fig. 7: Security Profile configuration

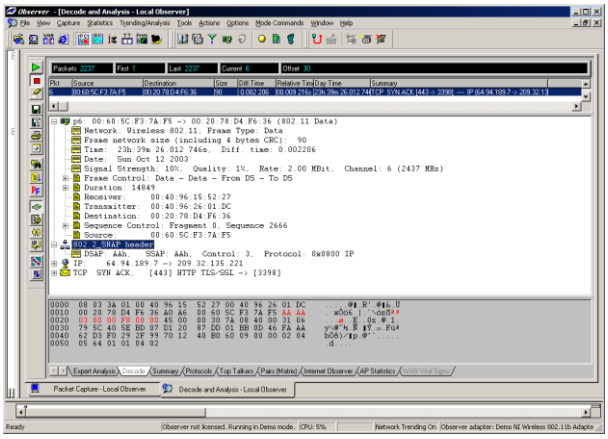


Fig. 8: Observer for packets analysis

As can be seen from the results, it was observed that authentication procedure is now being used when the EAP packets on client and PCs were captured. Please see the details of the packets analysis as follows:

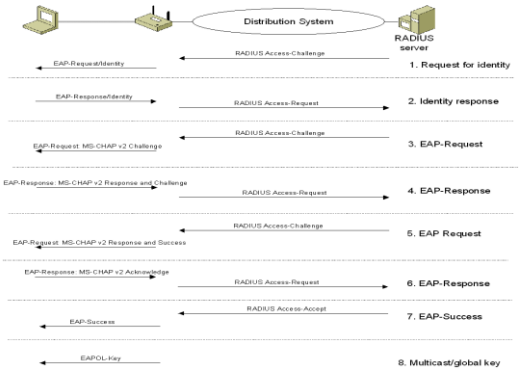


Fig. 9: Other IEEE 802.11 security measures

In addition to WEP encryption, the following techniques are sometimes used to protect 802.11 wireless networks**:** Non-broadcast wireless networks and MAC address filtering.

In the third experiment, the wireless APs for non-broadcast mode prevents the casual wireless client from discovering your wireless network. However, even the most unsophisticated malicious user can capture the messages containing the wireless network name sent by wireless clients or your wireless AP and determine your

wireless network name. Here, we determine the SSID of a Netgear AP that has had its broadcasting name facility disabled as shown in Figure 10. Configuration and the set up for the AP for open access and disable SSID broadcasting are shown in Figure 10. Capture packets for the AP and Show that the SSID is not displayed in the wlan packet.

Security Profile 3 Configuration 11b/g

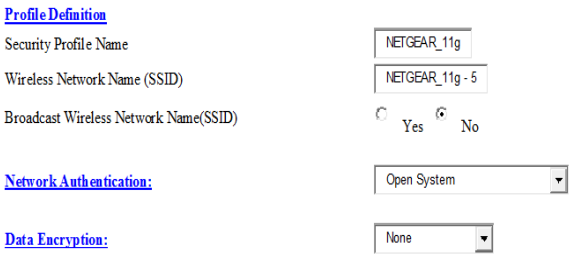
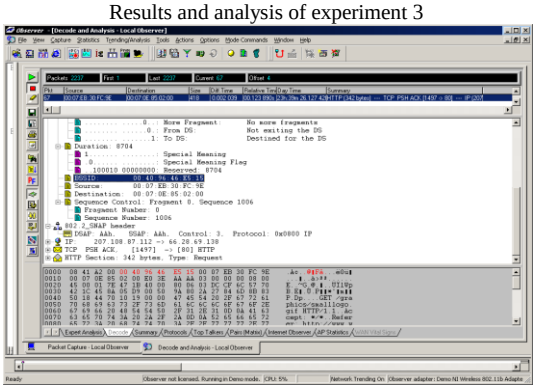


Fig. 10: Security Profile configuration

Capture probe/response packets with the Observer and decode to reveal the SSID of another client connecting to the network. The Kismet scanner will reveal hidden ssids without you having to analyse probe packets.

Results and analysis of experiment 3



The results of this experiment reflected that without SSID the packets captured can reveal the SSID of other clients connected to the network. In other words, turning off SSID broadcasting is useless because a hacker can use packet sniffing software to capture the SSID even if broadcasting is turned off. Turning off broadcasting won't deter a serious hacker, but it will protect from the casual "piggybacker".

5. Conclusion

This paper has presented the development of WPA_PSK and WPA_RADIUS for efficient and effective wireless communication. This is demonstrated by several experimental analysis conducted using wire shark analyser and observer packages. In terms of security and bandwidth consumption, the network systems developed have proven to be very robust such that it is almost impossible for hackers to crack the network guided with these latest protection measures.

Reference

[1] Bauman, Z 2007, Globalization and culture, Polity Press, Oxford.
[2] Tomlinson, J 2008, Globalization: the human consequences, Routledge, London.
[3] Besanko, D, Dranove, D, Shanley, M & Schaefer, S 2003, Economics of strategy, 3rd edn, J.Wiley, New York.
[4] Coates, K & Holroyd c 2009, Japan and the internet revolution, Palgrave Macmillan, New York.
[5] Denzin, NK & Lincoln, YS (eds) 2010, the landscape of qualitative research: theories and issues, 2nd edn, Sage, Thousand Oaks, CA.
[6] Fenna, A 2010, Australian public policy, 2nd edn, Pearson Education Australia, Frenchs Forest, NSW.
[7] Kizza, JM 2011, Computer network security and cyberethics, McFarland, Jefferson, N.C.
[8] Pfeiffer, JW (ed.) 2009, Theories and models in applied behavioural science, vol. 4, Organizational, Pfeiffer, and San Diego.
[9] Watts, MM (ed.) 2010, and Technology: taking the distance out of learning, Josser-Bass, San Francisco.
[10] Wynn, J & White, R 2010, Rethinking youth, Allen & Unwin, St Leonards, NSW.