DETECTION OF WIRELESS ROGUE ACCESS POINT ATTACK ON SERVER SYSTEMS

Thompson A.F1Adebayo O.T2

Department of Computer Science
Federal University of Technology, Akure,Nigeria.

afthompson@futa.edu.ng1adebayoot@futa.edu.ng2

ABSTRACT: Rogue Access Points, if undetected, can be an open door to vital and sensitive information on the network. Most hackers have taken advantage of the undetected rogue access points in enterprises to not only get free Internet access, but also to view sensitive information. Most of the current solutions to detect rouge access points are not competent enough as hackers have found their way round the solutions in which most of it are not automated and are dependent on a specific wireless technology. A software applicationwhich can be installed on a server in order to compare the clients IP addresses to the ones that have been preconfigured on it and to also notify the network administrator about the occurrence was developed in this research work.

Keywords: Wireless, Rogue, Connectify, Acess point

1. INTRODUCTION

As wireless implementations have increased in enterprise environments, the security of these devices has become more of a concern. Deploying access points and restricting the use of these access points to authorized users has been a challenge due to the weak authentication and encryption. An ancillary problem posed by wireless access points, outside the security of authorized access points, is the detection of unauthorized access points, also called rogue access points.Many disparate Network Access Detection (NAD) tools are currently used in various establishments; these tools are not effectively integrated to work in conjunction with each other. Cyber security governing bodies actively involved with network security such as Industrial Control Systems Emergency Response Team (ICS-CERT) and DHS lack complete and coherent incident response information from individual establishments. Vulnerabilities from devices and policy at the system level must be identified to advance systems and tools that will guarantee durability of our criticalinfrastructure.Wireless access hasspecial security considerations as hackers have also step up their research on how to bypass different network securities. Many wired networks base the security on physical access control, trusting all the users on the local network, but if wireless access points are connected to the wireless network, clients within the range of the AP (which typically extends farther than the intended area) can connect to the network.

2 LITERATURE REVIEW

The most common solution is wireless traffic encryption. Modern access points come with built-in encryption. The first generation encryptionscheme WEP proved easy to crack; the second and third generation schemes, WPA and WPA2, are considered secure if a strong enough password or passphrase is used. This particular security type request for username and password before connection but this is still not reliable enough as hackers have found their way round this, bypassing network security and causing irreparable damages. Introduction of wireless prevention system, wireless sensors, applying MAC address and VLAN which are more reliable has been able to at least reduce rate at which hackers gain unauthorized access to wireless networks which is the reason for this research work.

Wireless LANs can greatly increase productivity and flexibility by providing anytime-anywhere access to business networks and systems. The same properties that make WLANs so convenient, however, can also leave them vulnerable to misuse and attack by unauthorized or malicious users and devices.

Rogue access point detection is an important aspect of wireless IDS (Intrusion Detection System) which is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. (Potter, 2007) Rogue access points can pose significant threats as intruders get unauthorized access to internet or information on a server through this medium.

In this project work, rogue device detection is implemented by executing a program running directly on a server, this software is preconfigured with some set of system's IP addresses which it automatically grant access to on the network prior to request and also deny systems with different IP address access to the network.

Basically, rogue access points comes in two ways; which are Internal and External.

The internal rogue access points are those that (for instance) an employee brings in and plugs into a corporate network. The access point is outside the control of IT personnel and serves as a gateway for attackers to gain access to the network, while the external (which is more difficult to control) is one that is controlled by an attacker and designed to spoof legitimate clients into connecting to it rather than the correct access point. Usually this is accomplished by setting the rogue access point SSID to the same SSID as the friendly access point and then boosting the signal of the rogue access point. This will cause client associations to come to the rogue access point. The attacker may then attempt to steal user's credentials via spoofed web pages and portals designed to trick users into giving up passwords, credit card numbers and other personal information. These types of rogue access points are generally easy to detect but difficult to turn off as the attacker then needs to be physically located. (Potter, 2007).

Rogue (which can be of hardware or software) can be defined in many other ways. Many define it as anything other than legitimate clients while some says anything on the wireless networks that is not authenticated is a rogue. For this project work, I define rogue as a device, AP, or client which is trying to connect, attack or interfere to the wireless network without authorization. (malicious entity).

There are various ways by which connection can be established, computer systems can establish a reliable connection either by wired, wireless, bluetooth or through internet creating either LAN, WAN or VPN network.

Moreover someone can create Distributed Denial Of Service (DDOS) attack to the AP. At the same time they can start broadcasting with the same SSID. In this case they can ensure AP is not functioning anymore and at the same time spoof the MAC Address of the AP and show clients a fake login page, a process referred to as Evil Twin attack (ETA). The Evil Twin attack achieves its objective by spoofing the MAC address of the legitimate AP and creates an evil twin. It also create Denial Of Service (DOS) attack on the legitimate AP and broadcast with higher power.

On the other hand, there are cases where an AP can broadcast with higher power and same SSID.

Once an AP is discovered, the next step is to identify whether it is a rogue AP or not. One way to do this is to use pre-configured authorized list of APs. Any newly detected AP that falls outside the authorized list would be tagged rogue.

3 Designed Model

The model is divided into three major parts which are:

- The administrative end software (on the server)
- The Database (also on the server)
- The client systems

During the course of this project, the following measures were implemented to check rogue access point attack;

Installation of a software package which performs the following functions:

- Give room for addition of new systems IP addresses or deletion of previous ones.
- Takes the IP address of any system requesting for connection, compare it to the authorized ones in the database and then decide to either grant or deny access based on the result of the comparison
- Notify the network administration about the attempt

A database which consist of the list of IP address of systems that should be granted access to the network.

Installation of a software application known as connectify on the server which allows the server to create an offline wireless connection which through which the client systems can connect to the server so as to be on the same network.

3.1 Rogue Access Point

A rogue access point is a wireless access point installed on a wired network without authorization from the network administrator. A rogue AP may be naively installed by a legitimate user who is unaware of its security implications or it could be deliberately installed as an insider. A rogue AP could also be easily smuggled onto the premises by an outsider. In any case, a rogue AP poses a serious threat to a wired network as it gives a wireless backdoor into the network for outsiders, bypassing all wired security measures such as firewalls and network access control (NAC)

3.1.1 Rogue AP Risk

In an ideal world, the only wireless devices in or near your facility would be known, trusted stations and access points (APs). But, as WLAN adoption grows, that becomes increasingly unlikely. Wireless transmissions from neighboring businesses and homes can easily bleed into your facility, at distances ranging from yards to miles. Furthermore, contractors, customers, suppliers, and other visitors to your facility are more likely than not to carry wireless-capable devices, including laptops, PDAs, and tablet PCs. In this crowded environment, it can be tough to differentiate between friend and foe. Even the dividing line is not that simple. A new, previously-unknown AP may turn out to belong to a neighbor's network. It may be an unauthorized AP, installed by a well-intentioned but naïve employee. Or it may be a malicious AP, hidden inside your facility for the express purpose of gathering proprietary information.

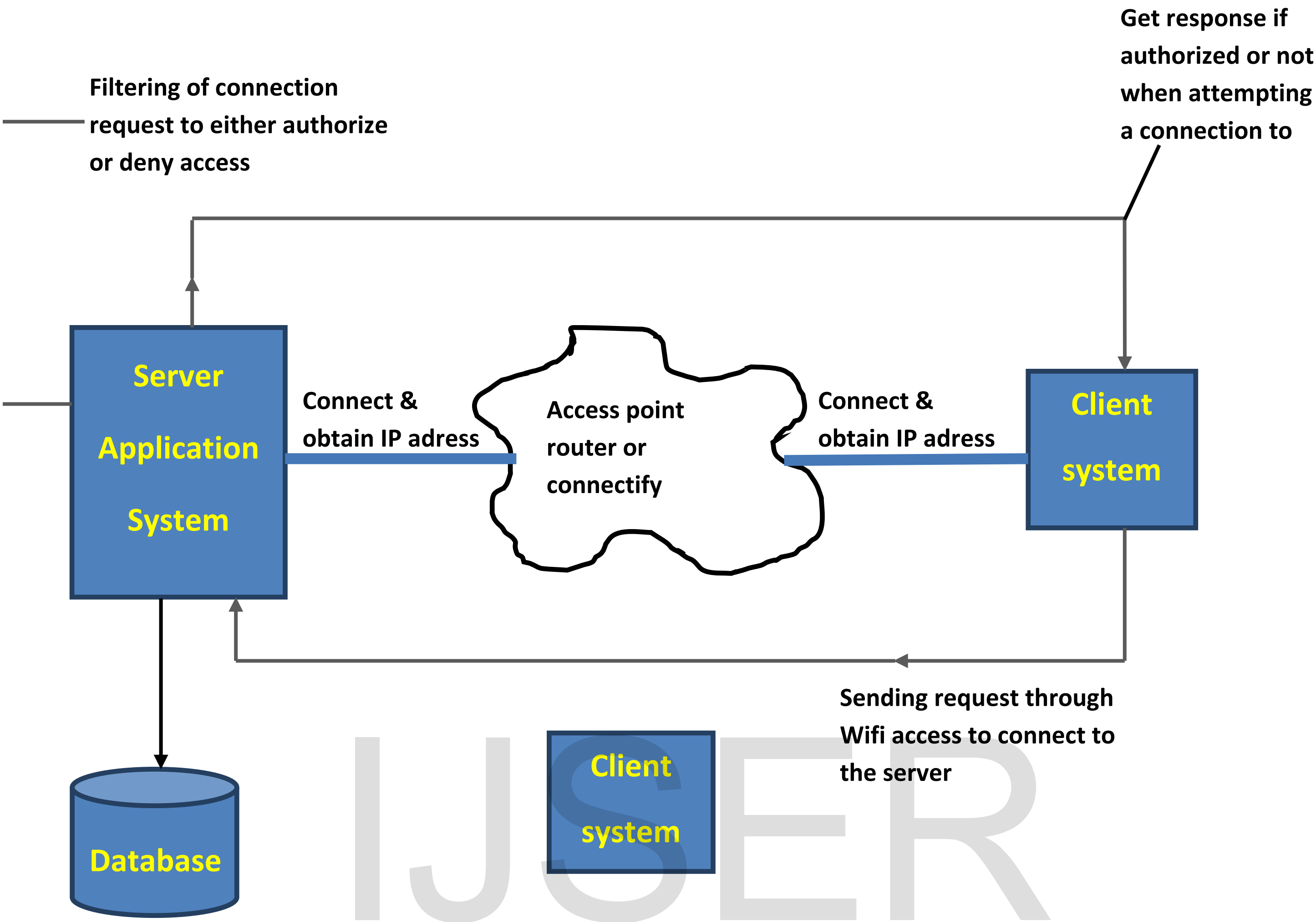

Get response if authorized or not when attempting a connection to
Filtering of connection request to either authorize or deny access
Server Application System
Connect & obtain IP adress
Access point router or connectify
Connect & obtain IP adress
Client system
Sending request through Wifi access to connect to the server
Client system
Database

Figure 1: System Architecture

4 SYSTEM IMPLEMENTATION

4.1 Administrators login page

This is a page where the network administrator login so as to make some necessary configuration such as adding the IP address of a new client or to delete an existing IP address depending on the administrators decision. This page is highly secured as the administrator don’t only need his/her login details to access this platform, the administrator can only perform this task on the dedicated server as the server IP address have been preconfigured with the login page so as to negate the risk of an intruder who may have secretly gotten the login details of the network administrator from having access to this page.

The figure below shows the administrator login page

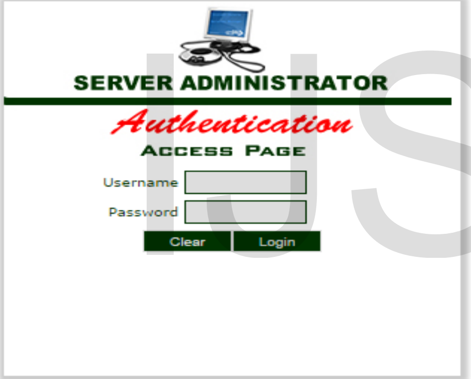


Figure 2: Administrators login page

4.2 User setup module

This is a platform where the network administrator performs his administrative duties. The network administrator can add new set of IP addresses or delete existing one.

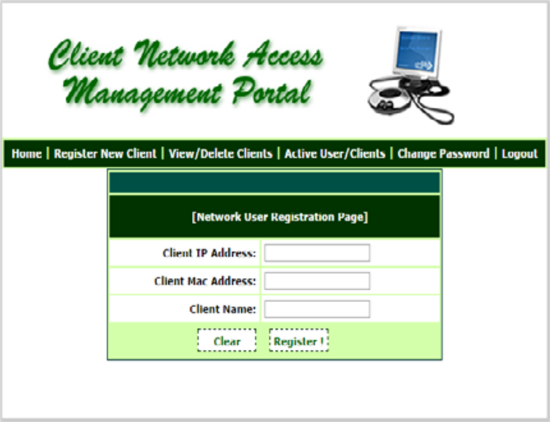
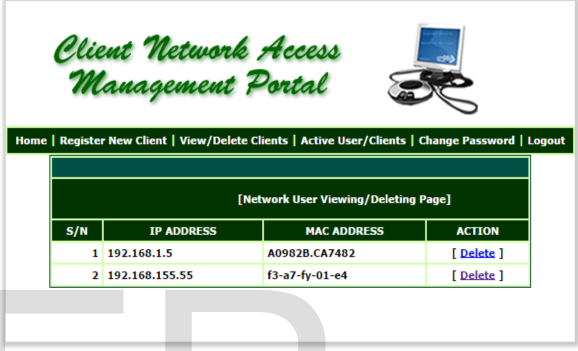

Client Network Access
Management Portal
Home | Register New Client | View/Delete Clients | Active User/Clients | Change Password | Logout
[Network User Registration Page]
Client IP Address:
Client Mac Address:
Client Name:
Clear
Register !

Figure3: Network user registration page


Client Network Access
Management Portal
Home | Register New Client | View/Delete Clients | Active User/Clients | Change Password | Logout

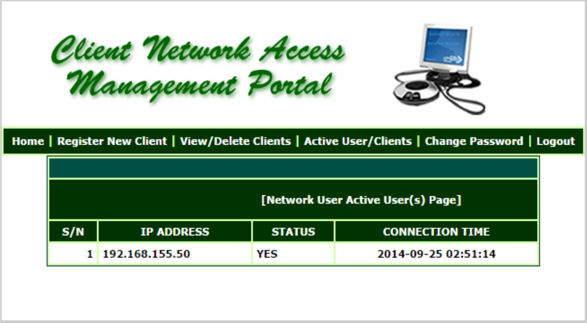
[Network User Viewing/Deleting Page]

S/N	IP ADDRESS	MAC ADDRESS	ACTION
1	192.168.1.5	A0982B.CA7482	[Delete]
2	192.168.155.55	f3-a7-fy-01-e4	[Delete]

Figure 4:Existinguser deletion page

4.3 User activity module

This is a platform where the network administrator monitors all the present activities on the server such as knowing the number of client connected to the server, been able to identify each client by their name and IP address and also know user's that are currently active or inactive on the network.


Client Network Access
Management Portal
Home | Register New Client | View/Delete Clients | Active User/Clients | Change Password | Logout

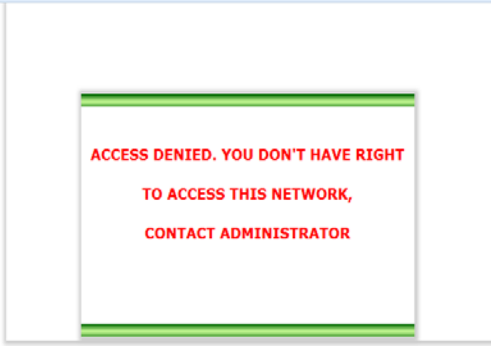
[Network User Active User(s) Page]

S/N	IP ADDRESS	STATUS	CONNECTION TIME
1	192.168.155.50	YES	2014-09-25 02:51:14

Figure 5:Client activity monitoring module

4.4 Error message notification

This refers to the error notification that will come up at the unauthorized client end when trying to gain unauthorized access to the network saying "***Sorry, you are not authorized to access this network***".



ACCESS DENIED. YOU DON'T HAVE RIGHT
TO ACCESS THIS NETWORK,
CONTACT ADMINISTRATOR

Figure 6: Error message page for unauthorized clients

4.5 Alert notification

This is a notification message which will pop-up at the administrators end notifying that a particular client with this name and IP address is trying to gain an unauthorized access into the network

5. Conclusion

Knowing fully well that the main purpose of this work is to improve network security, this project can be enhanced and further expanded to manage future security solutions and also provide a remote access in situations like capturing customers data by banks officials, processing of result by departmental exam officer, checking patient health record on the hospital central server. The work could be further developed to accommodate bigger network system and provide adequate security for organizations who wish to grant some limited and trusted employees access to some sensitive information or application on their main severs in a secured manner. This will serve as an invaluable improvement over the existing network solution and continually enhance the entire process of ensuring adequate security while granting some set authorized users access to a centralized server with vital and sensitive information.

REFERENCES

1. Ellingson, Jorgen. (2001). Layers One &Two of 802.11 WLAN Security.
   Retrieved July 22,2007, from http://www.giac.org/certified_professionals/practicals/GSEC/0996.php

2. Proxim White Paper: Rogue access point detection:
   automatically detect and manage wireless threats to your network
   http://www.proxim.com/learn/library/whitepapers/Rogue_Access_Point_Detection.pdf

3. Lane, Heather D. (02/6/2005). Security Vulnerabilities and Wireless LAN
   Technology. Retrieved July 22,2007, from http://www.giac.org/certified_professionals/practicals/GSEC/4383.php

4. Hurley, Chris; Puchol, Michael; Rogers, Russ; Thornton, Frank.
   Wardriving: Drive, Detect, Defend, A Guide to Wireless Security.
   Syngress. April 2004.

5. Wireless LAN Security 802.11b and Corporate Networks. (07/22/2007).
   Internet Security Systems White Paper. Retrieved July 22,2007, from
   http://www.iss.net/documents/whitepapers/wireless_LAN_security.pdf

6. Anand, Dev. (2004). Rogue Detection and Blocking. An Adventnet
   Technical Whitepaper. Retrieved July 22,2007, from

http://manageengine.adventnet.com/products/wifi-manager/roguedetection-and-blocking.pdf

7. Wireless Intrusion Protection (07/22/2007). Aruba Networks Technical
Brief. Retrieved July 22,2007, from http://www.arubanetworks.com/pdf/technology/tb_wip.pdf

8. Webopedia, http://www.webopedia.com
9. Gast, M. 802.11 Wireless Networks: The Definitive Guide Creating and Administering WirelessNetworks, O'Reilley Publishing, April 2002.

13. Ken Barnes. (2004). Introduction To SCADA Protection and Vulnerability. INEEL/EXT-04-01710 , 41.
Kim, D., & Solomon, M. G. (2010).Fundamentals of Information Systems Security. 1st ed. In K.

10. Wikipedia, http://www.wikipedia.org
11. Brandel, M. (2009, 09 17). How to Compare and Use Wireless Intrusion Detection and Prevention Systems. Retrieved 5 19, 2012, from http://www.csoonline.com: http://www.csoonline.com/article/502268/how-to-compare-and-use-wireless-intrusion-detection-andprevention-systems
12. Cisco. (2003, 11 7). The Science of Intrusion Detection System. Retrieved 5 25, 2012, fromhttp://www.cisco.com/warp/public/: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/idssa_wp.htm