A Review of Setting up a Secured Web Based Wireless Hotspot

[1]Chukwuemeka Odi Agwu, [2]Ifeanyi Isaiah Achi

[1]Lecturer 1, [2]Lecturer 11
[1]Department Of Computer Science Ebonyi State University-Abakaliki,
[2]Department Of Computer Science Our Saviour Institute Of Science And Technology

Abstract- The increasing desire and preference in recent times for wireless connectivity by individuals, firms, ministries has made it very important for network administrators to put into considerations the best measure to securing wireless network[2]. Corporate Organization are embracing the wireless hotspot technology for increased productivity and provision of a more flexible work arrangement for workers so as to work closely with their partners with the ability to access limitless volume of data anytime, anywhere. However, securing wireless network is the greatest challenge faced by network administrator [9] and as such there is need for constant research for a better security measure that will improve the existing security measures. Therefore a web based wireless authentication secured hotspot is one of the security measures we shall lay emphasis on in this work. Other researchers on this subject[7],[8],highlighted some other means of authenticating wireless network without emphasis on this web based authentication as mean means of securing wireless network. It is the wireless network security that will require the users to be authenticated or allowed access using the browsers login page. This paper centers on the technicality of setting up this web based secured wireless hotspot; configuring the server (router) and programming the authentication web page. The server runs on Linux operating system and the web pages were designed using HTML/Java/PhP script, using mysql for the data base that manages the radius server. My focus here is on the setting up of the wireless hotspot radius server that can work with the designed web authentication pages and not the actual design of the web pages.

Keywords- Wireless Hotspot, Radius Server, Linux, Security, Radius Client, Authentication, Browser, Web Administration.

INTRODUCTION

The world and the various ways corporate organization carry out their day to day business activities would had been a nightmare without a proper means of communication. Whether you are taking a vacation or transit to a new location, you will probably want to stay connected from point A to point B and not be constrained by the fixed hardwired devices. These could be resolved by seamlessly integrating wireless communication medium with wireless devices.

The need to cover the globe at large led to the advent of wireless networking materials and the technical knowhow to securing a wireless network [16], [21]. Currently, a tap on button could trigger a message to be transferred from one location to another. Hence, this had necessitated the massive patronage of the wireless hotspot by every sector of the society. The benefits of integrating wireless hotspot in all sector of our society cannot be over-emphasized. A

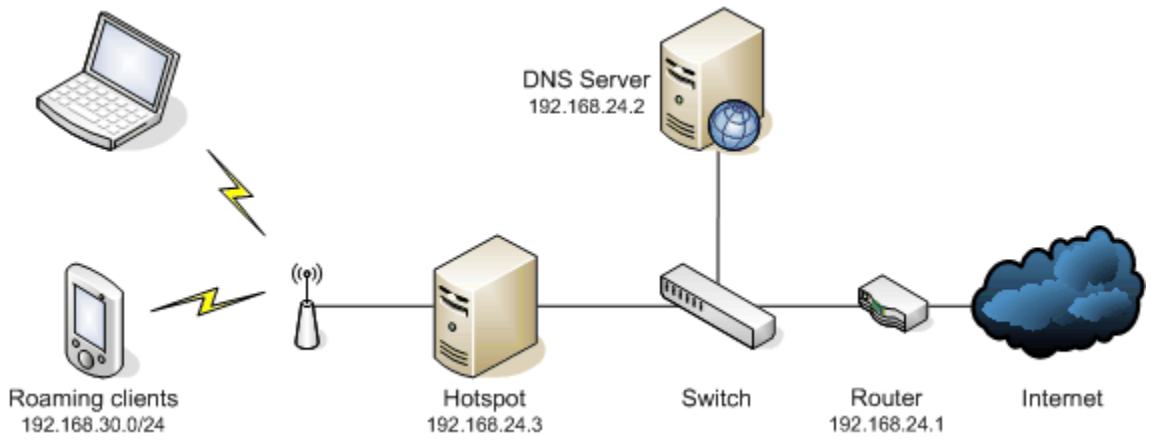
hotspot is a wireless network set up for shared internet access. As many people are adopting the wireless hotspot technology, it will be paramount to establish various techniques that could be deployed in securing data transmission especially at the server side wireless network. Because of the flexibility and ability to connect from anywhere, wireless networks are often more vulnerable to attacks [22]. In a server client network, the server controls or administers the network [3]. Setting up a wireless network is done, established by a network administrator. It implies that everything about the security is handled at the servers by the network administrator [9]. While setting up this radius server, the first thing that came to mind is the type of operating system that will best meet our need and the hardware it is going to run on. This server will run on Linux operating system and on any standard x86 PC hardware or a Router BOARD. The specification of the PC should be up to the minimum standard[11],[13],[14]. I chose to use Linux because of its immunity to virus attack than windows. Viruses cannot thrive in Linux operating system.

This server where the security is programmed is often times referred to as radius server and the programmed web pages used for the authentication are uploaded into it. This server handles everything about the wireless network. It manages everything about the client side like data base-timing of clients making use of the hotspot, generates pass code for users, shows the users online (active users), adding new users, shows the sections used by users and report of the general usage by users for certain periods in time. This is applicable to every server/client network system where a machine is dedicated to serve others clients system [9].

The management of this server is easy in the sense that someone with or without the knowledge of programming can administer it. This is possible with the use of File Transfer Protocol (FTP) software (Winbox) in connecting to this radius server. FTP is used in connecting to servers or server machines[16]. The nitty gritty of setting this radius server up is our concern here.

THE HOTSPOT STRUCTURE

In this paper, we considered a set up of a basic hotspot as shown in the diagram below. If you have a Domain Name Server (DNS) integrated into your router the same rule applies, just use the router Internet Protocol (IP) for your DNS server as well. The router serve in traffic control by seeking the best path signal can be routed at any point in time[10].



To help get started we will first of all highlight the basic parts of this hotspot which include a combined RADIUS server and simple web administration package(User Manager) that will be setup for the Router operating system (OS). This provides a much simpler means of user administration than the command line or FTP software (Winbox). The web administration package can be programmed and included in all standard versions of Router OS (Linux).

HOTSPOT CONFIGURATION REQUIREMENT

First of all you will need to have a copy of the Linux operating system(Router OS). You can purchase a license or download a 24-hour trial from the web. RouterBOARDs also usually come with Router OS pre-licensed and installed. You will also need a computer with at least a 100MHz CPU, 32MB RAM and an IDE hard disk, or routerboard. Any method you choose need a compatible wireless card and Ethernet adapter, or two Ethernet adapters with one connected to a standard wireless access point. You should check your hardware against the Router OS compatibility list.

If you are installing Router OS for the first time, download the ISO image from the web and burn it to CD. Note that installation of Router OS will completely wipe the contents of the hard disk. Boot the PC off this CD and install the following packages:

- System
- DHCP
- Wireless
- Proxy
- Security (optional - recommended)
- Advanced tools (optional)

When these packages are installed, it will now create the folder for the hotspot and that of the web administration (user manager) which is our concern in this paper. The network administrator will now have to design and program the content of those two folders created by virtue of installation and upload it via the FTP or the command prompt into the appropriate folder. The hotspot folder contains the secured authentication web pages for the hotspot wireless users. The pages therein are as follows: loin page, re-login page(rlogin), again login page(alogin), revert page, redirect page, the image folder, status page and logout page. The web administration folder contains web page that is synchronized with hotspot folder to administer or manage the hotspot.

- **Login page** is the first page with the two text boxes for the login information of the user.
- **Re-login page** redirects client from some other Uniform Resource Locator (URL) to the login page, if authorization of the client is required to access that URL.
- **Again login page** is shown after the client has logged in. It pops-up status page and redirects browser to originally requested page (before the user was redirected to the hotspot login page).
- **Revert page** redirects client to the scheduled advertisement link.
- **Redirect page** is the page that always takes every first user of the hotspot to the authentication login page.
- **Image folder** contains all the picture and logos used in designing the entire site.
- **Status page** shows statistics for the client. It is also able to display advertisements automatically.
- **Logout page** is shown after user is logged out. Shows final statistics about the finished session.

- **Error page** is shown when fatal errors occur.
- **MSD5.js file** is JavaScript for MD5 password hashing. Used together with http-chap login method.

CONFIGURING WIRELESS HOTSPOT

Now to get started logging onto the PC as admin with no password. If this box intended for deployment, change set a password by typing in password at the prompt. This is applicable to every router board and server systems, authentication is necessary for security purposes[1],[11],[12].

In this paper, we consider configuring two interfaces - one for the public and the other for the hotspot. The public interface is connected directly via a cross cable to the modem and the hotspot or wireless (wlan1) interface is connected to any wireless access point or a radio, it could be via a cross cable or a straight cable. This hotspot (wlan1) interface is synchronized via the administrator coding or programming to the hotspot folder created on installation of the linux operating system.

Then we can follow the following steps:

Enabling the interfaces

```
[admin@root] > interface set 1 disabled=no

[admin@root] > interface set 2 enabled=yes

Both commands are the same.
```

Change the hostname by typing in **name**.

```
[admin@root] > interface set 1 name=ether1

[admin@root] > interface set 2 name=wlan1
```

Assign an IP address to each interface. As this is going to be set up as a router, they will need to be on a different subnet.

Substitute wlan1 with ether2 if you have a separate access point.

```
[admin@root] > ip address add address=192.168.24.3/24 interface=ether1
[admin@root] > ip address add address=192.168.30.1/24 interface=wlan1
```

Now we need to add a default route to the IP of the satellite router (Modem).

```
[admin@root] > ip route add gateway 192.168.24.1
```

Since we have an access point running, we ensured to make sure it is running with no security enabled, use a suitable SSID and channel and change its admin password.

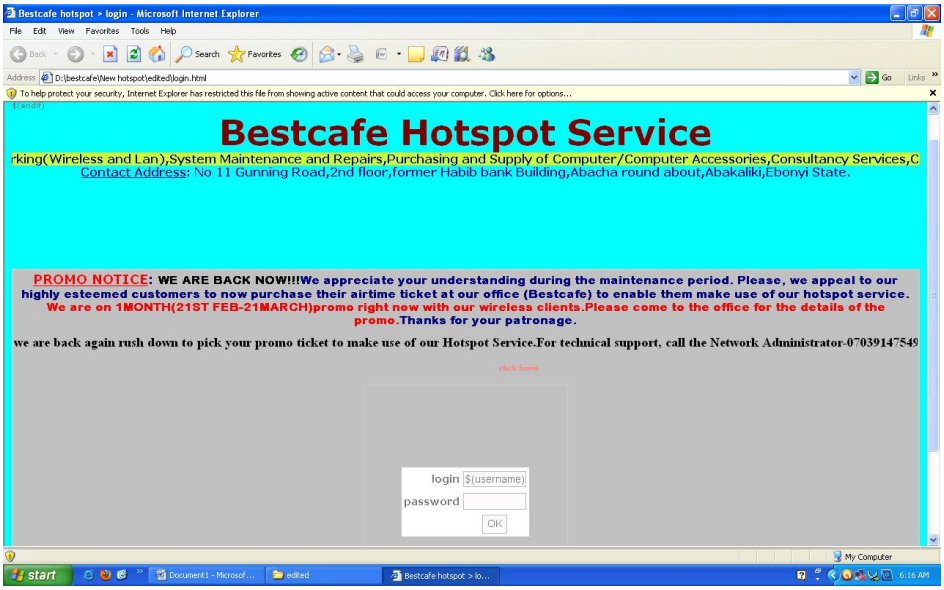
Substitute the values in italics to suit your network. The user account bears no relation to the admin account and is used for the hotspot service only. You may also need to add a host record to your DNS server for the hostname of the hotspot box. Make sure the address pool does not conflict with any devices using static IPs, such as access points.

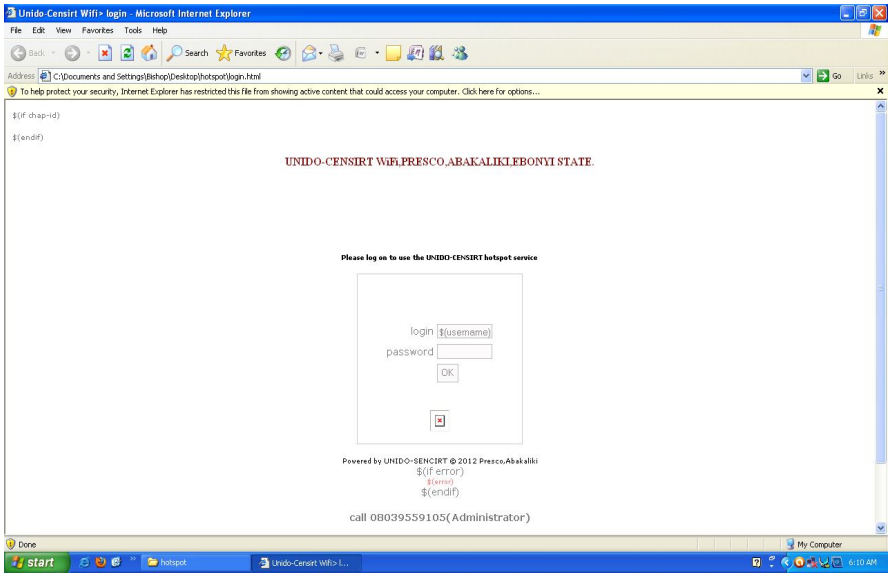
The system is made to use the hotspot authentication by connecting the hotspot interface with the hotspot folder as installed in the system. This can be realized by running the hotspot setup as below.

```
[admin@root] > ip hotspot setup
hotspot interface: wlan1
```

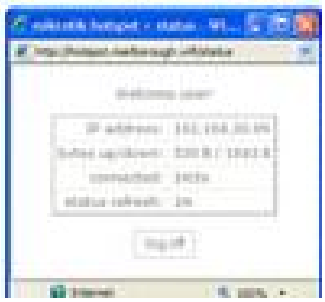
```
local address of network: 192.168.30.1/24
masquerade network: yes
address pool of network: 192.168.30.2-192.168.30.99
select certificate: none
ip address of smtp server: 0.0.0.0
dns servers: 192.168.24.2
dns name: hotspot.mydomain.net (or leave this blank)
name of local hotspot user: user
password for the user: password
```

Boot up your laptop, associate to the network and try to access a web page. You should be redirected to the hotspot login page instead of the original URL so you can enter the user credentials you set up earlier.





You should now be able to access the web normally and a pop-up window will display your connection time and data usage as you go-status page.



Bear in mind we have left out the certificate so usernames and passwords will be sent as plain text. If you intend on deploying the hotspot, you should install a certificate on it and set up Secure Socket Layer (SSL) to protect account data from being sniffed.

This hotspot can be managed from within the program or by associating or integrating the entire system with the web administration process. The previous can just be managed from either the network administrator setup code or command or by using the FTP software (winbox).This FTP can be downloaded from the internet and install in the administrative system. The later, web administration management is managed from a web browser incorporated within the web administration folder as designed by the programmer.

SETTING UP WEB ADMINISTRATION MODULE(USER MANAGER)

The web administration is a nice and simple for setting up user account for the wireless hotspot and other services. It can be hosted on either the same box as the hotspot or located in a separate box on the same local network. One web administration package can control multiple hotspots. Server being in control of the clients workstations in a typical network[16],[17].

Before getting the Web administration set up, ensure the web authentication web pages has been designed and uploaded into the appropriate folder in the box or system(server system), also the administrator has to create the hotspot accounts. To do this, run the following command:

```
[admin@root] > ip hotspot user print
Flags: X - disabled, D - dynamic
# SERVER NAME ADDRESS PROFILE UPTIME
0 fred default 0s
```

If any items are listed (in this case **bob**), run the following command to remove them:

```
[admin@root] > ip hotspot user remove 0
```

You can delete multiple items at the same time, simply separate each item number with a comma.

To get the web administrator working we first need to add a customer login. This is used to access the web administration management module. Make sure you substitute the values in italics to suit.

```
[admin@root] > tool user-manager customer add login=hs_admin
password=password
```

Now we need to add the hotspot as a RADIUS client to the web manager. This is done under the user manager router section. The shared secret can be any string of text and should be reasonably long and complex. If you are setting the user manager up on the same box as the hotspot, use **127.0.0.1** for the IP address.

```
[admin@root] > tool user-manager router add ip-address=hotspot-ip
shared-secret=12345 subscriber=hs_admin
```

In return, we need to set up the hotspot to use RADIUS for user authentication. First this involves creating a RADIUS client to communicate with the web administrative manager. Remember that if you have both services on the same box, the IP address should be set to **127.0.0.1**. The secret should be the same as you set up above.

```
[admin@root] > radius add service=hotspot address=ip-address secret=12345
```

Now we tell the hotspot itself to use a RADIUS client. First bring up a list of hotspot profiles:

```
admin@root] > ip hotspot profile print
```

Locate the profile in use and type the following command where **1** is the number of the profile to configure:

```
[admin@root] > ip hotspot profile set 1 use-radius=yes
```

Now we are done with configuration. Browse to **http://*router-ip*/userman** where **router-ip** is the IP address of the box you are configuring on. Login using the customer username and password created earlier.

Click on the **User** menu and select **Add**. Enter in a username, password and any other details you wish. You can limit the speed the client can access the internet by selecting the **Rate limits** checkbox and typing in a suitable speed (e.g. for a flat 128kBps download/64kBps upload speed limit simply type in **128k** in the **RX** field and **64k** in the **TX** field).

Click **Add** and you should be able to now access the hotspot using the username and password you specified. If you want to generate a printable ticket for the users you set up, click on the **Users** link, select the users to make a ticket for, click **Generate** and select the number of tickets per page.

CONCLUSION

This article explained the basic step to setting up a basic personal computer or operating system routerboard and explaining how a web authentication works with the system. The web authentication management is contained in the router software, operating system as user manager[16],[19]. Here we focused on the explanation of the router set and making it work with the web manager module. The web module is designed separately using html, php and java script with mysql as the database and uploaded into the radius server, hotspot. This entire system works with as

many computers as possible that are connected to it, even up to 100s of computers. This system works connected behind a satellite router and being distributed to the number of computers via the wireless access point connected to through the hotspot interface within the system. Provision of different interfaces for the both the satellite modem and wireless access point is a common feature for every router[6],[9],[17]. Every computer or client computer must have a wireless LAN to be able to connect to the existing network. The access point is configured with a name (SSID, Service Set Identifier) with which the intending users can use to enter the network. This is a typical wireless router setup for wireless network[1],[19],[21]. The only security measure in this platform is the web, meaning that every other security measure with the access point being used, will be disabled. When this is done, the hotspot is ready to be used.

REFERENCES

[1] B. Mitchell, "Service Set Identifier (SSID)", http://compnetworking.about.com/cs/wireless/g/bldef_ssid.htm, 2014.

[2] K. Sanka, S. Sundaralingam, A. Balinsky, and D. Miller "Cisco Wireless LAN Security",Cisco system inc, 2005.

[3] M. Kaafar, K. Salamatian, L. Mathy, T. Turletti, C. Barakat and W. Dabbous, "Securing Internet Coordinate Embedding Systems", In Proceedings of ACM SIGCOMM, 2007.

[4] P. Barford, "Measurement as a First Class Network Citizen", White Paper, 2005.

[5] G. Karame, D. Gubler, and S. Capkun, "On the Security of Bottleneck Bandwidth Estimation Techniques", In Proceedings of SecureComm, 2009.

[6] J. Edney, and A. Arbaugh, "Real 802.11 security wi-fi protected Access and 802.11i", Pearson Education inc, 2004.

[7] A. Arbaugh, and A, Williams, "Wireless LAN Security Measures" Pearson Education inc,2004.

[8] G. De, and S. Gert, "Network Security Fundamentals" Cisco System Inc, 2005.

[9] T. Maufer, "A Field Guide to Wireless Lans: For Administrators and Power Users" Pearson Education inc, 2004.

[10] M. Bradley, "802.11 Wireless Lan Fundamental", Cisco Press, 2004.

[11] Cisco, "Configuring Authentication", Cisco UCS Manager GUI Configuration Guide, 2014. www.cisco.com

[12] S. Wilkins, "Routing Protocol Authentication Concepts and Configuration", 2011. www.ciscopress.com

[13] D. Keller, "Installing and Operating a RADIUS Server", 2004. www.wifi.keller.com/CNIT107HW7.html

[14] C. Schroder, "Authenticating Wi-Fi Users with FreeRadius", Openlogic, 2011. http://www.openlogic.com

[15] C. Adam, and F. Glenn, "The Wireless Networking Starter Kit: The Practical Guide to Wi-Fi Networks starter kits", 2003.

[16] E. Blanchard, "Introduction to Data Communications", 2005.

[17] R. Banerjee, "Internetworking Technologies", An Engineering Perspective, (2002).

[18] H. Davis, and R. Mansfield, "The Wi-Fi Experience: Everyone's Guide to 802.11b Wireless Networking", 2001.

[19] J. Bola, "Wireless LANs Demystified", 2002.

[20] J. Bates, "Wireless Broadband Handbook", 2001.

[21] M. Ciampa, "CWNA Guide to Wireless LANs (Networking) Second Edition",2005.

[22] R. Scotland, "Unsecure or Secure: The Network Security Challenge for Small and Mid-size Businesses", 2013.