Talking Aboat WIFI's New Security

Ling He[1,*], *Yangxin Teng*[1] , *Mingxuan Li*[1] , *Qingrui Guo*[1] , *Feng Li*[1] , *Cailing Wang*[2], and *Jizhao Yi*[3,] *Jinshan Gao*[2]

[1]Information and communication technology center, State Grid Xinjiang Electric Power Research Institute, Urumqi, China
[2]Urumqi railway bureau,Urumqi, China
[3]Tianjin Science and Technology University,Tianjin, China

Abstract. Wireless network technology's widely used brings the web's users huge convenience and flexibility, and also brings great challenges for the security of network.This paper introduces the MAC address authentication, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WiFi Protected Access 2 (WPA2) and 802.1X and so on, giving priority to analysing their pros and cons. A new model will be used to cope with the security issues of WIFI based on it.

1 Introduction

WIFI means wireless local area network based on IEEE802.11b. As a new generation of wireless network technology, WIFI can get ethernet network performance, rate and availability for wireless network users, and also seamlessly combine variety technology of LAN. In recent years, the number of wireless AP is growing rapidly, on account of wireless network's convenience and efficiency can make it spread quickly[1].

At the same time, Open nature of the wireless network determines it is more vulnerable than wired network in safety. Accordingly, when we enjoy the convenience and flexible features which the wireless network brings, it will be of great use to take technical measures to improve security.

2 Development Prospects

WIFI is made up of access point and wireless network card. WIFI's network structure[2] is shown in Fig 1.

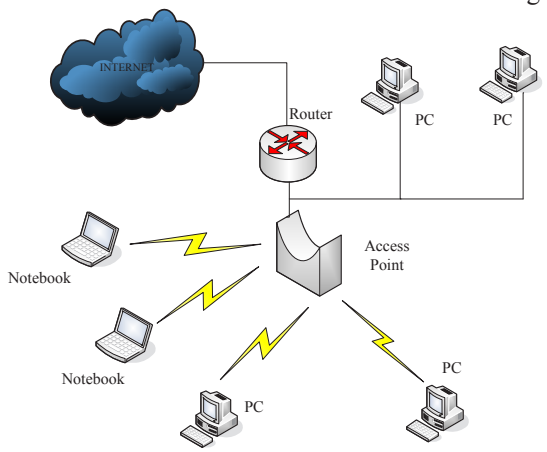

Fig 1. WIFI's network structure

The wi-fi technology is short distance in wireless information technology. It has widely used both in the office family. It usually uses 2.4 GHz frequency bands [3].

1) The radio waves used in wifi waves which covers a wide range. As an example, the Bluetooth radio waves can encompass a radius about 15 meters, at the same time the radio coverage of wireless technology can reach 100 meters. It makes the wireless technology to better meet the various needs of diverse types of users. With the continuous development of technological innovation, the effective coverage range will make further efforts to increase.

2) The high transmission speed. Depending upon the different criteria of wireless card are used, the transmission rate becomes different. For instance, the maximum number of IEEE802.11b can reach 11Mbps, the 802.11a and others can achieve 54Mbps. Comparing with the Bluetooth technology and others, the high-speed of WiFi technology can meet the requirements of the development of the information-based society.

3) The low application threshold. In China, wireless technology is growing rapidly. There are many public places use it, such as airports, stations, restaurants and business halls and so on, where set up wifi hotspots that we can use it by means of high-speed lines which access the Internet. On condition that wireless customers use laptops that support LAN pours into this area can easily access the network.

Owing to wireless networks have many virtues such as low cost and convenient use, which has become such an integral part of our daily life, at the same time, the most severe cases is that whether the security identification system of wifi technology is reliable. The following are comparative analyses about the security measures of wifi.

3 Compared

3.1. MAC address authentication

* Corresponding author: author@e-mail.org

Wireless AP checks whether the address is a legitimate user by checking the 48 bit MAC address contained in the data frame header sent by the user.

The drawback of this approach lies in that MAC address authentication is unreliable. Illegal invaders can track and detect by means of a sniffer software and then their phones can verify the MAC address of legal machines through modifying their own MAC address, on this count they can be disguised as legitimate users to connect the network.

3.2. Wired Equivalent Privacy

WEP[4] is a security protocol, which can be applied to wireless local area network (WLAN) of 802.11b standard. It is a kind of basic encryption measure for wireless devices. WEP uses the RC4 encryption algorithm based on 40/104-bit to share encryption keys and it uses this approach to encrypt all data transmitted by wireless network.

With the upgrade of wireless security, WEP encryption has occurred 100% crack methods. Linear CRC encryption algorithm, static keys as well as unspecified key management and vulnerability authentication mechanisms, which can make hackers disrupt confidential matters about WEP if they can get enough data packets by a network sniffer. For instance, AirSnortor or WEPCrack, they can try to break out of the 2.45*109 keys per second, which means that the 40-bit encrypted data can rank 240 keys will be deciphered provided that these tools collect enough data packets in 5min.

3.3. WPA and TKIP

Due to the vulnerability of WEP, before the new standards produced, WIFI alliance solutions develop a transitional solution — WPA. It will limit hacker attacks by adopting 48 bit IV, building mechanisms with each pack key and periodic alternating release keys as well as information coding. WEP uses the same symmetric encryption algorithm as RC4, which fixes quite a few dilemmas including short IVs in WEP and fixed keys etc. The protocol can be realized with software upgrades in the existing WEP so as to achieve the existing resources can obtain the maximum security.

Nevertheless, WPA still has many serious problems. Because of the weak encryption algorithm, it still may be cracked : hackers just listen to enough data packets with powerful computing equipment even under the protection agreement.

3.4. WPA2 and AES

In June 2004, IEEE 802.11i standard set up, wireless cable association re-release wireless security solutions — WPA2, which based on the latest IEEE 802.11i standard. WPA2 is a way to protect data security that is based on advanced Encryption Standard (AES). AES is a type of symmetrical block encryption technology, using 12bit block encrypting of data, and providing a more advanced encryption performance than RC4. WPA2 uses 48 bit IV and IV sequence rules to send the initial key, meanwhile, send out MIC using CCMP key tamper detection. CCMP adopts the cipher block chaining mode to encrypt the data into 128 bits, and provides information integrity detection via the MAC layer. Nevertheless, due to the high requirements of AES hardware, CCMP can not be achieved on the basis of existing equipment upgrades.

Currently, WPA2 encryption mode was once thought to be 100% safe but now it is considered to be extremely unsafe at present. Back when the original 2009, two Japanese security experts said that they had been developed a way that made use of wireless router to break WPA encryption system in a minute. Through the dictionary and PIN code we can easily solve almost 60% WPA2 secrets.

3.5. 802.1X

802.1x is a kind of port based network aceess control protocol [5]. It defines three important components: Supplicant’s System, Authentication’s System and authentication’s Server’s System. The following figure is the relationship between the three and communication between each other.

802.1x authentication protocol is layer protocol, its service message is directly loaded on the normal second layer message. In the course of the process of authentication, 802.1X doesn’t need encapsulate frames into the Ethernet, so the process is relatively efficient. And at present, most hardware devices support this protocol. The performance requirements of the devices are not high and relatively simple to achieve. Therefore, 802.1X is supported by many hardware and software vendors.

But 802.1X is not overwhelmingly safe in reality. A new study indicates that 02.1X is easily attacked by Session hold—It’s means that after attackers wait for legitimate users to pass authentication, on the one hand they through various forms of Dos to prevent legitimate users and servers’ connection. On the other hand, they pretend to be legal users to establish a connection with the servers, which has been challenging the security of wireless network.

4 Propose a New Model to Improve Security

In view of existing situation, there are some latest attack ways: sniffing, disguising, pretending, utilizing existing vulnerabilities to attack wireless network with brute-force, cracking by dictionary and grasp the package for analyse. These attack patterns utilize a variety of vulnerabilities to attack, for instance, authentication attack, forged disconnect, forged AP, probing AP information and guessing ESSID and so on. All the above of vulnerabilities will interact with that data with wireless devices. In the process of interaction, MAC address must be copied by wireless devices, but provided that you want to find hidden troubles through enhancements, you must login management interface. It

is unable to real-time monitor the security performance of the wireless devices and unable to find and solve cases. Many times, we don't even notice it until it's too late. How to better protect our safe router and display the status of wireless router to users in real time, which that needed to be addressed as a matter of urgency. We propose a new model based on this view that reinforce general wireless routers so as to quickly find the wireless network attacked and these issues can be received our immediate attention.

First we have to count client numbers who are connected by a wireless router and MAC address so as to form a standard document and lock (except public wireless routers). In order to obtain linked MAC addresses, we have to establish a session with a local wireless router. Comparing the two, once there are abnormal and connective MAC address records, it will prompt information to the desktop terminal instantly and inform the local administrator that there has been set up an illegal link. As shown in Fig 2.

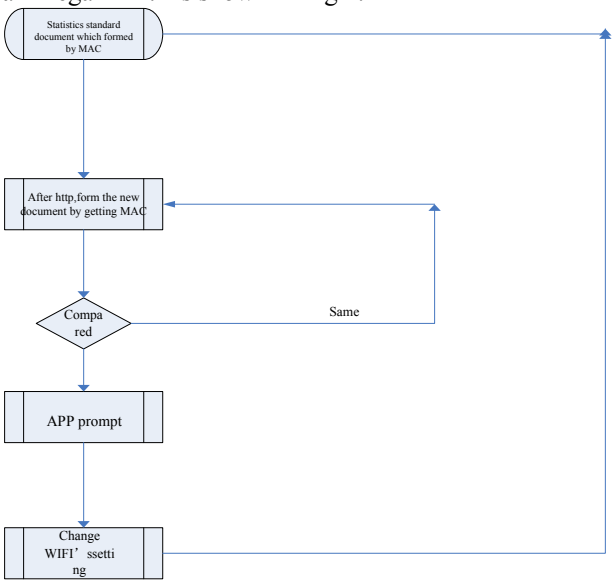

Fig 2. Security reinforce procedure

We need to find a cross-platform tool to realize the function that we can record the MAC visits and prompt authorized users and unauthorized users who get the relevant contents by visiting routers. We choose the Python to programme, it is a pure and free software, and source code and interpreter follow the GPL protocol. The advantages are clear grammars and rich and powerful databases,

The following we will take the TP-Link router as an example (the main noted type is TL-WR720N, the firmware version is TL-WR720N V3_120620 Standard Edition) Using Python as the platform to enhance the security of this router.

5 Solutions

1)Establishing a session named urllib2 with any wireless routers. We can simulate various kinds of loggings that meet the requirements through urllib2's various attributes. We obtain wireless routers' relevant information with GET:

```
ip = '192.168.1.253'
login_user = 'admin'
login_pwd = 'admin'
url = 'http://' + ip + '/userRpm/WlanStationRpm.htm?Page=1'
auth = 'Basic ' + base64.b64encode(login_user+':'+login_pwd)
heads = { 'Referer' : 'http://' + ip + '/userRpm/WlanStationRpm.htm','Authorization' :
auth }
request = urllib2.Request(url,None,heads)
response = urllib2.urlopen(request)
html = response.read()
```

Once we get the wireless router's landing permissions, we can read the special message from special webs for our subsequent queries and uses.

2)We transcode the information which we obtain from the html through a type of component — BeautifulSoup. In this article, we just get linking MAC addresses as following:

```
soup = BeautifulSoup(html)
res = soup.find_all('script')[1]
cont = res.prettify()
reg1 = re.compile("<[^>]*>")
res1 = reg1.sub('',cont)
mac = re.findall('..-..-..-..-..-..', res1)
i = len(mac)
```

We will be able to carry out various types of operations through the linking MAC addresses. You can add a router's white lists, and enable MAC filtering mechanism, etc.

3)Comparing the new MAC files with the standard files by continuous testing and then we can record the new MAC addresses.

```
file1 = open(r'tmp-b.txt','r')
file2 = open(r'tmp-c.txt','r')
file3 = open(r'tmp-ba.txt','w')
found = 0
l1 = file1.readline()
while l1:
    print
    print l1
    file2.seek(0,0)
    found =0
    l2 = file2.readline()
    while l2:
        print
        print l2
        if (l1==l2):
                found =1
            break
        l2 = file2.readline()
    if found == 0:
        file3.write(l1)
    l1=file1.readline()
file1.close()
file2.close()
file3.close()
```

We can identify some new MAC addresses through comparing and querying.

4)We can display the specific MAC addresses to users' desktop with Tkinter, which can remind the local users who have new MAC addresses to assess the wireless routers.

```
def show():
  bubb = Tkinter.Tk()
```

```
    f =open(r'tmp-ba.txt','r')
    mess = f.read()
    s = Label(bubb,text=mess,bg='blue',width='40',height='3')
    s.pack()

def creatmac():
    root = Tkinter.Tk()
    bub = Tkinter.Button(root,text="MAC",command=show)
    bub.pack()
    root.mainloop()
creatmac()
```

5)We can realize the real-time monitoring of local terminal by while loop and time components. The terminal can be a mobile phone or a computer that you only need to install the Python platform, and specific codes are as follows:

```
def main():
  while True :
    checkmac（）
      else :
        os.path.exists(r'tmp-c.txt')==True:
        break
    time.sleep(3)
```

It can achieve real-time monitoring of the local wireless routers' MAC address transforms from the above five steps, and it will make a reminder through the unfamiliar MAC addresses access so as to improve the protective capability of wireless routers. The real-time monitoring of the running state of the wireless device can effectively prevent the wireless device from being attacked, and to a certain extent, it can improve the security of wireless devices. But we should be aware of the daily management of wireless devices. And do the followings：

Enhancing password strength, which means to it contains 8 or else more bits complex passwords and pieces of letters, numbers and symbols. For example, Bu/eB7@2.

Hiding SSID, which makes the SSID of wireless network no longer be broadcast can greatly reduce the probability of being hacked

MAC binding. Like the way to hide SSID, MAC binding can greatly increase the difficulty of hacking network. The additional complexity of the operation to make the majority of the hackers involved.

Turn off wireless routers' QSS and WDS functions.

Try to avoid connecting your device to a public Wi-Fi. Even if connected to public wireless, you can't use applications involving personal privacy.

Provided that you feel the internet speed slower significantly, you maybe suffered a session hijacking. At this point, you should immediately cancel the exit account and clear cookies and immediately modify the Wi-Fi password.

Do both from the technique and management, we can better improve the safety performance of the wireless network.

6 Conclusions

With the pace of life speeds up and further popularization of wifi, the increasing demands of people for wifi. At least technically, we need to strengthen the security mechanism of wireless devices, the safety consciousness and safety management measures in order to keep the WiFi is reliable.

Acknowledgment

The authors would like to thank the editor and the anonymous referees for their valuable comments, and thank the members who had participated in"wireless communications security in the State Grid Xinjiang power company technical application research.

References

1. Li xiaoyang.WIFI Technology And its Application And Development[J].Information Technology,2012,2:196-198
2. Lu yan,Mao xu.Compare And Analysis Based on WIFI's wireless Network Security[J].Guangdong Communication Technology,2007，3:25-29
3. Yu zhenquan.A Wireless Network Security Protection System[J].Electronic Science and Technology,2006,9:1-9
4. Zhangyun.Analysis of Wireless Network Technology[J] .Science&Technology Information,2008,23:57-58
5. Lai yu,Zhang huajie.Information Network Security Measures to Explore Based on Wireless Network[J],Coal Technology,2013,10:234-235.