IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 1 (May. - Jun. 2013), PP 04-07
www.iosrjournals.org

Latest Developments in WirelessNetworking and Wireless Security

Asst. Prof. Shubhada Talegaon
Department MCA, Parul Institute of Engineering & Technology, Vadodara,Gujarat,India

Abstract: *This paper illustrates some key recent developments in the area of wireless networking. It also illustrates the key concepts of security, wireless networks, and security over wireless networks. Wireless security is demonstrated by explaining the main specifications of the common security standards. This paper also provides information about latest development in wireless security network with standards like 802.11ac 802.11n WPA and WPA2*

Keywords:*WPA, WPA2, 802.11ac,802.11,*

I. Introduction

Wireless local area networks (WLAN) are common nowadays and a lot of sensitive information goes through them. Their security is thus an essential feature of the broader issue of information security. The field of the study of WLAN security is quite transient because new techniques to break the security mechanisms are discovered quite frequently.

Recent developments on wireless communication technology have resulted in tremendous innovations to make wireless access networks able to replace the wired access networks with much more bandwidth.

II. Latest Development In Wireless Networking

Home and business networkers looking to buy wireless local area network (WLAN) gear face an array of choices. Many products conform to the **802.11a**, **802.11b**, **802.11g**, or **802.11n** wireless standards collectively known as Wi-Fi technologies. Additionally, **Bluetooth** and various other non Wi-Fi technologies also exist, each also designed for specific networking applications.

1. IEEE 802.11ac

IEEE 802.11ac is a wireless computer networking standard of 802.11, currently under development (Draft 5.0), providing high-throughput wireless lcoal area network on the 5GHz band and is backward compatible with 802.11n’s 2.4 GHz band. Standard finalization is in late 2012, with final 802.11 Working Group approvals in early 2014. According to a study, devices with the 802.11ac specification are expected to be common by 2015 with an estimated one billion spread around the world.

Theoretically, this specification will enable multi-station WLAN throughput of at least 1 giabit per second and a single link throughput of at least 500 megabits per second (500 Mbit/s).

802.11n brought improvements in data rates and link efficiencies

Table 1 - 802.11ac Major Features Enhancements

802.11ac Features	Customer Benefits
Wider channels	Higher data rates – up to 1.3Gbps per radio
Higher encoding density	Higher bit density per packet
Increased number of spatial streams	Higher data rates per AP/client link
Beamforming	Greater wireless AP/client link reliability
Multi-user MIMO	Greater AP/client capacity and efficient use of spectrum

The cumulative benefit of 802.11ac features will enable Wi-Fi solutions to meet today’s demand for high capacity and high quality mobile real-time applications like video and voice

2. 802.11n standard

IEEE 802.11n-2009 is an amendment to the IEEE 802.11-2007 wireless networking standard. Its purpose is to improve network throughput over the two previous standards—802.11a and 802.11g—with a significant increase in the maximum net data rate from 54 Mbit/s to 600 Mbit/s (slightly higher gross bit rate including for example error-correction codes, and slightly lower maximum throughput) with the use of four spatial streams at a channel width of 40 MHz. 802.11n standardized support for multiple-input multiple-output and frame aggregation, and security improvements, among other features. MIMO is a technology that uses multiple antennas to coherently resolve more information than possible using a single antenna

The main differences between 802.11b, 802.11g, 802.11a, and 802.11n are summarized below.

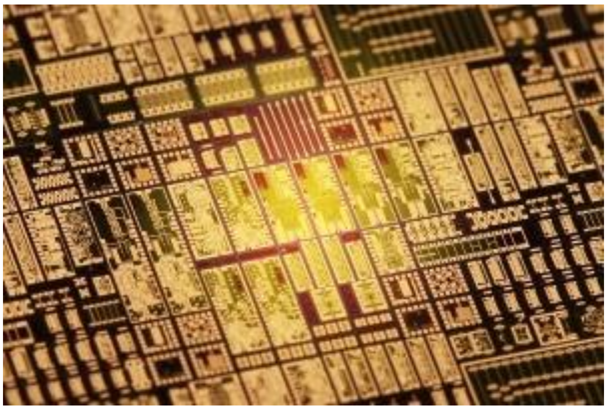
Apple Product	**Standard**	**Speed**	**Range**	**Frequency**
AirPort	802.11b	11 Mbps	150 Feet	2.4 GHz
AirPort Extreme	802.11g	54 Mbps	50 Feet	2.4 GHz
AirPort Extreme	802.11a	54 Mbps	50 Feet	5 GHz
AirPort Extreme	802.11n	300 Mbps 450 Mbps§	175 Feet	2.4/5 GHz

3. German Researcher test 40 GBPS wirelessbroadband

A pair of top German research institutions has shown impressive early gains in an effort to improve wireless broadband with speeds that would allow the download of a DVD in a single second.

German researchers on the hunt for wireless alternatives to fibre claim to have achieved 40Gbps wireless transmission speeds over a distance of 1km.

The speed is a new world record, according to researchers at the the Fraunhofer Institute for Applied Solid State Physics (IAF) and the Karlsruhe Institute for Technology. The pair has built transmitters and receivers that operate at a 240GHz frequency — much higher than the the IEEE 802.11n standard, which operates on 2.4GHz with top speeds of under 1Gbps,



The new transmitter is printed on a tiny IC chip. [Image Source: KIT]

4. DARPA has created the Wireless Network Defense program

The program aims to develop new protocols that enable military wireless networks to remain operational despite inadvertent misconfigurations or malicious compromise of individual nodes.

A key objective of the program is to develop protocols that determine the viability and trustworthiness of neighboring nodes and automatically adapt the network to operate through problems. Similar to a neighborhood watch program – where neighbors know each other and can identify suspicious or unusual behavior on their street – the protocols must help identify unusual activity that may indicate a problem on the neighboring nodes .

5. Wireless network for developing regions

Google is working on building up wireless networks in sub-Saharan Africa, Southeast Asia and other developing regions, reports Google is said to be "deep" in the process of funding and building such networks, Using technologies such as satellites, blimps, microcells and more, Google believes their plan will work.

III. Wireless Network Security

RSA Security questioned firms in London, Paris, Milan and Frankfurt to find out what steps were being taken to keep data secure. RSA said that many firms it questioned also seemed to be fitting and forgetting about wi-fi access points.

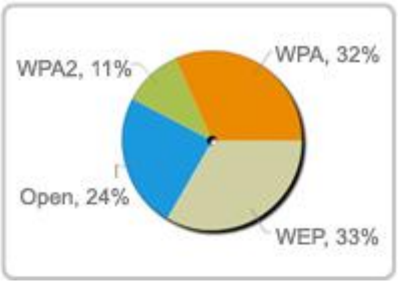
Many used the default settings that activated when the hardware was first plugged in and switched on.

AirTight Networks,The global leader in secure Wi-Fi solutions perform Financial Districts WiFi Security Survey. Survey Report

- Visited 7 financial districts (6 in US, 1 in UK)
- Scanned WiFi signal for 5 minutes at randomly selected location

- 3632 APs scanned
- 547 Clients scanned
- Picked up WiFi signals at 30 randomly selected points in:New York, Chicago, Boston, Wilmington,DE, Philadelphia, San Francisco, London
- A sample WiFi trace tells a lot about network security posture in each location.

Key Findings: Widespread Use of Insecure Practices



Overall Distribution of Wi-Fi security:

- 57% of Wi-Fi networks are either OPEN or using weak (WEP) encryption

Following measures are taken to make wireless network secured

1. Set up a security key for a wireless network

Personal information and files on your wireless network can sometimes be seen by people who pick up your network signal. This can lead to identity theft and other malicious acts. A network security key or passphrase can help to protect wireless network from this type of unauthorized access.

2. WPA

Wi-Fi Protected Access (WPA or WPA2) is more secure. There are two types of WPA authentication: WPA and WPA2. WPA2 is the most secure. short for ***Wi-FiProtected Access 2***, the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides high level of assurance that only authorized users can access their wireless networks.

There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server.

3. "Hole196" vulnerability

"Hole196" is vulnerability in the WPA2 security protocol exposing WPA2-secured Wi-Fi networks to insider attacks. AirTight Networks uncovered a weakness in the WPA2 protocol,

Central to this vulnerability is the group temporal key (GTK) that is shared among all authorized clients in a WPA2 network. In the standard behavior, only an AP is supposed to transmit group-addressed data traffic encrypted using the GTK and clients are supposed to decrypt that traffic using the GTK. However, nothing in the standard stops a malicious authorized client from injecting spoofed GTK-encrypted packets! Exploiting the vulnerability, an insider (authorized user) can sniff and decrypt data from other authorized users as well as scan their Wi-Fi devices for vulnerabilities, install malware and possibly compromise those devices

4. Change the router defaults

Make sure to change router’s factory presets (i.e. admin login and password) to something more secure to prevent any unauthorized users from accessing and changing router settings. Client may also change the Service Set Identifier (SSID) name.

Turn off SSID broadcasting

The SSID functions as a broadcast message that notifiesclient presence to any and every device within range of client network. All wireless routers have an option to turn off this broadcast, which hides client network from people who may want to access it. It won’t encrypt client data, but no one will try to access a network they don’t know client have

5. Allow access based on MAC addresses

Every network-enabled device – from desktops to tablets – is equipped with a unique, identifying number called a Machine Access Code (MAC). Most common wireless routers will have an option to filter access solely based on the MAC address, allowing wireless access only to devices client have preapproved and prohibiting all others

6. Limit DHCP

Dynamic Host Configuration Protocol (DHCP) allows limiting the number of IP addresses router can assign on client's wireless network, thus limiting the amount of devices that can connect. This can be done by accessing client's router's administrative setting and updating the number of devices client want to connect (both wired and wireless).

7. Disable remote administration privileges

Disabling remote administration privileges is a great way to close the door on anyone looking to access security settings. The option should be located in router's administrative settings and requires all security modifications to be changed directly through a wired connection to router.

IV. Conclusion

Almost on daily basis there are new developmentsreported in protocol, appliances and techniques of wireless networking. The use of WirelessNetwork has profoundly increaseddue to its fast connection capabilities covering larger areas. This also results in increased accessto unauthorized users and different types of attacks which lead to compromise in the security. WLAN vulnerabilities are mainly caused by WEP as its security protocol. However, these problems can be solved with the new standards, such as 802.11i.

References:

[1]. http://www.oreillynet.com/pub/a/wireless/2003/12/18/wap.html
[2]. http://www.oreillynet.com/lpt/a/3333
[3]. *www.sciencedaily.com/releases/2011/02/110214155503.htm*
[4]. www.everymac.com/.../what-is-**802.11n**-differences-between-**802.11n**-8..
[5]. Daily Tech - May 21, 2013
[6]. Forbes
[7]. http://www.digitaltrends.com/computing/how-to-secure-a-wireless-network/#ixzz2UXkC7okz
[8]. http://www.govtech.com/gt/406582
[9]. *www.digitaltrends.com*