Vol. 2 Issue 2, Feb.2012, pp. 320-324

Exploitation of WPA Authentication

Pranav S. Ambavkar, Pranit U. Patil, Prof. Pamu Kumar Swamy
VJTI, Matunga, Mumbai, India.

ABSTRACT
These days wireless communication is basic need of people. Users want to secure their important information. For security purpose different kinds of protocols are available. But fast development in codes, standards and technology gives opportunity to hack and steal the important information over wireless network. Therefore the security of network should be in consideration. Today there exist different kinds of tools and programs inbuilt in operating system. By using them and analyzing weaknesses of protocol used, cracking of protocol is easy. In this paper we will learn authentication WPA standard and way to crack WPA.

Keywords **- WPA, WEP, MAC layer, attacks, 4-way handshake.**

I. INTRODUCTION
The whole world of wireless communications, as we know it today, started in 1895, when Guglielmo Marconi transmitted the Morse code for letter "S" (three-dots) over a distance of 3 kms by electromagnetic waves. From this time, wireless communications have grown up into a key element of modern society. WiFi - Wireless LAN (Local Area Network) is the main technology for wireless connection to computer networks.Electronics devices can exchange information over network by using Wifi. [1]These devices can connect to each other also to Internet,router,bluethooth devices. Routers has a range of about 20 meters (65 ft) indoors and a greater range outdoors."Wi-Fi" is a trademark of the Wi-Fi Alliance and the brand name for products using the IEEE 802.11 family of standards.

Portable devices such as mobile, laptop, tablet can connect to Internet, wireless network, Wi-fi and share information among themselves. The information might be related to their personal, organization, national security. So for security purpose they have authentication protocols are designed.Without which no one can access network. There exist several standards for secure communication protocols in WiFi like WEP (Wired Equivalent Privacy), WPA (WiFi Protected Access) and WPA2. Different kinds of programs and tools are used to crack these standards such as operating system used for penetration.By using such tools cracker or hackers get practice to find weaknesses of authentication protocols.and by analyzing these weakenesses they hack the wireless network and steal the important information. Today for authentication used for good security is WPA.WPA cracking is done by by only brute force attack. But it takes a lot of time to crack WPA.In these paper we will also study how to crack WPA by using brute force attack.

In this paper we will discuss IEEE 802.11 architecture, general frame format, different kinds of attack on wireless network, authentication used for security and how WPA cracking is possible.

II. IEEE 802.11 ARCHITECTURE
A.Architecture Component[2] : IEEE 802.11 architecture is subdivided into cells. Each cell is called as basic service set (BSS).Each BSS has one access point and it controls the BSS. Every BSS is connected to each other by a single backbone line structure called as distribution system.

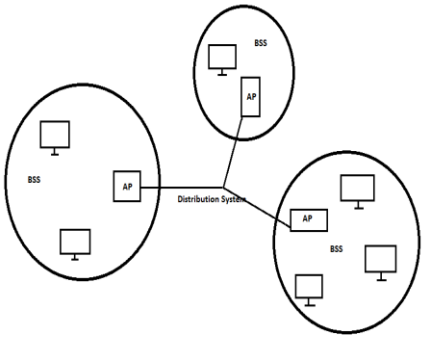

Fig1. Architecture Component

B. IEEE 802.11 Layers Description : IEEE 802.11 is covered by mainly two layers data link layer and physical layer. The physical layer of the original 802.11 standardized three wireless data exchange techniques:

-Infrared (IR)

-Frequency hopping spread spectrum (FHSS)

-Direct sequence spread spectrum (DSSS)

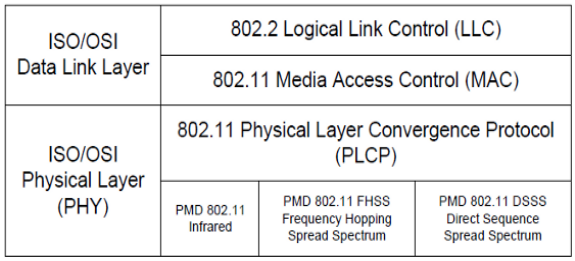

Fig.2 IEEE 802.11 Layers Description

[3]The 802.11 standard specifies a common medium access control (MAC) Layer, which provides a variety of functions that support the operation of 802.11-based wireless LANs. In general, the MAC Layer manages and maintains communications between 802.11 stations (radio network cards and access points) by coordinating access to a shared radio channel and utilizing protocols that enhance communications over a wireless medium. Often viewed as the "brains" of the network, the 802.11 MAC Layer uses an 802.11 Physical (PHY) Layer, such as 802.11b or 802.11a, to perform the tasks of carrier sensing, transmission, and receiving of 802.11 frames.

C. Introduction to 802.11 wireless frames : The best way to understand how any type of network protocol work is to look at it from the packet level. We'll first be describing how we can capture wireless frames that are flying through the air and then talk about dissecting and analyzing these frames for purposes of understanding how these packets look like under normal traffic conditions. Both the station and AP radiate and gather 802.11 frames as needed. The format of frames is illustrated below. Most of the frames contain IP packets. The other frames are for the management and control of the wireless connection.

D. General Frame Format : Each frame consists of

- A MAC Header: frame control, duration, address, and sequence control information

- A variable length frame body

- A frame check sequence (FCS), contains IEEE 32-bit cyclic redundancy code (CRC)

Frame Control	Duration/ID	Address1	Address2	Address3	Sequence Control	Address4	Frame Body	FCS
Octates:2	2	6	6	6	2	6	0-2312	4

Fig.3 General Frame Format

E. Capturing wireless packets : In case of wireless technology data or information is send or receive over air. Air makes a role as a mediator between two or more wireless devices. So that cracker can easily capture the packet over air and sniff the information.

To capture wireless packets sniffing device should know detail knowledge of capturing network and to this it should have proper hardware and software build over it. And that hardware should be Network Interface Card(NIC).

Under normal circumstances when your wireless NIC are sending and receiving wirelessly, they're placed into a mode called managed mode, and in this mode, the wireless NIC will not pick up any wireless packets which are not destined for it, thus defeating the purposes of being a sniffing station. In order for the wireless NIC to pick up all packets regardless of who the packet is for, the NIC will have to be placed in rfmon mode.

III. ATTACKS IN AD-HOC NETWORK[6][8]

From the point of view of intrusion detection and response, we need to observe and analyze the anomalies due to both the consequence and technique of an attack. While the consequence gives evidence that an attack has succeeded or is unfolding, the technique can often help identify the attack type and even the identity of the attacker. Attacks in MANET can be categorized according to their consequences as the following:

A.Drop Attack: An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order to reduce the quantity of routing information available to the other nodes

B.Routing Loop: A loop is introduced in a route path.

C.Network Partition: A connected network is partitioned into k (k >= 2) sub networks where nodes in different sub networks cannot communicate even though a route between them actually does exist.

D.Selfishness: A node is not serving as a relay to other nodes.

E.Sleep Deprivation: A node is forced to exhaust its battery power.

F.Denial-of-Service: A node is prevented from receiving and sending data packets to its destinations Some of the common attacking techniques are:

G.Cache Poisoning: Incorrect routes to be stored in the routing table of legitimate nodes

H.Fabricated Route Messages: Route messages (route requests, route replies, route errors, etc.) with malicious contents are injected into the network. Specific methods include: a) False Source Route: An incorrect route is advertised into the network, e.g., setting the route length to be 1 regardless where the destination is. b) Maximum Sequence: Modify the sequence held in control messages to the maximal allowed value. Due to some implementation issues, a few protocol implementations cannot effectively detect and purge these “polluted" messages timely so that they can invalidate all legitimate messages with a sequence number falling into normal ranges for a fairly long time

I.Rushing: An offensive that can be carried out against on-demand routing protocols

J.Wormhole: A tunnel is created between two nodes that can be utilized to secretly transmit packets.

K.Packet dropping: A node drops data packets (conditionally or randomly) that it is supposed to forward.

L.Spoofing: Inject data or control packets with modified source addresses.

M.Malicious Flooding: Deliver unusually large amount of data or control packets to the whole network or some target nodes

IV.WIFI AUTHENTICATION PROTOCOLS AND WPA BREAKING[7]

These protocols are important and provides fundamental knowledge of the following: i) WiFi security standards, how they work, where the weak points are, methods and approaches for hacking secured WiFi networks; ii) description of the techniques for password cracking and especially brute force password cracking; iii) an introduction to existing tools and algorithms for WPA cracking.

A. WiFi Authentication Protocols[5] : This section provides an overview of WiFi encryption standards. These standards are certificated by the WiFi Alliance much like the devices, which incorporate those standards. The main reason is interoperability between all certificated devices. All devices with the WiFi trademark have been certified by the WiFi Alliance and meets all the requirements. In these security standards stand security options like MAC (Media Access Control) / MAC ID / MAC address filtering. In the AP (Access Point) the list of MAC addresses is stored and only clients with a MAC address in the list are allowed to connect to the AP. Unfortunately, spoofing any MAC address (i.e., making a fake MAC address) is fairly easy. Another additional option is SSID (Service Set Identification) disabling. SSID is the identifier of the WLAN (Wireless LAN) which is broadcasted by the AP in the beacon frame to enable easy selection of the WLAN by the user. Disabling the SSID makes the network invisible for the ordinary users and SSID has to be set in the client's network manager. However, there are tools for sniffing the network communication, which can detect the WLAN with disabled SSID broadcasting.

Besides the two previously mentioned mechanisms, some encryption techniques can be applied to further secure wireless connections. In the following part of this section, the WEP, WPA and WPA2 standards are described.

B.WEP Encryption[4][15] : WEP has three settings: Off (no security), 64-bit (weak security), 128-bit (a bit better security). WEP is not difficult to crack, and using it reduces performance slightly. If you run a network with only the default security, where WEP is turned off, any of your neighbors can immediately log on to your network and use your Internet connection. For wireless devices to communicate, all of them must use the same WEP setting. (40-bit and 64-bit WEP encryption are the same thing 40-bit devices can communicate with 64-bit devices.) While there is no extra performance cost

to encrypting the longer key, there is a cost to transmitting the extra data over the network. 128-bit security is not much more difficult than 64-bit to crack, so if you are concerned about performance, consider using 64-bit. If you're very concerned about security, use WPA, which replaces WEP with a protocol that is given current technology, impossible to crack. The WEP concept of *passphrase* is introduced so that you do not have to enter complicated strings for keys by hand. The passphrase you enter is converted into complicated keys. Choose passphrases with the same care you would important passwords.

- With 128-bit encryption, you need to enter a passphrase to generate each key.
- All four keys must be specified, because WEP switches between them to make your traffic more difficult to break.
- All devices within your LAN must use the same passphrases (i.e., the same keys).

C. WPA/WPA2 Encryption[7] : WPA stands for WiFi Protected Access. WPA has been accepted in 2002 as a temporary solution by the WiFi Alliance, as a response to delayed development of the IEEE 802.11i standard (nowadays known as WPA2) WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark.. WPA2, which offers government- and enterprise-grade security, is available in all products that the alliance has anointed as "WiFi Certified." The security standard replaces the original WPA and has stronger security than WPA and other protocols, including WEP (Wired Equivalent Protocol), which is still an option with most routers. WEP was introduced in 1997 and was largely supplanted by WPA and WPA2.

E. WPA-PSK Cracking : It has been found out that WPA-PSK cracking is the only possible way to crack this security standard. To successfully crack WEP/WPA, you first need to be able to set your wireless network card in "monitor" mode to passively capture packets without being associated with a network. This NIC mode is driver-dependent, and only a relatively small number of network cards support this mode under Windows. One of the best free utilities for monitoring wireless traffic and cracking WEP/WPA-PSK keys is the aircrack-ng suite, which we will use throughout this article. It has both Linux and Windows versions (provided your network card is supported under Windows). The aircrack-ng site has a comprehensive list of supported network cards available here: NIC chipset compatability list.Here we will use aircrack-ng version 1.0 on a Linux partition (blackbuntu 2) on Dell Inspiron 4050 laptop, using the built-in Intel network card.

The aircrack-ng suite is a collection of command-line programs aimed at WEP and WPA-PSK key cracking. The ones we will be using are:

airmon-ng - script used for switching the wireless network card to monitor mode
airodump-ng - for WLAN monitoring and capturing network packets
aireplay-ng - used to generate additional traffic on the wireless network
aircrack-ng - used to recover the WEP key, or launch a dictionary attack on WPA-PSK using the captured data.

4-Way Handshake is also one of the thing to learn as it is related to wireless network. The information in the first two messages are enough for password cracking. Even though it is enough, it is important to eavesdrop the whole 4-Way handshake to be sure that the handshake was successful and that the information in the first two messages is valid. Host A sends a TCP SYNchronize packet to Host B, Host B receives A's SYN, Host B sends a SYNchronize-ACKnowledgement, Host A receives B's SYN-ACK, Host A sends ACKnowledge, Host B receives ACK. TCP socket connection is ESTABLISHED, SYNchronize and ACKnowledge messages are indicated by a bit inside the header of the TCP segment. TCP knows whether the network TCP socket connection is opening, synchronizing, established by using the SYNchronize and ACKnowledge messages when establishing a network TCP socket connection. When the communication between two computers ends, another 3-way communication is performed to tear down the TCP socket connection. This setup and teardown of a TCP socket connection is part of what qualifies TCP a reliable protocol. TCP also acknowledges that data

is successfully received and guarantees the data is reassembled in the correct order.

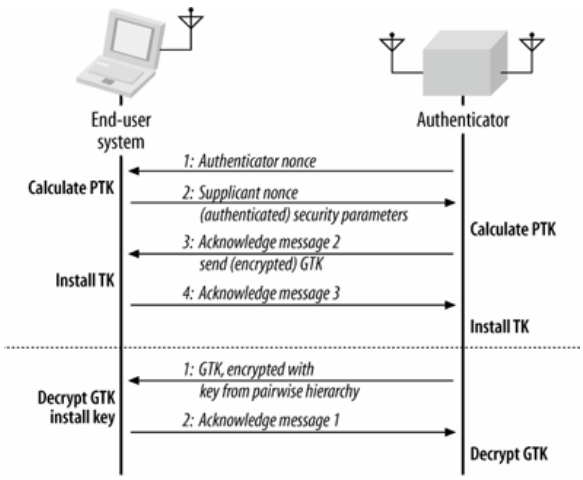

Fig.4 Way handshaking

a. WPA Cracking Tools : From the time of releasing WPA there are teams of security experts and hackers, who try to break it and some developers have even released tools for cracking WPA.

The list of used HW for this test: AP: D-Link**,** Client laptop OS: Blackbuntu2**,** WiFi card**,** Monitoring/capturing: laptop OS: Blackbuntu2, WiFi card**.**

IV. CONCLUSION AND FUTURE WORK

Thus we have successfully surveyed the important terms in the world of Wireless and acknowledged the important work done in these field. We also have studied the important attacks and their modus operandi. The study of authentication protocols led us to knowledge of WPA breaking and cracking. This study may lead us to harden our protocol system and making it resistant to cracking tools. Our future work will be mainly aimed at simulating various attacks on WPA by cracking it. Successful simulations will guide through hardening the present day protocols.

REFERENCES

1. http://en.wikipedia.org/wiki/Wi-Fi

2 .A technical tutorial on IEEE 802.11 protocol by Pablo Brenner

3.http://www.wifiplanet.com/tutorials/article.php/1216351

4.http://support.netgear.com/app/answers/detail/a_id/1141/~/what-is-wep-encryption-for-wireless-networks%3F

5. WPA password cracking by Master thesis, AAU, Applied Signal Processing and Implementation Spring 2009
6. A Practical Message Falsification Attack on WPA by Toshihiro Ohigashi1 and Masakatu Morii2 1 Hiroshima University

7. A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i) by ARASH HABIBI LASHKARI

8. Practical attacks against WEP and WPA by Martin Beck, TU-Dresden, Germany

9. Enhanced TKIP Michael Attacks by Martin Beck, TU-Dresden, Germany

10. MAC Layer Anomaly Detection in Ad Hoc Networks

11. Weakness Analysis and Attack Test for WLAN by LIU Wu

12. Your 802.11 Wireless Network has No Clothes William A. Arbaugh

13. Impact of Wireless IEEE802.11n Encryption Methods on NetworkPerformance of Operating Systems by Shaneel Narayan

14. New Protocol Design For Wireless Network Security by Prof. Dr. Gamal Selim

15. Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA) by ARASH HABIBI LASHKARI