Cracking the Wired Equivalent Privacy (WEP) Key

Project for ECE579W
Instructor: Dr. Wenjing Lou

Introduction:

The purpose of this project is to experiment with an IEEE 802.11 wireless network and learn how to exploit its security properties. In this project, you will learn how to use a variety of tools for surveying and sniffing wireless networks. The overall goal, however, is to crack the Wired Equivalent Protocol (WEP) protocol defined in the 802.11 standard. You have one month to complete this project. Don't start your project at last minute. It does require some effort to complete!

The WEP protocol is crippled with numerous security flaws. Most of these weaknesses are described in "Weaknesses in the Key Scheduling Algorithm of RC4" by Scott Fluhrer, Itsik Mantin and Adi Shamir. The first person to implement this attack was Adam Stubblefield.

System setup

The experimental system setup in this project is as follows.

A standalone wireless access point has been set up which is only connected to a linux server by wire. An authenticated laptop client is used to communicate with the server through the wireless AP. Through some kind of service, a file is being transferred to the clients. The data traffic is encrypted using 128 bit WEP key, and the server requires a username and password.

Your job is to: I) sniff the traffic, recover the WEP key; II) find out the username and password of the server, III) impersonate the legitimate client, connect to the server and download a secret file from the server.

Notes

No laptop will be provided for students in this project. You have to use your own personal equipment/laptop.

In order to sniff packets, your wireless card must be able to work under the promiscuous mode (monitoring mode). Do find it out before you carry out the project. Most of the 802.11b/g wireless card can be configured to run in the promiscuous mode; however, many USB based ones cannot. Most PCMCIA cards will do promiscuous mode just fine though.

Linux OS is highly recommended for this project, though Windows can do the same job as well. The best practice is to use a special security Linux distribution (such as WHAX, backtrack and etc) and a USB flash drive with at least 1G capacity. If you are not familiar with Linux, start your project as early as possible.

Please be advised that you should be very careful when you try different network sniffing and monitoring tools. Do not hack any wireless network other than the one provided for this course (SSID ECE579W).

Wireless Access Point (AP) Location:

The AP is located in AK018, running both 802.11b and 802.11g protocols. Please report to wjlou@ece.wpi.edu if the AP seems to be failing.

Guidelines

You are not required to follow the procedures/steps mentioned below as long as you finish the required task correctly. These steps are just meant to provide you with some guidelines.

Part I

To begin this project, you will have to figure out the detailed information about the wireless network with the SSID of "ECE579W". Such information includes which channel the AP is using, what kind of security features the AP is implementing, the AP's MAC address, the clients that are associating with the AP, etc. Of course, you are not going to be able to connect to it if you just simply set your client to associate with the AP.

- For windows users, you can survey the site using Netstumbler.
- For Linux users, you can use either Kismet or Airsnort.

After surveying the site, it should be fairly clear as to why you cannot associate properly.

Part II

This step requires you to sniff the traffic on the WLAN - hopefully your sniffing will provide you with enough information to crack the WEP key and associate with and use the WLAN. Tools such as Kismet, Airsnort, Airdump, Wireshark and OmniPeek can be used, but you may use whatever you like as long as it can work by configuring your wireless card into promiscuous mode.

Definitely be patient with the sniffing; wait until enough WEP encrypted data is collected. It is important to look for WEP-encrypted data sent to/from the SSID because they contain the most important data (the weak IVs). For a 64-bit WEP key, between about 50,000 and 200,000 packets are required, and between 200,000 and 700,000 are needed for a 128-bit key. Nevertheless, some students in the past have been unable to recover the key even with 1,000,000 packets collected.

Note that since in this project setup, the service between server and the client is simply set to be running continuously so that the time needed to collect enough packets should not be very long. In some other cases where there is not so much traffic, you can actively spoof the AP so that more "weak" IVs will be sent out. Therefore, you end up getting enough weak IVs with much less time. The record of recovering the WEP key was less than 2 hours.

Part III

After doing your reconnaissance, you should have acquired enough information to recover the encryption key and access the server. The WEP key is 13 bytes in hexadecimal format and the server's password is also 13 bytes but in ASCII format. Once you recover the password, you will know it is the right key immediately. ☺

Find out which file the client is downloading from the server. Your job is to go to the directory of the file that is being transferred, and get the other file that sits in the same directory. There are only two files under the same directory. Once you are connected to the network with the key you recovered, you will need to find out what's going on. Figure out who the server is by sniffing the network traffic. Also determine which services it provides.

In order to get the secret file, you can masquerade as a legal client to get that file. Please note that, all the necessary information needed to be a legitimate user has been collected in part II.

What to Turn In

Part I: (20 pts)
1. Describe the security features implemented at the wireless access point. (10 pts)
2. Provide the detailed information about the AP and its clients. (10 pts)

Part II: (60 pts)
1. Analyze the sniffed packets and find out the IP address of the server. (10 pts)
2. The WEP key you recovered. (20 pts)
3. Describe how you can connect to the wireless access point as a legitimate user. (20 pts)
4. Find out the vulnerable services running at the server. (10 pts) You may use tools such as Nessus to do this task.

Please provide detailed steps (including what tools/commands with parameters are used, provide snapshot if necessary) for each part above.

Part III: (20 pts)
Get the file, and provide a detailed description of how you got it. (20 pts)

Please put everything into a tar ball and email it to wjlou@ece.wpi.edu
Good luck and enjoy!

Windows Wireless Security Tools

Ethereal – a free network protocol analyzer (sniffer) http://www.ethereal.com/

Wireshark – an award-winning network protocol analyzer. http://www.wireshark.org/

WinPcap – for capturing packets http://winpcap.polito.it/default.htm

Netstumbler – site surveying utility http://www.netstumbler.com/

tinyPEAP – Official tinyPEAP site http://www.tinypeap.com

Change MAC address: http://www.nthelp.com/NT6/change_mac_w2k.htm or http://students.washington.edu/natetrue/macshift/

WepLab – a Wep Security Analyzer. http://weplab.sourceforge.net/

OmniPeek Network Analyzer. http://www.wildpackets.com/products/omnipeek/overview

Aircrack-ng - an 802.11 WEP and WPA/WPA2-PSK key cracking program.
http://www.aircrack-ng.org/doku.php?id=aircrack-ng

WepLab – a Wep Security Analyzer. http://weplab.sourceforge.net/

Linux Wireless Security Tools

Ethereal – a free network protocol analyzer (sniffer) http://www.ethereal.com/

LibPcap – should be available with your distribution of Linux.

Kismet – A VERY good tool for surveying wireless networks puts Netstumbler to shame
http://www.kismetwireless.net/

Airsnort – A utility for cracking WEP keys. Also, you can get information about Monitor mode on the Airsnort page. You may find this useful, although not essential.
http://www.wirelessdefence.org/Contents/AirsnortMain.htm

For changing you MAC address in Linux, use ifconfig <iface> hw ether <mac address>.

WepLab – a Wep Security Analyzer. http://weplab.sourceforge.net/

WepAttack – this tool uses different approach (active dictionary attack) to crack the WEP. You are welcome to try it. http://wepattack.sourceforge.net/

WEPCrack - an open source tool for breaking 802.11 WEP secret keys.
http://wepcrack.sourceforge.net/