Proceedings of the 7th International Conference on Applied Informatics
Eger, Hungary, January 28–31, 2007. Vol. 2. pp. 385–390.

Wireless security

Tamás Krausz

Department of Informatics, University of Debrecen

Abstract

The most common inefficient security methods using wireless network are MAC filtering, SSID hiding, LEAP authentication, disabling DHCP, antenna placement, using 802.11a, wep.

This paper deals with the weak points with modern free hacking tools: kismet, netstumbler (wireless scanners), airodump (traffic recorder), aireplay (wireless packet injector) aircrack (wep cracker), wepdecrypt (decrypt dump files). We can even use full live cd like auditor, backtrack. Finally we investigate what practical solutions can be done in different environment like, home, small business, large enterprise.

Keywords: wifi, security, 802.11

1. The most common inefficient security measures with wireless network

1.1. MAC filtering

The MAC address is just a 12 digit long HEX number that can be viewed in clear text with a sniffer. Once the MAC address is seen in the clear, it takes about 10 seconds to cut-paste a legitimate MAC address in to the wireless Ethernet adapter settings and the whole scheme is defeated. MAC filtering is absolutely worthless since it is one of the easiest schemes to attack. The shocking thing is that so many large organizations still waste the time to implement these things.

1.2. SSID hiding

There is no such thing as "SSID hiding". You are only hiding SSID beaconing on the Access Point. There are 4 other mechanisms that also broadcast the SSID over the 2.4 or 5 GHz spectrum. The 4 mechanisms are; probe requests, probe responses, association requests, and re-association requests. Essentially, you are talking about hiding 1 of 5 SSID broadcast mechanisms. Nothing is hidden and all you have achieved is cause problems for Wi-Fi roaming when a client jumps from AP to AP. Hidden SSIDs also makes wireless LANs less user friendly.

1.3. Disabling DHCP

This is much more of waste of time than it is a security break. DHCP allows the automatic assignment of IP addresses and other configurations. Disabling DHCP has zero security value and just wastes time. It would take a hacker about 10 seconds to figure out the IP scheme of any network and simply assign their own IP address. Anyone who tells you that this is a way to secure your wireless LAN does not know what they are talking about.

1.4. Antenna placement

The craziest thing from so called security experts that actually tell people to only put their Access Points in the center of their building and put them at minimal power. Antenna placement does nothing to deter hackers. Remember, the hacker will always have a bigger antenna than you which can home in on you from a mile away. Making a wireless LAN so weak only serves to make the wireless LAN useless. Antenna placement and power output should be designed for maximum coverage and minimum interference. It should never be used as a security mechanism.

1.5. Using 802.11a

There were so called security experts that went around telling people that they simply needed to switch to 802.11a or Bluetooth to secure their wireless LAN. 802.11a refers to a physical transport mechanism of wireless LAN signals over the air, it does not refer to a security mechanism in any way.

1.6. Wep

Wired Equivalent Privacy (WEP) is a scheme to secure IEEE 802.11 wireless networks. WEP was intended to provide confidentiality comparable to that of a traditional wired network. Several serious weaknesses were identified by cryptanalysts; a WEP connection can be cracked with readily available software in one minute or less.

2. Hacking tools

2.1. Kismet

Kismet is an 802.11 layer2 wireless network detector, sniffer and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. Kismet identifies networks by passively collecting packets and detecting (and given time, decloaking) hidden networks, and infering the presence of nonbeaconing networks via data traffic.

2.2. Airodump (traffic recorder)

Airodump is an 802.11 packet capture program that is designed to capture as much encrypted traffic as possible. each WEP data packet has an associated 3-byte Initialization Vector (IV).

2.3. Aireplay (wireless packet injector) sample

This injection procedure is required when there is not enough encrypted traffic being passed across the WLAN to break the WEP key (approximately 300,000 packets are required for breaking 64-bit WEP and approximately 1,000,000 packets for 128-bit WEP). This process involves:

- Deauthing a valid client (to increase the chances of acquiring an ARP packet, will also allows us to determine a hidden ESSID.
- Capture and replay of a valid ARP packet to speedup/generate the collection of encrypted packets.

2.4. Aircrack (wep cracker)

After a sufficient number of data packets have been collected, run aircrack on the resulting capture file. Aircrack will then perform a set of statistical attacks.

2.5. Wepdecrypt (decrypt dump files)

Wepdecrypt is a Wireless LAN Tool written in c which guesses WEP Keys based on a active dictionary attack, key generator, distributed network attack and some other methods, it is based on wepattack and GPL licensed. We can even use full live cd like auditor, backtrack.

3. Connecting to cracked wireless network in linux environment

3.1. Connecting to an OPEN / WEP WLAN (DHCP)

Note: replace [interface] with your interface name as required (e.g. eth1, wlan0, ath0 etc.).

iwconfig [interface] mode managed key [WEP key] (128 bit WEP use 26 hex characters, 64 bit WEP uses 10)

iwconfig essid "[ESSID]" (Specify ESSID for the WLAN)

dhclient [interface] (to receive an IP address, netmask, DNS server and default gateway from the Access Point)

3.2. Connecting to an OPEN / WEP WLAN (Manual IP Setup)

Note: replace [interface] with your interface name as required (e.g. eth1, wlan0, ath0 etc.)

It may be necessary to run some packet capture software (e.g. Ethereal) to determine the IP addresses of both the Default Gateway and DNS servers.

iwconfig [interface] mode managed key [WEP key] (128 bit WEP use 26 hex characters, 64 bit WEP uses 10)

iwconfig essid "[ESSID]"

ifconfig [interface] [IP address] netmask [subnetmask]

route add default gw [IP of default gateway] (Configure your default gateway; usually the IP of the Access Point)

echo nameserver [IP address of DNS server] » /etc/resolve.conf (Configure your DNS server)

iwconfig [interface] key 1111-1111-1111-1111 (set 128 bit WEP key)

iwconfig [interface] key 11111111 (set 64 bit WEP key)

iwconfig [interface] s:mykey (set key as an ASCII string)

4. Solution

Finally what practical solutions can be done in home and SOHO, small business, large enterprise environment.

4.1. Small office and home

- WPA PSK

WPA PSK mode can be an effective security mechanism but leaves a lot to be desired in terms of usability. This is because WPA PSK can be cracked with offline dictionary attacks so it relies on a strong random passphrase to be effective. Unfortunately, humans are very bad at memorizing long random strings of characters and will almost always use simple to remember words and phrases or some slight variation of that. This lends itself to dictionary attacks where a hacker will try every variation of every combination of words in the dictionary. To make this very difficult to hack, use a 10 digit string of random characters comprised of a–z, A–Z, 0–9 or use a very long word phrase made up of 20 or more characters. Unfortunately, this will force many users to write down their passphrases which in itself may lead to passphrase theft. WPA PSK is not a good long term security solution and leaves Level 1 security with much to be desired, but it can be safe when used correctly.

4.2. Small business

- Extensible Authentication Protocol
- Radius Username/password
- AES

Small businesses must move beyond Level 1 by incorporating authentication in to their Wireless LAN access controls. The standardized method for doing this is 802.1x and PEAP or TTLS authentication. 802.1x restricts access to the Datalink layer of a network by only permitting access to the network if a user proves their identity through the EAP (Extensible Authentication Protocol) mechanism. There are many forms of EAP, but the two forms of EAP that is most appropriate for Level 2 security is PEAP (Protected EAP) and TTLS (Tunneled Transport Layer Security). Note that PEAP in the general context refers to PEAP-EAP-MSCHAPv2 mode, which only requires a Server Side Digital Certificate and a Client Side Username/Password. There are stronger forms of PEAP which we shall cover later in the higher security levels. TTLS is actually a little better in security than PEAP-EAP-MSCHAPv2 because it does not divulge the username in clear text. However, both forms of authentication do a good job of protecting passwords because the MSCHAPv2 password challenge session is protected inside an encrypted tunnel.

4.3. Large enterprise

- Extensible Authentication Protocol
- Radius Username/password
- "soft" Digital Certificates, PKI

EAP-TLS or PEAP-EAP-TLS using "soft" Digital Certificates (certificates that are stored on the user's hard drive) would be the recommended authentication method for this security level. PEAP-EAP-TLS is an improved version of the original EAP-TLS protocol that goes further to encrypt client digital certificate information. Both PEAP-EAP-TLS and EAP-TLS have the same server and client side digital certificate requirements, but PEAP-EAP-TLS may not be compatible with some older Supplicants (Client Software) or some non-Microsoft client side implementations. The only way to compromise this security level is if the hacker can not only steal a user's password, but also steal that user's Digital Certificate which is much more difficult than just stealing a user's password. To steal a "soft" Digital Certificate, either the laptop needs to be stolen in which case it would be obvious and the certificate could be revoked, or a malicious program like a backdoor, virus or worm would have to be installed on the laptop to "harvest" the private key of the digital certificate. The latter option is much more sinister because a theft could occur totally undetected and the certificate would not be revoked. The same malicious code could also "log" the user's keystrokes and the user's password would be compromised as well.

References

[1] Jahanzeb Khan Ani Khaja, Building Secure Wireless Networks with 802.11, *Wiley Publishing* (2003).

[2] Jon Edney William A., Arbough Real 802.11 Security Addison Wesley (2003).

[3] Hack proofing your wireless network, *Syngress*.

[4] Hurley, C., Puchol, M., Rogers, R., Thornton, F., WarDriving: Drive, Detect, Defend: A Guide to Wireless Security Syngress (2004).

[5] Ou, G., Wireless LAN security guide `http://www.lanarchitect.net/`

[6] Cyrus Peikari, Seth Fogie Maximum Wireless Security, *Sams Publishing* (2002).

[7] Flickenger, R., Wireless Hacks O'Reilly, (2003).

Tamás Krausz
Department of Informatics
University of Debrecen
Egyetem tér 1
H-4032 Debrecen
Hungary