Attacks on wireless clients

HOTSPOTTING

Security experts are always concerned with WLAN access points, but they sometimes forget that the client is also open to attack. Public hotspots make it quite easy for attackers to hijack connections, as the Hotspotter tool demonstrates.

BY MAX MOSER

Thanks to today's complex security mechanisms, wireless networks appear to be getting safer by the minute. Authentication constructions based on the EAP framework (Extensible Authentication Protocol) promises to keep uninvited guests at bay. The Temporal Key Integrity Protocol (TKIP) [1], with its quickly changing WEP keys, prevents replay attacks and makes cracking the encryption technology more complex. And keys are getting longer.

WPA/WPA2 [2] and the move to AES encryption [3] would seem to provide a nearly perfect security solution for enterprise networks. And just to make sure, access points are also equipped with VLAN support, Intrusion Detection, and firewalling systems – all of which cost serious sums of money.

But danger lurks beyond the confines of the enterprise network. In our upwardly mobile age, many people like to work on the move. And this has become a reality; thanks to the increasing pervasiveness of wireless networks and good administrators, people really can work in many public places: at the airport, the hotel, or congress rooms. If you really want to work, there is very little to stop you.

Executives who need to travel around the world appreciate their new-found flexibility and often decide to emulate it in their own enterprise environments. IT departments are often forced to introduce highly complex security infrastructures to handle the sensitive traffic flying across the ether. Additionally, enterprise-wide wireless services often need to be restricted to authorized users.

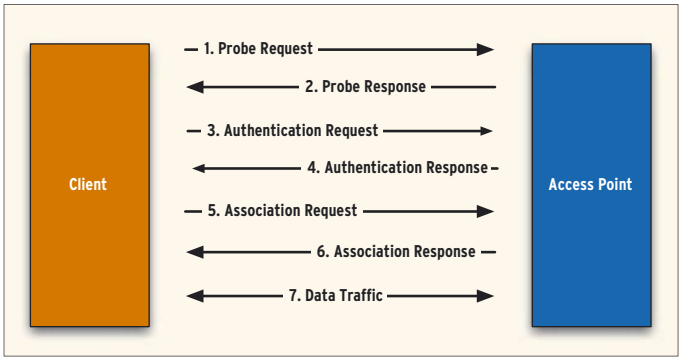

Figure 1: Logging on to an access point. Exploits hit clients while they are still searching for available networks in Steps 1 and 2.

Managers on the Move

A typical executive who travels the country with a WLAN-capable laptop under their arm will typically enable at least two wireless configurations, or profiles – one for working in public hotspots, that is, at airports or hotels, and another for secure access to the protected enterprise network. And the Internet gives you a number of databases that tell you where the next hotspot is located [4].

A wireless network comprises a number of components, and a variety of pack-

Figure 2: Tools like Ethereal allow you to analyze the structure of IEEE802 packets. The example shows a Probe Response packet, as used for the attack described in this article.

ets are needed to handle communications, for example, data, control, and management packets. Management packets are particularly interesting in this case, as they handle service advertising, logging on and off, and power management (see the box titled "Critical Management Packets").

In the Clear

Management packets within a wireless network are transmitted in the clear. As if this wasn't bad enough, there is almost nothing in the line of integrity checking or sender/receiver validation. A second access point could transmit Probe Response packets in reply to a client's Probe Request and then invite the client to associate. A Probe Response packet, like the one shown in Figure 2, comprises multiple segments.

The most important of these are:

- *Framecontrol (FC)* specifies the packet type ("0" for management packets) and subtype ("5" for Probe Response), as well as the flags, which are always set to 0 for a Probe Response.
- "Destination address" is the client MAC address.
- "Source address" is the MAC address of the access point.
- "BSS Id" is the MAC address of the access points.
- "Fixed parameters" comprise a timestamp and some capability information for the network.
- "Tagged parameters" include the SSID, its length and the channel, along with the supported transmission speeds.

The question is, how are users supposed to recognize that they really are connected to the trusted network they wanted to associate with, and not to a network controlled by an attacker? In fact, users have no way of knowing – and this is precisely where the security hole gapes.

On closer inspection, you will note that a network publishes the following information:

- Logical network name (SSID)
- MAC address of the access point
- Access point configuration

Any access point can use the SSID, that is, the logical name of the current network, as this is a freely configurable value which is not validated and does not need to be unique.

The access point MAC address could easily be duplicated if an attacker uses a software-based access point. And a duplicate MAC address will not typically have any impact on the network, in contrast to a traditional wired network. An access point will not typically inspect incoming packets to see if it originally sent these packets.

Some devices now include proprietary Intrusion Detection System modules to check for packet injection. But the only real way of mitigating the danger would be to introduce sender/receiver validation as implemented by an open source project called Wlsec [6]. Unfortunately, this project has drawn little response from the commercial wireless world thus far.

No Authentication

A rogue access point will not be able to spoof the authentication and encryption configuration, of course, as this information is not advertised. However, hotspot configuration parameters are designed to be anticipated, much in contrast to those used by enterprise access points. Both protection schemes are disabled, as a hotspot will not typically authenticate

Box 2: Monitor Mode

Monitor Mode, also known as RFMON mode, is a special mode in which the wireless card firmware passes any packets it receives to the driver software, rather than just the packets destined for the current node – you can liken this to listening to multiple radio stations at the same time.

Box 1: Critical Management Packets

Beacons: Are transmitted by the access point for timing purposes and to advertise network parameters.

Probe Request: Sent by the client to search for available networks and contains parameters such as the SSID and frequency.

Probe Response: The access point's reply to the Probe Response packet, which either confirms or rejects continuing transactions.

Association Request: The client announces its intent to join a specific network.

Association Response: The access point replies, saying whether it will allow the client to join the network.

Disassociation: The access point telling the client(s) to drop the current connection.

Authentication: The client authenticating for the network connection.

Deauthentication: Sent by the access point to remove the existing authentication.

users or encrypt data. Both would be inconvenient for potential customers.

This allows an attacker to spoof a trusted network; wireless clients will assume that they have connected to the trusted network, although in reality, they have connected to the attacker's network. Attackers could even use multiple wireless adapters to set up a man in the middle scenario, where the access point sniffs the client data before bundling the data off to the intended recipient.

This approach was first demonstrated with Airjack [7]. The Shmoo Group, which gained famed with Airsnort, quickly recognized the problem and developed the Airsnarf [8] tool, which generates a rogue software-based access point with a faked Web login page.

If a client refuses to release an existing session, the Void11 tool can generate deauthentication packets and force the client to go back and search for networks again.

Hotspotter

Airsnarf does not give users a fully automated exploit, as this would assume that some network parameters, such as the SSID, were known. The Hotspotter [9] tool, by the author, uses a similar approach to Airsnarf but autonomously reacts to clients searching for unprotected networks. The program can use any adapter that can be configured using *iwconfig mode monitor* and *iwconfig mode master*; cards with the Prism2 chipset and Atheros-based cards performed well in our labs.

Box 3: Grave Danger with Windows

To keep client administration as simple as possible, and to allow people to use more or less any hotspot without reconfiguring their laptops, users typically create a "My secure network" profile and an "ANY" profile. The latter is a special case and includes any network, regardless of the network name.

If an attacker tries to spoof the secure network, the client will typically not be able to associate with the network, as the encryption or authentication settings do not match. However, this is not always the case for Windows users with the configuration we just described as the "ANY" profile is implicit.

Hotspotter first switches the wireless card to RFMON or monitor mode (see the box titled "Monitor Mode"). In this mode, the program accepts any packets in the reception area and evaluates any probe request.

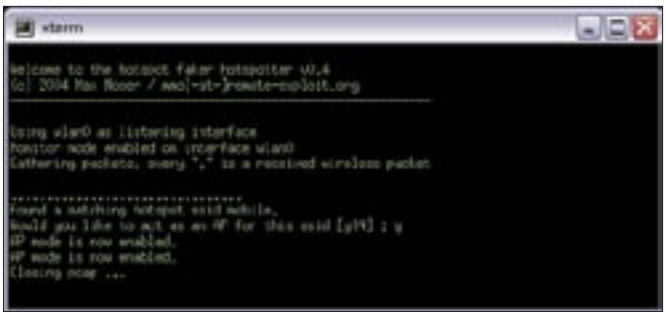

Figure 3: Hotspotter in action, each dot indicates a received network packet.

Probe Request packets include the details of the network the client is currently looking for (see the "Critical Management Packets" box.)

To search for a network, the client sends Probe Request packets with the SSID parameter of the required network. Put more simply, the client in our example shouts: Hello, is this network "a_hotspot_operator" or "my_secure_enterprise_network"?, and if this happens to be the case, the access point sends a response, and the connection can be established using the settings defined in the client's profiles.

If a client loses its network connection, it tries again. Depending on the settings, the client will either attempt to locate the networks defined in its profiles at regular intervals, or it may wait for the user to tell it to do so.

If the client fails to find the network it is looking for, it typically falls back to the next network name defined in its profile list. This allows an attacker to discover the profiles a client defines.

Hotspotter grabs the SSID of the requested network and compares it with a list of access points that do not provide encryption. If Hotspotter finds a match, it immediately quits monitor mode and automatically configures the card as a software access point (see Figure 3). Put more simply, Hotspotter replies to the client: Yes! Here's the "a_hotspot_operator" network; you can associate with me. The client is typically only too pleased to comply. This puts the network connection firmly in the attacker's hands.

Push-Button Exploit

If you specify the *-r* or *-e* option, and additionally pass Hotspotter a bash script, all of this happens automatically. *-r* means do this before switching to access point mode, and *-e* means wait for the attacker's wireless card to be configured as an access point.

Of course there are no limits to what the attacker can tell Hotspotter to do within the confines of the bash script. This might include automatic DHCP-based IP address assignment and DNS-based name resolution for the target client, automatic port scanning, automatic data sniffing, or even owning the system by installing another exploit or a trojan. The attacker could just as easily present the client with a spoofed login page.

Conclusions

If you think about the number of laptops that have embedded wireless adapters today, it quickly becomes apparent that wireless activities in trains, at airports, or trade fairs are a very serious problem. It is easier than you think to slip past expensive security measures and install trojans or steal data that might give an attacker new attack vectors for the oh-so-secure enterprise network. ■

INFO

[1] TKIP: *http://www.cisco.com*
[2] WPA: *http://wwww.wi-fi.org*
[3] AES: *http://www.faqs.org/rfcs/rfc3565.html*
[4] International hotspot directory: *http://mobile.yahoo.com/wifi*
[5] Odyssey client for Windows: *http://www.funk.com/radius/wlan/lan_c_radius.asp*
[6] WLSec project: *http://wlsec.net*
[7] Airjack: *http://sourceforge.net/projects/airjack*
[8] Airsnarf: *http://airsnarf.shmoo.com*
[9] Hotspotter: *http://wwww.remote-exploit.org*