Security strategies for wireless networks

ON AIR

WLANs give you Internet access without a bird's nest of wiring. But if you don't take security seriously, you might find yourself with uninvited guests. **BY ERIK BÄRWALDT**

Scott Maxwell, Fotolia

The wireless network has gained a permanent place in many home and small-office networks. Devices such as a WLAN router and a DSL or cable modem are available for little or no money from your Internet provider or local electronics shop. Most contemporary computers come with everything you need for wireless networking, and even if you have to upgrade your desktop system for wireless access, PCI WLAN cards for desktops are quite inexpensive.

But the fun stops when you discover that a neighbor has been using your WLAN to surf the web. Although an occasional clandestine surfer might not hurt your bank account in the age of flat-rate access fees, unauthorized surfing can have unpleasant consequences. If that nice guy next door happens to use your Internet connection to do something illegal, you can expect a visit from the police. Even if you don't find yourself in the center of an Internet crime ring, the very presence of an outside user on your network poses any number of security threats. Thus, it is very important – especially if you are still using legacy equipment – to make the most of the security features available with your wireless devices. In this article, I offer some tips for better security on wireless networks.

The 802.11b WLAN devices still used in many private households today belong to a hardware generation that dates back to the late 1990s. These devices support a maximum data transfer rate of 11MBps, with the bandwidth shared among the clients. This overall capacity means that, under perfect technical conditions, you can expect transfer rates of around 5MBps.

To improve the speed, many manufacturers launched proprietary extensions that promised faster transfer rates. However, most proprietary components will only work with matching products from the same manufacturer. Secure WLAN transmission is typically impossible with a collection of devices from various vendors, which explains why the Wi-Fi Alliance established its own certification program parallel to the WPA standard. Devices need to be 100% standards com-

Tips for WEP Networks

If you are still using a wireless network designed for the WEP standard, you can improve security with the following measures:

- Select a shared key that is as long as possible and make sure it is an arbitrary combination of numbers and letters. This reduces the risk of dictionary attacks.
- Define all four keys and change them at regular intervals to avoid brute force attacks.
- If possible, disable the DHCP server running on your WLAN router. Instead, assign static IP addresses and define as small an address space as possible.
- Change the router configuration password. Default passwords for popular router models are well-known on the Internet. The network is completely open to an attacker who gains access to your router.
- Disable SSID visibility and beacons (broadcasting) on your access point.
- Position your WLAN router so that reception is fine for your own needs but does not cover your neighbor's property. Note that radio waves also propagate vertically.
- If your hardware supports this option, set your router's transmission power to match but not exceed your own needs.

pliant for Wi-Fi Alliance approval (see Figure 1).

At the time the 802.11b standard was under development, nobody was really concerned about wireless network security. Additionally, many WLAN router manufacturers disabled the security mechanisms by default – an ill-advised strategy that left network traffic totally unprotected unless the user intentionally modified the security settings.

WEP

Configurations of this kind, which, believe it or not, still exist to this day, gave anybody within WLAN range the ability to associate with the access point and use the network. To make matters worse, even if the user made an effort to enable the encryption features available with the device, the security was often ineffective. The Wired Equivalent Privacy (WEP) security system used with the 802.11b standard soon turned out to be useless. As early as 2001, experts demonstrated that WEP encryption has some serious vulnerabilities.

The WEP method uses keys with a length of 40 or 104 bits (232 bits in exceptional cases). All the devices on the network use this key. The standard lets you configure a maximum of four different keys, but it does not support dynamic changes. Additionally, each data packet includes an initialization vector (IV) with a fixed length of 24 bits.

Manufacturers of WLAN components advertise 64- or 128-bit encryption for 802.11b; however, the initialization vector is transmitted in the clear. A maximum of 17 million values is available for the vector. If it is repeated multiple times in a session and if the key does not change, attackers can calculate the key and use it to decipher messages. An attacker only needs to sniff enough data packets and run a brute force attack to compromise the key.

For a large network with high volume, it does not take long for an attacker to sniff enough packets to break the key. For a small private network, the intruder has to listen for a longer time, but special tools are available to generate traffic to the access point to speed up the process of cracking the key.

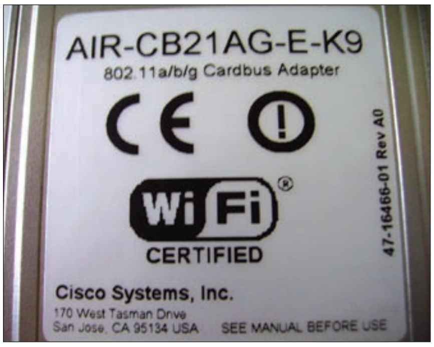
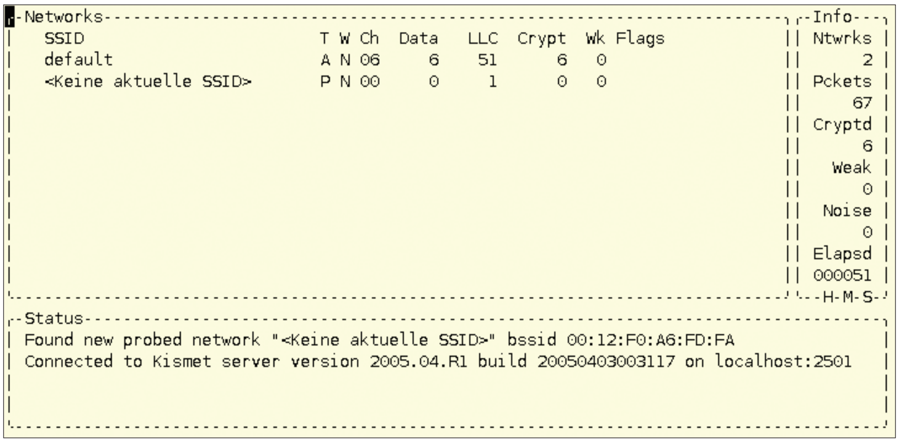


Figure 1: The WiFi logo identifies complete standards compliance.

Another way of breaking the key on a WEP-secured WLAN is to launch a dictionary attack. A dictionary attack involves the attacker trying out various keys (typically several million alternatives) until the correct key is discovered. This method is often successful, but it does take more time and more computer capacity.

Refer to the strategies in the "Tips for WEP Networks" box for raising the bar-



```
┌-Networks----------------------------------------------------------------┐ ┌-Info---┐
|   SSID                          T W Ch  Data   LLC  Crypt  Wk Flags      || Ntwrks |
|   default                       A N 06     6    51      6   0            ||      2 |
|   <Keine aktuelle SSID>         P N 00     0     1      0   0            || Pckets |
|                                                                          ||     67 |
|                                                                          || Cryptd |
|                                                                          ||      6 |
|                                                                          ||   Weak |
|                                                                          ||      0 |
|                                                                          ||  Noise |
|                                                                          ||      0 |
|                                                                          || Elapsd |
|                                                                          || 000051 |
'--------------------------------------------------------------------------' '--H-M-S-'
┌-Status---------------------------------------------------------------------------┐
| Found new probed network "<Keine aktuelle SSID>" bssid 00:12:F0:A6:FD:FA          |
| Connected to Kismet server version 2005.04.R1 build 20050403003117 on localhost:2501 |
|                                                                                   |
|                                                                                   |
'-----------------------------------------------------------------------------------'
```

Figure 2: The Kismet WiFi scanner can check your own wireless network for vulnerabilities – and discover information about the protocols used on your network.

riers for hackers. Most legacy 802.11b WEP devices are not compatible with later standards, which means that the move to improved WLAN security will almost always involve new hardware.

Interim Successor: WPA

WEP's many vulnerabilities spurred the Wi-Fi Alliance to develop an alternative, Wi-Fi Protected Access (WPA), to bridge the gap until the new 802.11i standard could deliver more robust security mechanisms. WPA is a compromise between WEP and the more recent WPA2: On one hand, it supports a new authentication method that relies on pre-shared keys, with passwords of between eight and 63 digits. On the other hand, the WPA developers kept the RC4 cipher algorithm, which is demonstrably insecure.

According to the Wi-Fi Alliance, this continued reliance on RC4 was necessary because of the technical shortcomings of access points available at the time. These devices did not have enough internal computational capacity to shift to a more secure encryption algorithm such as AES through a firmware update.

In introducing WPA, the developers modified the authentication and encryption methods to provide more security: clients use pre-shared keys or (in larger wireless LANs) a Radius server to associate with the access point. After authentication, the client and the access point negotiate an individual 128-bit key to prevent other workstations on the WLAN from sniffing the data traffic. In addition to these security improvements, WPA uses a 48-bit initialization vector. Periodic renegotiation of the key between the client and access point adds more security to the WPA standard, eliminating the possibility of an intruder launching a brute force attack against larger volumes of sniffed data packets.

State of Art

WPA2, which was introduced in 2004, makes the WLAN even more secure. The developers finally ditched legacy features of the wireless security infrastructure by replacing the insecure RC4 algorithm with the superior AES standard, for example. Atop this better foundation, the new standard incorporates the WPA authentication and encryption methods. Thanks to these improvements, attackers no longer benefit from sniffing a WLAN for hours or days and running brute force attacks against the results.

WPA2 introduces a two-part standard: The WPA2 Personal subgroup specifies a feature-reduced standard for the consumer and SOHO market. Although this variant provides all the popular basic security features, it does not support the additional benefit of authentication through a Radius server. The WPA2 Enterprise version covers the full 802.11i standard and thus supports Radius authentication.

Secure with WPA2

As of this writing, wireless networks based on WPA2 are regarded as mostly secure. Dictionary attacks on the pre-shared key are the most promising vector – assuming the attacker has enough time and computer power. Theoretically, the broadcast and multicast keys represent another vulnerability. All network nodes need to know them, and an attacker who discovers one of the keys can at least sniff the key exchange between the access point and the workstation.

Thanks to the WPA2 standard's security design, modern wireless networks now have fairly effective security. The biggest factor of uncertainty is with the user. Today, wherever an inquisitive intruder gains access to a modern WLAN infrastructure and applies enough criminal energy to access the network and cause damage, a careless access point configuration is usually the root cause. So take some time to consider your WLAN router's individual settings carefully (Figure 2).

If you want to reduce the residual risk even further, you can add software-based protection for the WLAN. If you use a tunnel, such as a VPN with IPSec, you can raise the barrier even for experienced hackers. As is often the case, the free Linux operating system, with its many built-in security components, is a perfect choice for eliminating residual risk. ■

Tips for WPA/WPA2 Networks

Better safe than sorry. As with any password authentication system, select passwords that are as long as possible and make sure they include an arbitrary combination of numbers and letters.

- Set up your WLAN router to automatically negotiate new keys with clients at regular intervals. This makes brute force attacks more difficult.
- Disable the default configuration of the DHCP server and assign static IP addresses.
- Use individual names for the SSID and ESSID.
- Disable beaconing on the router.
- If supported by your hardware, define Access Control Lists (ACLs) to query the MAC addresses of your network cards.
- Change your WLAN router's location and transmission strength so that reception is fine for your own needs, but does not cover your neighbor's property.
- In case of MIMO devices with three antennas, you should position the antennas to face away from each other to improve transmission and reception strength.
- Always use wired connections to configure your WLAN router; this prevents sniffing.