"Wireless networks: are we just leaving the stable door wide open?"

~ an examination of how companies can hit hackers hard with their own tools and techniques ~

Wireless networks are convenient and quick, but often unsecure. More and more home and business internet users are implementing wireless LAN (WLAN) without a comprehensive security framework. Never a better time then to examine once again best practice for protecting wireless networks from hacking and penetration attacks.

Hacking wireless networks and penetration testing could be seen as one and the same. Users can implement similar methods to a hacker to find weaknesses, test the resilience of their own WLAN and ensure their network is as secure as possible.

Most attacks follow the same pattern: find a network, then intercept and penetrate data packets. It's often no challenge for hackers as administrators and home users install WLAN-compatible routers and devices without adding extra levels of security. Additionally many products are made with SOHO users in mind, and come with inherent security features so that those with little technical knowledge can quickly set up their own network.

Setting up a secure foundation configuration isn't the stuff of witchcraft – just a few steps can lock out opportunistic hackers. The majority of the following configuration setups can be implemented by non-specialist administrators, for example in branch offices. When it comes to protection against targeted attacks, in-depth penetration tests should be carried out to check the resilience of a WLAN. On the whole, it's recommended that WLAN installations are executed using centrally-managed encryption policies and with additional client authentication.

Keeping passwords under wraps

One of the most used starting points for hackers in wireless networks is the service set identifier definition (SSID): Often WLAN users make the mistake of using the firm's name or their own name as the SSID – the network name. This is a fundamental thread for information for the hacker. For example this can enable a hacker to find the location of the WLAN and also provide an indication of what type of information will be available from the network. Sometimes it's also possible to detect the WLAN password from the SSID – around 30 – 40% of all passwords come from the user's personal life. Therefore a 'neutral' SSID identification should be employed so that no passwords can be traced back can be made. The WLAN password and the SSID should, of course, never be identical.

As well as an individual SSID, predefined user names and administrator passwords for access points and WLAN configurations should be modified. In many cases, equipment has a default mode using 'admin' as login and password, which hackers can take advantage of to quickly access a network. If a hacker gains administrator privileges to a wireless box, he or she can then modify the configuration to their own specification, and swiftly remove security defences and then, most importantly, hide their tracks. To prevent this, administrators should put in place another level of protection by integrating the WLAN completely with the fixed line network – any changes to the WLAN configuration can then only be made using a computer connected to the LAN. The same goes for remote management: functions that can control a unit over the internet should be deactivated.

Silent offer

WLAN boxes use what's known as 'beacon broadcasting' to transmit their SSID regularly – this is how clients can see which wireless networks are available. Deactivating beacon broadcasting creates an additional hurdle for hackers. An attacker then has to install a passive scanner to establish whether a wireless network exists at a particular location and what SSID it carries. The Kismet tool identifies the broadcast traffic from wireless networks and filters the SSID from data packets. Other hacking tools such as NetStumbler, which actively search radio networks, will fail if the SSID broadcast is switched off.

In practice, 'hobby hackers' do not search for 'invisible' WLANs without SSID broadcast. If an attacker is set on getting into a particular network, a suppressed broadcast won't stop them. And to add insult to injury, regular clients that access the network must also be configured so that they can't simply access the 'invisible' network.

Known players

The most up-to-date WLAN systems can now restrict access to recognised clients. Hardware addresses (MAC) for computers and wireless devices that can be connected to the wireless networks can found in the access control lists (ACL). Similarly, a connection path to other clients can be confirmed. MAC addresses are usually automatically logged after the initial connection with the router so that a type of 'learning phase' can help to reduce the amount of manual maintenance. In large organisations' networks, managing the ACL effectively is often seen as too laborious.

Although these measures still cannot provide total security, they do increase the network's resilience against attackers. Hackers can only access an ACL if they have convinced the access point that they are operating an authorised device. To do that, a corresponding MAC address must be recognised by the scanner, which can only be put to misuse when regular clients are absent.

As far as possible, the deployment of dynamic IP addresses for WLAN clients should be deactivated. Dynamic Host Configuration Protocol (DHCP) also makes it easier for regular users as well as hackers to get into the network. As an alternative to using fixed IP addresses, dynamic IP addresses can enable a reduction of the number of authorised computers. This makes it more difficult for hackers to get hold of a free dynamic IP.

Furthermore it should be considered that a WLAN-compatible end device can represent a back door to the network. The 'adhoc' mode connects end devices without the use of a WLAN router or access points. For regular clients the Infrastructure mode should be activated so that no additional attack points can exist. To uncover end devices with the adhoc mode activated, administrators can use WLAN sniffers like Kismet - just as a hacker would.

Encryption

Each data transmission over a WLAN needs to be protected by some form of encryption. Wired Equivalent Privacy was the original privacy for the IEEE 802.11 standard using either a 40 bit or 104 bit key for encryption. A 24 bit Initialisation vector was added giving keys of 64 and 128 bits respectively.

In 2001, it was systematically proven that WEP could be cracked with even the smallest amount of WLAN know-how and freely available hacking tools. The simplest variant of WEP with the 64 bit key can be cracked in a few seconds, the 128 bit can be cracked in less than 40 minutes.

WPA (Wi-Fi Protected Access) is a more secure encryption mechanism. The WPA protocol was developed to overcome the weaknesses of WEP and was an interim measure while the IEEE 802.11i standard was being prepared.

WPA2 implements the 802.11i standard using the Advanced Encryption Standard (AES) and also uses CCMP (Counter mode with Cipher block Chaining Message authentication Protocol).Both protocols change the key used for transmission security even whilst a connection is active.

The secrets hidden by the session keys and authentication can either be presented as Pre-Shared Keys (WPA-PSK (personal authentication), which categorises all WLAN users with the same 'password', or as a 'managed key' using a RADIUS server (enterprise authentication), which identifies a client with a digital certificate or by username/password.

Attacks on WPA and WPA2 are based on guessing or testing out passwords or pass phrases, which can provide the required access information: passwords that are too short or too simple can be uncovered through robust testing (known as brute force attacks) or clear text sentences through dictionary attacks. A minimum length of 14 characters, combining a mixture of lower and upper case letters and numbers will help prevent these kinds of attacks. Passwords cannot, however, be made up of words or parts of words from 'artificial' languages (for example, Klingon). WLAN security depends directly on the quality of the pass phrase. Nothing is more damaging than bad passwords that are derived from current events.

An alternative, or an elaboration of the network encryption is the use of virtual private networks (VPN). Protected user access doesn't depend on the WLAN device, but on a VPN server in the internal network. The communication from the client via the access point is protected by the VPN gateway, which is an interesting possibility for regional branch offices for larger enterprise, because not only the WLAN traffic but also internet data transfer to HQ are protected. If unencrypted wireless hotspots are being used, then a VPN is absolutely indispensible. VPNs protect end-to-end connections, not the WLAN itself, so it must remain cut off from other company resources. Otherwise, wireless networks can be accessed and used by non-employees - even if there's no danger of data being stolen. Implementation can, however, be hampered by incompatible VPN-client software or insufficient knowledge.

Denial of service

Because WLANs operate in an open frequency arena, they can easily be damaged by other signals. Hackers can easily do damage to a network using a jamming transmitter. An elegant method can bring what's known as 'deauthentication flooding' – deauthentication packets are used in the IEEE802.11 protocol in the normal way to split the connection to a recognised client and attach themselves to the access point instead. The weakness lies in the fact that the MAC address is checked, whether the received signal is actually coming from the registered client or not. This also works over encrypted WEP networks and deauthentication packets can be sent in an unencrypted format.

Upper limits

A further possible method to protect wireless network attacks is to use the strength and direction of the network signals. The scope of the WLAN should be kept small enough to allow all regular clients access, but will restrict the chances for attackers to target routers or access points. Ideally, the WLAN should be set up so that signals cannot be picked up outside the building. Also some SOHO systems reduce the signal limits using a corresponding function down to the smallest amount required for recognised clients. Further limiting factors include metal-framed windows and walls constructed to insulate signals as well as directional radio antennas.

And last but not least, hackers themselves often leave at least a few traces of their attempts after a successful attack on a wireless or internal network, so in general, only a minimum of administrators be given free reign of the corporate network, to help track any unusual activity.

Richard Millett, Firebrand Training.

About Firebrand Training

In our fast-changing world, learning and applying knowledge must match the industry pace. The only way to achieve this is through Accelerated Learning. The Firebrand Training pioneered this unique and innovative method of teaching IT and management programs and is the only company to offer it.

Accelerated Learning enables students to complete courses in less time (elapsed and time out of the office) than any other approach. The time saved has massive financial implications for both companies and individuals.

There are more advantages than just acquiring skills. For staff, our courses increase morale and promotion prospects; for companies, they minimise the risk of being out of date with knowledge and cut out the need for external consultants.

Firebrand Training teaches through all three learning styles organised throughout the day:

:· Visual in the morning when the brain is most receptive

:· Tactile after lunch when people need more stimulation

:· Auditory in the evening when a more relaxed atmosphere works best

Firebrand Training's instructors are cross-certified industry professionals - ranging from renowned authors to senior consultants, with extensive real-world knowledge. They combine technical expertise with a broad understanding of how technologies and methods are deployed, used and managed in business.

Accelerated Learning is the fastest, most comprehensive way of both earning your certification, and retaining the knowledge.

Call us on:	(freephone) 080 80 800 888
Email us at:	info@firebrandtraining.co.uk
Visit us online:	www.firebrandtraining.co.uk

FIREBRAND
Immerse. Accelerate. Measure.