



F.A.Q's

Is wi-fi security an issue to you? If you are utilising wireless technology on your network then it should be. For every wireless network that has been properly secured from potential attacks, there are many, many more that are not. It is all too easy for a hacker to gain access to a wireless network and cause untold damage to both your data and your reputation as a business.

The pitfalls are numerous, but the benefits of understanding the problems and then ensuring adequate security protocols are implemented will far outweigh the potential damage caused by a malicious attack. The following points should help you to understand the risks involved and how prevention is a far better solution than cure.

Problem 1: Easy Access

How easy it is to discover wireless networks?

It couldn't really be simpler!

Take any laptop or desktop computer with a wireless card attached and try looking for wireless devices within range. If you are in a busy residential or office area, you are almost certain to see a number of wireless networks in operation. This isn't necessarily a bad thing, as these devices need to broadcast their presence periodically to allow valid users to link up and use their services. However, the information needed to join a network is also the information used to launch an attack on a network.

Unless you are prepared to heavily shield the walls of your office or home to prevent signals escaping, there is no solution to this problem. In order to minimise the risk of such an attack, you should ensure you implement the strongest access controls and encryption solutions available to you. This will stop your wireless network from being used as an easy entry point into your network and ultimately into your data. Ensure firewalls are correctly deployed and use VPN's to manage sensitive connections.

Problem 2: "Rogue" Access Points

It is now far too easy for an area of your network to be turned into a wireless LAN by non-IT staff who do not understand the risks they are taking by potentially opening up your network to all and sundry. The cost and easy availability of wireless access points means that a junior manager can easily sign off the expenditure and run down to his local computer shop and set up his own wireless network.



As you can imagine, this is becoming an increasing headache for network administrators, as end users are often unaware of the great security risks they are taking. Users rarely bother to change the default settings of their wireless access points and therefore non-IT staff in large organisations are unlikely to do much better. This results in additional work for the network administrators, who have to use tools such as Net Stumbler as they wander around their building attempting to discover rogue access points.

Problem 3: Unauthorised Use of Service

It's a fact that most access points are installed with only minimal changes to their default settings. Encryption standards such as WEP (Wired Equivalent Privacy) are rarely activated, or if they have, then only the default key has been used on all the vendor's products.

Any wireless network which does not have secure encryption and access controls is usually there for the taking. If your network is breached, there are serious implications which should be considered.

Although your actual data may not have been compromised or destroyed, your bandwidth may have been used to upload and download data from external sources. As well as incurring additional charges for exceeding your bandwidth limits, you could potentially be party to illegal usage, such as e-mail spamming or downloading illegal software. This could ultimately lead to your ISP ceasing your service.

Of course, how secure your wireless network needs to be depends heavily on the type of business and network you are running. In a typical office environment, utilising mainly a wired network, access to wireless access points needs to be strictly controlled with strong authentication. If you have deployed a VPN to protect the network from wireless clients, it probably has built-in authentication already. Of course, if your business requires the need to provide wireless 'hot spots' such as in hotels and airports, the security techniques employed need to be radically different. In these circumstances, authentication is often carried out via a web browser and does not require specialised client software in order to gain access.

Problem 4: Service and Performance Constraints

Current wireless LAN technologies are limited in the speed at which they transmit data. The most common standards at present are 802.11b (which transmits at 11 Mbps) and the newer 802.11g (which transmits at 54 Mbps).



These standards are being developed all the time and there are already enhanced versions available running at much higher speeds than these.

The transmission speed is shared between all the users associated with an access point and in real terms the effective throughput is only around half of the nominal bit rate. This means that a build up of traffic through use of local applications could have a dramatic effect on the operation of the network and that an attack on the network could well result in a denial of service due to the limited resources available.

There are a number of ways which can result in wireless traffic becoming overwhelmed, such as traffic coming from the wired network transmitting at a higher rate than the radio channel can handle. An attacker launching a ping flood could potentially overwhelm not only a single access point, but several across a network. It is also possible for an attack to come from somebody not even attached to your wireless access point, but by simply broadcasting on the same space and radio channel. Even if there is no malicious attempt to attack your network, large movement of files across your network can also bring your infrastructure to a grinding halt.

There are now a number of devices on the market that can monitor and report on the performance of wireless networks. Whilst these devices do not help in defending your network from attacks, they do alert you to any such problems and also of possible heavy users within your organisation that may be monopolising the bandwidth.

Problem 5: MAC Spoofing and Session Hijacking

Traditional Ethernet wired networks and 802.11 wireless networks provide no protection against forgery of frame source addresses. In other words, data can be spoofed to appear to be sent within your network. Spoofed frames can be used to redirect and corrupt data. MAC addresses of wireless stations can also be observed and these addresses adopted for malicious transmissions.

To prevent this type of attack, technology is being developed to authenticate valid users of wireless networks. Without the correct authentication, potential attackers are denied access from the network, although this doesn't fully prevent access to the radio layer and denial of service attacks.

The standard for user authentication was first ratified in 2001. Currently, authentication can be used to validate a user before accessing the network. However additional features are currently being developed and are likely to be adopted as part of the 802.11i standard.



Spoofed frames can also be employed by attackers in active attacks, allowing access points to be exploited if there is a lack of authentication. Access points identify themselves on a network by the broadcast of beacon frames. If a station broadcasts the correct ident (SSID), it will appear to be part of the authorised network.

It is therefore possible for an attacker to appear as a genuine access point on the network, as nothing in the 802.11 standard requires an access point to prove it really is one. This could potentially lead to an attacker discovering network credentials to gain full access to the network.

Further developments in 802.1x will ensure that mutual authentication is supported. Access point will need to validate their identity before gaining access to the network and strong cryptography will be employed to maintain security over the airwaves.

Until frame authentication is fully utilised by 802.11, session hijacking will remain a problem. Until such time, additional cryptographic protocols will need to be employed on top of wireless networks.

Problem 6: Traffic Analysis and Eavesdropping

The 802.11 standard does not provide any protection for attacks on the passive monitoring of data in transit – in other words, eavesdropping. Anyone with a wireless network analyser can monitor packets of data as they are transmitted. Flaws in WEP encryption did not fully address the security of wireless networks, resulting in a number of options open to an attacker who might want to disrupt transmissions by transmitting spoof frames of data.

A number of cracking tools, such as AirSnort and WEPCrack make some WEP encryption easy to break, although the latest software and firmware updates available from the vendors have eliminated these attacks. The latest products have helped increase security and can even self-generate WEP encryption keys at regular intervals, to foil even the most persistent attacks.

Whilst vendors try and stay one step ahead of the attackers, how you protect your wireless networks is largely a question of risk management. WEP may be insufficient if your wireless LAN is being used for sensitive data and there may be a requirement for stronger cryptographic solutions such as SSH, SSL or IPSec. These technologies were designed to allow the transmission of data via public channels and are proven to give higher levels of security.



Problem 7: Higher Level Attacks

A successful attack on your wireless network can serve as a launch pad for attacks on other systems within your IT infrastructure. Once you're in, it's unlikely there will be sufficient internal controls to prevent access to all areas of your data.

It's quick and easy to deploy wireless LAN's, but it's also all too easy to therefore expose your network to attack. Other networks could then also be compromised if there is insufficient security in place. Ultimately, your own network could be used to attack networks across the world, which wouldn't win your business any awards in the popularity stakes.

Wireless networks should be treated as something outside of your usual safety net. It requires higher levels of security in order to gain access to your internal network. Whilst ensuring these principles are adhered to may be time consuming, the alternative could prove to be extremely damaging to your business.

Problem 8: Physical Security

There are strong comparisons in the development of wireless security to the challenges experienced implementing mobile phone technology. This also advanced in several stages and standards, from the initial analogue, through to digital, GSM and 3G technology.

In fact, the main threat posed to wireless users is not from attacks on your network from sophisticated hackers, but actually the likelihood of someone breaking into your car and stealing your wireless enabled laptop or PDA, complete with your passwords and encryption details.

Rather than try and break down security codes, it is often easier for a potential hacker to simply steal a device that will give them direct access to the network. This has led to telecommunication companies investing heavily in creating unique ID's on every mobile phone and sim card to deter physical theft.

Wireless technology is no different, although the security techniques are less advanced. Therefore physical security has become the main concern and the need to keep laptops and other wireless devices locked away from potential thieves has become the issue of the day.



Conclusion

The whole process of wireless LAN security may appear challenging. However, despite the pitfalls described here, it is still possible to successfully address these issues by implementing reasonable security precautions. Whilst network technologies are constantly developing and hacking techniques are becoming increasingly sophisticated, it is possible to keep on top of your security, providing your business doesn't bury its head in the sand!

The next generation of Wireless LAN's is already being driven by mobility, allowing users to move seamlessly across a network with their mobile device, without any interruption or loss of connection. However, technology hasn't yet fully embraced the facility for users to roam from one network segment to another. Developments in these areas are however sure to be just around the corner, providing even greater challenges for the network managers who have to make sense of it all.
