Wireless security

Wireless LAN Security

Wireless networks can be an effective way to extend network access. However they are not simply a continuation of a wired Local Area Network (LAN). Wired networks gain some privacy from their switches and routers and the buildings that enclose them. On a wireless network everyone can 'hear' everyone else, even in public spaces outside the building, so there are problems of privacy of communications, accountability for use and availability of service. Default installations of standard wireless equipment are unlikely to address these issues so additional steps must be taken before a wireless network is switched on.

Privacy

Wireless networks use radio broadcasts, so anyone with a wireless receiver can hear all communications on the network. Wireless transmissions can travel a surprising distance and are likely to leak through the walls of most buildings. Early designs for wireless relied on a protocol called Wired-Equivalent Privacy (WEP) that was supposed to encrypt all traffic; unfortunately this protocol has since been found to be faulty and programs can be downloaded off the web to read WEP-encrypted communications. The WPA2 encryption protocol should be used wherever possible; WPA is better than nothing, but a recent flaw in its cryptography means it should be regarded as obsolescent.

Any wireless LAN deployment that will be used for information that is not completely public must therefore use additional encryption if only to protect usernames and passwords. Encrypted Virtual Private Networks (VPNs) and application-layer encryption such as Secure Sockets Layer (SSL) are popular choices. The IEEE 802.1X protocol can provide encryption for the login process but not for subsequent traffic.

Accountability

Wireless networks not only allow outsiders to listen to traffic on an 'internal' network; they may also let them access computers on internal networks or the Internet. Such access will usually be untraceable. At most the Ethernet address of the wireless card may be recorded and this can be forged. The threat to internal systems and communications should be obvious, but uncontrolled access to the Internet can also cause problems. At least one wireless LAN provider has had their equipment seized by police investigating criminal misuse by someone who had borrowed their network and IP address.

All wireless LANs require authentication to ensure that only known users can gain access and that an audit trail exists. The authentication needed depends on the damage that could be caused. For a temporary installation that only gives access to a few systems for a few hours a secret Wi-Fi Protected Access Pre-Shared Key (WPA2-PSK) issued to legitimate users may

be sufficient. A permanent installation with access to internal and external networks should have at least the same authentication and logging as a wired network. If the main purpose of a network is to access a few protected local services then it may not be necessary to authenticate users until they try to access other, external, systems. Various means of authentication are possible, including username/password, authentication against a remote database, or a temporary account created by a local sponsor. All users, including guests, must accept the policies of the local network.

Availability

Availability may be the hardest part of wireless security to solve as the network is vulnerable at many different levels. Like any radio transmission, a wireless LAN signal can be silenced by metal or concrete, or drowned out by a stronger transmitter. The small number of separate frequencies available means that, if channel allocations and physical locations are not carefully managed, wireless LANs can even interfere with each other. Interference can also occur through misconfiguration at the network level, for example if wireless devices have the same names or if unauthorised systems advertise themselves as Dynamic Host Configuration Protocol (DHCP) servers or routers.

Finally, a wireless network is a truly shared resource and some network applications are unsuited to them. Protocols that demand excessive bandwidth will always cause problems. Some autoconfiguration protocols have been found to be a hazard on a foreign wireless LAN where their repeated broadcasts make the network unusable for others. This has been a particular issue with laptops at conferences. If the owner does not have sufficient knowledge or rights to prevent their own machine from swamping the network then there may be no alternative but to ban them from transmitting.

central allocation of frequencies, names and services, with regular surveys at all these levels supported by policies that allow problem devices to be disconnected or shut down, are the best way to achieve good availability from a wireless LAN installation.

Policy

Even organisations that do not plan to install official networks should have policies on setting up and connecting unofficial access points as these can easily become a legal and technical security hazard.

To achieve reasonable security, a wireless LAN must be well designed and be supported by policies on encryption, authentication and configuration. With these precautions, a wireless network can be as secure as a wired network.

References

The Janet website has more general advice on wireless networks [1].

Symantec publish a useful article on developing a wireless network policy: part 1 [2] and part 2 [3]

Sheffield University's wireless policy [4] has proved successful in building a consistent service across the campus

Drizzle has an extensive list of wireless security links [5]

Janet has a factsheet on connecting wired and wireless networks [6]

Links
[1] https://community.ja.net/library/advisory-services/wireless-technology-advisory-service
[2] http://www.symantec.com/connect/articles/wireless-policy-development-part-one
[3] http://www.symantec.com/connect/articles/wireless-policy-development-part-two
[4] http://www.shef.ac.uk/cics/policies/wireless
[5] http://www.drizzle.com/~aboba/IEEE/
[6] https://community.ja.net/library/advisory-services/connecting-wired-and-wireless-networks