The truth about Wireless LAN security

WLAN

The Truth about Wireless LAN Security

Swisscom Reprotechnique

By using wireless LANs (Local Area Networks), without taking proper security measures, companies leave their networks vulnerable to even relatively unsophisticated hackers using readily available, inexpensive equipment. And a security breach to the network is potentially a huge problem for any company.

Once in, hackers can gain access to corporate passwords, log on to servers and steal information, take over the corporate web site or even shut down the entire network.

STEVE WYLIE

Why does the corporate fortress mentality, which is evident in the physical building and on wired networks, not extend to wireless systems? The answer may be simple ignorance of what is available in terms of wireless security – a naïve assumption that the signals do not carry beyond the company's walls, or an instinctive head-in-the-sand idea that if you cannot see the information, you can not steal it.
Perhaps the most compelling message from the providers of these wireless security solutions is that it does not have to be this way – using a wireless LAN does not mean companies have to trade security for wireless convenience. It does mean that they have to use adequate security precautions.

WEP alone may not be enough

The most basic level of security for wireless LANs is the Wired Equivalent Privacy, or WEP, which is a standard feature on all Wi-Fi certified wireless LANs. WEP, which was created by the Institute of Electrical and Electronics Engineers (IEEE), is designed to (a) provide basic security, (b) prevent causal eavesdropping and (c) protect the network by encrypting all of the data that is sent wirelessly with an RC4 encryption algorithm based 40-bit shared key encryption.
In addition to designing a robust security solution, avoiding simple mistakes can be quite prudent. Avoiding mistakes, such as failing to turn on WEP, setting the access point inside the firewall, using the default WEP key and not changing the encryption key on a periodic basis, can by itself enhance the level of your wireless LAN security.
In theory, WEP keys are essentially shared-secret passwords that allow users to decode the encrypted data that travels on the wireless network. In practice, hackers can gain access to the keys by sitting outside the company building and capturing a stream of encrypted data on their laptops and decoding it using special software that can be found on the Internet. This process, a sort of reverse decoding, reveals the key to hackers and gives them access to the company's network.
The encryption key algorithm is not inherently flawed, although poor key management can make it quite vulnerable to hacking. Often system administrators will assign just one key for the entire company, meaning once a hacker gets the key, the hacker potentially can have access to all of the company's proprietary information and network resources.
Or the administrator will give every user a different key, but make them static by never changing them. Either way, once hackers get access, they can always retain unauthorised access in a static and shared key environment. Manual key management can be easily administered in smaller networks that are tightly managed. However, it can become a monumental and cumbersome task as the number of wireless users grow, often leading to negligence on the part of the system administrator.

Better Security through dynamic Key Management

Work is currently underway on the standards front to secure against the known vulnerabilities of WEP. Efforts are being undertaken by both WECA, as well as IEEE's Task Group i (TGi), to offer enhancements to WEP. Specifications are expected to be published shortly, and is expected to subsequently become part of the Wi-Fi certification probably by the end of 2002.
While this enhancement activity is ongoing on the standards front, 3Com is also actively engaged in giving customers the confidence to implement wireless on a broad scale. Specifically,

3Com is addressing the key management and authentication requirements through a capability called Dynamic Security Link.
When a 3Com wireless access point is used in conjunction with 3Com wireless clients, Dynamic Security Link automatically generates a brand new 128-bit encryption key that is unique to each user and to each networking session. This provides a much higher level of security than static shared-key schemes, and frees users from the hassle of manually entering confusing keys. This guarantees that each user has a unique key that is constantly changed, so even if a hacker does break the encryption and gain access to the network, that hacker's key will only work for a few hours, limiting potential damage.
For additional security, Dynamic Security Link also enables user authentication, requiring all users to log in with a name and password at each session. This user-based authentication capability offers an enhanced level of security and management compared to a device MAC-address based authentication scheme. The device MAC-address based schemes are particularly vulnerable to loss and theft of the device, prompting a change to the MAC-address database maintained inside each network access point each time such an instance takes place.
Another advantage of Dynamic Security Link is that the automated and dynamic key management capability is implemented right from the access point itself, so the solution does not require any additional servers or other infrastructure. This type of wireless security deployment makes it ideal for a small business that can not afford a large investment for wireless LAN security, and as well makes it an ideal solution for enterprises that handle security in a decentralised manner.

Bigger Networks need more Security
Security on larger wireless LAN networks needs similar types of security capabilities as Dynamic Security Link – automatically changing the keys – but also needs to extend well beyond it, due to large numbers of users and more complicated security requirements. Larger installations usually need a more robust encryption key management technology, scalable authentication mechanisms and centralised user management across the network infrastructure, which cannot be stored in the limited memory of a wireless LAN access point.
While the security in the WEP and Dynamic Security Link solutions are localized – managed within the WLAN access points – a larger system that must accommodate thousands of users and state-of-the-art encryption and authentication usually requires a security solution that is administered from a central location. Usually these systems are managed by a RADIUS (Remote Authenticated Dial-In User Service) infrastructure. RADIUS provides for a centralised management and administration of large number of users that are authorised to access resources on the network.
Supporting RADIUS with 802.1x, the standard for network login within both the wired Ethernet network and the wireless 802.11 network, further enhances the user authentication capability for your wireless enterprise network.
Given the mixed infrastructure platform nature of today's networks and the range of Windows operating systems that are deployed within the enterprise, the 802.1x capability delivers a range of superior and scalable wireless security capabilities. Among the technical functionality offered are the following:
– 802.1x network login support for legacy Windows operating systems
– Universal Client Certificate to enable certificate-based mutual authentication
– Protected key management with support for RADIUS-EAP-TLS protocol
– Integration into existing RADIUS environments that support MD-5 protocol
– Support for multiple authentication schemes with EAP protocol

This article has been written as part of a series of articles for Enterprise Wireless Technology 2002 being held at Olympia in London from October 2nd to 3rd, www.enterprisewireless.co.uk. 3Com were an exhibitor at Enterprise Wireless Technology 2002.

Whatever the level and scope of wireless security called for by the network infrastructure, a layered solution then can be customised to suit the specific wireless security requirements. Wireless security solutions can extend all the way from standard-based basic WEP to security administered within the access point, to robust and scalable security that is centrally managed and extend from the wired infrastructure to the wireless infrastructure. Rather than something that can just be slapped onto the network, security needs to be integrated into the fabric of the business. [3, 4]

***Steve Wylie**, Wireless Sales Manager for 3Com, UK*

Summary

WLAN

Firmen, die auf Wireless LANs setzen, ohne die gebührenden Sicherheitsmassnahmen zu ergreifen, setzen ihr Netz der Gefahr aus, dass es von Hackern geknackt wird. Und dies selbst mit Geräten, die leicht zu beschaffen sind und wenig Geld kosten. Dieser Artikel bespricht die bekanntesten Sicherheitstechniken von der elementarsten zur raffiniertesten und weist nach, dass niemand die Sicherheit den Vorteilen der Funktechnik zu opfern braucht. Es gibt Sicherheitstools, die Frage ist nur, was sie leisten und wie man sie am besten nutzt.