INDIA'S ONLY IT BUSINESS WEEKLY!
EXPRESS Computer

8 August 2005 – www.expresscomputeronline.com

Securing wireless network access

The author is CTO and VP, Technology, at Pronto Networks Inc.
He can be reached at rpr@prontonetworks.com

Wired or wireless, security will always be an issue, and there will always be newer methods of hacking a network. Fortunately, newer solutions will also be continuously developed to secure access.

In any network, security management consists of controlling, monitoring and managing access to the network and the application servers connected to it. This includes managing user credentials (username/ passwords), and analyzing security or access logs. Network administrators as well as equipment vendors implement these security practices. Despite this, the nagging question from the end user's perspective remains: Is access to the network secure? This question is regardless of whether the network is wired or wireless. The issue takes on a bigger dimension when the network in question is wireless. Generally, end-users perceive the wired network—for example a DSL/cable connection at home, or a wired office network—to be secure, which may not necessarily be true. This concern is especially so in the case of 802.11a/b/g WLANs and not for cellular data networks such as GPRS, W-CDMA, and the like. Here are some insights into the issue and the possible solutions.

A wireless LAN typically consists of one or more Access Points (APs) connected to a wired LAN, and users associate to the APs by selecting the right Service Set Identifier (SSID). A WLAN provides mobility to users. Its deployments are increasing more rapidly than that of any other IT technology, and this rise is happening in both home and office environments.

At the enterprise-level, wireless technology is complementing wired connectivity partly due to cost issues and partly because of convenience. Still, there is inadequate acceptance in enterprises primarily because of security concerns and inadequate training of IT staff. In companies where the IT department does not encourage or support the WLANs, office workers (un) scrupulously put APs in the office without the knowledge of the IT department. Such an AP is called a rogue AP, and it is likely to jeopardize network security as it gives unhindered access to the corporate network or servers, even to those who are physically outside the office. This issue gets amplified when these APs are used with their default settings.

In general, corporate wired networks are considered to be secure because of physical access security. There is no connectivity (network access point) available outside an office building. When a visitor enters the office building once the office security grants him physical access, the office network is wide open for access. The visitor can connect his notebook/device to any point in the office and get free access to the network. In these cases, the responsibility of security is entrusted with the office reception or security guard, and is often weak. Thus it becomes quite a daunting task for an IT department to ensure that enterprise networks remain secure from unauthorized access. They need to use the right tools, environment, and define and enforce policies.

Securing the network

The enterprise network can be made secure by using the 802.1x mechanism. This ensures that each user needs to be authenticated, and simple physical access to the office building does not give free access to the network. Deploying 802.1x would require upgrading the existing switches to those with 802.1x authenticator capabilities, installing and configuring supplicants on user devices (PCs, notebooks, servers, etc), and deploying a 802.1x authentication server. The installation and configuration of user devices become a big task especially with respect to installing certificates and user credentials to make it seamless for the corporate user. The complexity increases with the choice of EAP authentication protocols and support available in devices and authentication servers. Not all the implementations will support all the EAP protocols, for instance, EAP-TLS, EAP-TTLS, EAP-PEAP and EAP-LEAP. Alternatively, one can use MAC address-based filtering to allow / deny users or browser-based authentication using a corporate authentication server such as a LDAP server or SQL repository.

The enterprise environment is still a controlled one as the IT department has full control on what users can and cannot do, and thus implements a uniform access policy and enforces compliance with it. The environment in public access hotspots requires a different thinking altogether. In public hotspots, which are usually wireless, one has no control over user devices and no restrictions can be imposed. The service provider needs to support all kinds of users, and cannot demand any configuration change. The 802.1x protocol is too complex even for the enterprise, and, therefore, will take time before it gains acceptance in public hotspots. Public access is still primarily geared towards browser-based authentication. Users typically buy prepaid cards and provide prepaid PIN numbers to authenticate themselves and access the network.

When connecting wirelessly, users can be authenticated using either browser-based authentication in public hotspots (and MAC-based filtering) or any authentication method in the corporate network. These are typically used for authenticating users and then giving full-unsecured access after authentication, i.e. without any encryption. Since the access medium is wireless, it is open for prying, and anyone with a good sniffer tool can capture a user's entire network traffic. This can be used to capture sensitive and confidential user information. Wireless access is therefore considered extremely insecure. It is a different matter that the same thing can be done with wired connectivity, for example, by any misbehaving corporate staff or service provider staff in case of DSL/cable connectivity. In the latter case, access to wired media is physically limited to the service provider staff, and hence is considered secure in general, and users are not too concerned about it. We will therefore focus only on wireless access.

The HTTPS protocol

If a user is using a browser to access any Web site using HTTPS, say for example www.icicibank.com, one does not have to worry at all. The HTTPS protocol ensures that all the traffic is encrypted and cannot be broken (assuming it is using 128-bit encryption). It is identified by the lock symbol in the status bar of the browser. Further, it is hacker-proof even from 'man in the middle' attacks. The HTTPS protocol authenticates the server, i.e. verifies that the server is actually what it claims to be. For example, someone can sabotage the network (change the DNS servers to point to some rogue servers) to resolve www.icicibank.com to the saboteur's own IP address, but it cannot get the server certificate for www.icicibank.com and has to install its own private certificate. When a server is configured with its own certificate, then the browser will detect it and caution the user with a pop-up warning about the server credentials; the user should make an intelligent decision at this point. In general, it is recommended that such access should be denied and connection aborted unless the user verifies the server.

VPN, the other option

When users are not using HTTPS, for example when accessing www.yahoo.com or using a POP account for downloading mail, then such communication happens in clear text which can be easily snooped. Thus, if a user does not use some kind of encryption mechanism, information is vulnerable. WEP (Wired Equivalent Privacy) is known to be quite weak and hence is not worth discussing. The burden of securing the communication lies with the user since there is no corporation here to manage security. In such cases, a user has a few choices—set up a Virtual Private Network (VPN) between the notebook and the server being accessed, set up a VPN between the notebook (or PC) and the access point, and use other security mechanisms such as SSH-based tunneling and 802.11i. Each mechanism has its pros and cons. Microsoft Windows has a built-in VPN client and no extra installation is required.

In the first case, the user can set up a VPN tunnel between the notebook and corporate server. This encrypts the entire traffic between the user and corporate network. By default, all Internet traffic (for instance, accessing yahoo.com) also goes via the corporate network, which is subject to corporate policies. If a user chooses to use the local access point gateway for non-corporate traffic, then that traffic will not be encrypted and thus is not secure. Hence this option is recommended only if the user wants to access the corporate network, or if the corporate network enforces the use of VPN, in which case a user has no choice. In the second case, VPN will be set up between the notebook and AP; the entire traffic up to the AP will be encrypted, and therefore will be safe. However, traffic from the AP to the Internet will be on a wired network, and will be as safe as in the case of using DSL/cable at home or corporate connectivity to the Internet. In this case, we are using Wi-Fi Protected Access to provide secure network access till the AP (like the option above), and after the AP, it is the usual unencrypted traffic to the Internet.

In short, whether wired or wireless, security will always be an issue, and there will be newer methods of hacking the network access. At the same time, solutions will be continuously developed to secure the access, and the end-user needs to be aware of the pros and cons of these before choosing a particular solution.