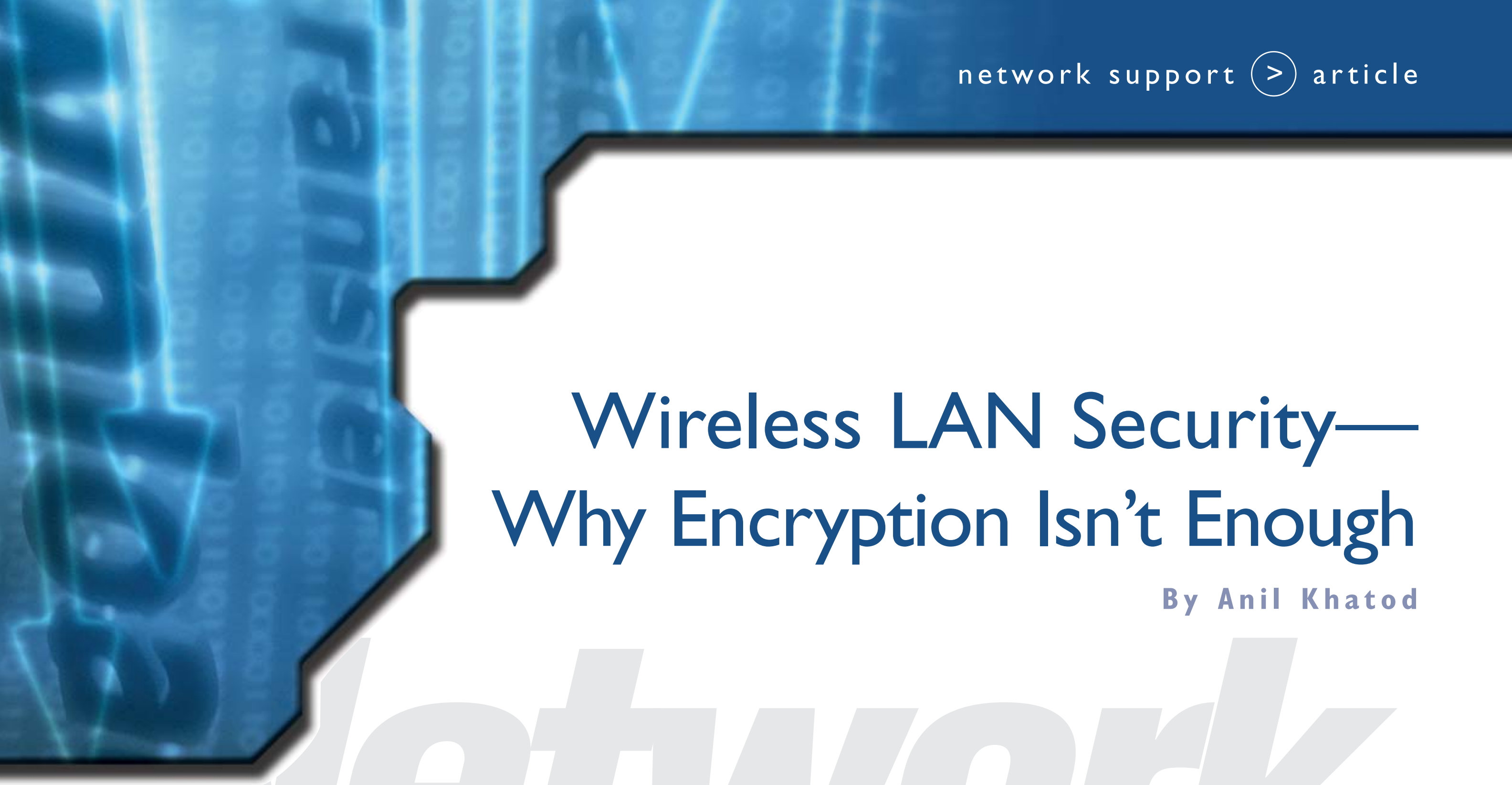

Wireless LAN Security—Why Encryption Isn't Enough

By Anil Khatod

THE benefits of 802.11 wireless LAN connections are easy to see from the mobility of un-tethered workers connecting to the network from a conference room, retailers easily running cash registers throughout a store, or manufacturers wirelessly connecting operations throughout a plant. However, the risks of wireless LANs are still being identified as hackers become more familiar with the technology and develop more creative ways to compromise wireless security.

Many feel that by encrypting the information transmitted through the air, they are utilizing an affordable, easy answer to wireless security. While encryption is certainly a critical aspect of securing WLANs, it is not the end-all, be-all solution and there are many other risks to wireless networks, including:

Ad hoc networks—Peer-to-peer wireless networking between laptops without an access point opens up a laptop to be directly attacked and used as a conduit to the network.

Policy violations—Authorized users who violate network policies against rogue access points, file sharing, and turning off security measures circumvent your investment in network security.

Identity theft—Intruders can pick off Service Set Identifiers (SSIDs) and Media Access Control (MAC) addresses to steal the identity of an authorized user.

Man-in-the-Middle attacks—Hackers can force a rogue station between an authorized station and an access point where all traffic between the authorized station and access point is routed through the rogue station.

Denial-of-Service—Outsiders who cannot gain access to a WLAN can none the less pose security threats by jamming or flooding the airwaves with static noise that causes WLAN signals to collide or simply force stations to continuously disconnect from access points.

Securing the Wireless Network

To ensure a secure network, security conscious enterprises must fortify their wireless LANs with a *layered approach* to security. This article will cover some of these methods.

LOCK DOWN ALL ACCESS POINTS AND STATIONS

The first step of wireless LAN security involves the basics of configuring all access points to implement the best practices of wireless LAN security.

Enterprises should change the default Service Set Identifiers (SSIDs), which are essentially the names of each access point. The SSIDs should be changed to names that are meaningless to outsiders. An SSID of "CEO Office" or "East Cash Register" only calls attention to valuable information that a hacker would like to get into.

Enterprises should also configure access points to disable the broadcast mode where the access point constantly broadcasts its SSID as a beacon in search for stations with which to connect. By turning this default feature off, stations must know the SSID in order to connect to the access point.

Most enterprise-class access points allow you to limit which stations can connect to it based on filtering of MAC addresses of authorized stations providing basic control over which stations can connect to your network. Larger enterprises with more complex wireless LANs that allow hundreds of stations to roam between access points may require more complex filtering from remote authentication dial-in service (RADIUS) servers.

In addition, to eliminate the threat of intruders connecting to your wireless LAN from the parking lot or the floor above you where connection speeds will be greatly reduced, access points should be configured to not allow the slower connection speeds.

ENCRYPTION & AUTHENTICATION

In 2001, researchers and hackers demonstrated their ability to crack Wired Equivalency Policy (WEP), the standard encryption for 802.11 wireless LANs. Soon after, hackers published freeware tools, such as WEPCrack, which allow anyone to crack the encryption after observing enough traffic over the network to figure out the encryption "key." WEP can be configured with a variety of key lengths, the longer of which can be harder to crack. While the longer key lengths take longer to crack, they remain vulnerable.

With authentication vulnerabilities stemming from WEP, the wireless LAN standards group introduced 802.1x as strengthened authentication for all 802.11 networks. However, 802.1x also has proven to be vulnerable to hackers.

Because these encryption and authentication standards are vulnerable, stronger encryption and authentication methods should be deployed to more completely secure a wireless LAN. The recently ratified 802.11i has accounted for weaknesses in previous protocols but is still subject to vulnerabilities if improperly implemented or bypassed by rogue devices.

SET & ENFORCE WIRELESS LAN POLICIES

Every enterprise network needs a policy for uses and security. Wireless LANs are no different. While policies will vary based on individual security and management requirements of each wireless LAN, a thorough policy—and enforcement of the policy—can protect an enterprise from unnecessary security breaches and performance degradation.

Wireless LAN policies should begin with the basics of forbidding unauthorized access points and ad hoc networks that can circumvent network security. Because many security features are controlled on the access points and stations, policies should be in place to forbid the reconfiguration of access points and wireless LAN cards to alter these features.

24X7 RF MONITORING

The overarching layer of security organizations need to adopt to secure their WLAN is 24x7 RF Monitoring, which includes intrusion detection and protection and rogue access identification for the entire organization.

DISCOVERY OF ROGUE DEVICES & VULNERABILITIES

Because a simple wireless LAN can be easily installed by attaching an access point to a wired network and a wireless LAN card to a laptop, employees are deploying unauthorized WLANs when IT departments are slow to adopt the new technology. These rogue access points generally lack standard security and thus circumvent an enterprise's investment in network security.

The same insecurity can come from network vulnerabilities originating from improperly configured wireless LANs. Upon a power surge or after a power failure, some access points restart in their default modes that do not include encryption, authentication, or other security measures with which they were configured.

Neighboring wireless LANs located in the same vicinity as your wireless LAN also pose risks of the neighboring stations accessing your network and interfering on wireless channel.

INTRUSION DETECTION & PROTECTION

Security mangers rely on intrusion detection and protection to ensure that all components of 802.11 wireless LANs are secure and protected from wireless threats and attacks. While many organizations have already deployed intrusion detection systems for their wired networks, only a wireless LAN-focused intrusion detection system can protect your network from attacks in the airwaves before the traffic reaches the wired network.

As wireless LANs become further engrained in the business landscape, it is critical to consider their security a top priority. A layered approach is the only way to fully secure a network. Locking down devices and communication between devices is a start; however, organizations must also have visibility into their wireless network to understand where breaches are occurring. To achieve this, 24x7 monitoring of the air space is required to enable safe deployment of wireless LANs.

Anil Khatod is president and CEO of AirDefense, the thought leader and innovator of 24x7 wireless network security and operational support solutions.