



White Paper

Securing Wireless Enterprise Networks

March 2004

Table of Contents

Mobility, Ubiquity, Security – the reality of Wireless LANs.....	3
Protecting your organization and its critical information – The basics	3
Protecting your organization and its critical information – The next generation	4
You’re safe, right?	4
Four Common Vulnerabilities	4
The Cost of Wireless Vulnerabilities.....	5
How can I avoid these threats?.....	6
Location is the key to Prevention	6
Approaches to determining location of wireless devices	7
Key Benefits of Location.....	8
Summary.....	9

Mobility, Ubiquity, Security – the reality of Wireless LANs

Like it or not, wireless LANs (WLANs) are everywhere. Despite tight budgets for enterprise information technology spending, WLAN spending and adoption continues to grow at a rapid pace. Recent reports show that at the end of 2003, over 2 million wireless access points are in use by over 1 million enterprises in the United States. Even if your organization has not formally adopted 802.11 technologies and networks, it is likely that your employees, neighbors, business partners and vendors have already deployed WLANs that put your information security in jeopardy.

Wireless LANs (WLANs) will be the largest growing wireless security problem faced by enterprises through 2008.” (Gartner Group).

Wi-Fi hotspots continue to sprout up in retail shops and cafes in both rural and urban areas. The number of Wi-Fi hotspots doubled in 2003 to nearly 11,000 across the U.S. according to Pyramid Research with the pace of deployments to increase throughout 2004. Additionally, wireless access points are increasingly installed on delivery trucks. Since 802.11 traffic knows no boundaries, these signals leak into your facilities and have the potential to touch anyone with a wireless card.

Centrino-based laptops are flying off the shelves as users crave the painless setup and longer battery life. According to In-Stat/MDR, more than 16 million notebook PCs with embedded Wi-Fi have shipped to businesses in 2003 alone. The Gartner Group forecasts “90% of the laptop PCs are expected to be WLAN-equipped by 2005.”

When a user turns on a laptop with a built-in Centrino chip, that computer automatically creates a WLAN, instantly emitting an 802.11 signal. At the same time, Windows XP includes the ability to detect and connect to 802.11 networks automatically. Other readily available tools make it very easy to sniff out and snoop 802.11 traffic.

Recent research by the Gartner Group warned that 30% of enterprises using wireless LANs would experience serious security exposures before the end of the year.

Protecting your organization and its critical information – The basics

The fundamental challenge of Wi-Fi is that you cannot control where 802.11 traffic goes. Wireless networks typically cover a 300-foot radius, signals can bleed out through brick and glass to the hallway, up and down floors, out to the sidewalk, and even to the parking lot across the street. For the first time in computing history, you don't know where your device or user is. And because you don't know where that user is, you also don't know who that user is.

Over the last two years, dozens of sources have outlined best practices for deploying a wireless LAN. A few of the most commonly cited recommendations are for organizations to:

- Change the factory defaults on your devices – especially administrator credentials
- Configure your access points to not broadcast ESSIDs
- Implement encryption such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA)
- Use MAC Lists to identify the valid clients that can associate to your access points

While these practices will generally keep out neighbors and casual freeloaders, they do nothing to slow down a determined intruder. Spoofing MAC addresses and breaking WEP and WPA are straightforward exercises for any hacker.

Protecting your organization and its critical information – The next generation

After organizations meet the basic requirements for wireless LAN security, the next level of protection typically requires investment in new switch and AP hardware, additional authentication server software, as well as manpower. Naturally, the cost of implementation and ongoing administration increase as the sophistication and reliability of encryption and authentication methods improve. Also, organizations have to make difficult choices between standards based approaches and vendor developed proprietary approaches.

So far, history has shown that vendor agnostic, standards-based encryption methods fall short. Techniques for breaking both Wired Equivalent Privacy (WEP) and the first version of Wi-Fi Protected Access (WPA) were identified and published only weeks after those standards were codified. The next generation of encryption standards are being developed but they often take too long to develop and require time for vendors to deliver devices that support the standard. In fact it has taken months for the IEEE task force to release the latest draft of the 802.11i specification for review by the engineering community. At this point, it is already several months behind schedule and device vendors have not yet begun to seriously develop 802.11i compliant devices.

In attempts to provide alternatives, several vendors have delivered their own proprietary approaches such as Cisco's Lightweight Extensible Authentication Protocol (LEAP) and Protected Extensible Authentication Protocol (PEAP) co-developed by Cisco, Microsoft Corp. and RSA Security Inc. LEAP has been shown to be vulnerable to straightforward dictionary attacks. While much harder to break, PEAP can be expensive to implement and difficult to administer.

You're safe, right?

Wrong. Even with strong encryption and authentication solutions, your information is still at risk. The most disturbing news is that the most common holes in your security are often created by un-knowing and well-intended employees.

Keep in mind that if your organization has not yet implemented a wireless LAN, you are not immune to these threats. They can, and often do, exist long before enterprise IT has formally begun deployment of wireless technologies.

Four Common Vulnerabilities

Open doors to your secure building.

- **Rogue Access Points.** Perhaps the most common security breach in an enterprise setting is when an employee or hacker plugs an off-the-shelf access point into an open wired network port. This set-up broadcasts corporate network access — not to mention mission-critical data or resources — to anyone with an 802.11 device, authorized or unauthorized. In most cases, the employee doesn't understand the

security implications. They're merely looking to enjoy the benefits of mobility while remaining connected to the network.

- **Ad Hoc Mode.** Ad hoc mode can be handy for spontaneously creating a WLAN. But although establishing an ad hoc network is great for smaller, peer-to-peer groups, it poses security problems. When an employee sets his laptop's network card into ad hoc mode, he also turns his computer into a gateway to the rest of the network they've connected to. Worse, it is easy for a user to be unaware that his network card is in ad hoc mode. Regardless of whether ad hoc mode is chosen deliberately or accidentally, any casual network snooper or hacker can connect to the corporate network via an employee's ad hoc mode network card.

Both of these scenarios (and other closely related issues such as Soft-AP configurations) pose enormous risks because they bypass all the investments you've made in encryption and authentication schemes. This means that any one with a wireless device can connect to your network without authenticating at all. They can also detect the unencrypted traffic to steal passwords so they can attack other elements of your security infrastructure.

Doors to Neighboring Devices – Accidental AND not-so-accidental associations

- **Accidental Associations.** With the proliferation of wireless LANs, it is very likely that your employees' wireless devices are within range of neighboring access points. When an employee connects her laptop to a wired network, and her wireless connection connects with the access point at the business across the street, network security is at risk. Using basic system utilities in Linux or Windows XP, the intruder can bridge the connection between the laptop and the corporate network. The result is that the neighboring business can easily log on to the employee's laptop and get a direct connection to the corporate network and your information. Or maybe your employees are breaching a neighbors network. This is a legal nightmare.
- **Connection hijacking:** Similar to neighborhood nuisance/accidental associations, connection hijacking is a more purposeful and malicious threat. A hijacker plugs an access point into his laptop, perhaps even configures it to match your ESSID with a spoofed MAC address matching a valid access point. The hijacker's access point has Dynamic Host Configuration Protocol bridging but no Wired Equivalent Privacy (WEP) capabilities turned on. Unsuspectingly, users on the wired network connect wirelessly to this fake access point, thus giving the hijacker access to their systems as well as to the wired network to which they're connected.

These four simple examples illustrate how well intended and often un-witting employees, open up gaping holes in the extensive and expensive security measures that your organization has implemented.

The Cost of Wireless Vulnerabilities

Consider the possibility of someone stealing your corporate information. The breadth of valuable data available via your network is enormous: payroll, HR, product plans, personal customer information, emails, financial forecasts, partner agreements, medical records. The list goes on and on.

The potential cost of these security holes is huge. The source of these threats range from freeloaders who eat up bandwidth and decrease the level of service, to employees who stumble across interesting files in neighboring networks, to amateur snoopers poking around readily available folders for interesting information, to skilled hackers intent on causing substantial damage.

Hackers generally have three goals:

- opportunistically steal corporate information,
- bring your network down, or
- use your network to attack others networks.

Hackers use an array of attacks to get on your network. Those attacks all boil down to systematically disabling or defeating the authentication and encryption systems giving the attacker access to the network and your corporate information. The four security holes, described above, make a hacker's job very easy.

How can I avoid these threats?

- **Education and process.** In each of these cases, IT personnel and corporate security analysts can implement processes and company-wide education to minimize security risks. The first step is to educate your employees about the risks involved with buying and installing their own access points. The second step is to teach wireless users how to turn off ad-hoc mode and avoid logging into unauthorized wireless LANs. However, this is minimally effective because the software does not readily provide users the information they need to avoid these threats.
- **Detection.** The next step is to detect security holes and breaches so that you can resolve them. Wireless sniffers can help you monitor and test your network airspace. Handheld sniffers only provide limited protection (though the IT and security team will be more physically fit from all the extra walking they will be doing). Passive sensors provide 24x7 coverage, but are plagued by "false positives" due to the vast number of wireless clients and access points that are both inside and outside your facility (for example every time a delivery truck drives by).
- **Prevention.** The real goal is to not just detect potential threats and intrusions but to prevent them in the first place – especially before they occur. By preventing intrusions in the first place, the number of potential threats that must be investigated is dramatically reduced. But how can these be prevented? Control.

Location is the key to Prevention

The common element in each of the threats described above is that unauthorized users are able to access your network. Interestingly, those unauthorized users are almost always not in your building. Ironically, you likely have security procedures already in place to physically keep strangers out of your building in the first place. But how do you keep your wireless traffic inside your building and keep other wireless networks out of your building?

One suggestion often made is to deploy specialized directional antennae and adjust broadcast strength on AP's to reduce the leakage of your RF traffic. But these recommendations do not address any of the threats described above – for example, rogue access points that are not configured by your IT team and neighboring wireless LANs that leak into your facilities.

Since it is impossible to control where RF traffic goes, it is imperative to control access to that RF traffic based on where the wireless device is – inside or outside your facility.

The real challenge is to provide a way to accurately determine the physical location of wireless devices and then provide detection and authentication mechanisms that consider the location of wireless devices before allowing users to access the wireless network.

Approaches to determining location of wireless devices

There are three generally available methods for locating wireless devices.

Nearest Access Point. The simplest and least accurate location methods determines the AP that is closest to the device by monitoring signal strength. Given that APs have typical coverage areas with a 50-foot radius including up and down, this level of granularity will point you toward the likely area within 7,500 square feet on multiple floors. This does not provide sufficient granularity to determine if devices are inside or outside your facility. Nearest AP location tracking provides no security.

Triangulation or Trilateration. The idea behind trilateration is that a network of sensors (either access points or passive radios) detect signals from a wireless device. The sensors each report the signal strength of the wireless device. Then a distance from each sensor is determined by making an assumption that a device with a given signal strength is a certain distance from a sensor based on circular coverage maps. By specifying the location of the sensors, a set of distance measurements from each sensor are estimated. These estimates are combined to identify points of intersection around each sensor to estimate the location of the wireless device. The areas with the most intersection points is presumed to be the area of the wireless device.

With RF signals that radiate in a uniform circle from all devices, the trilateration algorithm has an error rate of plus or minus 20 feet in any direction so now you can narrow location down to within 2 floors. This is certainly better than Nearest Access Point, but still not sufficient to determine if devices are inside or outside.

Further, trilateration suffers from significant problems that dramatically reduce the accuracy of its location algorithm. Trilateration assumes that RF traffic is very uniform. Because of the short wavelength of 802.11 signals, trilateration is seriously error prone due to a wide range of environmental issues from buildings, device interference, and even humans. These environmental factors cause four problems with trilateration:

- **Attenuation.** When objects affect the RF signal by reducing the signal strength. For example, walls, glass, and other common building structures reduce the signal strength of an RF signal as it passes through that object. This prevents any RF signal from emanating from a device in a uniform radial pattern. The actual coverage map for any wireless device is rarely a perfect circle.
- **Occlusion.** When objects completely block an RF signal, a given sensor may not detect a wireless device at all even though it is within range and maybe very close to the sensor.
- **Reflection.** When an RF signal reflects off of objects (walls, projector screens, desks), its path to a sensor is longer than expected and the resulting signal strength will be lower.
- **Multi-path.** When an RF signal is sent, it can follow multiple paths before arriving at a sensor. If the signal does not take the most direct path to the sensor, the sensor will indicate a lower signal strength making the wireless device appear much farther from the sensor than it really is.

Pattern Matching. The most accurate and most complex method of location tracking is RF pattern matching. RF pattern matching is different from nearest AP and trilateration. Rather than being negatively impacted by the unpredictable behaviors of RF traffic, RF pattern matching considers the real-life behavior of RF signals and factors in attenuation, occlusion, reflection, and multi-path effects when determining device location.

RF pattern matching systems define RF signatures that represent how RF signals sound at different points in the physical space. Then the RF signatures are associated with human defined locations such as front conference room, hallway, or parking lot. Physical locations correlate to the RF signatures that devices exhibit when in those locations.

Sensors listen for the RF signals from wireless devices. The sensors receive data that has followed multiple possible paths and also has been attenuated, occluded, and reflected by objects in the area. Each sensor transmits its data to a pattern matching system that matches the collection of sensor data to a library of RF signatures. A match is found and the system identifies the associated physical location for the wireless device.

RF Pattern matching has accuracy within 10 feet. This level of granularity enables location tracking to specific offices, rooms, or cubicles. More importantly, the features of RF pattern matching enable highly accurate determination of locations inside vs. outside your facility.

Humans are not GPS devices

An additional note: a classic flaw of most location tracking systems is that they are oriented to describe location in X, Y, Z coordinates. Unfortunately, humans do not think about location as "ten feet from the east wall and twenty feet from the south wall." Instead humans think of that location as "the boardroom" or "the third floor lobby" or "the Main Street sidewalk." Using RF Pattern Matching, the location algorithm accurately maps RF space to the physical space.

Key Benefits of Location

With an accurate determination of the physical location of any wireless device, it is now possible to revisit the assumptions about wireless security. Thinking again about the most inexpensive, most common, and unfortunately also the most dangerous wireless threats to your LAN, how can accurate location tracking solve these problems?

Each of the threats described in this paper ultimately involve unauthorized users outside your facility accessing your network and stealing your information or attacking your network or others' networks. If you can determine where a wireless device is when it is accessing any wireless network, you can significantly reduce the risk when Rogue APs and Ad-hoc networks appear.

- **Keep outsiders off of your network** and away from your information. Using location based authentication, which defines not only who can access the network but where they can access it, it is possible to prevent neighbors and hackers from getting on your network even if they're using specialized antennae.
- **Keep insiders on your network** and off of unknown and often dangerous networks. Immediately identify when devices inside your facility associate with devices outside your facility. This prevents users from accidentally connecting to a neighbors network or worse a hackers trap. This is especially valuable in environments where neighbors are in close proximity to your facility such as multi-floor office buildings and high density urban areas.

- **Distinguish true rogues** from unidentified neighboring LANs. Determine if new unidentified wireless LANs due to Ad-hoc networks or rogue APs are within your walls and controllable or are outside your walls and out of your control. While insiders access to those neighboring LANs is controlled with location, it is not necessary to waste time tracking down each new rogue only to discover it is not even in your building. When rogues are found inside your facility, track them down faster with specific physical location information.
- **Detect and prevent an array of wireless attacks** by accurately characterizing attacks based on whether they are coming from the outside or within your own walls so you can focus on detecting and preventing attacks appropriately. With location tracking you can determine where an outsider is attacking your network from even if they are using a high-gain antenna.

Rather than having to detect each specific type of threat and then alerting when one is detected, it is possible to eliminate entire classes of threats once you know the location of wireless devices.

Summary

WLANs are here, you do not have a choice. It's only a matter of time before your employees, customers and partners demand some form of WLAN access when working or visiting your facilities. Most devices, whether you like it or not, either have or will soon have 802.11 radios built into them. Therefore, they carry with them an instant WLAN every time they turn on the device or walk into your doors.

With accurate location tracking that maps to real physical space, you can once again think about security in physical terms. By tracking devices based on RF signatures and determining their true physical location you can establish a virtual physical perimeter that effectively manages RF traffic within your facility. The idea behind physical perimeter security is to help you bring back the control and manageability you've experienced with wired-side networks but lost with WLANs. The missing ingredient in a secure WLAN is the walls.

Multi-layer security is essential in WLAN deployments. There are too many variables (ubiquitous access) and risks (open signals, wireless attacks) with WLANs to treat them like your wired-side networks. A complete WLAN security solution considers location as an essential component to bringing back your walls.



745 Boylston Street
Boston, MA 02116
Phone (617) 867-7007
Fax (617) 867-7001

www.newburynetworks.com

Copyright © 2004, Newbury Networks, Inc. All Rights Reserved. WiFi Watchdog, Newbury Networks, and the Newbury Networks logo are trademarks of Newbury Networks, Inc. All other products and services are trademarks, service marks, or registered service marks of their respective owners.