An ISS Technical White Paper

INTERNET SECURITY SYSTEMS™

Wireless LAN Security

802.11b and Corporate Networks

6303 Barfield Road • Atlanta, GA 30328 Tel: 404.236.2600 • Fax: 404.236.2626

Introduction

Although a variety of wireless network technologies have or will soon reach the general business market, wireless LANs based on the 802.11 standard are the most likely candidate to become widely prevalent in corporate environments. Current 802.11b products operate at 2.4GHz, and deliver up to 11Mbps of bandwidth – comparable to a standard Ethernet wired LAN in performance. An upcoming version called 802.11a moves to a higher frequency range, and promises significantly faster speeds. It is expected to have security concerns similar to 802.11b.

This low cost, combined with strong performance and ease of deployment, mean that many departments and individuals already use 802.11b, at home or at work – even if IT staff and security management administrators do not yet recognize wireless LANs as an approved technology. This paper addresses the security concerns raised by both current and upcoming 802.11 network technologies.

Wireless LAN Business Drivers

Without doubt, wireless LANs have a high gee-whiz factor. They provide always-on network connectivity, but don't require a network cable. Office workers can roam from meeting to meeting throughout a building, constantly connected to the same network resources enjoyed by wired, desk-bound coworkers. Home or remote workers can set up networks without worrying about how to run wires through houses that never were designed to support network infrastructure.

Wireless LANS may actually prove less expensive to support than traditional networks for employees that need to connect to corporate resources in multiple office locations. Large hotel chains, airlines, convention centers, Internet cafes, etc., see wireless LANs as an additional revenue opportunity for providing Internet connectivity to their customers. Wireless is a more affordable and logistically acceptable alternative to wired LANs for these organizations. For example, an airline can provide for-fee wireless network access for travelers in frequent flyer lounges – or anywhere else in the airport.

Market maturity and technology advances will lower the cost and accelerate widespread adoption of wireless LANs. End-user spending, the primary cost metric, will drop from about $250 in 2001 to around $180 in 2004 (Gartner Group). By 2005, 50 percent of Fortune 1000 companies will have extensively deployed wireless LAN technology based on evolved 802.11 standards (0.7 probability). By 2010, the majority of Fortune 2000 companies will have deployed wireless LANs to support standard, wired network technology LANs (0.6 probability).

Reality Check

For the foreseeable future wireless technology will complement wired connectivity in enterprise environments. Even new buildings will continue to incorporate wired LANs. The primary reason is that wired networking remains less expensive than wireless. In addition, wired networks offer greater bandwidth, allowing for future applications beyond the capabilities of today's wireless systems.

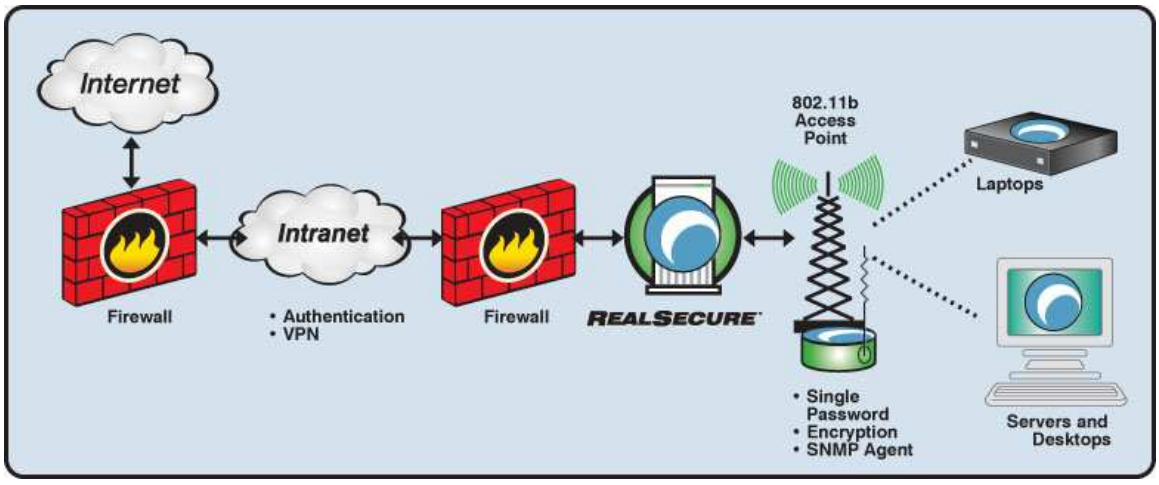
Although it may cost 10 times more to retrofit a building for wired networking (initial construction being by far the preferred time to set up network infrastructure), wiring is only a very small fraction of the cost of the overall capital outlay for an enterprise network. For that reason, many corporations are only just testing wireless technology. This limited acceptance at the corporate level means few access points with a limited number of users in real world production environments, or evaluation test beds sequestered in a lab. In response, business units and individuals will deploy wireless access points on their own. These unauthorized networks almost certainly lack adequate attention to information security, and present a serious concern for protecting online business assets.

Finally, the 802.11b standard shares unlicensed frequencies with other devices, including Bluetooth wireless personal area networks (PANs), cordless phones, and baby monitors. These technologies can, and do, interfere with each other. 802.11b also fails to delineate roaming

(moving from one cell to another), leaving each vendor to implement a different solution. Future proposals in 802.11 promise to address these shortcomings, but no shipping products are on the immediate horizon.

Wireless Security In The Enterprise
802.11b's low cost of entry is what makes it so attractive. However, inexpensive equipment also makes it easier for attackers to mount an attack. "Rogue" access points and unauthorized, poorly secured networks compound the odds of a security breach.

The following diagram depicts an intranet or internal network that is properly configured to handle wireless traffic, with two firewalls in place, plus intrusion detection and response sensors to monitor traffic on the wireless segment. One firewall controls access to and from the Internet. The other controls access to and from the wireless access point. The access point itself is the bridge that connects mobile clients to the internal network.



The access point has a dedicated IP address for remote management via SNMP (Simple Network Management Protocol). The wireless clients themselves – usually laptops or desktops and handhelds – may also use SNMP agents to allow remote management. As a result, each of these devices contains a sensor to ensure that each unit is properly configured, and that these configurations have not been improperly altered. The network itself is regularly monitored to identify access points in operation, and verify that they are authorized and properly configured.

While this paper focuses on the risk issues from a corporate network perspective, these same issues apply to home networks, telecommuters using wireless, and "public use" networks such as those being set up by Microsoft to allow wireless Internet access at select Starbucks locations. Remote users are now able to access internal corporate resources from multiple types of foreign networks. Even organizations without internal wireless networks must take wireless into account as part of their overall security practices.

Known Risks

Although attacks against 802.11b and other wireless technologies will undoubtedly increase in number and sophistication over time, most current 802.11b risks fall into seven basic categories:

- Insertion attacks
- Interception and unauthorized monitoring of wireless traffic
- Jamming

- Client-to-Client attacks
- Brute force attacks against access point passwords
- Encryption attacks
- Misconfigurations

Note that these classifications can apply to any wireless technology, not just 802.11b. Understanding how they work and using this information to prevent their success is a good stepping stone for any wireless solution.

Insertion Attacks
Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review.

- ***Unauthorized Clients*** – An attacker tries to connect a wireless client, typically a laptop or PDA, to an access point without authorization. Access points can be configured to require a password for client access. If there is no password, an intruder can connect to the internal network simply by enabling a wireless client to communicate with the access point. Note, however, that some access points use the same password for all client access, requiring all users to adopt a new password every time the password needs to be changed.

- ***Unauthorized or Renegade Access Points*** – An organization may not be aware that internal employees have deployed wireless capabilities on their network. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources through a rogue access point. Organizations need to implement policy to ensure secure configuration of access points, plus an ongoing process in which the network is scanned for the presence of unauthorized devices.

Interception and Monitoring of Wireless Traffic
As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be within range of an access point (approximately 300 feet for 802.11b) for this attack to work, whereas a wired attacker can be anywhere where there is a functioning network connection. The advantage for a wireless interception is that a wired attack requires the placement of a monitoring agent on a compromised system. All a wireless intruder needs is access to the network data stream.

There are two important considerations to keep in mind with the range of 802.11b access points. First, directional antennae can dramatically extend either the transmission or reception ranges of 802.11b devices. Therefore, the 300 foot maximum range attributed to 802.11b only applies to normal, as-designed installations. Enhanced equipment also enhances the risk. Second, access points transmit their signals in a circular pattern, which means that the 802.11b signal almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings, or even through floors in multistory buildings. Careful antenna placement can significantly affect the ability of the 802.11b signal to reach beyond physical corporate boundaries.

- ***Wireless Packet Analysis*** – A skilled attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of these tools capture the first part of the connection session, where the data would typically include the username and password. An intruder can then masquerade as a legitimate user by using this captured information to hijack the user session and issue unauthorized commands.

- ***Broadcast Monitoring*** – If an access point is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcasted out over the wireless network. Because the Ethernet hub broadcasts all data packets to all connected devices including the wireless access point, an attacker can monitor sensitive data going over wireless not even intended for any wireless clients.

- ***Access Point Clone (Evil Twin) Traffic Interception*** – An attacker fools legitimate wireless clients into connecting to the attacker's own network by placing an unauthorized access point with a stronger signal in close proximity to wireless clients. Users attempt to log into the substitute servers and unknowingly give away passwords and similar sensitive data.

Jamming
Denial of service attacks are also easily applied to wireless networks, where legitimate traffic can not reach clients or the access point because illegitimate traffic overwhelms the frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, corrupting the signal until the wireless network ceases to function. In addition, cordless phones, baby monitors and other devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. These denials of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

Client-to-Client Attacks
Two wireless clients can talk directly to each other, bypassing the access point. Users therefore need to defend clients not just against an external threat but also against each other.

- ***File Sharing and Other TCP/IP Service Attacks*** – Wireless clients running TCP/IP services such as a Web server or file sharing are open to the same exploits and misconfigurations as any user on a wired network.

- ***DOS (Denial of Service)*** – A wireless device floods other wireless client with bogus packets, creating a denial of service attack. In addition, duplicate IP or MAC addresses, both intentional and accidental, can cause disruption on the network.

Brute Force Attacks Against Access Point Passwords
Most access points use a single key or password that is shared with all connecting wireless clients. Brute force dictionary attacks attempt to compromise this key by methodically testing every possible password. The intruder gains access to the access point once the password is guessed.

In addition, passwords can be compromised through less aggressive means. A compromised client can expose the access point. Not changing the keys on a frequent basis or when employees leave the organization also opens the access point to attack. Managing a large number of access points and clients only complicates this issue, encouraging lax security practices.

Attacks against Encryption
802.11b standard uses an encryption system called WEP (Wired Equivalent Privacy). WEP has known weaknesses (see http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html for more information), and these issues are not slated to be addressed before 2002. Not many tools are readily available for exploiting this issue, but sophisticated attackers can certainly build their own.

Misconfiguration
Many access points ship in an unsecured configuration in order to emphasize ease of use and rapid deployment. Unless administrators understand wireless security risks and properly configure each unit prior to deployment, these access points will remain at a high risk for attack or misuse. The following section examines three leading access points, one each from Cisco, Lucent and 3Com. Although each vendor has its own implementation of 802.11b, the underlying issues should be broadly applicable to products from other vendors.

- ***Server Set ID (SSID)*** – SSID is a configurable identification that allows clients to communicate with an appropriate access point. With proper configuration, only clients with the correct SSID can communicate with access points. In effect, SSID acts as a single shared password between access points and clients. Access points come with default SSIDs. If not changed, these units are easily compromised. Here are common default passwords:

  "tsunami" – Cisco
  "101" – 3Com
  "RoamAbout Default Network Name" – Lucent/Cabletron
  "Compaq" – Compaq
  "WLAN" – Addtron
  "intel" – Intel
  "linksys" – Linksys
  "Default SSID", "Wireless" – Other manufacturers

  SSIDs go over the air as clear text if WEP is disabled, allowing the SSID to be captured by monitoring the network's traffic. In addition, the Lucent access points can operate in Secure Access mode. This option requires the SSID of both client and access point to match. By default this security option is turned off. In non-secure access mode, clients can connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any."

- ***Wired Equivalent Privacy (WEP)*** – WEP can be typically configured as follows:

  No encryption
  40 bit encryption
  128 bit encryption

  Most access points ship with WEP turned off. Although 128 bit encryption is more effective than 40 bit encryption, both key strengths are subject to WEP's known flaws.

- ***SNMP Community Passwords*** – Many wireless access points run SNMP agents. If the community word is not properly configured, an intruder can read and potentially write sensitive data on the access point. If SNMP agents are enabled on the wireless clients, the same risk applies to them as well.

  By default, many access points are read accessible by using the community word, "public". 3Com access points allow write access by using the community word, "comcomcom". Cisco and Lucent/Cabletron require the write community word to be configured by the user or administrator before the agent is enabled.

- ***Configuration Interfaces*** – Each access point model has its own interface for viewing and modifying its configuration. Here are the current interface options for these three access points:

  Cisco – SNMP, serial, Web, telnet
  3Com – SNMP, serial, Web, telnet
  Lucent / Cabletron – SNMP, serial (no web/telnet)

  3Com access points lack access control to the Web interface for controlling configuration. An attacker who locates a 3Com access point Web interface can easily get the SSID from the "system properties" menu display. 3Com access points do require a password on the Web interface for write privileges. This password is the same as the community word for write privileges, therefore 3Com access points are at risk if deployed using the default "comcomcom" as the password.

- ***Client Side Security Risk*** – Clients connected to an access point store sensitive information for authenticating and communicating to the access point. This information can be compromised if the client is not properly configured. Cisco client software stores the SSID in the Windows registry, and the WEP key in the firmware, where it is more difficult to access. Lucent/Cabletron client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry, but it is encrypted using an undocumented algorithm. 3Com client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry with no encryption.

- ***Installation*** – By default, all three access points are optimized to help build a useful network as quickly and as easily as possible. As a result, the default configurations minimize security.

Wireless Information Security Management

Process and technology are always easily confused, and never more so than with wireless information security management. In fact, the same business processes that establish strong risk management practices for physical assets and wired networks also work to protect wireless resources. The following cost-effective guidelines help enable organizations to establish proper security protections as part of an overall wireless strategy – and will continue to work in spite of wireless networking's rapid evolution. The following items are an introduction to this approach.

Wireless Security Policy and Architecture Design – Security policy, procedures and best practices should include wireless networking as part of an overall security management architecture to determine what is and is not allowed with wireless technology.

Treat Access Points As Untrusted – Access points need to be identified and evaluated on a regular basis to determine if they need to be quarantined as untrusted devices before wireless clients can gain access to internal networks. This determination means appropriate placement of firewalls, virtual private networks (VPN), intrusion detection systems (IDS), and authentication between access point and intranets or the Internet.

Access Point Configuration Policy – Administrators need to define standard security settings for any 802.11b access point before it can be deployed. These guidelines should cover SSID, WEP keys and encryption, and SNMP community words.

Access Point Discovery – Administrators should regularly search outwards from a wired network to identify unknown access points. Several methods of identifying 802.11b devices exist, including detection via banner strings on access points with either Web or telnet interfaces.

Wireless network searches can identify unauthorized access points by setting up a 2.4 GHz monitoring agent that searches for 802.11b packets in the air. These packets may contain IP addresses that identify which network they are on, indicating that rogue access points are operating in the area. One important note: this process may pick up access points from other organizations in densely populated areas.

Access Point Security Assessments – Regular security audits and penetration assessments quickly identify poorly configured access points, default or easily guessed passwords and community words, and the presence or absence of encryption. Router ACLs and firewall rules also help minimize access to the SNMP agents and other interfaces on the access point.

Wireless Client Protection – Wireless clients need to be regularly examined for good security practices. These procedures should include the presence of some or all of the following:

- Distributed personal firewalls to lock down access to the client
- VPNs to supplement encryption and authentication beyond what 802.11b can provide

- Intrusion detection and response to identify and minimize attacks from intruders, viruses, Trojans and backdoors
- Desktop assessments to identify and repair security issues on the client device

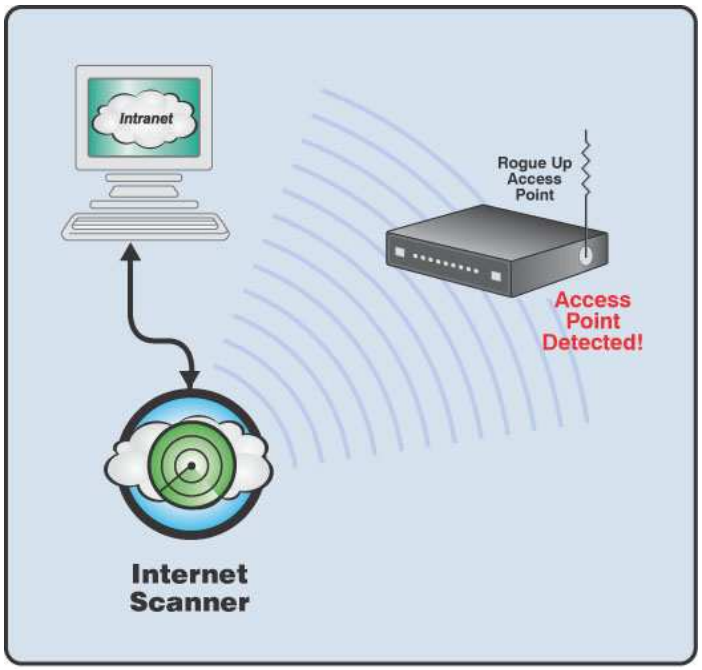
Managed Security Services for Wireless – Managed Security Services (MSS) helps organizations establish effective security practices without the overhead of an extensive, in-house solution. MSS providers handle assessment, design, deployment, management and support across a broad range of information security disciplines. This 24/7/365 solution works with the customer to set policy and architecture, plus provides emergency response, if needed. These services help an organization operating wireless networks to:

- Deploy firewalls that separate wireless networks from internal networks or the Internet
- Establish and monitor VPN gateways and VPN wireless clients
- Maintain an intrusion detection system on the wireless network to identify and respond to attacks and misuse before critical digital resource are placed at risk.

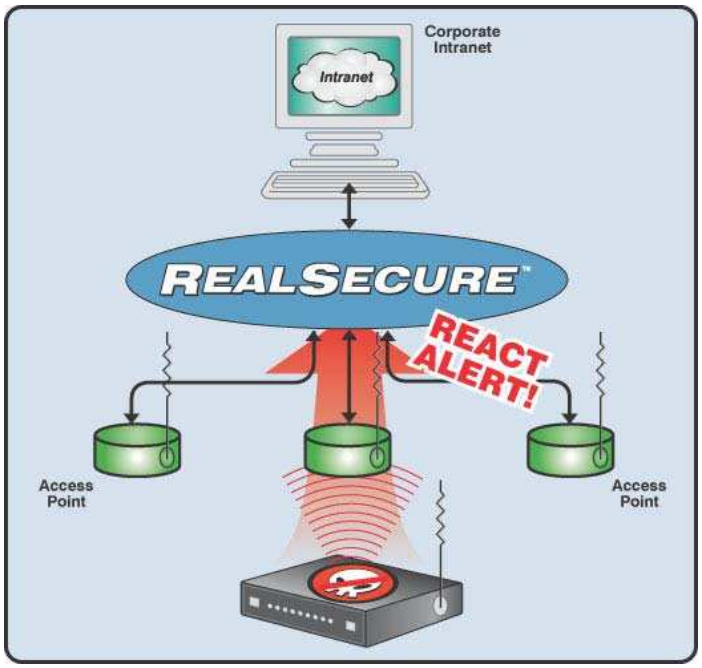
Internet Security Systems Wireless LAN Solutions

Internet Security Systems products and services provide a robust security management solution for wireless LANs. These rapidly expanding offerings encompass:

Security Software Products – Internet Security Systems' security products already protect wireless LAN environments against known security risks. ISS' ***Internet Scanner***™ network vulnerability assessment product probes networks to detect unauthorized or poorly configured wireless access points, as represented in the diagram below.



The ***RealSecure™ Protection System***, deployed between a wireless access point and the corporate network, recognizes and reacts to attacks and misuse directed over the wireless LAN (below). In addition, ISS' renowned ***X-Force™*** research and development team continually update these products.



Managed Security Services – Internet Security Systems' Managed Security Services protect wireless LANS on a 24x7 basis through remote network assessments and tactical deployment of remotely managed intrusion protection services. As new wireless protections are added to ISS security products, Managed Security Services will deliver these additional capabilities to our customers.

Security Architecture Consulting – Internet Security Systems' Consulting Solutions Group has in-depth security knowledge, expertise, and proven methodology required that helps organizations assess, integrate, design, and configure their wireless LANs and surrounding security infrastructure.

Wireless LAN Security Education – Internet Security Systems' ***SecureU™*** education services organization has developed wireless LAN security content to help customers understand the nuances of wireless LAN security and establish valid defensive techniques to minimize security risks.

Product Updates – Internet Security Systems' X-Force research and development team continually adds product enhancements that deliver new protections against wireless LAN risks. These ***X-Press Update™*** enhancements quickly and easily integrate into existing product installations.

About Internet Security Systems (ISS)
Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a world leader in software and services that protect critical online resources from attack and misuse. ISS is headquartered in Atlanta, GA, with additional operations throughout the United States and in Asia, Australia, Europe, Latin America and the Middle East.