VOSTROM

The Wireless LAN VPN Jail

Weakness in the common wireless network security implementation

November 2003

Acknowledgments

Disclaimer

VOSTROM Holdings, Inc. (VOSTROM) shall not be liable for technical or editorial errors or omissions contained herein. The information in this publication is subject to change without notice and is provided “AS IS” WITHOUT WARRANTY OF ANY KIND. THE ENTIRE RISK ARISING OUT OF THE USE OF THIS INFORMATION REMAINS WITH RECIPIENT. IN NO EVENT SHALL VOSTROM BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR OTHER DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION OR LOSS OF BUSINESS INFORMATION), EVEN IF VOSTROM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Intellectual Property Notices

Authors

B. Watson, V. Oppleman, J. Willett

Introduction

While there are many mechanisms available to secure wireless networks, numerous vulnerabilities have made those mechanisms obsolescent. This document serves to outline one popular method, termed the "wireless jail," to secure a wireless LAN, while pointing out that vulnerabilities **still** exist, even with diligence in designing the wireless LAN.

The "Wireless Jail"

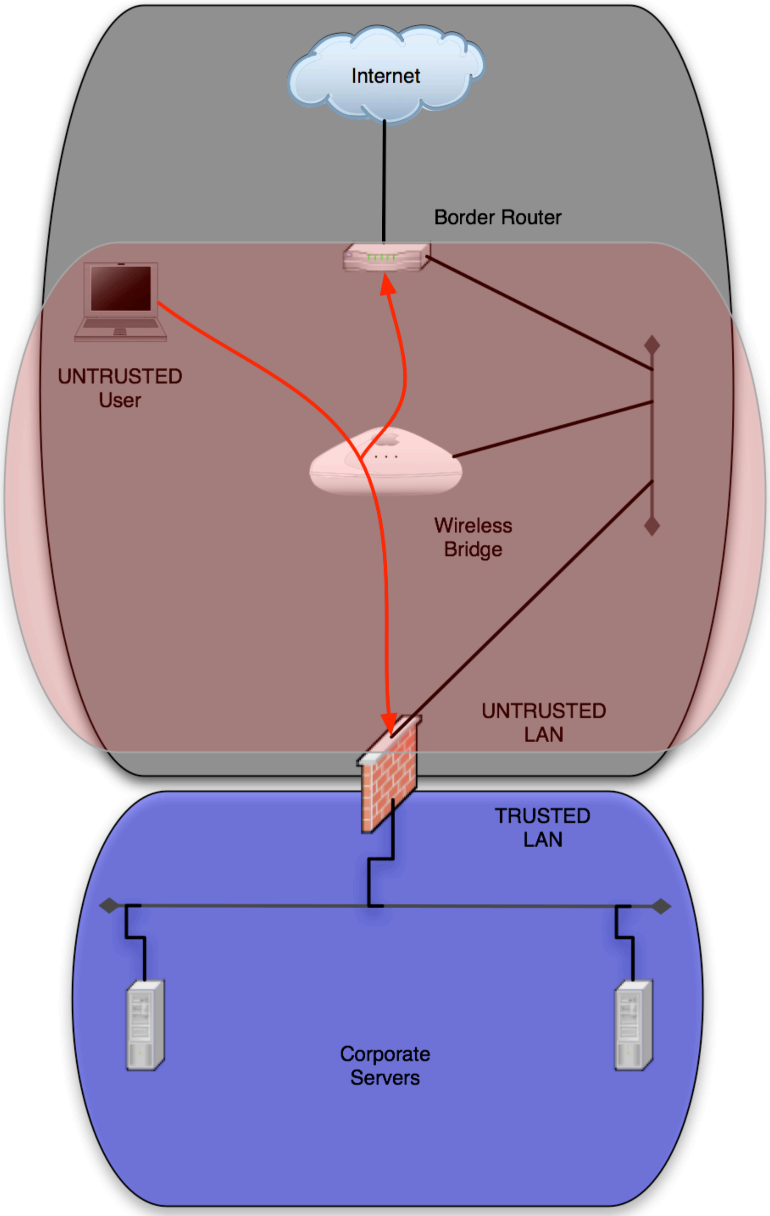
In many cases, an enterprise deploys wireless LAN equipment directly on the enterprise LAN infrastructure. Typically, the wireless bridges are connected directly to the core-switching infrastructure. This method assumes that wireless users can be trusted. However, many tools exist today that allow attackers to capture wireless network SSIDs and in many cases to attack and defeat wireless encryption keys. These tools can brute-force attack WEP, LEAP, and a variety of other wireless encryption mechanisms.

Administrators should assume that wireless users cannot be trusted, and instead deploy wireless access points *outside* the firewall (trust barrier) of the enterprise LAN, creating a wireless jail. The goal of the jail is to make it easy for wireless clients to access the wireless network, but harden this network in such a way as to make this layer-2 access insufficient for accessing the organization's resources. Therefore, accessing the wireless LAN is merely a prerequisite to utilizing more sophisticated and secure methods of access to organizational resources. Once layer-2 access has been achieved, the only options available to the client on the wireless LAN should be 1) finding the address of the organization's virtual private network (VPN) concentrator, 2) routing to the VPN concentrator, 3) securely authenticating to the VPN concentrator and 4) establishing a VPN tunneling protocol that will allow the client access to the organization's internal networks over an encrypted channel.

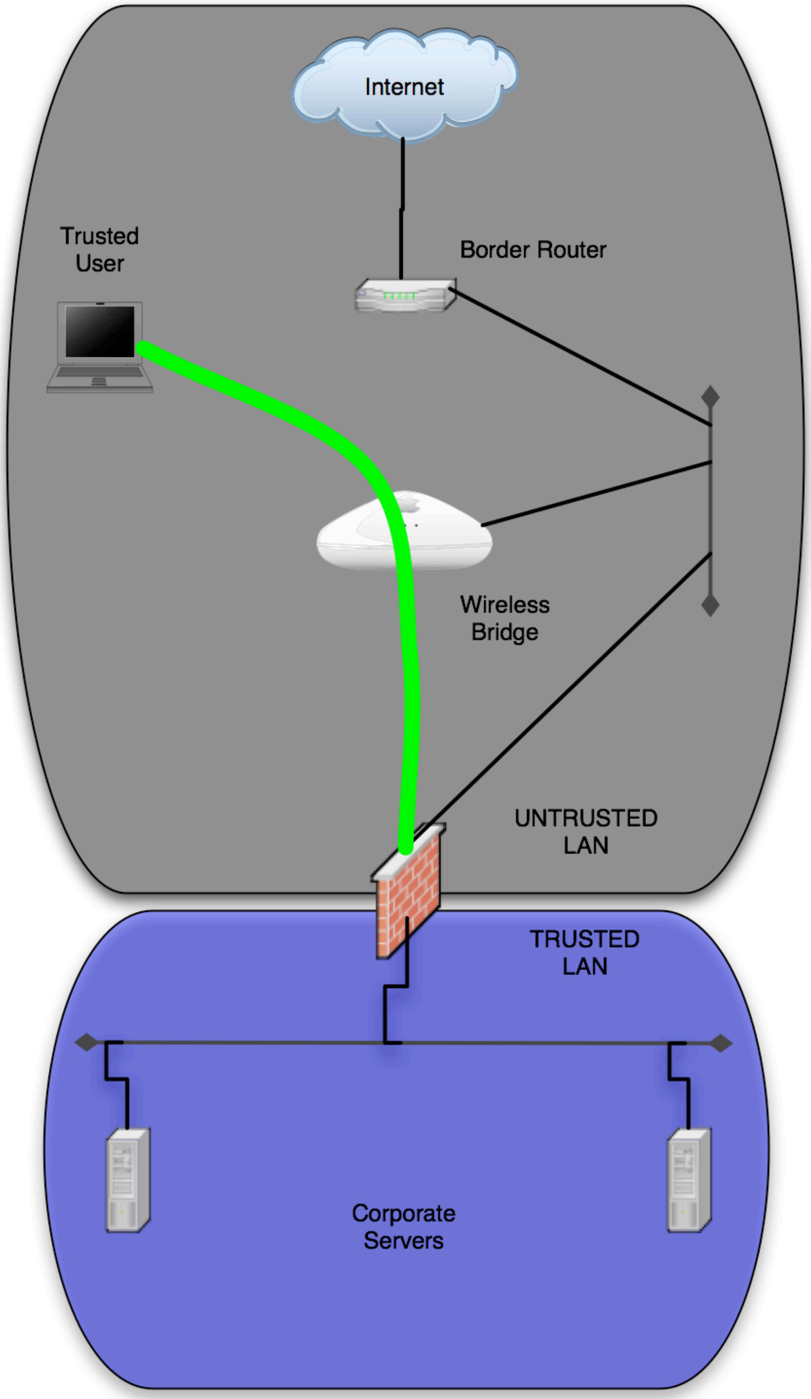
The wireless jail described above may be easily constructed using the following steps (reference diagram on the following page):

1. Deploy wireless access points on an *untrusted* ethernet segment/VLAN and IP network block (using RFC 1918 or routed Internet addresses) outside the organization's firewalls (between the firewall and the Internet border router, for example).
2. Configure an SSID but **do not** broadcast the SSID (requiring wireless users to at least know the SSID before connecting)
    a. NOTE: Attackers can find the SSID with freely available tools, so one may wish to broadcast the SSID anyway for interoperability with various wireless cards.
3. Configure the wireless access point to assign wireless clients IP addresses (from inside the jail segment) and DNS servers.
    a. These DNS servers should be either located directly inside the jail, thereby unable to perform recursive queries, or they must be configured and routed in such a way as to deny recursive queries and essentially, ONLY respond to requests for the address record of an organization's VPN concentrator. This is convenient so that wireless clients may enter the name of their VPN concentrator instead of its IP address.
    b. By configuring wireless clients with the IP address (instead of a hostname or fully qualified domain name) of their VPN concentrator, the need for jailed DNS servers may be eliminated.
4. Create security policies for the jail's IP address block on the border router and/or the organization's firewall, preventing clients inside the jail from routing to the global Internet or to the internal networks of the organization. The organization's firewall should deny access to any request originating from the jail other than PPTP, L2TP, or IPSec protocols and helper protocols such as GRE, AH, and ESP.

The following diagram depicts the *untrusted* user in the "wireless jail." Access is blocked to both the Internet (through the border router) and the corporate LAN (through the firewall). The only way a user can access the Internet or the corporate LAN is to authenticate to the firewall and/or VPN concentrator and establish an encrypted VPN tunnel.


Internet
Border Router
UNTRUSTED
User
Wireless
Bridge
UNTRUSTED
LAN
TRUSTED
LAN
Corporate
Servers

The next step provides the authentication and encryption mechanism (PPTP or IPSEC tunnel) whereby the user gains full access to the Internet and corporate LAN:



Security Concerns

At this point, one might assume that the wireless LAN is completely secure. However, there is still one significant and easily overlooked vulnerability apparent to educated attackers.

Remember that the wireless users are assigned an IP address once they connect to the wireless access point. Granted, the clients are assigned a new address once a tunnel has been negotiated using secure VPN mechanisms. However, the primary address is still active on the network interface and because of the nature of ethernet, it may still be used. Many a network engineer would argue that if the VPN concentrator delivers a default route to the wireless client, all traffic will route through the concentrator, but we would ask them to keep in mind that a "connected" network is always given a lower (more relevant) routing metric. Meaning, on Ethernet, connected networks route without consideration being given to the default route.

Therefore, this presents two technical vulnerabilities:

1. Wireless clients that have not yet authenticated to the organization's VPN concentrator are vulnerable to attack from other wireless clients in the jail.
2. Wireless clients that have already established a tunnel to the organization's VPN concentrator are vulnerable to attack from other wireless clients in the jail.

An attacker could port scan the wireless users to find vulnerabilities on their systems, then attack those systems, and potentially propagate worms or Trojan programs through that system. Given that a legitimate user is now authenticated and authorized to access the corporate LAN behind the firewall, this potentially opens the corporate LAN to further attack through this trusted system.

The most obvious form of attack would be some sort of worm such as the Welchia, Blaster, Slammer or other varieties. To describe a real-world attack: a wireless client that has been configured perfectly and has securely established a connection through the jail into an organization's VPN concentrator may then be attacked (using a worm) by a random client also attached to the wireless jail (not necessarily a legitimate user). Then, the authenticated client may spread the worm throughout the organization's internal network—all within a matter of seconds.

The following diagram depicts the wireless jail with an authorized user being attacked from within the wireless jail.

Summary

While the wireless jail might seem like a completely secure wireless security method, due to the requirement of encrypted tunnels for access to the corporate LAN, this paper shows that attacks are still possible due to the nature of IP addressing and IP routing.

There are some obvious solutions to the vulnerabilities discussed herein:

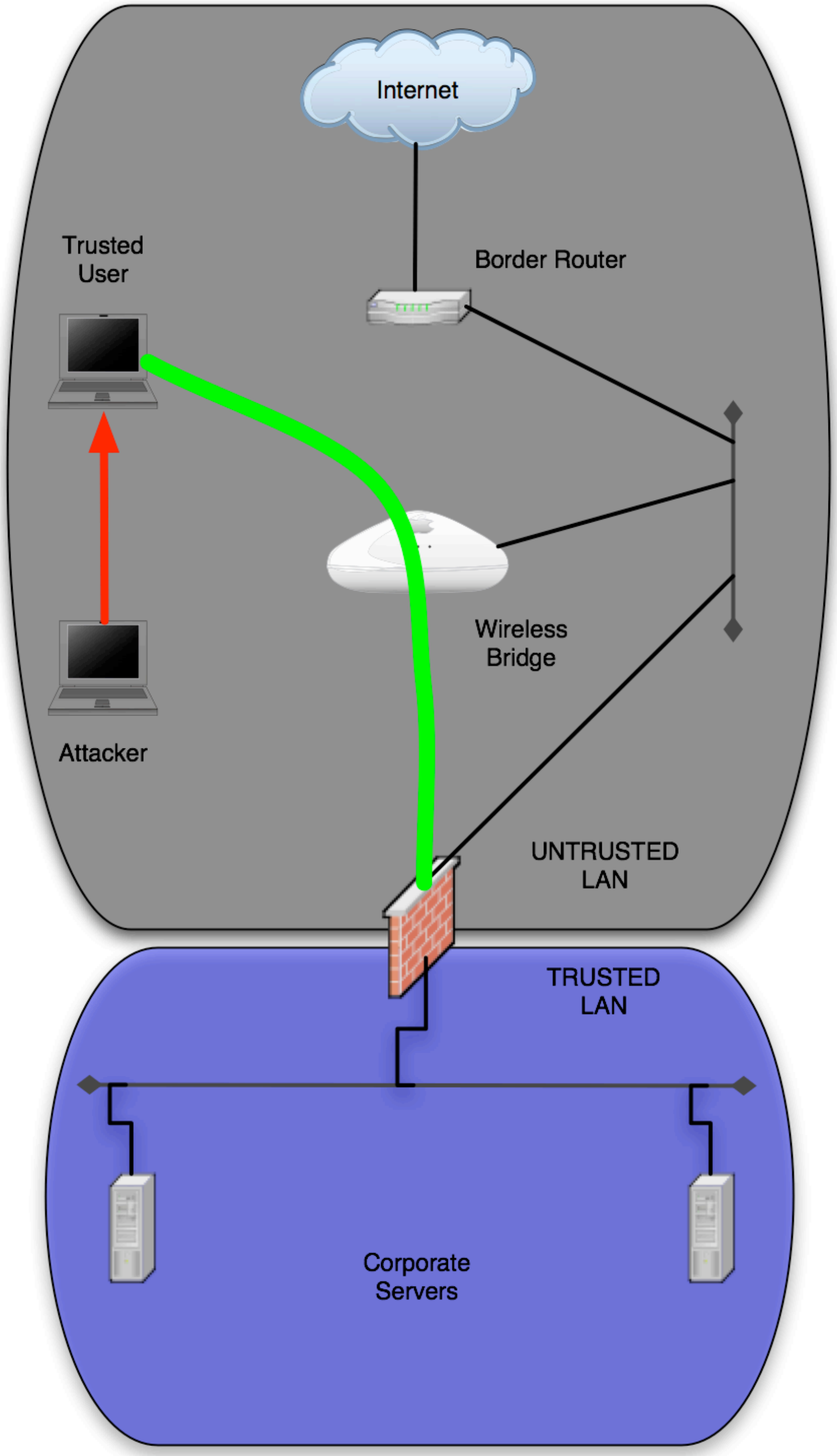
1. **OUR RECOMMENDATION:** Configure access points to echo (forward) only specifically-required traffic instead of acting as a general ethernet switch. DNS, DHCP, and VPN protocols are the only necessary transactions that should be taking place on your wireless LAN.

2. Utilization of host-based firewalls would provide additional security, however we do not recommend using them because of economics (cost) and no guarantee of global distribution. Some laptops may not have the firewall software and/or it may have been disabled or reconfigured by the user.

3. Utilization of pre-layer-2 "media negotiation authentication" mechanisms such as 802.1x (network port authentication) may solve this problem, though many of these mechanisms have proven vulnerable to intrusion.

4. Standard physical placement or wireless access points to limit signal exposure are still practices which should be used as with any wireless implementation.

Finally, it should be mentioned that ad-hoc network negotiation with nomadic clients is also a significant threat to the security a jail can provide, though this threat is outside the scope of this particular methodology discussion.


Internet
Border Router
Trusted
User
Wireless
Bridge
Attacker
UNTRUSTED
LAN
TRUSTED
LAN
Corporate
Servers