Security for Wireless LAN's

The Real Issues and Solutions

ARHONT
ANSWERS TO INFORMATION SECURITY CHALLENGES

Introduction

If you have, or are thinking of deploying, a Wireless LAN (WLAN) you need to think seriously about security. Your entire wireless network segment will be broadcast "out there" in the unlicensed radio spectrum. Walls alone will not contain the traffic.

Anatomy

The components of a WLAN are typically WLAN Bridges referred to as Access Points (AP), and WLAN user-end client devices already built into laptops, PDA's or smartphones. These devices and AP's are usually interconnected using IEEE standard 802.11g or 802.11n protocols. Upon starting, the WLAN client will first search the ether and then "associate" your computer with an available WLAN matching the expected network name and authentication settings. Ad-hoc networks can be built between wireless clients in the absence of access points, and are casually used to exchange data during business meetings.

Security

Mechanisms IEEE 802.11i standard-based mechanisms are implemented by Wireless Protected Access (WPA) industry certifications to control access to your WLAN. WPA Personal uses a shared secret key to protect smaller SOHO networks against eavesdropping and intrusion. WPA Enterprise relies on additional security mechanisms, such as 802.1x authentication protocol with extensions, to offer stronger protection for larger corporate networks. It requires deployment and configuration of RADIUS servers.

Although you can disable network announcements (broadcasts) and filter client connections on the basis of MAC addresses, this won't stop a hacker as we will see later.

Wired Equivalent Privacy (WEP), an obsolete WLAN security protocol, can be broken within five minutes and shouldn't be used at all.

Out-of-the-box most AP's will have a default network name and AP login password, and no WPA-based protection is enabled.

The Issues

A great amount of on-going work in the wireless security field has uncovered multiple flaws that may allow bypassing even the most powerful defences:

- Monitoring from up to 20 miles away has been achieved using high gain directional antennae. Connections to victim networks have also been achieved at these distances.
- Default (out of the box) settings are still widely used. Statistically, about a third of all real world WLANs are not protected at all while another third employs highly insecure WEP, thus making trespassing easy.
- Unruly users or physical intruders can install unauthorised wireless devices connected to the enterprise LAN and easily accessible outside the company premises.
- Insidious lateral attacks targeting separate wireless client devices and not the whole WLANs can be employed by hackers to circumvent WPA defences. As long as the wireless client is turned on, your laptop, PDA or smartphone can be hacked into in the airport, hotel, café, park, at home and so on. Authentication credentials extracted from it can later be used for unauthorised logins into your corporate WLAN. Physical loss and theft of mobile computers, containing corporate WLAN authentication credentials (e.g. digital certificates) alongside other sensitive data, is also highly common.
- Weak shared WPA Personal keys can be recovered with a dictionary attack. Some 802.1x extension protocols have known security flaws that can be abused.

Perhaps the greatest danger is the overall popularity of wireless combined with the ease of installation and low prices. WLAN "starter kits" that can be easily deployed in SOHO networks have unofficially permeated the corporate environment. The plug and play nature of the starter kits means that anyone with a laptop, a network connection at their desk and moderate computing knowledge can have a WLAN up and running within minutes. Your IT staff wouldn't even notice it was there. Also, your users may even be connecting from home over a secure link to your corporate network. That's fine until an adventurous user installs an unprotected WLAN at home, blowing a big hole right through your corporate security measures.

The second most important threat is client-side attacks. Many users don't suspect at all that wireless connectivity on their mobile computer is enabled and it's constantly searching for a suitable network to link up to. A hacker who sets up a "rogue" AP or an ad-hoc network can lure hundreds of end-user computers to associate with it, while providing fake services, intercepting sensitive traffic and exploiting flaws in the systems ranging from specific holes in the wireless drivers to commonly unprotected Windows network shares.

Other issues of note are:

- Even if network announcements are disabled, traffic is still visible to a hacker. MAC addresses are very easy to spoof.
- Any WLAN can be brought to a standstill with a wireless-specific denial-of-service (DoS) attack.

Recommendations

There are three levels of action to improve the security of your WLANs.

Level 1

Make users and the board aware of the dangers and define a security policy covering WLANs, even if your enterprise doesn't use or plans to deploy wireless. Limit the spread of wireless signal by regulating it's output strength and properly selecting and placing antennae. Keep an up-to-date inventory of all wireless-enabled computers in the company. Their loss and theft must be promptly reported to the IT helpdesk.

Level 2

Configure and maintain WPA-based protection of your WLANs. Using WPA Enterprise is always preferable. Ensure that interconnected wireless and wired networks are properly and securely separated. Regularly clean wireless profiles on all client computers from unnecessary entries. Keep their wireless drivers updated.

Level 3

Implement distributed wireless intrusion prevention system to monitor corporate WLANs in real time, thwart hacking attempts and trace physical locations of any attackers and unauthorised wireless devices.

Conclusions

WLAN are here to stay and can only grow in popularity. But they can also create gaping holes in your IT security if proper care is not exercised. Thankfully, most of the weaknesses can be overcome.

Dr. Andrew Vladimirov
Arhont Information Security