



207 Tremont Street
Rochester, NY 14608
585-436-0400
www.nexusisr.com

A Defense-in-Depth Security Strategy for an Anytime, Anywhere Workforce

Part 1: Securing Mobile Access Appliances
Part 2: Securing Mobile Computing Devices
Part 3: Securing Mobile Data/Knowledge Assets

*By Evhen Tupis
Director of Engineering
Nexus iSR, LLC*

Contents

Introduction	2
Problem Statement	2
Environmental Differentiators	2
Layered Security Strategies	3
Access Point/Appliance Security	5
Implementation Checklist	5
Summary	5

Introduction

To the uninitiated, “security” may seem to be the antithesis of “communication” – the very foundation on which modern networks were built. Yet if the strategy is correctly crafted, “security” simply assures that meaningful “communication” can take place clearly, unambiguously and without non-valued clutter.

According to *Infoworld* magazine author Ephraim Schwartz, “security” is the top concern of organizations that are presently deploying a mobile strategy. This white paper will both discuss “security” *and offer tiered strategies for providing secured access to a mobile workforce* – at the point-of-access to network and Internet services.

Problem Statement

Most newly mobile companies and workers are naïve as to the risks that lay before them, believing that either (1) the anytime, anywhere environment is no different than the more traditionally-cabled brick-and-mortar office that they are already accustomed to –or- (2) security is someone else’s responsibility and that “it will all work out in the end.”

More-savvy companies and organizations realize that security should be a concern yet they may not know how to go about addressing it (either strategically or tactically) in an anywhere, anytime environment.

Environmental Differentiators

Security issues in the Anywhere, Anytime (AA) environment are a **superset** of those found in the Brick-and-Mortar (BaM) environment. Whereas BaM’s are filled with point-to-point copper or fiber connections that hold electrons and photons captive, AA’s are built around freely

radiated radio signals that can be interfered with and/or otherwise exploited both passively and actively. Whereas many BaM's are now employing 802.11 Access Points, they are fixed in location. AA workers require **remote**, **portable** and **mobile** Access Points, adding yet another dimension to the security strategy and its roll-out. In the same Infoworld article, Jay Highley, president and CEO of Integrated Mobile, was quoted as saying that most organizations don't even know how many mobile devices may be deployed at any given time.

Such variables result in significant challenges for the security conscience organization.

Layered Security Strategies

The spectrum of "secure" runs from "none" to "extreme". Even so, "extreme" can change over time as new exploits are uncovered and addressed. Said another way, "That which was considered 'extremely' secure two years ago may be considered only 'moderately' secure today." As such, it is best to place sensitive information into a "vault" or behind a "firewall", allowing only trusted agents to have access to it. This is accomplished by layering several strategies.

Layer 1: Safety through Proxy

AA staff is quickly becoming familiar with cellular data cards. They are easy to use because they provide their laptops with a direct connection to the Internet through a cellular telephone provider's block

of public IP address. Simply insert the PCMCIA/CardBus card into the laptop, load the drivers and the host is "surfing the 'net". This presents a potentially major security hole for two primary reasons: (1) hackers routinely port-scan publicly routable IP addresses, requiring that the laptop now assume the burden of providing a software firewall and assuring it is both up-to-date and configured correctly –and- (2) data card driver versions must be kept up-to-date to assure maximum throughput, safety and security (older drivers may have bugs that allow unauthorized access to the systems that they are connected to).

Solution: use a proxy, separating the computer from the network/Internet and allow the proxy to bear the burden of isolating the computer from online threats. The Nexus Hawk™ is one such device. All data card drivers are pre-loaded on the Nexus Hawk and may be easily uploaded with each firmware update. As delivered, no ports are open to exploit by potential intruders. The Nexus Hawk is based on an embedded Linux operating system that is 'intruder hardened' – with all settings stored in encrypted tables.

Layer 2: Fire-walling at the Proxy

Most proxies rely on Network Address Translation (NAT) to isolate its served clients from the Internet. Savvy hoodlums understand that all they must do is traverse the Proxy and scan 192.168.x.x for open devices. NAT is therefore only somewhat effective. A more robust strategy is to assure that your Proxy employs Stateful Packet Inspection (SPI) – a superior approach designed to ensure that clients served by a Proxy receive only data they have specifically requested.

Layer 3: Virtual Private Networking

Savvy security plans will include some sort of Virtual Private Networking (VPN) strategy. A VPN is as secure as its endpoint allows it to be. Assuming that *Layer 1* has been applied, then it should allow for VPN Pass-through at a minimum. This would allow for a VPN to “tunnel” through the access appliance to reach a client, which would have the proper software loaded and configured on it.

While this may be an adequate solution for a single-client-to-single-Internet-connection environment, it can be quite a complex environment to manage if there are multiple clients being serviced by a single Access Point – as is becoming the case in an increasingly AA world. This is because there is no reduction in the number of clients that must be managed, yet they are now behind a shield that makes both intrusion and proper management more difficult.

To mitigate this issue, one may configure their Access Point as the VPN endpoint and then heavily encrypt the connection between the Access Point and the clients using standard (and often easier to manage) encryption schemes such as WEP, WPA and WPA2/PSK (in order of least to most secure).

Layer 4: Securing the Management Console

Even newbie war drivers (people that scan for open WiFi AP’s to exploit them) know that the default account name and password of certain

popular WiFi AP’s management console is “admin”/”admin”. CHANGE YOURS – NOW. This is BAD.

Layer 5: Use Native Firewalls

Even with the Access Point acting like a Proxy/Firewall, it is a good idea to use any firewalls that are native to most popular operating systems. Microsoft Windows XP, for instance, includes a “personal firewall” which can further filter incoming attacks and probes. Microsoft Windows Vista includes a bi-directional fire wall.

Layer 6: Security through Obfuscation

Every network has a unique identification label referred to as a Service Set Identifier (SSID). It is the SSID that is shown when scanning for available WiFi Access Points. This is because most Access Points will periodically broadcast their presence, including the name of their network (the SSID). Administrators can eliminate “nuisance intruders” simply by switching “Broadcast SSID” to the “Off” position. This is considered “light weight” security because a savvy intruder can still passively monitor traffic to ascertain a network’s SSID. Even so, there is often enough “low hanging fruit” in the form of other WiFi traffic to attack that hiding the SSID can prove to be an effective strategy to employ.

WiFi traffic may occur on two bands: A and B. The B-band is further divided by the terms: G and N (with more on the way). Because of the proliferation of easy to purchase equipment, the WiFi B-band is by-far the most often targeted band for war driving and hacking. It is for this reason that communications using the WiFi A-band are considered both more secure and less prone to interference.

Layer 7: Secure, by Invitation Only

It may be advantageous to restrict who may use an AA's Access Point. This is most effectively accomplished through Machine Access Code (MAC) white listing. A MAC is a universally unique number assigned to a network access card. By populating a MAC white list table with "allowed" clients' MAC address, only those clients will be allowed to connect and use the Access Point. Because the same principles of "traffic sniffing" apply here (as they do to the SSID strategy), this is considered a "light weight" protection mechanism. However, it is quite effective against the casual to moderate intruder.

Layer 8: Disallowing Back Doors

As AA staff roams from one location to another, they will encounter rogue WiFi Access Points provided by both unwitting sources as well as individuals who wish to exploit them through posing as an unwitting Access Point. Unless such things are accounted for by the security system that is loaded on each WiFi enabled device, it is best to disable (1) ad-hoc networking and (2) automatic connections to networks that the AA staff is unfamiliar with or otherwise unauthorized to connect to.

Failing to do so will open a widespread security hole for all client devices that are served by a highly secure Access Point/Appliance because they would be circumventing it.

Access Point/Appliance Security Implementation Checklist

1. Use a hardware Access Point/Appliance between your Anytime/Anywhere staff's computers and their network/Internet service – use it as a proxy and/or firewall.
2. Change the Access Point/Appliance Management Console's default password.
3. Use the strongest WiFi encryption scheme that is supported by the Access Point/Appliance's clients.
4. Use WiFi's A-channels if the Access Point/Appliance's clients can.
5. Disable ad-hoc WiFi networking and automatic connections to unapproved networks.
6. Use a Virtual Private Network (VPN).

Summary

The Nexus Hawk™ "faces" the Internet, taking the brunt of Internet-based attacks or exploit attempts. As delivered from the factory, it appears to the hacker to be a dumb appliance with no exploitable services or open ports. Nexus Hawk clients are safely hosted behind a NAT/SPI service.

All data card drivers are embedded in the Nexus Hawk, simplifying asset management for I-T departments and freeing laptop processors from managing communication.

Virtual Private Networking (VPN), SSL based remote management, WiFi SSID/channel obfuscation/encryption and MAC-based user white/black listing is fully supported by the Nexus Hawk.