

# ***Wireless In-Secure Networks – The New Frontier***

By Gary S. Miliefsky, CISSP®

September 18, 2008

We're constantly hearing stories about government agencies, airlines and transit authorities, retailers and financial institutions being exploited daily by remote attackers. What most people don't understand is that wireless encryption is a complete fallacy. There are only a few ways to properly secure a wireless network and most people do not know how to do this. Turning on WPA or WEP encryption just slows down the exploit for a few seconds to about ten minutes. Hacking tools like WEPCrack and KISMET are among the thousands of ways to break into wireless networks.

The wireless network is the new frontier for attacks. Why? Because attackers can be sitting many blocks away either on a rooftop or in their car. This is called Wardriving. It is typically viewed as the act of searching for Wi-Fi wireless networks by one or more hackers in a car using a laptop and a Pringles can to extend and focus the antenna or a simple PDA.

Wardriving tools are freely available on the Internet, notably NetStumbler for Windows, Kismet or SWScanner for Linux, FreeBSD, NetBSD, OpenBSD, DragonFly BSD, and Solaris, and KisMac for Macintosh. There are also homebrew wardriving applications for handheld game consoles that support Wi-fi, such as sniff\_jazzbox for the Nintendo DS, Road Dog for the Sony PSP and Stumbler for the iPhone. There also exists a mode within Metal Gear Solid: Portable Ops for the Sony PSP (wherein the player is able to find new comrades by searching for wireless access points) which can be used to wardrive (source: Wikipedia).

The notion of a wireless network being secure is nearly impossible because it does not require physical connectivity by a wire through the network. This has been devised as a convenience and to help us 'untether' ourselves and our new internet enabled devices (such cell phones, pdas, laptops, bar code scanners, front door locks, cameras, printer servers and much more). So, what methods have been made available to protect our wireless networks and why are they failing?

Initially, good security was to password protect your wireless network. That was easily hacked by simply sniffing the password in clear text over the wireless traffic. The next step was to encrypt wireless communications by adding keys, passphrases and fully encrypted traffic between wireless routers and end-users. Also, intrusion detection packet sniffers looking for traffic-based exploits was added to these wireless routers. All of the above have resulted in customers having a warm-and-fuzzy good feeling that they were secure, until ten minutes later, they were hacked.

How can a hacker breach these multiple layers of wireless security in ten minutes or less? It's simple. Because wireless traffic flows over the airways, there is simply no way to protect public and private key encryption properly. Within 10 minutes of logged encrypted traffic, tools like WEPcrack can obtain these keys. So encryption on wireless is really useful at keeping out honest people but not real hackers or those terrorists, who recently exploited wireless networks in India, see <http://www.networkworld.com/news/2008/091708-india-wants-to-secure-wi-fi.html>

Most of the new attacks are not traffic based but they are asset based. So, instead of sending malicious traffic to a wireless router, which could set off the intrusion detection alarm, most hackers only send good traffic to the router which will not set off the alarm.

So, one might use an additional layer of security by only allowing trusted assets onto their wireless network. The way to do this is to limit access to a list of devices based on their MAC address. The problem with this approach is that a MAC address can be spoofed. In fact, Microsoft Windows allows you to change your MAC address on your Ethernet card with a few mouse clicks and keystrokes.

The real answer to solving this problem comes in two parts – 1) get rid of wireless networks (and we doubt anyone would accept this solution in the long haul, based upon the conveniences we derive) or 2) take a radically different, more proactive approach to wireless security by focusing on the wireless router and those assets which connect to this router. Does the wireless router have any known vulnerabilities that are remotely exploitable? You can visit <http://nvd.nist.gov> and look them up. Then, see if there is a way to close these holes and remove these exploitable weaknesses either through a patch upgrade or a trade-in for a newer model.

Ultimately, if you can track all the assets that are truly allowed to connect to your wireless router, you can do the same thing to them, harden them against exploit and ensure that only those who are allowed to connect to your wireless router are on your trust list. If someone attempts to connect to your wireless router and you are certain they are not on your trust list then you should boot them off immediately. There are numerous ways to boot someone off your wireless router – one is to log into the router and remove them from the access list, the second is to limit the number of wireless connections allowed – if you have 10 employees who use the wireless router, why would you allow an unlimited number of connections, which is the usual default? Finally, you can turn the tables on the attacker and deny them service. The best way to automate this process is to find an agent-less network access control (NAC) solution that works with your wireless router so this NAC solution can do all of the above and act on your behalf and provide you with a more controlled, trusted wireless network.

## **About the Author**

Gary S. Miliefsky is a network security expert with 20 years experience. He is a founding member of the U.S. Department of Homeland Security. He helped President Clinton's team on the e-Chip initiative and the President's Critical Infrastructure Protection Board, under the George Bush Administration, which is now known as the National Infrastructure Advisory Council (NIAC) and operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace. He currently serves on the National Information Security Group ([www.naisg.org](http://www.naisg.org)) Board of Directors and is a member of an Advisory Board to MITRE ([oval.mitre.org](http://oval.mitre.org)). He has advised numerous governments around the globe on securing critical network infrastructure and is a frequent network security speaker.

Miliefsky is the founder of NetClarity, Inc. For more information visit him at <http://www.netclarity.net>