Whitepaper | July 2010

Wireless Clients in the Crosshairs

Wireless intrusion prevention counters growing threat

Enterprises are expanding their wireless networks with increasing confidence, believing that rooting out rogue access points and implementing WPA2 will put an end to Wi-Fi security concerns. But attackers are, nevertheless, zeroing in on the many millions of corporate client devices, exploiting them to gain entry to corporate networks and sensitive information. These new hacking tools and techniques underscore the need for wireless intrusion prevention systems (WIPS) that can leverage the power of stateful traffic analysis to effectively deal with these and other security threats.

AIRMAGNET®
now part of Fluke Networks

Introduction

Wireless LANs are not nearly as secure as organizations might think. Even with all the attention focused on security at the access point (AP), in the form of stronger authentication and encryption, many enterprises have thus far ignored the actual wireless network traffic itself. This has left over-the-air connections as a prime target into the network, and network end users.

Many of today's organizations feel they have a strong grip on wireless security because they detect and root out rogue APs. This has been a focal point for most organizations – and perhaps *the* focal point around discussions of wireless security.

It is true that tremendous effort has been expended to watch for, and root out, rogue APs, whether they are malicious or inadvertently hooked into the wire network by a well-intentioned employee. And, Wi-Fi Protected Access Version 2 (WPA2) is a vast improvement over the flawed Wired Equivalent Protection (WEP) encryption model. Yet malicious attackers can circumvent even the strongest defenses.

While companies focus their security efforts on locking down and monitoring corporate APs, attackers are now directly targeting the enterprise's ubiquitous and most vulnerable assets – client devices.

Client wireless devices will be attacked and enterprises must start thinking in terms of the same kind of end-to-end, defense-in-depth strategy that has characterized wired security since organizations first began deploying firewalls, antivirus and intrusion detection systems.

Using new wireless client attack tools and techniques, outsiders can gather login and password data, or send traffic directly to an end-user, without ever touching the approved enterprise wired network. Equally important, new trends in wireless functionality actually open up tunnels into the network, and these tunnels (and the traffic they bear) will appear completely authentic.

Unfortunately, wired security systems do little to protect against this over-the-air malicious traffic. Airborne traffic requires the same level of continuous monitoring and analysis as wire-bound traffic so IT managers can detect criminal activities that may threaten to expose corporate data.

Attackers are Gunning for Client Devices

It is no wonder attackers are turning their attention to client devices, exploiting them from corporate parking lots, and in airports and other hotspots. They are compromising both managed corporate devices and unmanaged smart phones, as well as unmanaged business associate devices. And yes, they can attack Mac OS, as well as Windows devices.

The fact is that rogue AP detection is trivial compared to managing client-side wireless exposures, and the client threat has become far more dangerous. Rogue APs are easy to find because there are few of them, and APs are relatively static. As mentioned earlier, newer wireless LAN systems can automatically scan for unauthorized wireless APs, and security and network managers are attuned to the threats and generally proactive – and even aggressive – about seeking them out.

On the other hand, client vulnerabilities and exploits are *much* harder to detect, and far more threatening because they require stateful monitoring and analysis of network traffic in the air.

Malicious hackers now have a vast number of devices to target such as Wi-Fi-enabled laptops in the office, at home and on the road; Wi-Fi-enabled smart phones, typically privately owned and unmanaged, increasingly used as important work tools; partner, vendor, contractor and service provider laptops – also Wi-Fi enabled. All of these devices are coming onto the corporate network, but are *not* underneath the corporate security umbrella.

Owning Wireless Clients

Attackers' ability to gain access to wireless clients is largely a product of the way these wireless connections work. Wireless technology is designed to facilitate fast, easy connectivity in a variety of settings, to a broad range of trusted and untrusted APs — making it easy to spoof. Even worse, virtualization allows a device to simultaneously operate as both a legitimate client and an open access point, creating an unmanaged bridge (or tunnel) to the outside world. Moreover, this transparent connectivity and seamless virtualization are active *trends* within the industry; they are capabilities that vendors throughout the industry are working to expand and enhance every day. Consider it a feature rather than a vulnerability – a feature, that is, until it is exploited and the attacker gains access to the corporate network.

There are two important points to take from all of this: 1) the majority of Wi-Fi threats occur, and are only detectable, in the air, and 2) the majority of evolving hacks and vulnerabilities revolve around end-user client devices, not enterprise APs.

Client Connections

In order to understand these vulnerabilities, it is important to recognize that there are multiple methods for connecting clients in a wireless network, and some of these approaches will inadvertently open up security holes.

The two most basic approaches are an "ad-hoc mode" (*Figure 1*) where clients connect directly user-to-user over the air, and more commonly in an enterprise setting, an infrastructure mode (*Figure 2*) where users connect to the wireless network through an intermediate device, the access point. This intermediary is designed to not only provide a connection, but also to ensure the security of that connection and protection of the network and associated clients.

Figure 1 – Ad-Hoc Mode

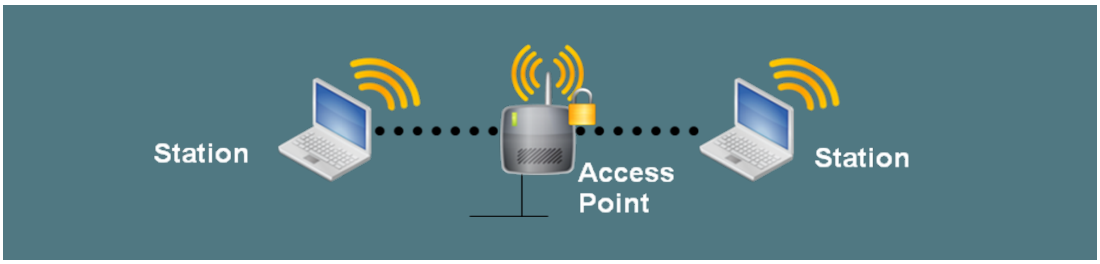


Figure 2 – Infrastructure Mode

While APs are typically purpose-built devices (base stations, routers, etc.), they can just as easily be a "soft AP" – software run on a traditional end-user device, such as a laptop, that allows the Wi-Fi adapter to behave as an access point to serve multiple clients (*Figure 3*). An important distinction, however, is that this soft AP is an either/or setting; the Wi-Fi adapter itself can act as either a client or an AP, but not both. This makes it relatively straightforward to judge what mode (or state) the adapter is in, and thus monitor, manage and secure it appropriately.

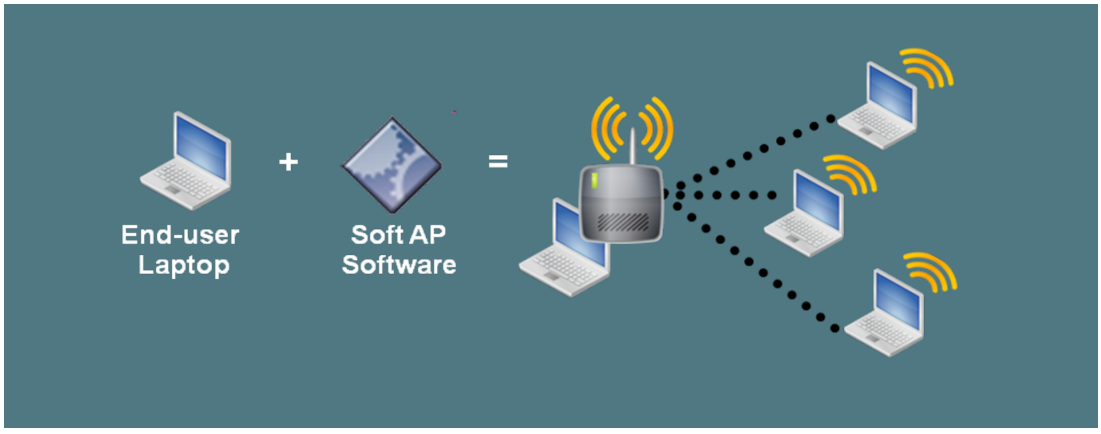


Figure 3 – Soft AP

As we've mentioned earlier, though, there is a new industry trend toward virtualization that eliminates this certainty about the state (client vs. AP) of any given wireless device. And this in turn can open up both individual client devices, and the network itself, to attack. Let's explore Wi-Fi virtualization, and the tools and exploits used to take advantage of the resulting vulnerability, in greater detail.

Virtualization, Vulnerability and Attack

Virtualization is obviously a major initiative across the IT industry as a whole, and no less so in the wireless market, where it has taken the form of adapters that can simultaneously hold multiple roles (or states). Specifically, a single adapter device can simultaneously serve as both a client station and an AP, such that they can take an authorized, secure AP/client network connection and share it out, often unsecurely, to other Wi-Fi devices (*Figure 4*). Chillingly, these secondary virtualized Wi-Fi connections are both weakly secured and *completely invisible to the enterprise network*. Traffic across these connections looks completely valid to the authorized AP and the wired network.

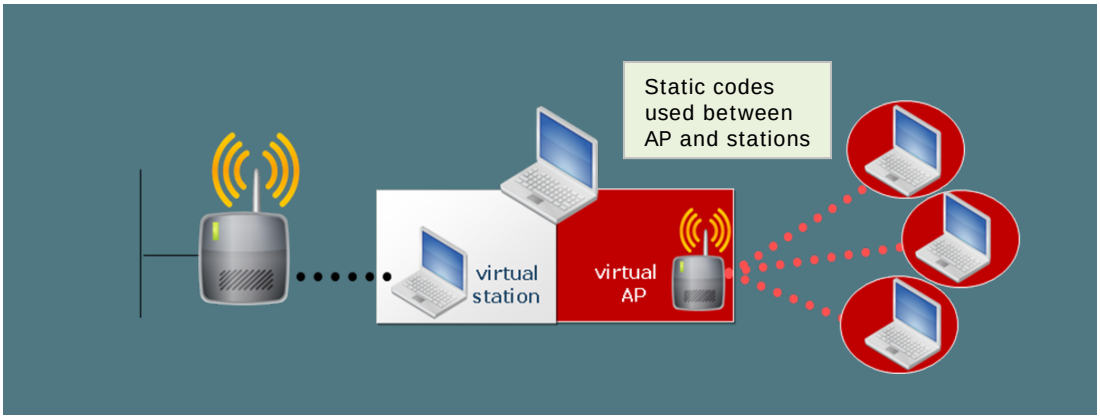


Figure 4 – Virtualization Opens up Wi-Fi

As mentioned earlier, this virtualization is an active Wi-Fi industry trend, as it provides new client device capabilities. It is actively pushed by chip vendors, adapter manufacturers, the Wi-Fi Industry Alliance, and others. One of today's most talked about items is the Windows 7 virtual Wi-Fi adapter, which allows users to readily set up personal networks and share wireless network connections right from within the operating system. This is clearly a beneficial development, and it is simply a case of the operating system providing hooks to leverage the industry's ongoing virtualization trend. However, it also allows the Wi-Fi adapter to turn the laptop into a rogue AP, able to bypass most security measures because it otherwise appears as an authorized device on the network.

Essentially, virtualization creates a vulnerability at the device level by turning a secure client connection into an unmanaged bridge into the network; unknown connections (hackers, unauthorized users, etc.) can now access the network through a secure tunnel. And the only way to monitor, assess and block the connection is through stateful analysis (i.e., recognition that the device is in multiple client/AP states) in the air.

Tools for Client Exploit

Perhaps the most popular tool for exploiting client devices over the air is KARMA (http://www.theta44.org/karma/), a wireless security assessment tool developed by Dino Dai Zvoi and Shane Macaulay. It is used by attackers to discover wireless clients by passively listening for their preferred networks and tricking the device into associating with it. The attacker can use a wide range of exploits once he gains access, but for good measure he can use Karmetasploit, which combines KARMA and H.D. Moore's immensely popular Metasploit pen-testing/exploit framework.

Another application is MDK3, a denial-of-service (DoS) tool that works by de-authenticating clients from the access points, then flooding nearby APs with authentication requests that create a flood of fake APs. The notion of client denial of service is somewhat alien on the wired side – there is little to be gained by disconnecting someone's computer from the wired network – but it can be an important step in compromising a wireless client.

Furthermore, there are also new variations to the Temporal Key Integrity Protocol (TKIP) attack, which targets end-user stations and not APs, allowing hackers to capture larger packet payloads and re-route traffic. This list can go on and on, as many vulnerabilities and exploits exist today, with new ones popping up daily.

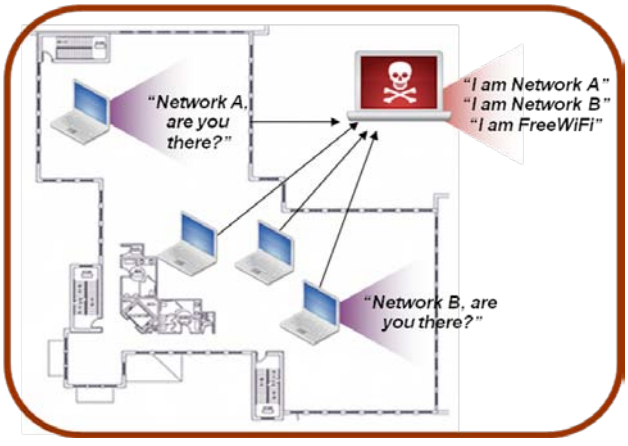
Exploiting Clients: From the Parking Lot to the Database

It is important to keep in mind that compromising client devices isn't the endgame for a wireless attack, it is the entry point into corporate networks and databases.

Hackers are discovering that they can target end users directly, without requiring visibility into the corporate infrastructure itself. Once they find a weak point, they quickly impersonate the end user and start to pull out valuable information.

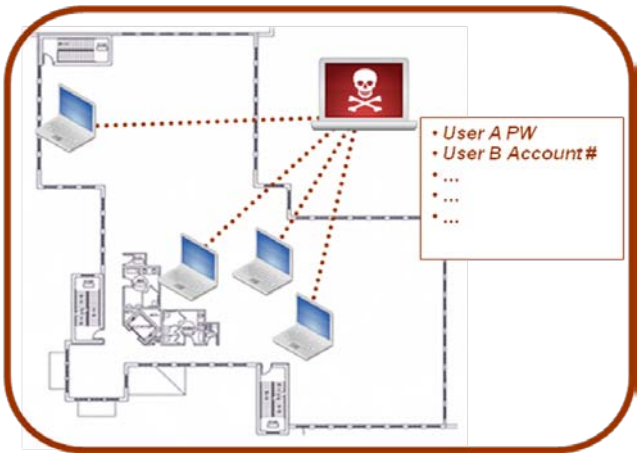
How is this done? In a typical scenario, the attacker may be sitting in a parking lot, armed with a laptop and a high-gain antenna, using KARMA to passively monitoring one or a number of corporate clients' wireless broadcasts. Even if the clients are using strong security – WPA2 with AES encryption – the attacker is not discouraged.

The attacker's goal is to lure end users into connecting with his/her laptop (and vice versa), allowing the hacker to gather information that will enable enterprise access. Even though the attacker can't see the encrypted data load, they can see who the client is talking to, configuration information, and networks it commonly connects to, or has connected to in the past.



The latter point is key. Windows XP in particular will always beacon for networks it has connected to. Your laptop is almost certainly beaconing for the home wireless network you used this morning and probably the airport network you'll use again this afternoon while you wait for your flight. So, the attacker aims to take advantage of that to peel off end users and get them to connect to him instead. KARMA can spoof those network connections, posing as a legitimate access point for a bona fide home network, hotspot connection, etc.

The attacker then launches a denial of service attack against the client(s), cutting off their corporate wireless access. The client then beacons for reconnection, going through its preferred network list. Denied its corporate connection, it will find, instead, what appears to be the user's home wireless network or coffee shop or airport wireless network. But it is the attacker's spoofed network. It's likely that the user won't even notice; all they know is their service was briefly interrupted, but now they are back in business.



From this point, the attacker has a number of ways to see if he can exploit the client machine, typically capturing login information, perhaps by sending a Web page that looks like an Outlook login. The user, thinking he was just disconnected, serves up his credentials, unaware of what is happening.

Road Kill: Clients on the Go

Client devices can be exploited even more readily outside the office, at hot spots, where they are likely to encounter public networks without the benefit of WPA or WPA2 security. Imagine a number of laptops exploited in this way, taking their vulnerabilities back to corporate HQ. But laptops using wireless connectivity have to be used out on the road – it's a primary business driver for using wireless in the first place. In short, clients are being attacked because they are, by nature, dynamic.

So, without exploiting or planting a rogue access point at an organization, without cracking wireless traffic to get the encryption key, without attempting to discover or exploit the wireless infrastructure, the attacker has a foothold in the enterprise simply by luring a client device when outside the organization's network, or piggybacking on an unsecure virtualized connection. It can be that simple.

Detecting and Preventing Client-Side Attacks

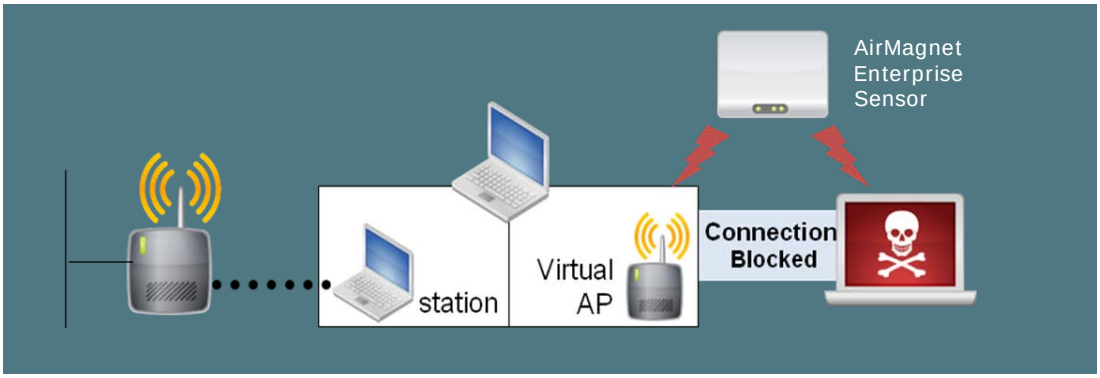
As wireless usage becomes pervasive and an integral part of the extended corporate network, it's time to adopt security policies, procedures and technologies that can meet the challenges of this dynamic environment. Rogue AP detection is simply not enough anymore, as it assumes that you can "see" the unauthorized device. As we've seen, the vast majority of new Wi-Fi threats occur in the air, and focus on spoofing or hijacking or tunneling through authorized client devices. And, these client devices are literally everywhere in the enterprise; with the proliferation of new devices (tablets, smart phones, etc.), the volume is growing every day. Add in the trend toward virtualization, where potential holes are being baked right into chips, adapters and operating systems, and client-side security quickly becomes a losing game – it requires you to know about and control every single device. Miss one device, and the game is over.

The only way to effectively avoid this trap is to adopt the same approach that is used in the wired world: look at the network traffic itself. And just as in the wired world, detecting anomalous and illicit wireless traffic – including attempts against client devices, devices holding multiple states, or compromised or spoofed devices – requires stateful, continuous traffic monitoring and analysis. But existing wired traffic monitoring won't cut it; by the time the hacker has access to the network, the connection looks legitimate. Rogue AP detection alone won't cut it. These hacks avoid the legitimate APs and target client devices instead. The only way to do this wireless traffic monitoring efficiently in an enterprise environment is to deploy wireless intrusion prevention (WIPS) technology, which is unique among wireless security tools because of its ability to look at all traffic in the air statefully. Constant monitoring and analysis enables WIPS to accurately detect all types of attack tools. This includes, for example, wireless traffic intended for corporate clients, such as those DoS attacks designed to separate clients from the corporate network and connect to the attacker. WIPS can also monitor and analyze attack scenarios where the client is first separated from the corporate network and then re-associates with the spoofed networks.

WIPS and AirMagnet Enterprise

AirMagnet Enterprise is designed to provide comprehensive and deep security scanning and analysis across large and distributed organizations. Its dedicated sensors – unlike proprietary systems that use AP-based scanning that doesn't provide the same capability – are scanning all the time. AirMagnet Enterprise is looking at all the traffic, performing complex analyses in real time; this isn't simply identifying malware and attacks from a library of signatures. AirMagnet performs analyses of complex attack techniques and patterns that only a dedicated WIPS tool, backed by the AirMagnet Intrusion Research Team's deep expertise and attention to the latest advances and trends in criminal wireless technology.

AirMagnet Enterprise automatically looks for threats and blocks suspect or compromised devices or anomalous traffic as it detects, for example, connections that aren't supposed to be happening. It looks for countless types of DoS attacks against stations, infrastructure blanketing the air itself. By deploying AirMagnet Enterprise, security personnel will know when someone is trying to disrupt individuals, when a device is pretending to be someone else, and when a hacker is trying to spoof an authorized identity or inject traffic into a conversation. Much like wired IPS, AirMagnet Enterprise WIPS monitors packets and conversations back and forth, but on the wireless side.



The AirMagnet Intrusion Research Team feeds their expertise into the AirMagnet AirWISE® engine, which constantly analyzes all wireless devices and traffic using a combination of frame inspection, stateful pattern analysis, statistical modeling, RF analysis, policy, analysis and anomaly detection, enabling AirMagnet to detect hundreds of specific threats, attacks and vulnerabilities.

Conclusion

Wi-Fi is not only critical to business, but is now a dominant and increasingly pervasive means of communicating in the office, in the home and on the road. Client devices, countless in number, go everywhere, connecting in all types of environments. Because of their dynamic nature, as we have seen, they are vulnerable, even when deployed with the strongest available security standards.

Enterprises understand that they must secure the boundary between the inside and outside world; what they must in turn recognize is that Wi-Fi increasingly acts as a connection point – or bridge – between the trusted inside network, users and data, and that outside world. And this bridge is literally in the air around us.

Just as with wired networks, wireless security requires stateful inspection and traffic analysis. As enterprises rely more and more on wireless communications to service employees, partners and customers, and, with the advent of 802.11n, make it an integral part of their network infrastructure, they must adopt and leverage dedicated WIPS technology if they are to keep up with the mounting threats across the airwaves.

About AirMagnet

AirMagnet is the leader in security, performance and compliance solutions for wireless LANs. The company's innovative products include AirMagnet Enterprise, the leading 24x7 WLAN security and performance management solution, and AirMagnet Laptop Analyzer – which is known as the "de facto tool for wireless LAN troubleshooting and analysis." Other products provide WLAN site survey and design, RF interference detection, remote diagnostics, and the world's first voice over Wi-Fi analysis solution. AirMagnet has more than 8,500 customers worldwide, including 75 of the Fortune 100.

Corporate Headquarters
830 E. Arques Ave.
Sunnyvale, CA 94085
United States
Tel: +1 408.400.1200
Fax: +1 408.744.1250
www.airmagnet.com

EMEA Headquarters
Science Park Eindhoven 5110
5692EC SON
The Netherlands
Tel: +44 207 942 0721
Fax: +44 870 139 5156