Whitepaper | November 2010

Overlay vs. Integrated Wireless Security

The pros and cons of different approaches to wireless intrusion prevention

There are a few different ways to deploy monitoring systems that scan the airwaves for unauthorized devices and intrusion attempts. Wireless intrusion detection and prevention systems (WIPS) can be built directly into your wireless LAN, for example, using a couple of different approaches. Alternatively, WIPS can run as a standalone, dedicated security system from a third-party specialty company. Each approach has its merits. It's up to the enterprise IT department to understand the tradeoffs so it can appropriately balance the organization's risk profile, depth of security required and budget as it builds an effective, comprehensive wireless security strategy.

AIRMAGNET®
now part of Fluke Networks

Introduction

A well-known best practice in the enterprise is to take a layered, defense-in-depth approach to network security to guard against different kinds of attacks and intrusions. Likewise, the wireless LAN (WLAN) environment requires multiple security layers, too.

Unfortunately, wired security systems do little to protect against 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 could expose corporate data.

IEEE 802.11i security standards do a fine job of authenticating users to the corporate network and encrypting both authentication and user data over the air. The latest WLAN products use encryption and authentication algorithms based on the robust Advanced Encryption Standard (AES), which has been around for many years and has yet to be cracked. So 802.11i provides one layer of the security you need, and it comes already baked into the Wi-Fi Alliance-certified 802.11 equipment you buy.

However, some security issues aren't specifically related to the authentication and data transfer processes protected by 802.11i (also known as "WPA2"). In fact, because Wi-Fi-connected smart phones, tablet computers and laptops store corporate data locally, an attacker wishing to steal corporate data doesn't necessarily have to penetrate the wired side of the network anymore. Many Wi-Fi threats now revolve around client devices and are usually detectable only in the air; in other words, wired-side intrusion detection systems and other traditional security mechanisms won't discover them.

This means that enterprises need a way to uncover and thwart unwanted attempts to do the following: inject denial of service (DoS) attacks into the wireless network; lure Wi-Fi client devices unwittingly to malicious access points (APs); and piggyback onto a user's already-established wireless connection. This is all in addition to detecting attempts by unauthorized ("rogue") APs to connect to the wired network for malicious reasons or for innocent ones that could nonetheless leave a hole in your network security.

Detecting all this activity requires a smart monitoring system that scans the WLAN channels, notifies personnel of any suspicious activity and, sometimes, automatically blocks activity it discovers. One approach is to deploy a dedicated WIPS system from a third-party wireless security specialist. Such systems continually scan all channels with granular depth and have extensive threat libraries that are frequently updated as new threats emerge.

In recent years, some WLAN systems vendors have begun integrating similar capabilities into their systems, too. Procuring monitoring capabilities from your WLAN vendor has some convenience advantages. The primary tradeoff is that WLAN vendors typically provide less detection depth than security specialists. It pays to know the difference before procurement and deployment to avoid a false sense of security.

WLAN-Integrated WIPS

Several of the leading wireless LAN vendors have added WIPS monitoring to their feature sets. There are some basic cost and convenience benefits to procuring these capabilities from the same vendor that's supplying your wireless network infrastructure. Doing so cuts down on the number of vendors you have to manage, for example. And it possibly adds to your volume discount bargaining power with that vendor. Also, the wireless event data collected by the system is likely to be sent up to the same management console that displays information about the status of the rest of your Wi-Fi network, which is convenient.

As noted, though, there is a tradeoff in how much security protection these systems provide. This is because most WLAN vendors offer airwave-scanning sensors that were originally designed as APs for wireless data forwarding purposes, but now can also be configured to run in sensor mode either part time or full time to collect security event information.

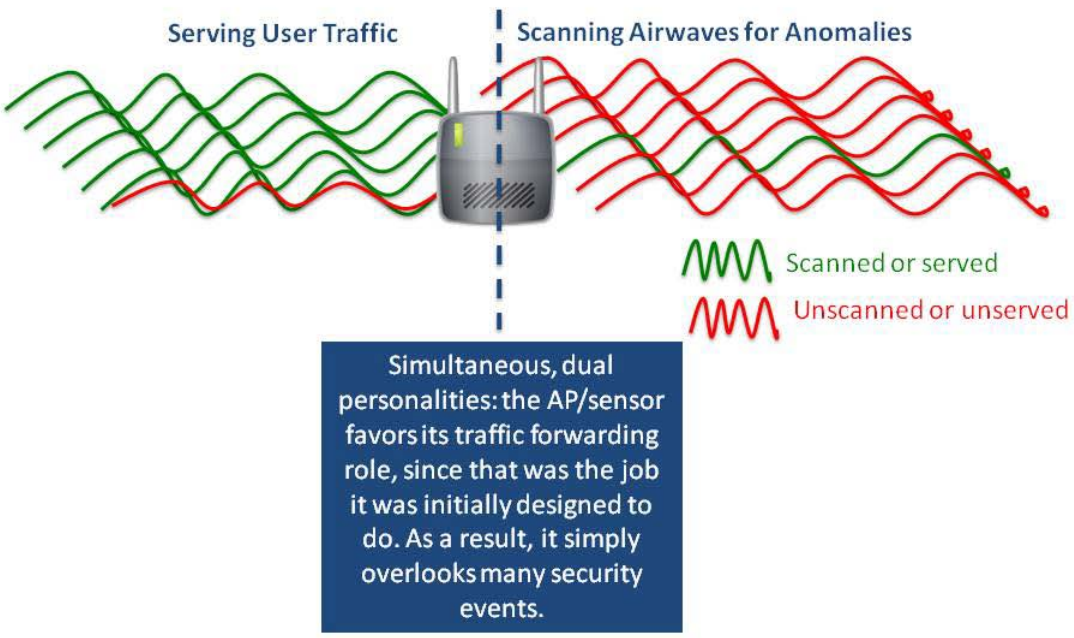
Depending on the environment and the applications in use, the recommended number of sensors to deploy for adequate scanning and detection is one sensor for every three to five APs. However, the ability to assign an appropriate ratio of sensing to forwarding doesn't work if you are using one method of WIPS commonly supported by WLAN vendors called "time slicing."

Time Slicing. This common implementation of WIPS by WLAN vendors is to have regular Wi-Fi APs doing "double duty" as APs forwarding traffic and as security sensors scanning the air for anomalies. This shared AP/WIPS approach is called time slicing, because the data forwarding and WIPS functions quickly alternate based on time.

While it seems convenient and cost effective to get two uses out of one AP infrastructure (data forwarding and security sensing), there are several reasons that the time-sliced approach is falling out of favor. First and foremost, if you are using the same AP radio to perform WIPS functions and serve client data, you are limited in what you can detect and enforce. This is partially a matter of simple math: shared sensors using time slicing end up "listening" for intrusions for less than 1 second per minute. So they miss a lot. And one sensor can't simultaneously serve traffic and block an intrusion.

Because of their limited amount of "listening time," the time-sliced configuration can only catch problems that are obvious and can be conclusively identified by a single packet or two – situations that tend to be few and far between. As a result, the system won't detect the majority of exploits and hacks, and the time-sliced sensors aren't able to gather enough information for the robust compliance auditing and reporting required by governance mandates such as SOX, HIPAA and PCI.

Figure 1: Time Slicing - AP Does Double-Duty as Security Sensor



Vendor-Specific Overlay. However, there are also newer configurations offered by WLAN systems vendors that use what basically constitutes an overlay approach similar to that of a third-party security specialist. In this scenario, a designated number of the vendor's APs operate exclusively in sensor mode and scan for anomalous traffic all the time. This is an improvement over time slicing and also conveniently sends wireless event data to a common WLAN/WIPS security console provided by the WLAN vendor.

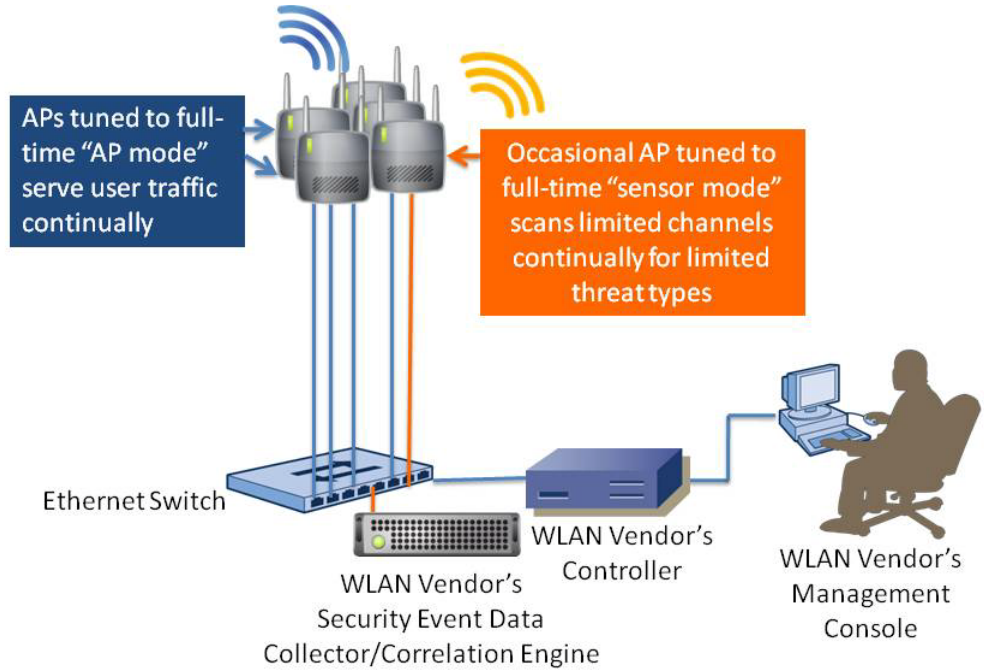
Yet security threats continue to grow more sophisticated, driving a need to examine more data even more deeply and requiring significant processing power. At the same time, the latest 802.11n networks are distributing more and more general networking functions out to the AP to avoid centralized, controller-based performance bottlenecks.

This adds up to APs being asked to consume more resources to perform everyday wireless networking tasks, while the need for more thorough security monitoring is growing. The AP isn't powerful enough to do both well, so configuring it with dual personalities, even if they run one at a time, will result in either lower WLAN performance (particularly of real-time voice and video traffic), less effective security monitoring or perhaps both.

Because an AP has only so much capacity, a number of key capabilities simply aren't supported in these APs-turned-sensors. Among the typical downsides:

- Inability to discover whether a rogue is actually connected to the corporate Ethernet
- Limited threat libraries; the AP-turned-sensor will only identify a subset of threats that actually exist
- Single point of failure. This is a fundamental design flaw, in that a network ingress/egress point such as an AP should not be where security is deployed. There are always ways to compromise a data-serving device such as an AP. Thus, your security and monitoring capabilities could fail every time your network fails if security isn't deployed elsewhere.
- Inability to scan extended channels (see section, "Scanning Frequency Differences: A Biggee")

Figure 2: Integrated WLAN Vendor Overlay with APs Dedicated to Scanning



Depending on the vendor, the overlay WIPS capabilities might entail several layers of equipment, such as a WIPS engine reporting up to a WLAN controller, which reports up to a WLAN controller manager, which, in turn, reports up to a manager of the WLAN controller managers. Such configurations are generally complex, difficult to use and expensive to deploy. They might also show a limited view of a given security issue, rather than multiple perspectives.

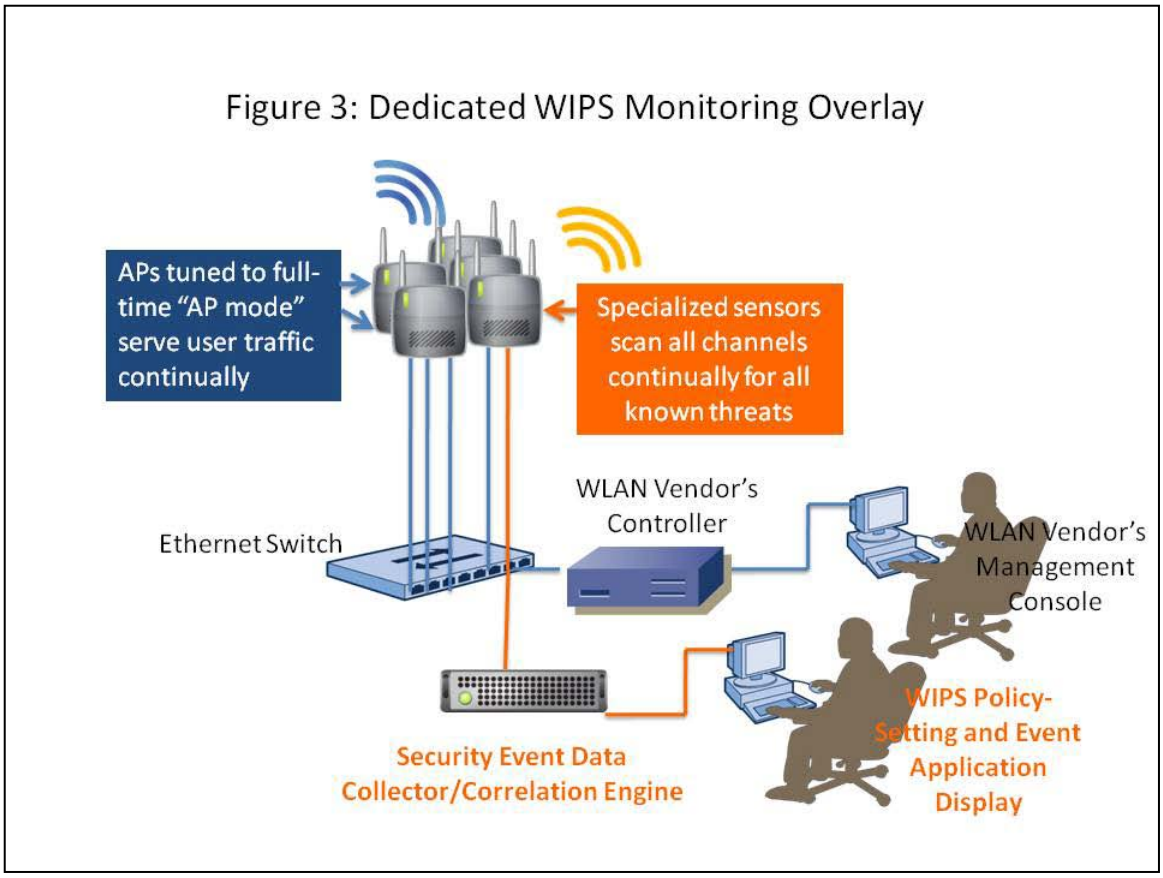
Also, with security just one of many applications being run, security event data can more or less get lost in the shuffle. For example, most WLAN vendor-implemented approaches have limited data retention capabilities and lack the ability for the user to lengthen the retention and data storage window. Keeping the data around for periods longer than 30 days is often important for historical security analysis tracking and compliance auditing.

Dedicated WIPS Overlay

Dedicated WIPS overlay networks offered by a third party do add another vendor for enterprises to manage. However, they are generally the most secure option. Because they were designed specifically to combat intrusions and threats to the wireless network, they have been outfitted with far greater security depth and features. Dedicated systems offer capabilities that generally aren't available in integrated solutions, including the following:

- Comprehensive regulatory compliance reporting
- Forensics for after-the-fact analysis
- Event troubleshooting
- A fully resilient configuration with automatic sensor failover to a secondary WIPS engine, or server, if the primary should fail. In the case of the AirMagnet architecture, for example, security event data can be cached for up to 24 hours in the sensor, and the system will continue to enforce policies even when the connection is lost.
- Recognition of far more threats, including the most sophisticated and potentially dangerous ones

With respect to threat recognition mentioned in the last bullet above, WLAN security is changing rapidly, so threat libraries require regular updates to stay current with the state of the art and changes in the hacking community. New threats could be actual hacks or intrusion techniques, or they could emerge in the form of a new client that is resistant to blocking. By having the security layer separated from the network itself, managers can easily update the security system on demand without risking an upgrade to the entire infrastructure.



Scanning Frequency Differences: A Biggee

One of the most important differences between purpose-built dedicated overlay WIPS and WLAN APs functioning as part-time or full-time sensors is that dedicated systems can continuously scan all channels. This capability is a must for ensuring that no unusual activity goes unnoticed.

APs, by contrast, are allowed by federal regulation around the world to operate only in the channel bands on which data transmission is allowed in that country. So – because they are inherently data forwarding devices – the APs are tuned only to the frequencies they're allowed to use based on the country to which they're being shipped. The other channels are blocked. Because of these rules and resultant blocking, APs can only scan legitimate channels – even though intrusions can occur on any channel. These sensors are thus "blind" to activity on the non-legal channels.

By contrast, dedicated sensors fall under different rules. They are allowed to passively "listen" on all channels because they aren't transmission devices. As such, dedicated sensors are shipped tuned to all frequencies, to which they can listen 24x7. They are thus able to do a much more thorough job.

Cost Perceptions

As noted earlier, integrated WIPS using the time-slicing method can reduce CapEx, because it leverages the existing AP infrastructure for security scanning. It might also reduce CapEx if APs are purchased to run in sensor mode, simply because of increased volume business with a given vendor.

On the other hand, WLAN solutions also require you to purchase additional scanning data collection and management equipment upfront while missing some elements that you'd get with the dedicated overlay. If you're going to have to buy extra equipment anyway, it could be considered prudent to get the full-time security monitoring of all channels that the standalone configuration provides. Otherwise, there could be unpredictable potential security breach costs down the road. In other words, what you may save in CapEx you pay for in increased exposure.

Both AP-based approaches are likely to significantly increase OpEx, though the time-sliced alternative will increase it more. The reason is simply that APs are less adept at the job of security than a dedicated security sensor and corresponding purpose-built monitoring software. As a result, using APs will increase manual involvement of network administrators as they manage WLAN threats. For example, they will deal with a large number of false positives that have them chasing after non-events. More dangerous, they will receive false negatives, implying that no security threats are present, when that might not be the case. And they will conduct physical walk-arounds for most compliance audits using WLAN sniffers running on a laptop or specialized device, because the WLAN-based systems can't support them.

Also, dedicated systems are more likely to have sophisticated capabilities such as forensics analysis, mentioned earlier. This means that when a sensor triggers an event, it copies the packet(s) going by at the time and tags the information onto the actual alarm. Off-line after the fact, network administrators can review an alarm and see the actual frames that were passing by when the alarm triggered. This, too, reduces OpEx by reducing the manual operations required when information is simply missing from the security puzzle.

Note, also, that if you change your WLAN vendor, you will also have to change your security vendor, which will have a cost associated with it.

In the longer term, investment in dedicated WIPS will lower total cost of ownership as compared to integrated WIPS. See the chart below for a basic summary comparison of the three main types of WIPS systems and the primary traits associated with them that can raise or lower wireless security TCO.

Figure 4: Comparative Traits
Dedicated, Time-Sliced and Sensor-Mode AP Systems*

	Dedicated WIPS	Time-Sliced	Sensor-Mode AP
Scanning capabilities	24x7, all legal and non-legal channels	Approximately 1 second per minute, legal channels only (extended channels left unmonitored and exposed)	24x7, legal channels only (extended channels left unmonitored and exposed)
Threat library size	Very Large	Small	Medium
Threat library update frequency	High	Low	Low
No. of false negatives (missed security events)	Low	Very High	High
Comparative CapEx	High	Low	Medium
Comparative OpEx	Low	Very High	High
Comparative TCO	Low	High	High
Compliance reports supported	Many	Very Few	Few

** Typical traits of most suppliers.*

Conclusion

The primary perceived advantage of integrating security into the AP is a cost advantage. However, if using time-sliced WIPS monitoring, enterprises get a false sense of security by looking only at a snapshot of traffic. The tradeoff is a substantial amount of risk, the cost of which is incalculable until an intrusion occurs.

Using an AP with extra radios dedicated to full-time scanning is a stronger alternative. However, APs are vulnerable to single-point-of-failure issues and can't monitor extended channels. And because 802.11n APs support far greater traffic loads than earlier WLANs, networking tasks other than dedicated security monitoring – such as data forwarding, quality of service and roaming – are being distributed out to them to alleviate centralized controllers from becoming bottlenecks. That leaves few AP processing cycles for scanning; again, delivering an "abbreviated" security solution.

There is potentially less upfront capital outlay with the WLAN-integrated systems, particularly the time-sliced approach. However, in addition to part-time scanning leaving the enterprise airwaves largely open and vulnerable, OpEx grows because network administrators must chase down a number of false positive alerts.

Dedicated third-party overlay systems are the optimum choice if an enterprise's requirements for security monitoring are high. The size of threat libraries maintained by dedicated security specialists is large and the sensors from such companies are able to scan all legal and non-legal channels, resulting in the most comprehensive security picture and allowing detailed compliance auditing and reporting.

About AirMagnet

AirMagnet, now part of Fluke Networks, 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 WiFi 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 9,500 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