Whitepaper

Dynamic Wireless Threat Protection

When agility counts

As enterprise wireless networks have matured, effective threat detection and prevention have grown indispensible. But wireless networks are constantly changing in composition and location, requiring nimble defenses that can rapidly recognize and prevent emerging threats. Dynamic security updates have long been a best practice in wired networks. To enable mission-critical wireless deployments while maintaining acceptable security posture, wireless intrusion prevention systems (WIPS) must follow suit, delivering fast, flexible response to zero-day threats, without business disruption.

March 2011

Lisa Phifer, Core Competence Inc.

AIRMAGNET®
now part of Fluke Networks

Introduction

Enterprise wireless LANs have matured into critical network infrastructure, vital to every-day operation. As a result, effective wireless threat detection and prevention have become indispensible. Service outages and security holes, once accepted as a trade-off for mobility, are no longer tolerable.

However, unlike their wired counterparts, wireless networks are highly dynamic, continually changing in endpoint composition and location. A moving target such as this requires a nimble defense that can rapidly recognize and prevent new threats. But a static and increasingly stale Intrusion Prevention System (IPS) could leave an otherwise secure WLAN vulnerable to emerging attacks and exploits for quite a long time.

Dynamic threat updates have long been a best practice in wired networks. In fact, very few enterprises would consider a Unified Threat Management firewall or Network IPS appliance which lacked this agility. To enable mission-critical wireless deployments while maintaining acceptable security posture, Wireless IPS (WIPS) must follow suit. Specifically, a robust WIPS must be flexible enough to incorporate dynamic updates whenever needed to mitigate zero-day threats, without business disruption.

Wireless threat evolution

Contemporary enterprise WLANs bear little resemblance to their predecessors. Long gone are the days when wireless was a casual amenity in isolated areas such as conference rooms and cafeterias, or a point-solution used in warehouses or stores by purpose-built devices. Instead, wireless has become the dominant method of network access, expected to reliably and securely connect a plethora of business and consumer electronic devices, no matter who owns them or where they might roam throughout any kind of workplace.

This evolution from limited casual use to mission-critical ubiquitous adoption has raised the stakes with respect to performance, availability, and security. Businesses cannot rely on WLANs to deliver workforce and application connectivity unless IT can secure them at least as well as Ethernet. Some industry advances have narrowed this gap – for example, robust AES encryption has been required in every Wi-Fi device certified since 2006. But other changes have made securing WLANs more difficult – mostly notably the consumerization of IT.

According to ABI Research, 761 million Wi-Fi products shipped in 2010 – 29 percent more than 2009 – with annual sales expected to top two billion by 2015. Devices with the largest Wi-Fi growth include smartphones, netbooks, TVs and portable music players. Furthermore, mobile device sales now exceed desktop PCs, with the majority purchased by individuals rather than procured by IT. The average employee today carries at least two and often three or more Wi-Fi devices. This explosive transformation means that security can no longer realistically rely on restricting device type or ownership.

In fact, many IT organizations are now being challenged to enroll and enable rather than detect and block unknown mobile devices – including those carried by contractors, customers, and guests who routinely appear and then disappear just as quickly. Increasingly, these visiting devices are more than Wi-Fi clients. From portable personal APs like Mi-Fi's and smartphone hotspots to new de facto standards like Wi-Fi Direct, wireless device populations and inter-relationships are evolving. Any WIPS that cannot recognize such devices for what they really are will either flood IT with false positive alerts or turn a blind eye to potentially risky leaks.

Back when WLANs first hit the enterprise, vulnerabilities and exploits were relatively well-known and static. Attack tools like WEP crackers and Deauth frame generators took advantage of documented 802.11 protocol weaknesses. The most pervasive "wireless backdoor" threats resulted from informal deployments and risky practices, such as rogue or mis-configured APs installed by careless workers, or promiscuous clients silently reconnecting to any previously-used network name (SSID).

Today, every enterprise WIPS – and even a few WLAN controllers – can spot a number of these legacy attacks and typical policy violations. But that's no longer good enough. Emerging wireless threats are more likely to focus on new devices, naïve users, and related mistakes, popping up when and where you least expect, at an ever-faster pace. For example:

- Bugs recorded in the Common Vulnerabilities and Exposures (CVE) database show that new IP-enabled consumer electronics are often rushed to market with code flaws and unsecured interfaces that leave them vulnerable to attack.

- Many wireless adapters and their drivers have fallen victim to fuzzing attempts to identify and exploit faulty frame handling, including buffer overflows that can permit hacker execution of arbitrary code on Wi-Fi client devices.

- Popular new devices such as iPads make it easy for anyone to use Wi-Fi – but in doing so, automate connections and hide previously-used SSIDs, leaving users open to Evil Twins and related man-in-the-middle attacks (e.g., Karmetasploit, Firesheep).

- According to an RSA 2011 panel on advanced persistent threats, criminals that target businesses have started to exploit "harmless" embedded devices like wireless printers and cameras that frequently fly under IT radar and don't run anti-malware.

These are but a few of the emerging threats now facing enterprise WLANs. New attacks and exploits will no doubt continue to be discovered; criminals are always drawn to popular technologies that create large, lucrative targets. However, given enterprise wireless adoption, such threats are too potentially impactful to ignore and too dynamic to thoroughly detect or prevent based solely on yesterday's knowledge.

Next-generation wireless threat protection

Intrusion prevention is widely-recognized as an essential best practice for any business network. Unmitigated intrusions have triggered hefty losses, such as the Heartland Payment Systems breach that compromised 130M records to the tune of $60M. To encourage use, some regulations (e.g., PCI-DSS, FISMA) mandate intrusion monitoring.

A wired IPS monitors traffic over Ethernet by running on an in-line firewall/appliance or by gathering packets from passive sensors tethered to span ports or taps. A wireless IPS extends this by capturing over-the-air transmissions, using Wi-Fi sensors that scan RF channels. In both cases, an IPS not only detects threats – it classifies, locates, and contains them to prevent loss or damage.

But there's a difference between monitoring traffic and determining if it poses a threat. Threat detection methods are often combined to complement each other and offset weaknesses inherent to each.

- Signature-based detection examines traffic (IP packets/fragments, 802.11 frames), searching for pre-defined patterns that match known threats. These signatures are developed using traffic samples from past incidents. Well-written signatures excel at detecting precisely the same threat, over and over. However, signatures can be evaded by variants that incorporate even small differences.

- Another common method is protocol anomaly detection. Here, an IPS searches for traffic that doesn't follow the rules – arriving in the wrong order or making nonsensical requests. Protocol anomaly detection can preempt fuzzing exploits created by hackers who send permutations until they stumble upon a code flaw.

- Some attacks send otherwise legitimate traffic at high rates to disrupt network and business operation. Rate-based detection can stop many different denial-of-service (DoS) threats, including previously-unseen attacks. But poorly chosen rates can also mistakenly block non-malicious usage spikes.

- An IPS can use behavioral analysis to examine clean traffic, searching for deviations from "normal" behavior, assuming that intruders are more likely to exhibit atypical behavior. For example, behavior analysis might detect a device that has always been a client suddenly acting like an AP. This can be useful to spot "zero day" threats but requires establishing a very good "normal" baseline.

- Finally, policy-based detection can be used to warn IT about non-compliant devices and traffic. For example, an IPS may check all detected APs against a policy that specifies security settings for each permitted SSIDs. If the IPS overhears an allowed SSID with the wrong security, it may trigger a compliance alert. Policy-based detection adds value by using context to spot risky behavior.

Each IPS product employs unique methods; detection engines are closely-guarded intellectual property. However, for any IPS, it is clear that signatures are important for efficient, accurate operation. Signature detection is a first line of defense, reliably filtering out many recognized threats so that other methods can better focus on what's left.

However, without proper maintenance, this foundation can grow weak. Frequent, non-disruptive signature updates are required for an IPS to recognize new threats, variants, and exploits. This is why every wired IPS product has long supported this capability.

Surprisingly, the same cannot be said for wireless IPS. For years, every WIPS has relied on static signatures, embedded in detection engines, updated by installing new software. With WIPS releases coming up to a year apart, Wi-Fi threat detection now lags behind protocol advances, threat research, and attack tools. To be truly effective against rapidly-evolving wireless threats, WIPS must become more agile.

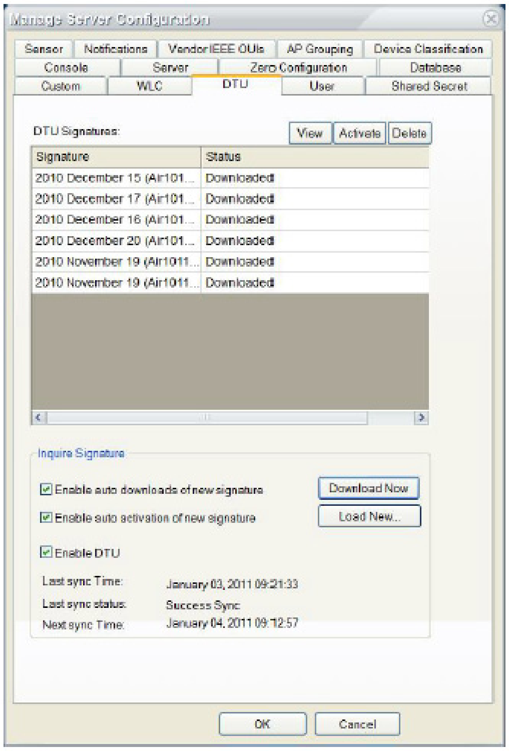
AirMagnet Enterprise Dynamic Threat Update

The latest release of AirMagnet Enterprise (9.0) includes Dynamic Threat Update (DTU) technology which lets customers import new Wi-Fi threat signatures, without installing new WIPS software. De-coupling these definitions from the AirMagnet Enterprise engine helps businesses move more rapidly whenever new threats emerge, without causing any downtime or burdening IT staff.

In AirMagnet Enterprise 9.0, threat definitions were relocated to their own loadable module. New signature files can be loaded manually, or they may be loaded automatically upon download from AirMagnet.

Similar to auto-update controls commonly offered by enterprise anti-malware and wired IPS products, IT administrators can now opt to download new AirMagnet Enterprise signature files on demand or automatically by querying AirMagnet for updates.

Server settings (right) let organizations take advantage of DTU while conforming to their own IT practices. Some will prefer to download and activate new signatures as soon as they are published to minimize zero-day attacks. Others will routinely test all new signatures before production roll-out. Those with air-gapped servers can load signature files offline. DTU is compatible with all of these practices.



DTU Signatures:

Signature	Status
2010 December 15 (Air101...	Downloaded
2010 December 17 (Air101...	Downloaded
2010 December 16 (Air101...	Downloaded
2010 December 20 (Air101...	Downloaded
2010 November 19 (Air1011...	Downloaded
2010 November 19 (Air1011...	Downloaded

Inquire Signature

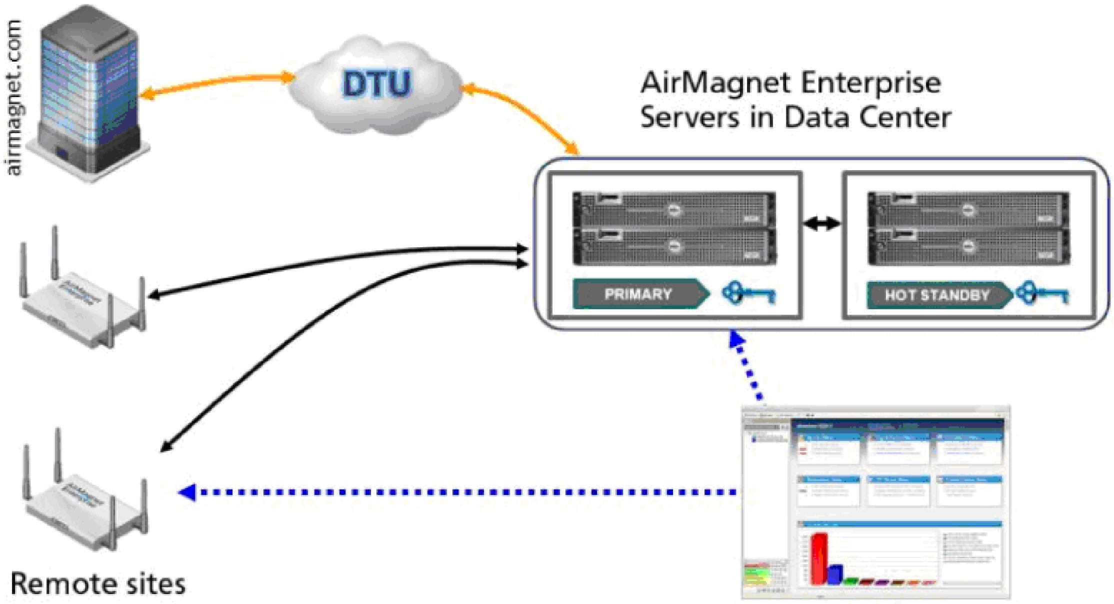
☑ Enable auto downloads of new signature

☑ Enable auto activation of new signature

☑ Enable DTU

Last sync Time:	January 03, 2011 09:21:33
Last sync status:	Success Sync
Next sync Time:	January 04, 2011 09:12:57

To learn about the threats that each new signature file can detect, administrators can view loaded signatures before activating them. Activating a signature file causes it to be added to all existing AirMagnet Enterprise Policy Profiles; all contained alarms are enabled by default. Updated Policy Profiles are pushed to all AirMagnet Enterprise Sensors (local or remote) in the usual fully-automated fashion, without requiring any IT effort or Server restart/reboot.



Once activated, new threat signatures are enforced by AirMagnet Enterprise in exactly the same way as those supplied with any software release. For example, new alarm types will be reflected in charts, roll-up counts, and statistics displayed by Consoles, and new threat descriptions will supplied through the AirWISE screen. Finally, activated signatures can be deleted in the unlikely event that roll-back is ever desired.

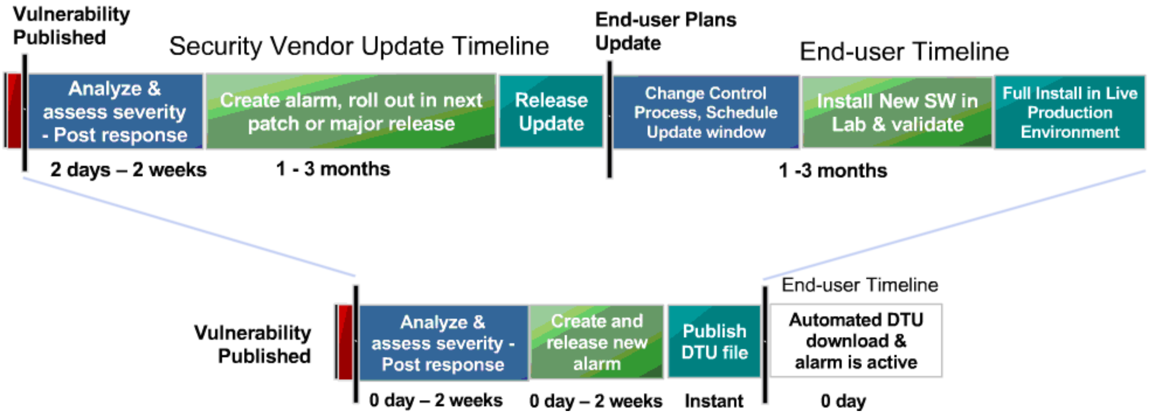
By decoupling threat updates, AirMagnet Enterprise 9.0 becomes a more agile and flexible WIPS. Initially, new signature files will be developed, tested, and published by AirMagnet, based on threat research and customer requests. The AirMagnet Intrusion Research Team continually monitors emerging threats and will now be able to move very quickly to deliver enhanced threat protection in accordance with severity. For example, low severity threats may be bundled into quarterly updates, while high severity threat updates may be published immediately after QA verification.

This DTU technology can be used to develop new signature files that reflect each organization's policies, devices, and sensitivities. To request unique custom signature files, customers may contact AirMagnet. To suggest new signature files of potential interest to many enterprises, visit AirWISE Community Security Center.

Benefits of dynamic threat protection

For AirMagnet Enterprise customers, DTU offers several key benefits. First, this technology can deploy threat updates without disruption, at lower cost. As shown below, industry response to a newly-discovered Wi-Fi vulnerability or attack tool can easily take 6 months without DTU. For example, consider a newly-discovered Wi-Fi vulnerability that is submitted to CERT and published in the CVE database.

In the past, each WIPS vendor would analyze the vulnerability, assess impact, and develop new signature(s) and alarm(s) for inclusion in their next WIPS patch or regularly-scheduled release. Upon receiving updated WIPS software, IT would comply with their organization's processes for software change control and scheduled Server, Sensor, and/or WLAN updates. Given the sensitive nature of WIPS and the potential for downtime or failure to impact mission-critical network services, most enterprises test all updates first in a non-production environment. Only after the WIPS patch or release is verified and installed can that emerging threat be mitigated in a live WLAN. This timeline can be further extended in deployments where APs are used as part-time or full-time WIPS Sensors, due to required collaboration between security and network teams.


Vulnerability Published
Security Vendor Update Timeline
End-user Plans Update
End-user Timeline
Analyze & assess severity - Post response
Create alarm, roll out in next patch or major release
Release Update
Change Control Process, Schedule Update window
Install New SW in Lab & validate
Full Install in Live Production Environment
2 days – 2 weeks
1 - 3 months
1 -3 months
End-user Timeline
Vulnerability Published
Analyze & assess severity - Post response
Create and release new alarm
Publish DTU file
Automated DTU download & alarm is active
0 day – 2 weeks
0 day – 2 weeks
Instant
0 day

As shown above, DTU substantially abbreviates this process, reduces risk, eliminates downtime, and alleviates the burden otherwise imposed on IT. While the back-end of the process remains the same, new threat definitions and alarms can now be bundled into downloadable signature files, deployed in a fully-automated fashion if the organization so chooses. Time-to-mitigate can be reduced to days or weeks rather than months. While major WIPS releases must continue to follow the longer timeline, a network's security posture is no longer held hostage to that far-less-frequent upgrade process.

Additionally, when updating any security system to mitigate an emerging threat, it is critically important to avoid gaps in surveillance. Taking a production WIPS offline to install a software update could temporarily blind an organization to the very threat it is trying to address. There are no such gaps when pushing new Policy Profiles to SmartEdge Sensors. Furthermore, lower cost-to-deploy means that organizations can easily afford broader, deeper threat protection. Not only are published signature files freely available for download by all AirMagnet Enterprise customers, but little or no incremental effort may be required to activate them.

Ultimately, the biggest benefit afforded by DTU is the ability to expand efficient, reliable detection of both security threats and performance events. Over time, DTU is expected to enrich AirMagnet Enterprise by making it easier to address concerns that face the community at large as well as individual companies. For example:

- Many enterprises are grappling with new Wi-Fi enabled devices and how to best deal with them. The first step is to identify what is (trying to) use your WLAN. Signature files can be developed to fingerprint devices, alerting IT to their presence and providing tools to automatically block banned devices.

- As new Wi-Fi devices are adopted, they draw attention from criminals. Signature files can be developed to spot nearly any bit or frame sequence generated by new vulnerability exploits, such as those used to trigger buffer overflows.

- It is not uncommon for WLAN infrastructure vendors to offer proprietary extensions for competitive advantage. However, those extensions can result in mis-configurations that cannot be detected by existing signatures, but that could be detected by custom signatures which search for vendor-specific Information Elements (e.g., Cisco WPA Migration Mode).

- As non-traditional mobile devices become more common in the workplace, enterprises must establish policies for acceptable use. For example, devices have already started to ship with Wi-Fi Direct peer-to-peer technology. Signature files can be developed to detect this kind of activity by detecting new protocol elements and states.

- DTU goes beyond single frame pattern matching; it can also be used to extend rate-based detection – for example, to spot DoS attacks that may well emerge to take advantage of new Wi-Fi products or protocol extensions.

- Today, the rather diverse and often unexpected behavior of Wi-Fi clients is a common cause of performance complaints. In some instances, misbehaving clients may even be mistaken for attackers. New signature files can be used to specifically identify errant clients, enabling more effective trouble-shooting.

- Finally, as enterprises expand Wi-Fi use, they may impose more stringent requirements on device configurations – for example, new EAP types for seamless roaming between Wi-Fi and cellular networks. New signature files can be developed to detect use/non-use of options and settings, helping to enforce policy compliance and mitigate violations.

Conclusion

These examples represent just a few of the security threats and performance events that can potentially be detected and then prevented through Dynamic Threat Updates.

With DTU, AirMagnet Enterprise takes WLAN threat protection to a whole new level. No longer must WIPS be less responsive or agile than its wired network counterpart. By breaking the traditional WIPS dependency between signature and software updates and enabling fully-automated signature file download and activation, AirMagnet Enterprise enables rapid, non-disruptive, dynamic wireless threat protection.

To learn more, visit http://www.airmagnet.com/products/enterprise

About the Author

Lisa Phifer is President of Core Competence, a leading-edge technology consulting firm. She has been involved in the design, implementation, and evaluation of network and security products for over 25 years. At Core Competence, Lisa has advised companies large and small regarding security needs, product assessment, business use of emerging technologies, and best practices. She often teaches about wireless LANs, mobile security, and vulnerability assessment, and has written extensively for numerous publications, including Wi-Fi Planet, Information Security, SearchMobileComputing, EnterpriseNetworkingPlanet, SearchNetworking, and eSecurityPlanet. An AirMagnet user since 2002, Lisa contributes frequently to the AirWISE Community Security Center.

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.

Additional Information

http://www.airmagnet.com
http://www.airwisecommunity.com