

Top Ten Wi-Fi Security Threats

By Lisa Phifer

<http://www.esecurityplanet.com/article.php/3869221/Top-Ten-Wi-Fi-Security-Threats.htm>

March 8, 2010

Gone are the early days of Wi-Fi, when CSOs lost sleep over threats like WEP cracking and war driving. 802.11n products have matured to the point where many enterprises are investing in larger, faster WLANs to support mission-critical applications. And yet, pros know that security is never to be taken for granted. Here, we offer our Top Ten Wi-Fi Threats and explain why diligence is (still) required.

1. **Data Interception:** Today, it's widely understood that data sent over Wi-Fi can be captured by eavesdroppers – easily, within a few hundred feet; even farther with directional antennas. Fortunately, all Wi-Fi CERTIFIED products now support AES-CCMP data encryption and integrity. Unfortunately, there are still legacy products that only speak TKIP, and many WLANs are configured to accept both AES and TKIP. But TKIP is vulnerable to message integrity check (MIC) attacks that allow a limited set of spoofed frames to be injected – for example, ARP. Although resulting risks are modest, the writing is on the wall: The time has come to retire TKIP and require AES-CCMP.

Denial of Service: WLANs are inherently vulnerable to DoS. Everyone shares the same unlicensed frequencies, making competition inevitable in populated areas. The good news: As enterprise WLANs migrate to 802.11n, they can use channels in the larger, less-crowded 5 GHz band, reducing “accidental DoS.” Moreover, contemporary access points (APs) can auto-adjust channels to circumvent interference. But that still leaves DoS attacks: Phony messages sent to disconnect users, consume AP resources, and keep channels busy. To neutralize common DoS attack methods like Deauth Floods, look for newer products that support 802.11w management frame protection.

3. **Rogue APs:** Business network penetration by unknown, unauthorized APs has long been a top worry. Fortunately, most enterprise WLANs now use legitimate APs to scan channels for possible rogues in their spare time. Unfortunately, verifying “true rogues” by tracing their wired network connectivity is a skill that ordinary WLAN gear has yet to perfect. Without accurate classification, automated rogue blocking is a risky proposition. To not just detect, but effectively mitigate rogue APs, deploy a Wireless IPS that can reliably differentiate between harmless neighbors, personal hotspots, and network-connected rogues that pose real danger, taking policy-based action to trace, block, and locate the latter.

4. **Wireless Intruders:** Wireless IPS products like Motorola AirDefense, AirMagnet, and AirTight can also detect malicious Wi-Fi clients operating in or near a business' airspace. However, truly effective defense requires up-to-date, properly deployed WIPS sensors. In particular, 802.11a/b/g sensors must be updated to monitor new 5 GHz channels (including 40 MHz channels), parse 802.11n protocols, and look for new 802.11n attacks. Furthermore, because 802.11n clients can connect from farther away, WIPS sensor placement must be reviewed to satisfy both detection and prevention needs.

5. **Misconfigured APs:** Back when standalone APs were individually-managed, configuration errors posed a significant security threat. Today, most enterprise WLANs are centrally-managed, using coordinated updates and periodic audits to decrease TCO, improve reliability, and reduce risk. But 802.11n adds a slew of relatively complex config options, the consequences of which depend on (highly variable) Wi-Fi client capabilities. Prioritization and segmentation for multi-media further complicates configuration. The answer here: Combine sound, centralized management practices with 802.11n/WMM education and planning to reduce operator error.

Related Articles

- [Review: Motorola AirDefense Wireless VA Tool](#)
- [Honeypots No Longer Effective?](#)
- [Phishers Targeting More \(And Bigger\) Fish](#)
- [Better Wi-Fi Network Security: Advanced Techniques](#)

6. **Ad Hocs and Soft APs:** Wi-Fi laptops have long been able to establish peer-to-peer ad hoc connections that pose risk because they circumvent network security policies. Fortunately, ad hocs were so hard to configure that few bothered to use them. Unfortunately, that barrier is being lifted by "soft APs" in Windows 7 and new laptops with Intel and Atheros Wi-Fi cards. Those virtual APs can provide easy, automated direct connections to other users, bypassing network security *and* routing traffic onto the enterprise network. Measures used to deter Ad Hocs may also prove useful against unauthorized Soft APs, such as IT-managed client settings and WIPS.

7. **Misbehaving Clients:** Clients that form unauthorized Wi-Fi connections of any type, whether accidentally or intentionally, put themselves and corporate data at risk. Some enterprises use Group Policy Objects to configure authorized Wi-Fi connections and prevent end-user changes. Others use host-resident agents and/or WIPS to monitor Wi-Fi client activity and disconnect high-risk connections. However, many businesses (especially SMBs) still depend on end-users to connect only to known, authorized wireless APs. Given ubiquitous deployment, longer reach, and broader consumer electronics integration, accidental or inappropriate Wi-Fi connections have never been easier. If you haven't already taken steps to stop Wi-Fi client misbehavior, start now.

8. Endpoint Attacks: Now that over-the-air encryption and network-edge security have improved, attackers have refocused their attention on Wi-Fi endpoints. Numerous exploits have been published to take advantage of buggy Wi-Fi drivers, using buffer overflows to execute arbitrary commands – sometimes at ring 0 (high-privilege kernel mode). Automated attack tools like Metasploit can now be used to launch Wi-Fi endpoint exploits with minimal effort. Although vendors do (usually) patch these bugs once discovered, Wi-Fi driver updates are not distributed automatically with OS updates. To protect your workforce, track Wi-Fi endpoint vulnerabilities (for example, using WiFiDEnum) and keep your Wi-Fi drivers up-to-date.

9. Evil Twin APs: Fraudulent APs can easily advertise the same network name (SSID) as a legitimate hotspot or business WLAN, causing nearby Wi-Fi clients to connect to them. Evil Twins are not new, but easier-to-use hacker tools have increased your risk of running into one. Tools like Karmetasploit can now listen to nearby clients, discover SSIDs they're willing to connect to, and automatically start advertising those SSIDs. Once clients connect, DHCP and DNS are used to route client traffic through the Evil Twin, where local (phony) Web, mail, and file servers execute man-in-the-middle attacks. The only effective defense against Evil Twins is server authentication, from 802.1X server validation to application server certificate verification.

10. Wireless Phishing: In addition to the above man-in-the-middle application attacks, hackers continue to develop new methods to phish Wi-Fi users. For example, it's possible to poison Wi-Fi client Web browser caches, so long as the attacker can get into the middle of a past Web session – such as by using an Evil Twin at an open hotspot. Once poisoned, clients can be redirected to phishing sites long after leaving the hotspot, even when connected to a wired enterprise network. One technique for mitigating this threat is to clear your browser's cache upon exit. Another possibility is to route all hotspot traffic (even public) through a trusted (authenticated) VPN gateway.

In summary, the state of Wi-Fi security has significantly improved over the years. Today's enterprise WLANs can be effectively hardened against intrusion and misuse. However, end-to-end security still cannot be assumed; just enabling Wi-Fi encryption will not make applications running over wireless networks "safe." Wi-Fi technologies, products, and attacks will continue to emerge. Security admins still need to keep abreast of new threats, assess their business risk, and take appropriate action.

Lisa Phifer owns Core Competence, a consulting firm focused on business use of emerging network and security technologies. A 28-year industry veteran, Lisa enjoys helping companies large and small to assess, mitigate, and prevent Internet security threats through sound policies, effective technologies, best practices, and user education.

