Applying Wired IDS History to Wireless IDS

Joshua Wright

With the increasing number of attacks against wireless networks, many organizations are investigating wireless LAN IDS systems - specialty monitoring systems designed to identify and defend against wireless threats. Small startups are currently dominating this product space, offering organizations the ability to identify rogue APs and clients, active reconnaissance scanning with tools like NetStumbler and targeted attacks that exploit weaknesses in wireless protocols such as LEAP, WEP and TKIP.

However, the WLAN IDS market is still young, and does not have the grizzled experience of wired IDS systems that has influenced today's embattled detection systems. As the WLAN IDS market matures, organizations should consider whether vendors are applying the successes and the difficult lessons of the wired IDS industry to wireless intrusion detection:

Open rules language – Arguably, the feature that propelled Snort to the most powerful IDS system available is the flexible and open rules language. This feature allowed consumers to openly assess the strengths and weaknesses of rules with the ability to augment the supplied rule-base with local additions.
Wireless application – A wise instructor once asked me, "Are we supposed to simply take the IDS's word that the attack was a legitimate attack?" With today's wireless IDS systems, vendors treat their attack signatures as intellectual property and don't disclose the "secrets" of how they detect wireless attacks. This puts consumers at a disadvantage to the attacker; without the ability to assess a specific rule, the organization deploying the wireless IDS is unable to evaluate the robustness of the rule to identify the risk of false-negatives.

Evasion mitigation – In 1998, Tim Newsham and Thomas Ptacek published the landmark paper "Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection", describing a number of techniques attackers can use to evade intrusion detection systems. Shortly thereafter, Dug Song released fragrouter, allowing an adversary to obscure their presence from the IDS system without sacrificing the ability to exploit network targets. One of the most effective techniques implemented by fragrouter is the use of IP fragmentation to slice a packet that would otherwise trigger an IDS signature into several pieces. Without reassembling the fragments, the wired IDS system is unable to identify the contents that would otherwise trigger an alert.
Wireless application – Since WLAN IDS systems are typically focused on layer 2 analysis techniques, it is the responsibility of upstream wired IDS systems to perform IP fragmentation reassembly tasks. However, the IEEE 802.11 MAC specification accommodates fragmentation at layer 2 using the sequence control portion of the 802.11 header. In a recent evaluation of four popular Wireless IDS vendors, I discovered that while vendors were able to identify an EAP-Logoff flood as a denial-of-service attack, none of the vendors were able to identify the same attack when the payload was broken up into two or more fragments, allowing an attacker to easily evade the wireless IDS. While this evasion technique won't work for every wireless attack (it doesn't allow the attacker to fragment the 802.11 header itself, for example), it demonstrates the relative immaturity of wireless IDS systems compared to the wired counterparts.

Logging Fidelity – Seasoned IDS analysts understand that it is necessary to evaluate the alerts generated by an IDS to identify and correlate events of interest. To empower analysts, wired

IDS vendors make as much information about the attack available to the analyst as possible, often providing full packet traces that can be evaluated manually or with other tools.
Wireless application – Unfortunately, wireless IDS systems have not similarly empowered analysts with sufficient logging fidelity to evaluate alerts independent from the capabilities of the wireless IDS. This is quite unfortunate, since the analyst has no information available to make an informed decision about the success or impact of the attack.

Session Countermeasures – Perhaps considered an early intrusion prevention system, Snort and other vendors included the ability to exercise “flexible response” in rules, reacting to an attack by tearing down a connection with a spoofed TCP RST or ICMP Port Unreachable packet. Wired IDS vendors learned early on that it isn't sufficient to send the “teardown” packet only to the attacker; rather, it is necessary to tear down both ends of the connection. By sending the teardown bidirectionally, the IDS mitigates the attacker's ability to ignore the spoofed frames and preserve the hostile connection.
Wireless application – The wireless analogy to wired IDS flexible response has several names including WLAN IPS, Wireless Countermeasures, Session Containment and more. The concept is often the same however; leverage weaknesses in the IEEE 802.11 MAC specification to indefinitely DoS an attacker, preventing them from communicating on the wireless network. In a recent evaluation of this feature however, I discovered that some vendors mount the DoS attack unidirectionally, allowing the attacker to simply ignore the spoofed packets and maintain access to the wireless network. What's more, vulnerable vendors weren't able to identify the sustained connection, leading the analyst to believe that the attacker was successfully contained.

Wireless LAN IDS systems are still an emerging technology, but it is one that more organizations will be relying on in the future to monitor and protect their wireless infrastructure. George Santayana is credited with the oft-repeated line “Those who cannot remember the past are condemned to repeat it”; hopefully wireless LAN IDS vendors don't force their customers to re-live these failures.