

Threat Mitigation Technologies

William H. Wolfe II (7 mins)

I like to spend a few minutes talking about some specific threat mitigation technologies that are available from Cisco to help round up our threat and vulnerability discussion.


So one of the things that Cisco offers specifically, an attack detection mechanism is intrusion detection, and that's actually built into Cisco's wireless LAN controller software, very specifically in that WLC environment that uses the Lightweight access points or controller based access points, and those can be configured to use either local mode or monitoring mode when the access points are configured for the controller.

Optionally, Cisco offers an Adaptive wireless Intrusion Prevention System and that actually requires the Cisco MSE product, and that will also work with either monitor mode or local mode access points.

The wired IPS integration which is part of Cisco's Unified Intrusion Prevention product suite, helps mitigate general network misuses - hacking and malware from wireless LAN base clients. So in this environment, the traffic is actually inspected for harmful applications as well as block wireless client connections in the case of harmful applications. It'll do layer three through seven deep packet inspection. This is actually handled through a Cisco ASA with the Intrusion Prevention System module, or now with the Sourcefire integrated software. This eliminates the risk of contamination from wireless clients and helps to facilitate 'zero day' responses to viruses, malware and the like.

Another technology that Cisco offers is called 'Clean Air' technology, and this 'Clean Air' technology is actually a specific chipset that resides with inside the wireless access points so it doesn't impact any CPU performance or wireless access point performance. This particular chipset helps to identify many RF interferences. Some of those are RF jamming, video camera integration, any type of RF signal that might impact or impede the performance of a proper 802.11 wireless environment. It also monitors the RF signal to maintain a quality RF environment. That's called the air quality monitoring process.

Lastly, as one that we've spoken about briefly, in a couple of our other discussions around threats, and that is Management Frame Protection. So generally speaking, the industry does not support Management Frame Protection as a standard. This is a Cisco enhancement and is available in the wireless LAN controller and, Lightweight or controller based access point configuration.



Basically what the problem is- is that the wireless Management frames which constitute frame such as authentication and association frames, they are not authenticated, encrypted or signed, generally speaking. Therefore, there's a common attack vector that can be used in order to say, for example, force a client to de-authenticate from an SSID unnaturally, and force them to then re-authentic to another SSID that might in fact be a rogue access point or a rogue SSID. So the way that Cisco goes about solving this problem is there is a Message Integrity Code, also known as a MIC that gets inserted into each management frame, and cooperatively the client and the access point will use that MIC code to validate the authenticity of any management frame that is sent and received from either the access point or from the client. This allows the access points to instantly identify rogue or exploited management frames, thus, almost eliminating the ability for a de-authentication or disassociation flame from being propagated in a Cisco Wireless LAN controller based wireless deployment.

In summary, as we go back to our vulnerability and threats screen, our On-Wire attacks and our Over-the-Air attacks can all be detected by the Cisco Intrusion Prevention System technologies, and the non 802.11 attacks can be detected and mitigated through Cisco's proprietary 'Clean Air' technology. So, rogue detection, classification and mitigation will basically address all of the On-Wire attacks. Over-the-Air attacks can be mitigated by using technologies such as MFP - Management Frame Protection and the upcoming discussions that we will have on the use of WPA2 and the IEEE 802.11i advanced security capabilities