

10 TRUTHS

of WiFi RF Layer Security



Cognio provides RF-level analysis tools needed to fill the security holes left by conventional IDS/IPS systems. For more information, please visit www.cognio.com.

Making sense of the risk Layer 1 security for Wireless LANs

By Neil Diener, CTO, Cognio

Truth 1: WiFi AP software can be easily modified to operate on undetectable channels.

The 802.11 standard defines 14 valid channels at 2.4 GHz, and 24 valid channels at 5 GHz. The typical WiFi chipset, however, is able to tune to an arbitrary center frequency in those bands. By changing the software load on a Linux-based AP, a hacker can easily configure an AP that operates at a random center frequency that is not one of those specified by the 802.11 standard.

For a conventional IDS system to detect these off-channel rogues, the system would need to tune to a center frequency every 500 KHz when scanning the band. If the IDS system spent 100 ms on each channel, a single scan of the 2.4 GHz and 5 GHz bands would take four minutes! And if the scanning is done part-time by the WiFi infrastructure, it could take hours.

In the same way they can be tuned off-channel, WiFi chipsets can often be tuned to the edges of the band, operating out-

side the operating frequencies approved by the FCC.

The only effective way to detect APs operating on non-standard center frequencies or on the edge of the band is with spectrum-level sensing.

Truth 2: WiFi APs can also be modified in hardware to be undetectable.

For certain WiFi chipsets, it's possible for hackers to make a board-level modification that inverts the I/Q signals between the radio and baseband chip. Two WiFi devices with their I/Q signals reversed can easily talk with each other, but remain completely hidden to a standard WiFi IDS system.

The only effective way to detect modified WiFi devices is with spectrum-level sensing.

Truth 3: IDS systems don't detect all varieties of WiFi rogue devices.

Older versions of WiFi equipment that pre-date 802.11b are still available on the Internet. These devices are also found in hospitals and industrial environments, where they are used in conjunction with other equipment. These devices are undetectable by current IDS systems, which only detect 802.11b and beyond.

To detect these older devices, you need an RF-level analyzer.

Truth 4: IDS systems don't detect other non-WiFi rogue devices.

Bluetooth AP devices are popular in Europe, and can operate at power levels and ranges equal to those of WiFi. In



“Older versions of WiFi equipment that pre-date 802.11b are still available...are found in hospitals and industrial environments... and are undetectable by current IDS systems.”

Neil Diener

order to reliably detect rogue Bluetooth devices, you need to be able to both detect that Bluetooth is present and reduce false alarms by filtering out Bluetooth voice devices, such as cellular headsets.

In addition, there are HomeRF and HyperLAN devices out on the market. These are similar to old WiFi equipment—devices based on standards that have been relegated to the dustbin.

The only way to detect these non-WiFi rogues is with an RF-level analyzer.

Truth 5: A proprietary wireless bridge is an even bigger threat.

Many non-WiFi wireless bridging devices operate in the unlicensed band but use proprietary protocols—some examples would be systems from Alvarion, Motorola, and Trango. These devices represent a significant threat to your RF security because the bridges are actually designed to transmit signals up to miles away from your building! That means that a rogue transmitter in your building could be sending a signal to a transmitter beyond your ability to see it.

The only way to detect proprietary bridges is with an RF-level analyzer.

Truth 6: Rogue RF devices can also operate in other bands.

There's more than just the 2.4 and 5 GHz bands to worry about. First, there are numerous proprietary LAN and bridging devices that operate in the unlicensed 900 MHz band. These devices are all rogue threats.

Beyond the unlicensed band, you need to consider the licensed bands. Many laptops now have 3G cellular cards that can act as accidental bridges into your network, and 3G cellular backhaul products are beginning to come onto the market. These cellular products operate in the 800 MHz or 1.9 GHz bands in the U.S. and 900 MHz and 1.8 GHz in Europe. Over the next year, WiMax systems will also become an increasing threat. WiMax radios will exist in all laptops, and there will also be backhaul and bridging products. The WiMax radios will operate at 2.5 GHz in the US, and at other frequencies elsewhere.

The only way to detect devices in non-WiFi bands is with an RF-level analyzer.

**Proprietary Wireless Bridging Systems**

Outdoor systems that will cause problems with Wi-Fi networks indoors, and can be used to hack into otherwise secure networks.

Truth 7: WiFi denial-of-service attacks occur most easily at the RF level.

WiFi is designed to be a polite protocol, using the “listen-before-talk” algorithm. For this reason, WiFi devices will not transmit when there is other noise in the spectrum. This means that a jammer signal (which broadcasts a continual or very fast sweeping signal across the whole band) effectively shuts down WiFi altogether.

In fact, this is the reason that management frames were not even authenticated. The 802.11 standards body reasoned that even if they protected management frames (such as de-authorization frames, which knock a client off the network), it would always be possible for someone to shut down a WiFi network using an RF jammer.

The only way to detect jammer devices is with an RF-level analyzer.

Truth 8: WiFi RF jammers are very easy to come by.

Several new, inexpensive jamming devices have emerged for sale on the Internet, making it quite easy for a malicious hacker to cause network failure. In addition, the Queensland Attack and other hacker software is able to turn certain WiFi cards into jammers by putting them into diagnostic modes. The threat of physical layer denial-of-service attacks is on the rise due to the increasing number of mission-critical enterprise Wi-Fi networks.

If your WiFi system is mission critical, you need to monitor for jamming attacks.

Truth 9: RF-level security threats require RF-level analysis, and most IDS systems don't have it.

IDS systems will all say they monitor your RF. But you need to read their claims carefully to make sure they really have spectrum-level monitoring—that means going beyond using a standard WiFi chip for listening. They need custom hardware to perform spectrum analysis and detect the threats outlined above.

Truth 10: Security specialists need RF-level analysis tools that are easy to use.

Chances are, your security staff is not made up of RF scientists. They don't want a \$40K spectrum analyzer with wiggly lines. They want tools that work 24x7, and that can name and locate intruding devices.

Cognio is the only company with spectrum analysis technology that is easy to use and easy to embed in this way. Cognio's custom SAgE chip is able to do what a spectrum analyzer can do (and more) in a very small form factor. The SAgE chip is available in a laptop-ready solution, Spectrum Expert for WiFi, that enables security staff and network engineers to see lists of devices causing interference. Spectrum Expert also features graphs and charts that clearly show the effect of interference on your network, and it includes an RF “Geiger counter” for zeroing in on the location of malicious devices.

Cognio provides the RF-level analysis needed to fill the security holes left by conventional IDS solutions. For more information, please visit www.cognio.com.

10 Truths of Wi-Fi RF Layer Security

Truth 1: WiFi AP software can be easily modified to operate on undetectable channels.

Truth 2: WiFi APs can also be modified in hardware to be undetectable.

Truth 3: IDS systems don't detect all varieties of WiFi Rogue rogue devices.

Truth 4: IDS Systems systems don't detect other non-WiFi Rogue rogue devices.

Truth 5: A proprietary wireless bridge is an even bigger threat.

Truth 6: Rogues RF devices can also operate in other bands.

Truth 7: WiFi Denial-of-service attacks occur most easily at the RF level.

Truth 8: WiFi RF Jammers jammers are very easy to come by.

Truth 9: RF-level security threats require RF-level analysis, and most IDS systems don't have it.

Truth 10: Security specialists need RF-level analysis tools that are easy to use.



20400 Observation Drive
Suite 206
Germantown, MD 20876
+1 301 540 4900
<http://www.cognio.com>