

# New risks in 802.11n

Security expert identifies emerging wireless vulnerabilities

[Wireless Alert](#) By Joanie Wexler , Network World , 07/16/2008

Sponsored by:

Along with the potential performance and coverage benefits of 802.11n come a few new security risks, says industry security guru Joshua Wright. Wright presented a Webinar last week that outlined several new vulnerabilities that high-speed 802.11n networks introduce.

Wright, who has spent a decade ferreting out wireless security attacks (Compare [WLAN Security](#) products), is an instructor for the SANS Institute, an information technology watchdog organization that offers information security training, certification and information resources. He's also a senior security researcher at Aruba Networks.

Here are a few 802.11n vulnerabilities he highlighted:

## \* **Wireless intrusion detection system (WIDS) gap.**

If using channel bonding to transmit across 40MHz channels (recommended primarily for the channel-abundant 5GHz band), it will take WIDSs twice as long to scan the frequencies for malicious patterns as it did to scan earlier 20MHz channels. The situation effectively doubles the time a hacker has to penetrate a given frequency until the scanner makes its way around to that frequency again – from about 4 seconds to about 8 seconds, Wright says.

## Related Content

Viewed another way, in a 20MHz channel, an attack must last about 4 seconds to be detected; in a 40MHz channel, it has to last 8 seconds. What kind of attack could be mounted in 4 to 8 seconds? “Mostly driver exploits [see below], which are 1- or 2-packet attacks,” says Wright.

## \* **Driver exploits.**

Wright says there is “lots of vulnerable code out there driven by the [industry] frenzy to get 802.11n into the hands of users. When you have a driver vulnerability, a hacker can gain administrative access.”

Of possible help here is a free tool from Aruba called the WiFi Driver Enumerator (WiFiDEnum). Using a database of known wireless vulnerabilities, WiFiDEnum assesses the versions of installed drivers and produces a vulnerability report, identifying systems and specific drivers that are at risk to wireless driver exploit attacks.

## \* **No protection yet for “block” acknowledgements (ACK).**

IEEE 802.11n introduces a mechanism to acknowledge a block of packets, instead of individual packets, identified by a beginning and ending sequence identifier. “This block ACK mechanism is not protected; any attacker can spoof one of these messages and create an obscenely large window within which frames can be sent with no ACK,” thereby creating an 802.11n denial-of-service vulnerability, says Wright. At this juncture, “There is no fix for this mechanism,” he says.

This document was created with Win2PDF available at <http://www.daneprairie.com>.  
The unregistered version of Win2PDF is for evaluation or non-commercial use only.