



At RSA, Some Security Pros Don't Practice What They Preach

Dark Reading

By Tim Wilson

March 5, 2010

http://www.darkreading.com/vulnerability_management/security/encryption/showArticle.jhtml?articleID=223101624&cid=RSSfeed_DR_News

SAN FRANCISCO -- RSA Conference 2010 -- You'd think the behavior of wireless users at one of the industry's biggest security conferences would be -- well, secure.

Not so, says a quick study from wireless security company Motorola AirDefense.

In a study during the first two days of the show, AirDefense identified 293 wireless access points -- but an alarming 315 ad-hoc networks were also discovered.

Ad-hoc networking is a mode of operation that allows two stations to communicate directly with each other, without the use of an access point. This could allow an attacker to impersonate a common service set identifier (SSID) and potentially gain connectivity to the wireless station, AirDefense observes.

Some 116 wireless clients were found to be associated to these ad-hoc networks, many offering security-risky SSIDs, such as "Free Public WiFi," "Free Internet Access," "Hotel WiFi," and "lounge."

While there was more encryption at this year's conference than last year, the majority of the networks using encryption were found to be using technologies known to be vulnerable to attack. Sixty-two percent were using WEP -- which was cracked years ago -- or TKIP, for which researchers have rolled out several proofs of concept research during the past two years. The recommended encryption is AES/CCMP.

More than half of the 2,444 wireless clients were found to be probing for multiple SSIDs, or the name of the wireless LAN. This approach makes these stations vulnerable to evil twin, hotspotter, and man-in-the-middle (MITM) attacks, AirDefense says. More than 1,000 of the devices were Apple, and 206 were running RIM, the BlackBerry operating system.

AirDefense advised Windows administrators to push out policies to desktop/laptops that disable ad-hoc support and disable the command to "automatically connect to nonpreferred networks." Similar settings can be found in other operating systems, the company says.

On the open networks, AirDefense discovered Web-based email conversations, as well as other infrastructure data. "Many Web-based email sites provide for a secure login, but once logged in, the email application is clear text," the company says. "These vulnerabilities expose Web

applications, Web-based email, and critical infrastructure devices. Encryption should be used whenever possible."

Identity theft by media access control (MAC) spoofing was observed from some wireless clients, AirDefense says. "This can sometimes be an indication of malicious users impersonating a legitimate access point or station, with the goal of performing MITM attacks or bypassing access point security mechanisms," the report says.

AirDefense also spotted examples of one of the newest wireless attack vectors. SSID SQL Injection attacks were identified coming from four different sources at the show. By injecting SQL code into the SSID portion of a frame, one can potentially gain a back door into the AP, allowing the attacker to change configurations and gain access to the broader network, the company says.