



Security Products Magazine

March 11, 2010

http://secprodonline.com/articles/2010/03/11/study-wireless-security-rsa.aspx?sc_lang=en

Study Examines Wireless Network Security At RSA

Motorola AirDefense performed wireless security monitoring at the RSA 2010 conference. Leveraging its Wireless Intrusion Prevention System platform and wireless security expertise, Motorola AirDefense collected and analyzed the security of the wireless networks present at the show.

The monitoring was conducted from Day 1 through Day 2 of the conference (March 2-3.) The following is a summary of the findings from the two days. No attempts were made to interrupt or decrypt traffic at the show.

In terms of the infrastructure, 293 Access Points were identified, while an alarming number of Ad-hoc networks (315) 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 SSID and potentially gain connectivity to the wireless station. 116 wireless clients were found to be associated to these ad-hoc networks using common SSID's (Service Set Identifiers) such as "Free Public WiFi," "Free Internet Access", "UCSB wireless web", "Hotel WiFi", and "lounge".

This year, a higher average number of access points (86 percent) were found to be using encryption.

This is an improvement over last year's show where a significant number of conference access points were found to be open with no encryption.

The majority (63 percent) of the networks using encryption were found to be using encryption types known to be vulnerable to attack. WEP has been cracked for years, and TKIP is becoming increasingly vulnerable due to ongoing proof of concept research over the last 2 years. The recommended encryption is AES/CCMP.

The survey also revealed that a good percentage of the wireless networks were using WPA-PSK (pre-shared key) authentication. WPA-PSK is known to be vulnerable to dictionary attacks.

Use of 802.11n enabled access points still appears to be low, but 802.11a appears to be more common this year, perhaps due to wider availability, and is advantageous for people looking to use a less congested spectrum (5GHz).

More than half of the 2,444 wireless clients were found to be probing for multiple Service Set Identifiers (SSIDs), or the name of the wireless LAN.

This makes these stations could be vulnerable to evil twin, hotspotter, and MITM (Man in the Middle) attacks). These included laptops, PDAs, and phones with Wi-Fi support. In fact, 1034 of the devices were Apple and 206 were RIM devices.

For those devices using Microsoft Windows, it's recommended that administrators push out policies to desktop/laptops that disable Ad-Hoc support and disable "Automatically connect to non-preferred networks."

Similar settings can be found in other operating systems.

On the open networks, web-based email conversations were discovered, amongst other infrastructure data. Many web-based email sites provide for a secure login, but once logged in the email application is clear text. Numerous web-based emails from hotmail, gmail, and Yahoo! were discovered. 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. This can sometimes be an indication of malicious users impersonating a legitimate access point or station with the goal of

performing Man in the Middle (MITM) attacks or bypassing access point security mechanisms. This was evidenced by the number of Ad-Hoc networks and Soft APs discovered at the show.

One of the more recent wireless attack vectors was also discovered. SSID SQL Injection attacks were identified coming from four different sources at the show. By injecting this into the SSID portion of a frame, one can potentially exploit vulnerable access points. This can then allow a backdoor into the access point and allow the attacker to change the access point configuration, thus allowing them open access to the network.

A variety of wired traffic was found to be leaking from the wireless networks as well, including: NetBIOS, STP, IPX, and IGMP. The unencrypted routing protocols reveal the inner workings of the network and are visible to anyone sniffing the traffic, also known as a form of Extrusion.

This is a clear indication that firewall or filtering mechanisms are inappropriately configured and allowing undesirable traffic to leak from the wired networks. This information could be used by a hacker to enumerate the wired network and read information clear-text. Numerous Windows system names and usernames were enumerated during the analysis. All of this traffic should be properly blocked by a firewall by blocking not only incoming traffic (wireless to wired), but also outgoing traffic (wired to wireless).

Motorola AirDefense's wireless security survey at the RSA 2010 Conference revealed that common vulnerabilities continue to exist within wireless infrastructures. Clearly the best approach to these ongoing problems involves continued user awareness, leveraging stronger encryption and authentication options available in access points, improving the security posture in layers of defense such as firewalls, and a wireless intrusion prevention system to detect and block intrusion attempts