



**February 9, 2007**

## **AirDefense completes RSA Conference wireless network monitoring: half of wireless devices vulnerable to attack**

Wireless security firm AirDefense Inc. today released results from its wireless airwave monitoring yesterday at the RSA Conference, the world's leading information security conference.

For three consecutive days AirDefense studied the wireless LAN traffic from the show floor.

Yesterday, it discovered 309 out of 547 wireless devices such as laptops, PDAs, phones and vendor PCs susceptible to Evil Twin types of attacks combined with some of the latest zero-day attacks.

In total, 1,137 out of 2,017 wireless devices over a three day period could have easily been compromised.

“It is important for people to understand that the vulnerability of 309 wireless devices on Thursday, 481 devices on Wednesday and 347 devices on Tuesday was not the problem of RSA Conference organizers,” said Richard Rushing, the firm's chief security officer.

“Any compromised devices at this year's conference resulted from conference attendees who joined a wireless network through hotels and hotspots that were insecure.”

AirDefense's wireless airwave monitoring discovered more than 90 wireless chipset driver attacks being conducted at the show to compromise inspecting laptops.

Denial of Service attacks slowed down with AirDefense noticing 47 different attacks on Thursday versus 85 on Wednesday trying to disrupt the wireless network, from CTS flooding of the airwaves to de-authentication types of attacks, to jamming attacks.

AirDefense noticed that many clients, when connected to an unencrypted network, would disclose information about the organizations networks such as Domain, Authentication Server, Active Directory, User Name and Computer Name in the clear.

Leaking out NetBIOS and IPX traffic was common on these devices.

“An Attacker could and might have captured the corporate username and authentication hash (password), that the unsuspecting user would have sent over the airwaves,” the company said.

“As the laptop is not aware of its location, it does not know if it is at the office, home or hotspot. This has the potential to worsen as the number of laptops and wireless laptops become more prevalent than the corporate computer.”

Further information is available at [www.airdefense.net](http://www.airdefense.net).