

RE: Dumb question abt. Wireless WEP security

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-01/0328.html>

From: Shawn Jackson (sjackson_at_horizonusa.com)

Date: 01/22/04

Date: Thu, 22 Jan 2004 12:25:15 -0800

To: "Vizo Bilisim Ltd." <vizo@vizo.com>, <security-basics@securityfocus.com>

After being a wireless engineer for over a year I'll offer some humble advice. The Cisco Aironet LEAP system, or any system that will rotate pre-designed keys after a while can be broken, it just takes a lot longer. I haven't tired to hack a wireless network in over a year so I don't know if the technology improved any, but when deploying wireless you need to think of more then WEP the placement and technology of your devices matters a lot. You can use WEP in coordination with other technologies, VPN, IPSEC, etc to make your network more secure. For customer (SMB/SOHO) locations we used normal WiFi gear. We used MAC control, disabled the broadcasting of the SSID and enabled WEP and that was a good 'secure by default' solution. The attacker would need to guess the SSID, then get around the MAC control then guess the WEP key before being able to get access to the network. Still not the most secure but fine for most people out there.

At a 'big' business deployment we used two Aironet 350's to bridge to distant buildings. The buildings were at a fairly remote location and no 'other' people were between the two buildings. We ran at 2.4Ghz (which is clear in that 'small' area) and used directional Yagi antennas to complete the connection, which kept the signal in a directional and controlled manor. The antennas were mounted in front of a wall so the signal pretty much stopped at the wall. You only had a little play between the two yagi's before your signal faded, which was security all on its own. We also used the LEAP/WEP Rotation and other Cisco features to secure the connection. Using materials to 'soak up' the signal you can prevent the signal from propagating and keep it extremely controlled. Some of the casino's in my area use this technique and you would have to be floating in mid air right between the buildings to even see the signal.

The wavelength of a 2.4Ghz band transmitter is smaller then that of say a 5Ghz. Basically the lower you go the smaller 'footprint' your signal has. So the 2.4Ghz signal can pass through more things then the 5.0Ghz signal. We proved this true when using our two wireless internet broadband products at the ISP I worked for. Basicall