

Re: VPN vs. Cisco LEAP for wireless security ?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-04/0101.html>

From: Lanwench [MVP – Exchange] (lanwench@heybuddy.donotsendme.unsolicitedmail.atyahoo.com)

Date: 04/01/03

From: "Lanwench [MVP – Exchange]" <lanwench@heybuddy.donotsendme.unsolicitedmail.atyahoo.com>

Date: Tue, 1 Apr 2003 13:59:58 -0500

Can't take credit for this answer – ran yer Q by my husband & business partner and he wrote you a nice little novel in response!

Apples and oranges, my friends...but both are still in the fruitbasket.

<or>

The answer is that neither is a complete solution.

LEAP in a corporate environment is not a question of "if" or of "what else" as it would be plainly nuts to do otherwise. LEAP can tie into you're A/D, so you can use ordinary remote access policies to determine who could even use the wireless, and then (assuming you have adequate user account password strength policies) assure that only authorized users could get in.

LEAP would accomplish a number of things—namely if properly configured (along with properly configured access points and wireless clients) it would significantly security harden the basic wireless transport itself, and allow integration into access control and auditing mechanisms such as RADIUS.

Steps/What Each Would Accomplish:

1. Use LEAP/if properly configured would prevent someone from even getting an IP address if they do not possess proper credentials—KEEP OUT THE ORDINARY HACKS. Scrubs at this level can do no harm/compromise no data if they can't get past the front door.
2. Do not let broadcast SSID associate. Keep out the total neophytes.
3. Use Aironet Extensions, the latest version of the client and access point firmware, and the latest client software and driver, use MMC hashing and automatic WEP key rotation/The former addressed the initial 40 bit vulnerability to WEP, restoring it to near 128-bit encryption strength. The latter if configured with a fairly short interval (say 10 minutes tops) would have each client automatically renegotiate/change the WEP key in use on the fly on that interval, making a hack/decrypt pretty much impossible up

microsoft.public.security: Re: VPN vs. Cisco LEAP for wireless security ?

to and including the NSA—not enough traffic would exist on any given
dynamic key to len