New tool cracks most enterprise wireless LANs

If your company or organization runs an enterprise wireless LAN network, I have some troubling news for you. Odds are high that your current "enterprise-class" wireless LAN deployment is vulnerable to authentication leakage which not only exposes your internal network but all of your server access controls.

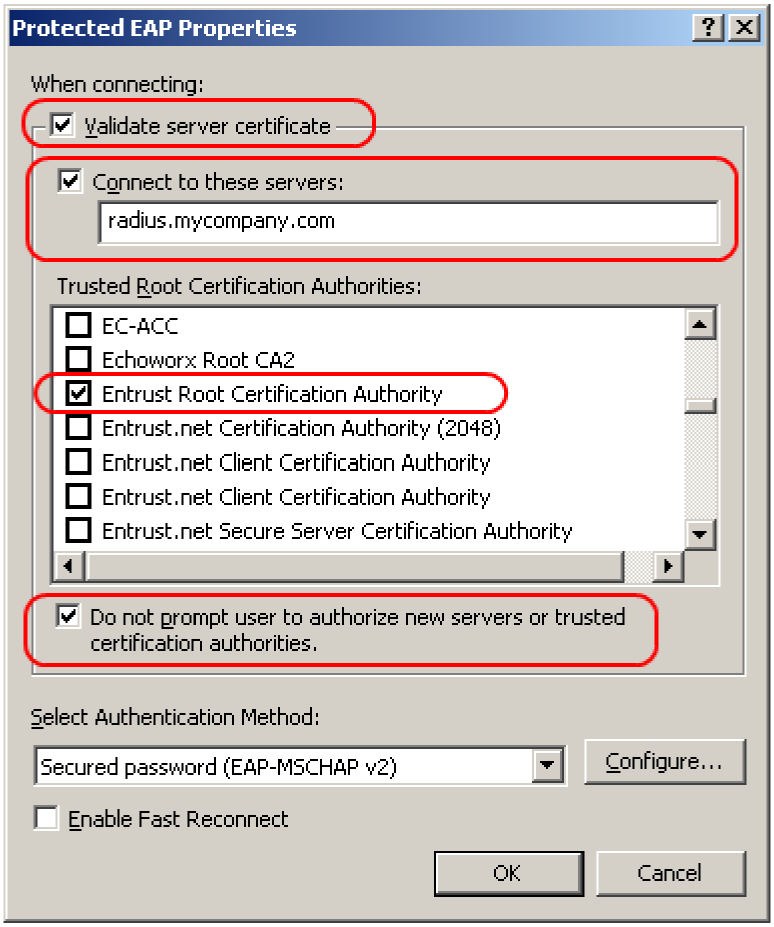
You can use all the strongest authentication protocols such as PEAP, EAP-FAST, or EAP-TTLS and the strongest encryption algorithms like AES, but you're still easily vulnerable because of poor wireless client design. Mainstream wireless clients from Microsoft, Apple, and Funk software make it impossible for normal people to discern when they're being tricked. They provide so little pertinent information to the user that they qualify as a fairly serious design flaw in the client TLS implementation.

The problem with the wireless LAN EAP authentication is that there is no natural and intuitive way to match the name on the digital certificate to the SSID name. More specifically, the "subject" field (AKA CN "Common Name" or DN - "Designated Name") on the server's digital certificate can be anything you want to call it. Most organizations will at least have some part of their company name in the certificate and if the certificate is purchased from a commercial Certificate Authority, then the domain name must be at the end of the subject field.

HTTPS clients (Web Browsers) by contrast don't have this problem since they automatically match the domain in the URL address to the subject field in the digital certificates. So when a user goes to SSL/TLS secured https://secure.mybank.com and the certificate subject field contains secure.mybank.com, a nice little lock icon lights up and assures you that some trusted entity like VeriSign or Entrust certifies that you're really at secure.mybank.com. But for a wireless client that utilizes a TLS-based EAP authentication, it's not so simple. If you see a Wireless network with an SSID called "MyCompany", the certificate might be ".some.cryptic.corporate.IT.name" which looks nothing like the SSID.

Microsoft's Windows XP SP2 client and Vista when deployed using Group Policy offers the highest level of lockdown possible if the administrator knows how to lock it down. The standalone configuration of the Microsoft wireless client on the other hand is not only confusing, but it's flawed because of the fact that it hides the certificate name from view. When the user is presented with a new certificate and all it shows is VeriSign trust network but the name on the certificate "hacker.from.anywhere" is hidden from view, they can easily be fooled in to making the connection.

However, Windows XP SP2 and Vista do allow you to lock things down so that the user will never be prompted by fake RADIUS servers but that depends on proper user configuration which can't always be depended on. To make it easier on you, see the following screen shot to see what you need to lock down. You can also look at my guide on enterprise wireless LAN security which teaches you how to manually or automatically deploy these settings and a whole lot more.



Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

radius.mycompany.com

Trusted Root Certification Authorities:

□ EC-ACC
□ Echoworx Root CA2
☑ Entrust Root Certification Authority
□ Entrust.net Certification Authority (2048)
□ Entrust.net Client Certification Authority
□ Entrust.net Client Certification Authority
□ Entrust.net Secure Server Certification Authority

☑ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect

The key things to ensure is that

- Validate server certificate is enabled
- The "Connect to these servers" field in the wireless supplicant specifies the subject field in the X.509 digital certificate AKA CN or DN. If that's confusing to you, you're not alone. Additional server names can be entered separated by a semi-colon. Note that in my enterprise wireless LAN security guide, I don't specify this field but it's ok to leave out in a very specific situation. If you use a private certificate authority and lock down the certificate authority and you don't prompt users for new servers or certificate authorities, you don't have to have this field populated. But if you use a public signing authority, you must have this field locked down.

- The CA (certificate authority) must be specified whether it’s a public CA or your own private CA.
- The “do-not-prompt user to authorize new servers or trusted certificate authorities” option was a key enhancement to the Windows wireless client. Funk’s Odyssey client also has this security feature but it’s missing from other wireless LAN clients like Mac OS X. Letting users add additional certificate authorities is extremely dangerous.

To drive this point home, security researchers Joshua Wright and Brad Antoniewicz have produced a weapons-grade penetration tool called FreeRADIUS-WPE that exploits these deployment weaknesses. Why would they release such a thing? To raise awareness since no one ever cares about these things until they see it with their own eyes or they read it in the news. Without the tool, the massive problem still exists and can be exploited with less convenient but still effective methods but no one actually does anything about it since it’s not on their list of things to audit for. Now that the tools are public knowledge, security auditors will have to use FreeRADIUS-WPE to perform penetration testing on their own networks before the bad guys get to them first.