

RE: [fw-wiz] Link level security with static arp tables

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-10/0109.html>

From: Ben Nagy (*ben_at_iagu.net*)

Date: 10/15/03

To: <firewall-wizards@honor.icsalabs.com>

Date: Wed, 15 Oct 2003 16:11:56 +0200

> -----Original Message-----

[Magosanyi Arpad]

> *If real authentication, integrity and confidentiality is needed,*

> *I would do IPSEC. Any other (or same) ideas?*

[This is Paul]

[Strong reservations expressed, but IPsec is]

> *a viable alternative, as is a gateway between*

> *user segments*

> *and backbones similar to those found in airports and coffee*

> *shops isn't all*

> *that bad an idea (or an authenticating firewall...)*

I know....how about SOCKS!

Seriously, we're just indulging in over-engineering here. However, if I were doing it for a strong security environment I have grave concerns about IPsec. Hard to install, hard to maintain, ugly protocol at the best of times and at the basic level it only does machine-level authentication.

The Microsoft IPsec/Kerberos implementation is a better approach, but we all know there are lots of interop and fast-and-loose standards problems. At least it tries to authenticate the user and the station, which is a big step in the right direction.

Frankly, in a real world environment that needed strong security along these lines I would apply a combination of good physical security, no active unused wall-points and the switch Port/MAC thing. All external access would be via a proxy which can authenticate each user. A circuit level gateway really is a good match for this problem. If only SOCKS didn't suck. :)

If I can't have any physical security I vote for 802.1x over IPsec. The problem with the IPsec thing is that the attacker is physically able to see

Firewall-Wizards: RE: [fw-wiz] Link level security with static arp tables

and interfere with traffic and we rely on our technical controls to deal with it from there. 802.1x starts with the port in a null VLAN where the attacker sees nothing.

I am not aware of how PEAP is "known broken" for this kind of application (assuming one takes just a little care), and I'm not sure it will go away. If anyone has any good stuff to point me at I'd be interested in discussing this aspect further. I am, of course, familiar with the IETF draft. [1] I agree that I much prefer EAP-TTLS [2], since it's a cleaner design, but "word on the street" has it that PEAP is looking more likely to emerge as market victor.

ben

[1] <http://www.ietf.org/internet-drafts/draft-puthenkulam-eap-binding-03.txt>

[2] <http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-03.txt>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>