



The New WLAN Security Paradigm

Pat Calhoun

Dan Harkins

Eugene Chang

Michael Maggio

David Piscitello, Moderator



Where are we, today?

- Standards have improved
 - Authentication
 - Privacy and Integrity
- Products have evolved to
 - Integrate wired and wireless networks
 - Provide realtime monitoring and analysis
 - Optimize RF and mobility
- Are we 'there' yet?



Airlink Security

- Can I get by with WEP?
- How often do I need to renew a key to effectively harden WEP?
- What does it mean to harden WEP?
- Is it OK to use WEP if I use 802.1x/EAP and eliminate static keys from the picture?



802.11i

- Now that 802.11i is completed, do I have all I need to make my network secure?
- What is the difference between WPA and WPA2?
- What is the story behind FIPS and 802.11i?
- Are WPA and WPA2 really available?



802.1x

- What is the difference in workload between EAP authentication and traditional login methods?
- Is there enough 802.1X software to make the switch from security gateways and VPNs?
- Can small-and-medium businesses really afford the cost of implementing 802.1x?
- Why are there so many EAP methods? Does it matter which one I use?
- What does 802.1X deployment in wired Ethernets buy me?
- Why don't public hot spots use 802.1X?



Whither VPNs?

- Can I really retire my VPN for wireless security when I deploy 802.11i?
- Why should I use more expensive WPA or WPA2 equipment when:
 - VPNs are mature and inexpensive
 - VPNs are not limited to WLANs
- What secure tunneling method works well and scale for both my WLAN roamers and mobile workforce?



Monitoring WLANs

- What impact can location tracking have on WLAN security?
- Is it necessary to have an wireless monitoring overlay network?
- How can I detect rogues APs connected on my network?
- What is "Evil Twin"?



“Out-of-band” security issues

- How do neighboring WLAN's affect my wireless environment security?
- What measures can an enterprise take to avoid accidental associations with outside APs?
- What risks are commonly associated with Ad-Hoc connections?



Do I really need to secure a WLAN...

- If my data are already secured (by VPNs) for all connections?
- If I don't care about bandwidth lost to visitors and 'drivers'?
- Can unauthorized users of a network create liability problems for my organization if I don't take measures to secure my WLAN?

What's still missing from
wireless security?

