Home Wireless Security

David Mitchell
12/11/2007
Home Wireless Security

- Why?
- Open
- WEP
- WPA
- WPA2
Why?

- If you live in a house, your wireless network probably reaches to your neighbors.
- If you live in an apartment, your wireless network certainly reaches your neighbors.
- Check your laptop. Can you see your neighbors wireless?
Why?

- What are the risks?
- Most likely is simply 'theft' of your service.
- If the neighbors just do email and light web surfing, you would be unlikely to notice.
- If you don't notice, do you care?
- If your neighbors do much p2p downloading of music or movies, your connection may slow to a crawl. Then you would care.
Why?

- Less likely but more serious risk is legal trouble.
- There is a minuscule chance your neighbor would get the attention of the police by downloading child porn, hacking banks, emailing threats to the President, etc.
Why?

- Slightly more likely is an RIAA filesharing lawsuit.
- Over 20,000 have been filed as of July, 2006
- If your neighbor uses your network to run their P2P applications, the RIAA may come after you.
- You probably won't like the effect on your network speed either.
Why?

- Just because there are risks doesn't mean you have to lock down your wireless.
- Lots of individuals and businesses run open networks. In many cases, intentionally.
- Coffee shops have them to increase business.
- If you don't see a benefit, you should enable security to minimize your risk.
WEP

- Wired Equivalent Privacy is the security in the original standard.
- Supported by almost every 802.11 device.
- Unfortunately, contained fatal design flaws.
- Off the shelf tools can crack it passively in days, or actively in minutes.
Many devices began including '128' bit WEP instead of the 40 bit specified in the standard. Each additional bit makes it twice as hard to crack in theory. Or 295,147,905,179,352,825,856 times. Previously mentioned flaws means its about three times as hard instead.
WPA

- Interim 'standard' for wireless security.
- Addressed the most severe flaws in WEP
- Compatible with most older hardware
- Uses the same RC4 encryption cipher that WEP uses
- Has both Enterprise and Pre Shared Key (PSK) modes.
WPA2

- WPA2 is the current standard defined via IEEE 802.11i.
- Replaces RC4 cipher with stronger AES cipher.
- Also has both Enterprise and PSK modes.
If you decide to protect your wireless, what should you do?

- Disable SSID 'broadcast'.
- Use the newest encryption supported by your devices.
- Use a really random passphrase.
- MAC address filtering: don't bother
What To Do?

- Disable the network 'SSID' broadcast.
- This doesn't increase security by much if any.
- If you aren't going to let people use your network, there is no reason for it to advertise itself.
- Akin to turning your porch light off on Halloween if you aren't giving out candy.
What To Do?

- Use the strongest security available on all your devices. Prefer WPA2 over WPA over WEP.
- WPA is available for XP SP1 and OSX 10.3
- WPA2 is available for XP SP2 and in OSX 10.4.
- If you have WEP-only devices, consider replacing them.
What To Do?

- Use PSK (Pre Shared Key) mode.
- May also be called “Personal” mode.
- Enterprise mode would require you to run an authentication server at home.
- Passphrase is subject to offline guessing attacks, so it should be really random.
- You only have to type it in a few times so you don't have to be able to remember it.
Wi-Fi Protected Setup

- Newest addition
- Tries to make it really easy to enable security in a home environment
- Mandatory mode is to enter a PIN from the wireless card into the access point
- Another is to have a button on both client and AP which must be pressed to enable them to sync up.
Questions?

- Any questions?