Wireless Security

By Donald Jolley

donald@dwc.za.net

Intro to Wireless World

- PAN – Bluetooth; Infrared – 5 to 100m
- LAN – 802.11a/b/g Wifi – 50m – 20km
- WAN – 802.16 WiMax, 3G – up to 50km

802.11a

- 54Mbits
- 5 Ghz
- Many channels
- Expensive
- Shorter range
- Less interference

802.11b

- 11Mbits
- 2.4Ghz
- 11-14 channels
- Cheap
- Much interference with other devices
- Can connect to 802.11g devices if WiFi certified

802.11g

- 54Mbits
- 2.4Ghz
- 11-14 channels
- More expensive then 802.11b
- Can connect to 802.11b
- Interference

Wireless networking

- Is it worth setting up a wireless network? Is it needed? Will it serve the purpose vs the risk.
- Don’t need to lay cables
- No physical boundaries
- Slower then cable
- Can push WiFi long distance

Choosing Hardware

- What do you want to use it for? Indoor/outdoor. Range?
- What’s your budget?
- You get what you pay for.
- Check the product/firmware features
- Security options, WPA2, WPA, RADUIS
- Connection options: AP, client mode, WDS
- Other features you may need eg, QoS, Fire walling

Increasing the distance of your link

- More power from unit – mw
- External antenna – db
- Cable and connectors – low loss
- Correct channel selection
- Polarization of antenna

What is War driving?

What fun can you have with Wifi

- People looking for open networks
- Steal data and bandwidth
- Sniff data at hotspots
- Setup Honey Pots
- Pushing the boundaries of Wireless – Distance / meshing

Figures

- 2 Hour drive in Durban reviled
- 371 Networks
- 188 Networks not Encrypted (50.6%)
- 183 Networks Encrypted (49.4%)
- 11 default (3%)

Myths

- Wireless is vulnerable
- MAC authentication is enough
- Encryption is enough.
- Hiding you SSID will stop them.

Is Wireless Vulnerable ?

- Only 1% of attacks came from wireless
- 49% can from the Internet
- A well setup network is difficult to break
- More though is put into protecting a wireless network. Spare points on wired network?

Secure your network

- Change the admin password
- Turn Off DHCP
- Put on MAC authentication
- Turn on Encryption WPA2, WPA, WEP 256, 128, 64
- Transmit as far as you need to
- Use secure protocols
- Tunnel. PPTP, IPsec, VPN
- Be aware of SSID name
- Monitor

Links

- http://www.dwc.za.net – Durban Wireless Community
- http://www.remote-exploit.org – Auditor Website
- http://www.tomsnetworking.com/Sections-article118.php – WEP crack part 1
- http://www.tomsnetworking.com/Sections-article120.php – WEP crack part 2