802-**Not-**11

The Forgotten Wireless Device Threats

Brad “RenderMan” Haines
Hacker / Security Consultant
RenderLab.net, Churchofwifi.org, NMRC.org
render@renderlab.net

CONfidence 2010
November 29-30th, 2010
http://www.renderlab.net/projects/presentations


HELLO
my name is
inigo montoya
you killed my father
prepare to die

Who Am I?

Who Am I?

Consultant – Wireless, Physical, General Security

Author – 7 Deadliest Wireless Attacks, Kismet Hacking, RFID Security, etc

Trainer – Wireless and Physical security

Who Am I?

Consultant – Wireless, Physical, General Security

Author – 7 Deadliest Wireless Attacks, Kismet Hacking, RFID Security, etc

Trainer – Wireless and Physical security

Hacker – Renderlab.net

Security Researcher

Hacker Group Member – Church of Wifi, NMRC

Frequent Speaker – Defcon, Westpoint Military Academy, HOPE, etc

Wireless Networks

- Wireless networks are everywhere
- We've gotten pretty good at the basic security of standard 802.11 networks
- WEP: Sucks
- WPA-PSK: Better, but has issues, showing wear and tear
- WPA-Radius: Best, but more complex than other solutions, not easy for home use
- Security is an issue that has been addressed for years, the message has been received

Wireless Devices

- Wireless devices are everywhere
- We all use them all day everyday without thinking about them
- Wireless, Cordless, radio, etc. Many different names
- These devices pose risks to security
- These devices are often overlooked

Bluetooth Threats

- Old threat, still relevant
- Issue is not with the protocol, mostly the implementation
- If device is on discoverable with default PIN, anyone can connect
- Paired devices get access to whole device
- Read/Write SMS, Phonebook, notes, images
- Remote AT commands on some models
- Premium rate calls

Bluetooth Threats

/home/render/Dropbox/Defcon 16/Last HOPE/Bluetooth_scam.avi

Apologies to Major Malfunction

Bluetooth Threats

- Cheap headsets use default PIN
- Bluebump and re-pair
- Listen to conversations: Boardroom bug
- Inject audio (car whisperer): Make people think they are crazy
- We already think they are crazy...

Eavesdropping on Headsets

/home/render/Dropbox/Defcon 16/Last HOPE/Eavesdropping on Bluetooth Headsets.AVI

I Hate Headsets

/home/render/Dropbox/Defcon 16/Last HOPE/BlueTooth fun.AVI

Bluetooth Bad Ideas

- Bluetooth Access points allow network access via Bluetooth network profile
- Do you audit for Bluetooth devices?
- Does your wireless IDS cover Bluetooth?
- Other devices that make you go WTF?
- It's not discoverable but...
- Who thought this was a good idea

'The Toy'


Imagine...
a shared naughty secret...
tease...please...excite...control...
from anywhere in the world with a simple text message...

'The Toy'

- Bluetooth enabled vibrator, 'reacts' to special SMS messages when paired to a compatible phone
- Each character has it's own reaction
- thetoy.co.uk

Stopping Bluetooth threats

- Turn off Bluetooth or just discoverability
- Change default PIN
- If possible, limit access to paired devices
- Prompt for pairing
- Turn off headsets when not in use
- Consider the security implications of your devices
- Scan for unauthorized Bluetooth devices along with WiFi

DECT Phones

- Older cordless phones, baby monitors
- Next gen are supposed to be secure, right?
- Old issues with new twists

DECT Phones

- Digital Enhanced Cordless Telecommunications (DECT)
- Digital, 1.9Ghz, Very flexible standard
- Encryption is in the DECT standard
- Encryption not mandatory.....
- Many manufacturers not implementing crypto, its cheaper not to
- Marketing touts DECT's security, but they aren't using it. No external indications of this

DECT Phones

"Looks Like I Picked The Wrong Week To Stop Sniffing Glue" - Steven McCroskey - Airplane

- Hackcon, Norway, February 2010
- When I get bored, bad things happen
- Fired up deDECTed and started sniffing
- Not long to find something interesting
- Not long until I got scared...

DECT Phones

- Caught several unencrypted phone calls in progress, recorded the results
- Unfortunately encrypted to me (Norwegian)
- Had native speaker listen and select a clip without any identifying details
- Realized where I was and the potential gravity of the situation
- Got out of the country successfully!
- Scared to go back!

DECT

- www.dedected.org
- Uses cards no longer available
- Wardriving for phones
- Not popular in the US, yet...

Infrared Device Threats

- Used everyday by most everyone here
- Old, Simple, ubiquitous
- Infrared light pulsed in sequence to issue commands, transfer data, etc
- Television remotes most common use
- No encryption or authentication on most if not all
- How to make life interesting....

Gizmodo at CES 2008

/home/render/Dropbox/Defcon 16/Last HOPE/Gizmodo_CES.avi

Passports

Passports

- New RFID passports can be easily read at a distance
- Encryption not very strong
- Key made up of details on the photo page = limited keyspace
- Even US “Tin Foil Hat” doesn't work well

Passports

/home/render/Dropbox/Defcon 16/Last HOPE/passport.avi

GSM Cell Phones

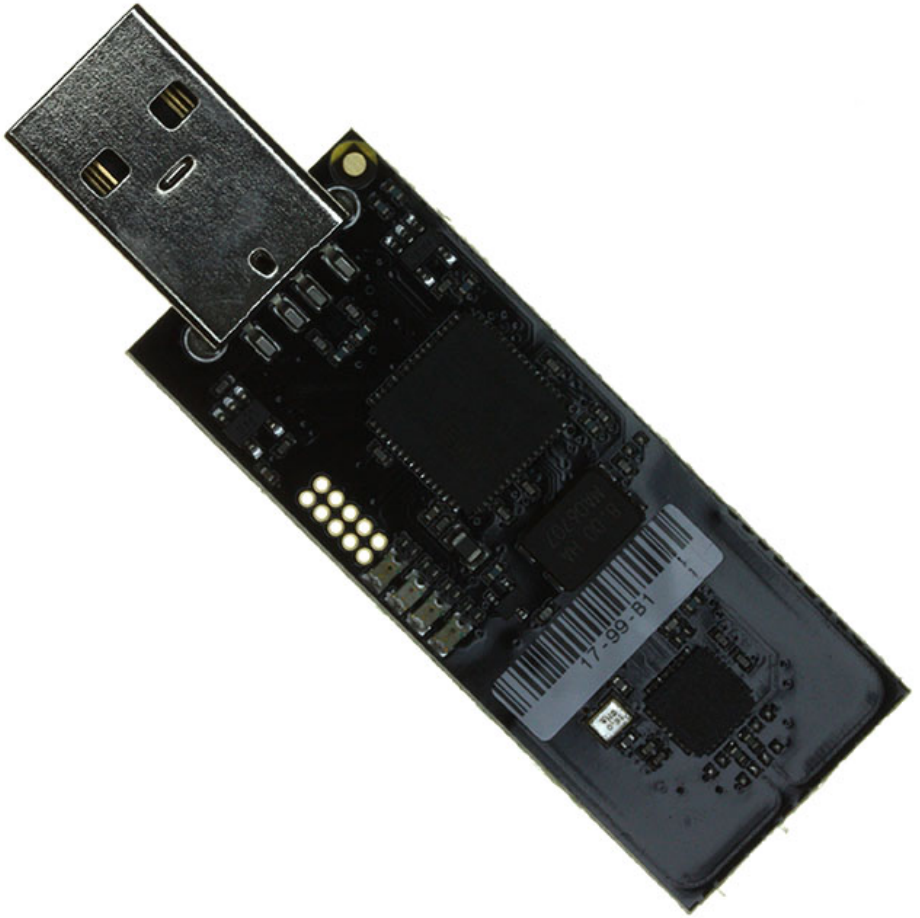
- Rough cost of $1500 for USRP
- OpenBTS, Laptop, antennas = Your own Cell Tower
- Chris Paget debuted at Defcon 18
- GSM is encrypted: A5/1, A5/2
- Encryption not mandatory
- Handsets supposed to inform about unencrypted connections. They don't due to user confusion issues
- Attacker is the strongest tower nearby

GSM Cell Phones

- Your phone automatically switches to attackers cell tower
- Negotiates A5/0 (Cleartext)
- Literally now the man in the middle
- Can impersonate any companies cellsite with ease
- 3G calls safe, except for 100 Watt jammer
- Data safe for now, but give it time....
- Great talk to watch to learn

Zigbee Threats

- Zigbee, 802.15.4
- Basis for “Smart Grid”
- Virtually no security
- Easy to sniff, inject, manipulate
- Adapter ~$40
- Killerbee framework, Kismet plugin
- willhackforsushi.com



Analog Radio Threats

- Traditional analog radio is often forgotten
- New tools forget old school threats
- Old cordless phones the worst culprit
- Older analog headset mics, newer stage mics
- It's a radio, it broadcasts beyond the intended receiver
- Conference mics broadcasting private talks

Conclusion

- Know what your devices can do and how they can be defeated
- Understand the risks and evaluate the threat
- Why are you going wireless in the first place?
- Look around and see what you do every day

Thanks

render@renderlab.net