Shifting the Focus of WiFi Security:

Beyond cracking your neighbor's wep key

Who are we and why do you care?

- Thomas “Mister_X” d'Otreppe de Bouvette
  - Founder of Aircrack-ng

- Rick “Zero_Chaos” Farina
  - Aircrack-ng Team Member
  - Embedded Development
  - FD: Also works for a WIPS Vendor

DISCLAIMER:

Some of the topics in this presentation may be used to break the law in new and exciting ways…

of course we do not recommend breaking the law and it is your responsibility to check your local laws and abide by them.

DO NOT blame us when a three letter organization knocks on your door.

History of WEP Attacks / Why it doesn’t work

- Passively Sniff for a long time
  - Slow, not enough data, impatient
  - No more weak ivs
- Replay/Injection Attacks
  - Fast but very noisy
  - Simple signatures
  - AP features that try to block (PSPF)

History of WPA Attacks / Why it doesn’t work

- Pre-shared key
  - Requires catching both sides of a quick handshake
  - Must be in range of client and AP
- Enterprise
  - Nearly impossible to crack passively
  - Most EAP types are difficult (at best) to MiTM

The Well Guarded Door

- Nearly 100% of attacks focus on the AP
- APs are getting more and more secure
- New features built into AP
  - PSPF / Client Isolation
  - Strong Authentication / Encryption
  - Lightweight controller based architecture
- APs are no longer the unguarded back door
  - Well deployed with for thought for security
  - Well developed industry best practices

Take the Path of Least Resistance Attack the Clients!

- Tools have slowly appeared recently
- Difficult to use
- Odd requirements to make function

Attacking Client WEP Key

- Wep0ff
- Caffe-Latte
- Caffe-Latte Frag

Attacking Client WPA Key

- WPA-PSK
  - No public implementation
- WPA-ENT
  - Freeradius-wpe (thanks Brad and Josh!)
  - Requires hardware AP

Attacking the Client

- Many Separate Tools
- Difficult to configure
- Typically sparsely documented
- Odd requirements and configurations

Until now…

Introducing Airbase-ng

- Merges many tools into one
- New and improved, simplified implementations
- Full monitor mode AP simulation, needs no extra hardware
- Easy, fast, deadly (to encryption keys at least)

Airbase-ng Demo

- Evil Twin / Honey Pot
- Karma
- WEP attacks
- WPA-PSK attacks
- WPA-Enterprise attacks (if completed in time)

What are you, a blackhat?

- No seriously, this doesn’t promise a win
- There are ways to defend as well
- APs are finally being configured securely, now clients must be as well

Simple Defenses

- Proper Secure Client Configurations
- Check the right boxes
- GPO
- (Still in process of completing this section, please download final slides from link at the end of presentation)

Beyond the Basics

- Wireless Intrusion Detection and Prevention
- Systems designed to detect attacks and sometimes even prevent them
- (Full explanation of WIPS systems and features will follow, with no vendor bashing, however Rick is still gaining permissions required by his employer so this section will be left uncompleted for now)

A Step Beyond Crazy

- WiFi Frequencies
  - .11b/g 2412-2462 (US)
  - .11a 5180-5320, 5745-5825 (US)
- Does this look odd to anyone else?

Licensed Bands

- Some vendors carry licensed radios
- Special wifi cards for use by military and public safety
- Typically expensive
- Requires a license to even purchase
- Frequencies of 4920 seem surprisingly close to 5180

Can we do this cheaper?

- Atheros and others sometimes support more channels
- Allows for 1 radio to be sold for many purposes.
- Software controls allowed freqencies

Who Controls the Software?

- Sadly, typically the chipset vendors
- Most wifi drivers in linux require binary firmware
- This firmware controls regulatory compliance as well as purposing

What can we do?

- Fortunately, most linux users don’t like closed source binaries
- For many reasons, fully open sourced drivers are being developed
- As these drivers become stable, we can start to play

Let’s Play…

- Madwifi-ng is driven by a binary HAL
- Ath5k is the next gen fully open source driver
- Kugutsumen released a patch for “DEBUG” regdomain
- Allows for all supported channels to be tuned to

New Toys

- Yesterday
  - .11b/g 2412-2462 (US)
  - .11a 5180-5320, 5745-5825 (US)
- Today
  - .11a 4920-6100 (DEBUG)

What to do now?

- What is on this new frequencies?

(insert full image of frequency map)

- But does it really work?

Spectrum Analyzer Demo

- Fully tested frequencies
  - (finish complete testing)

- Warning: This may differ from card to card

Limitations

- Many real licensed implementations are broken
- Card reports channel 1 but is actually on 4920MHz
- This is done to make is easy to use existing drivers
- This breaks many open source applications

Airodump-ng

- Airodump-ng now supports a list of frequencies to scan rather than channels
- Only channels are shown in display, may be wrong
- Strips vital header information off of packet so data saved from extended channels is useless

Kismet

- At time of writing is unable to handle most of the extended channels
- Displays channels not frequencies
- Does save usable pcap files

Improvement Needed

- Sniffers are two trusting, they believe what they see
- Never intended to deal with oddly broken implementations such as channel number fudging
- Sniffers need to be improved to report more reality, and less assumptions

Final Thoughts

- Remember everyone here is a white hat
- Please use your new found knowledge for good not evil
- In the United States it is LEGAL to monitor all radio frequencies (except those used by cell phone)
- Have fun…

Thanks

- Updated Slide Presentation can be found at: http://www.aircrack-ng.org/defcon16.ppt

- Bibliography
  - http://www.willhackforsushi.com/FreeRADIUS-WPE.
  - etc