Wifi Security

Nick Kartsioukas

What's wifi?

- Communicate using the MAGICAL POWER OF THE ÆTHER!
- 802.11: 1997, 2mbit/sec, 2.4GHz
- 802.11b: 1999, 11mbit/sec, 2.4GHz
- 802.11a: 1999, 54mbit/sec, 5GHz
- 802.11g: 2003, 54mbit/sec, 5GHz
- 802.11n: 2009, 72-300mbit/sec, 2.4/5GHz
- 802.11ac: 2013, 100-1300mbit/sec, 5GHz

What's a gigzahurt?

- Cycles/second (Hertz) of a radio signal
- Wifi is channelized, 20/40/80/160MHz wide channels
- 2.4GHz has 70MHz bandwidth in 11 channels
  - Only 3 non-overlapping (1, 6, 11)
- 5GHz has 665MHz bandwidth, in 45 non-overlapping channels
  - 30 are DFS, have special requirements to prevent interference with RADAR

What do I need for teh wifis?

- Ad-hoc
- Bridged
- Infrastructure
  - AP
    - ESSID
  - Client(s)
  - All traffic goes via AP

MOAR DETAIL PLZ

- Management frames
  - Association request/response, beacon, auth/deauth…
- Control frames
  - Power save, RTS/CTS…
- Data frames
  - Payload, QoS, ACKs…

How do I keep people from mooching?

- Security!
  - MAC filtering
  - WEP
  - WPA
  - WPA2

What's WEP?

- "Wired Equivalent Privacy" (lol)
- 64/128-bit seed (24-bit IV + 40/104-bit shared key)
- RC4 stream cipher
- CRC32 integrity check
- Open or handshake authentication
- "Weaknesses in the Key Scheduling Algorithm of RC4", Fluhrer, Mantin and Shamir, 2001
  - Related key attack, exploits small IV keyspace (16.7M)
  - Key recovery in a short time (minutes on a busy network)

Well that's terrible…how about WPA?

- "Wifi Protected Access"
- Sort of fixes WEP…kinda?
- Uses TKIP
  - Key mixing instead of straight concatenation
    - Dynamic session key
    - Session key + IV -> RC4
  - Sequence numbering
  - 64-bit message integrity check
    - 2 invalid MICs in 60 seconds triggers session key rotation
    - Rotation requires a 60-second timeout, DoS anyone?

Didn’t you mention WPA2?

- Totally new design
- CCMP
  - Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
  - AES block cipher
  - PBKDF2 to generate encryption key from PSK

That sounds great!

- Well…
- WPS
  - Wifi Protected Setup
  - PIN-based key exchange

What about large environments?

- 802.1x
  - LEAP
  - PEAP
  - EAP-TTLS
  - EAP-TLS

How are they broken?

- aircrack-ng
  - WEP, WPA, WPA2
  - deauth, replay, injection, fake AP, capture
- John the Ripper
  - Wordlist
- hashcat
  - GPGPU brute-forcing
  - Wordlist, rule engine
- crunch

How do I keep others out?

- WEP – Yeah, no chance, don't use it
- WPA – Meh. Why bother?
- WPA2 – Long, strong passphrase or random string
  - Except "correct horse battery staple"
  - pa9ieweesuphaeRoo0eephoo2ahdohgo1IeZ3QuohVoo1ithiel0ooZieng2iec
  - COOK^feed&middle_shine!December
- WPA2-Enterprise
  - PKI + RADIUS

Where do I learn more?

- http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/
- 802.11, 802.1x, and Wireless Security https://www.sans.org/reading-room/whitepapers/wireless/80211-8021x-wireless-security-171
- Hacking 802.11 Basics: https://www.youtube.com/watch?v=zxs0sclPEfg
- Wireless Pentesting: https://www.youtube.com/watch?v=kMq7uzWY_jI
- Aircrack-ng tutorials: http://www.aircrack-ng.org/doku.php?id=tutorial

Where do I find you?

- Twitter, @explodinglemur
- github.com/explodinglemur/presentations