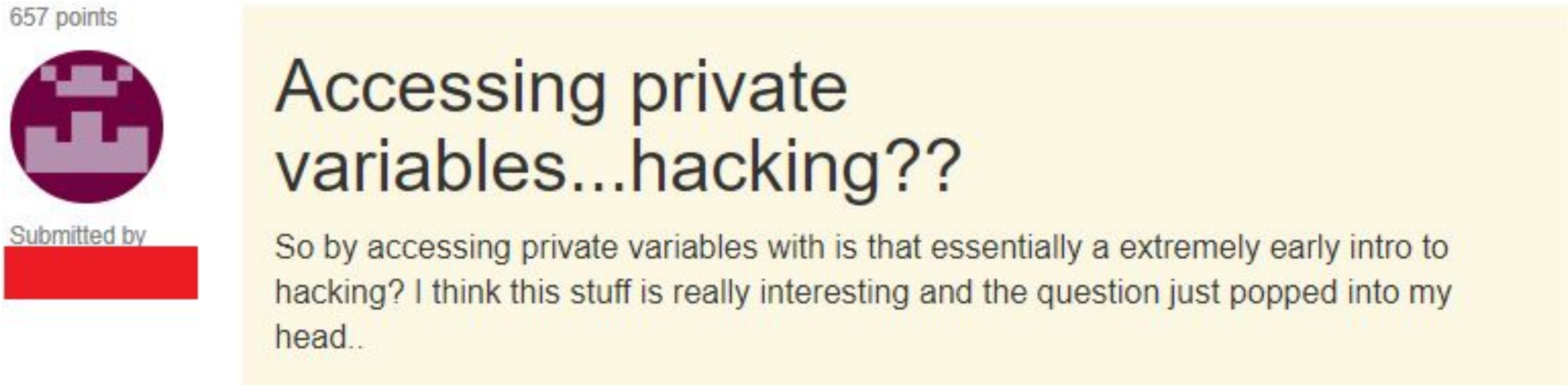
Don’t Do KRACK, Kids!

Wireless Exploitation 101

Claudia Richoux

* Want to learn more? Google terms that are <u>underlined</u>!

~Important Legal Warning~



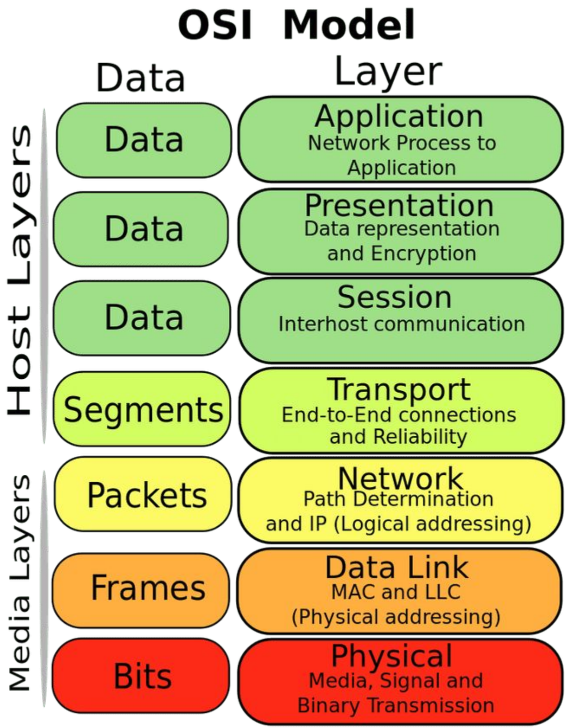
657 points

Submitted by [redacted]

Accessing private variables...hacking??

So by accessing private variables with is that essentially a extremely early intro to hacking? I think this stuff is really interesting and the question just popped into my head..

Why Wi-Fi Security? Don’t We Have SSL?


OSI Model
Data
Layer
Host Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Media Layers
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

Netflix and Chill (Binary exploits, web stuff)

TCP/IP (Shijacking, DNS attacks, MITM)

WiFi: 802.11 and WPA/WEP is here

Wireless Comms And Why They Are Terrible

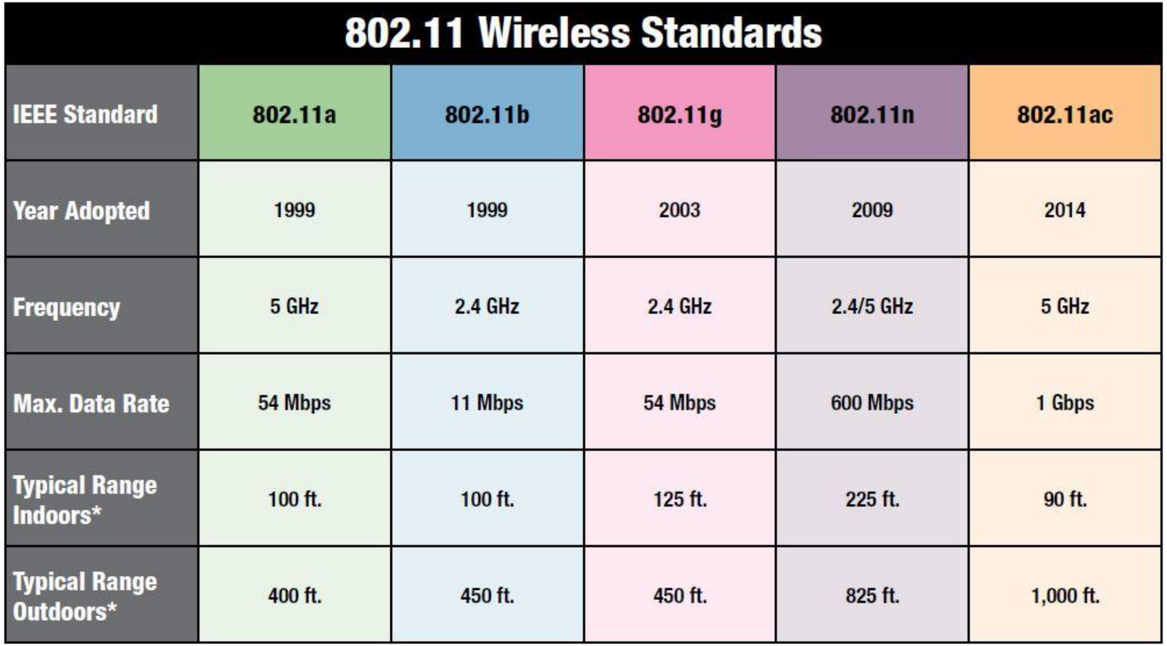
- Very convenient: Transferring information without being connected by an electrical conductor
- Very insecure: No physical boundaries for perimeter defense
- Cannot prevent people from injecting information without compromising performance
- Cannot prevent people from wiretapping you without compromising performance
- Intruder can look at information, tamper w/ info, deny service, use network resources, traffic-activity correlation

People Are Stupid And Other Cyber Mantras

- Best Buy (2002)/Lowes (2003)
- BJ’s Wholesale Club/PG&E
- Wake Forest University
- Nov 2003: Guy downloads child porn over residential WiFi in Toronto
- 2004: FL homeowner gets arrested for someone sending death threats on his wifi

Under The Hood: 802.11 101(.11)

- Defined by IEEE, specifies details of the standard
- MAC (Access Control)
- Physical Layer
- Frequency/Power
- Security

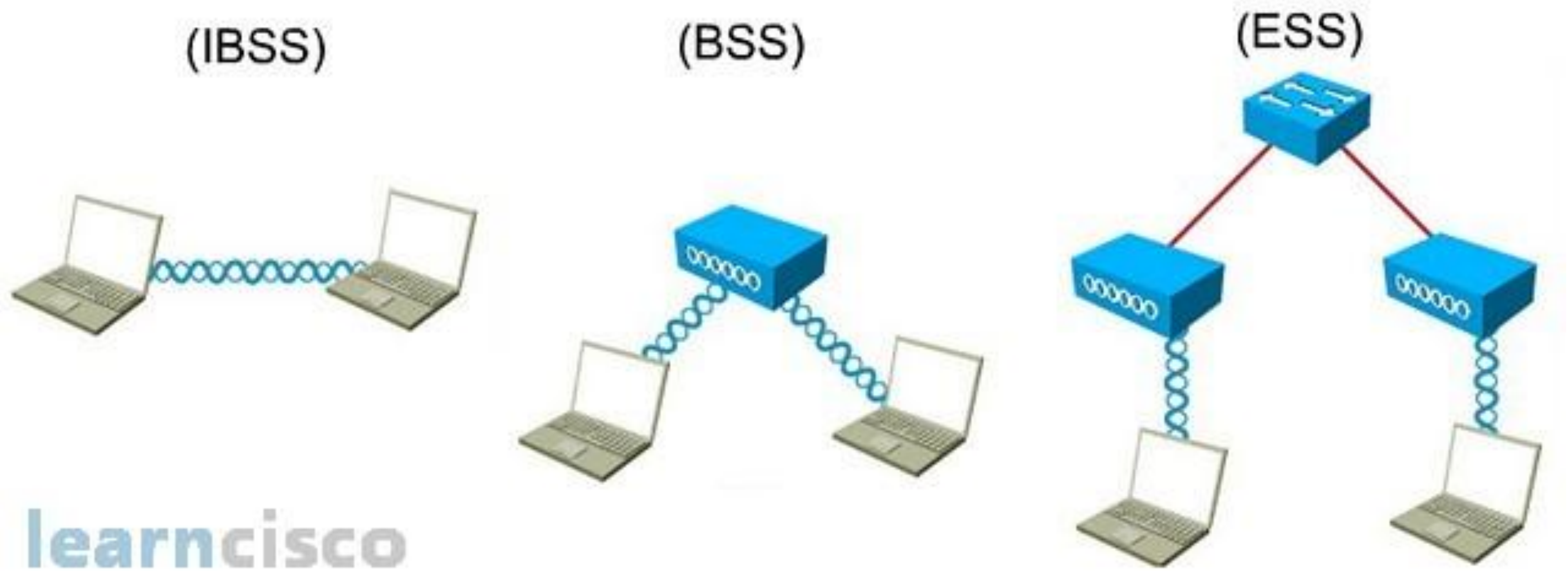


802.11 Wireless Standards

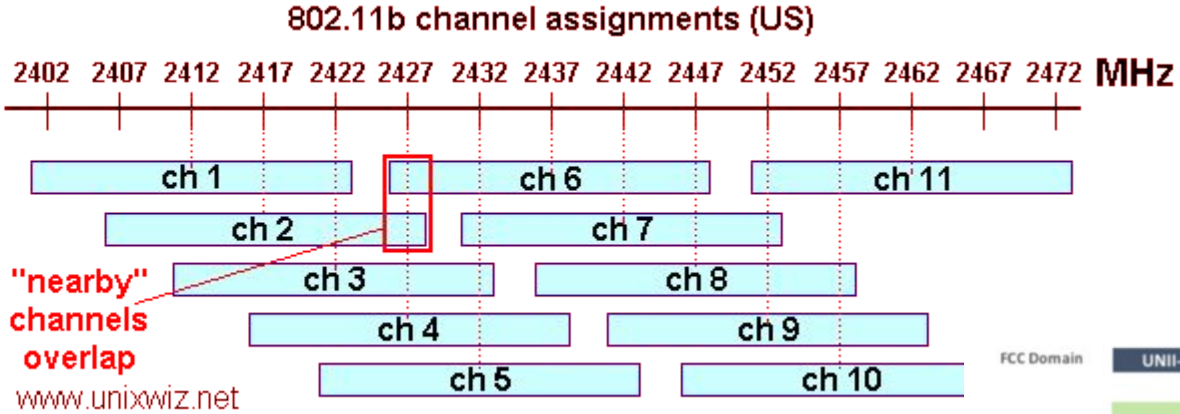
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

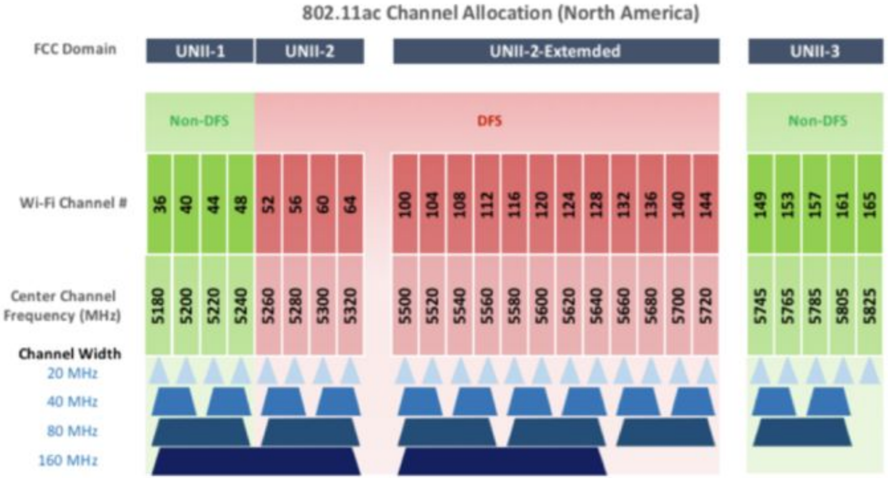
Clients and Access Points

Network Topologies



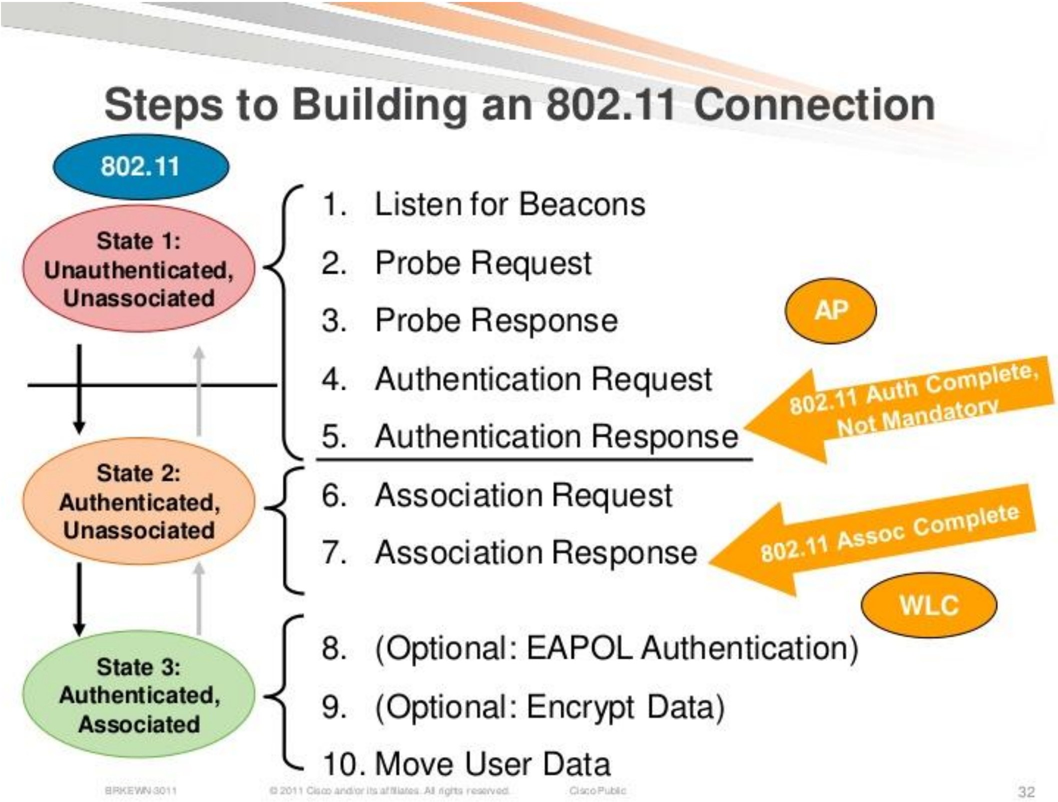
Channels


802.11b channel assignments (US)
2402 2407 2412 2417 2422 2427 2432 2437 2442 2447 2452 2457 2462 2467 2472 MHz
ch 1
ch 6
ch 11
ch 2
ch 7
ch 3
ch 8
ch 4
ch 9
ch 5
ch 10
"nearby" channels overlap
www.unixwiz.net



Wi-Fi Channel #	Center Channel Frequency (MHz)
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
144	5720
149	5745
153	5765
157	5785
161	5805
165	5825

Frames



Steps to Building an 802.11 Connection

802.11

State 1: Unauthenticated, Unassociated

1. Listen for Beacons
2. Probe Request
3. Probe Response
4. Authentication Request
5. Authentication Response

AP

802.11 Auth Complete, Not Mandatory

State 2: Authenticated, Unassociated

6. Association Request
7. Association Response

802.11 Assoc Complete

WLC

State 3: Authenticated, Associated

8. (Optional: EAPOL Authentication)
9. (Optional: Encrypt Data)
10. Move User Data

BRKEWN-3011 © 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public 32

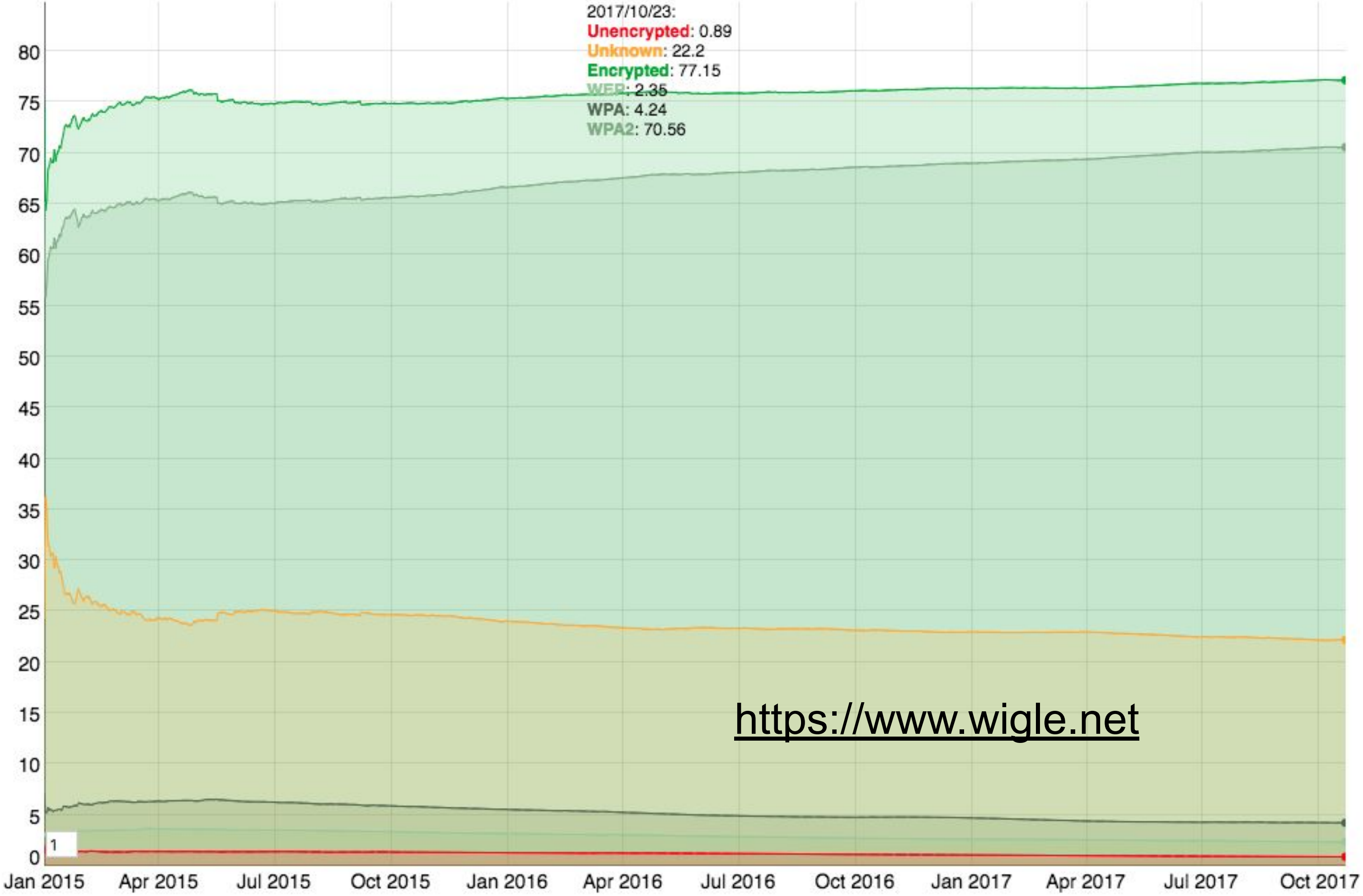
What You’ve All Been Waiting For

Theoretical Attack Vectors

- Unprotected Physical Layer
- Protocol Security
- Lack of Authentication
- Bad Encryption
- Default Settings
- Broadcasting Network Info

Ready, Aim… Wardriving?

- Derived from War Dialing, AKA brute forcing phone numbers to attack over dialup, from the 1983 movie WarGames.
- All you need is an antenna, your laptop, and transport!
- I like airodump-ng because it integrates with the aircrack-ng suite well, Kismet has a nice GUI tho.



https://www.wigle.net

Weaponizing your Pets

The War Kitteh and the Denial of Service Dog

DefCon
10 August 2014

Data Seepage

- Ferret and Hamster by Errata Security analyze leaked data
  - NetBIOS/Printer/SMB Probes tell me where you’ve connected
  - AIM tells me who’s on your friend list
  - Skype will send out all sorts of info about you
  - iTunes/Bonjour broadcasts keys that allow me to DL your music
  - CUPS basically gives me a network map
  - DHCP/ARP also give me a network map
- Can do TCP/ping response analysis to figure out current build of software and map out vulnerabilities (use NMAP)
- Wifi Probe Requests (Wireshark or Kismet)

CATS: ALL YOUR DATA ARE BELONG TO US.

Authentication/Encryption/ACL (yay vulns!)

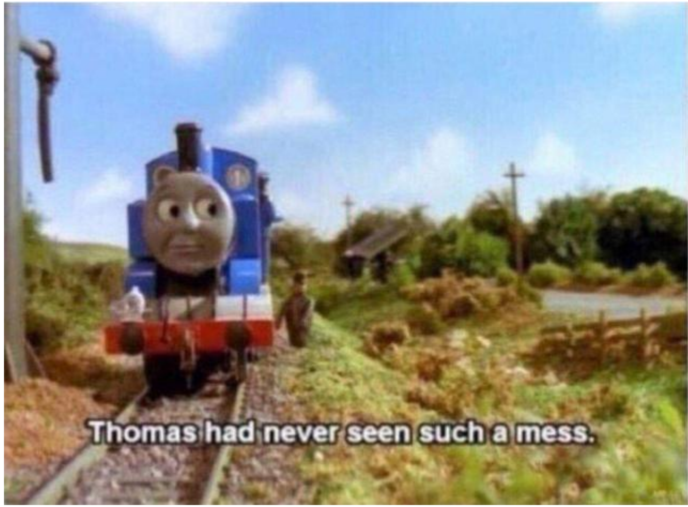
- Authentication
  - Open: “No Authentication”
  - Shared Key: “The Most Misguided Authentication Scheme Ever Devised”
  - Closed: “The Weakest Authentication Scheme Ever Devised”
- Encryption
  - Wired Equivalent Privacy/WEP ← (rekt)
  - WPA + TKIP + RC4 ← temporary solution after WEP was broken (0/10 do not)
  - WPA2 + AES + CCMP ← ~~gooooood~~ ~~KRACK’d~~ OK if u update (@UChicago??!?!)
- Access Control Lists
  - MAC filtering (lol that’s not keeping anyone out)

Authentication

- Open
  - No auth, anyone can join
- Shared key
  - AP sends 128 bytes of plaintext
  - Client encrypts it with WEP key
  - AP decrypts and compares, if they agree, authenticate!
  - Attacker can recover key!
- Closed
  - Literally just uses SSID as key

WEP

- Brute Force, Dictionary, IV Collision
- FMS Attack, then Hulton and h1kari
- KoreK’s Chopchop
- didn’t think it was a problem… wrong.
- Injection to increase traffic- aireplay
- Largest key size can be broken in under 60 seconds with current tech on a crappy laptop- aircrack-ng
- “WEP is, at best, like securing written information by putting a sheet of paper face down”



WPA

- TKIP/CCMP: big key size and dynamically distributed keys
- AES for encryption- much better old vulnerable RC4!
- MIC prevents injection attacks
- WPA2 Enterprise with RADIUS
- WPA-PSK
  - dictionary attacks: aircrack/rockyou
  - Use DICEWARE
- MIC “Michael” DoS vulnerability
- KRACK

Internet of Shit @internetofshit · Oct 16

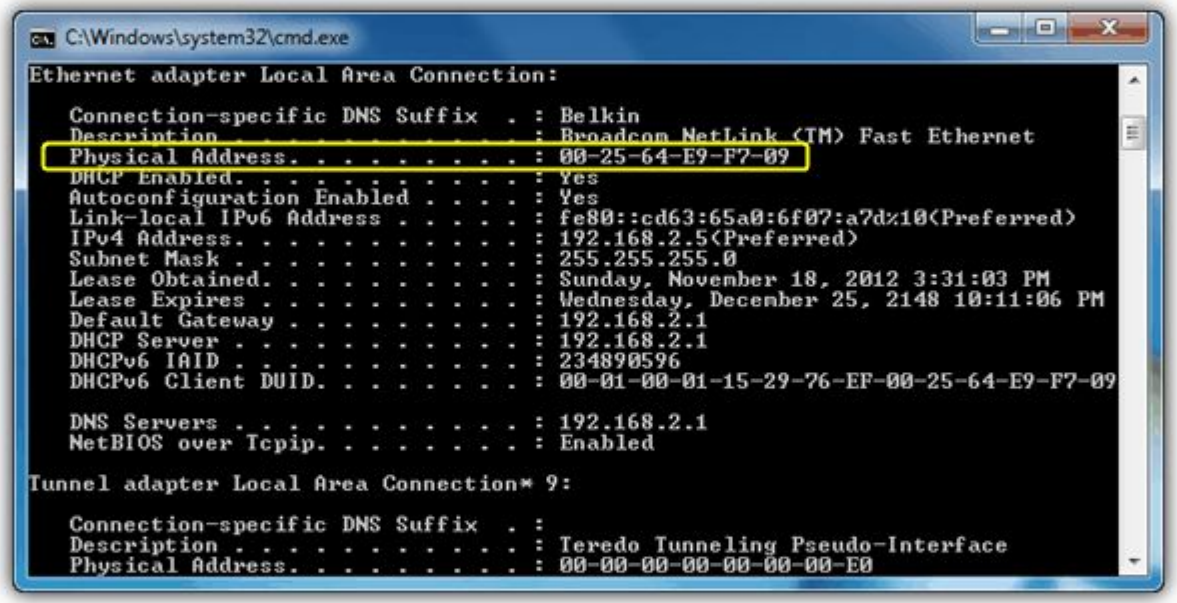
hi dad i'm just calling cause you need to patch your router

oh you're using it without a password

ok never mind

MAC Spoofing

just change it with ifconfig or relevant Windows/Mac settings

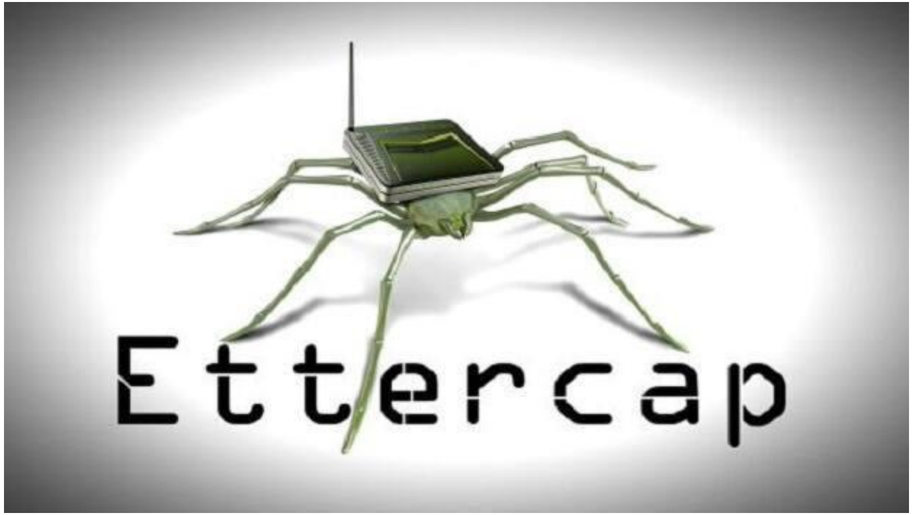


```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : Belkin
   Description . . . . . . . . . . . : Broadcom NetLink (TM) Fast Ethernet
   Physical Address. . . . . . . . . : 00-25-64-E9-F7-09
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::cd63:65a0:6f07:a7d%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, November 18, 2012 3:31:03 PM
   Lease Expires . . . . . . . . . . : Wednesday, December 25, 2148 10:11:06 PM
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 234890596
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-15-29-76-EF-00-25-64-E9-F7-09

   DNS Servers . . . . . . . . . . . : 192.168.2.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter Local Area Connection* 9:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
```

If You Like Piña Coladas

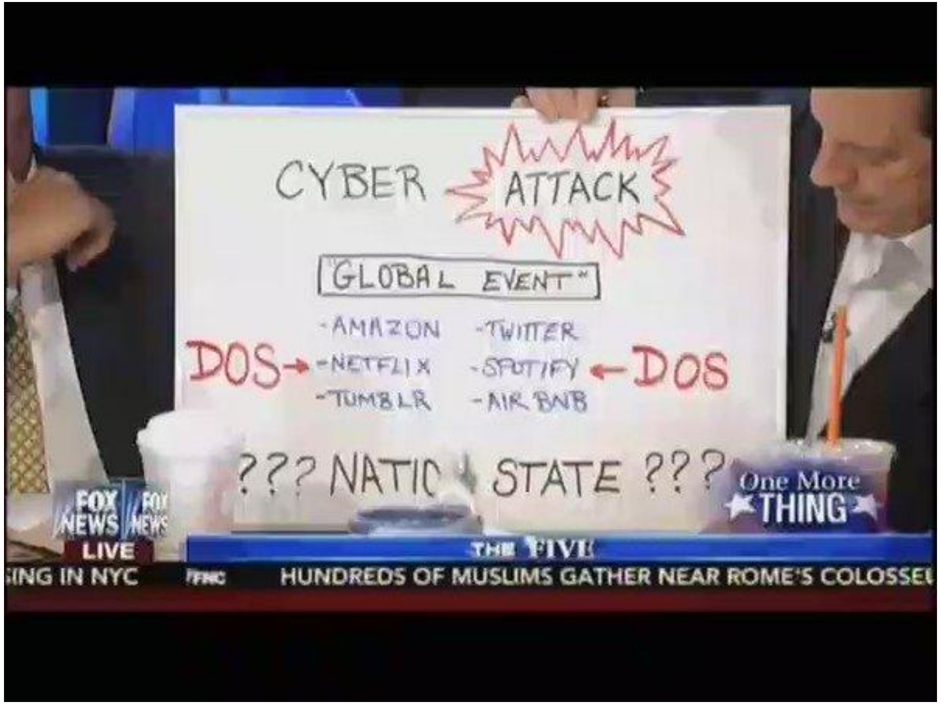
Conn-jacking/MITM

- Conn-jacking: Watch authentication, force client to deauth, impersonate either client or AP
- MITM: sniff authentication, force deauth, impersonate with ARP poisoning to both sides. Relay messages, view everything they’re sending
- Ettercap/Wireshark/void11
- Cain and Abel



The Obvious Ones: DOS and Theft

- Jamming
- De-auth packets
- Barraging an AP
- Aforementioned Conn-jacking/MITM techniques
- Stealing computers? Plaintext key storage!



TL;DR

'S' in WiFi means 'Security'
The More You Know

Before I Take Questions...

- If you have a specific question about a tool… Google
- If you have cryptography questions… Wikipedia

- If you want to start a cybersecurity team/club… hit me up
- If you want these slides, they're at https://elgar.laudiacay.net/wifi_talk.pdf
- If you want me to give another talk about another hacking-related topic… hit me up
- My contact info is all at https://elgar.laudiacay.net/

Questions?