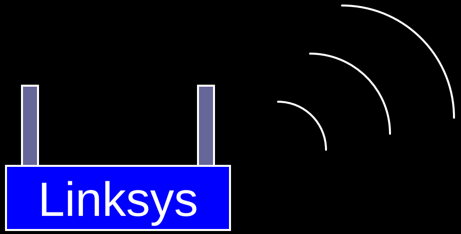
Wireless Hacking
(for Fun and Profit)

Mark Whitteker, CISSP, GSNA, GCFA



Agenda

- Wireless overview
- Legal Issues
- Hardware
- Software
- Wireless detection
- Data capture
- WEP cracking
- War driving
- SideJacking
- Preventative measures
- Demo / Questions

Wireless Overview

- Based on the 802.11 specification
- 802.11a - 5GHz - 54 Mbps data rate
  - Indoor range ~35 meters
  - Outdoor range ~120 meters
- 802.11b - 2.4GHz - 11 Mbps data rate
  - Indoor range ~38 meters
  - Outdoor range ~140 meters
- 802.11g - 2.4GHz - 54 Mbps data rate
  - Indoor range ~38 meters
  - Outdoor range ~140 meters
- 802.11n - 2.4/5GHz - 248 Mbps data rate (MIMO technology)
  - Indoor range ~70 meters
  - Outdoor range ~250 meters

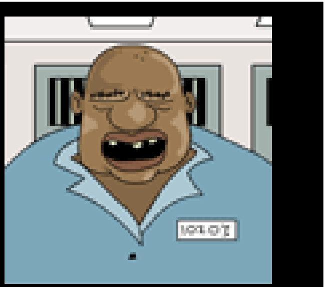
Wireless Overview cont.

- Security was added to wireless as an afterthought
- WEP - Wired Equivalent Privacy
  - Developed without participation by the cryptanalysis community
  - Beginning in 2001 several weaknesses were identified
  - Can be cracked in minutes with widely available and free software
  - 64-bit WEP (WEP-40) - Very weak
  - 128-bit WEP (WEP-104) - Weak
    - 40/104 refers to the encryption key length
    - Remaining size (24) refers to the Initialization Vector (IV)
    - Together they form the RC4 traffic key
  - Larger key size requires more captured data to crack
  - Attacks available to stimulate necessary traffic
  - Other weaknesses such as IV collisions, altered packets, etc. are not effected by use of longer key

Wireless Overview cont.

- Wi-Fi Protected Access (WPA / WPA2) developed to replace WEP
- WPA implements the majority of the 802.11i standard, and will run on pre-WPA cards (through firmware upgrades)
- WPA2 implements the full standard, but will not work with some older cards
- Typically no longer an issue, as all currently manufactured hardware supports WPA / WPA2
- Two flavors: Personal and Enterprise
- Personal utilizes a pre-shared key (PSK)
  - Security depends on the strength and secrecy of the key
- Enterprise utilizes an IEEE 802.1X authentication server
- Like WEP, data is encrypted using RC4
  - Uses the Temporal Key Integrity Protocol (TKIP) to dynamically change keys
  - Larger initialization vector (IV) of 48 bits
- More difficult to crack than WEP

Legal Issues



- Searching for wireless networks is legal in the US
- Unauthorized use of wireless networks *may* be illegal depending on local laws
  - Currently legal in NC
- Intentionally circumventing the security of a private network to gain unauthorized access IS illegal
- Conduct your testing on your own private network, or obtain written permission from the network owner (especially in the case of corporate testing)

Hardware

- Laptop - the more Linux friendly, the better
  - The majority of tools are Linux based
  - Mac OSX gaining popularity among testers
  - Personal success with:
    - IBM ThinkPad T60p
    - Dell Latitude D820
    - Apple MacBook Pro
    - Superman Learning Laptop

Hardware cont.

- Wireless Card
  - Internal OK for localized testing
    - Limited power and range
  - PCMCIA or USB with external antenna connector best
    - High-gain antenna for war driving
    - Directional antenna for directed attacks
  - Chipset depends on the tools you plan to use
    - Orinoco
    - Prism
    - Atheros
  - Not as big an issue as it used to be
  - Needs to support promiscuous mode

Hardware cont.

- GPS Receiver
  - Used if you want to map networks to physical locations
  - Basic receiver with serial connection is all that is necessary (such as the Garmin eTrex)
- External Antenna
  - High-gain for greater range
  - Directional for targeted attack

Software - The Platform

- Linux - choose your favorite flavor
- Personal choice - BackTrack “Live” distro
  - Pre-built with numerous security tools
  - CD “lite” version and USB (1GB) version
  - Based on Slackware Linux
  - http://www.remote-exploit.org/backtrack.html
  - Current version: Beta 3

Software - The Tools

- Numerous to choose from
- Some work better on specific chipsets
- We’ll look at a few of the most used
  - Kismet - Wireless detection
  - Airodump-ng - Data capture
  - Aircrack-ng - WEP cracking
  - Ferret - data seepage collection
  - Hamster - Windows tool (but compliments Ferret)

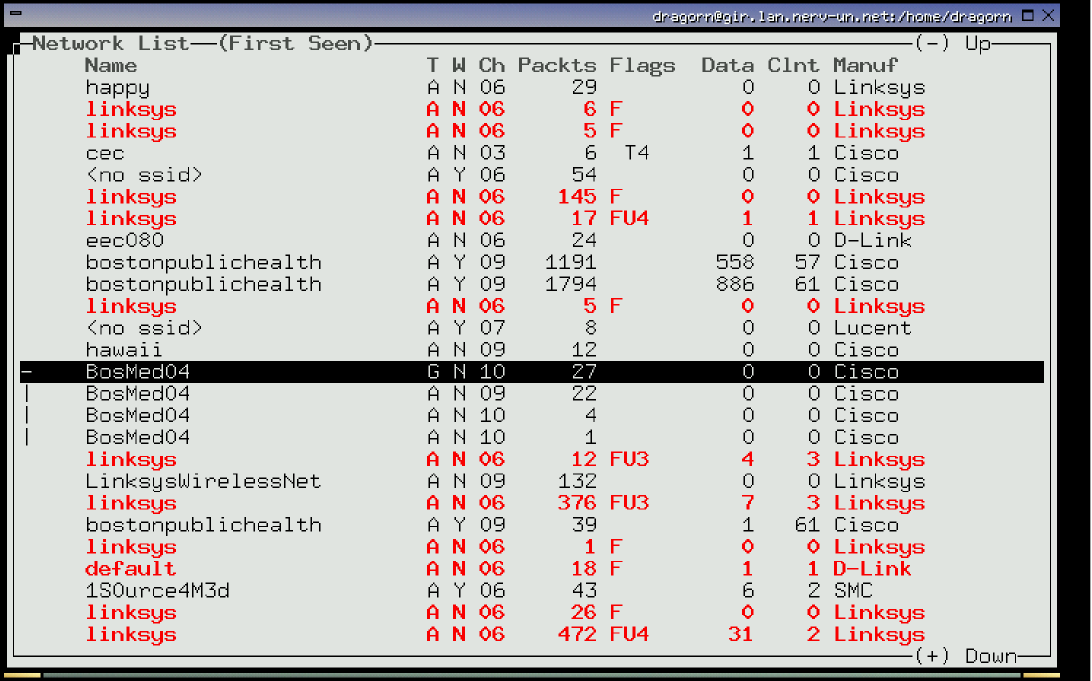
Wireless Detection

- Kismet
  - http://www.kismetwireless.net/
  - Identifies networks by passibely collecting packets
    - Detects standard named networks
    - Detects hidden networks
    - Infers the presence of non-beaconing networks via data traffic

Wireless Detection

KISMET

- SSID
- Type
- Encryption
- Packets
- Flags default configuration



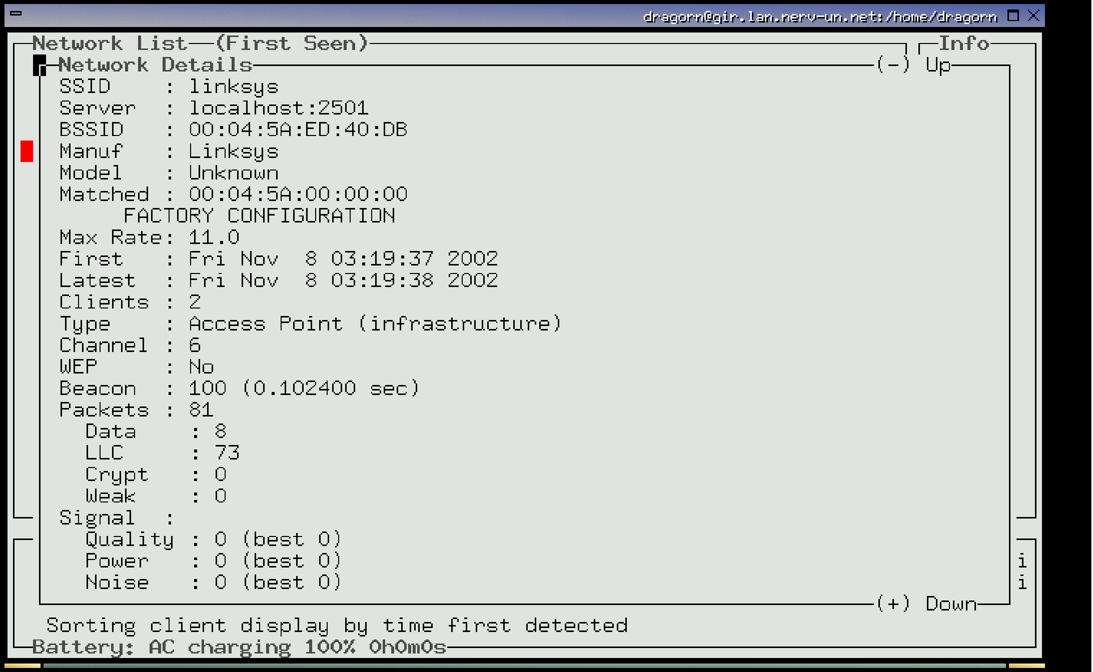
dragorn@gir.lan.nerv-un.net:/home/dragorn

```
 Network List—(First Seen)————————————————————————————————(-) Up
     Name                      T W Ch Packts Flags  Data Clnt Manuf
     happy                     A N 06     29            0    0 Linksys
     linksys                   A N 06      6 F          0    0 Linksys
     linksys                   A N 06      5 F          0    0 Linksys
     cec                       A N 03      6  T4        1    1 Cisco
     <no ssid>                 A Y 06     54            0    0 Cisco
     linksys                   A N 06    145 F          0    0 Linksys
     linksys                   A N 06     17 FU4        1    1 Linksys
     eec080                    A N 06     24            0    0 D-Link
     bostonpublichealth        A Y 09   1191          558   57 Cisco
     bostonpublichealth        A Y 09   1794          886   61 Cisco
     linksys                   A N 06      5 F          0    0 Linksys
     <no ssid>                 A Y 07      8            0    0 Lucent
     hawaii                    A N 09     12            0    0 Cisco
-    BosMed04                  G N 10     27            0    0 Cisco
|    BosMed04                  A N 09     22            0    0 Cisco
|    BosMed04                  A N 10      4            0    0 Cisco
|    BosMed04                  A N 10      1            0    0 Cisco
     linksys                   A N 06     12 FU3        4    3 Linksys
     LinksysWirelessNet        A N 09    132            0    0 Linksys
     linksys                   A N 06    376 FU3        7    3 Linksys
     bostonpublichealth        A Y 09     39            1   61 Cisco
     linksys                   A N 06      1 F          0    0 Linksys
     default                   A N 06     18 F          1    1 D-Link
     1SOurce4M3d               A Y 06     43            6    2 SMC
     linksys                   A N 06     26 F          0    0 Linksys
     linksys                   A N 06    472 FU4       31    2 Linksys
                                                          ——(+) Down
```

Wireless Detection

KISMET

- Additional details for each network
- Data packets
- Weak packets



```
Network List—(First Seen)                                          Info
 Network Details                                              (-)  Up
  SSID     : linksys
  Server   : localhost:2501
  BSSID    : 00:04:5A:ED:40:DB
  Manuf    : Linksys
  Model    : Unknown
  Matched  : 00:04:5A:00:00:00
       FACTORY CONFIGURATION
  Max Rate: 11.0
  First    : Fri Nov  8 03:19:37 2002
  Latest   : Fri Nov  8 03:19:38 2002
  Clients  : 2
  Type     : Access Point (infrastructure)
  Channel  : 6
  WEP      : No
  Beacon   : 100 (0.102400 sec)
  Packets  : 81
    Data     : 8
    LLC      : 73
    Crypt    : 0
    Weak     : 0
  Signal   :
    Quality  : 0 (best 0)
    Power    : 0 (best 0)                                              i
    Noise    : 0 (best 0)                                              i
                                                              (+)  Down
 Sorting client display by time first detected
Battery: AC charging 100% 0h0m0s
```

Data Capture

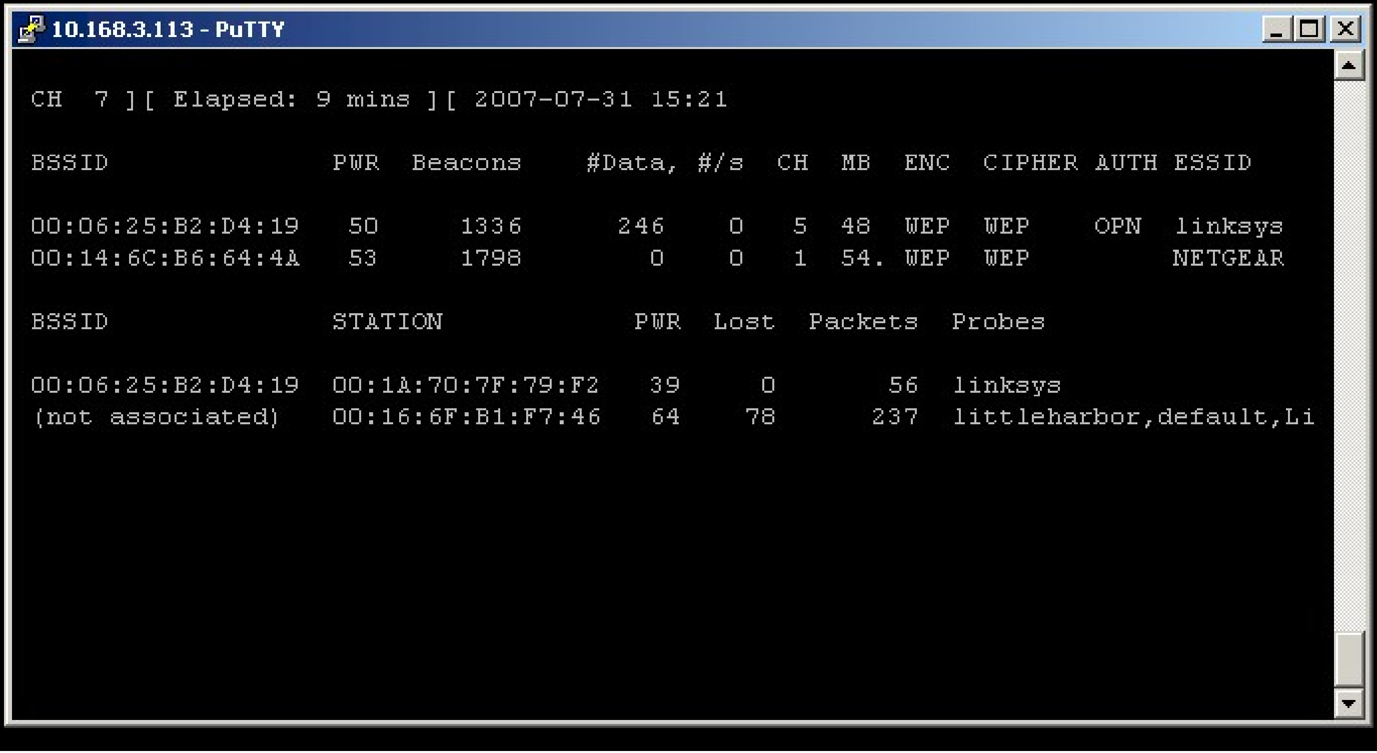
- Airodump-ng
  - http://www.aircrack-ng.org/doku.php?id=airodump-ng
  - Packet capturing of raw 802.11 frames
  - Excellent tool for collecting WEP IVs
  - Also supports the use of GPS receiver to log coordinates of detect access points
  - Collected data can then be used by aircrack-ng to crack WEP keys

Data Capture

- Must collect enough IVs for aircrack-ng
- Relatively easy on high use networks such as enterprise users
- May take several days or weeks for a typical home network
  - Typically need 250,000 or more unique IVs for 64 bit keys
  - Will need 1.5 million or more for 128 bit keys
- Aircrack-ng can be configured to run while capturing data

Data Capture

- Sample capture



```
CH  7 ][ Elapsed: 9 mins ][ 2007-07-31 15:21

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:06:25:B2:D4:19   50     1336      246    0   5  48  WEP  WEP    OPN  linksys
00:14:6C:B6:64:4A   53     1798        0    0   1  54. WEP  WEP         NETGEAR

BSSID              STATION            PWR  Lost  Packets  Probes

00:06:25:B2:D4:19  00:1A:70:7F:79:F2   39     0       56  linksys
(not associated)   00:16:6F:B1:F7:46   64    78      237  littleharbor,default,Li
```

WEP Cracking

- Aircrack-ng
  - http://www.aircrack-ng.org/doku.php?id=aircrack-ng
  - Can recover a WEP key once enough packets have been captured
  - Uses two methods
    - PTW - Pyshkin, Tews, Wainmann
      - If successful, requires few data packets
    - FMS/KoreK
      - Combines statistical and brute force attacks
  - Can optionally use a dictionary attack
    - Dictionary attack is the method used for WPA / WPA2 PSK

WEP Cracking

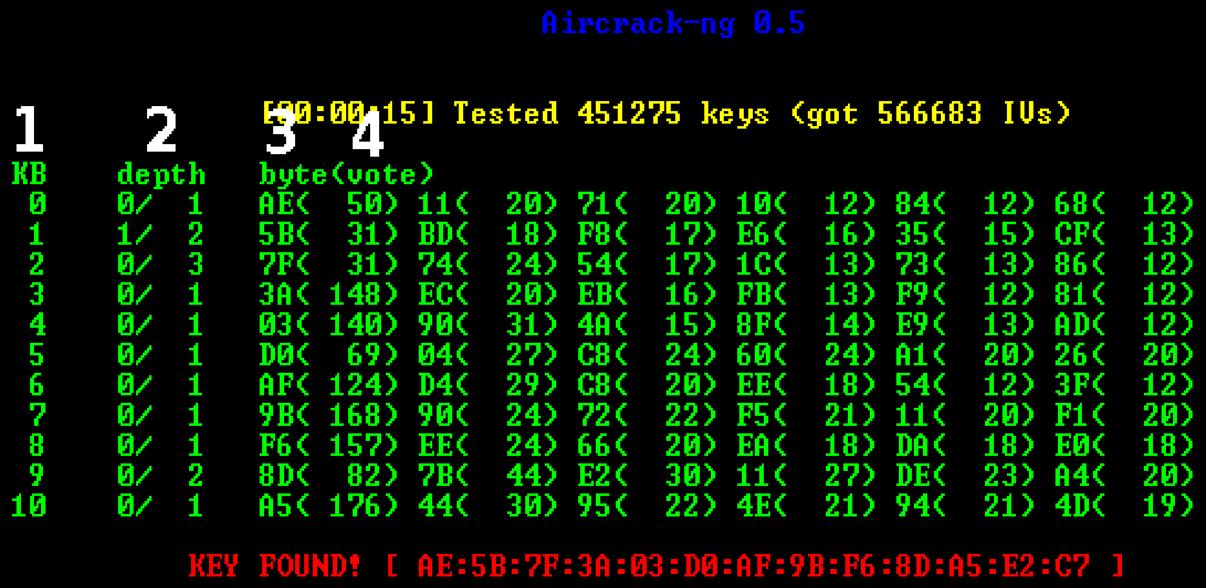
- Sample screenshot

1 = Keybyte

2 = Depth in current search

3 = Byte the IVs leaked

4 = Votes indicating this is correct



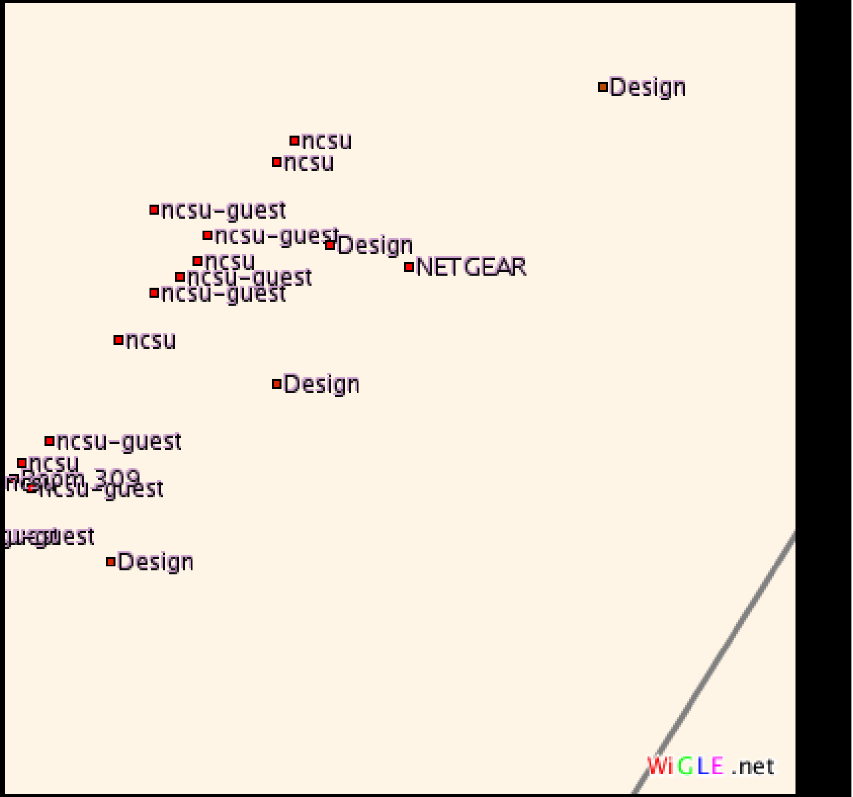
```
                              Aircrack-ng 0.5

                   [00:00:15] Tested 451275 keys (got 566683 IVs)

 KB    depth   byte(vote)
  0    0/  1   AE(  50) 11(  20) 71(  20) 10(  12) 84(  12) 68(  12)
  1    1/  2   5B(  31) BD(  18) F8(  17) E6(  16) 35(  15) CF(  13)
  2    0/  3   7F(  31) 74(  24) 54(  17) 1C(  13) 73(  13) 86(  12)
  3    0/  1   3A( 148) EC(  20) EB(  16) FB(  13) F9(  12) 81(  12)
  4    0/  1   03( 140) 90(  31) 4A(  15) 8F(  14) E9(  13) AD(  12)
  5    0/  1   D0(  69) 04(  27) C8(  24) 60(  24) A1(  20) 26(  20)
  6    0/  1   AF( 124) D4(  29) C8(  20) EE(  18) 54(  12) 3F(  12)
  7    0/  1   9B( 168) 90(  24) 72(  22) F5(  21) 11(  20) F1(  20)
  8    0/  1   F6( 157) EE(  24) 66(  20) EA(  18) DA(  18) E0(  18)
  9    0/  2   8D(  82) 7B(  44) E2(  30) 11(  27) DE(  23) A4(  20)
 10    0/  1   A5( 176) 44(  30) 95(  22) 4E(  21) 94(  21) 4D(  19)

           KEY FOUND! [ AE:5B:7F:3A:03:D0:AF:9B:F6:8D:A5:E2:C7 ]
```

War Driving

- Kismet with GPS and high-gain antenna
- Supports “gpsmap” command for mapping detected APs to GPS maps
- Web sites exist where you can upload war driving data to area maps
    - http://www.wigle.net/

War Driving

- Sample map from NCSU campus



SideJacking

- Data is leaked from unencrypted wireless connections
- Doesn’t require a “man-in-the-middle” attack
- Sniff wireless packets to collect cookies
- Tweak Firefox with the collected specific cookies
- Visit the website and impersonate the user

SideJacking

- Allows the attacker to assume a user’s authenticated session without obtaining the username and password
  - Gmail
  - Blackboard
- User is unaware that anything has happened

SideJacking

- Ferret
  - Collect packets from wireless data seepage
  - Passive attack
  - Undetectable

SideJacking

- Hamster
  - Windows executable that will provide cookies collected by Ferret through a web interface

Preventative Measures

- Don’t use WEP!
- WPA / WPA2 w/ strong keys (64 random HEX)
- Don’t use wireless AP default settings
    - Change the SSID
    - Don’t broadcast the SSID
        - Doesn’t provide security, but prevents casual users from finding your network
    - Disable remote administration
    - Require encrypted access (HTTPS)
    - MAC filtering - can be spoofed, but takes more effort
- Use a VPN when connected to public wireless APs

Demo / Questions