Wi-Fi PNLs

Assessing & Evaluating Risk

Setting the stage

Explosion in mobile devices as well as laptops with wi-fi

User convenience nearly always prioritized over security

Understanding Risk

"The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization".

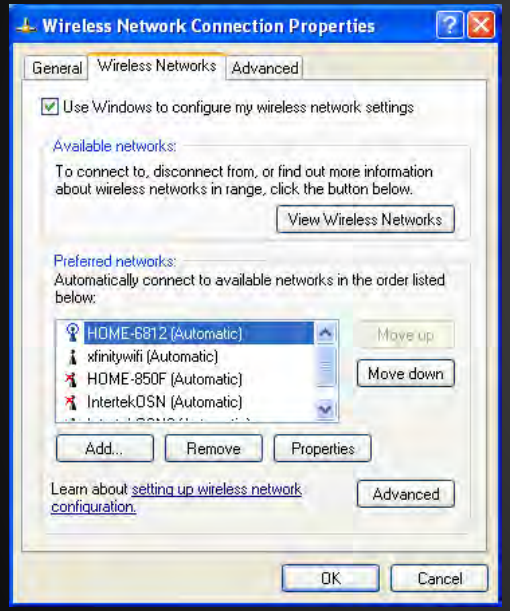
Risk

Threats
+
Vulnerabilities

Risk


Risk Matrix
High Impact
Low Probability
High Impact
High Probability
Low Impact
Low Probability
Low Impact
High Probability
Impact
Probability

What are PNLs?



- List of known wi-fi networks the client has connected to the in past and is willing to connect to again
- Local client repository

Wi-Fi PNL Behavior

- Wi-fi devices send 802.11 probe requests for networks periodically
- Probe requests search for networks on the devices PNL

Wi-fi Methods

- Passive Discovery : Listen for beacon frames transmitted from the AP
- Active Discovery: Send probe requests to AP to gather beacon frame info
- Monitor Mode Capture: Capture packets to AP and clients (totally passive!)

Wi-fi Tools

Alfa Wireless Card (AWUS051NH)
Kali Linux VM, incl:
- Aircrack-ng suite
- Kismet
- Wireshark

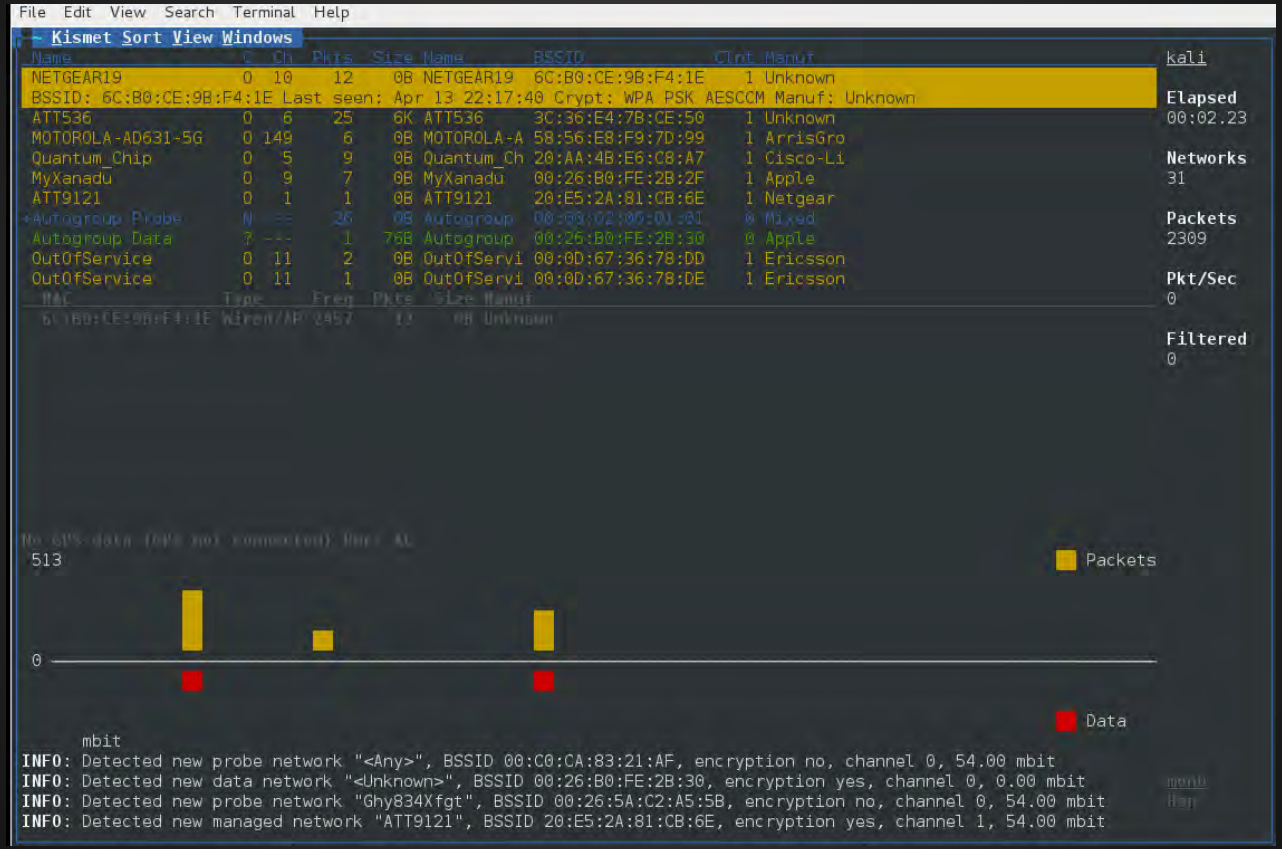
Wi-Fi Quick Primer

802.11 Probe Requests & Responses

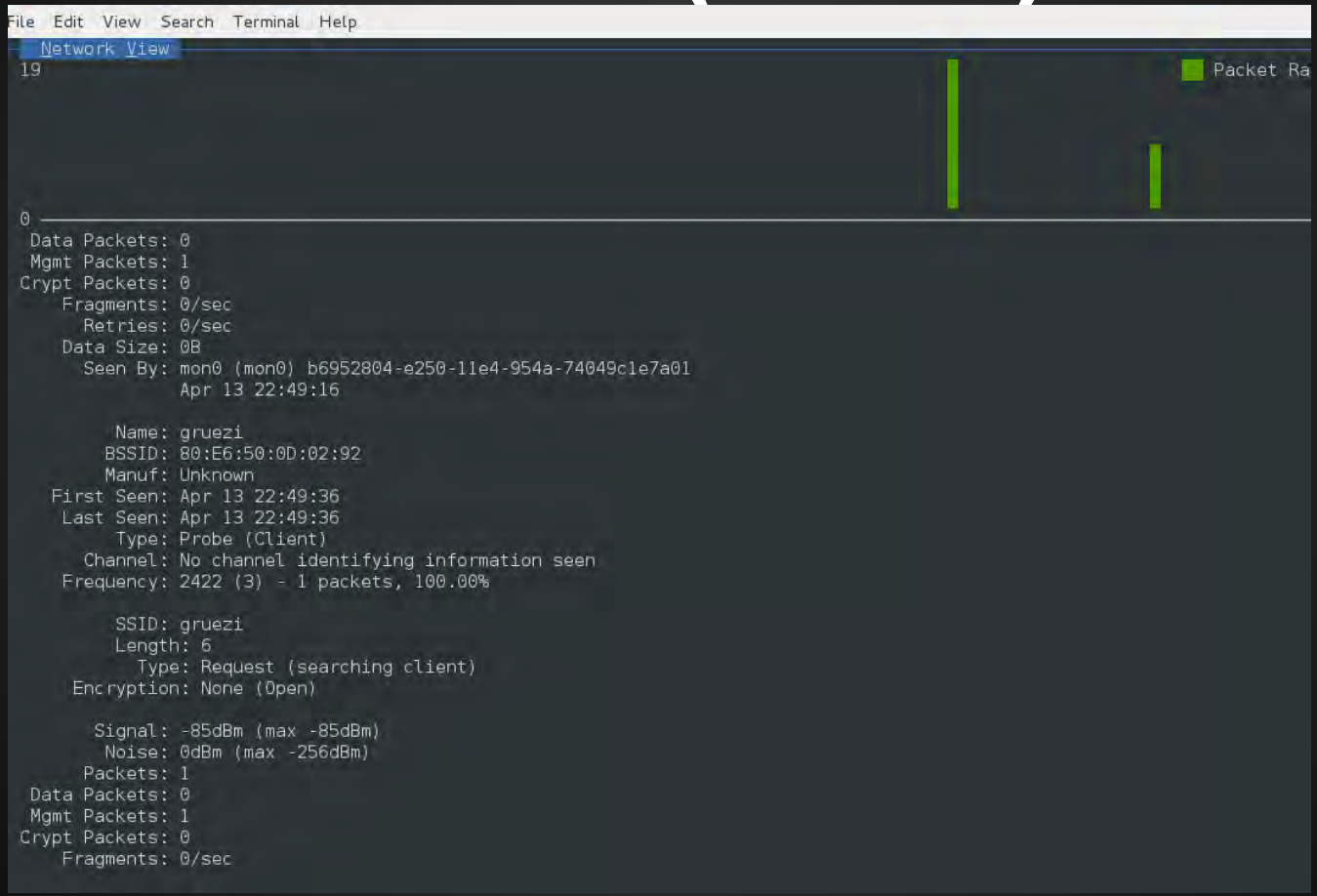
Client -------probe request----> AP

Client <------probe response---- AP

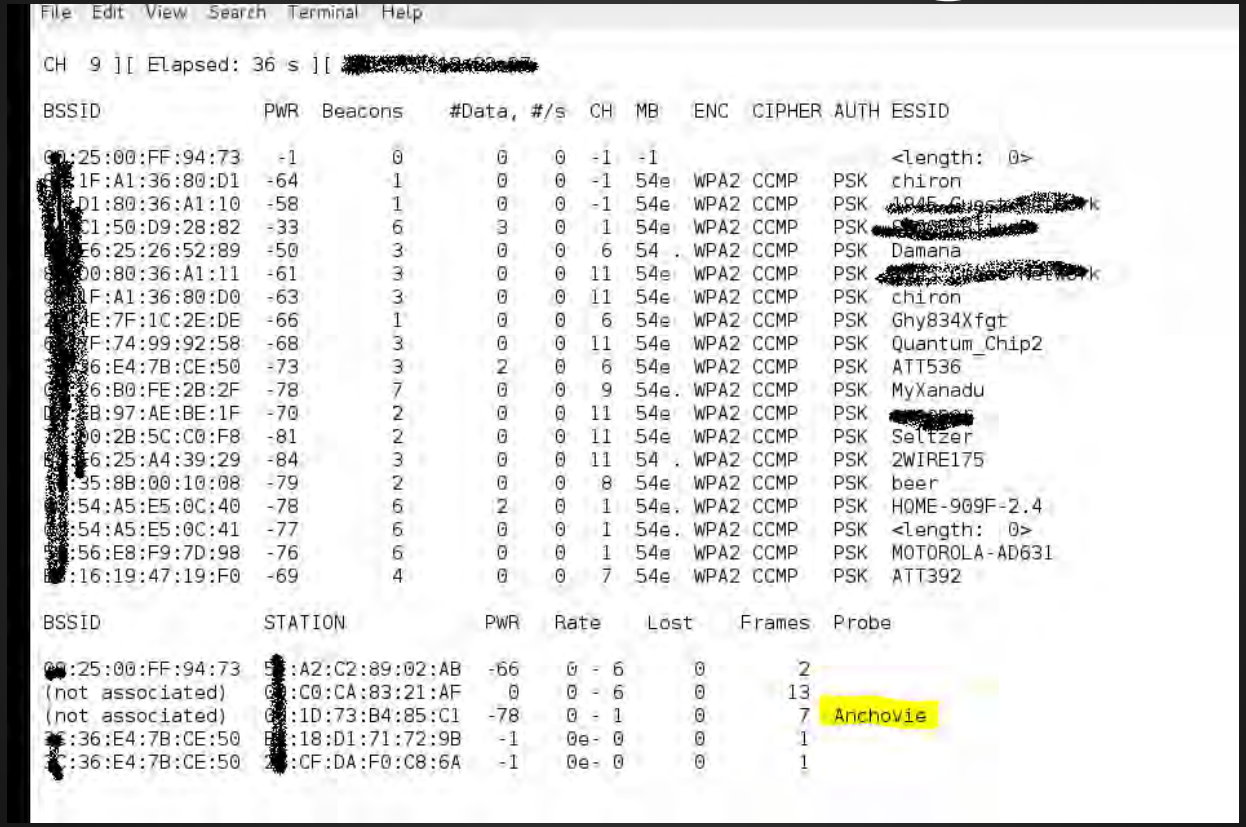
Kismet


File Edit View Search Terminal Help
Kismet Sort View Windows
Name T Ch Pkts Size Name BSSID Clnt Manuf
NETGEAR19 0 10 12 0B NETGEAR19 6C:B0:CE:9B:F4:1E 1 Unknown
BSSID: 6C:B0:CE:9B:F4:1E Last seen: Apr 13 22:17:40 Crypt: WPA PSK AESCCM Manuf: Unknown
ATT536 0 6 25 6K ATT536 3C:36:E4:7B:CE:50 1 Unknown
MOTOROLA-AD631-5G 0 149 6 0B MOTOROLA-A 58:56:E8:F9:7D:99 1 ArrisGro
Quantum_Chip 0 5 9 0B Quantum_Ch 20:AA:4B:E6:C8:A7 1 Cisco-Li
MyXanadu 0 9 7 0B MyXanadu 00:26:B0:FE:2B:2F 1 Apple
ATT9121 0 1 1 0B ATT9121 20:E5:2A:81:CB:6E 1 Netgear
Autogroup Probe N --- 26 0B Autogroup 00:00:02:00:01:01 0 Mixed
Autogroup Data 7 --- 1 76B Autogroup 00:26:B0:FE:2B:30 0 Apple
OutOfService 0 11 2 0B OutOfServi 00:0D:67:36:78:DD 1 Ericsson
OutOfService 0 11 1 0B OutOfServi 00:0D:67:36:78:DE 1 Ericsson
MAC Type Freq Pkts Size Manuf
6C:B0:CE:9B:F4:1E Wired/AP 2457 13 0B Unknown
kali
Elapsed
00:02.23
Networks
31
Packets
2309
Pkt/Sec
0
Filtered
0
513
Packets
0
Data
mbit
INFO: Detected new probe network "<Any>", BSSID 00:C0:CA:83:21:AF, encryption no, channel 0, 54.00 mbit
INFO: Detected new data network "<Unknown>", BSSID 00:26:B0:FE:2B:30, encryption yes, channel 0, 0.00 mbit
INFO: Detected new probe network "Ghy834Xfgt", BSSID 00:26:5A:C2:A5:5B, encryption no, channel 0, 54.00 mbit
INFO: Detected new managed network "ATT9121", BSSID 20:E5:2A:81:CB:6E, encryption yes, channel 1, 54.00 mbit

Kismet (cont.)


File Edit View Search Terminal Help
Network View
19
Packet Ra
0
Data Packets: 0
Mgmt Packets: 1
Crypt Packets: 0
Fragments: 0/sec
Retries: 0/sec
Data Size: 0B
Seen By: mon0 (mon0) b6952804-e250-11e4-954a-74049c1e7a01
Apr 13 22:49:16
Name: gruezi
BSSID: 80:E6:50:0D:02:92
Manuf: Unknown
First Seen: Apr 13 22:49:36
Last Seen: Apr 13 22:49:36
Type: Probe (Client)
Channel: No channel identifying information seen
Frequency: 2422 (3) - 1 packets, 100.00%
SSID: gruezi
Length: 6
Type: Request (searching client)
Encryption: None (Open)
Signal: -85dBm (max -85dBm)
Noise: 0dBm (max -256dBm)
Packets: 1
Data Packets: 0
Mgmt Packets: 1
Crypt Packets: 0
Fragments: 0/sec

Airodump-ng



```
File  Edit  View  Search  Terminal  Help

CH  9 ][ Elapsed: 36 s ][ [redacted]

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

[redacted]:25:00:FF:94:73   -1        0        0    0  -1  -1                  <length:  0>
[redacted]:1F:A1:36:80:D1  -64        1        0    0  -1  54e  WPA2 CCMP   PSK  chiron
[redacted]:D1:80:36:A1:10  -58        1        0    0  -1  54e  WPA2 CCMP   PSK  1945_Guest[redacted]k
[redacted]:C1:50:D9:28:82  -33        6        3    0   1  54e  WPA2 CCMP   PSK  [redacted]
[redacted]:26:25:26:52:89  -50        3        0    0   6  54 . WPA2 CCMP   PSK  Damana
[redacted]:00:80:36:A1:11  -61        3        0    0  11  54e  WPA2 CCMP   PSK  [redacted]k
[redacted]:1F:A1:36:80:D0  -63        3        0    0  11  54e  WPA2 CCMP   PSK  chiron
[redacted]:4E:7F:1C:2E:DE  -66        1        0    0   6  54e  WPA2 CCMP   PSK  Ghy834Xfgt
[redacted]:1F:74:99:92:58  -68        3        0    0  11  54e  WPA2 CCMP   PSK  Quantum_Chip2
[redacted]:36:E4:7B:CE:50  -73        3        2    0   6  54e  WPA2 CCMP   PSK  ATT536
[redacted]:26:B0:FE:2B:2F  -78        7        0    0   9  54e. WPA2 CCMP   PSK  MyXanadu
[redacted]:2B:97:AE:BE:1F  -70        2        0    0  11  54e  WPA2 CCMP   PSK  [redacted]
[redacted]:00:2B:5C:C0:F8  -81        2        0    0  11  54e  WPA2 CCMP   PSK  Seltzer
[redacted]:26:25:A4:39:29  -84        3        0    0  11  54 . WPA2 CCMP   PSK  2WIRE175
[redacted]:35:8B:00:10:08  -79        2        0    0   8  54e  WPA2 CCMP   PSK  beer
[redacted]:54:A5:E5:0C:40  -78        6        2    0   1  54e. WPA2 CCMP   PSK  HOME-909F-2.4
[redacted]:54:A5:E5:0C:41  -77        6        0    0   1  54e. WPA2 CCMP   PSK  <length:  0>
[redacted]:56:E8:F9:7D:98  -76        6        0    0   1  54e  WPA2 CCMP   PSK  MOTOROLA-AD631
[redacted]:16:19:47:19:F0  -69        4        0    0   7  54e  WPA2 CCMP   PSK  ATT392

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

[redacted]:25:00:FF:94:73  [redacted]:A2:C2:89:02:AB  -66    0 - 6      0        2
(not associated)   [redacted]:C0:CA:83:21:AF    0    0 - 6      0       13
(not associated)   [redacted]:1D:73:B4:85:C1  -78    0 - 1      0        7  Anchovie
[redacted]:36:E4:7B:CE:50  [redacted]:18:D1:71:72:9B   -1    0e- 0      0        1
[redacted]:36:E4:7B:CE:50  [redacted]:CF:DA:F0:C8:6A   -1    0e- 0      0        1
```

PNLs & Devices

- With PNL behavior across many devices, it is fairly easy to convince a client to connect to rogue or evil twin ap
- Disclosure of full PNL curtailed by vuln disclosures (in some cases)
- Each device/os has different abilities to manage the PNL (Apple ios = nothing)

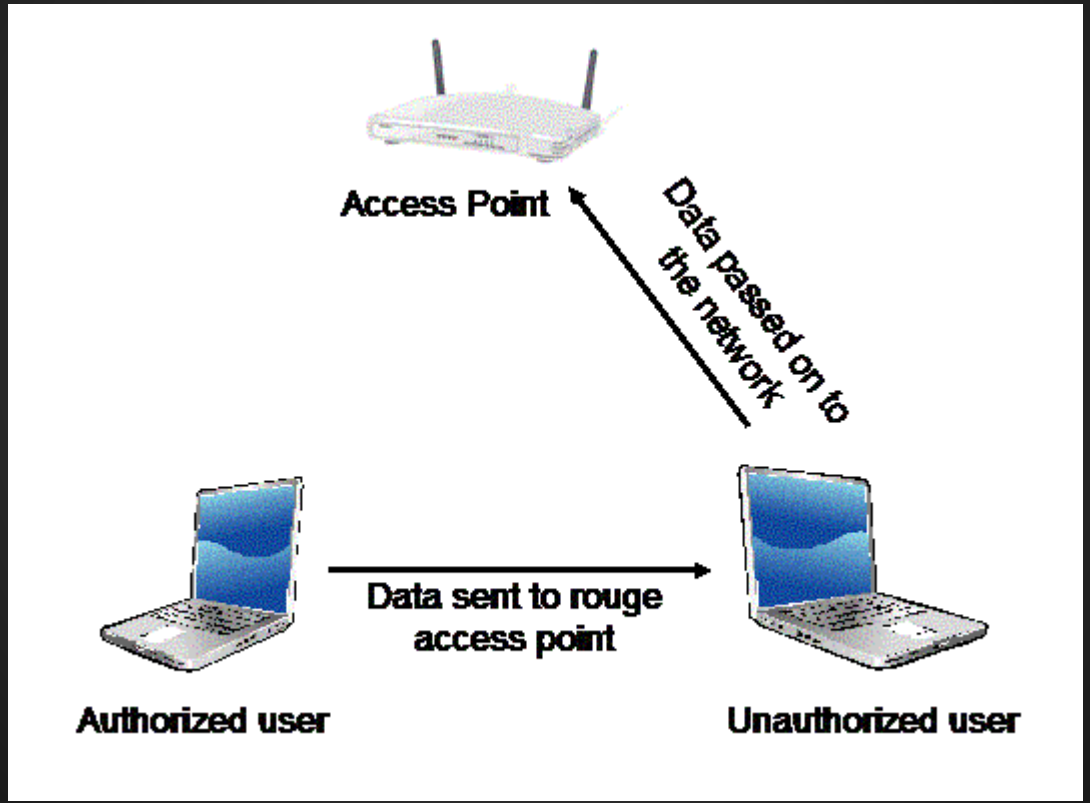
Exploiting PNLs

Karma - ~2005 published and highly visible to impersonate AP (Evil Twin)

Manna - Intelligent Rogue

Credential Harvesting - Capture enterprise creds to use elsewhere

MitM


Access Point
Data passed on to the network
Data sent to rouge access point
Authorized user
Unauthorized user

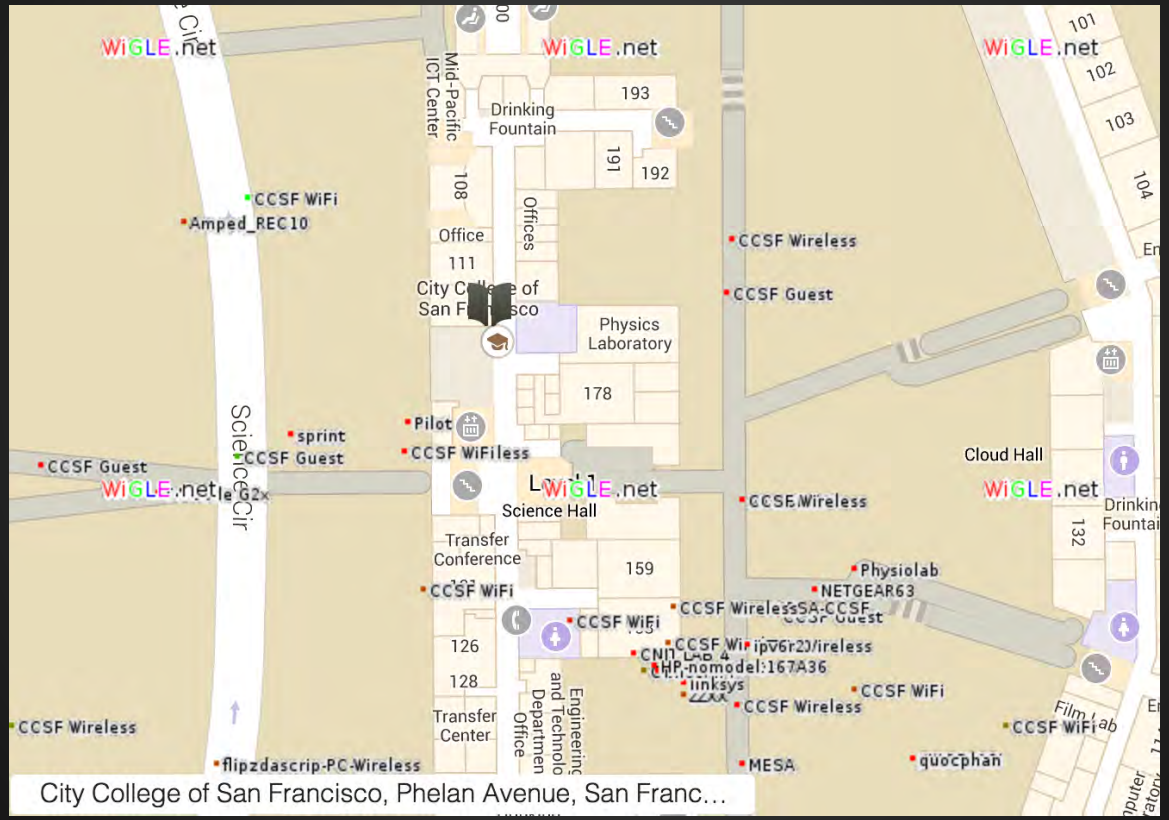
PNL Rich Environs

Coffee Shops
Airports
On airplanes
Universities
Malls

Exploiting PNLs

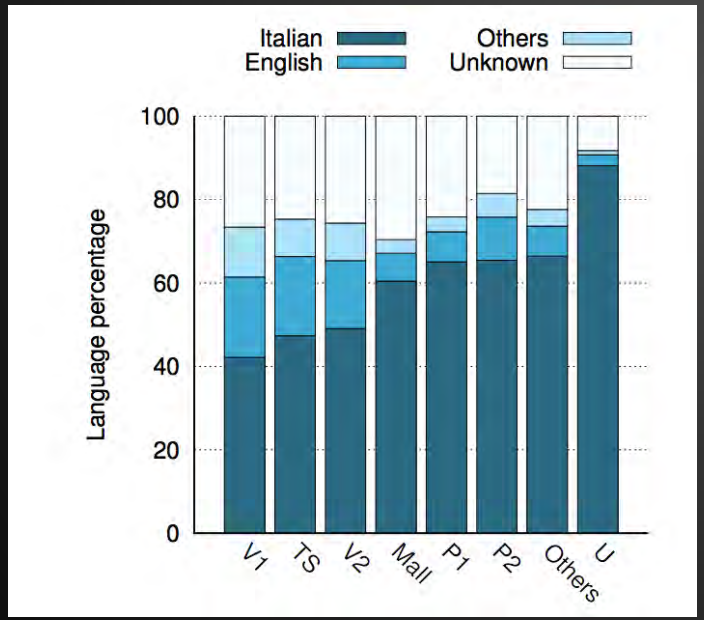
What else can I do with the PNL information?!

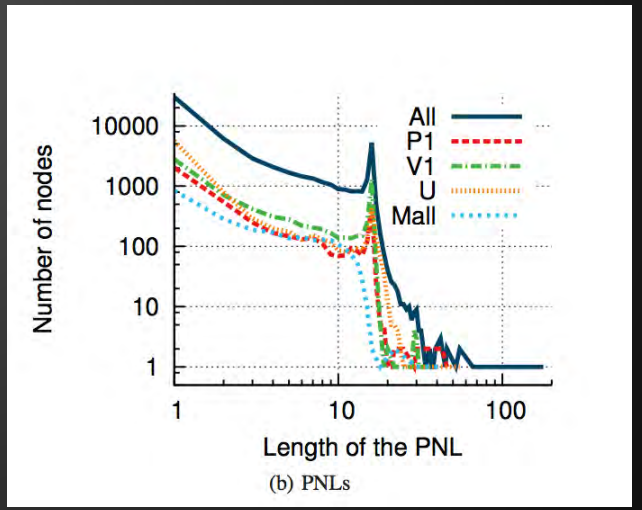
Other goodies



Other goodies, cont.

Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes

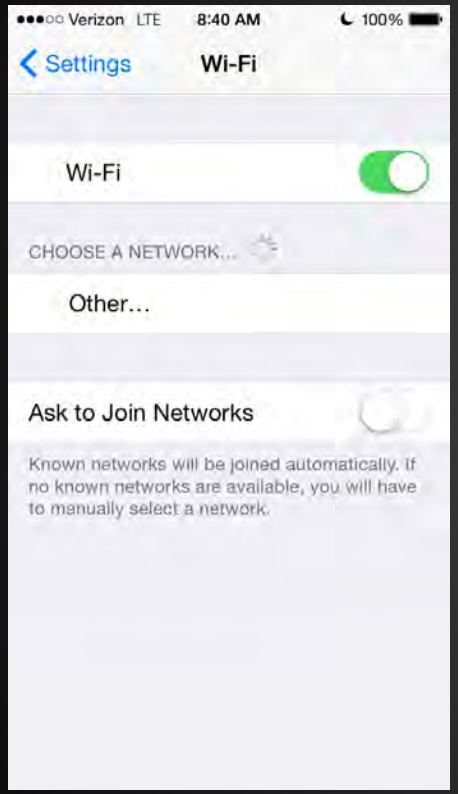




Risk Options

- AVOID the risk
- MITIGATE the risk
- TRANSFER the risk
- ACCEPT the risk

Mitigate the risk



- Educate users
  - Avoid open APs
- Always use VPN
- SSL
  - even this has risks
- Disable auto-connect
- Change IEEE 802.11?!

Risk: Redux

- Importance of providing accurate risk assessment to org leaders
  - Work with facts and objective data
  - Explain risks and clear language
  - Tie to events in the news
  - Evaluate what peer orgs are doing
  - Use metrics & graphs

Q&A
Discussion

References & Links+

http://conferences.sigcomm.org/imc/2013/papers/imc148-barberaSP106.pdf
http://www.privatewifi.com/a-hacker%E2%80%99s-toolkit/
http://www.slideshare.net/rgillen/code-stock-wireless
http://www.securitytube.net/groups?operation=view&groupId=9
http://www.willhackforsushi.com/presentations/Practical_Wireless_Security_Threats-VA_Tech_2008.pdf
http://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html
http://www.net-security.org/secworld.php?id=14934
http://www.techrepublic.com/resource-library/whitepapers/new-avatars-of-honeypot-attacks-on-wifi-networks/
http://www.sophos.com/en-us/security-news-trends/security-trends/bottom-line/project-warbike.aspx?cmp=701j0000000ZaL9AAK
http://forums.imore.com/ios-6/260534-how-clear-wifi-network-preferred-list.html
https://www.youtube.com/watch?v=szroUxCD13I
https://www.defcon.org/images/defcon-22/dc-22-presentations/White-deVilliers/DEFCON-22-Dominic-White-Ian-de-Villiers-Manna-from-Heaven-Detailed-UPDATED.pdf
Vivek's SecurityTube Website - "MegaPrimer"

Cyberwire
Bsides
RSA
ISSA http://www.issaef.org/active_scholarship