PARKING LOT UNDER POLICE SURVEILLANCE
DO NOT LEAVE VALUABLES IN VEHICLE

Am I Being Spied On?

Low-tech Ways Of Detecting High-tech Surveillance

Dr. Phil

@ppolstra

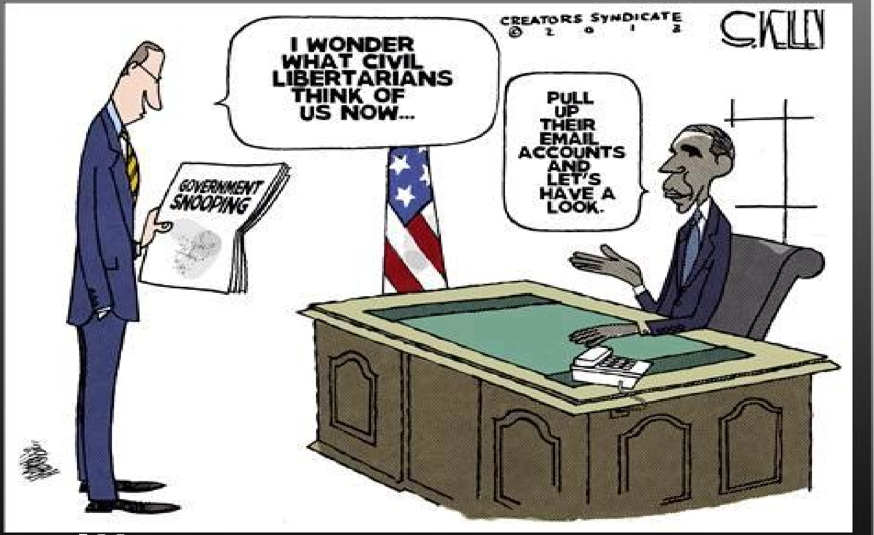
http://philpolstra.com

What this talk is about

- Determining if you are a victim of spying
  - Video surveillance
  - Tailing
  - Audio eavesdropping
  - Devices embedded in your computer, tablet, or smart phone

Why you should care

- Government assault on Constitution is well known
- Local governments
- Competitors
- Stalkers
- People who just don't like you


CREATORS SYNDICATE © 2013
C.KELLY
I WONDER WHAT CIVIL LIBERTARIANS THINK OF US NOW...
GOVERNMENT SNOOPING
PULL UP THEIR EMAIL ACCOUNTS AND LET'S HAVE A LOOK.

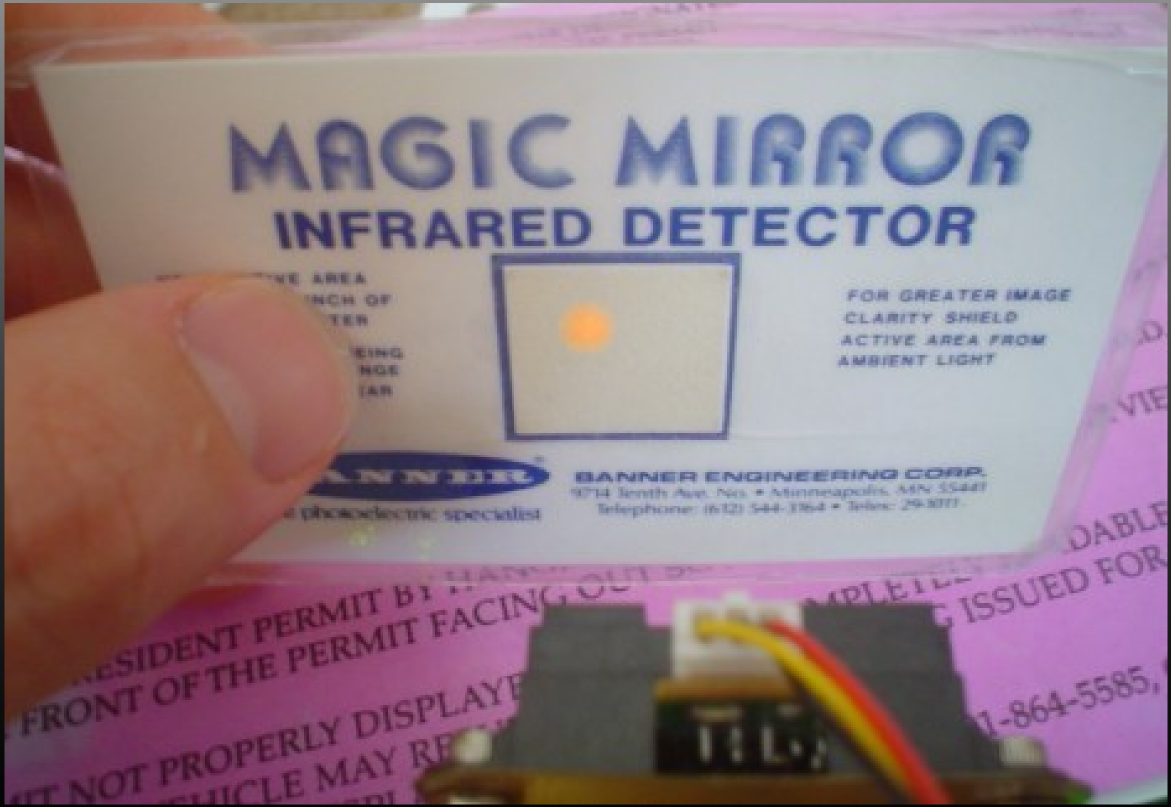
Video surveillance

Common flaw all night vision cameras share

Detecting this flaw with any digital camera

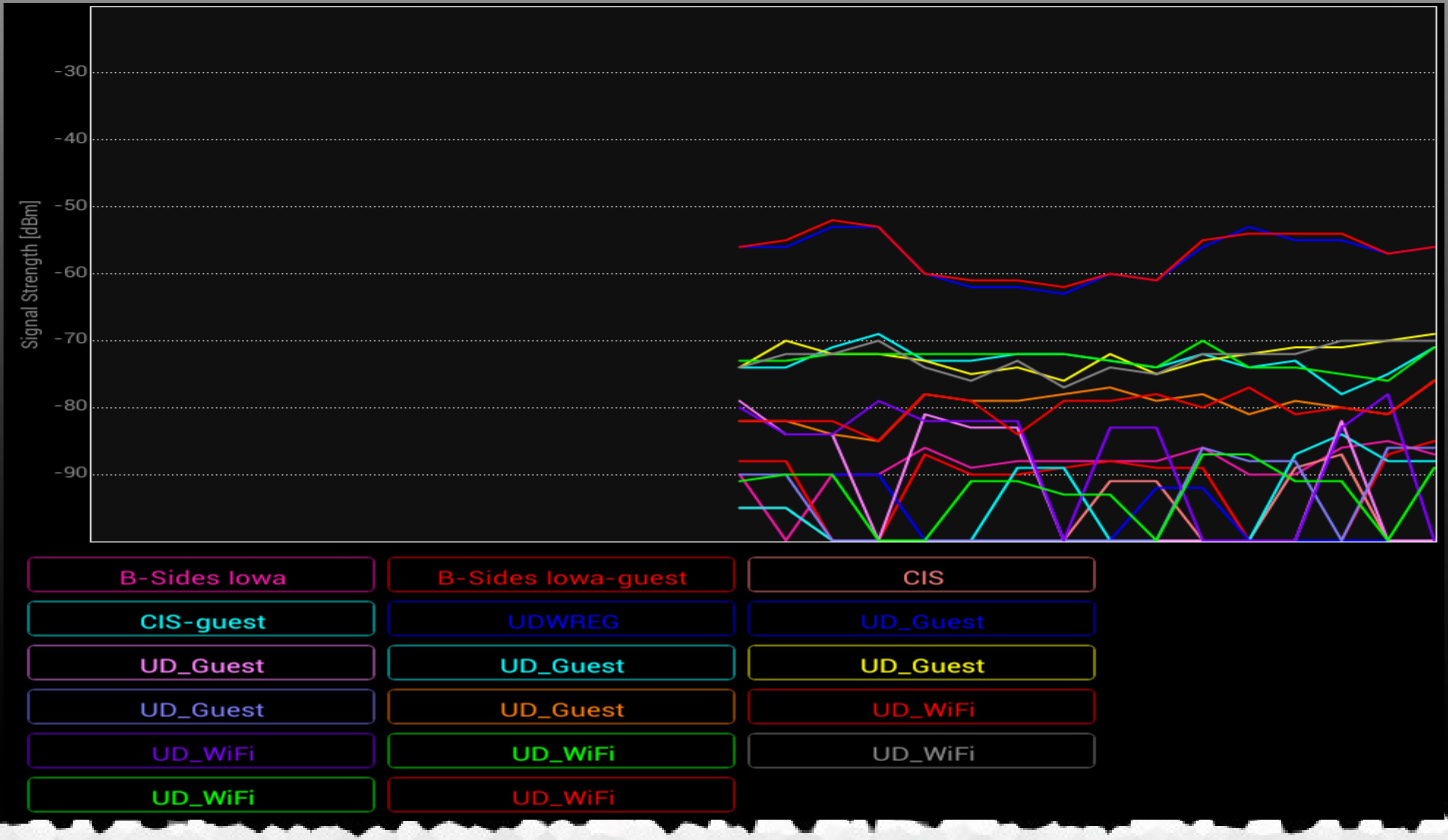
Finding a camera with a phone

Other Ways to Detect IR


MAGIC MIRROR
INFRARED DETECTOR
FOR GREATER IMAGE CLARITY SHIELD ACTIVE AREA FROM AMBIENT LIGHT
BANNER
photoelectric specialist
BANNER ENGINEERING CORP.
9714 Tenth Ave. No. • Minneapolis, MN 55441
Telephone: (612) 544-3164 • Telex: 29-1017
RESIDENT PERMIT BY
FRONT OF THE PERMIT FACING OUT
NOT PROPERLY DISPLAYE
VEHICLE MAY RE
ISSUED FOR
1-864-5585,

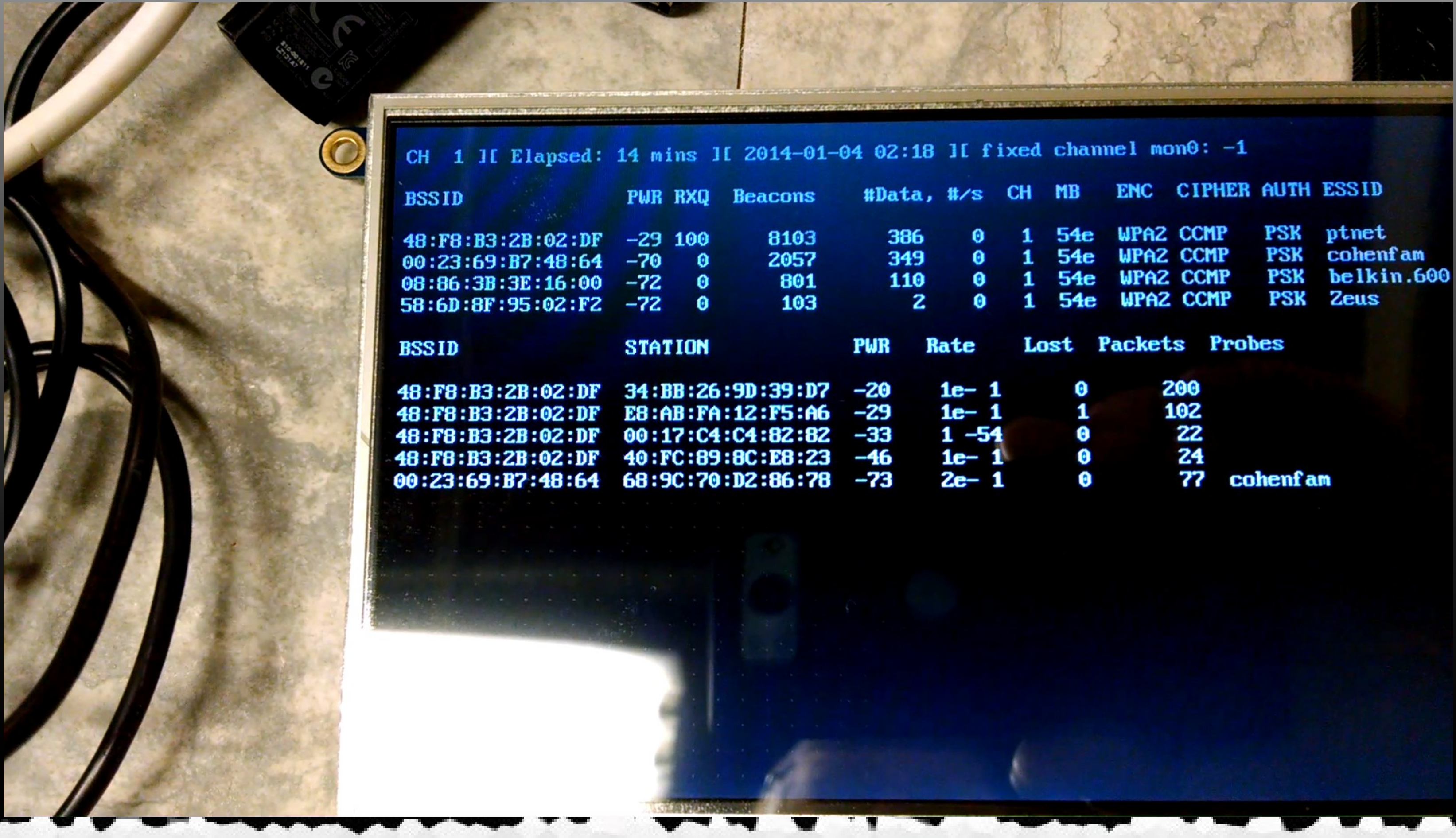
Detecting wireless cameras

Free way: Android tablet or smartphone (ad hoc nets)



Inexpensive way: BeagleBone based system

Simple way using Airodump-ng



```
 CH  1 ][ Elapsed: 14 mins ][ 2014-01-04 02:18 ][ fixed channel mon0: -1

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

 48:F8:B3:2B:02:DF  -29 100     8103      386    0   1  54e  WPA2 CCMP   PSK  ptnet
 00:23:69:B7:48:64  -70   0     2057      349    0   1  54e  WPA2 CCMP   PSK  cohenfam
 08:86:3B:3E:16:00  -72   0      801      110    0   1  54e  WPA2 CCMP   PSK  belkin.600
 58:6D:8F:95:02:F2  -72   0      103        2    0   1  54e  WPA2 CCMP   PSK  Zeus

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 48:F8:B3:2B:02:DF  34:BB:26:9D:39:D7  -20    1e- 1      0      200
 48:F8:B3:2B:02:DF  E8:AB:FA:12:F5:A6  -29    1e- 1      1      102
 48:F8:B3:2B:02:DF  00:17:C4:C4:82:82  -33    1 -54      0       22
 48:F8:B3:2B:02:DF  40:FC:89:8C:E8:23  -46    1e- 1      0       24
 00:23:69:B7:48:64  68:9C:70:D2:86:78  -73    2e- 1      0       77  cohenfam
```

Slightly more sophisticated with Python

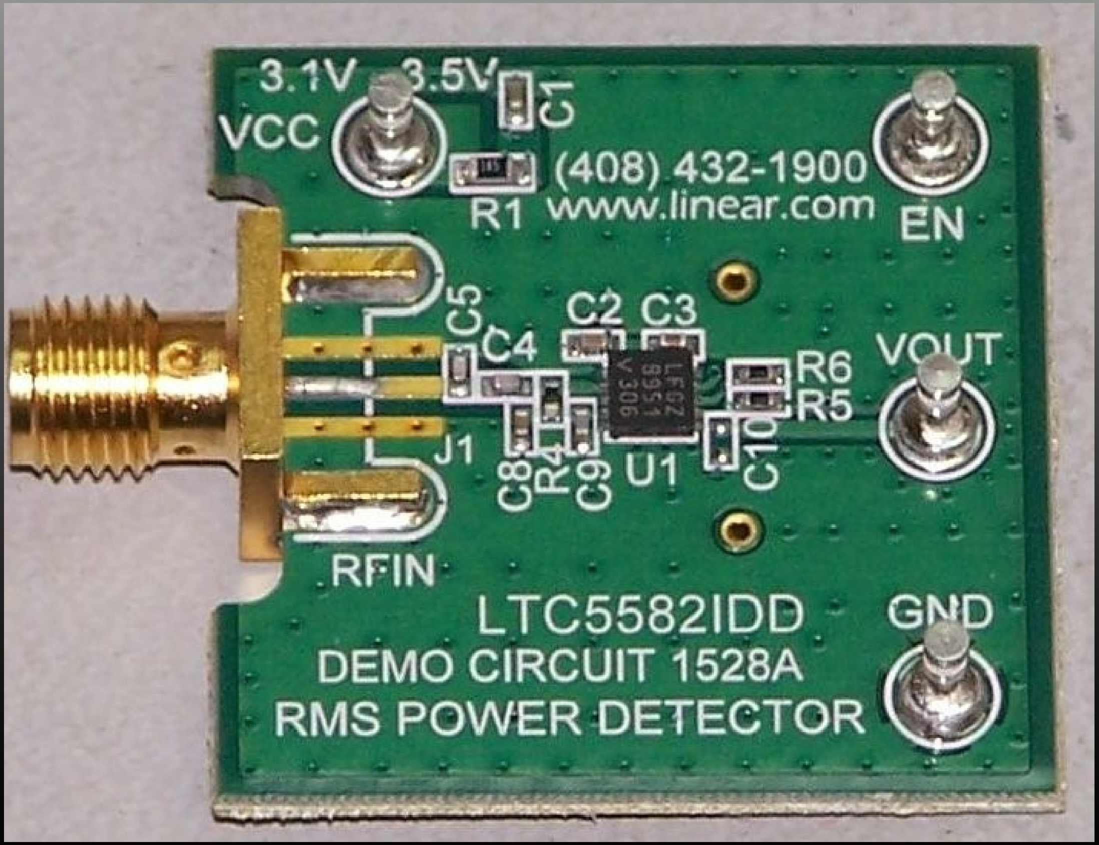
```
#!/usr/bin/env python
from scapy.all import *
import os, sys, time, operator
interface = "mon0"
clientsIKnow = { }

def sniffClientStrength(p):
    if p.haslayer(RadioTap) and p.haslayer(Dot11):
        try:
            sigStrength = int(-(256-ord(p.notdecoded[-4:-3])))
            if str(p.addr2) not in clientsIKnow.keys():
                clientsIKnow[str(p.addr2)] = sigStrength
            else:
                if sigStrength > clientsIKnow[str(p.addr2)]:
                    clientsIKnow[str(p.addr2)] = sigStrength
        except KeyboardInterrupt:
            sys.exit(1)
        except:
            pass

def main():
    os.system('clear')
    try:
        while True:
            sniff(iface=interface, prn=sniffClientStrength, timeout=2)
            if clientsIKnow:
                sorted_list = sorted(clientsIKnow.items(), key=lambda x: x[1], reverse=True)
                for item in sorted_list:
                    print item[0], item[1]
            time.sleep(1)
            os.system('clear')
            clientsIKnow.clear()
            sorted_list = []
    except KeyboardInterrupt:
        pass

if __name__ == '__main__':
    main()
```

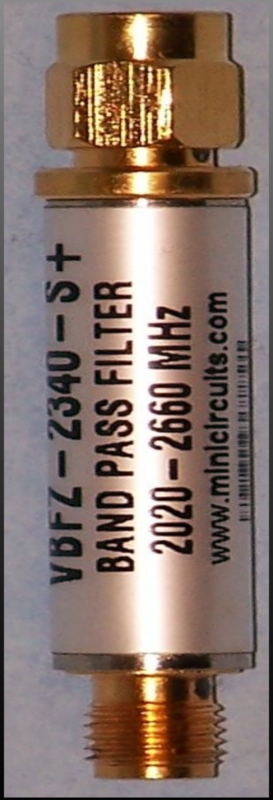
More sophisticated Way

Moderately expensive way: Detecting signals in licensed bands

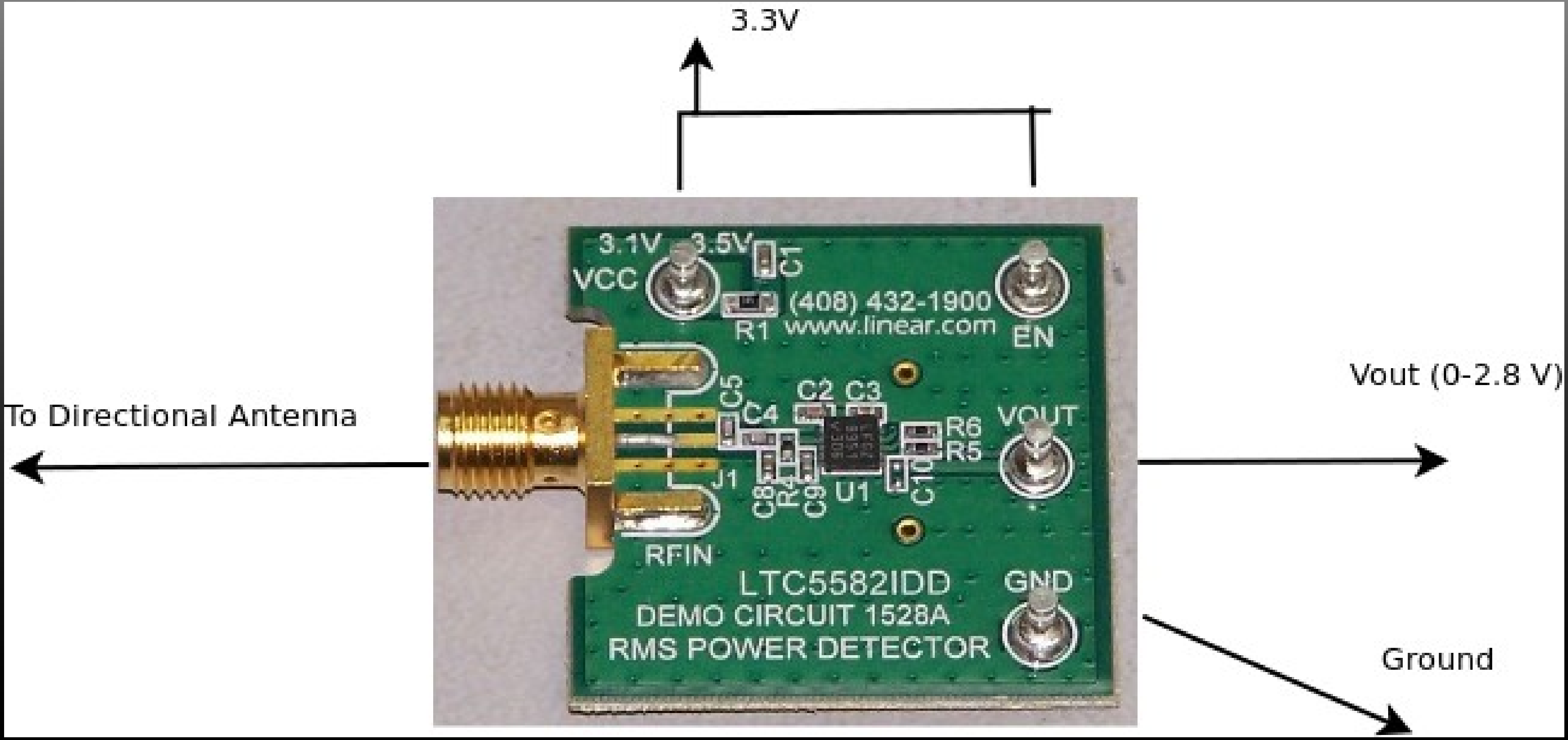
- Use an Linear Technologies LTC5582 RMS RF power detector
- Measure LTC5582 output on volt meter or BeagleBone or ??
- Bandpass filters can be used to look at individual frequency bands

Moderately Expensive Way





Moderately Expensive Way



Physical surveillance

- Tailing
  - Common vehicles used
  - Standard techniques
- Stakeout
  - Common vehicles used
  - Standard techniques

Tailing Vehicles

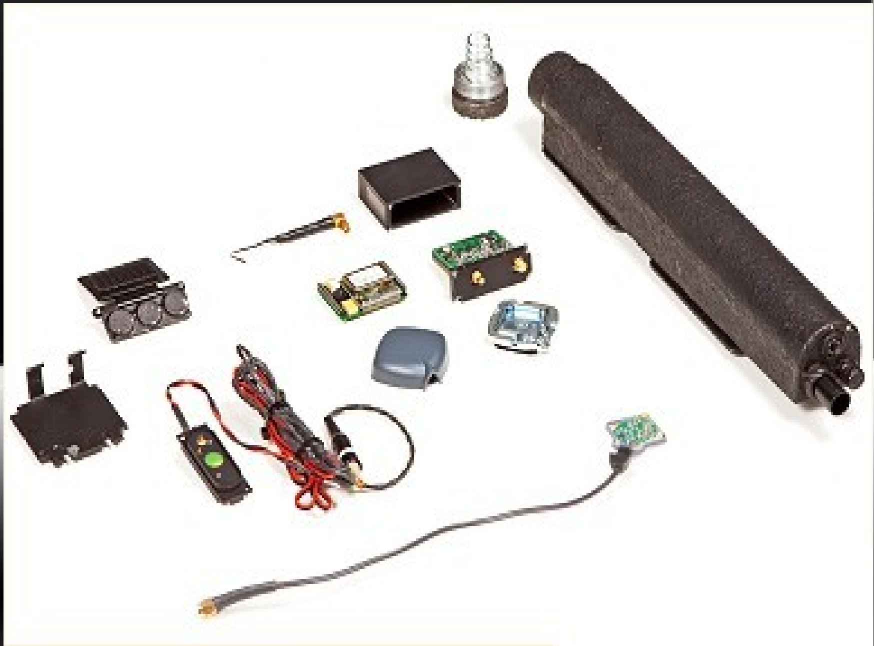
- Non-government spies choose vehicles to blend in
  - Probably not the red Ferrari behind you
  - Likely vehicles
    - Bland colored Honda or Toyota sedan
    - Bland colored SUV
    - Whatever is commonly seen in the area
- Government spies drive vehicles issued to them
  - Black SUV
  - Crown Victoria
  - Other vehicles too!

General Tailing Techniques

- Follow distance varies from about 2 cars behind to a block
- Bumper beeper may be used to extend follow distance to 0.5 – 10.0 miles
- Tail is generally considered blown if subject has 3 suspicious impressions

Single Car Tailing

- Generally will be closer than multi-car tails
- More likely to follow traffic laws
- May use a bumper beeper to help relocate the subject if lost



Multi-car Tailing

- In most cases everyone is behind the subject
- Some cars may be on parallel streets
  - More likely in urban areas
- Tailing vehicles may change relative positions
- Vehicles might occasionally appear to go a different direction only to rejoin later

Combating Tailing

- Look!
  - Check around your car for trackers
  - Watch for vehicles who seem to be behind you for long distances
  - Watch for vehicles that go away and then come back

Combating Tailing (contd)

- Detect electronic devices
  - Use the previously describe RF detection system without any filters
  - Scan the AM radio band on your car radio before you go
    - Many homemade or privately available trackers operate in this frequency band
    - If you hear nothing but a strong tone it is probably a tracker on your car!

Combating Tailing (contd)

- Active techniques
  - Drag a few traffic lights
  - Take unusual routes
  - Drive through residential neighborhoods
  - Take a few alleys or deserted side streets
  - Occasionally park for no reason

Stakeout Vehicles

- Same vehicles used in tailing may be used
- Additional vehicles might be used
  - SUV
  - Commercial vans
  - Pickup trucks with toppers

Combating Stationary Surveillance

- Look!
  - People in parked vehicles
  - Construction/utility workers who are around too long or appear to be doing nothing
  - Commercial vans parked for extended periods
  - Anyone with view of all your exits

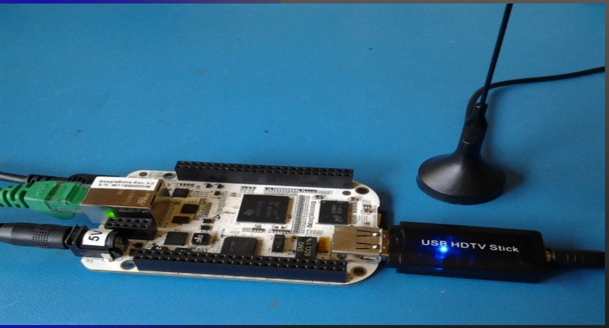
Combating Stationary Surveillance (contd)

- Active techniques
  - Get out your binoculars and spy back
  - Run outside and jump in your car
    - Run back inside and see if anyone seems to notice
    - Drive around the block and see if anyone followed you

Audio bugging

Detecting active bugs

- Free way: analog AM/FM radio might detect some bugs
- Inexpensive way: USB TV Tuner Software Defined Radio (SDR)



  - Can detect signals in 50 MHz - 2 GHz
  - Commercial bugs are usually 10 MHz - 8 GHz
- Moderately expensive way: Broadband amplifier connected to TV antenna
- Expensive way: Drop $500 on a commercial detector

Detecting bugs with a radio

- Must be analog
- Scan through the AM/FM bands to see if you can hear the audio you are generating
- Works with only the simplest bugs

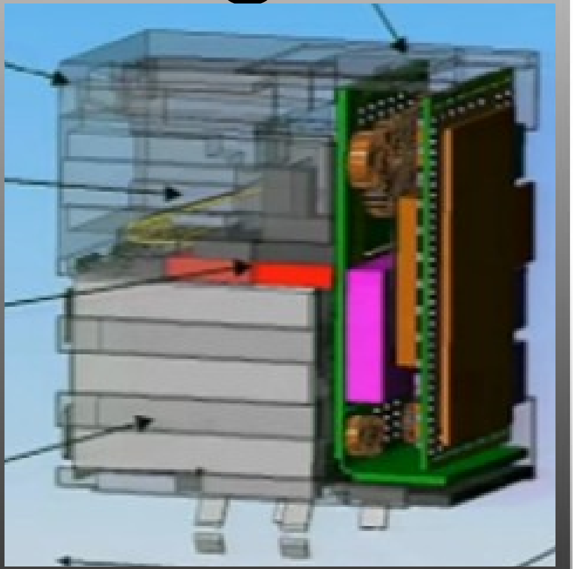
Detecting passive bugs

- Must try to excite bug with RF in correct band
- If you are close enough and the signal is strong can still work with wrong frequency
- Detection is same as active bugs

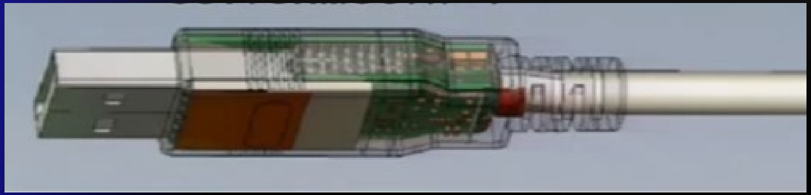
Exciting the bug

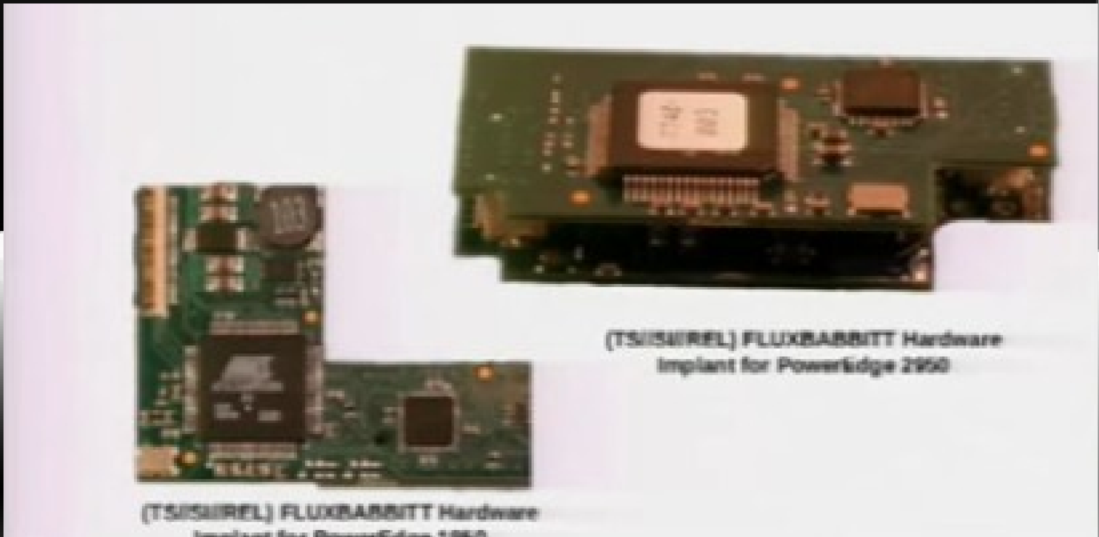
- Free way: Blast it with 2.4 GHz from your Alfa
- Inexpensive way: Noisy broadband transmitter attached to TV antenna

Bugs in your computing devices



- Bugs can be installed by
  - intercepting shipments
  - "service" professionals
  - spies in your local IT staff
  - pissed off guy in your office

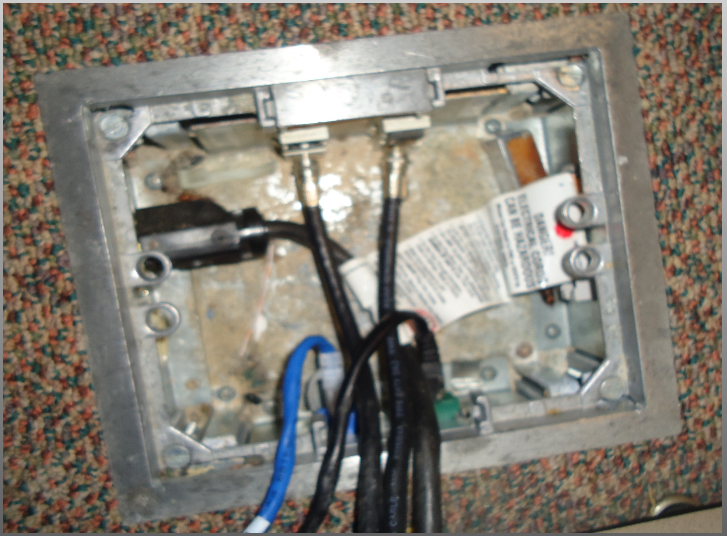


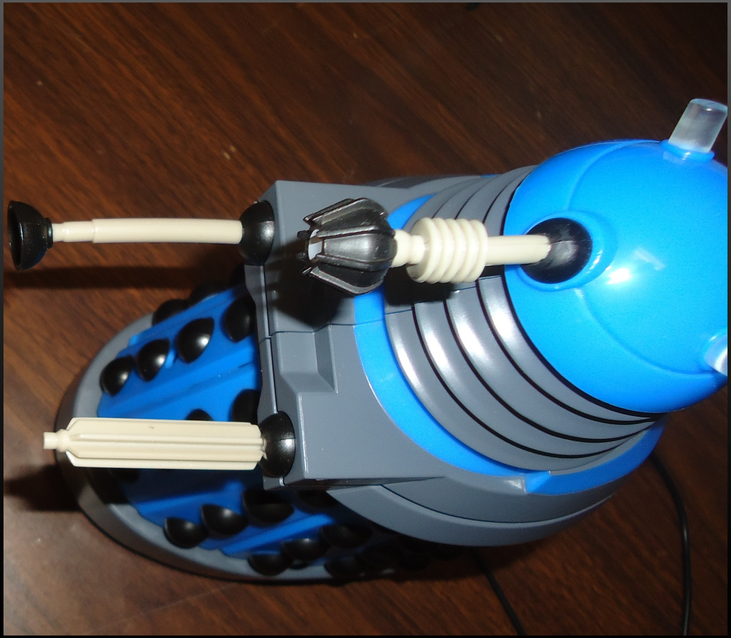

(TS//SI//REL) FLUXBABBITT Hardware
Implant for PowerEdge 2950
(TS//SI//REL) FLUXBABBITT Hardware

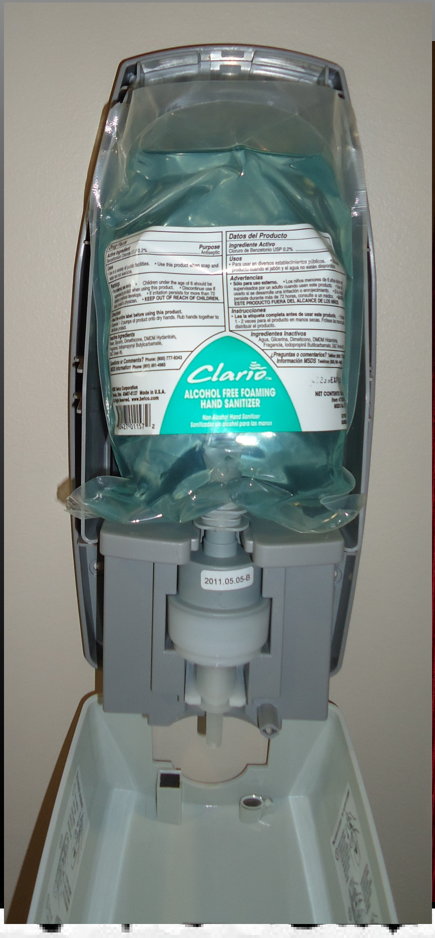
Detecting bugs

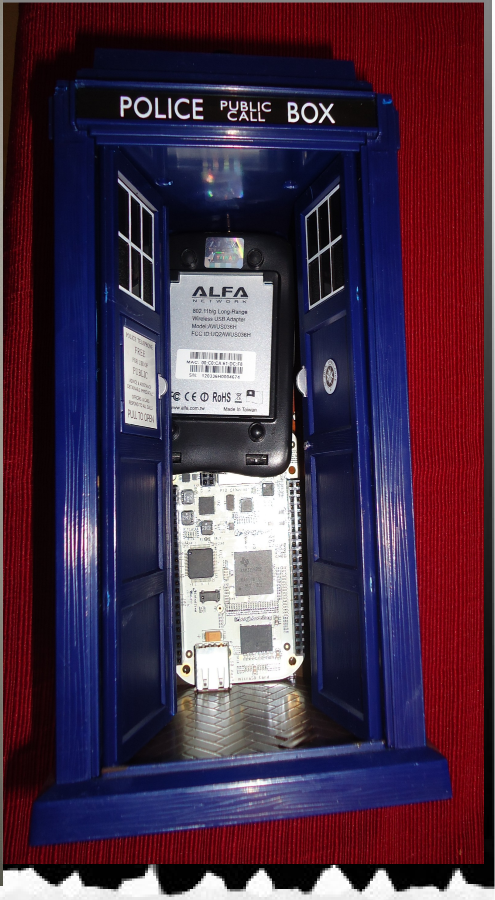
- Free way: Look!
  - Bugging devices can be installed externally
  - I described a small dropbox easily hidden behind a computer at DC21
  - Same dropbox is easily hidden in other items on your desk
    - Example: Dalek desktop defender
    - Example: TARDIS
- Check every device connected to your computer especially USB and network

Hiding Places









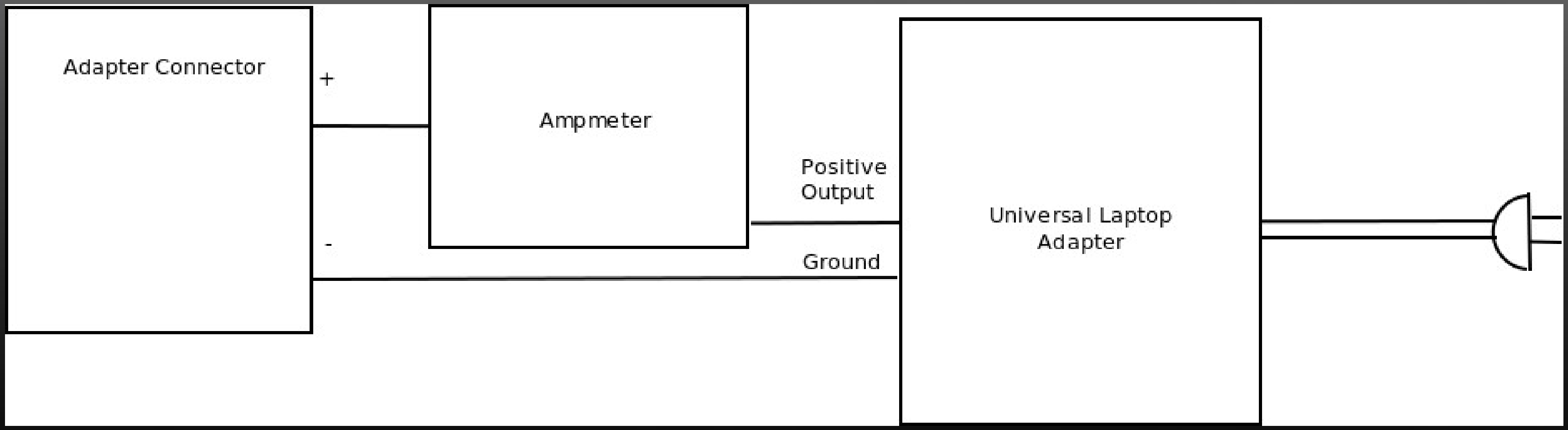
Bugs may be internal

- Open the case and look for obvious signs
- Pictures of NSA devices have been leaked
- Inexpensive way: Current leaks
  - Bugs need current to run
  - Turned off devices shouldn't draw any power

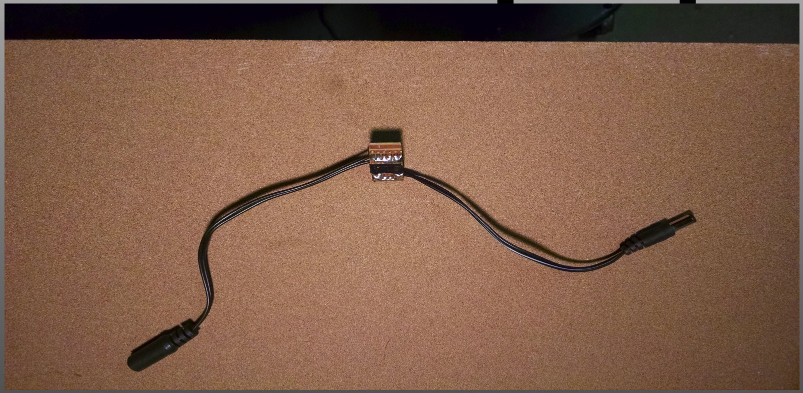
A modified universal laptop power supply can be used to detect this current leakage

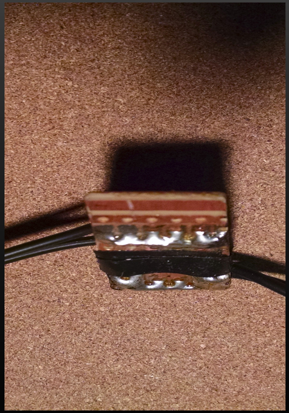
- Modify the power supply to detect current
- For laptop or phone remove the battery and measure current with device "off"
  - Current flow indicates possible bug
- For tablet fully charge the battery
  - Measure the current flow
  - Small current might indicate issue with charging circuit or battery
  - If the current peaks when you speak or move in view of the camera there may be a bug

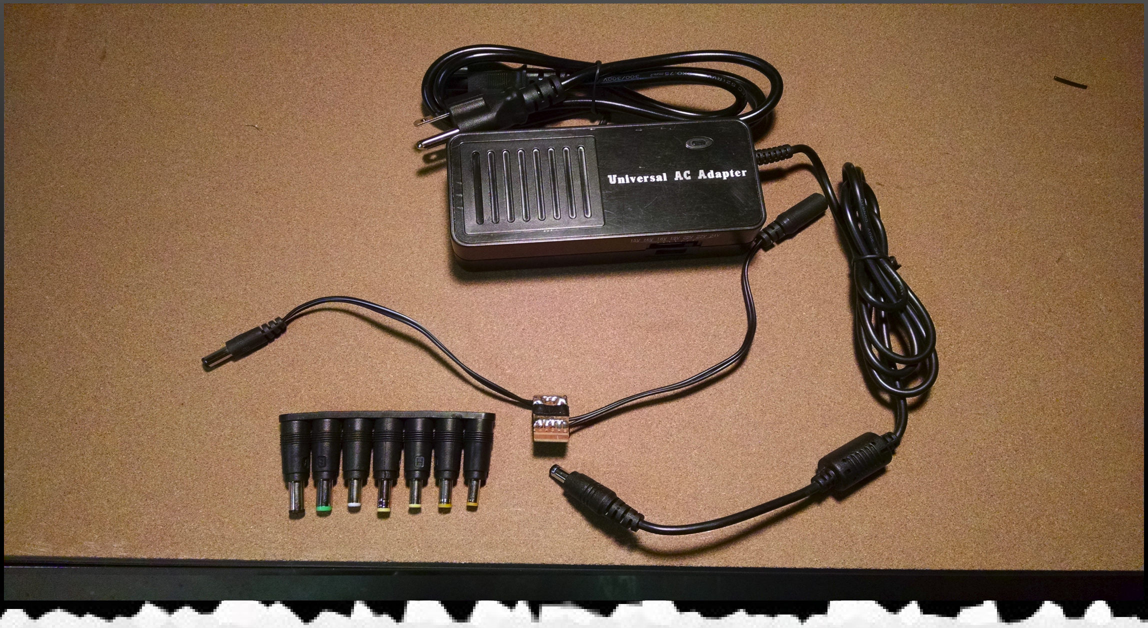
Laptop Adapter



Laptop Adapter







For a desktop computer

- Physical inspection is best
  - Can attempt to detect leakage current with Kill o Watt or similar
- Many computer power supplies leak current so this is not conclusive
- Desktop bug might only work when computer is on

Passive bugs

- Excite as described for passive audio bugs
- Use same techniques as described above to detect excited bug
- Won't detect all passive bugs (such as the expensive NSA bugs)

Summary

- Chose your level of paranoia
- Even if you aren't paranoid you can still detect many spying activities at no cost
- Truly paranoid can still test without financial ruin

References

- **Hacking and Penetration Testing with Low Power Devices** by Philip Polstra (Syngress, 2014)
- Jacob Appelbaum talk on NSA spy device catalog https://www.youtube.com/watch?v=vILAlhwUgIU

Questions?

- Come see me after
- @ppolstra on Twitter
- Http://philpolstra.com or http://polstra.org
- More info on BeagleBone drones