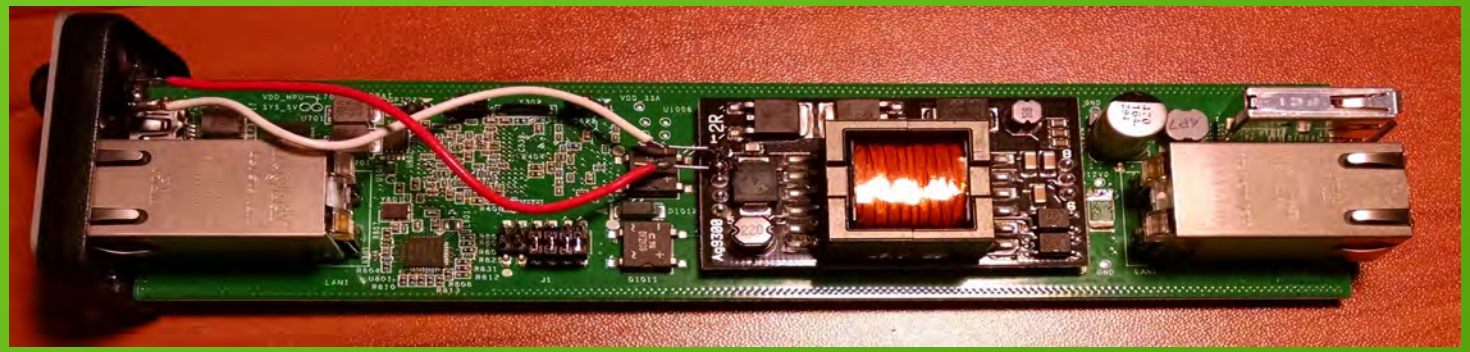
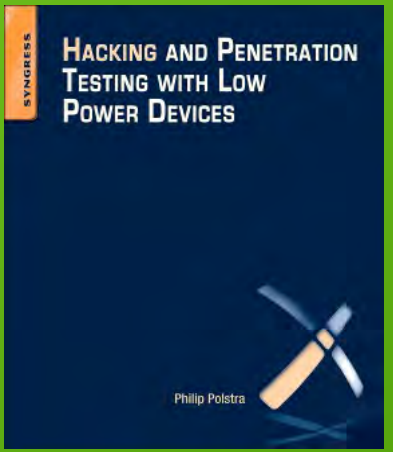
Hacker in the Wires

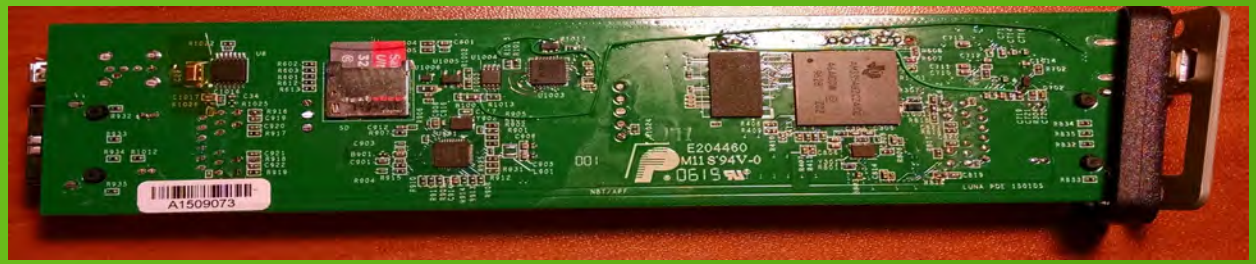
Phil Polstra
Bloomsburg University of Pennsylvania
@ppolstra
http://philpolstra.com



What is this talk about?

- A hacking device that lives on a gigabit Ethernet wire
  - Device is a CatchWire from WAW Technologies
  - Running DECK LINUX
  - Multiple command & control / exfiltration options
    - Network on which it is installed
    - Remote control via IEEE 802.15.4/ZigBee
    - Cellular network





Why should you care?

- CatchWire running Deck Linux is
  - Small
  - Flexible
  - Can be networked to integrate into sophisticated pentests
  - Easily installed
    - Data center: get all the packets
    - LAN segment: target part of the organization
    - Inline to single PC: laser focus
    - Unused desk: bypass all perimeter defenses

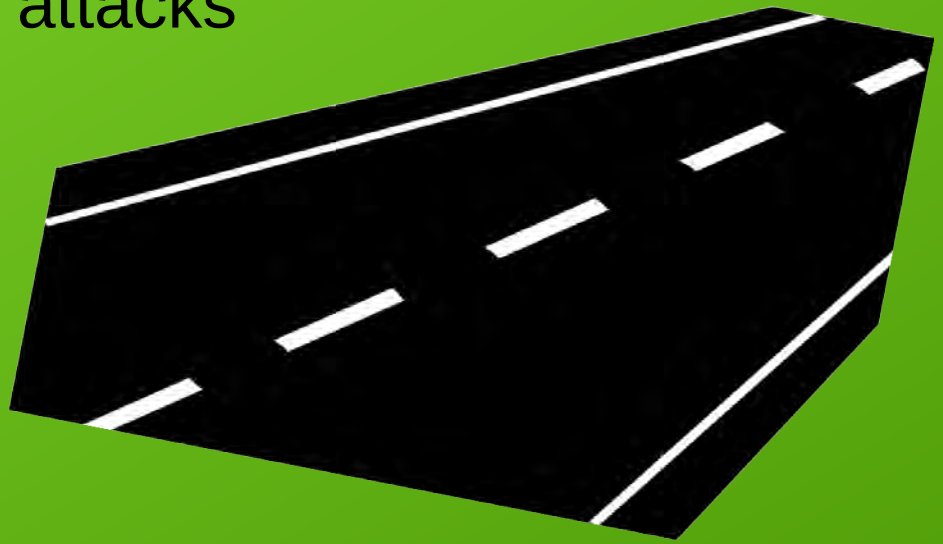
DECK LINUX

Who am I?

- Professor at Bloomsburg University teaching digital forensics & information security
- Author: Linux Forensics & HPTWLPD
- Programming from age 8
- Hacking hardware from age 12
- Also known to fly, build planes, and do other aviation stuff
- Course author for PentesterAcademy.com and others

Roadmap

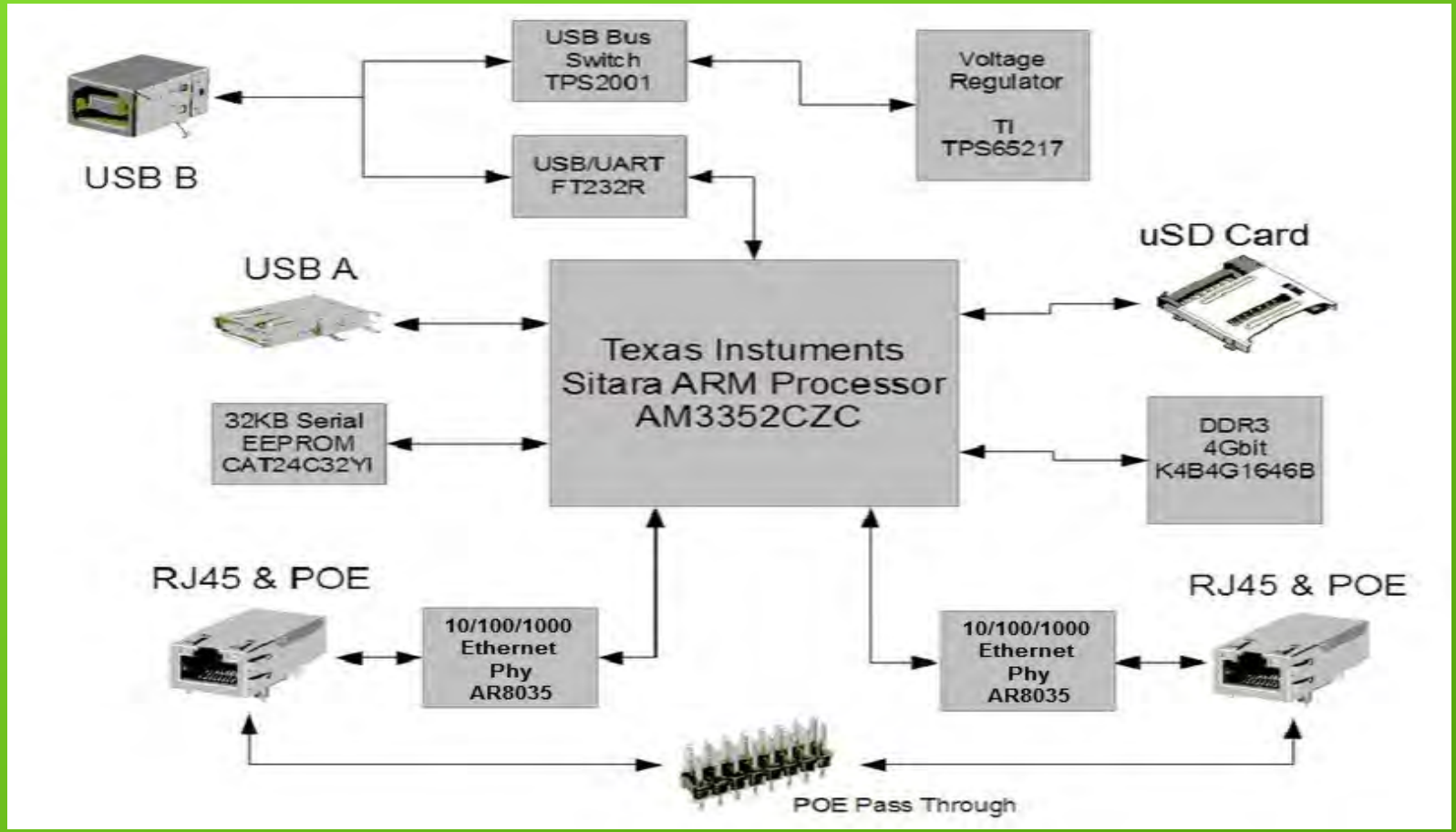
- Introduction to the CatchWire
- Introduction to The Deck Linux
- Attacks from CatchWire or BeagleBone Black (BBB)
- CatchWire specific attacks
- Future Directions



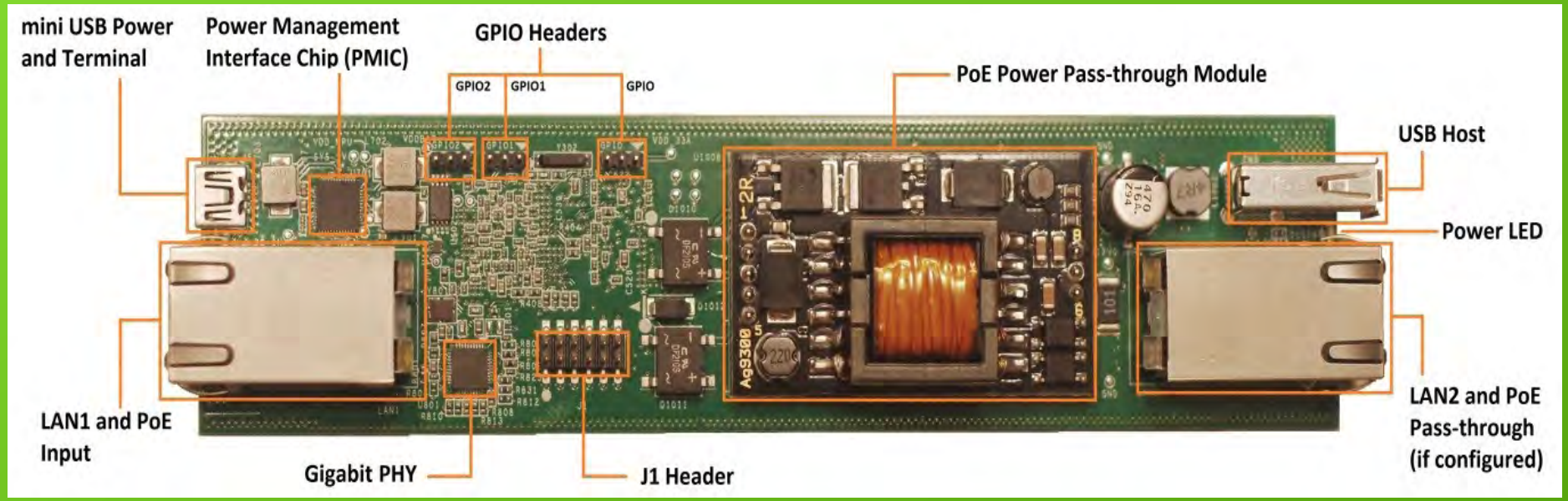
Meet the CatchWire

- Formerly Little Universal Netwwork Appliance (LUNA)
- Like BeagleBone Black (BBB) except:
  - Two gigabit Ethernet interfaces
  - Power over Ethernet (PoE)
  - Integerated FTDI USB to UART
  - No HDMI or GPIO headers

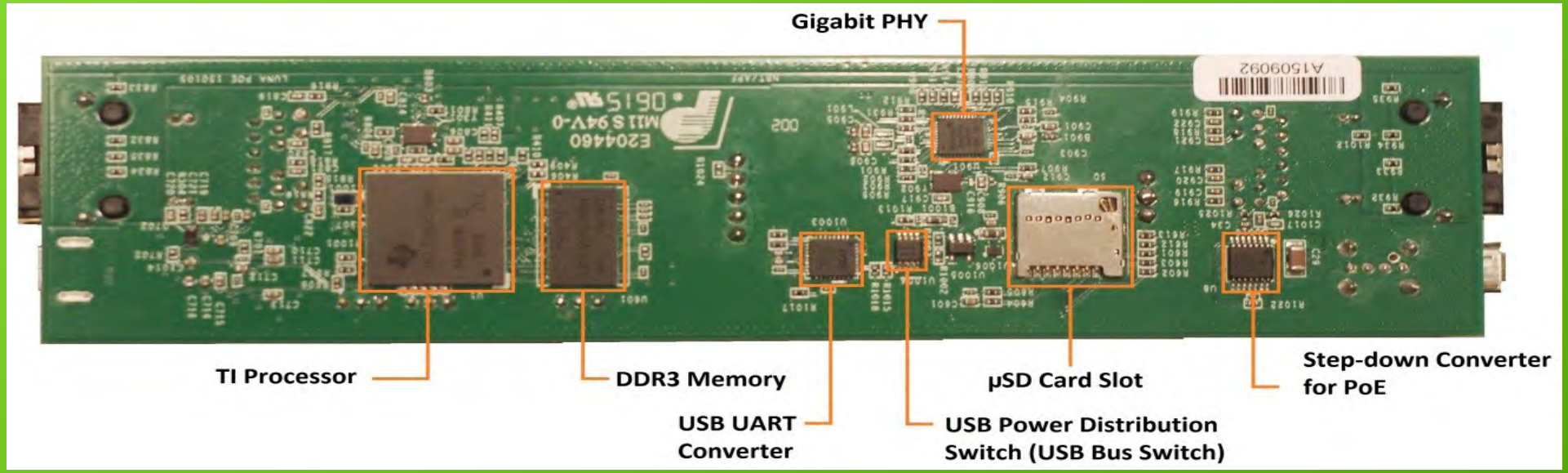
CatchWire: Block Diagram



CatchWire: Hardware

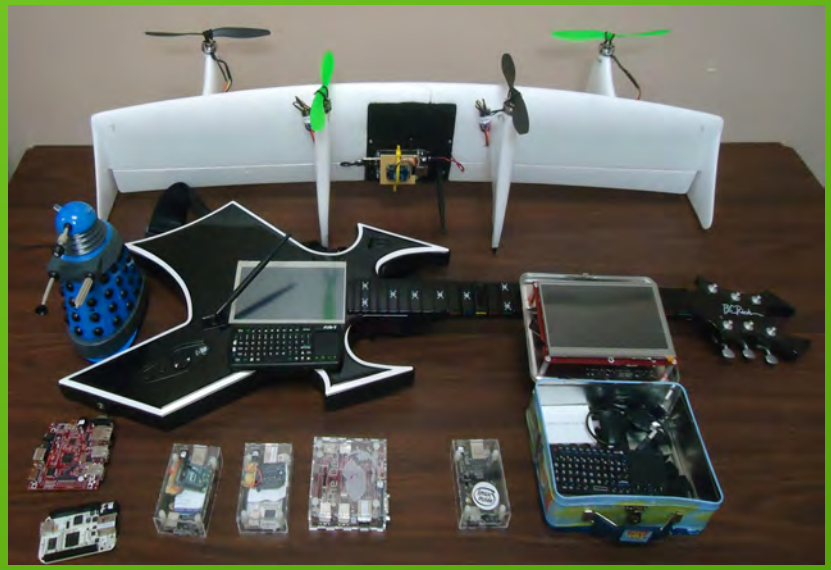


CatchWire: Hardware (cont.)



DECK LINUX

- Base OS
  - Built on Ubuntu 14.04
  - Optimized for pentesting with the BBB, CatchWire, and similar
  - Use as dropbox or hacking console
  - Over 4000 packages pre-installed (fluff free)
- MeshDeck
  - Adds remote control via 802.15.4/ZigBee networking
  - Allows coordinated attacks with multiple remote drones
- AirDeck
  - Combined with the MeshDeck to allow airborne drone or router
- 4Deck
  - Forensic add-on that automatically write blocks USB mass storage devices (udev rules-based)
- Udeck (USB-based attacks)
  - This is what my other talk (tomorrow) is about



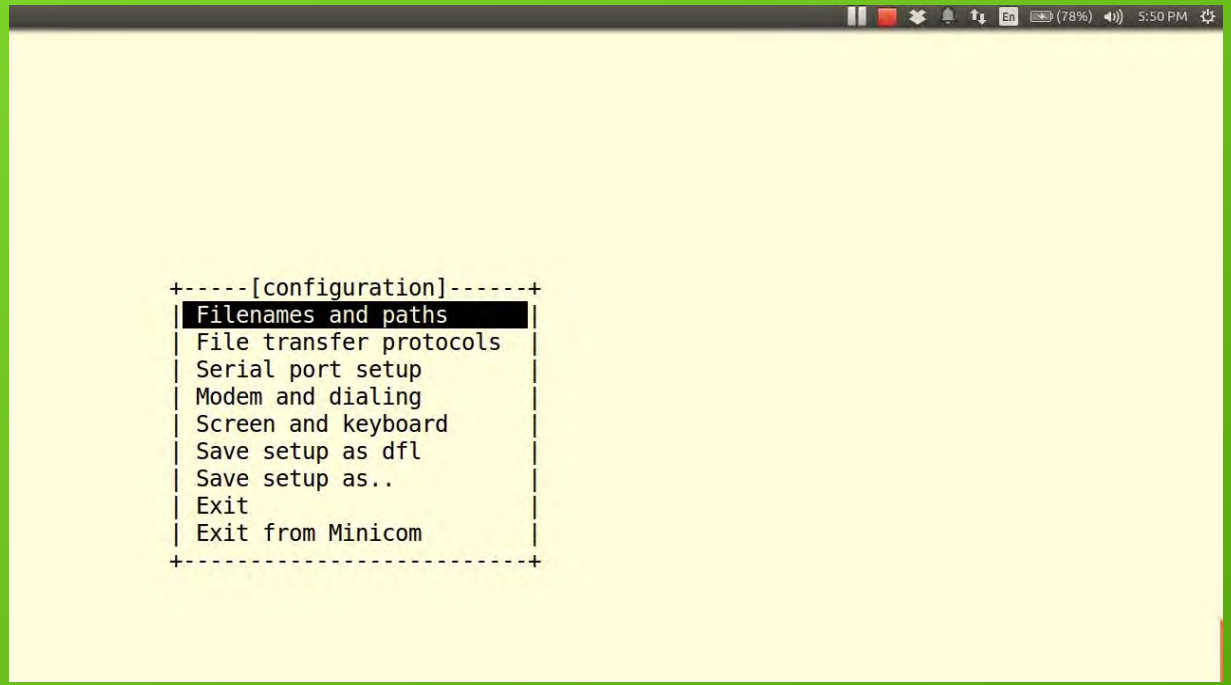
Powering the CatchWire

- PoE
  - Best choice when available
  - Power can be passed through using jumpers
- DC adapter
- USB power
  - Can be via a USB charger (2A or greater)
  - From PC, but not when Ethernet in use
    - USB specification limits power to 500 mA for USB 2.0

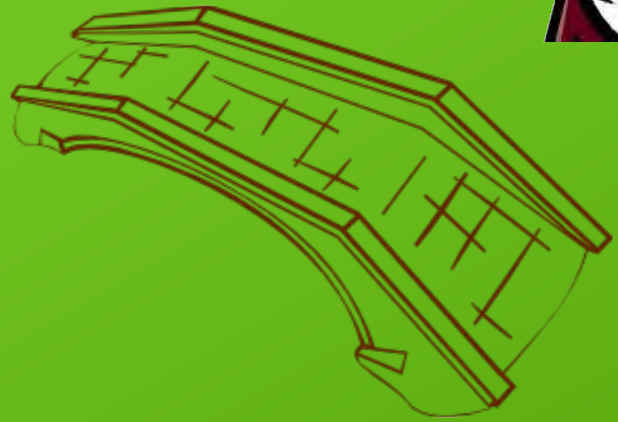
Initial Configuration

- Obtain image from http://facstaff.bloomu.edu/ppolstra
- Create microSD card using provided script (16 GB+)
- Install microSD card into CatchWire
  - Remove screws from microUSB socket side & slide out
- Connect to PC via USB
  - Log in as ubuntu/temppwd
  - Add/configure software as needed

Booting via USB power from PC



Selecting a Network Configuration



- Default is to bridge two Ethernet ports
- These can be split

cd /boot/uboot/dtbs

cp am335x-luna-demac.dtb am335x-luna.dtb

Comment out all lines in /etc/udev/rules.d/70-persistent-net.rules

- Going back
  - Uncomment lines in 70-persistent-net-rules
  - cp am335x-luna-switch.dtb over am335x-luna.dtb

Install the MeshDeck?

- MeshDeck allows remote control / exfiltration
  - Range up to 2 miles (3.2 km) without gateways/extenders
  - Out-of-band communication for most targets
  - Easy integration into multi-device pentest
  - Star network via IEEE 802.15.4 (Xbee series 1 adapters)
  - Mesh network via ZigBee (Xbee series 2 or ZB adapters)
- Requires USB Xbee adapter
- See DC21 talk and/or **Hacking & Penetration Testing with Low Power Devices** for details
- Permits access to CatchWire when Ethernet blocked

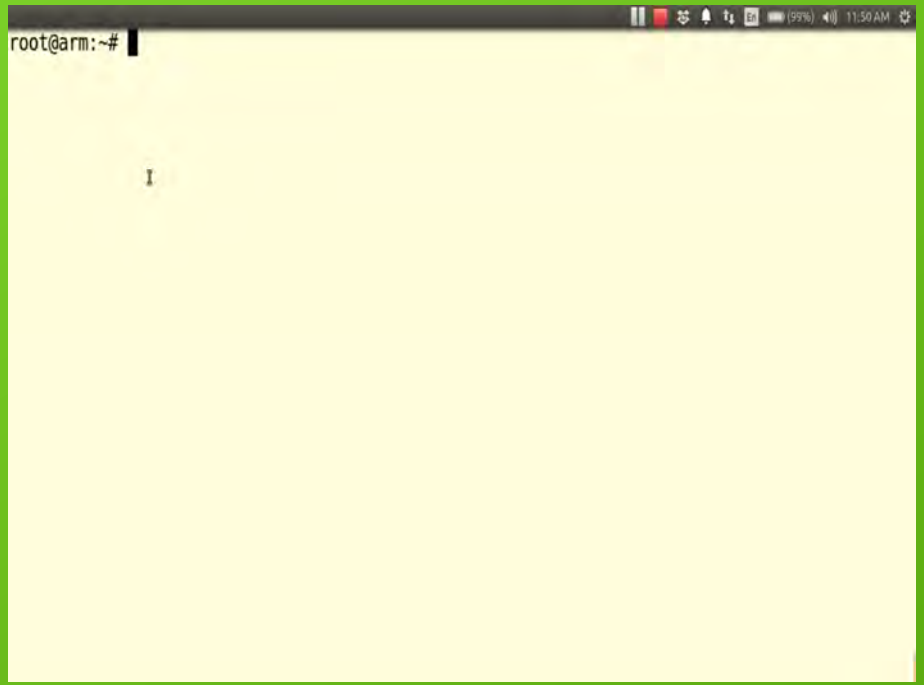
Demo: Exploiting an Old Friend

Let's Get Sniffing!

- CatchWire is installed inline for a LAN segment
- FTP server is running on a machine in this segment
- Capture all traffic to/from the host and pipe to egrep to get login

```
tcpdump -n host 192.168.1.120 -v -A | egrep '(USER\ )|(PASS\ )'
```

Demo: Sniffing Passwords

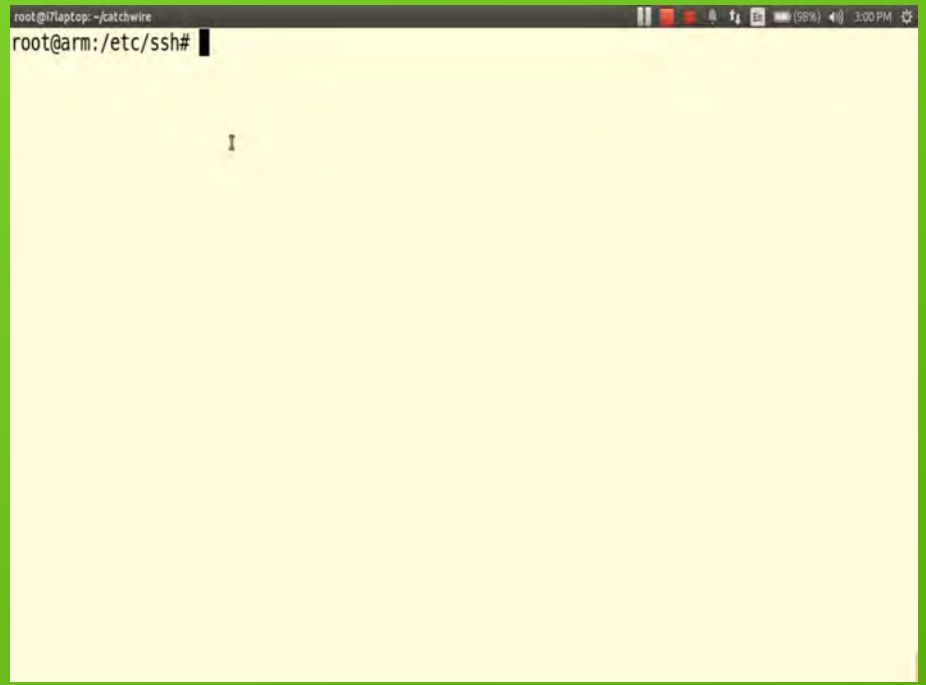


I Want To Use Wireshark

- You can use WireShark on your workstation to display packets passing through the CatchWire
- Must enable root login first
  - In /etc/ssh/sshd_config change “PermitRootLogin without-password“ to “PermitRootLogin yes”
- This can generate a lot of traffic, so you should probably use tcpdump filters!

ssh root@catchwire "/usr/sbin/tcpdump -s0 -w - " | wireshark -k -i -

Demo: Using CatchWire with WireShark



Other Possibilities

- Use MeshDeck to announce CatchWire IP address
- Use MeshDeck to toggle and/or focus sniffing
- Don't just sniff, inject some packets
- Use MeshDeck to communicate cracked passwords to other hacking drones running Deck Linux
- Try some online password cracking with Hydra
- Social engineering
  - Add stickers from IT deparment to CatchWire
  - Sell it as a network extender or performance booster

Questions?

- Demo Labs Saturday 12:00 – 14:00
- PentesterAcademy booth (??, ask if I'm not there)
  - Sign up for a chance to win one of two gift sets which include:
    - **Hacking and Penetration Testing with Low Power Devices**
    - **Linux Forensics**
    - CatchWire appliance