



# HARDWARE HACKING CHRONICLES

---

## IOT HACKING FOR OFFENCE AND DEFENCE

Fatih Ozavci

Managing Consultant – Context Information Security

# SPEAKER

---



- Fatih Ozavci, Managing Consultant
  - VoIP & phreaking
  - Mobile applications and devices
  - Network infrastructure
  - CPE, hardware and IoT hacking
- Author of Viproxy and VoIP Wars
- Public speaker and trainer
  - Blackhat, Defcon, HITB, AusCert, Troopers

# HEADLINES

---



- Subscriber services and IoT
- Hardware hacking chronicles
- Hacking broadband devices
- Hacking office devices
- Improving defense and offense

# INTERNET OF THINGS



- Everything is connected
- Broadband services
  - Smart modems
  - IPTV equipment
- Office devices
  - 3g/4g modems
  - IP phones
  - Keyboards & mouse
- Why should we evolve?

# WHY SHOULD SERVICE PROVIDERS CARE?

The image is a collage of various screenshots from different websites and news articles, illustrating the concept of 'information overload'. The screenshots include:

- A red banner with the text "WIR the IN" and "Home".
- A sidebar with "Pr" and "Anthon" at the top, followed by "Hacking", "Hack on yo", "Router fl", "exploit", "Out-of-date f", "By Chris Merri", "Wed May 27 201", and social sharing icons for Facebook (173), Twitter, Pinterest (28), and LinkedIn (25).
- A sidebar with "I WILL NO Back", "If you want your pull-re", "Some rand", "The backd", "Possible fix", "Probable s", "Backdoor I", and "Networking hardware vendor TP-Link says it will prevent the loading of open source firmware on routers it sells in the United States in order to comply with new Federal Communications Commission requirements".
- The Australian Government logo and the text "Australian Government" and "Office of the Australian Information Commissioner".
- A navigation bar with links to "About us", "Media & speeches", "Engage with us", "Privacy law", "Individuals", "Agencies & organisations", "Freedom of information", and "Information policy".
- A large article title "Opening statement to Senate Estimates – Timothy Pilgrim" with a photo of a man speaking.
- A paragraph about Timothy Pilgrim appearing at Parliament's Senate Estimates to answer questions on the current work of the Office of the Australian Information Commissioner (OAIC). It mentions his opening statement outlining priority areas and updates on the OAIC's workload and responsibilities under the Privacy Act 1988 and the Freedom of Information Act 1982.
- A link to "» Read the opening statement".
- A section titled "Privacy".
- Two sections at the bottom: "For individuals" and "Agencies & organisations".
- A sidebar on the right with "CONTACT US" (1300 363 992, [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)), "Make a privacy complaint", and "» More contact details".
- A "TRANSLATIONS" section with flags of various countries.
- A "Community languages" section.
- A "NEW WEBSITE HELP" section.

# CONSUMER SERVICES AND PRODUCTS

---

Broadband & 3G/4G

IPTV/Satellite Broadcasting & VoD

Home & Office Equipment

# TRADITIONAL TESTING IS NOT SUFFICIENT

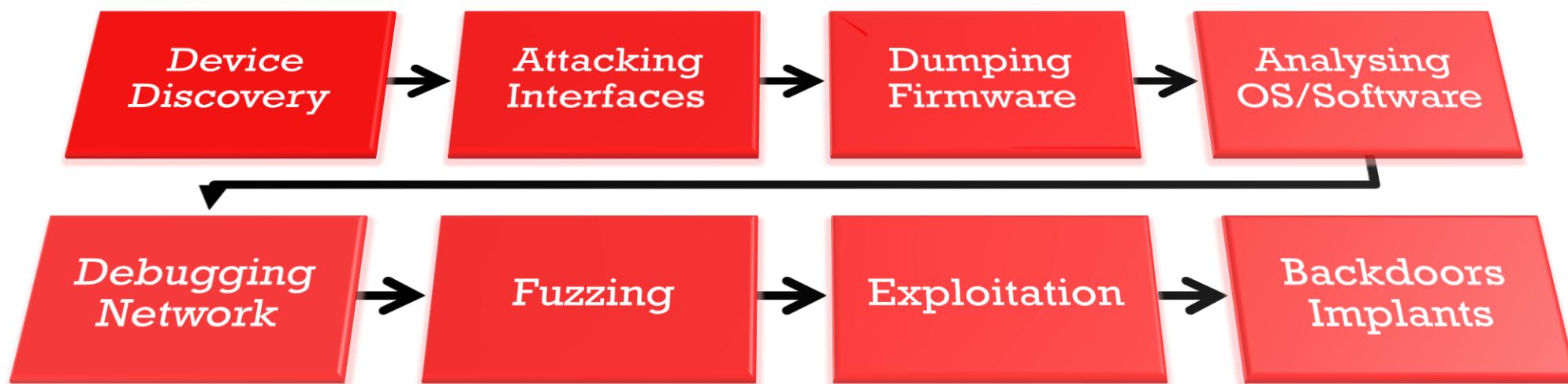
---



- Combining testing skills
  - Design reviews do not show business logic issues
  - Tech must be tested for various perspectives
- Traditional tests do not cover
  - Devices' firmware and hardware
  - Management in a protected network
- Very limited days for testing

# EMBEDDED SYSTEMS SECURITY TESTING

- Testing methodology must be flexible
  - Various devices - ARM vs MIPS, Phone vs Modem
  - Various OSes - Android vs Linux vs VxWorks
- Testing must always focus on the device's roles



# HARDWARE HACKING CHRONICLES

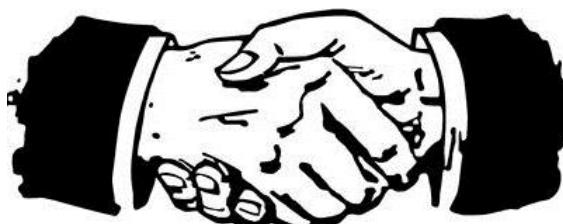


# EASIER WAYS OF COMPROMISING A DEVICE

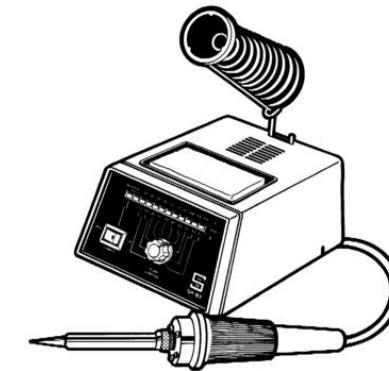
---



Configuration  
Edit & Re-Upload

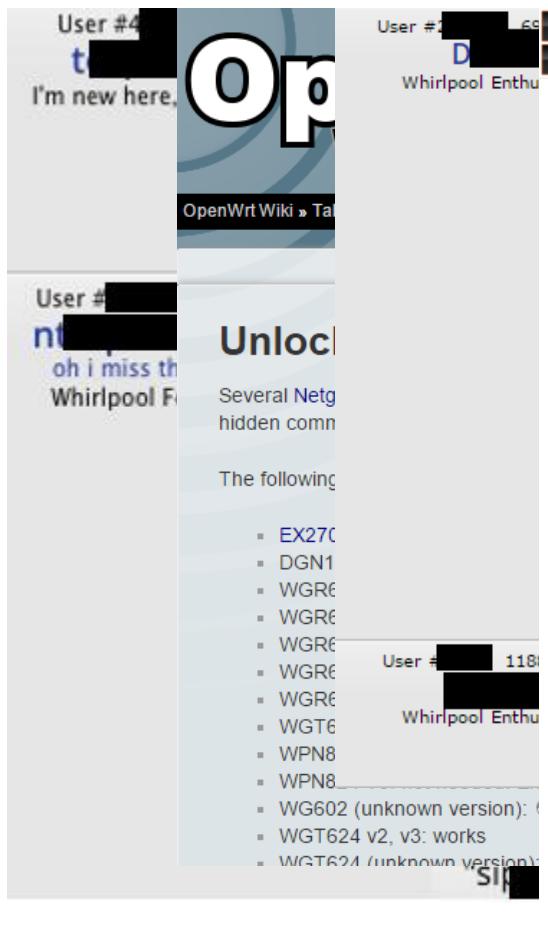


Secret Handshake  
to Enable Telnet



Physical  
Interfaces

# PUBLIC INFORMATION IS ALREADY AVAILABLE



```
#!/home/bin/python

# Remote Exploit: SAGEM F
# Date: 15-August-2011
# Author: Elouafiq Ali
# Version: 3304-V1 / 3304
# Tested on: Linux Ubuntu
# Tested Router: SAGEM FA
# Tested on Resellers/ISPs
# Products affected: Sage
# Blog: http://keelhaule...
```

\*\*\*

Sagem Fast Routers (3304) ...  
That the ISPs don't change  
the root password directly.  
Thus, each unique router has  
After reverse engineering the  
This exploit opens a telnet session  
(Generally its an Alcatel)

Usage: ./{file\_name}

\*\*\*

```
from telnetlib import Telnet
import time, sys, tty, termios
from threading import *
```

```
host = ''
port = 23
user = "root"
password = ""
class ReaderThread(Thread):
    def __init__(self):
        self.telnet = Telnet(host, port, 1)
        Thread.__init__(self)
```

```
    def run(self):
        self.telnet.read_until("User name: ")
```

## **Router Security**

[Home](#) | [Introduction](#) | [Router Bugs](#) | [Security Checklist](#) | [Tests](#) | [Resources](#) | [About](#)

If you care about the security of your router, and you should, it is best to avoid consumer grade routers. On the whole. Below is what I base this opinion on. This list is *far* from complete.

You may be thinking that all software is buggy but router software is probably worse. One reason for this is your ISP, router/gateway in an insecure way, either on purpose to allow spying or out of laziness or incompetence. Another reason is that routers are often designed to be as cheaply as possible. Security is not the prime directive. You can tell this just by looking at the box a router ships in. Many routers are shipped in boxes that are barely larger than the router itself.

Many others have also pointed out the sad state of consumer router software/firmware.

Be sure to read about the port 32764 issue from January 2014 and April 2014. The way the backdoor was hidden, after keeping back doors in routers on purpose, and hiding them *really* well. Another flaw not to be missed is the Misfortune flaws do not yet get their full due here. WPS, for one. WPS is like having a "hack me" sign on your back and yet its implemented by the Wi-Fi Alliance. Another *huge* flaw was the one with UPnP.

2016

FEBRUARY 2010

## A ton of new router flaws discovered

New firmware analysis framework finds serious flaws in Netgear and D-Link devices

by Lucian Constantin of IDG News Service Feb 29, 2016

Been there done that. Once again, a group of researchers looked at many router firmwares and found a ton of bug framework called FIRMADYNE built by Daming Chen, Maverick Woo and David Brumley from Carnegie Mellon University. They found 887 firmware images that were vulnerable to at least one of 74 known exploits. They also fi

# PUBLIC INFORMATION IS ALREADY AVAILABLE



- Weaknesses are already known
  - Configuration dump for credentials
  - Editing the conf to enable a feature
- Vulnerabilities are public and easy
  - Telnet authentication bypass  
Sagem: <https://www.exploit-db.com/exploits/17670>
  - Netgear:  
<https://wiki.openwrt.org/toh/netgear/telnet.console>
  - E.g. admin password leak  
`wget http://1.1.1.1/password.html -t 1 -q -O - | grep pwd`

# PHYSICAL INTERFACES

---

## UART

Console Debugging  
TX, RX, GND, V

## JTAG

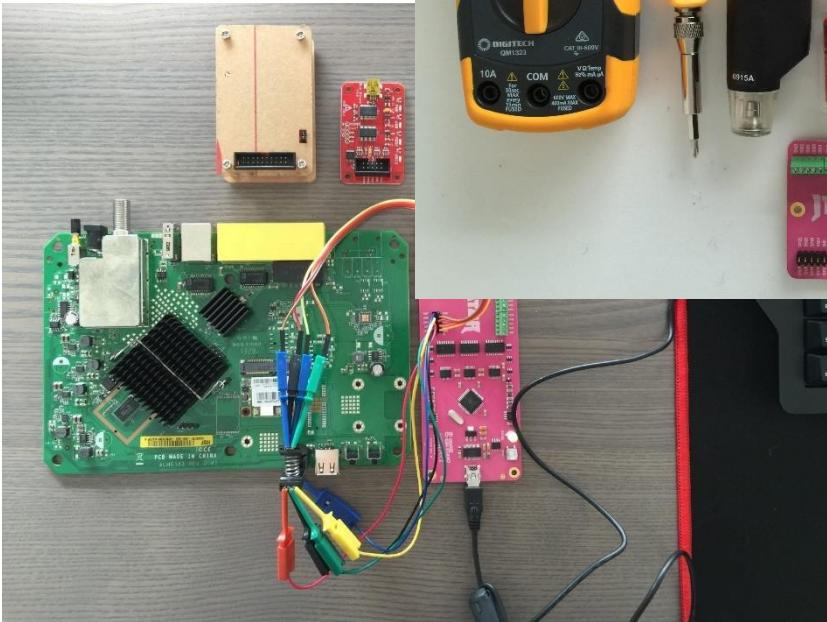
Debugging On-Chip  
Debug TDI, TDO,  
TCK...

## SPI

Access to Flash  
Read/Write Data  
SCK, MOSI, MISO...

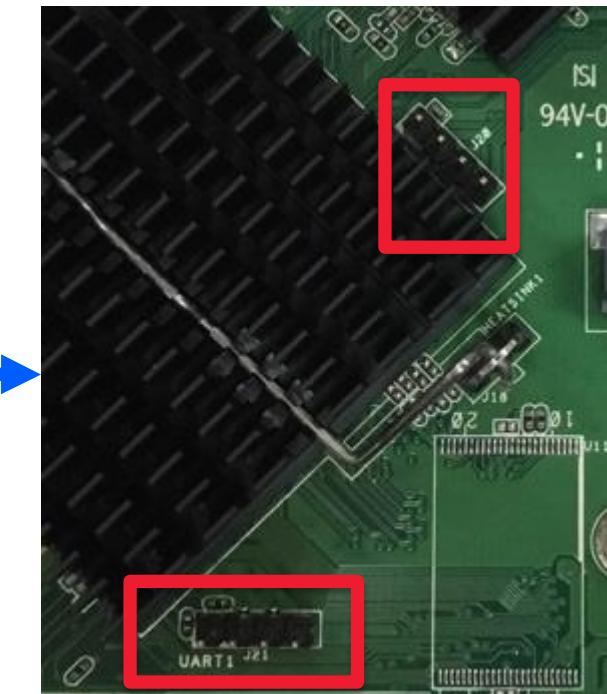
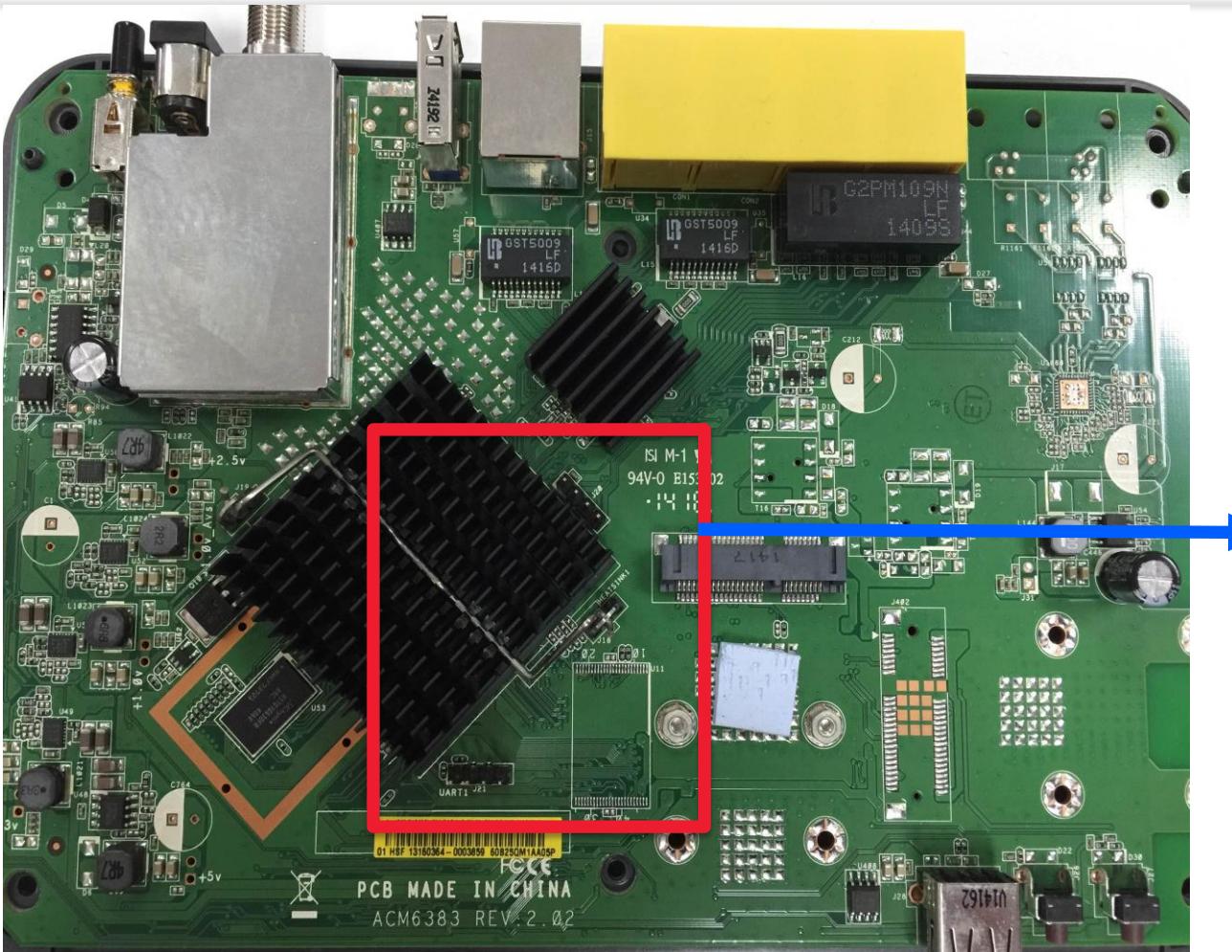
# HARDWARE ANALYSIS EQUIPMENT

---

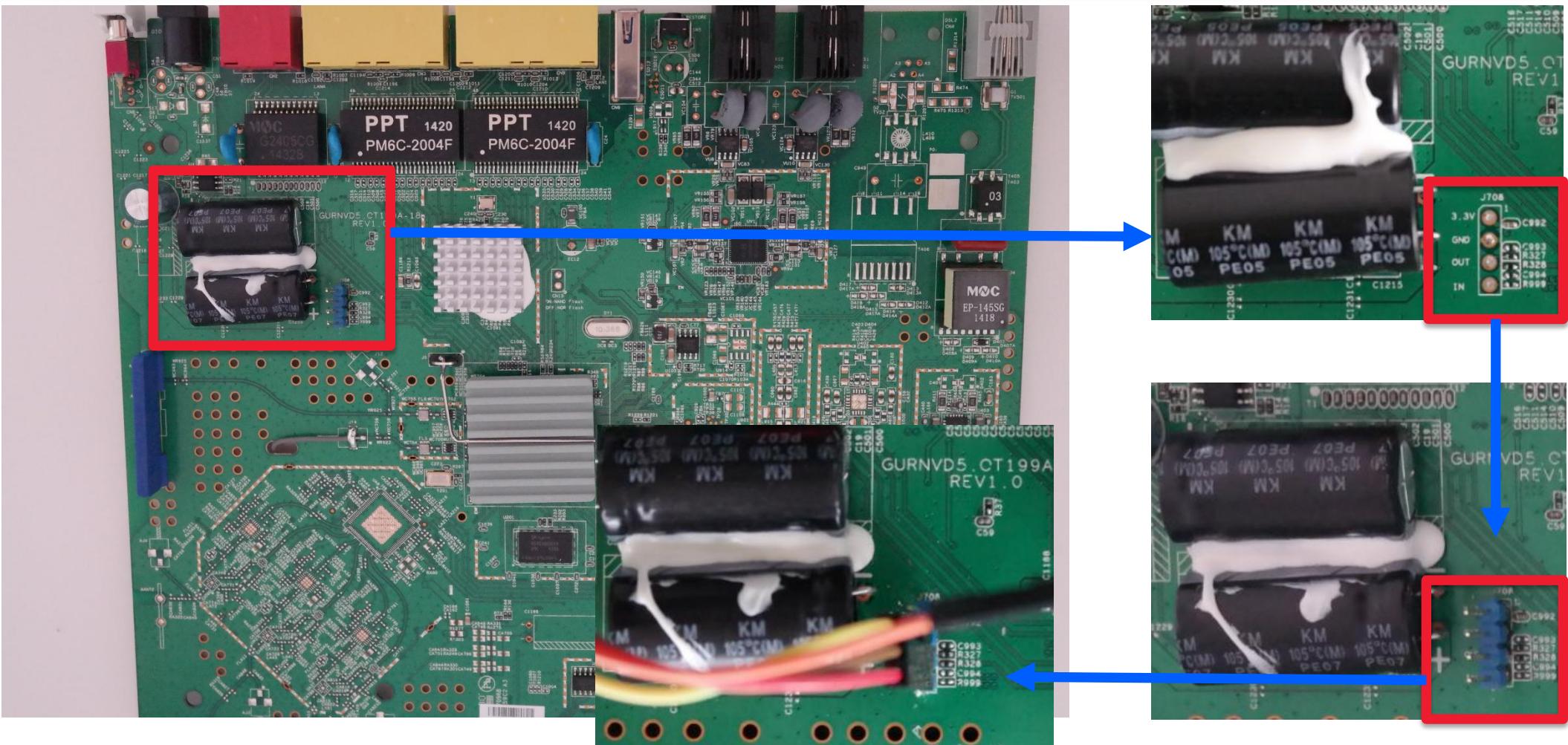


- Bus Pirate
- Bus Blaster
- Shikra
- HydraBus
- Jtagulator
- GoodFet/GreatFet
- Logic Analyser
- SOIC8/16 Clips

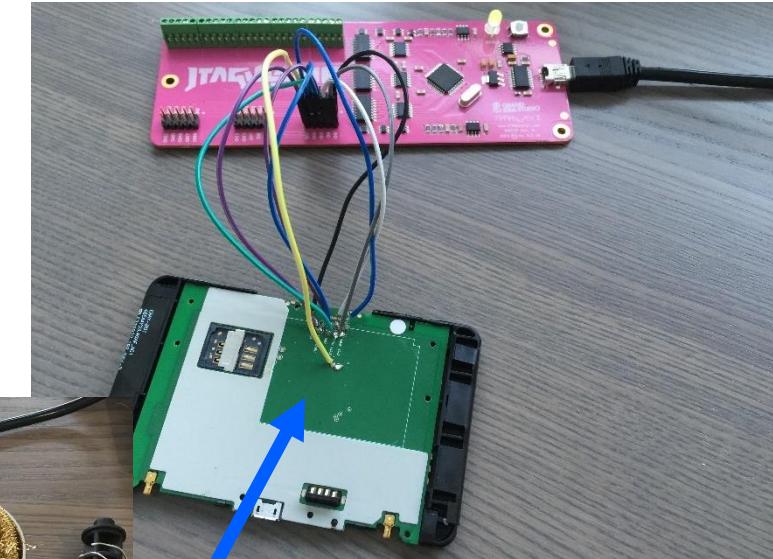
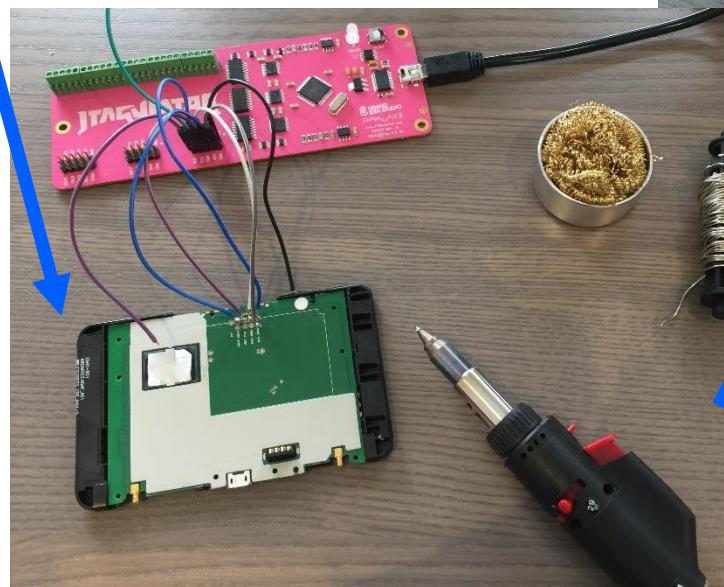
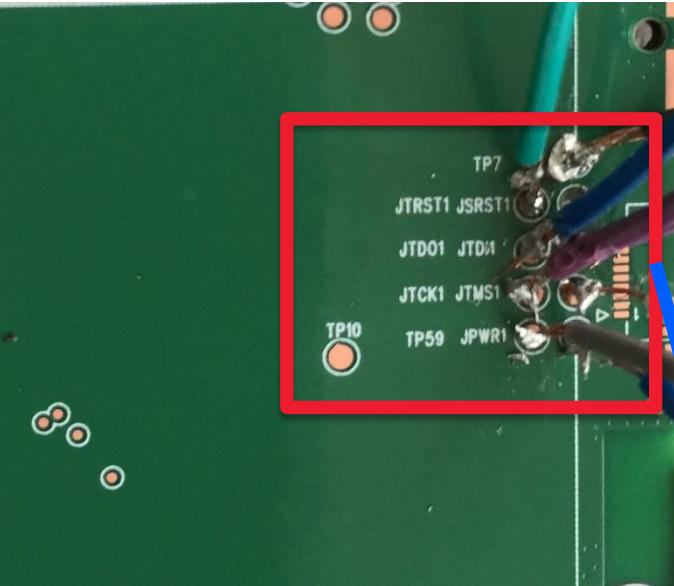
# PHYSICAL INTERFACES



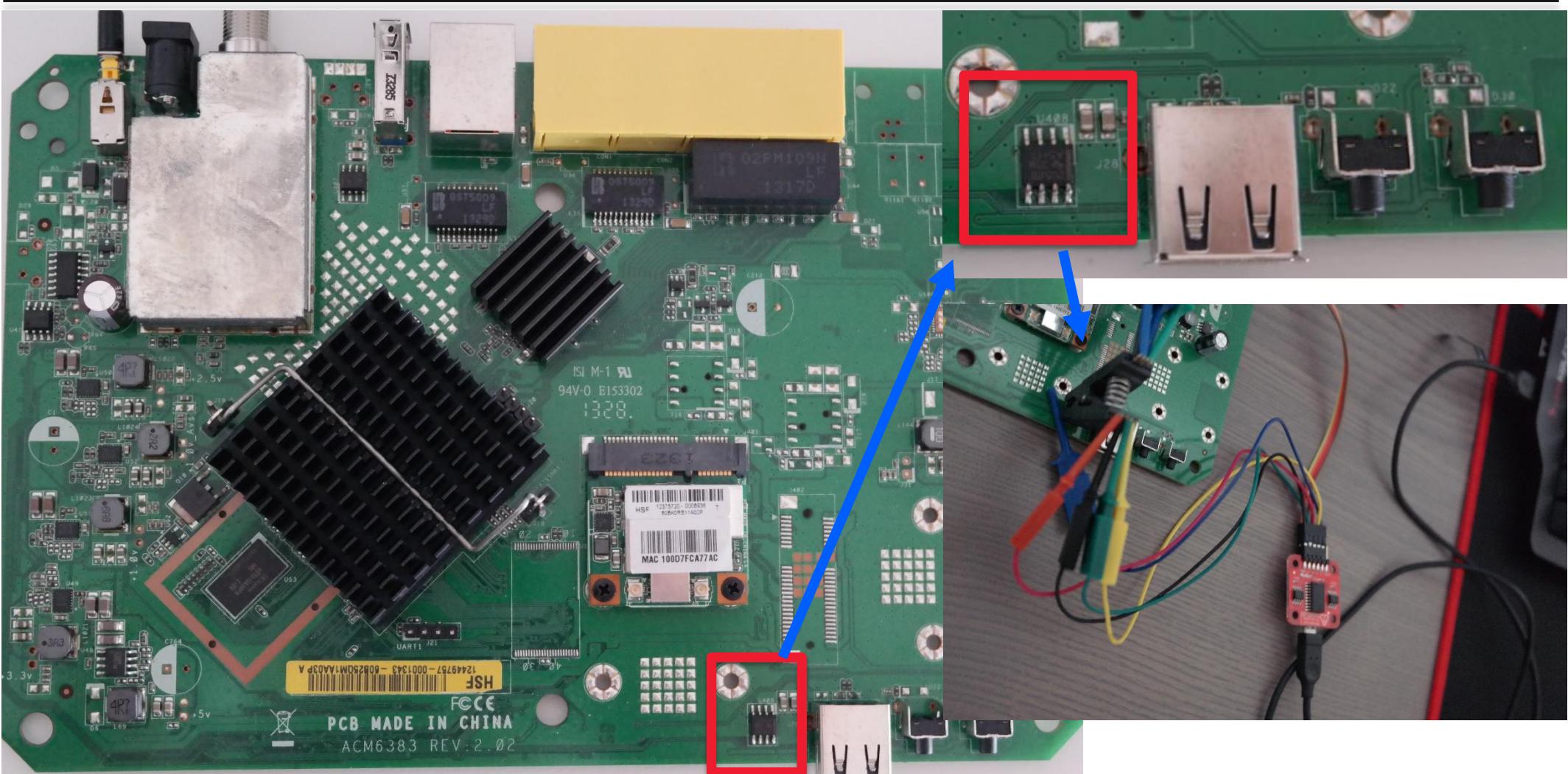
# PHYSICAL INTERFACES



# PHYSICAL INTERFACES

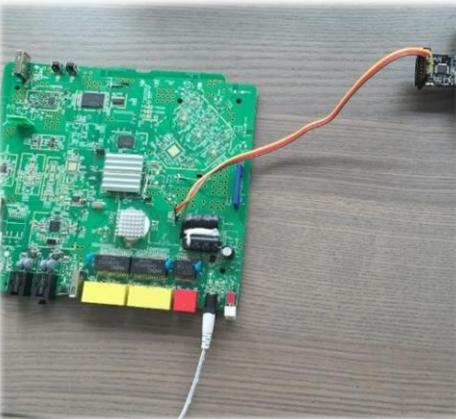


# PHYSICAL INTERFACES



# UART/SERIAL CONNECTION

---



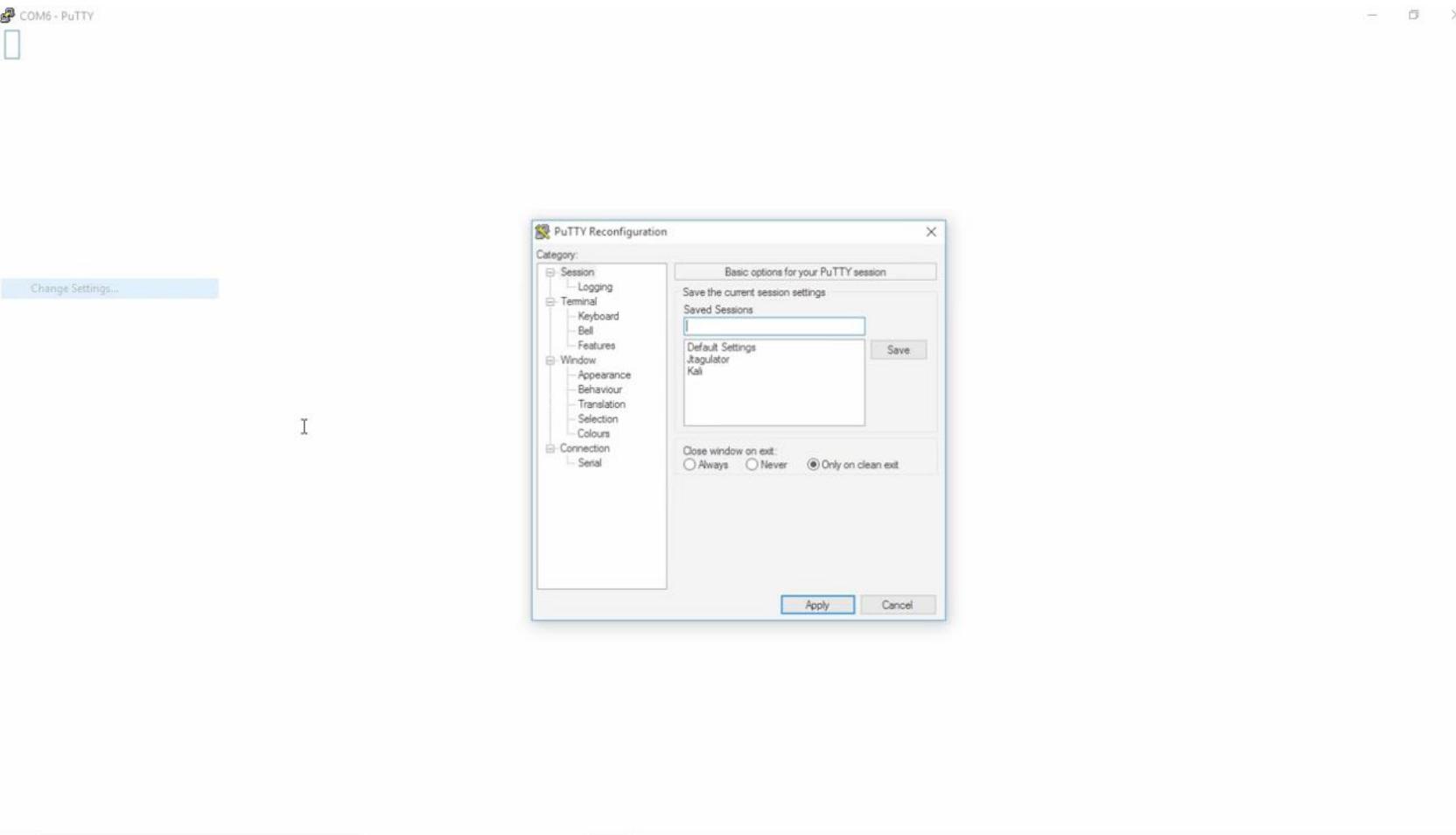
- Usually 4 PINs
  - TX, RX, GND, Voltage
- Provides device access
  - Bootloader, console access
- Real-time debugging
- Access without a password

# DEMO: IDENTIFYING UART PINS/PINPADS

- Find the ground
- Find the voltage
- Set the target voltage
- Try to send/receive
  - TX vs RX
  - Various baud rates
  - Analyse the output
- Jtagulator



# DEMO: UART INTERFACE DISCOVERY

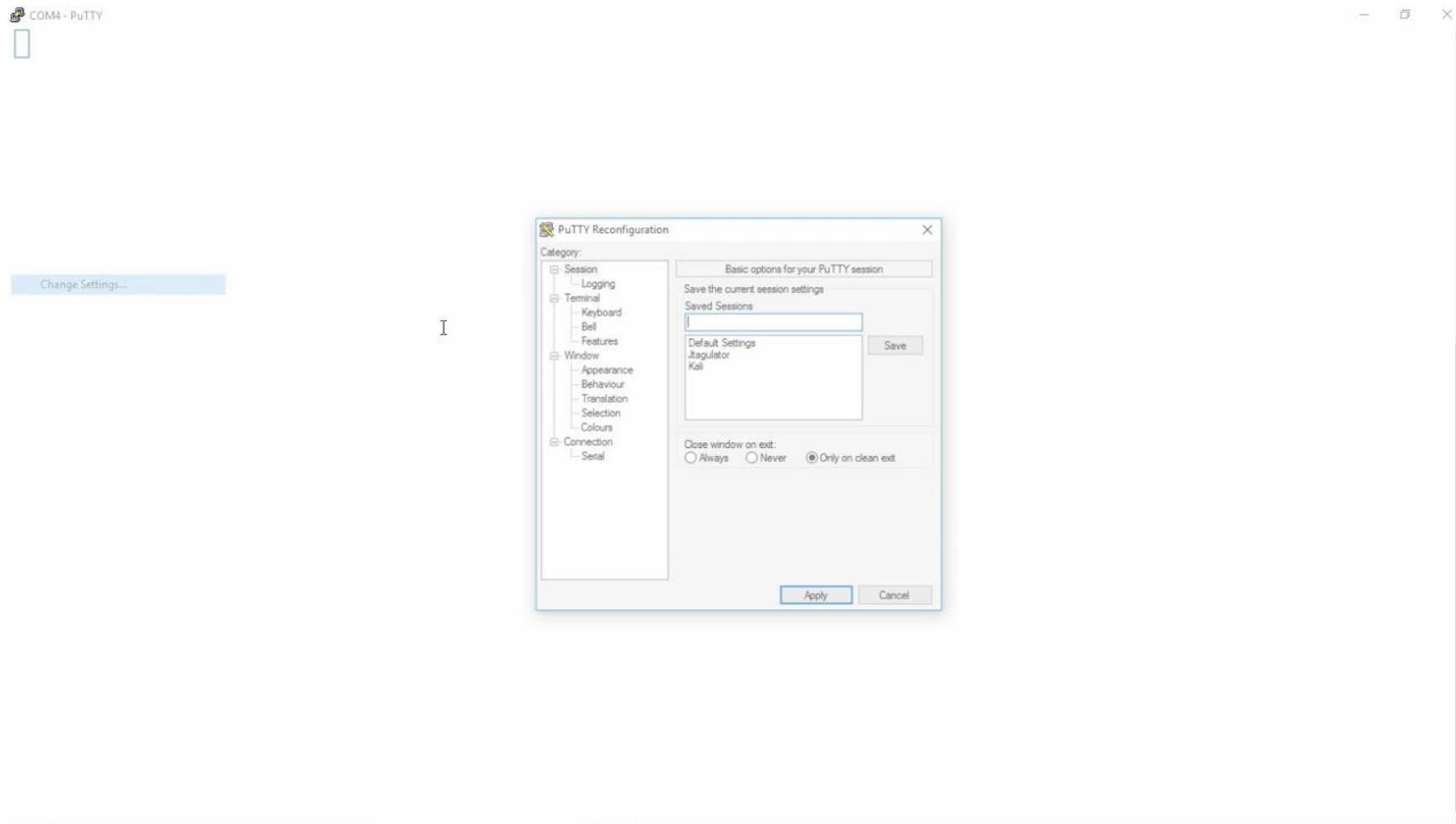


# BENEFITS OF UART ACCESS

---

- Debugging and logging
- Intercepting boot sequence
  - Boot parameters
  - CFE access
- Getting console access
- E.g. Netgear CG3100D

# DEMO: UART/SERIAL DEBUGGING



# CFE – COMMON FIRMWARE ENVIRONMENT

```
CFE version 7.253.2 for BCM963268 (32bit,SP,BE)
Build Date: Fri Apr  4 14:49:33 CST 2014 (cookiechen@sz01017.ads.local)
Copyright (C) 2005-2012 SAGEMCOM Corporation.
```

```
NAND flash device: name <not identified>, id 0x92f1 block 128KB size 131072KB
External switch id = 53125
Chip ID: BCM63168D0, MIPS: 400MHz, DDR: 400MHz, Bus: 200MHz
Main Thread: TP0
Memory Test Passed
Total Memory: 134217728 bytes (128MB)
Boot Address: 0xb8000000
```

```
Board IP address          : 192.168.1.1:fffffff00
Host IP address           : 192.168.1.100
Gateway IP address        :
Run from flash/host (f/h) : f
Default host run file name: vmlinux
Default host flash file name: bcm963xx_fs_kernel
Boot delay (0-9 seconds)  : 1
Board Id (0-15)            : F@ST3864V2
Number of MAC Addresses (1-32): 11
Base MAC Address          : d0:84:b0:3e:db:c9
PSI Size (1-64) KBytes     : 40
Enable Backup PSI [0|1]    : 0
System Log Size (0-256) KBytes: 0
Main Thread Number [0|1]    : 0
Voice Board Configuration (0-0): SI32261
```

```
*** Press any key to stop auto run (1 seconds) ***
Auto run second count down: 1
CFE>
web info: Waiting for connection on socket 0..[J]
```

- Stop the boot process
  - UART/Serial connection
- Possibilities
  - Re-flash for OpenWRT
  - Get information
    - Credentials?
  - Dump the firmware
- Eg. Sagemcom 3864v2  
ADSL & NBN

# DEMO: COMMON FIRMWARE ENVIRONMENT

The screenshot shows a terminal window titled "GtkTerm - /dev/ttyUSB0 115200-8-N-1". The window contains a list of memory regions and their addresses, likely from a memory dump or configuration file. The regions are listed in pairs, separated by a colon. The first column lists the region names, and the second column lists their addresses. The regions include: HEL0:CPUI, L1CI:HELO, CPUI:L1CI, DRAM:PHYS, PHYS:STRF, STRF:400H, 400H:PHYE, PHYE:DDR3, DDR3:SIZ4, SIZ4:SIZ3, SIZ3:SIZ2, SIZ2:DINT, DINT:USYN, USYN:LSYN, LSYN:MFAS, MFAS:LMBE, LMBE:RACE, RACE:PASS, PASS:ZBSS, ZBSS:CODE, CODE:DATA, DATA:L12F, L12F:MAIN, MAIN:FP. The terminal window has a standard Linux-style interface with a menu bar (File, Edit, Log, Configuration, Control signals, View) and a toolbar with buttons for Help, DTR, RTS, CTS, CD, DSR, and RI.

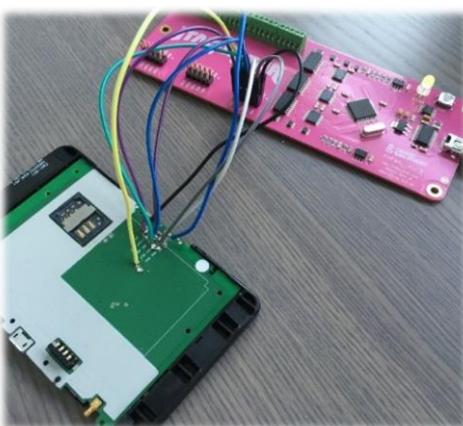
```
File Edit Log Configuration Control signals View
GtkTerm - /dev/ttyUSB0 115200-8-N-1
Help
DTR RTS CTS CD DSR RI

HEL0:CPUI
L1CI:HELO
CPUI:L1CI
DRAM:PHYS
PHYS:STRF
STRF:400H
400H:PHYE
PHYE:DDR3
DDR3:SIZ4
SIZ4:SIZ3
SIZ3:SIZ2
SIZ2:DINT
DINT:USYN
USYN:LSYN
LSYN:MFAS
MFAS:LMBE
LMBE:RACE
RACE:PASS
PASS:ZBSS
ZBSS:CODE
CODE:DATA
DATA:L12F
L12F:MAIN
MAIN:FP

/dev/ttyUSB0 115200-8-N-1
```

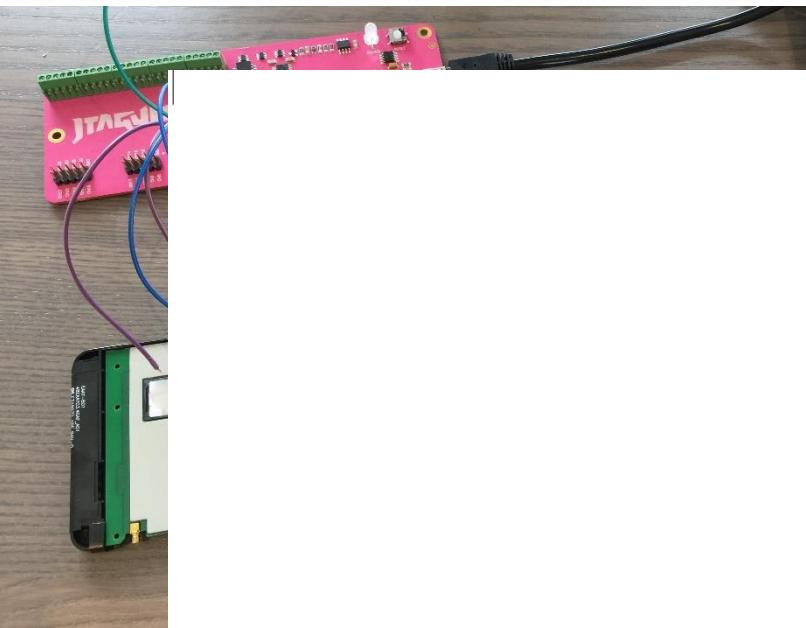
# JTAG - JOINT TEST ACTION GROUP

---

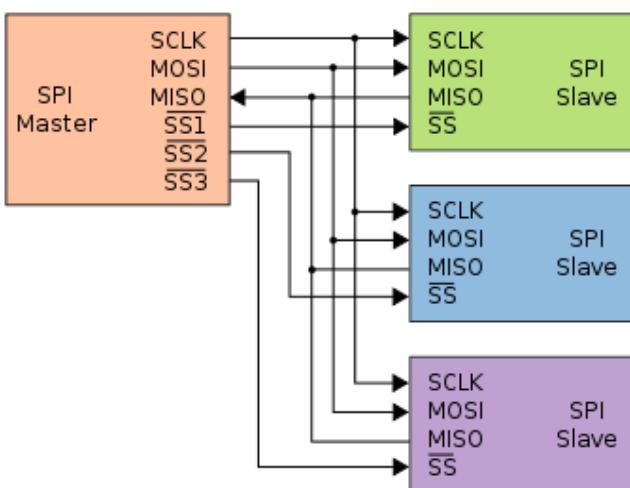
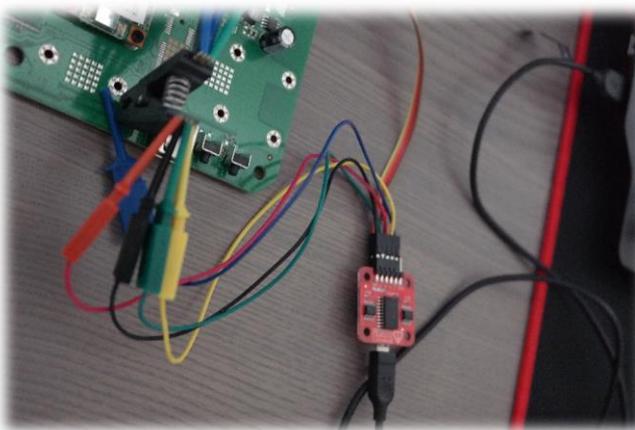


- Debugging standard
- Everything depends on the vendor
- Device or system testing
- Daisy-chained JTAG
  - TDI (Test Data In)
  - TDO (Test Data Out)
  - TCK (Test Clock)
  - TMS (Test Mode Select)
  - TRST (Test Reset)

# DEMO: IDENTIFYING JTAG PINPADS



# SPI – SERIAL PERIPHERAL INTERFACE BUS



- Internal communication interface
- Direct connection to the flashes
- Logic signals
  - **SCLK** : Serial Clock
  - **MOSI** : Master Output, Slave Input
  - **MISO** : Master Input, Slave Output
  - **SS** : Slave Select

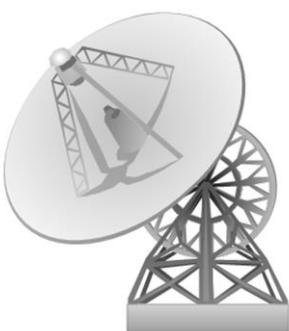
Image: [https://en.wikipedia.org/wiki/Serial\\_Peripheral\\_Interface\\_Bus](https://en.wikipedia.org/wiki/Serial_Peripheral_Interface_Bus)

# CUSTOMER PREMISES EQUIPMENT



# CONSUMER AND SUBSCRIBER SERVICES

---



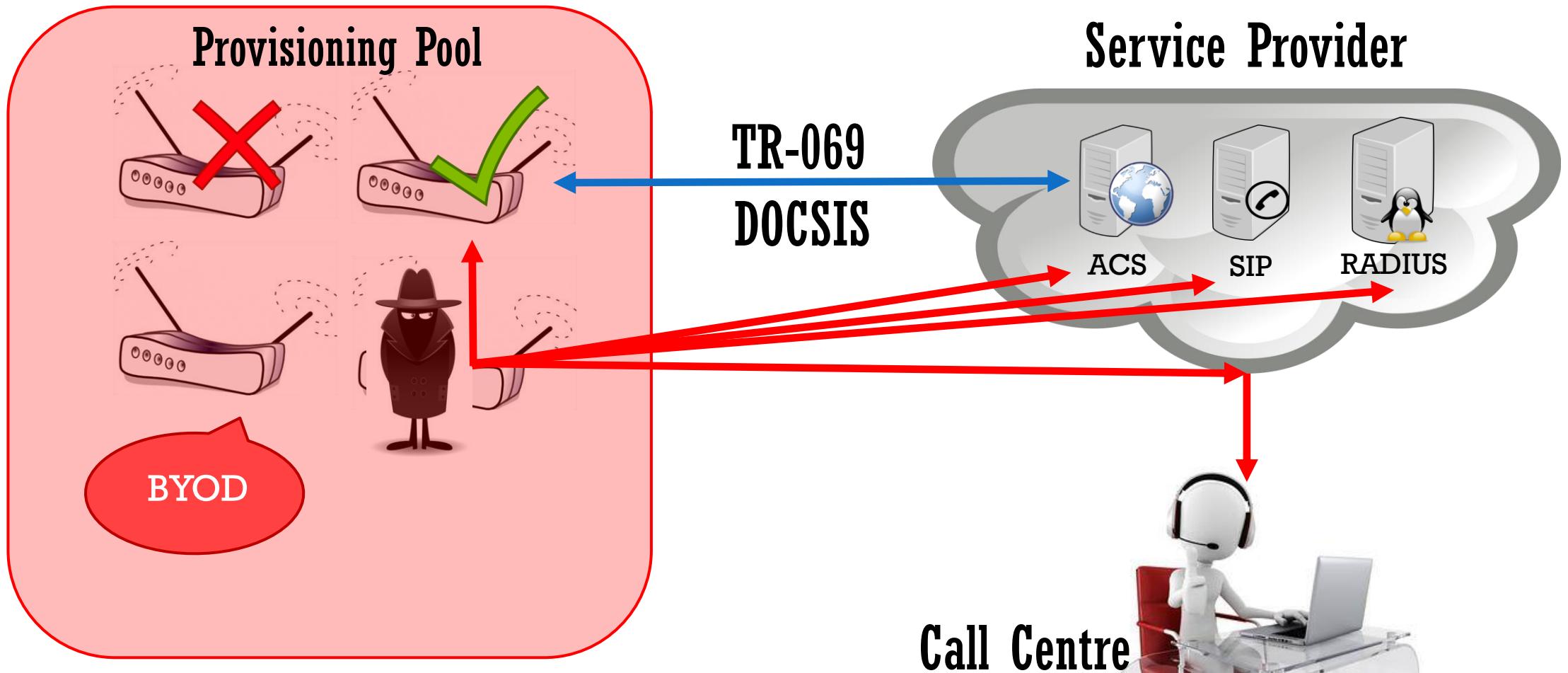
- Broadband, IPTV, Satellite...
- Devices are
  - connected to the infrastructure
  - managing by service provider
  - in the consumer premises
- Relying on vendors for security
  - Default configuration
  - Legacy or unpatched software
  - Management interfaces

# CONSUMER AND SUBSCRIBER SERVICES

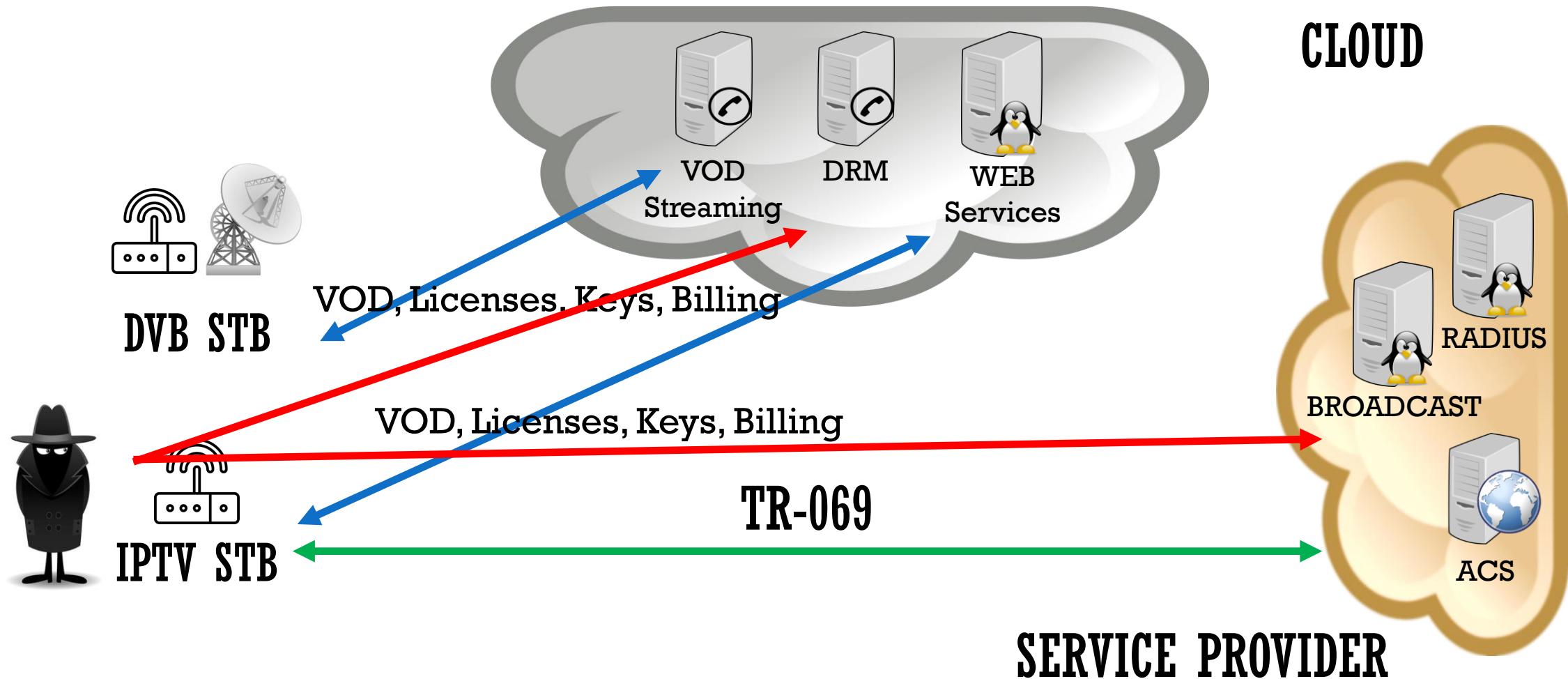


- Various vendors in a pool
  - Device provisioning
  - Software & configuration management
  - Call centre connections
- Generic information in the wild
  - Custom software (e.g OpenWRT)
  - Bypassing controls is common
- BYOD on subscriber services

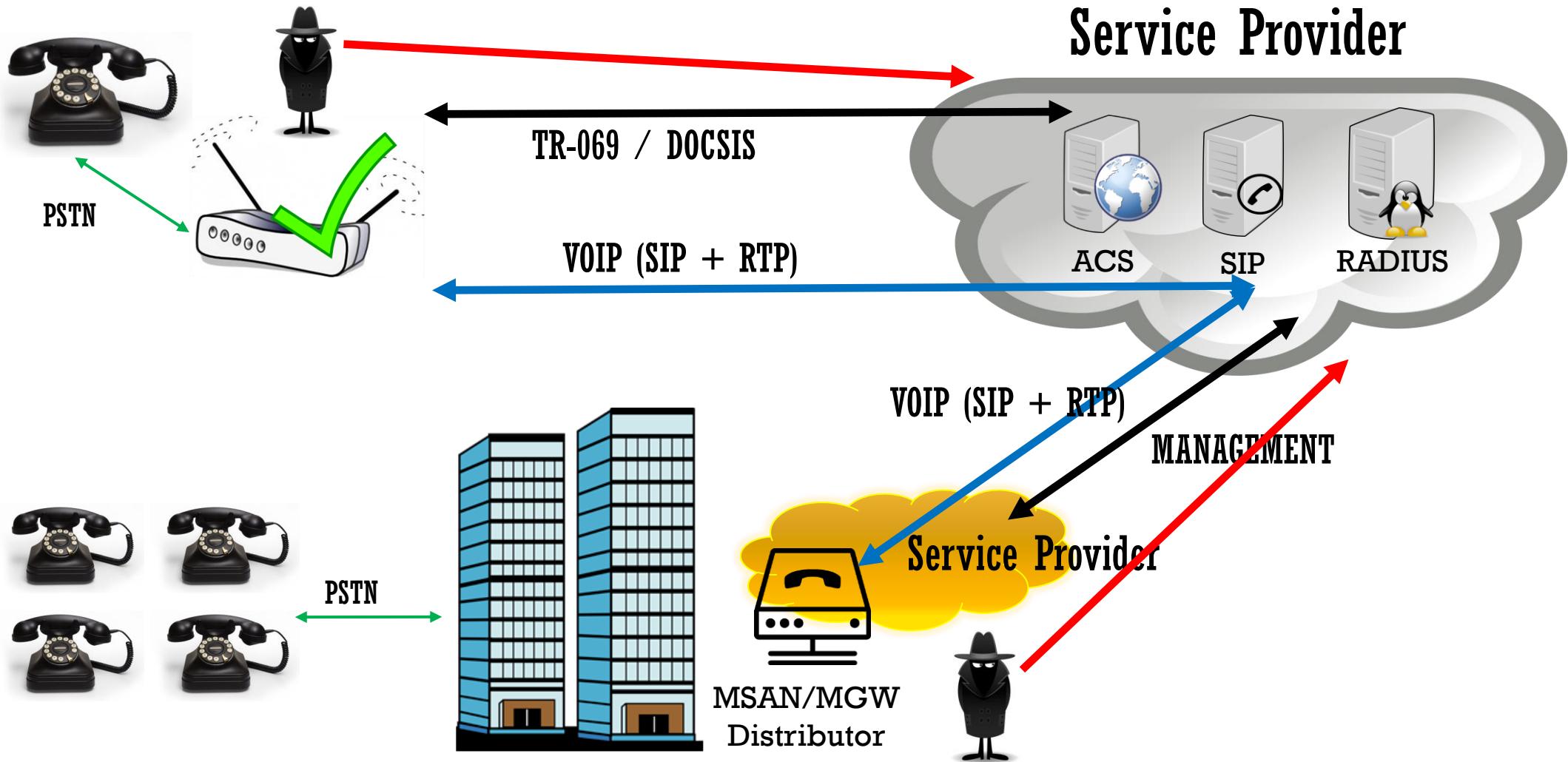
# BROADBAND DEVICES



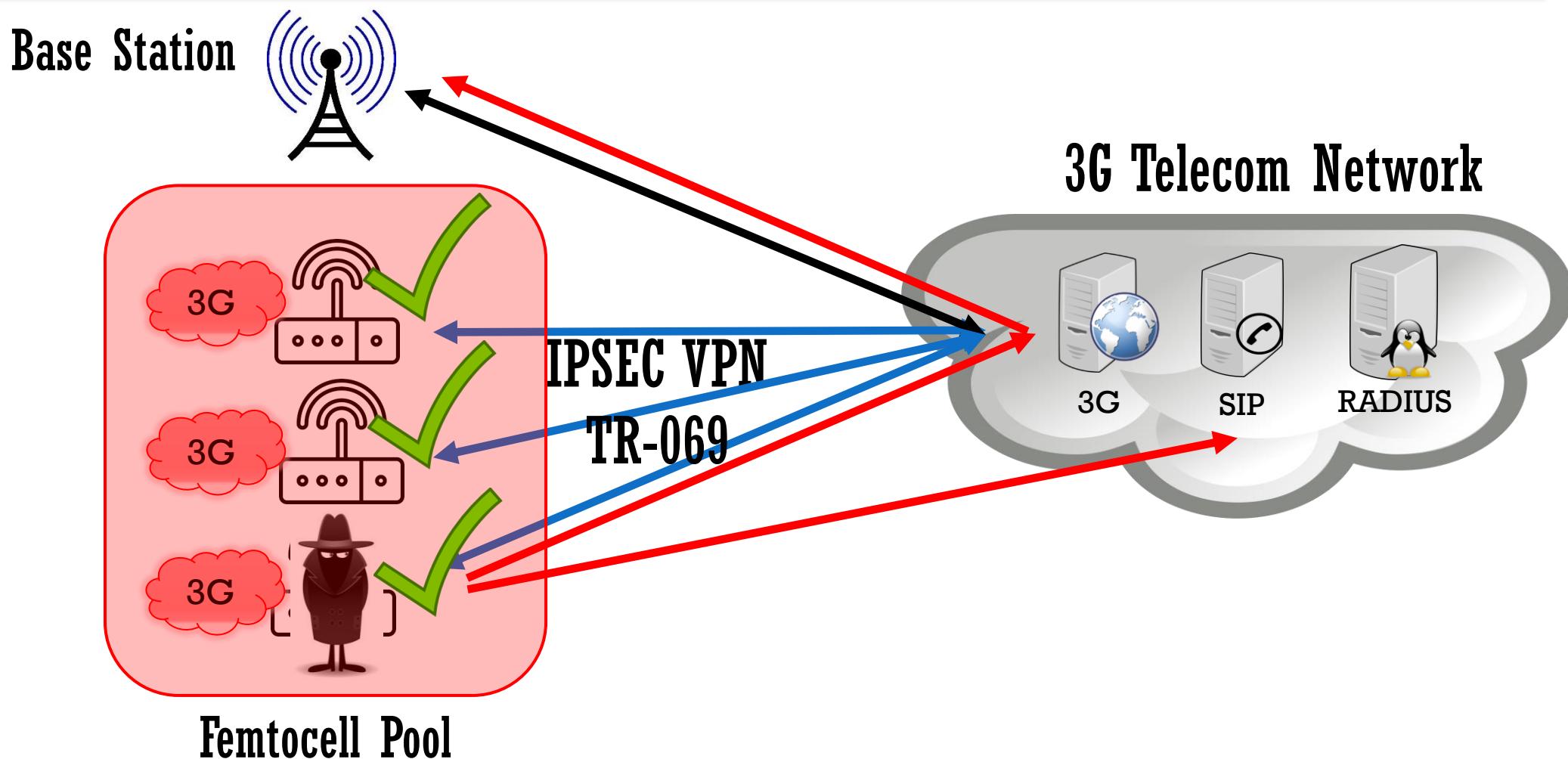
# DVB & IPTV DEVICES



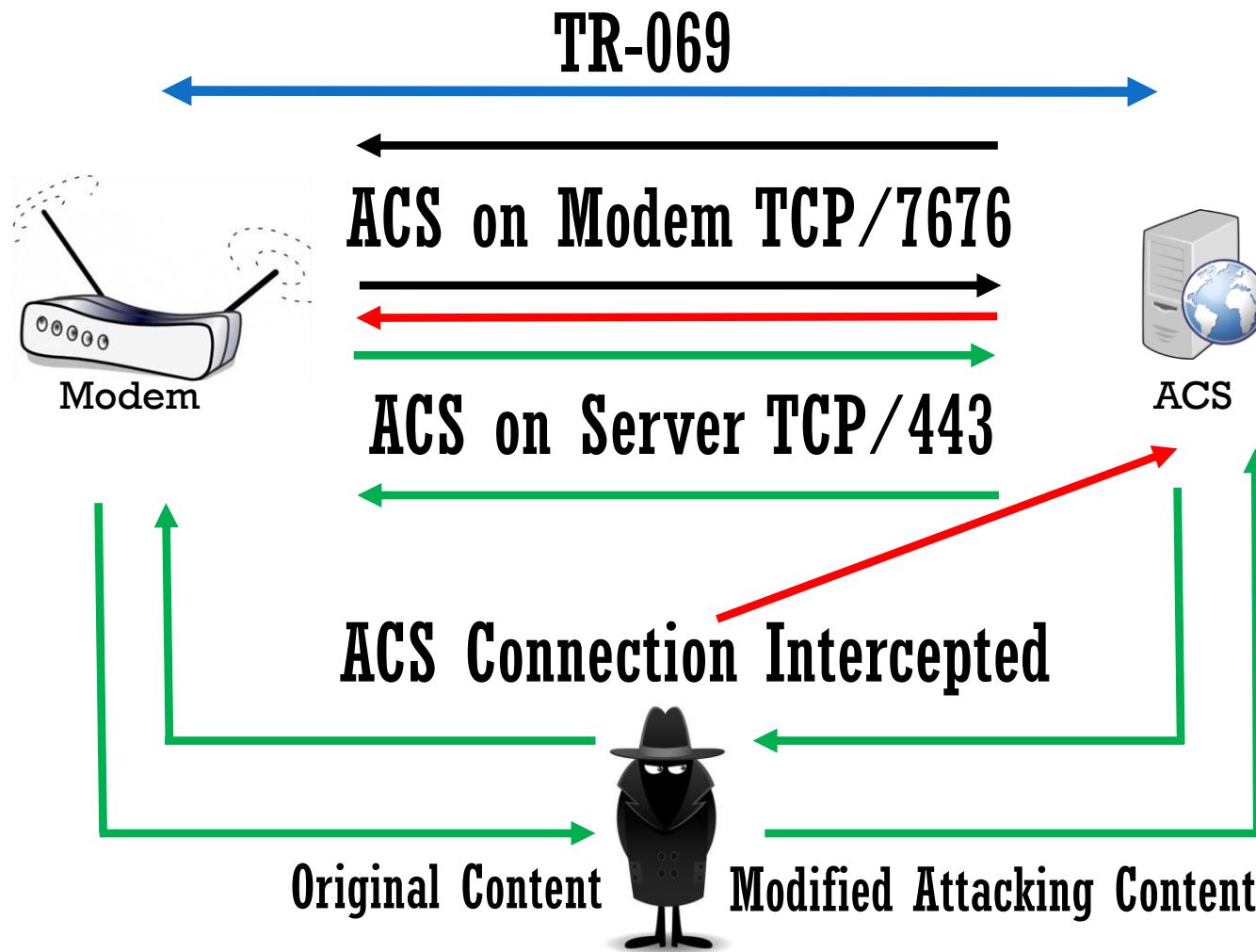
# UNIFIED COMMUNICATIONS DEVICES



# FEMTOCELL DEVICES



# ATTACKING TR-069 NETWORKS



- Debugging
- Gathering Information
- Attacking
  - Server
  - Service network
  - Clients connected

# CPE TO SERVICE PROVIDER NETWORKS



- Dumping device memory
  - X.509 certificates for IPSEC Auth
  - PINs, passwords and config data
  - Broadcasting and DRM keys
- Dump device firmware
  - Reverse engineering, exploit dev
- Driving a consumer device
  - Fake base station, billing bypass
  - Altering VoD content, security bypass

# OFFICE DEVICES



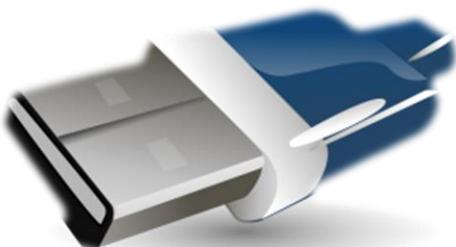
# HARDWARE IMPLANTS, BACKDOORS, SNIFFERS



- Backdoors on devices are common
    - Open source, distribution, vendors...
  - Expensive to replicate the attack
  - Red teaming engagements
    - Putting a Raspberry Pi in everything
    - Collecting keyboard & mouse input
  - Human factor pen-testing
    - Sending backdoored devices

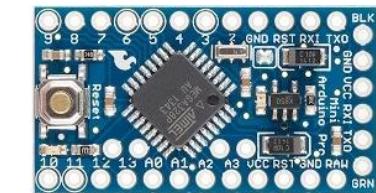
# BACKDOORING A DEVICE FOR TESTING

---



- 3G/4G Modems
  - WiFi models with services and features
  - USB models require drivers
  - Internal storage and card reader
- Unauthorised access via services
- Firmware operations
  - Dumping and reversing the firmware
  - Backdooring the firmware
- Using their shelves for USB duckies

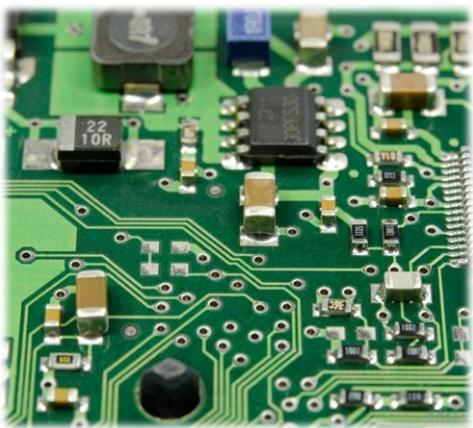
# WIRELESS KEYBOARD ATTACKS



- Keysweeper by SamyKamkar
  - Arduino/Teensy based sniffer
  - Sniffing Microsoft Wireless Keyboard
  
- Mousejack by Bastille Security
  - RF keyboard & mouse receivers
  - Force pairing vulnerability
  - Force pairing a remote keyboard

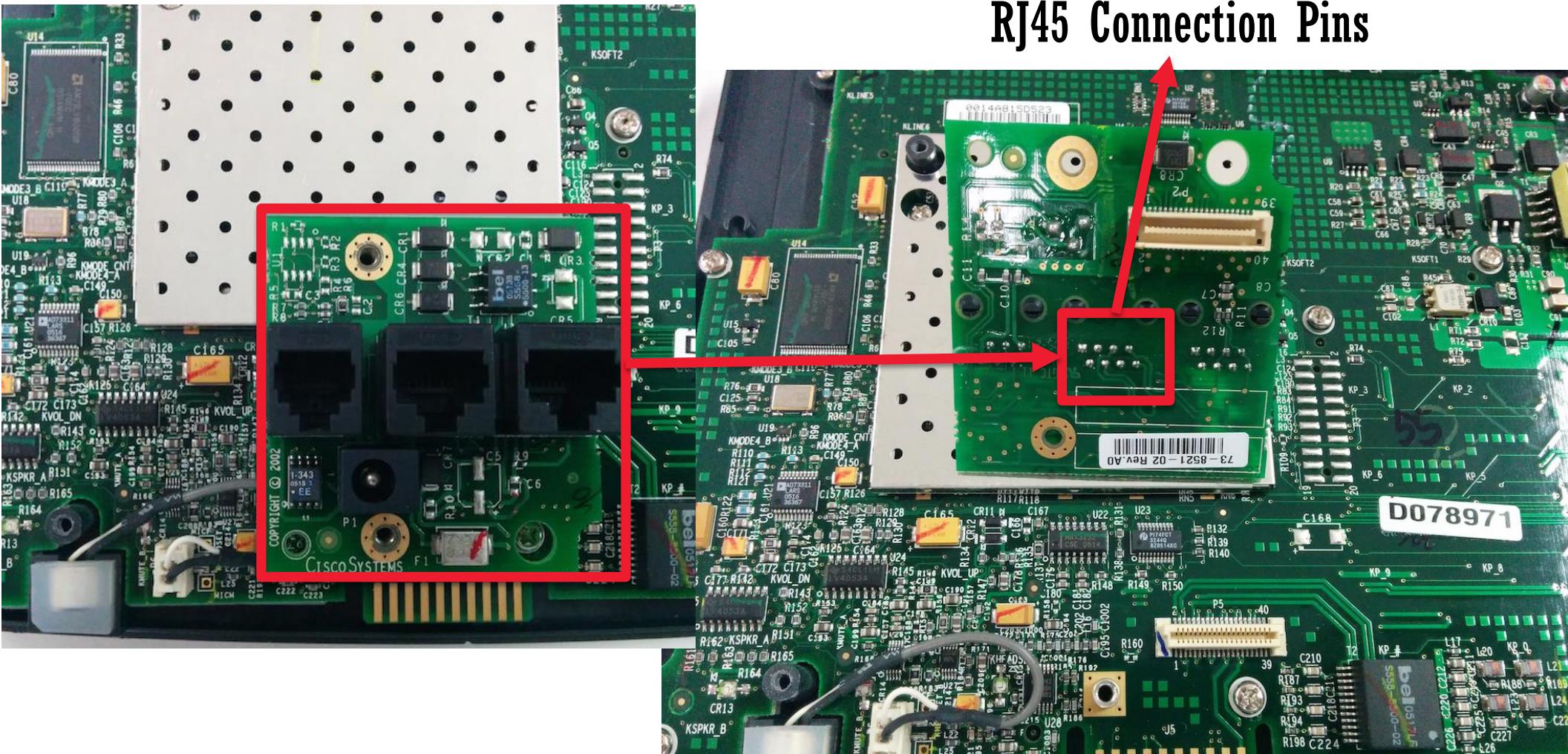
# MAKING AN IMPLANT FOR TESTING

---



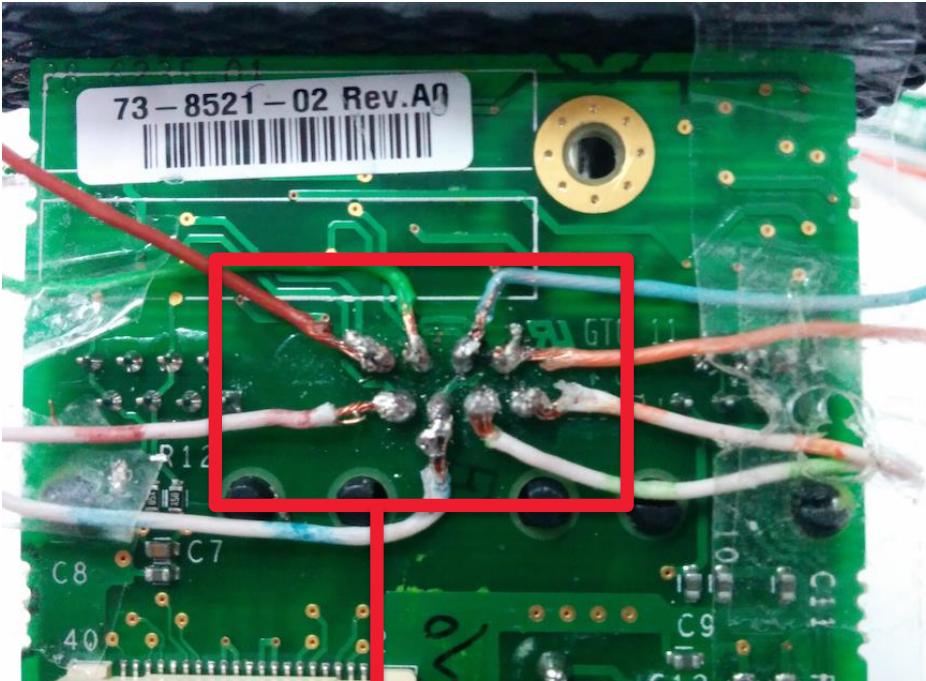
- Efficient for persistent access
  - Raspberry Pi, Arduino
  - Can fit in many devices
- Find a suitable device to backdoor
  - Find a power source
  - Find a network connection
  - Solder and connect the pieces
  - Broadcast the network connected
- Advanced implants take time

# MAKING AN IMPLANT FOR A CISCO IP PHONE

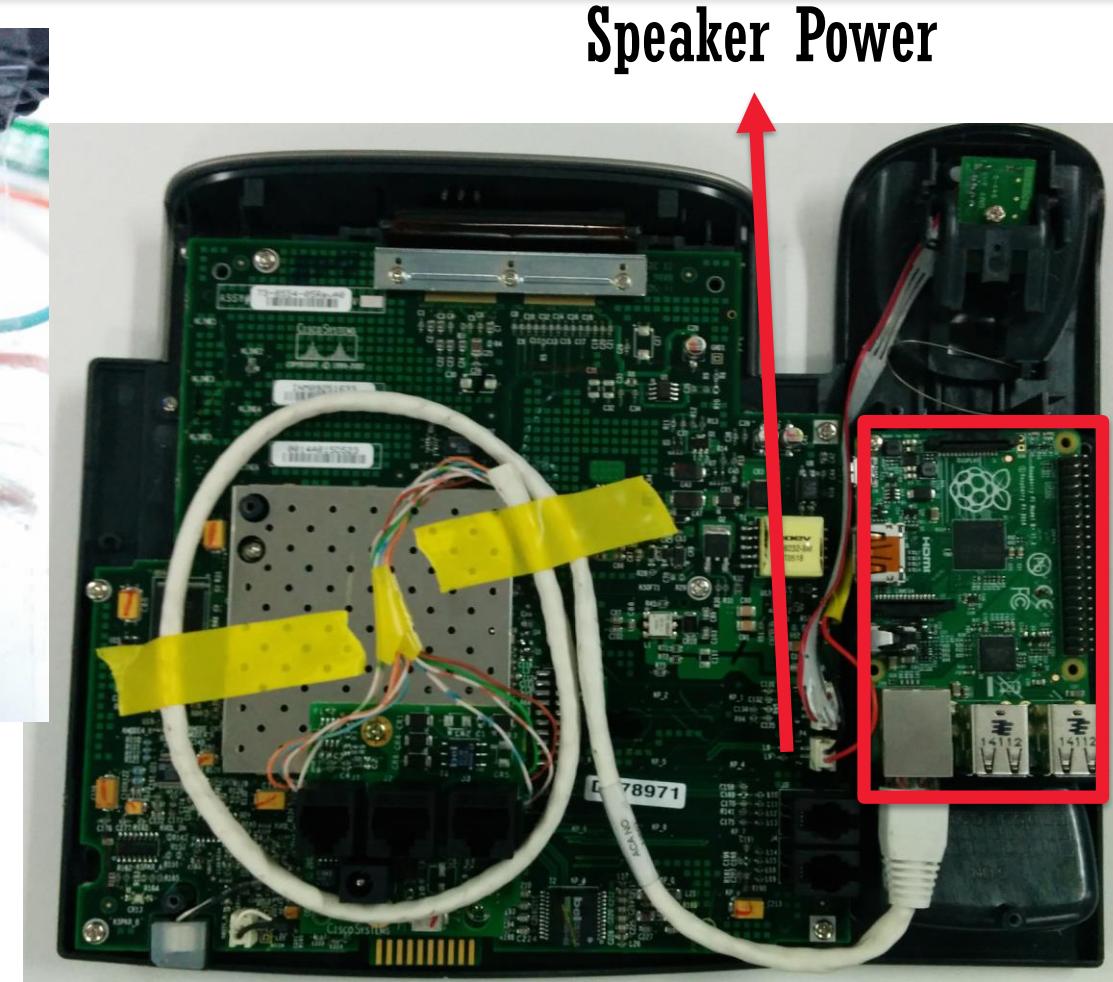


RJ45 Connection Pins

# MAKING AN IMPLANT FOR A CISCO IP PHONE



Patch the Cat5 cable



Speaker Power

# DEFENSE AND OFFENSE



# DEFENDING SUBSCRIBER SERVICES

---



- Enforcing vendors to
  - Disable physical interfaces
  - Use encryption and access keys
  - Follow a security standard
- Network isolation for subscribers
- Tailored research for
  - Vendor product vulnerabilities
  - CPE management services
  - Backdoor analysis

# IMPROVING TESTING SERVICES

---



- Devices are IN SCOPE
- Think different and combine skills
- Everything is a target
  - Home automation, CCTV, phones...
- Testing service operator networks
  - Test services through devices
  - Extract information from devices
  - Access and fuzz tests through devices

# TAILORED RESEARCH

---



- Focuses on all components
  - Devices, infrastructure, software...
- Focuses on exploitable issues
- Combines various disciplines
  - Embedded systems, mobile, network...
- Closes the gap between offense and defense

# REFERENCES

---

- Context Information Security

<http://www.contextis.com>

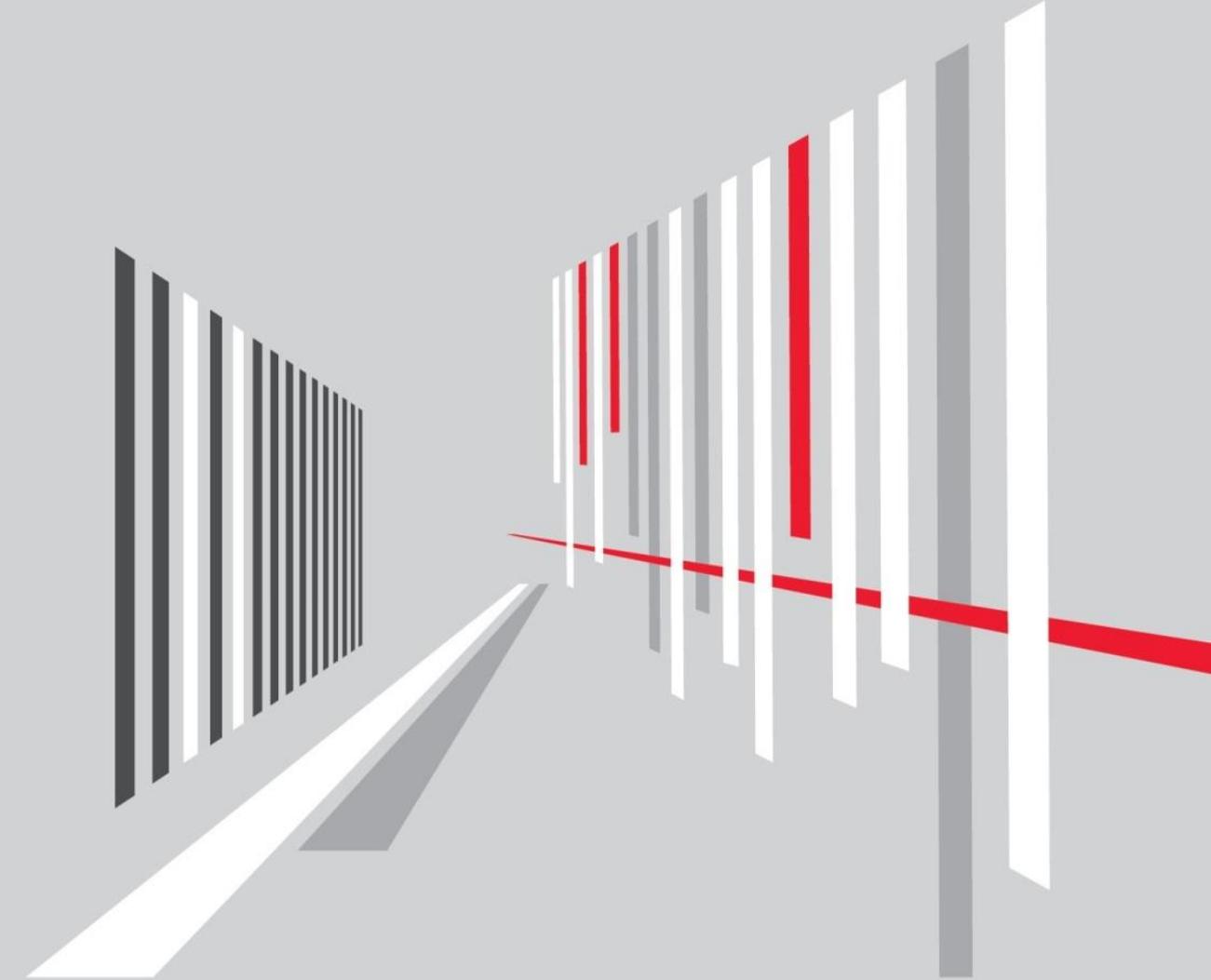
- AusCERT

<https://www.auscert.org.au>

- IoT Security Wiki

<https://iotsecuritywiki.com>

# QUESTIONS?



# THANKS!

