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 Viproy 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?

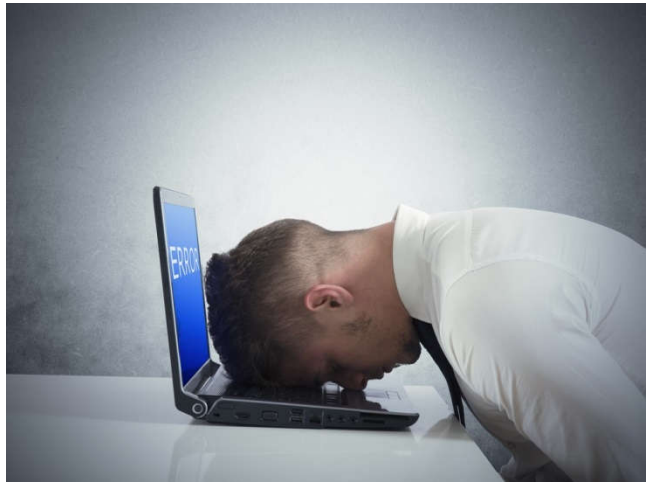
context

WHY SHOULD SERVICE PROVIDERS CARE?

CONSUMER SERVICES AND PRODUCTS

- Broadband & 3G/4G
- IPTV/Satellite Broadcasting & VoD
- Home & Office Equipment

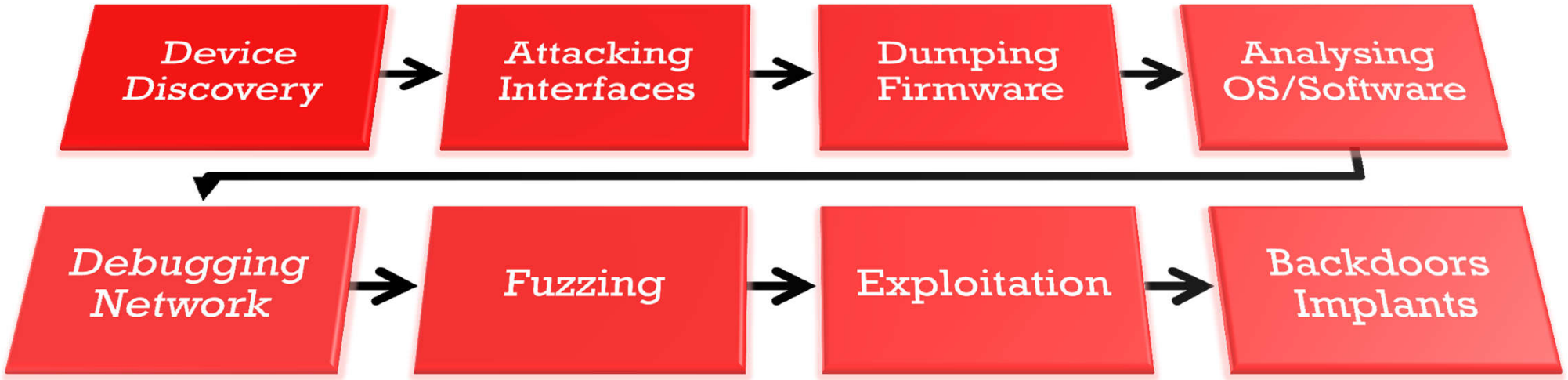
TRADITIONAL TESTING IS NOT SUFFICIENT



- 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



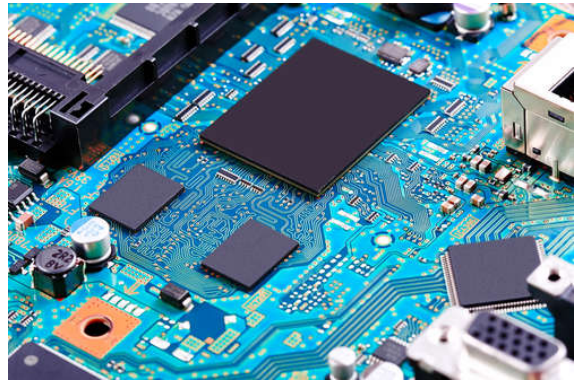
context

HARDWARE HACKING CHRONICLES

EASIER WAYS OF COMPROMISING A DEVICE

Configuration
Edit & Re-Upload

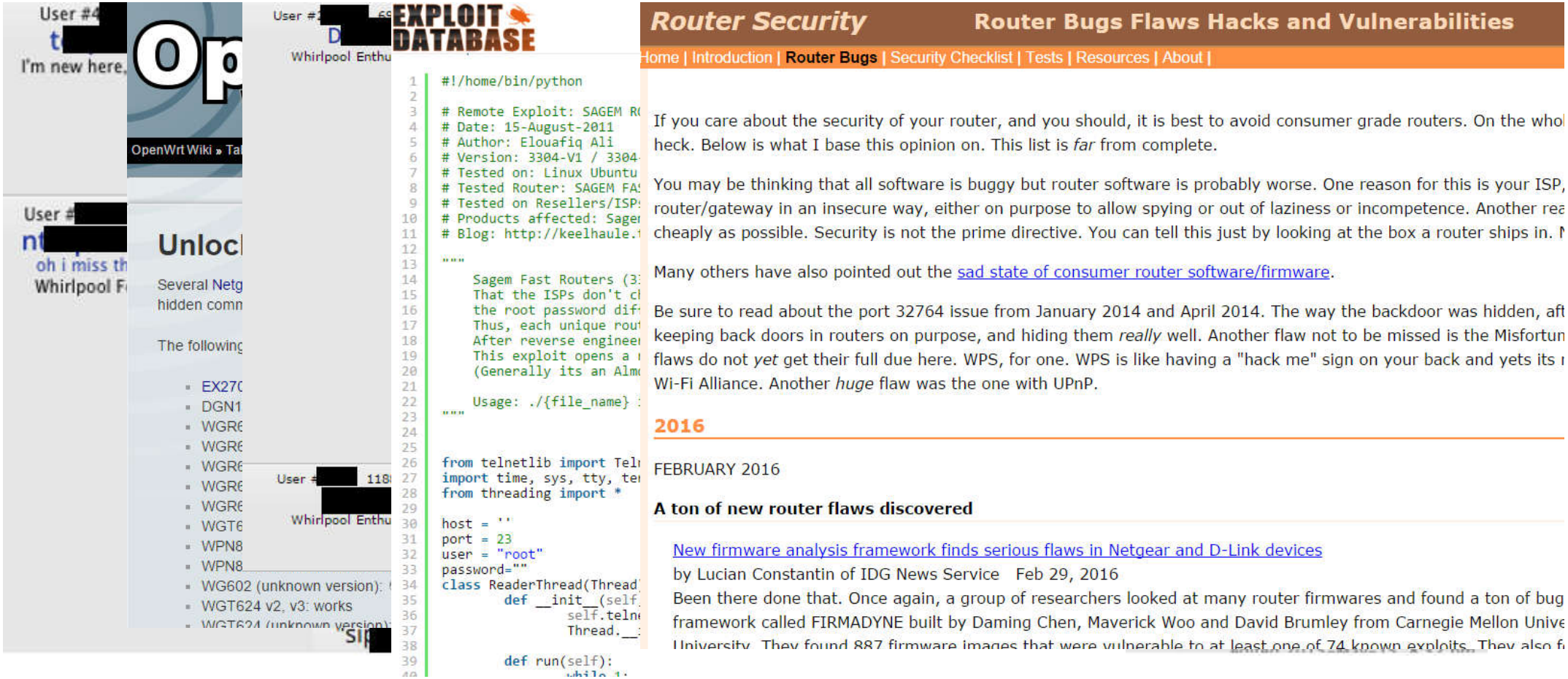
Secret Handshake
to Enable Telnet



Physical
Interfaces

context

PUBLIC INFORMATION IS ALREADY AVAILABLE



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…

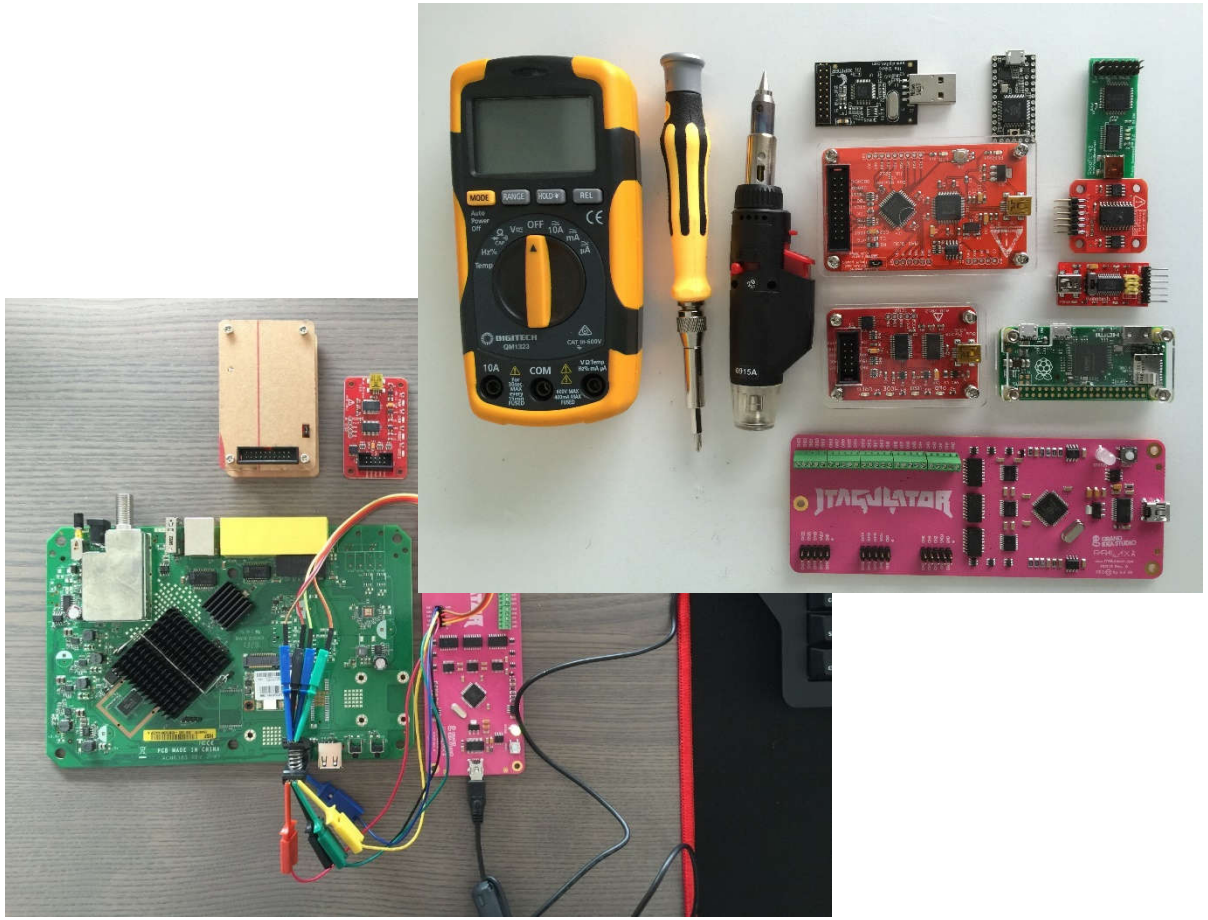
SPI

Access to Flash

Read/Write Data

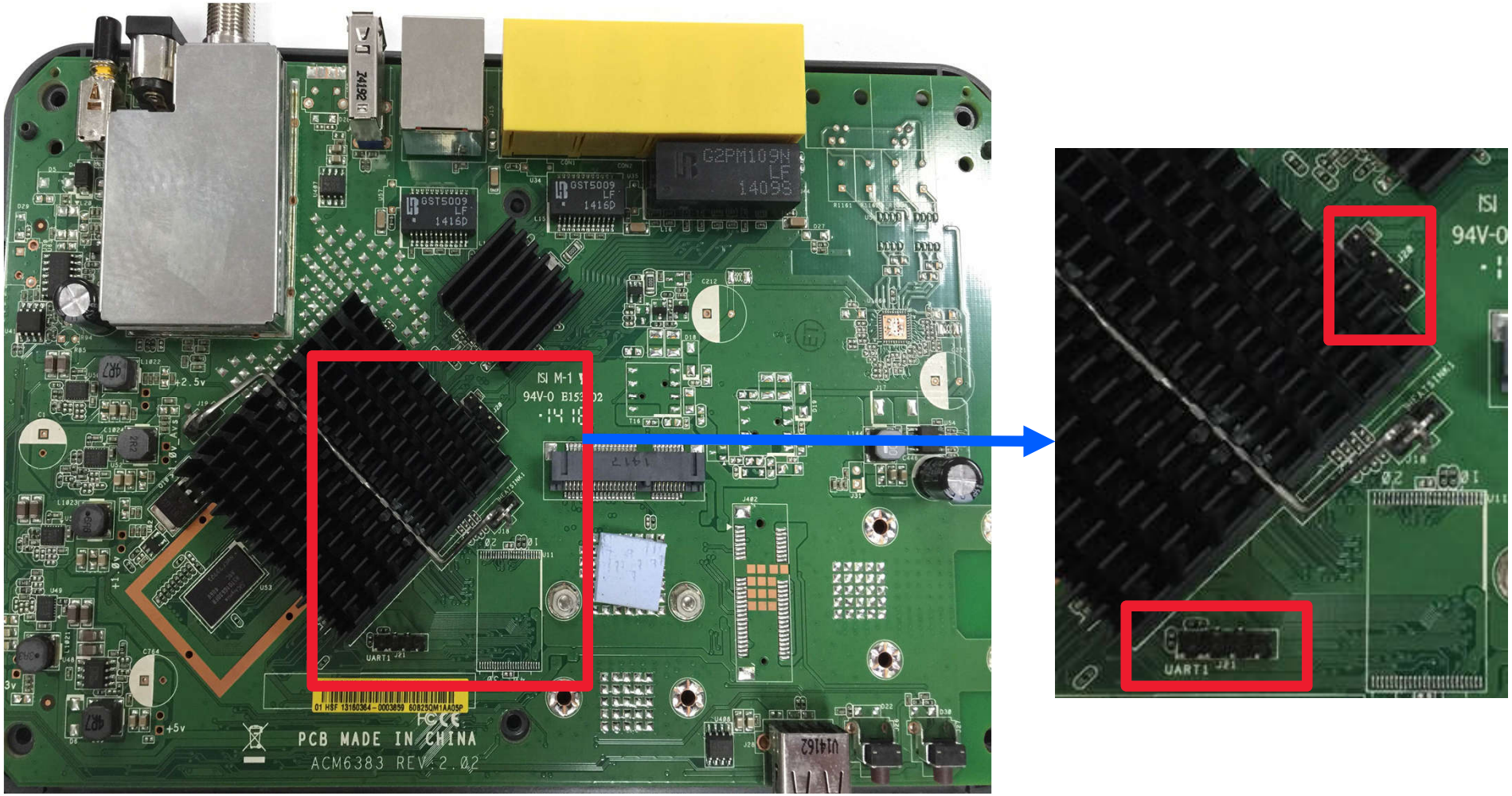
SCK, MOSI, MISO...

HARDWARE ANALYSIS EQUIPMENT



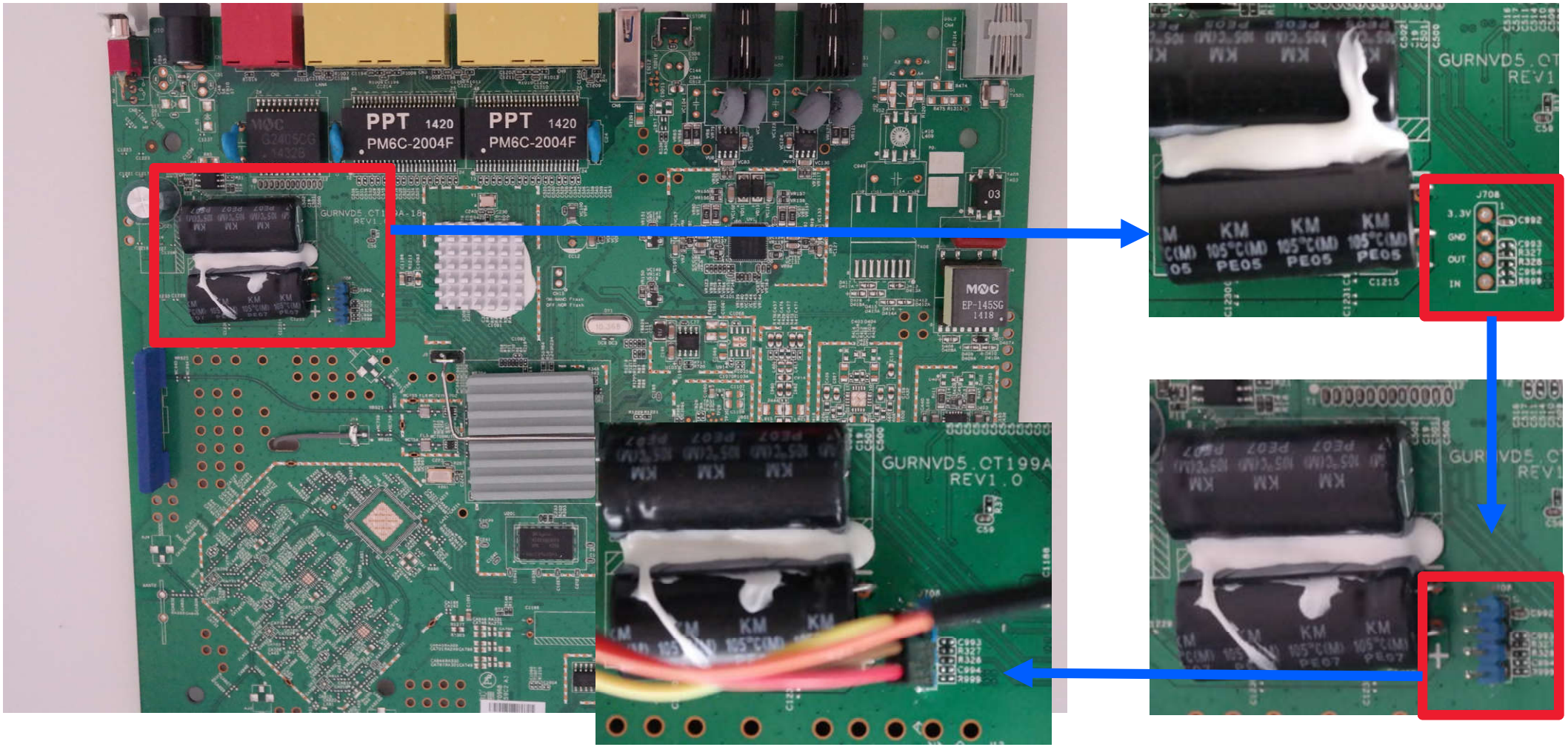
- Bus Pirate
- Bus Blaster
- Shikra
- HydraBus
- Jtagulator
- GoodFet/GreatFet
- Logic Analyser
- SOIC8/16 Clips

PHYSICAL INTERFACES

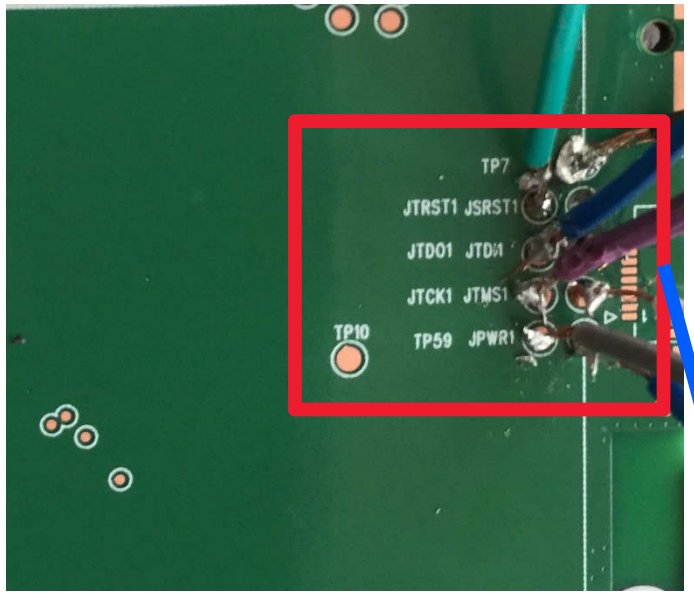


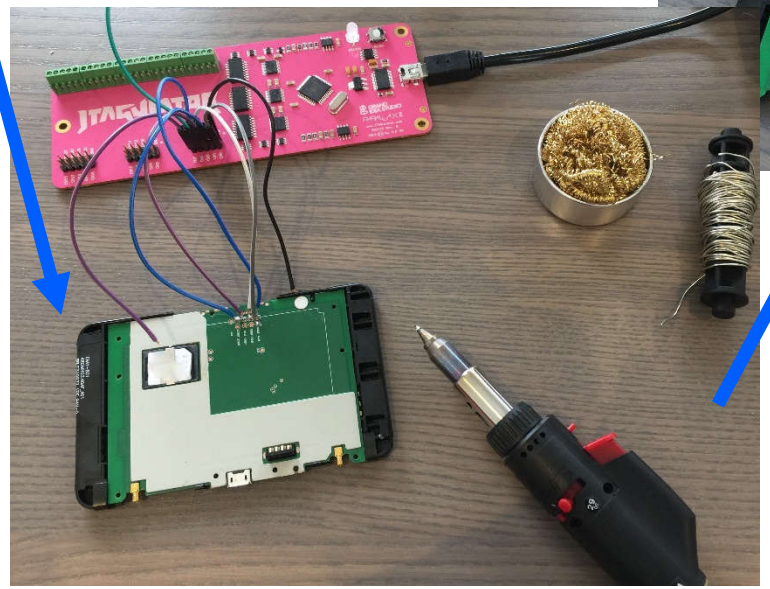
context

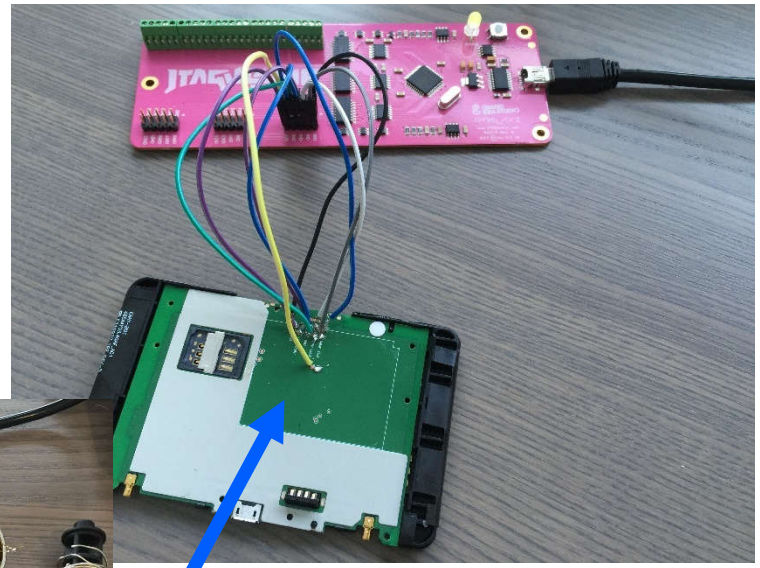
PHYSICAL INTERFACES



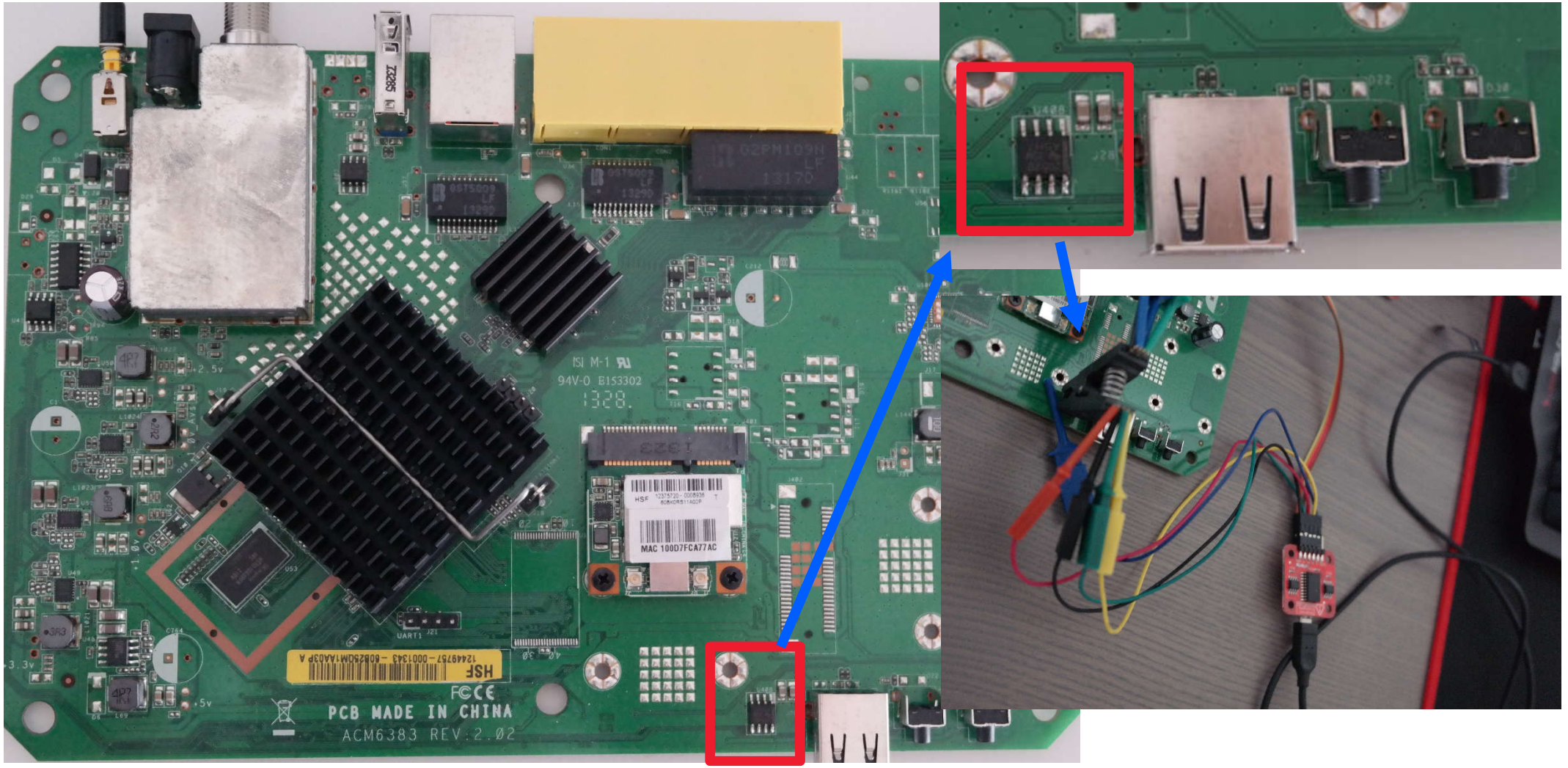
PHYSICAL INTERFACES



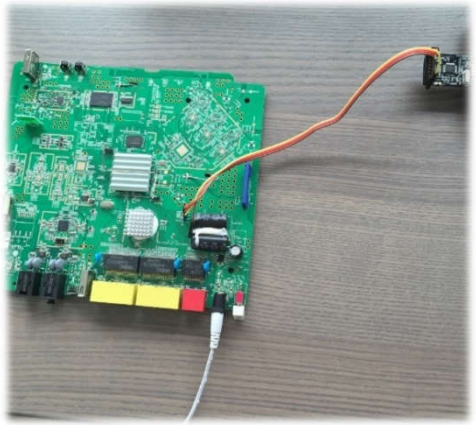




PHYSICAL INTERFACES



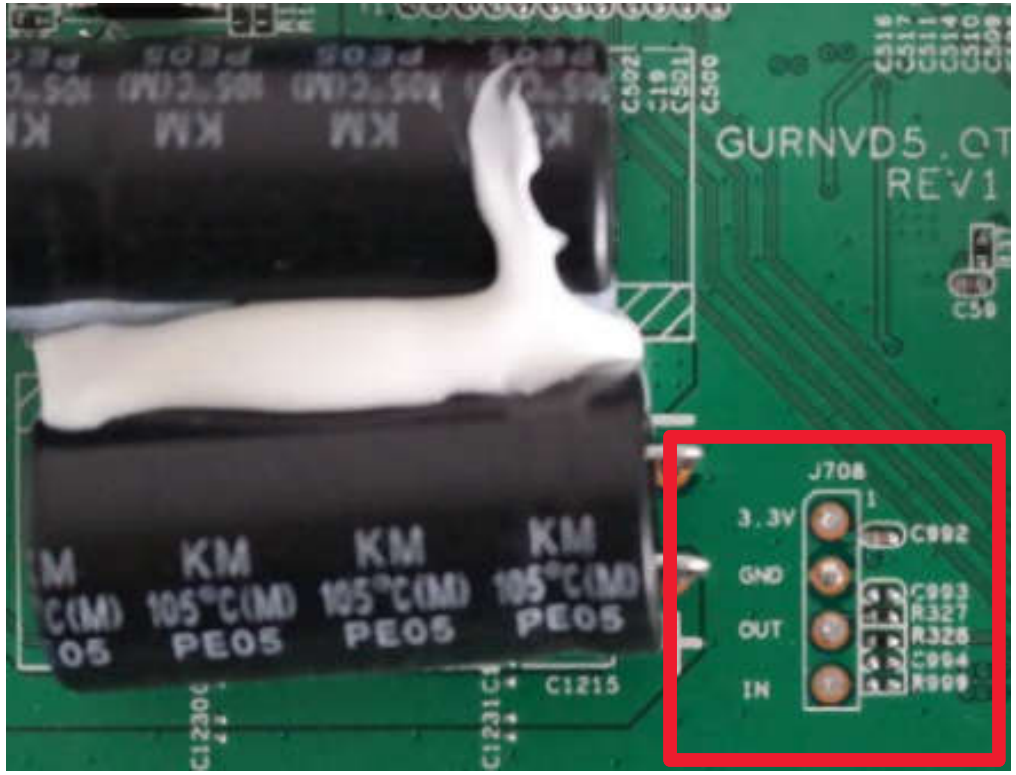
UART/SERIAL CONNECTION



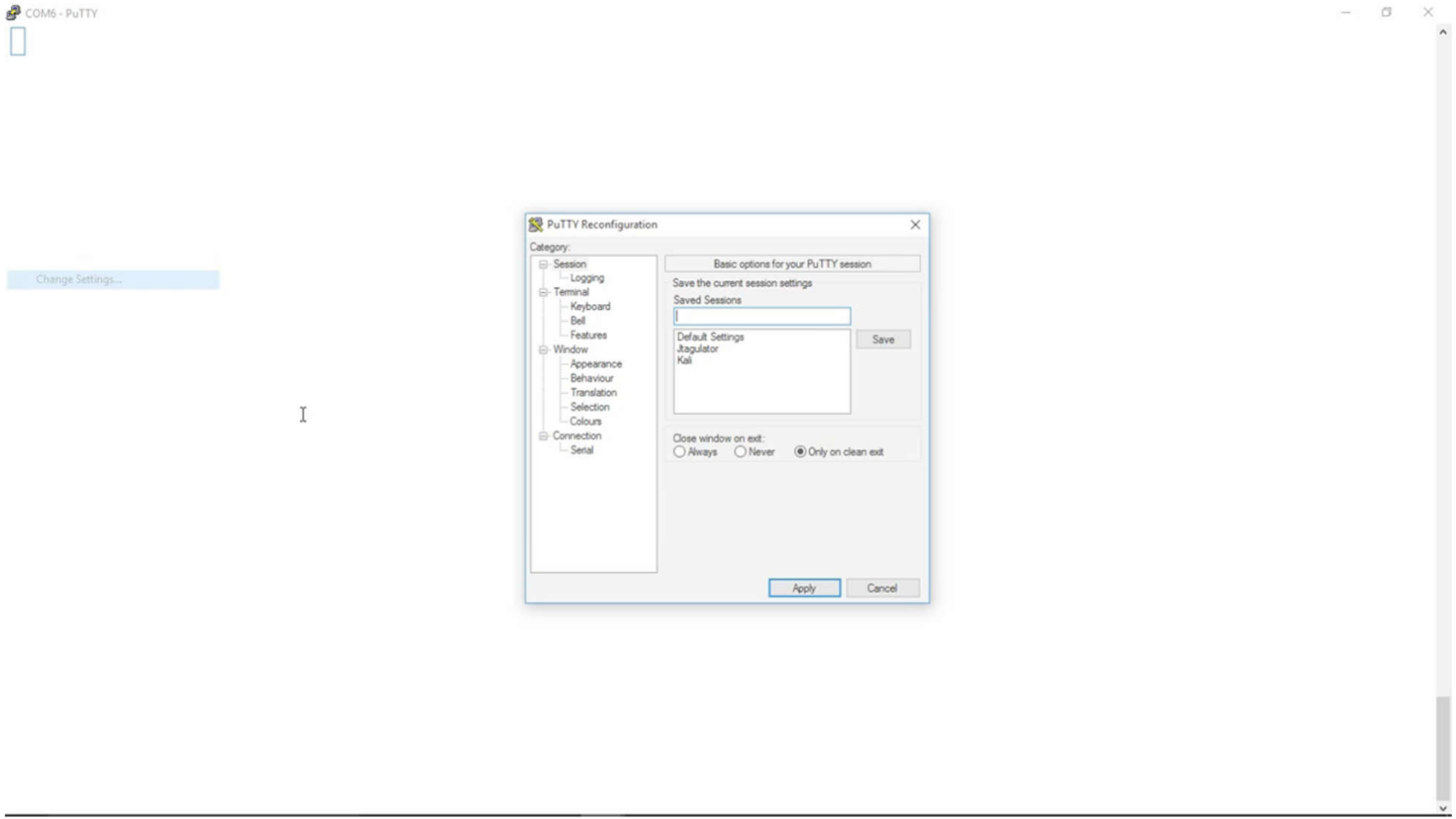
- Usually 4 PINs
  - TX, RX, GND, Voltage
- Provides device access
  - Bootloader, console access
- Real-time debugging
- Access without a password

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

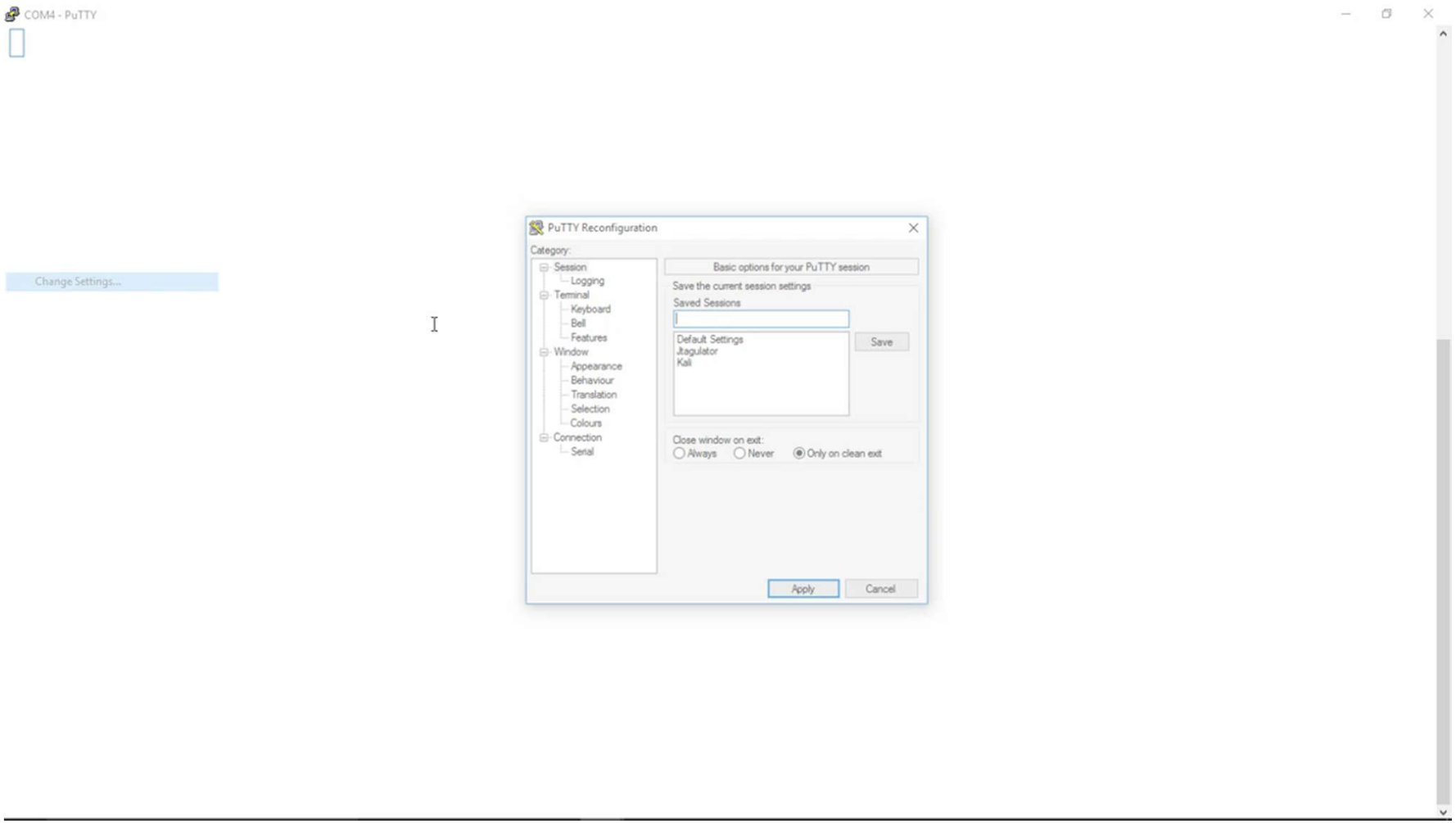


BENEFITS OF UART ACCESS

- Debugging and logging
- Intercepting boot sequence
  - Boot parameters
  - CFE access
- Getting console access

- E.g. Netgear CG3100D

DEMO: UART/SERIAL DEBUGGING



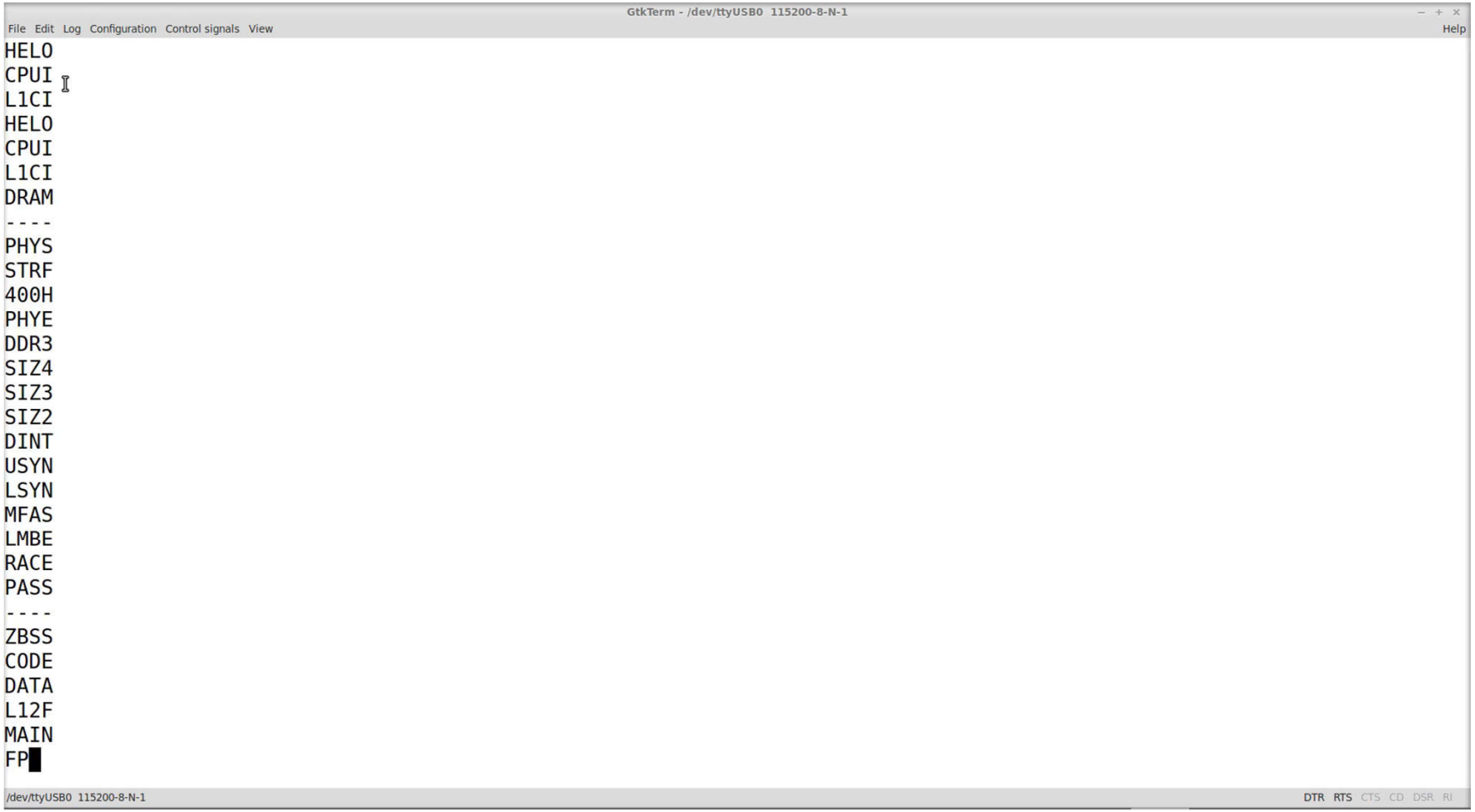
CFE – COMMON FIRMWARE ENVIRONMENT

```
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:ffffff00
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
```

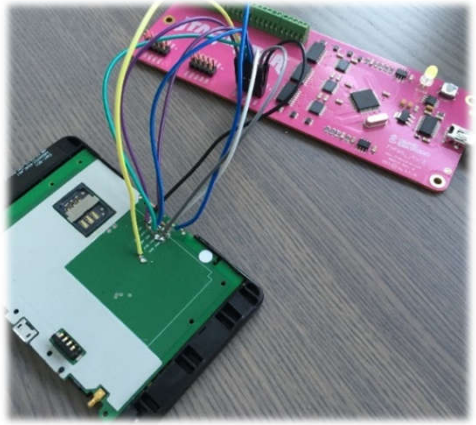
- Stop the boot process
  - UART/Serial connection
- Possibilities
  - Re-flash for OpenWRT
  - Get information
    - Credentials?
  - Dump the firmware
- Eg. Sagemcom 3864v2
  ADSL & NBN

context

DEMO: COMMON FIRMWARE ENVIRONMENT



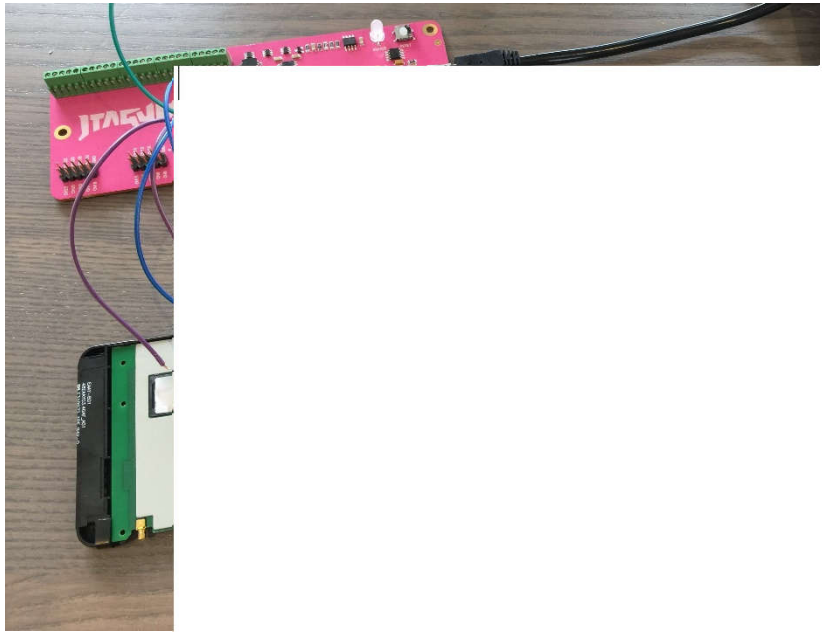
JTAG – JOINT TEST ACTION GROUP



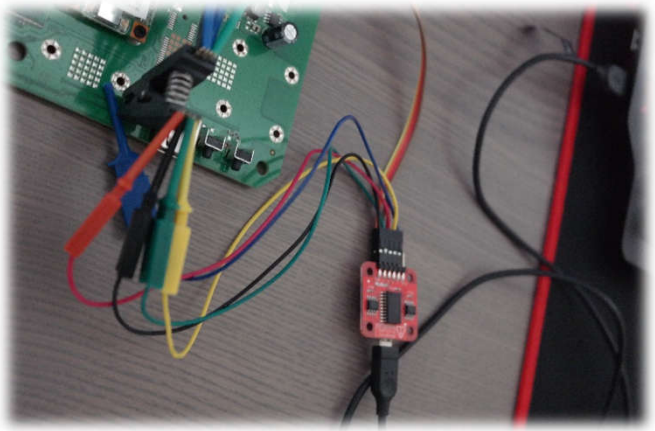
- Debugging standard
- Everything depends on the vendor
- Device or system testing
- Daisy-chained JTAG
  - **TDI** (Test Data In)
  - **TDO** (Test Data Out)
  - **TCK** (Test Clock)
  - **TMS** (Test Mode Select)
  - **TRST** (Test Reset)

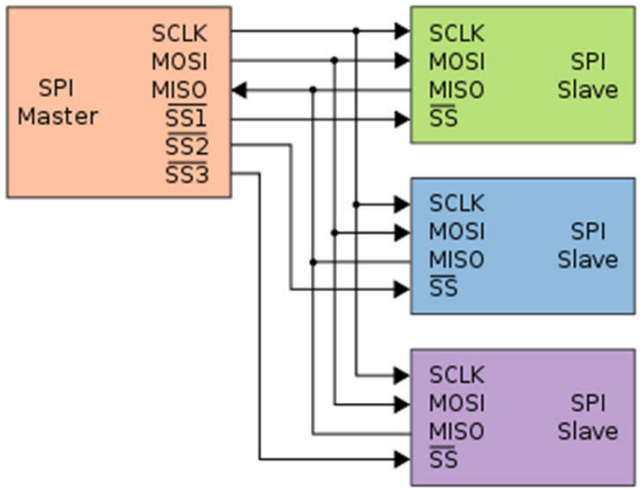
context

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

context

CUSTOMER PREMISES EQUIPMENT

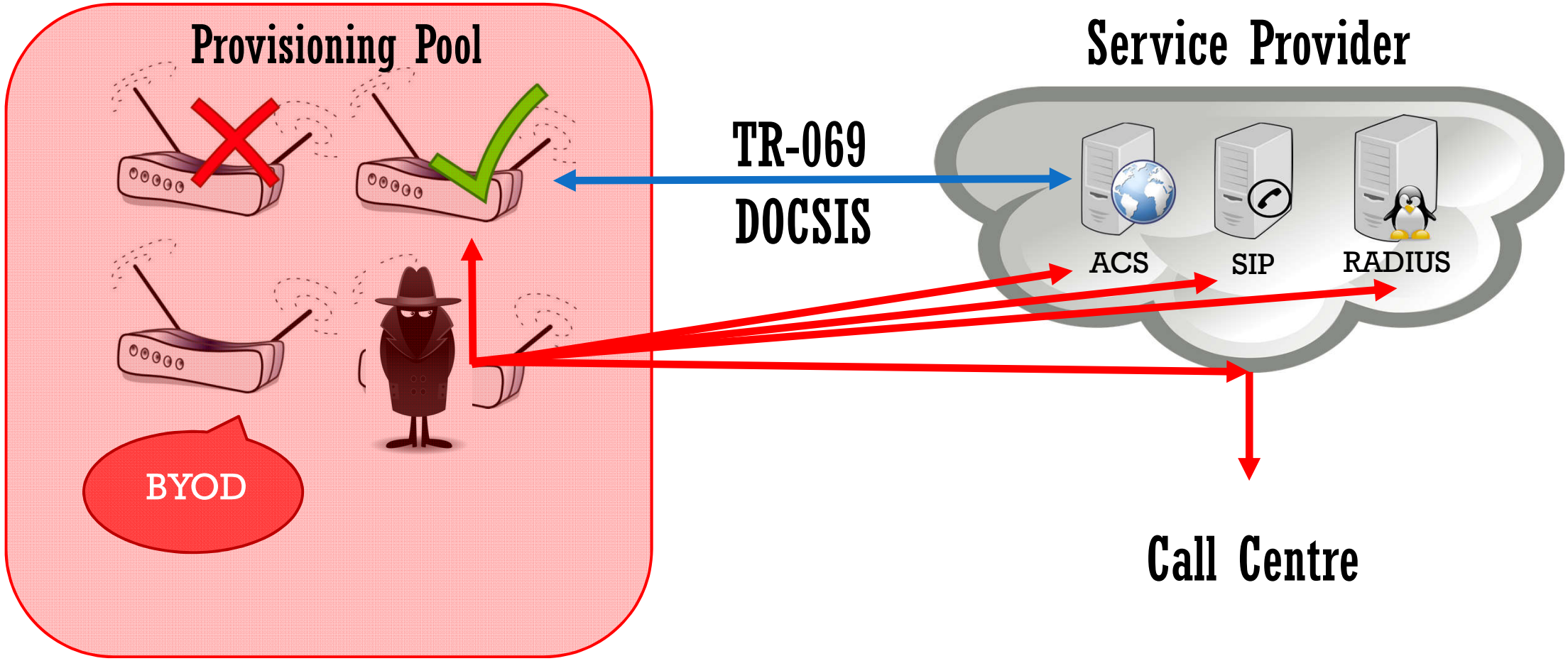
CONSUMER AND SUBSCRIBER SERVICES

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

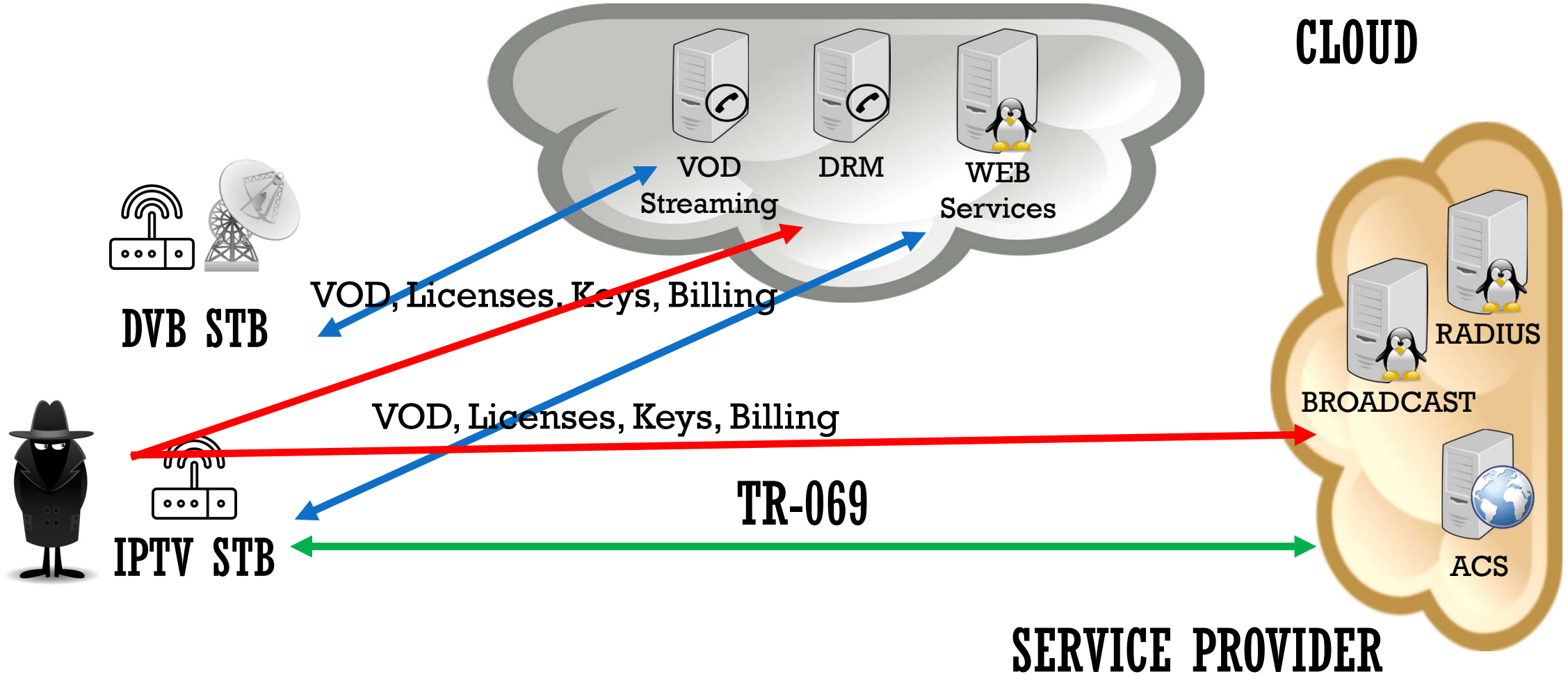
CONSUMER AND SUBSCRIBER SERVICES

- 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

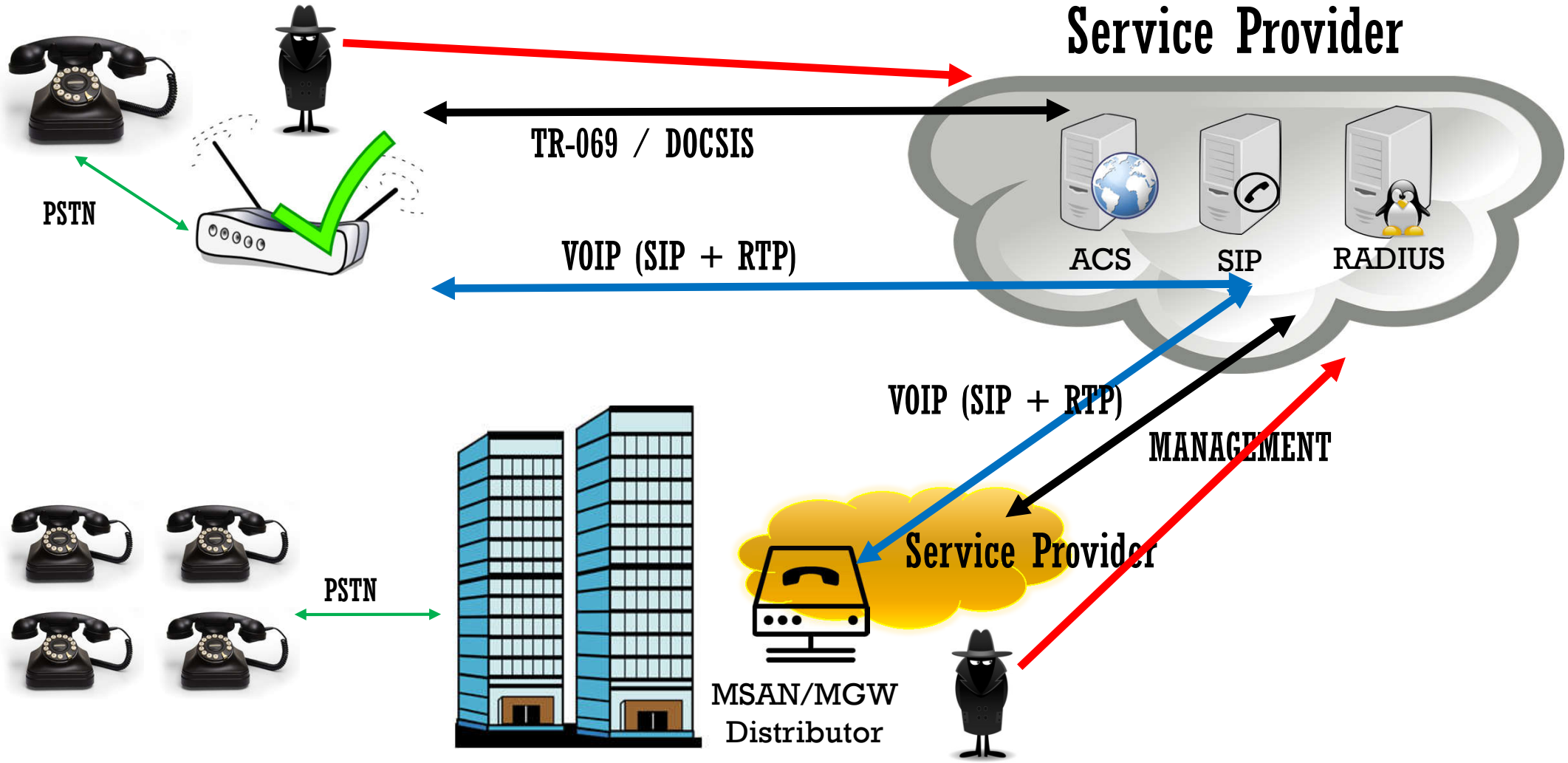
BROADBAND DEVICES



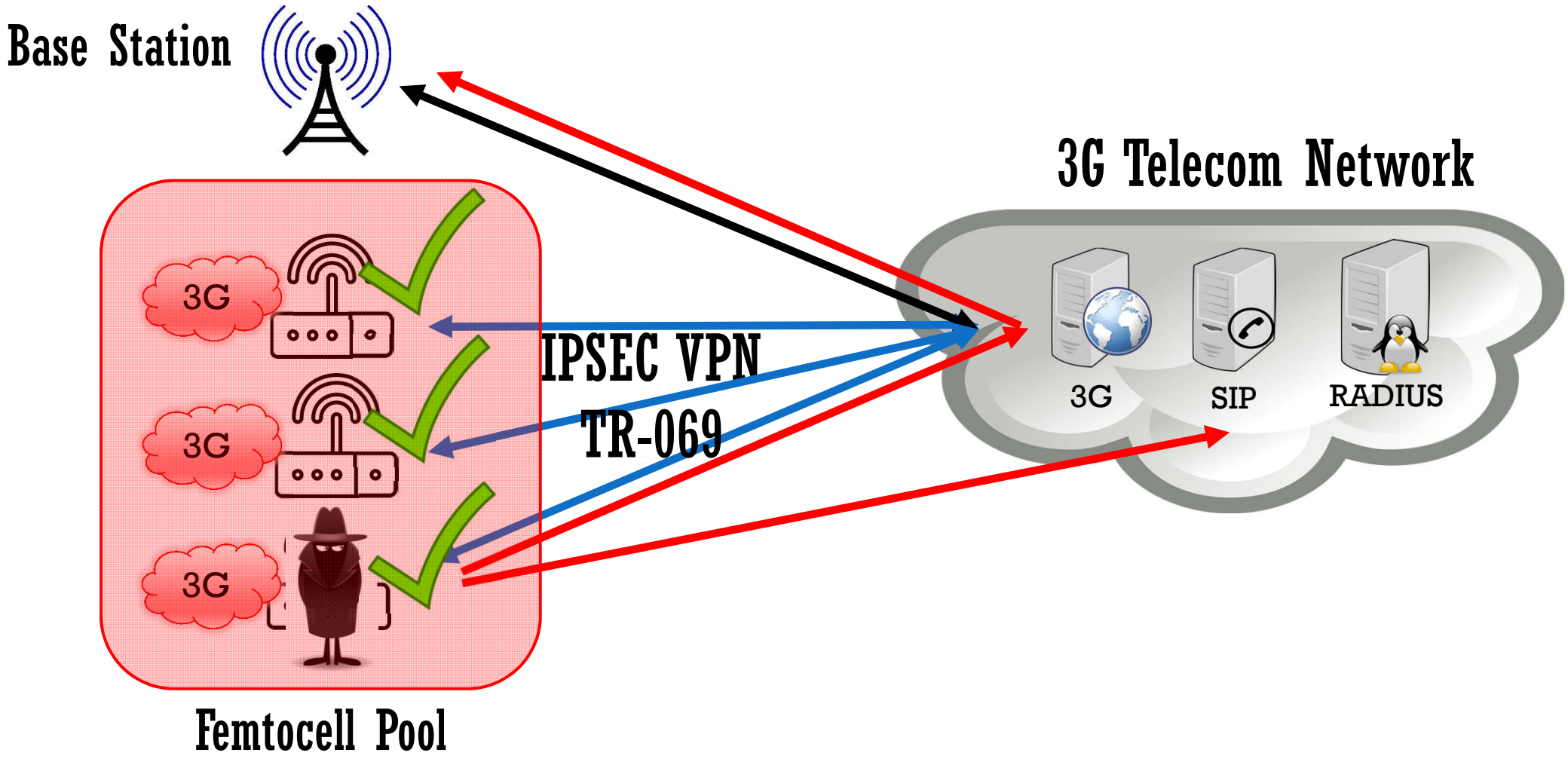
DVB & IPTV DEVICES



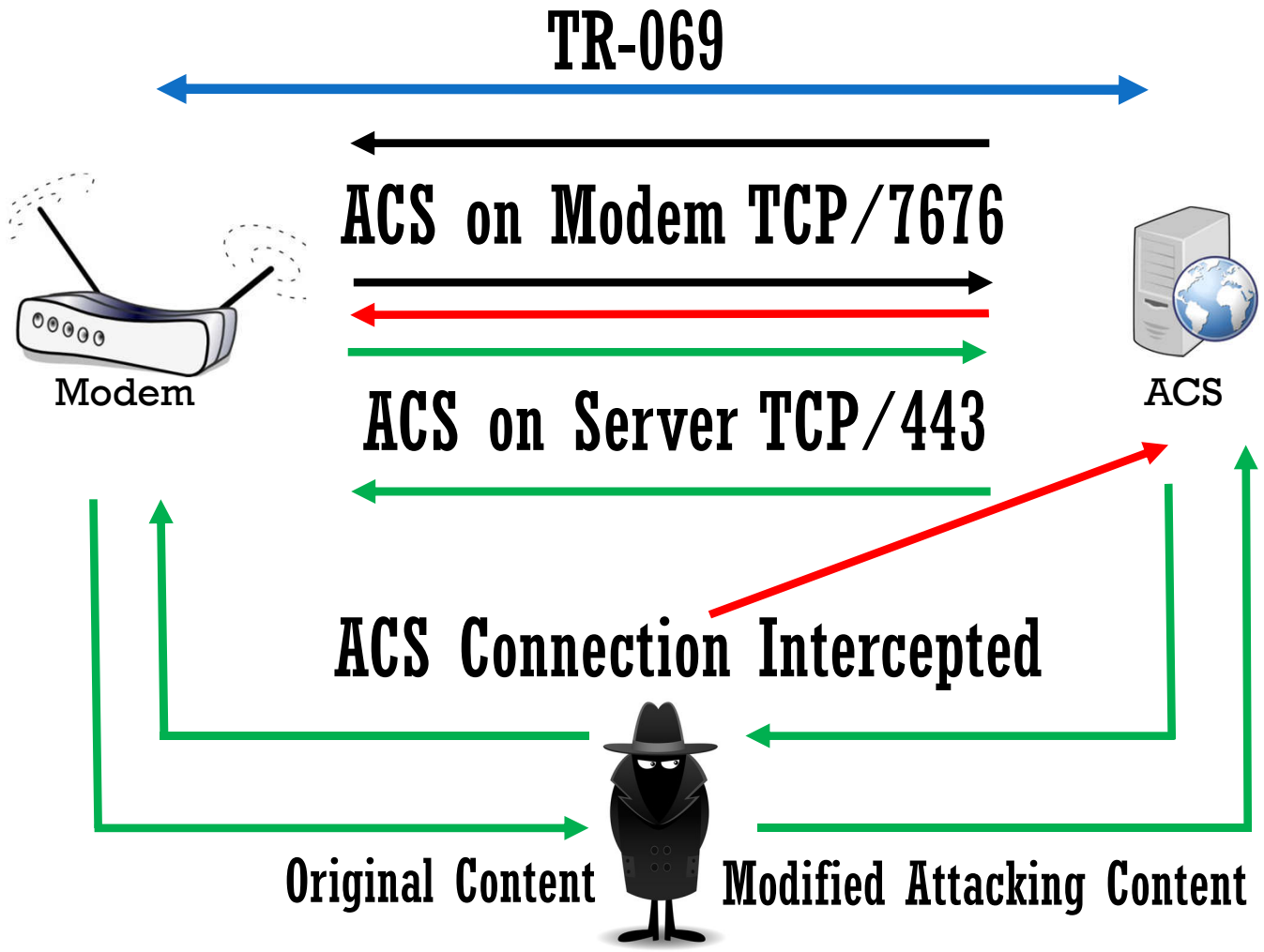
UNIFIED COMMUNICATIONS DEVICES



FEMTOCELL DEVICES



ATTACKING TR-069 NETWORKS



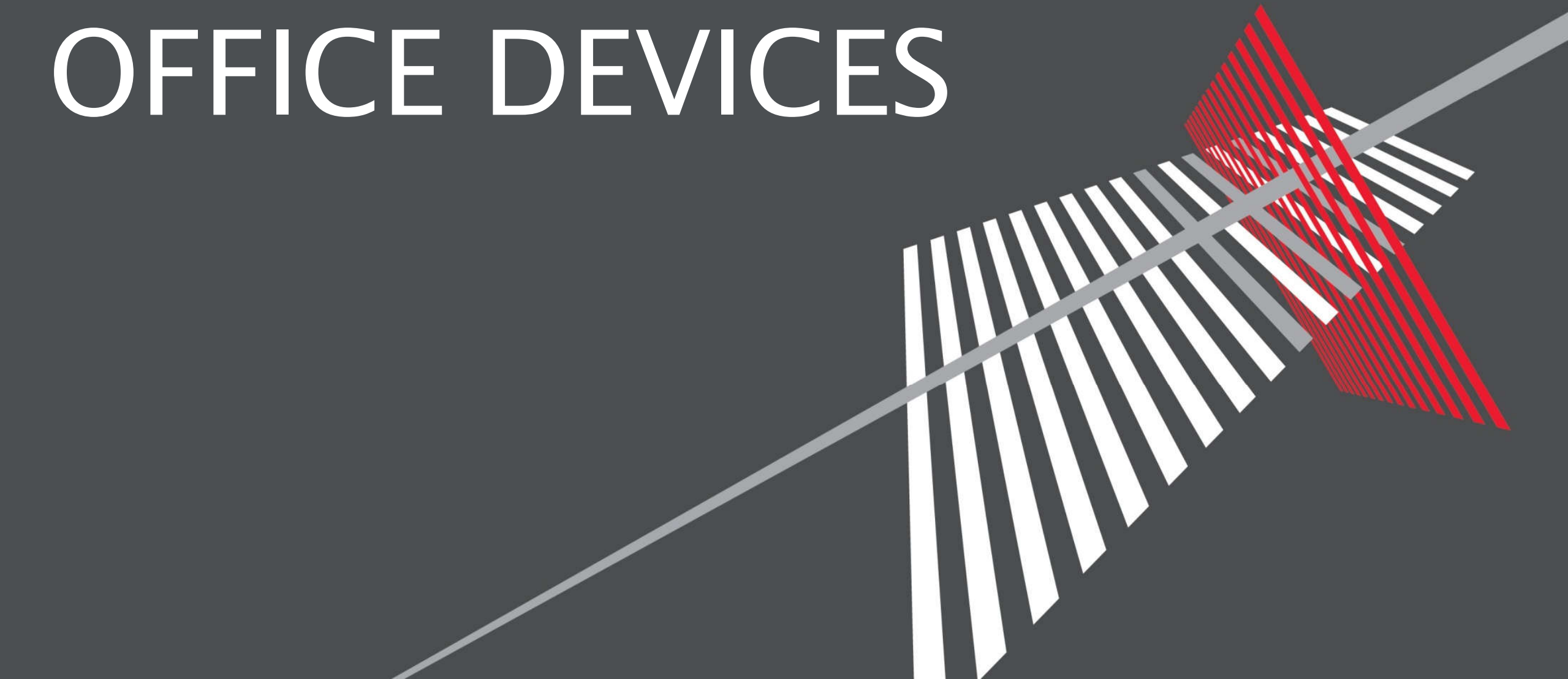
- Debugging
- Gathering Information
- Attacking
  - Server
  - Service network
  - Clients connected

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

context

OFFICE DEVICES



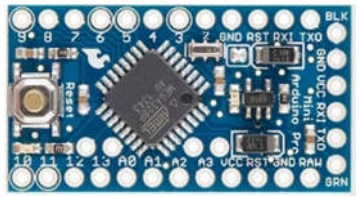
HARDWARE IMPLANTS, BACKDOORS, SNIFFERS

- 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

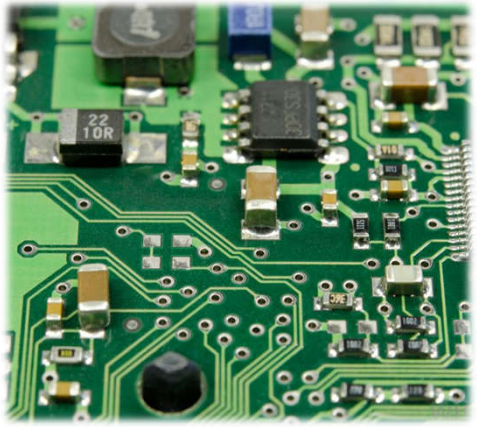
- 3G/4G Modems
  - WiFi models with services and features
  - USB models require drivers
  - Internal storage and card reader
- Unauthorised access via services
- Firmware operations
  - Dumping and reversing the firmware
  - Backdooring the firmware
- Using their shelves for USB duckies

WIRELESS KEYBOARD ATTACKS



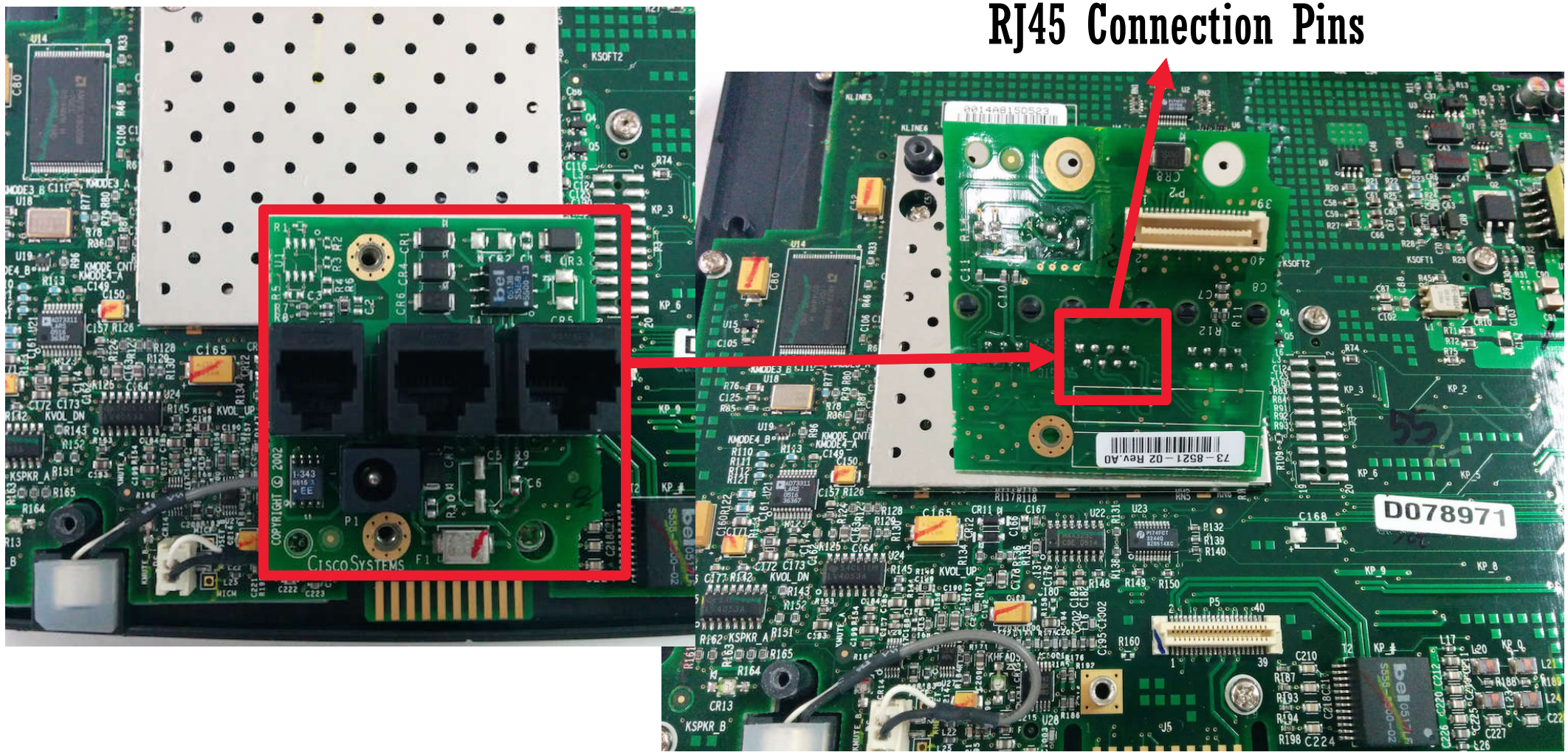
- Keysweeper by SamyKamkar
  - Arduino/Teensy based sniffer
  - Sniffing Microsoft Wireless Keyboard
- Mousejack by Bastille Security
  - RF keyboard & mouse receivers
  - Force pairing vulnerability
  - Force pairing a remote keyboard

MAKING AN IMPLANT FOR TESTING

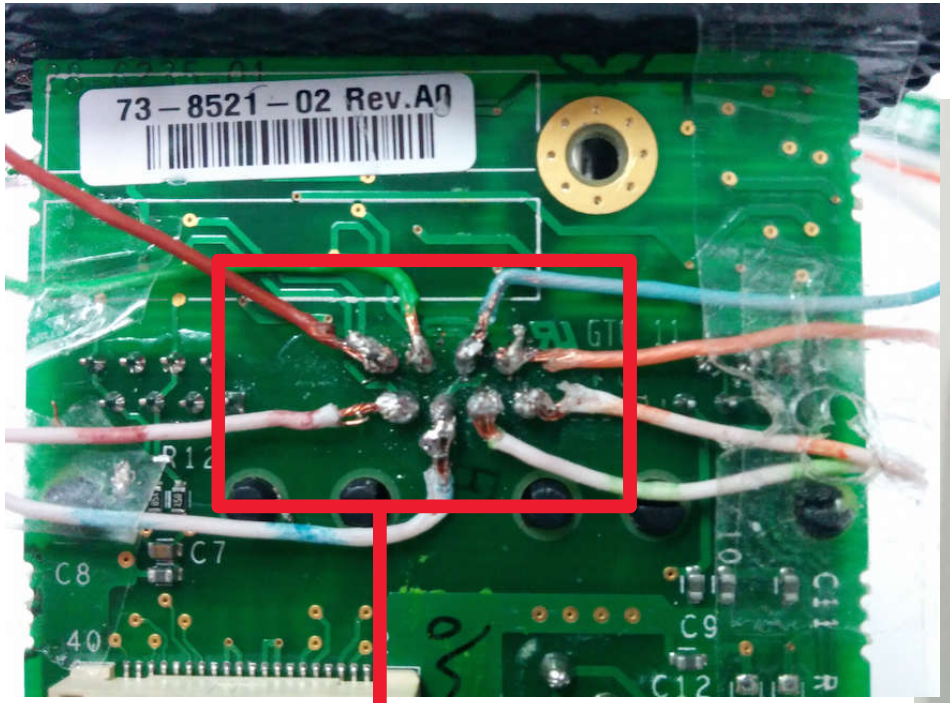


- Efficient for persistent access
  - Raspberry Pi, Arduino
  - Can fit in many devices
- Find a suitable device to backdoor
  - Find a power source
  - Find a network connection
  - Solder and connect the pieces
  - Broadcast the network connected
- Advanced implants take time

MAKING AN IMPLANT FOR A CISCO IP PHONE

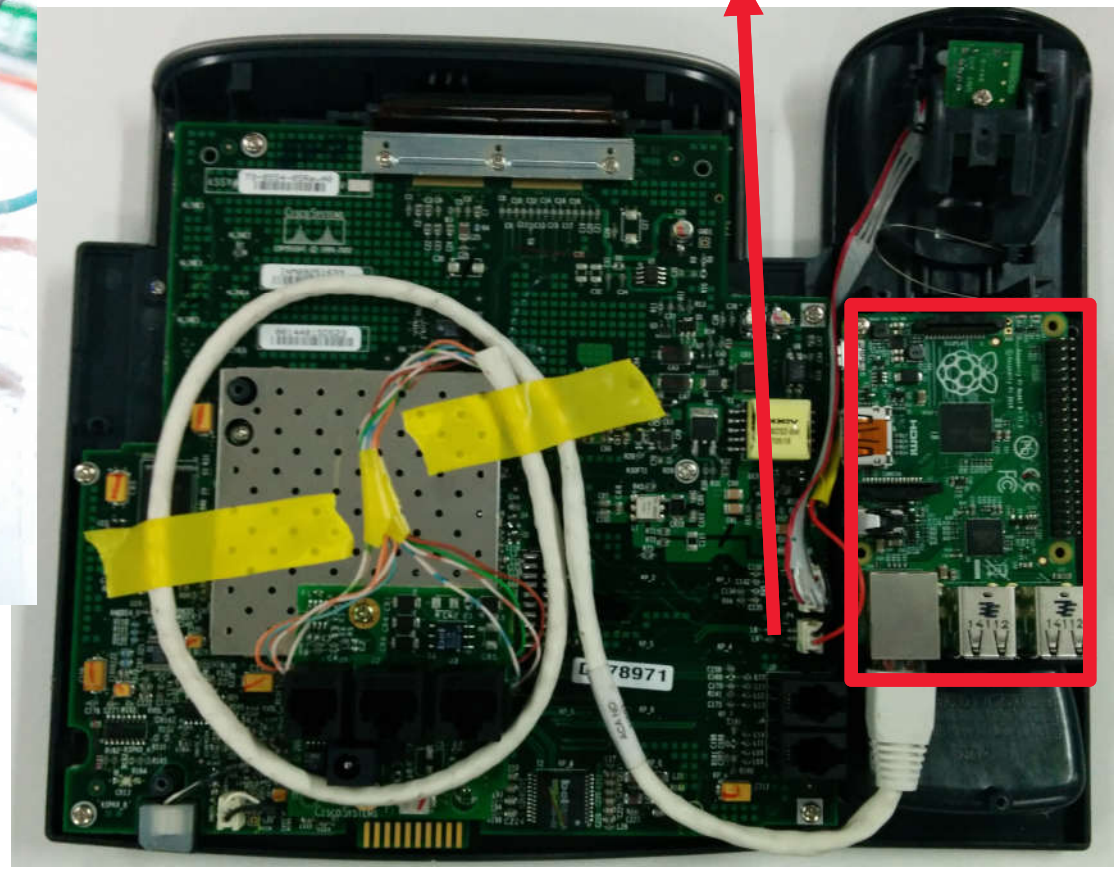


MAKING AN IMPLANT FOR A CISCO IP PHONE



Patch the Cat5 cable

Speaker Power



context

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

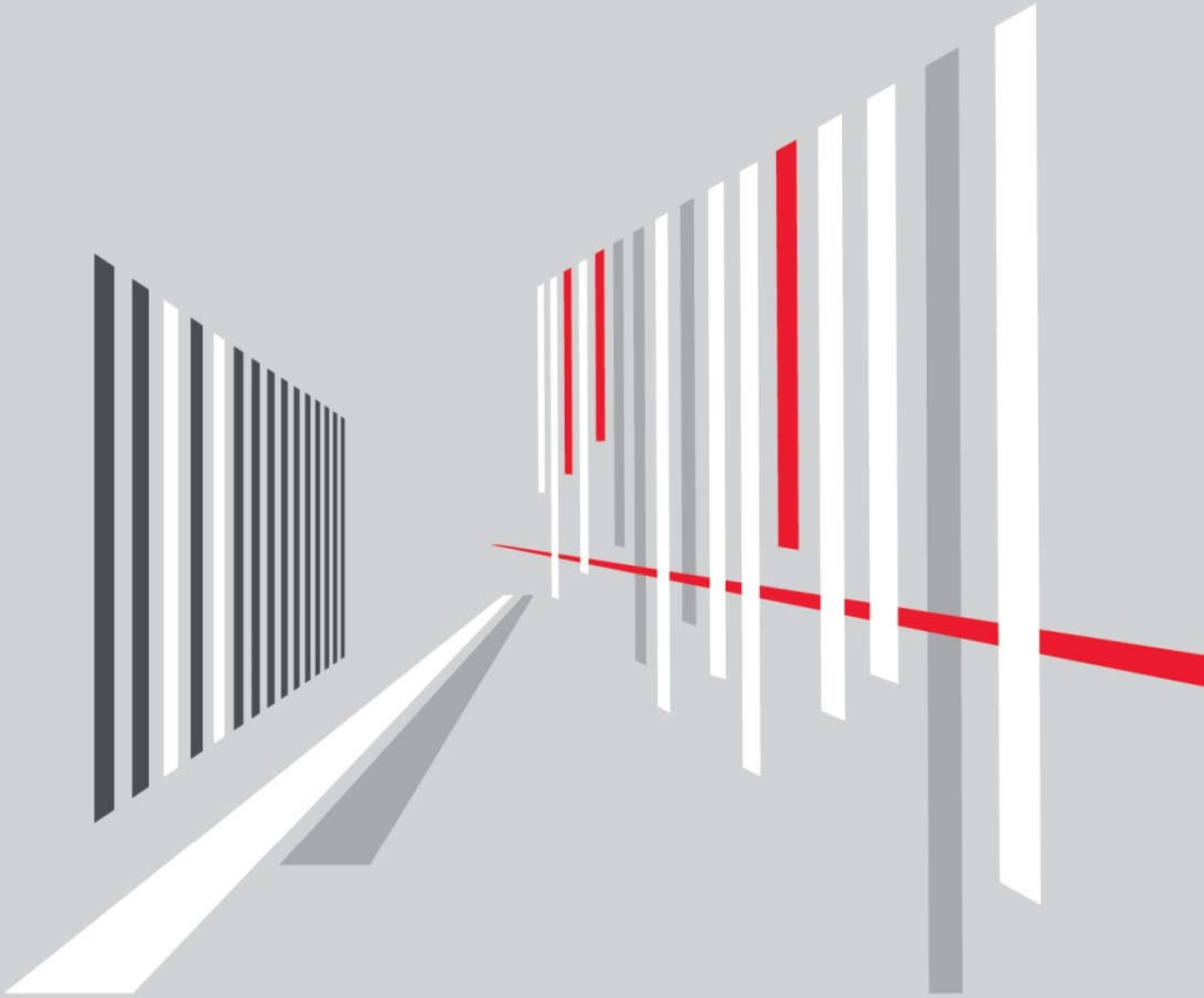
https://www.auscert.org.au

- IoT Security Wiki

https://iotsecuritywiki.com

context

QUESTIONS?



context

THANKS!