To dock or not to dock, that is the question:
Using laptop docking stations as hardware-based attack platforms

Andy Davis, Research Director NCC Group

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Thame

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland

North American Offices

San Francisco

Atlanta

New York

Seattle

Australian Offices

Sydney

Agenda

- Why docking stations?
- How do docking stations work?
- What would a hardware implant do?
- The Control Platform
- Physical space available
- Detecting docking station-based hardware implants
- Attack mitigation
- Conclusion

Why docking stations?

- Access to all the ports available on the connected laptop (often several that aren't)
- Used in "hot-desking" environments - access to a different laptop each day
- Permanently connected to a power supply and to the network
- “Dumb" devices, trusted by users and IT admins
- Passive and anonymous – easily replaced with an “implanted” dock
- Often enough space inside the case for additional hardware
- Encrypted data is decrypted at the laptop and is therefore accessible in the clear
- Is the threat realistic?...Yes, I believe it is

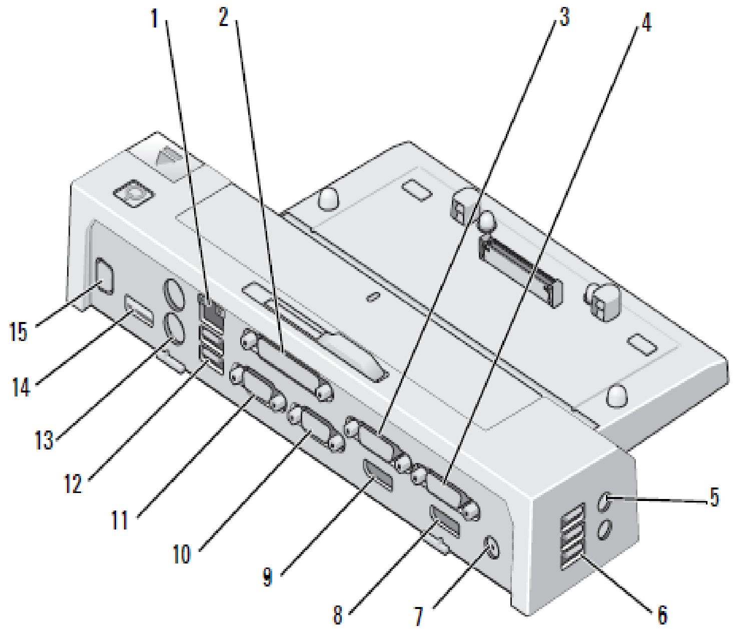
How do docking stations work?

- Focus of this research was the Dell E-Port Plus (PR02X)
  - I'm familiar with it, as we use them at NCC Group
  - Has a useful property – plenty of spare space inside
- Extends interfaces on the laptop
- Provisions new interfaces e.g. USB and extra DisplayPort via additional circuitry
- Has passive Ethernet switch – laptop Ethernet port disabled when docked
- Also has internal 5-port USB hub
- If headphones/microphone are connected to the laptop then any connected to the dock will not work

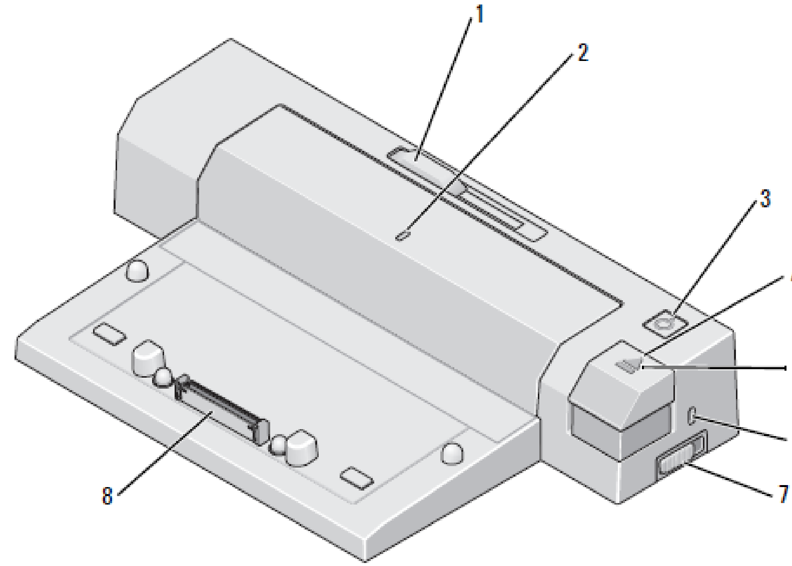
How do docking stations work? (2)

- No publicly available information about the PR02X circuit design
- No public details about the Dell E-Series dock connector
- Time to look at the PR02X more closely…

PR02X Interfaces and buttons

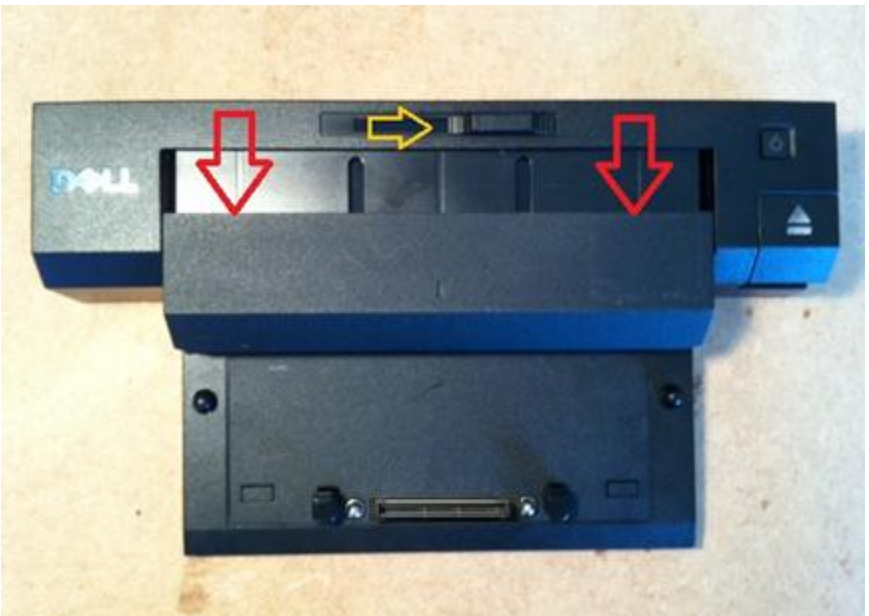


1	network connector	2	parallel connector
3	video 2 DVI connector	4	video 1 DVI connector
5	audio connectors (2)	6	USB connectors (3)
7	AC adapter connector	8	video 1 DisplayPort connector
9	video 2 DisplayPort connector	10	VGA connector
11	serial connector	12	USB connectors (2)
13	PS/2 connectors (2)	14	USB or eSATA connector
15	E-Monitor Stand connector		



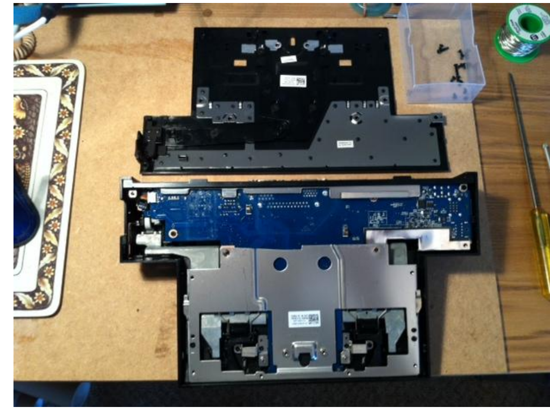
1	battery bar adjuster	2	alignment mark
3	power button	4	eject button
5	docking light	6	security cable slot
7	lock/unlock switch	8	docking connector

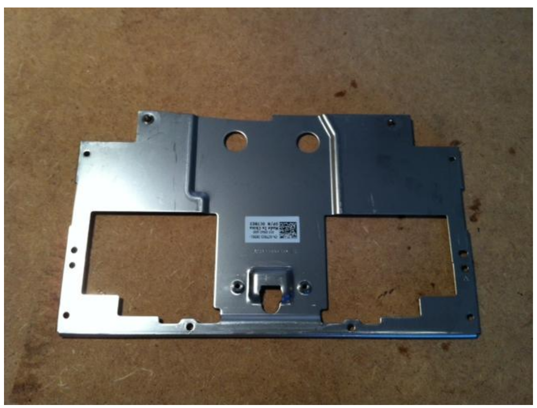
PR02X Useful feature – extra space!

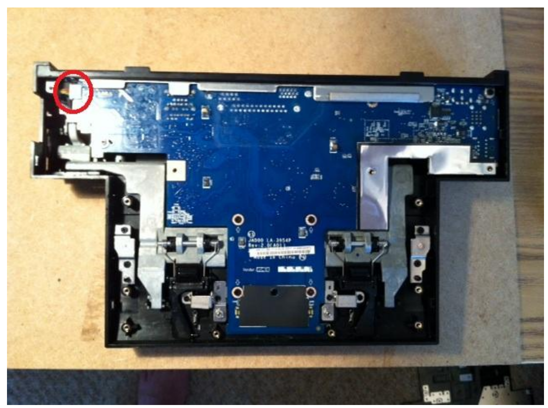


- Move slider (yellow arrow) right
- Compartment extends (red arrows)
- Not configured for extra-large battery
- Internal free space doubles
- Extra room for additional features ☺

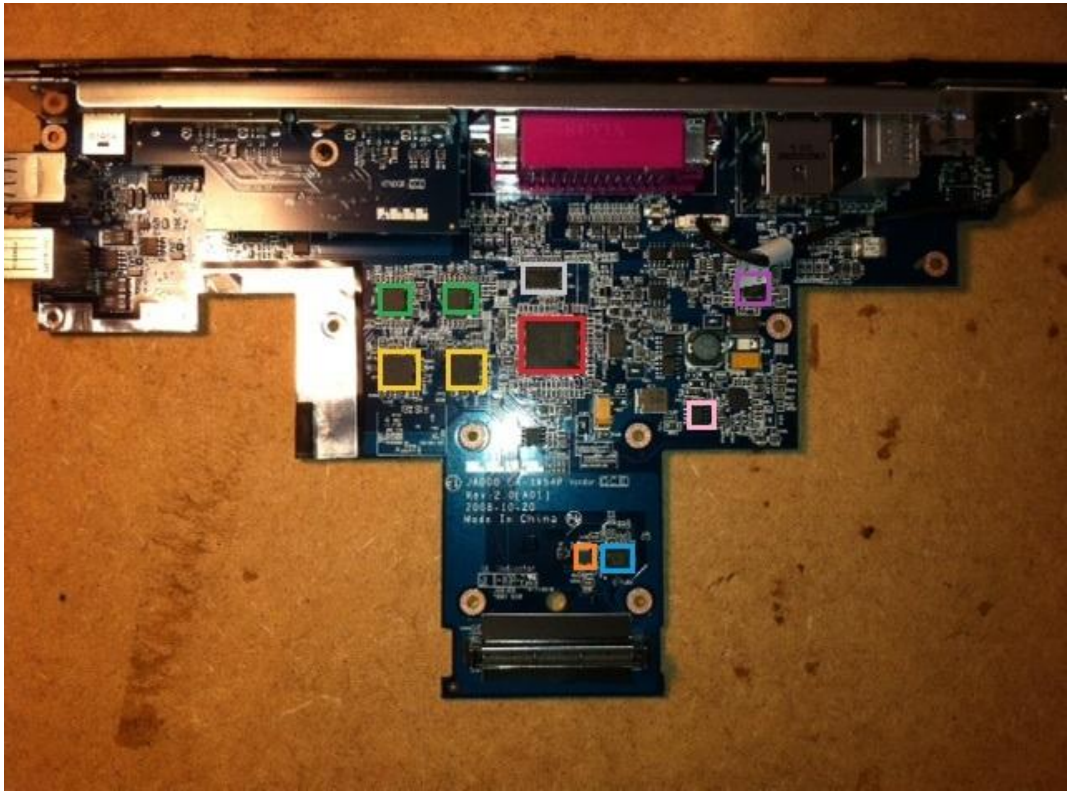
PR02X Teardown







PR02X Teardown



Red - I/O Controller for Port Replicators and Docking Stations

Yellow - DisplayPort 1:2 Switch with Integrated TMDS Translator

Green - Dual Mode DisplayPort Repeater

Blue - 3.2Gbps 2-channel SATA ReDriver

Orange - Fast Response Positive Adjustable Regulator

Pink - Adjustable-Output, Step-Up/Step-Down DC-DC Converter

Purple - USB 2.0 High-Speed 3-Port Hub Controller

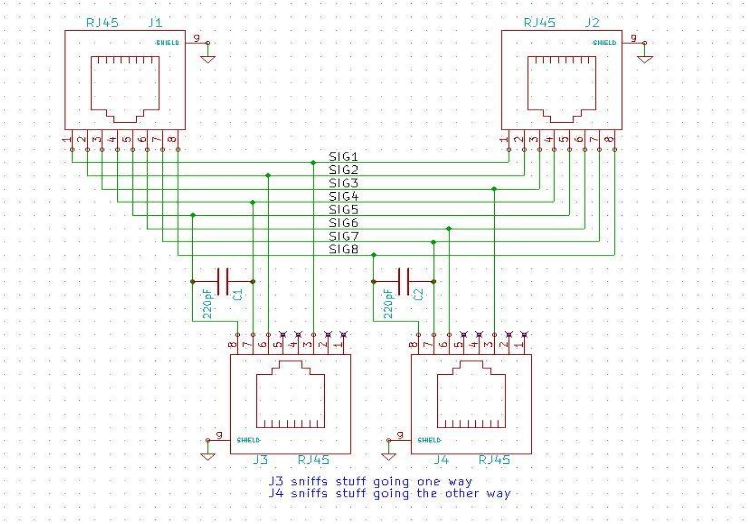
Grey - Multichannel RS-232 Line Driver/Receiver

What would a hardware implant do?

- Capture data from connected laptop via interfaces
- Insert data, emulating devices
- Exfiltrate stolen data via an out-of-band channel
- Identify when different laptops are connected
- Remain as stealthy as possible

Passive network tapping

- Two interfaces required (one for each direction)
- Only 10BASE-T and 100BASE-TX supported
- For 1000BASE-T capacitors downgrade speed
- Lots of data would be captured – filtering required
- **Advantages:** Very stealthy

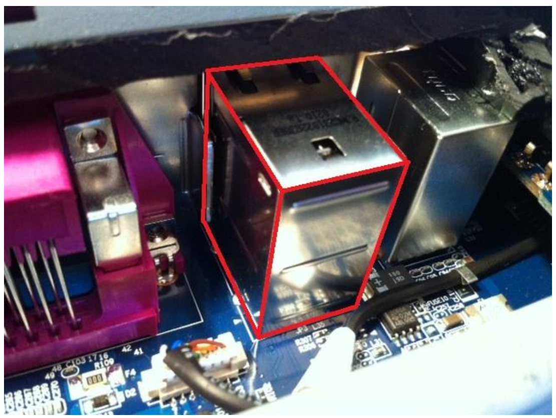


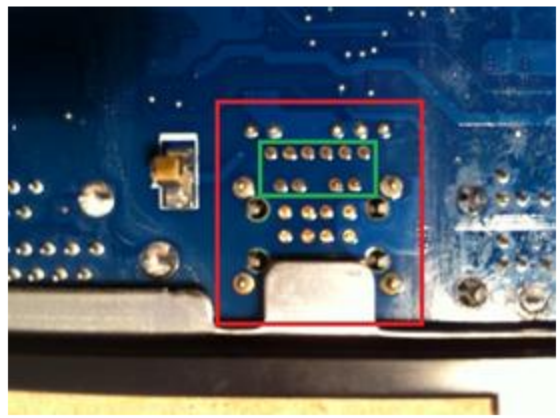
Circuit design by Michael Ossmann

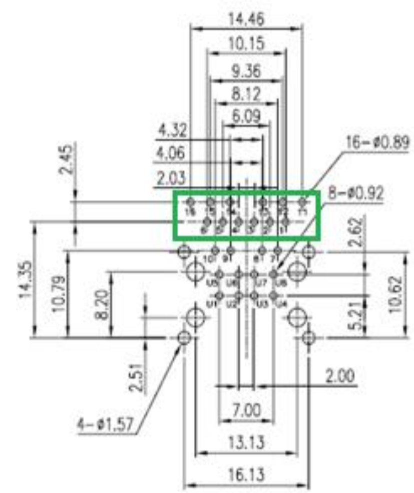
nccgroup
freedom from doubt

Passive network tapping – where to tap

RJMG2310 series module produced by Amphenol Corporation in Taiwan







RECOMMENDED PCB LAYOUT
(ALL TOLERANCES ARE ±0.05)

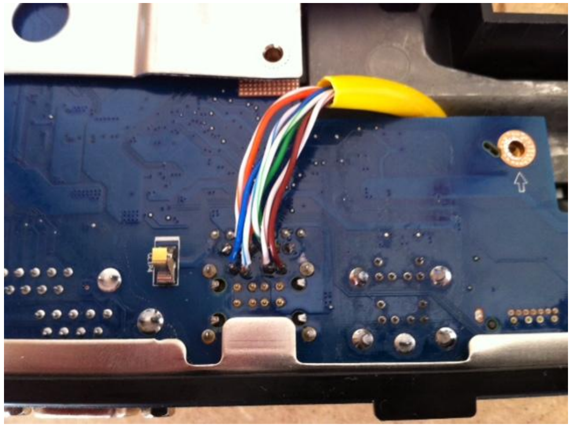
PIN	SYMBOL
1	GND
2	T/R1+
3	T/R1–
4	T/R2+
5	T/R2–
6	COMMON CT
7	T/R3+
8	T/R3–
9	T/R4+
10	T/R4–

GIGA BIT RJMG PINOUT

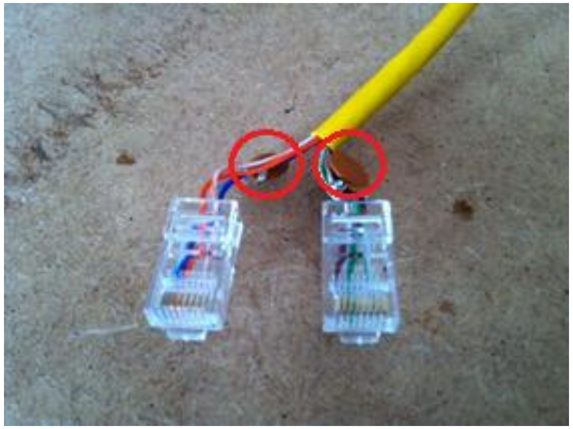
PIN	SYMBOL
1	VCC
2	–DATA
3	+DATA
4	GROUND
5	VCC
6	–DATA
7	+DATA
8	GROUND

STACKED USB PINOUT

Passive network tapping – where to tap (2)



Tap in place on the dock



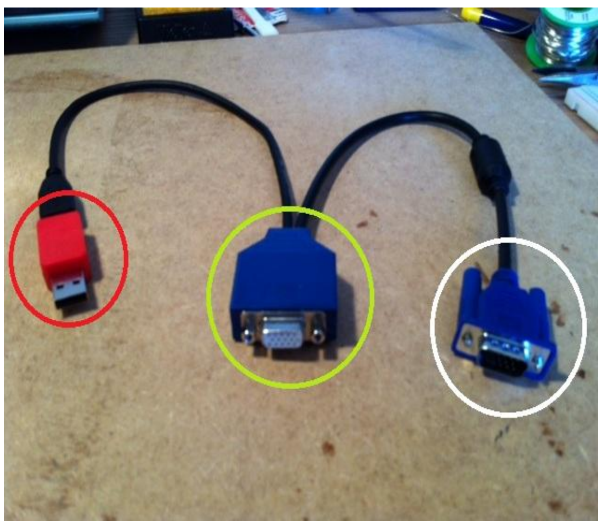
Other end of the tap ("downgrade attack" capacitors circled)

Active network attack

- More useful – can mount network-based attacks from the implant
- More space required – Ethernet hub needs to be inserted into the dock
- More engineering required – hub needs to be inserted between the laptop and dock
- More likely to be detected – new device will appear on the LAN

Passive video monitoring

- Obtain periodic screenshots of the laptop’s display
- **Advantage:** Very Stealthy



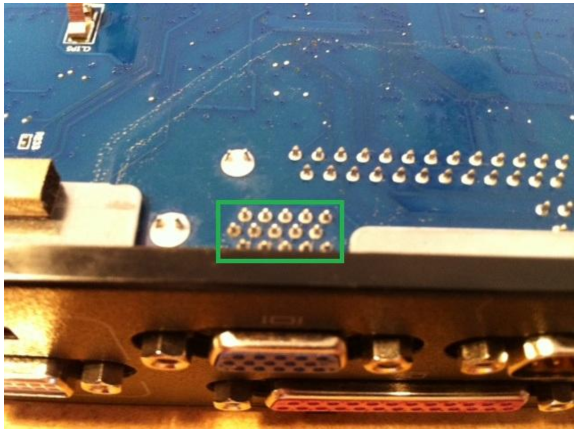
VideoGhost VGA video monitor:

Red circle - USB connector, used to retrieve screenshots via a mass-storage device

Green circle - VGA socket into which a display would be connected

White circle - VGA plug, which connects to the VGA socket on a PC

Passive video monitoring – where to tap



At first glance this seems straightforward

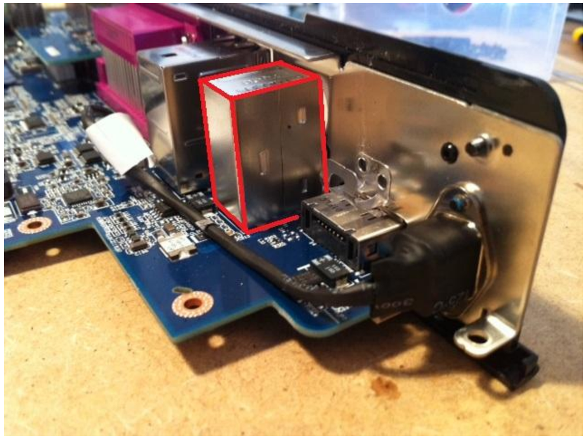
Hmm... Maybe not quite so straightforward ☹

VGA (yellow arrow), Serial port (green arrow)

USB / PS/2 keyboard monitoring

- Hardware key-loggers have been around for many years
- PS/2 sometimes used for security reasons
- Tap would be easier if PS/2 keyboards were used by target
- USB tap would require prior knowledge of which port is used for the keyboard

PS/2 keyboard monitoring – where to tap



Dual PS/2 module

Pins easily accessible

USB / PS/2 keystroke insertion

- USB HID emulation easily achievable with an Arduino microcontroller
- PS/2 emulation also possible with a microcontroller

Advantage: Would enable command execution on a docked, unlocked laptop

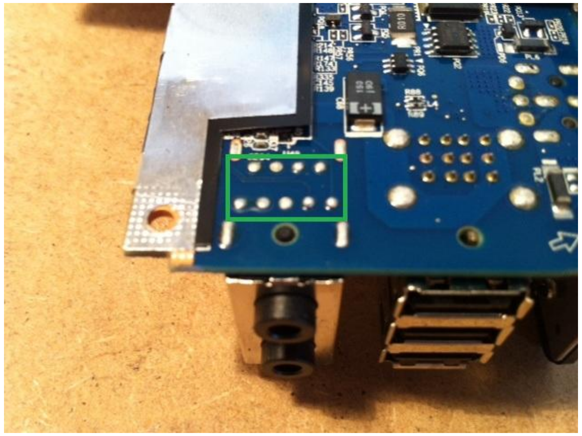
Disadvantage: Highly likely to result in suspicious laptop behaviour being reported

Audio monitoring

- Sensitive corporate presentations may be delivered via streamed media
- More and more corporates are using VoIP with softphones
- Even with string network encryption - audio socket it’s just plain analogue audio
- Assuming that the audio mini-jack sockets are being used rather than USB

Audio monitoring – where to tap

Headphones / microphone module – just analogue audio signals

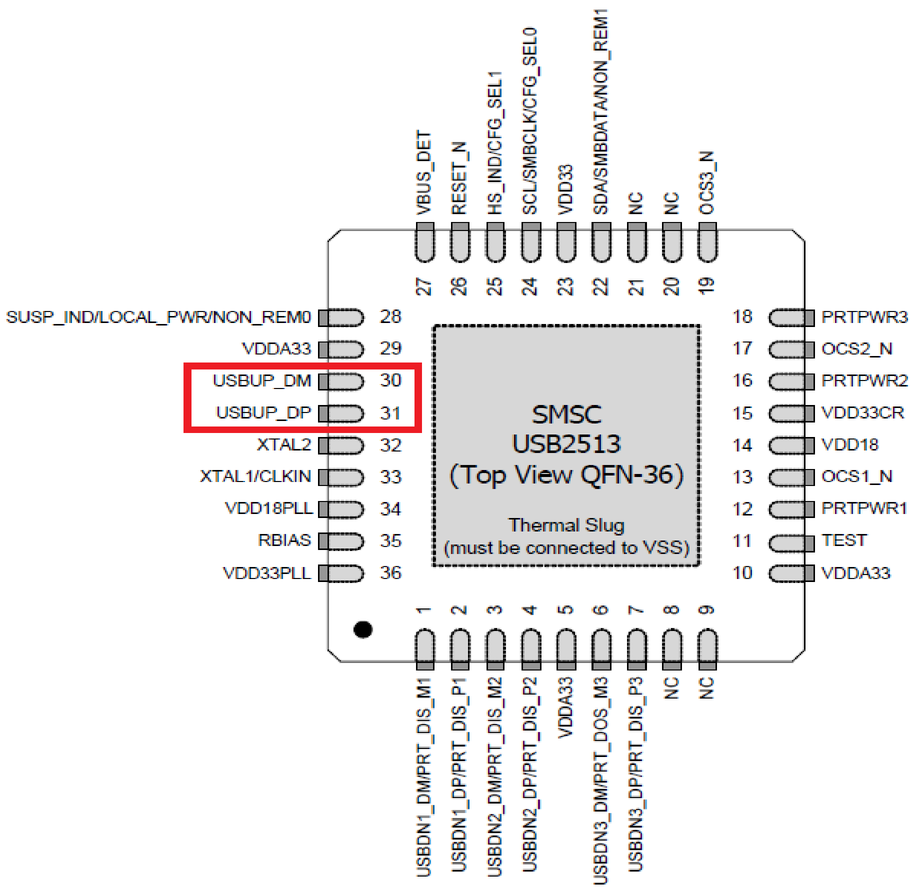


Pins are easily accessible

Webcam monitoring

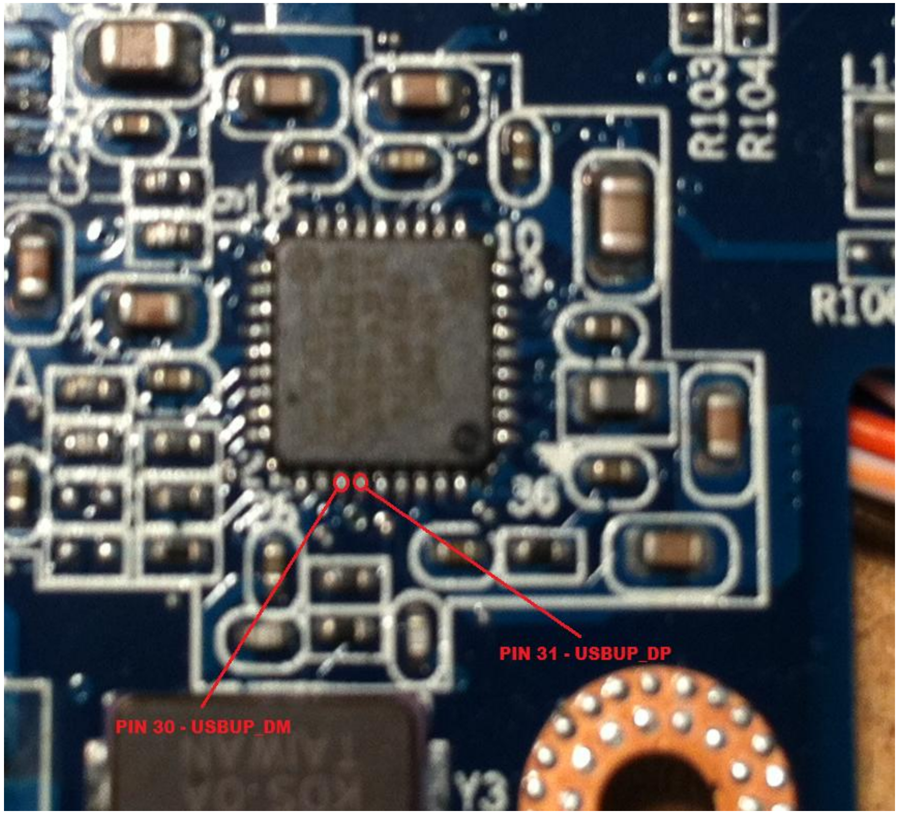
- Many modern laptops have inbuilt webcams
- If we can tap the upstream USB bus we can capture the traffic
- If the data encoding can be reverse-engineered then the video can be recovered
- Useful to see if there’s anyone in the office during lunch break
- Video-conference sessions could be monitored

Webcam monitoring – where to tap



Two inputs for the upstream USB hub connection on pins 30 and 31

Webcam monitoring – where to tap



Pins 30 and 31 are easily accessible on the PCB

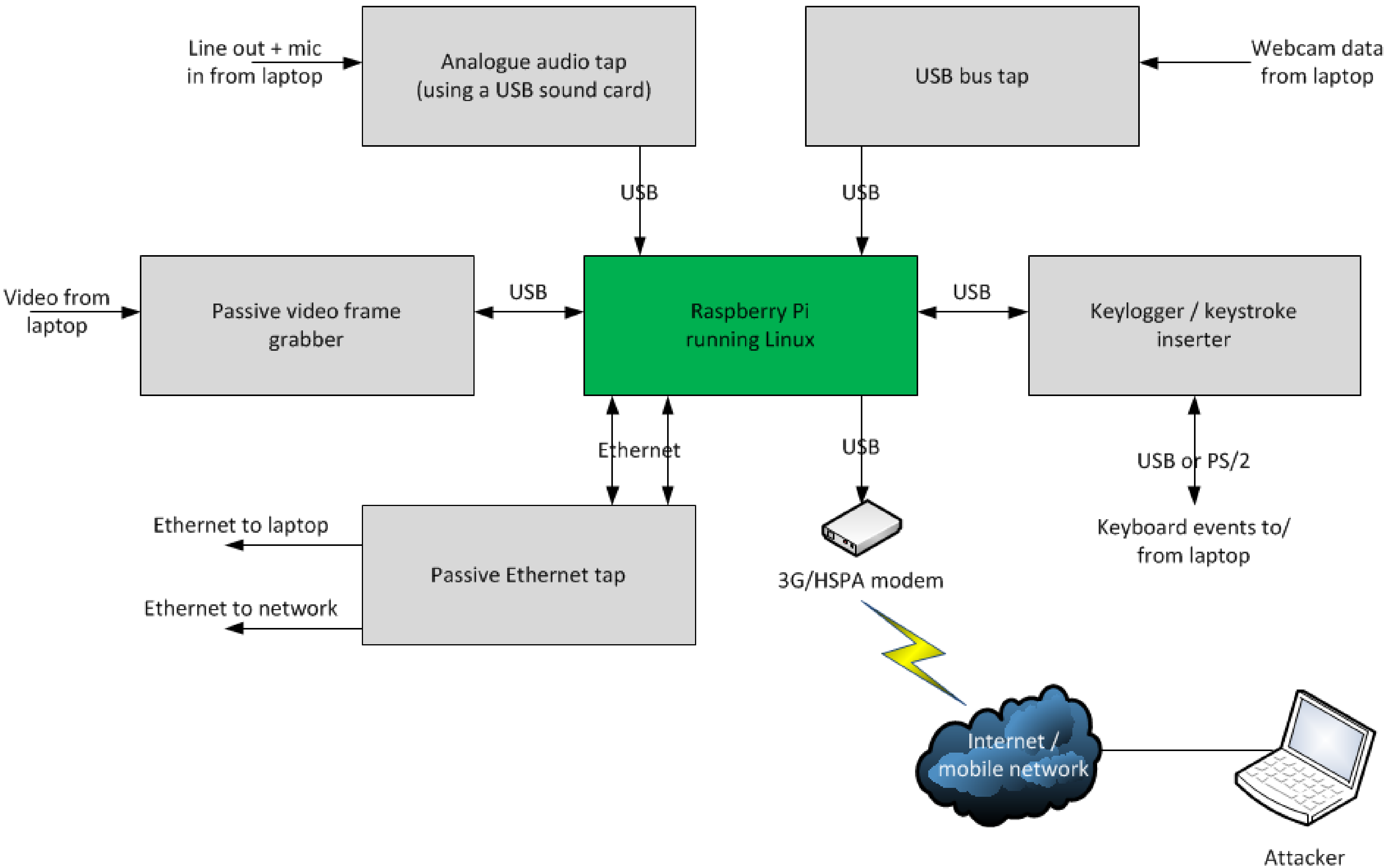
Going deeper – the dock connector

- 144 pin proprietary connector
- No public information about the E-Series connector, but there is for C-Series:
  - Various voltages
  - Microphone, speaker and line out
  - USB connectivity
  - Video (VGA)
  - RS-232 serial
  - System address bus
  - SMBus
  - I^2C Bus

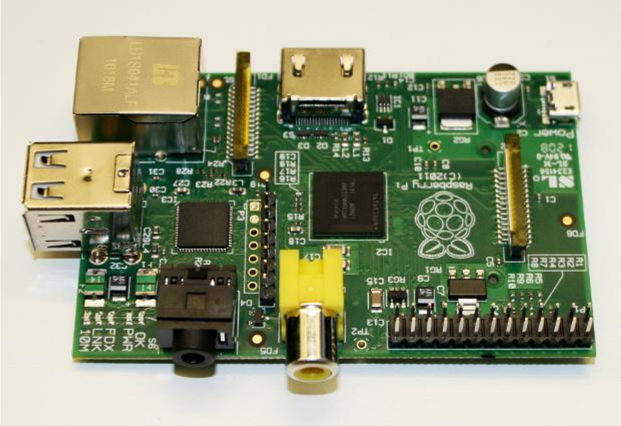
Control Platform - requirements

- Small enough to fit inside the dock
- Configurable enough to handle many different input interfaces
- Powerful enough to process the intercepted data
- Remotely controllable via an our-of-band communications path

Spy-Pi Control platform overview



The Raspberry Pi Model B computer



- Measures 86mm x 56mm x 21mm
- Weighs only 45g
- Based on an ARM 11 processor
- Runs Linux

Other devices required

USB Ethernet adapter: The Pi only has one Ethernet port – we need two

USB sound card: The Raspberry Pi does not have an analogue audio input

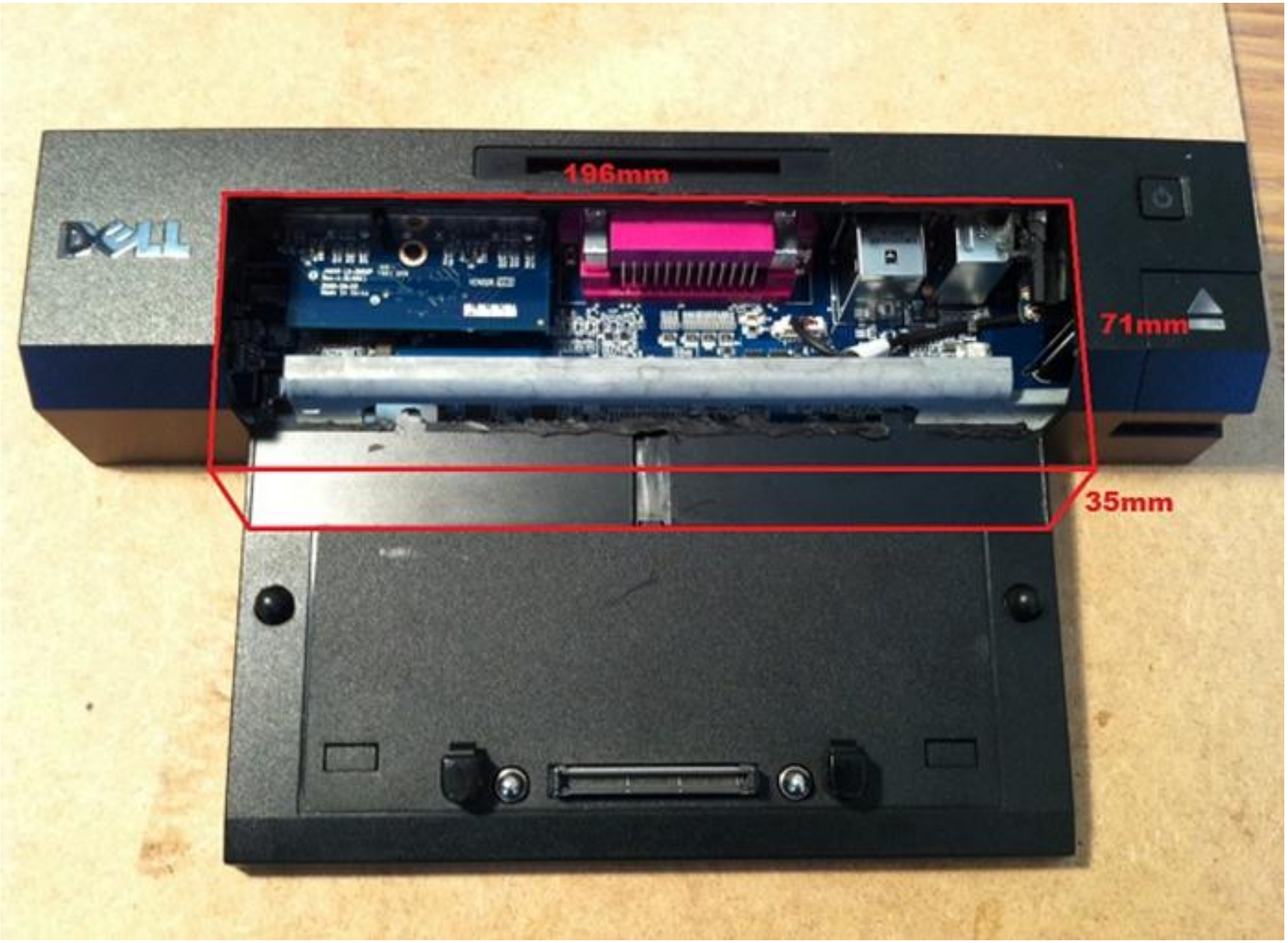
Remote connectivity

- out-of-band connectivity to the device will be via a 3G/HSPA modem

- Two main design choices:
  - “Store and forward”
  - “Remotely initiated full control”

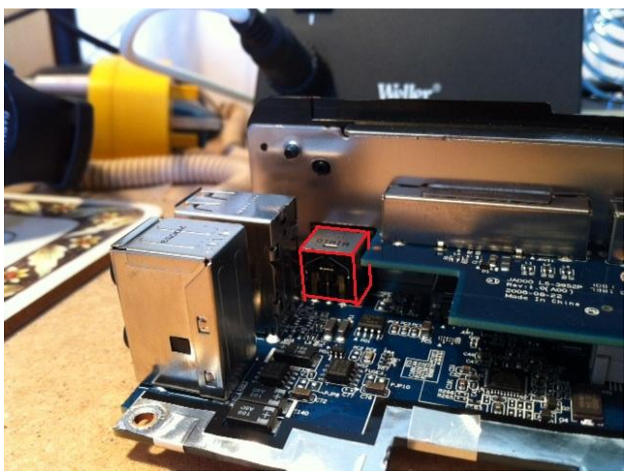
Physical space available

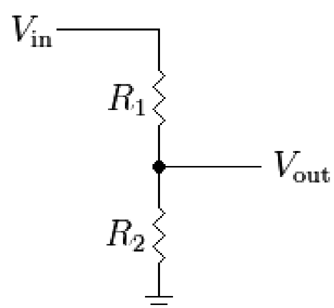
nccgroup
freedom from doubt



Power considerations

- Permanently connected to a power source – power should not be a problem.
- The DC voltage provided by the power supply is +19.5V. We need +5V
- Easiest approach is to tap directly off the DC power input





We can use a simple voltage divider to provide our +5V

$$V_{out} = \frac{R_2}{R_1 + R_2} \cdot V_{in}$$

Putting it all together #1

Putting it all together #2

Putting it all together #3

nccgroup
freedom from doubt

Detecting hardware implants

Passive network tapping: Ethernet speed downgrade on Gigabit Ethernet

Active network attack: A new MAC address will appear on the network

Keystroke insertion: Easily visually spotted

Other detection techniques - weight

Weigh a new "known-good" docking station for later comparison

Advantages:

- Simple technique
- No specialised equipment required

Disadvantages:

- Labour-intensive to periodically weigh all your docking stations
- Weight could be removed to offset the implant by modifying the internal design of the docking station

Other detection techniques - heat

The infra-red heat signature should highlight additional electronics

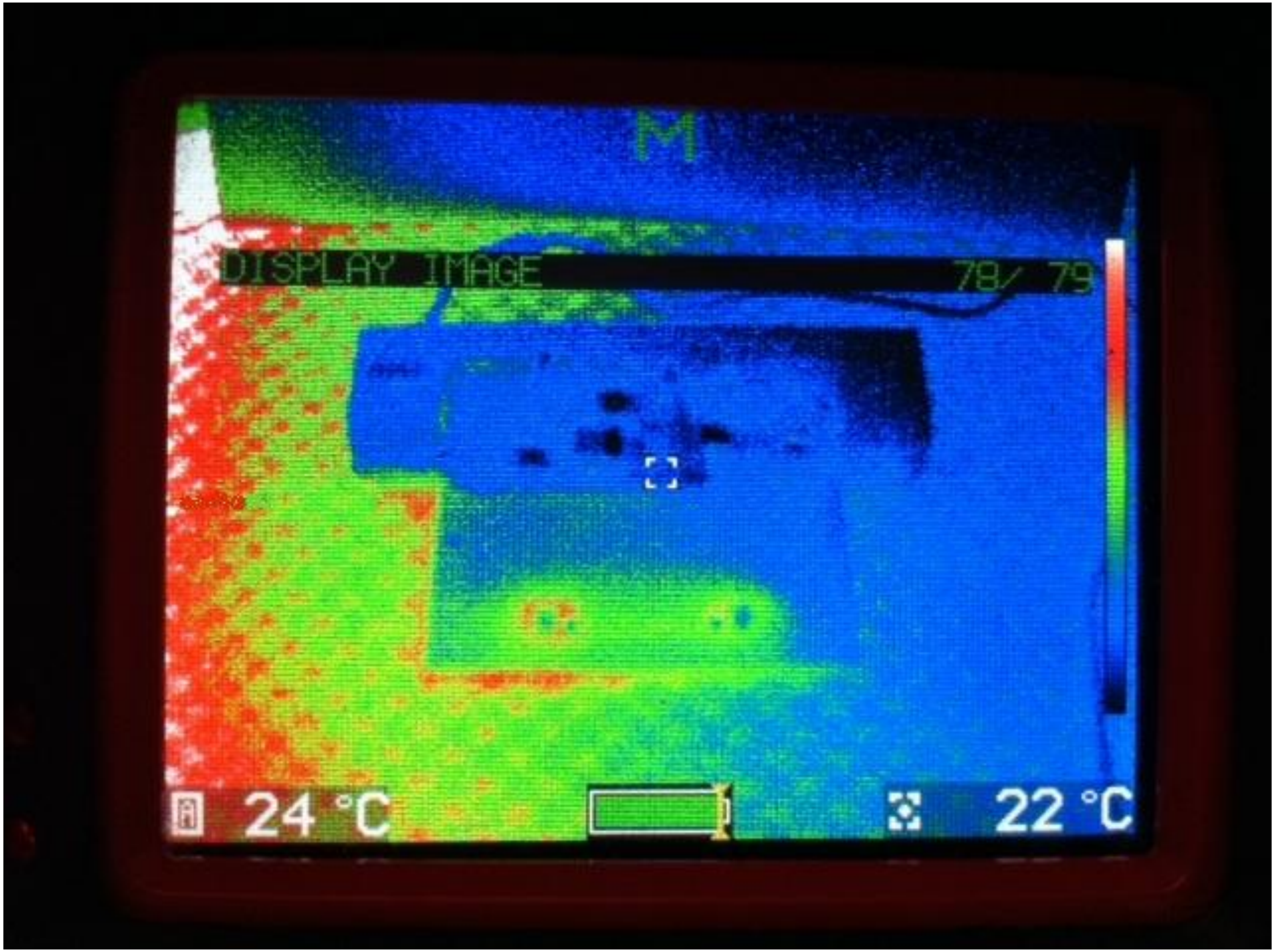
Advantages:

- Simple technique
- Thermal imaging cameras are easy to use with some basic training

Disadvantages:

- Labour-intensive to periodically check all your docking stations
- Thermal shielding techniques could be employed to hide the implant

Implant powered off



Implant powered on

Thermal imaging camera

Thanks to Mike Tarbard of e2v.com for lending me this Argus thermal imaging camera:

P7130 Series
Argus®4-HR320
Thermal Imaging Camera

http://tinyurl.com/thermal-imaging-camera

Other detection techniques – RF emanations

The RF emanations from the 3G/HSPA modem could be detected

Advantages:

- RF emanations must be present so that the implant can be remotely controlled

Disadvantages:

- Specialist equipment would potentially be required
- Differentiating between the implant and employees mobile devices would be difficult

Other detection techniques – current consumed

The additional electronics in an implant require more current

Advantages:

- More current will definitely be consumed when an implant is in place
- Easy to measure using a current clamp or inline device

Disadvantages:

- Accurately measuring the current consumption of each dock would be very labour-intensive
- There may be variations in the baseline current drawn by a dock

Attack mitigation

Preventing implants from working or from being installed in the first place

- Active network connection
  - Only allow one MAC address per switch port
- Passive Network sniffing
  - Ensure all sensitive network traffic is suitably encrypted
- Physical security
  - Physically secure all docking stations
  - Anti-tamper seals
- RF shielding
  - Prevent the implant from communicating

Future research

- Investigate what could be achieved via the dock connector
- Look at some other docking stations to identify different capabilities
- Survey corporates to discover if they have encountered any dock “incidents”

Conclusions

- Laptop docking stations are widely used and trusted devices, which provide extensive access to potentially sensitive data
- Attackers have historically targeted hardware for attack e.g. key-loggers / video-loggers - docking stations are the next logical step
- There are a number of potential techniques for detecting hardware implants
- By far the easiest approach is physical security – locks and anti-tamper stickers

Questions?

Andy Davis, Research Director NCC Group

andy.davis ‘at’ nccgroup.com