An NCC Group Publication

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

Prepared by:
Andy Davis
Research Director
andy.davis ‘at’ nccgroup.com

Contents

1 List of Figures and Tables

2 Introduction

Laptop docking stations are widely used in organisations, often in hot-desking environments. They provide a neat connectivity solution for workers who are semi-mobile and therefore use laptops rather than desktop PCs. However, laptop docks are an attractive target for an attacker. They have access to the network, to all the ports on a laptop, often some that aren't and they are permanently connected to a power supply. But most importantly, they are considered to be trusted, "dumb" devices – the perception is that they just connect all the ports on your laptop to the ports in the dock. The IT department is typically more concerned about someone stealing your laptop, so they'll ask you to secure your laptop with a Kensington-style lock[1] , but not necessarily to secure the dock. This paper details how attackers can exploit the privileged position that laptop docking stations have within an environment. It will also describe the construction of a remotely controllable, covert hardware implant, but most importantly it will discuss some of the techniques that can be employed to detect such devices and mitigate the risks that they pose.

Docking stations e.g. the Dell E-Port Plus[2] (PR02X – Figure 1) are familiar devices in a variety of organisations.

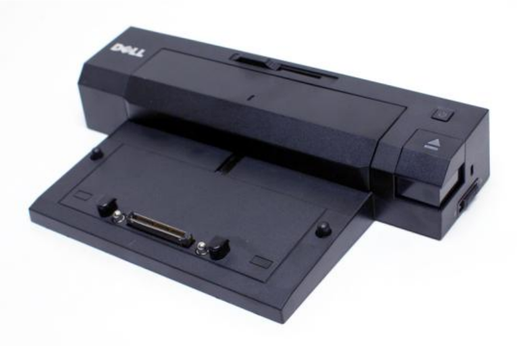


Figure 1: Dell PR02X dock

They enable users to connect their laptops to monitors, keyboard, mouse, network etc. without the need to plug and unplug lots of cables every morning and evening. Some literally just "extend" the ports available on the laptop, whilst others include additional ports, which are not available on the connected laptop e.g. the PR02X has dual DVI and DisplayPort outputs for connecting two monitors, whereas the laptop that connects to the dock may just have a single DisplayPort output e.g. Dell Latitude E6510. This research focused on the Dell PR02X primarily because it was the dock that the author is familiar with using, but also because it has a useful property from an implant perspective – plenty of internal space for additional electronics.

2.1 How realistic is the threat?

In 2005 criminals attempted to steal an estimated £229m from the Sumitomo Mitsui Bank[3] in the City of London. They used hardware-based key-loggers[4] to perform their attack. This example is probably the most high profile hardware-based attack in recent years, but based on the ease with which these attacks can often be mounted Sumitomo Mitsui is unlikely to an isolated incident. As the price of miniaturised PCs and associated interface technology continues to fall, a hardware-based implant can be developed for only a few hundred pounds by an attacker with a moderate skillset.

2.2 Previous Research

The author is not aware of any public research which investigates inserting hardware-based implants into laptop docking stations. Although covert hardware implants have been demonstrated previously by companies such as Pwnie Express[5].

3 How does a docking station work?

Essentially, the main function of a docking station is to extend the ports available on a laptop, via a proprietary connector, which is usually on the laptop's base to the rear of the docking station. There are specific integrated circuits within the device that help to provide this functionality, such as an I/O Controller and if additional ports such as DisplayPort or HDMI are present then further integrated circuits such as DisplayPort 1:2 Switches are also included.

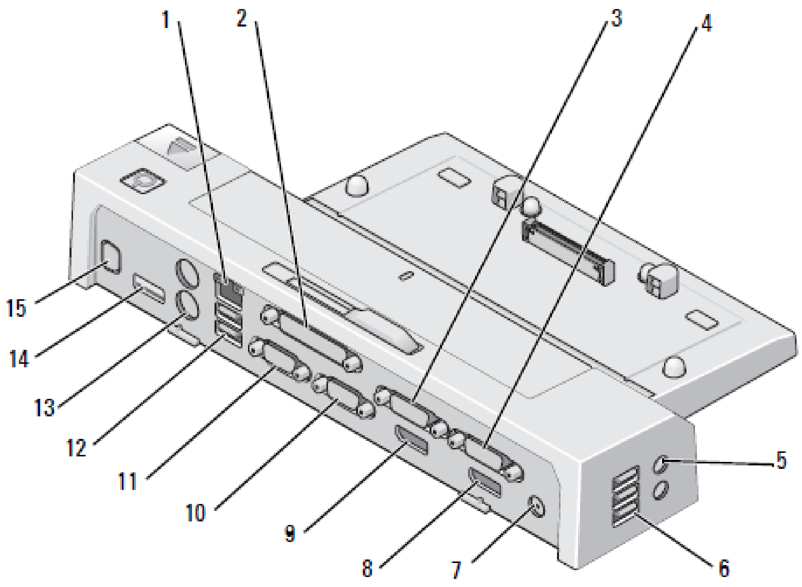
Further details about the PR02X include:

- The device has a passive Ethernet switch, which essentially means that the port on the rear of the laptop is disabled when the laptop is connected to the docking station.
- There is an internal USB hub that provides connectivity to five USB ports on the docking station in addition to those on the laptop.

If headphones or a microphone are connected to the laptop then any connected to the dock will not work as expected. Audio is present (verified using an oscilloscope), it's just at an extremely low level and is therefore, potentially recoverable with suitable amplification.

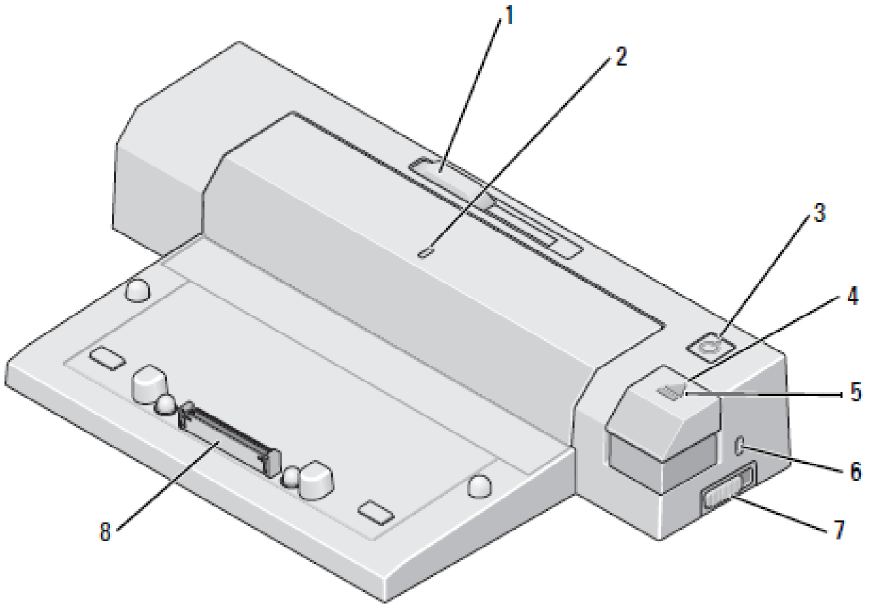
3.1 Dell PR02X Teardown

Figures 2 and 3 show all the available connectors on the PR02X docking station:



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		

Figure 2: Dell PR02X dock rear - Dell™ E-Port Plus User's Guide ©Dell 2008



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

Figure 3: Dell PR02X dock front - Dell™ E-Port Plus User's Guide ©Dell 2008

There are two proprietary connectors - the "E-Monitor stand connector", which looks like a slightly miniaturised 9-pin D-type socket and the "docking connector", which has 144 pins. As the functionality of the E-Monitor stand is extremely basic, the primary purpose of this connector appears to be the transmission of DC power.

The author has not managed to locate any freely available public available documentation about the PR02X internals or pin-outs of the proprietary connectors and therefore, in order to understand how it works, the first step is to disassemble to facilitate analysis.

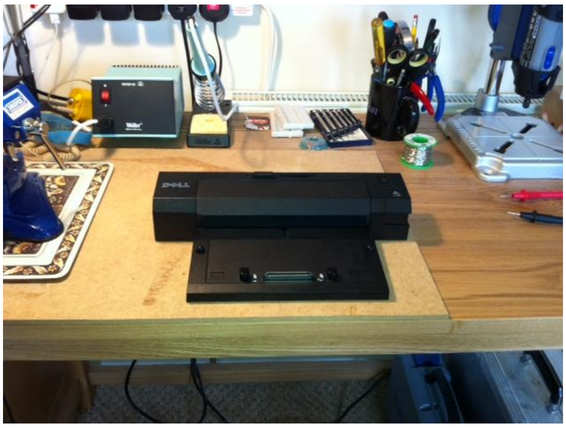


Figure 4: Dock teardown #1

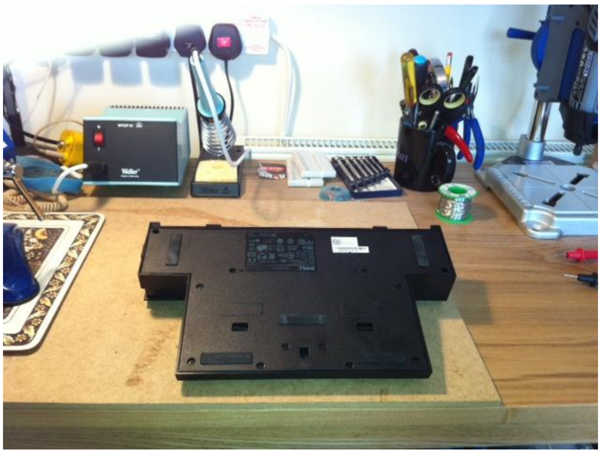


Figure 5: Dock teardown #2

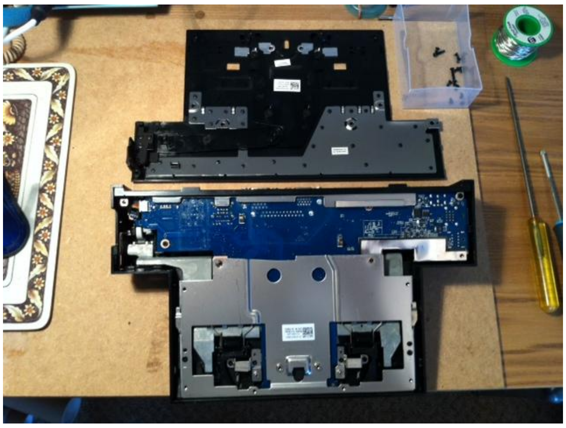


Figure 6: Dock teardown #3

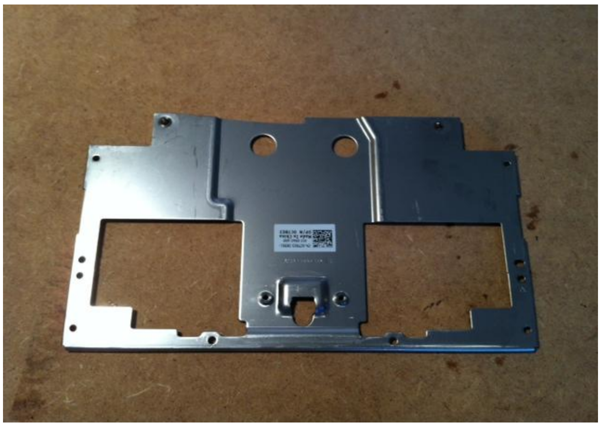


Figure 7: Dock teardown #4

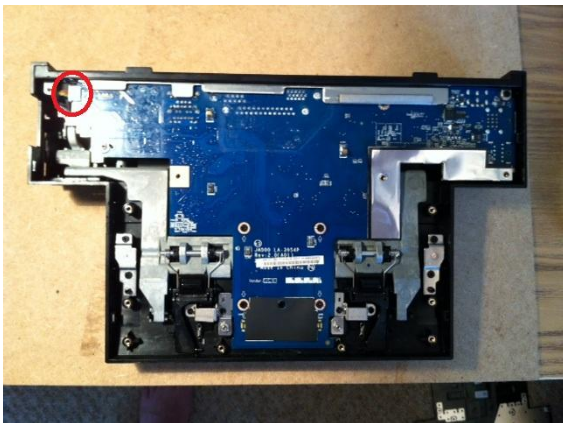


Figure 8: Dock teardown #5

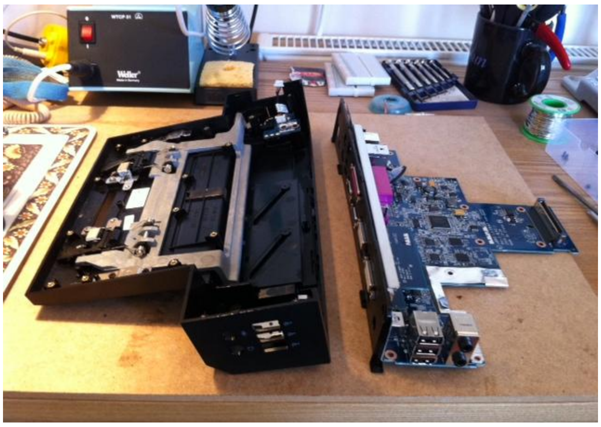


Figure 9: Dock teardown #6

Dock Teardown:

1. Front of the device
2. Back of the device
3. Remove all visible cross-head screws on the base and rear. Then using a flat-blade screwdriver prise open the base carefully all the way around - the base will then just lift off
4. Remove the two cross-head screws holding the metal plate to the PCB then remove the plate
5. Remove the power connector (circled in red) and the six cross-head screws that secure the PCB to the enclosure
6. Very carefully prise the PCB upwards until it releases

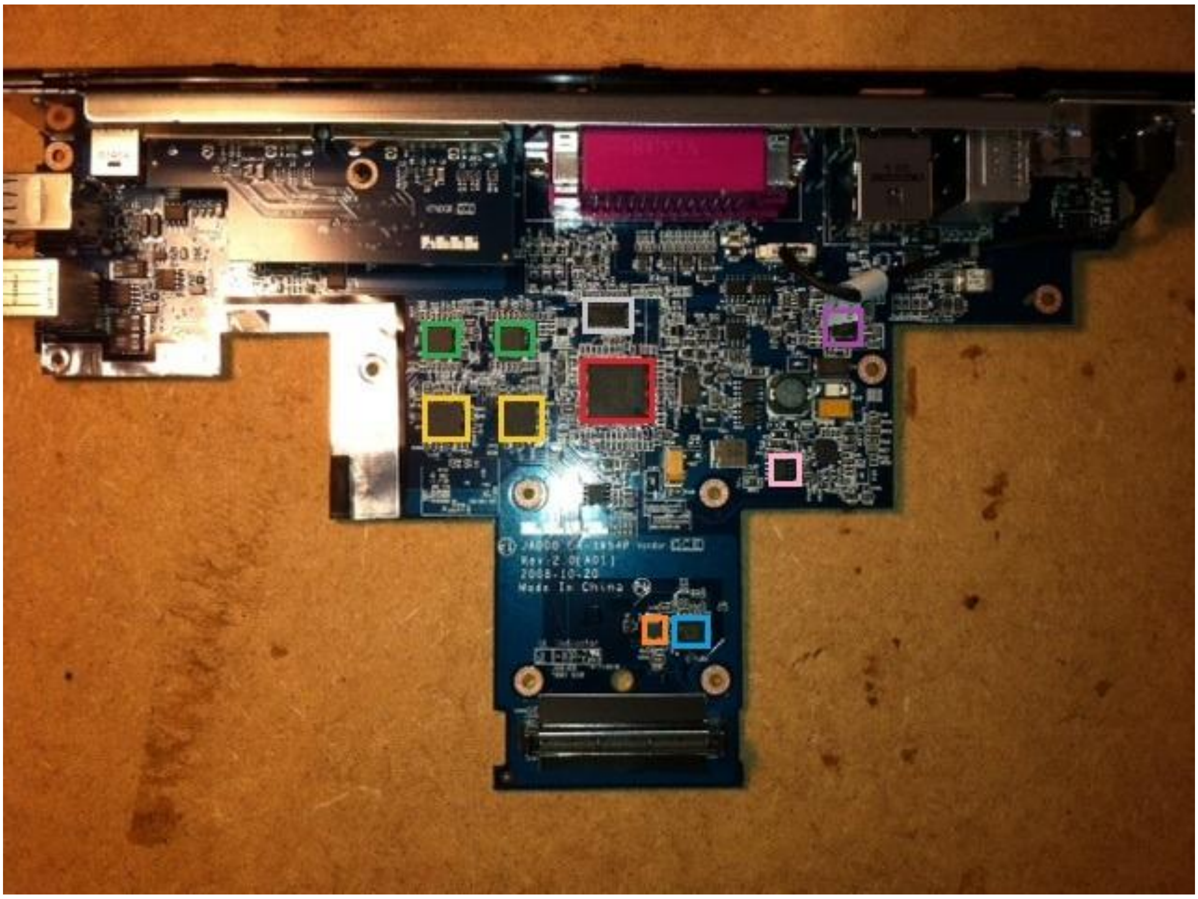


Figure 10: The main dock PCB

The primary integrated circuits are highlighted in the picture above; they are:

- Red - SMSC LPC47N237[6] - 3.3V I/O Controller for Port Replicators and Docking Stations
- Yellow - SN75DP122A[7] - DisplayPort 1:2 Switch with Integrated TMDS Translator
- Green - PS8121ED[8] - Dual Mode DisplayPort Repeater
- Blue - PI2EQX3211CM[9] - 3.2Gbps 2-channel SATAi/m ReDriver
- Orange - APL1117[10] - Fast Response Positive Adjustable Regulator
- Pink - MAX877[11] - 5V/3.3V/3V/Adjustable-Output, Step-Up/Step-Down DC-DC Converter
- Purple - USB2513[12] - USB 2.0 High-Speed 3-Port Hub Controller
- Grey - MP243EC[13] - 3-V TO 5.5-V Multichannel RS-232 Line Driver/Receiver

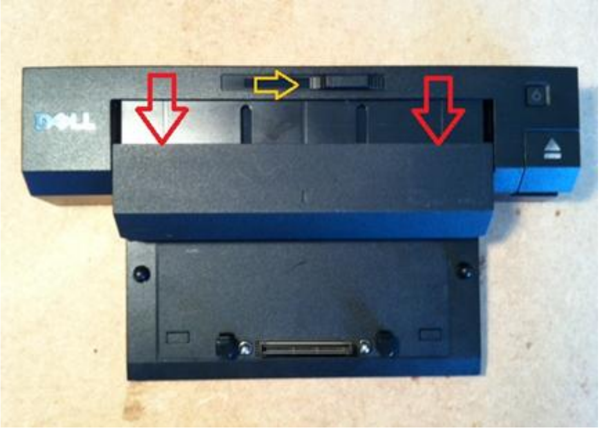


Figure 11: Battery extender

In Figure 11 we can see that by moving the slider to the right (yellow arrow), the cover expands downwards (red arrows). This is the default position for most laptops, as the cover is only moved to the retracted position when an extra-large battery is fitted and protrudes from the rear of the laptop. In this extended position, the space inside for additional electronics more than doubles.

4 Useful properties of laptop docking stations for an attacker

Docking stations are an attractive target to attackers for a number of reasons:

- As a result of their primary function, access can easily be gained to all the ports available on the connected laptop and often several that aren't on the laptop
- They are often used in "hot-desking" environments and therefore, one implant can potentially target a different laptop each day
- They are permanently connected to a power supply and to the network
- They are generally considered to be "dumb" devices and are therefore, trusted by users and IT administrators
- They are passive and anonymous and therefore, can easily be replaced with another identical looking docking station that contains a hardware implant
- There is often enough space inside the case for additional hardware
- Any data that is encrypted as it traverses the network will be decrypted at the laptop and therefore, sensitive audio or video can be captured *after* it has been decrypted or before it is encrypted if the data originates from the laptop

5 What would a hardware implant do?

There are a number of attacks that could be performed from a docking station; these are each described in this section, but at a high level the requirements for a hardware implant in this scenario are as follows:

- 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

5.1 Network tapping

The most obvious attack is passive network sniffing. The circuit shown in Figure 12 (designed by Michael Ossmann[14]) shows how this can be achieved (note that there are two tap points one for traffic flowing in each direction). The obvious benefit of this approach is stealth, as the monitoring implant will not be visible as a network-connected device:

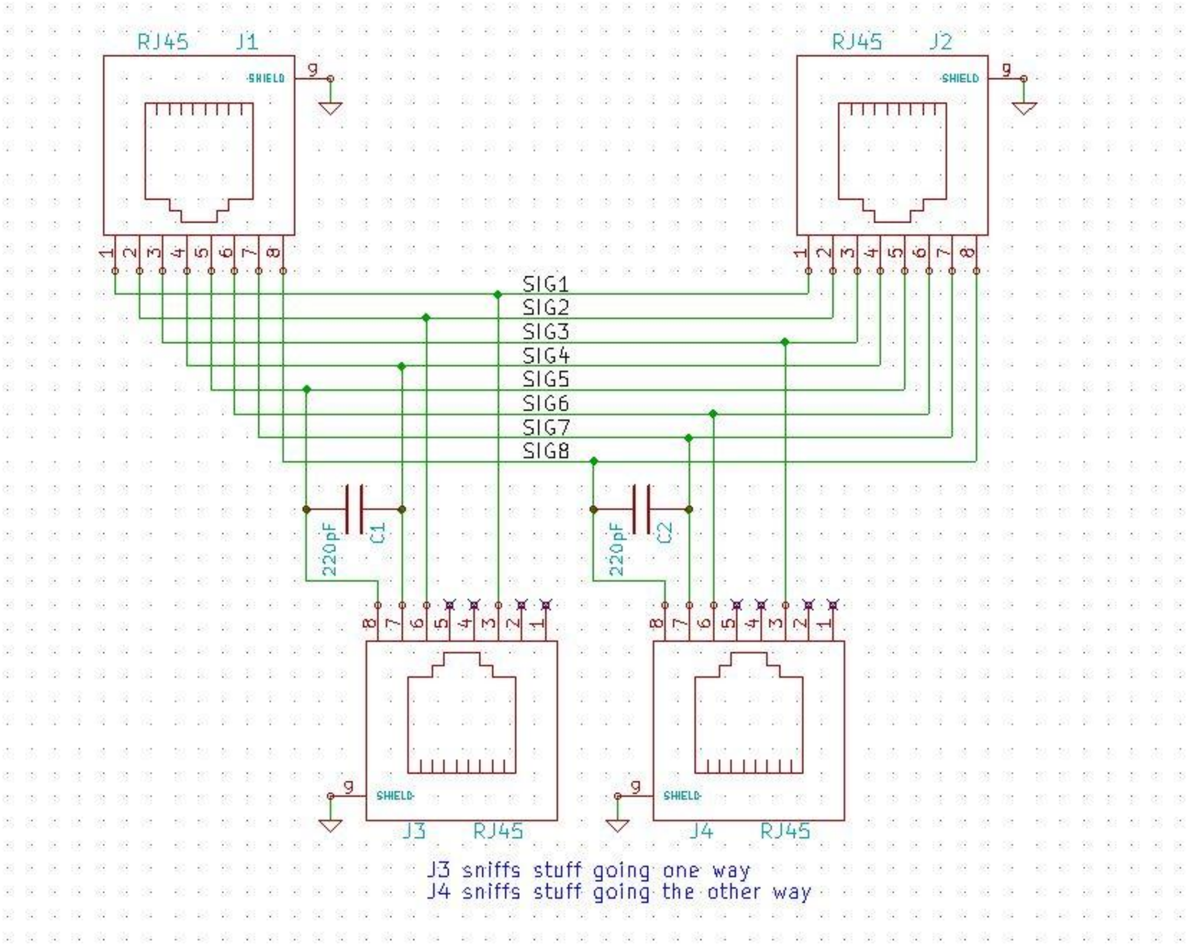


Figure 12: Passive Ethernet tap

One problem with tapping Ethernet is how to handle 1000BASE-T[15] (Gigabit Ethernet). Because 1000BASE-T signals travel in both directions simultaneously on each individual wire, it is not possible to build a passive tap for the technology. To properly tap 1000BASE-T, an active device such as a powered LAN tap[16] or a switch with port mirroring[17] (also known as SPAN) enabled is required. However, instead of making the tap compatible with 1000BASE-T another option is to force it to downgrade. Since 1000BASE-T uses two more pairs of conductors than 10 or 100 Mbps Ethernet, each of those extra pairs can be bypassed with a 220pF capacitor. This filters out the high frequency signals of 1000BASE-T, forcing the target devices to revert to 100BASE-TX[18] which can then be monitored. Clearly, this technique makes the approach slightly less stealthy, as a network administrator monitoring the switch connected to the docking station would be able to see that the Ethernet connection had been downgraded from 1000BASE-T to 100BASE-TX.

Capturing raw network traffic could clearly result in extremely large capture files and therefore, filtering would be required to only capture “interesting” data.

5.1.1 Where to tap

So where does the tap need to connect to Ethernet on the docking station PCB? The PR02X has a combined Ethernet / 2 x USB module, as shown in Figure 13.

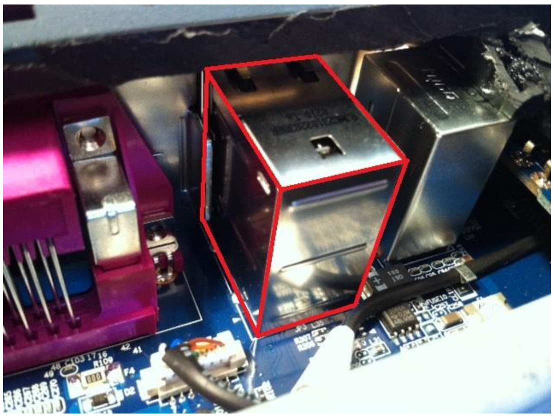


Figure 13: Combined Ethernet / 2 x USB module

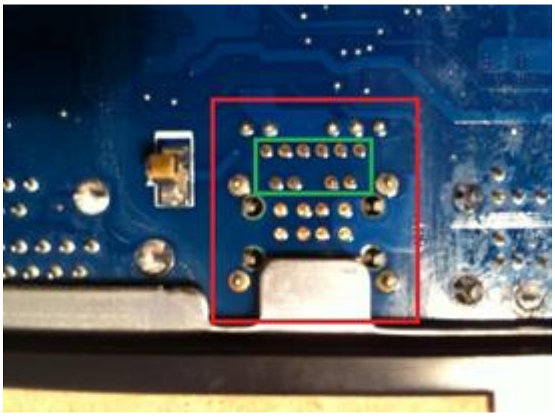


Figure 14: The module pins on the PCB

The underside of the PCB reveals the pins (Figure 14). Printed on the module is "RJMG231022830ER" - this is the part number from the RJMG2310[19] series modules produced by Amphenol Corporation[20] in Taiwan. The datasheet reveals that the pins we need to tap are those enclosed by the green box (Figures 15 and 16).

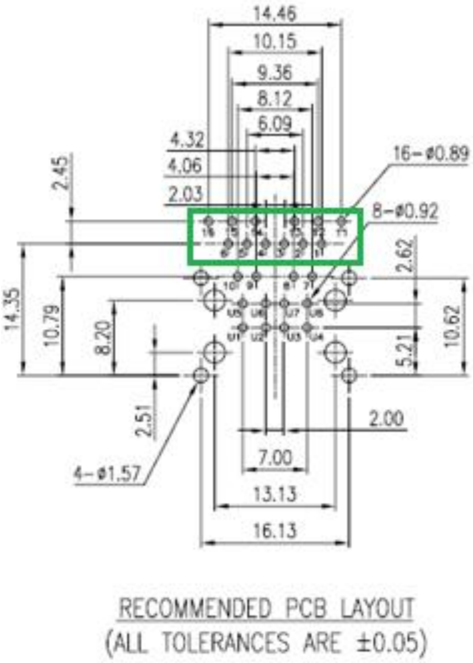
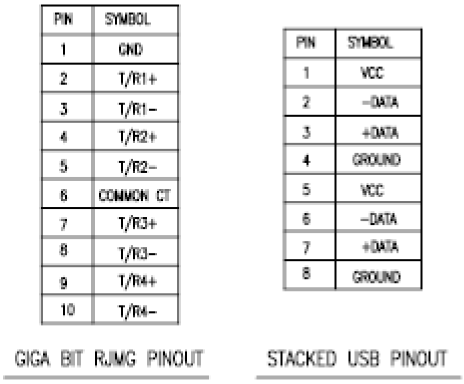


Figure 15: Ethernet pin locations



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

Figure 16: Module pin-outs

The connected Ethernet tap is shown in Figure 17 and the two Cat 5 Ethernet connectors on the other end of the tap are shown in Figure 18. Note the presence of the two capacitors (red circles) to perform the hardware-based downgrade attack from 1000BASE-T to 100BASE-TX.

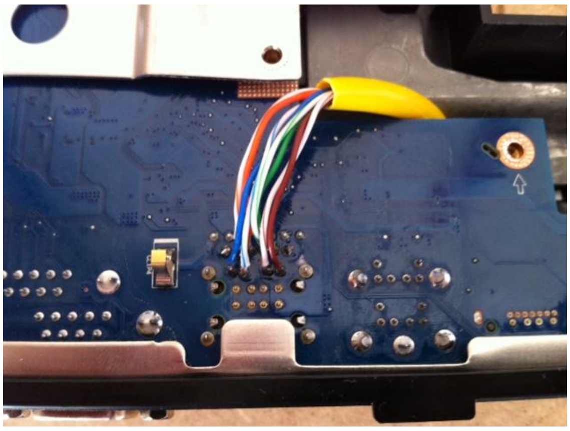


Figure 17: Connected Ethernet tap

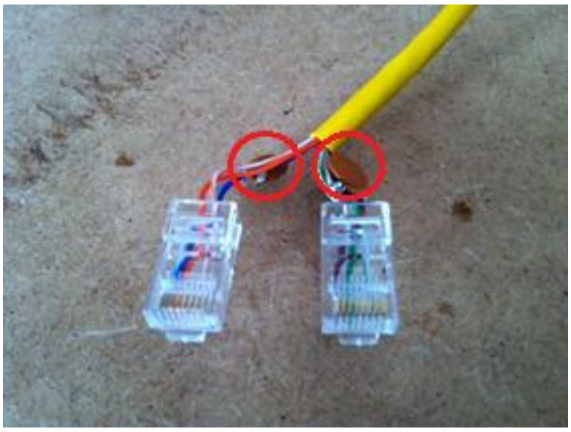


Figure 18: Cat 5 Ethernet connectors on the tap

5.2 Active network attack

More aggressive and hence more detectable is active network attack. Instead of using a passive network tap, a hub would be used to connect the attack platform directly to the target network. This would obviously then allow for network-based attacks to be remotely performed against the target network from the implant.

From an implant perspective, the hardware modification required would be more complex, as a hub would need to be inserted between the current Ethernet connections on the docking station PCB and the RJ-45 Ethernet socket so that it was situated between the docked laptop and the Ethernet cable connected to the rear of the docking station.

5.3 Passive video monitoring

The attacker may wish to see what is being displayed on the target's monitor, as sensitive information could be obtained. This could be performed using a Video Frame Grabber like VideoGhost[21]. Figure 19 shows the different connectors on the VideoGhost:

- 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

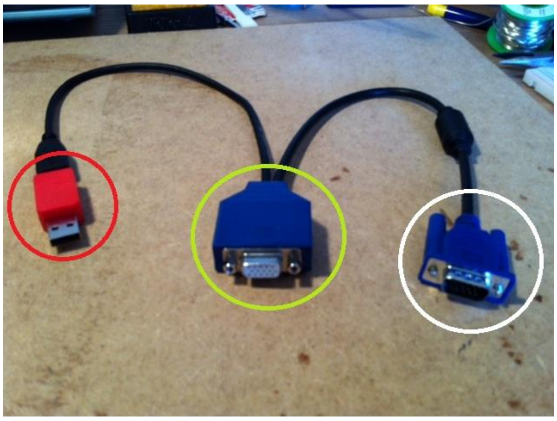


Figure 19: VideoGhost VGA frame grabber

5.3.1 Where to tap

The pins associated with the VGA port are easily available (Figure 20); however, the VideoGhost needs to be connected inline between the PCB and the VGA connector. Therefore, the connector would need to be de-soldered and replaced with a non-PCB-mount VGA connector, and then the appropriate connections could be made to the VideoGhost and to the PCB.

Under normal circumstances, this would be annoying but not a major problem, however, Figure 21 shows that the VGA connector (indicated by the yellow arrow) is hidden away in a kind of cage formed by the wires associated with the parallel port connector (the pink block at the top). This is a multi-port module that contains the parallel port, VGA port and also a serial port (indicated by the green arrow). This configuration means that in order to insert the VideoGhost we'd need to first de-solder the parallel port, VGA port and serial port connections so that the entire module could be removed to perform the tap. Also, as all three connectors are part of the same module, they would need to be replaced with individual connectors, as the VGA connector would be replaced for a non-PCB-mount variant.

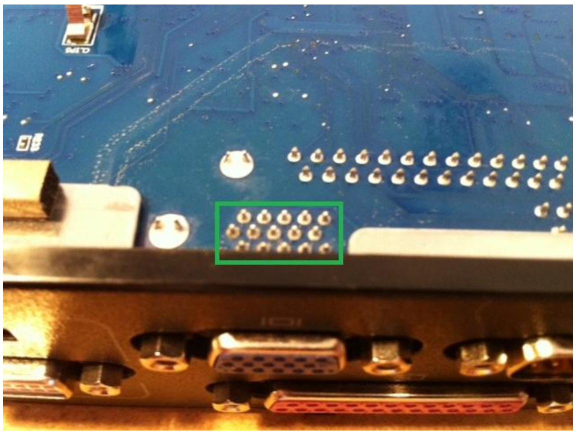


Figure 20: VGA connector pins

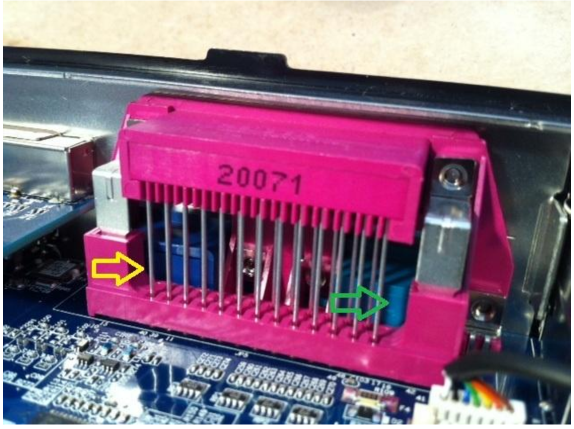


Figure 21: VGA connector hidden behind a cage of pins

5.4 USB / PS/2 keyboard monitoring

Hardware key-loggers have been around for many years now and are clearly useful for obtaining passwords and other sensitive data. This attack could be performed using a hardware-based key-logger like KeyGhost[22]. This tap would be significantly easier to accomplish if the target organisation used PS/2 keyboards (although outdated, some organisations still use them for security reasons and then prevent USB usage with Endpoint Protection Software[23]). The reason it would be easier is that there is only one PS/2 keyboard socket and therefore, that is where the key-logger tap would be inserted. If USB keyboards were used by the target then some kind of prior surveillance would need to be performed to establish if the keyboards were generally connected to the same USB socket in each docking station within the organisation. Tapping every USB socket would be impractical because of the additional electronics required. However, an alternative approach would be to monitor the USB bus rather than just the socket (see Section 5.7 Webcam monitoring).

5.5 Keystroke insertion

Once the attacker has the user's authentication credentials (gathered using a key-logger), as there is a connection to the USB or PS/2 interface, the attacker can then start remotely "typing" on the target's laptop by the emulation of key-presses[24]. Although this could be accomplished via either USB or PS/2, it is probably easier and would certainly be stealthier via the PS/2 interface.

5.5.1 Where to tap

The PS/2 mouse and keyboard connectors are located in a single module from TE Connectivity[25] (formerly Tyco Electronics) as shown in Figures 22 and 23.

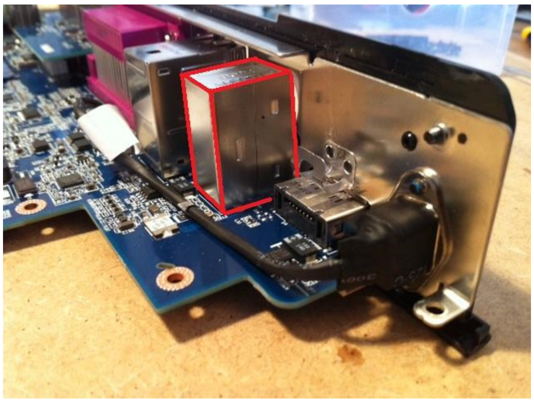


Figure 22: PS/2 dual module

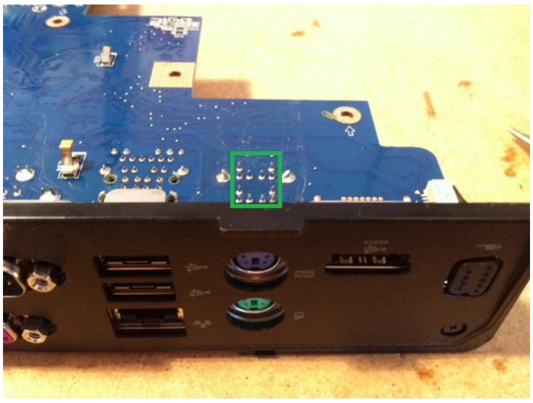


Figure 23: PS/2 module PCB pins

5.6 Audio monitoring

If the target user has a headset with an attached boom microphone (which uses the audio mini-jack sockets) then this audio could easily be recorded, stored and forwarded, in addition to any audio that the user was listening to on their laptop. Even if the strongest encryption algorithm is used to protect the audio data over the network, at the audio socket it's just plain analogue audio.

5.6.1 Where to tap

The microphone and headphone jacks are located in a single module produced by the Taiwanese company Suyin Group[25] . This is shown in Figures 24 and 25.

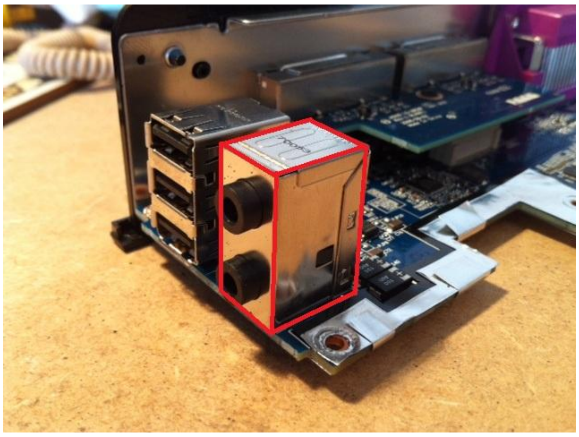


Figure 24: Audio module

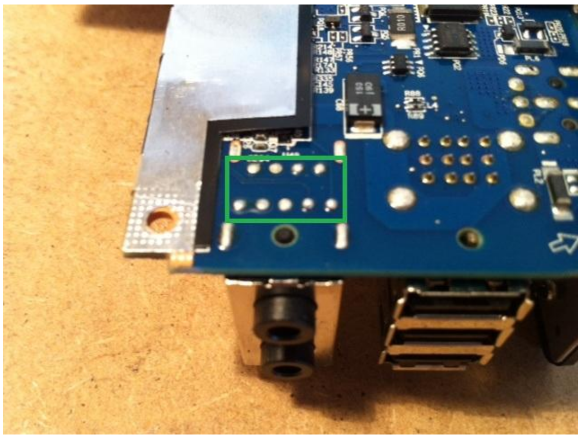


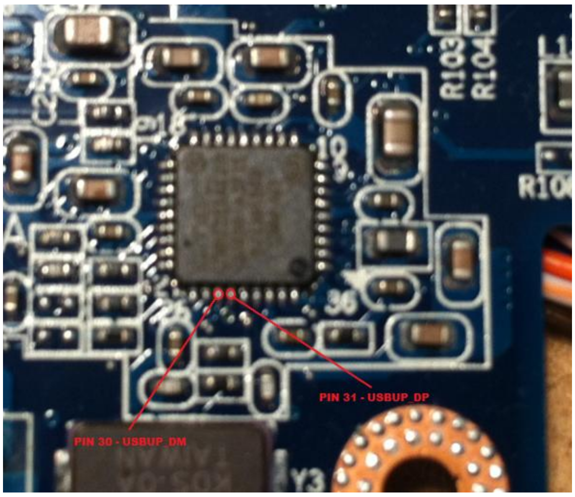
Figure 25: Audio module PCB pins

5.7 Webcam monitoring

Many modern laptops have inbuilt webcams, which are internally connected to the USB bus. The video stream from a webcam could potentially be intercepted if still enabled, stored and forwarded to an attacker. This would be useful if an attacker wanted to know when everyone was out for the office e.g. at lunchtime, if they intended to physically break into an office. Also, sensitive videoconference discussions could be intercepted. In order to access the webcam the USB upstream hub connections need to be tapped rather than the hubs provided by the docking station. These can be accessed on the inputs to the USB hub controller chip.

5.7.1 Where to tap

The USB2513 hub controller chip (which provides a 3-port USB hub) has two inputs for the upstream USB hub connection on pins 30 and 31 (shown in Figure 26).



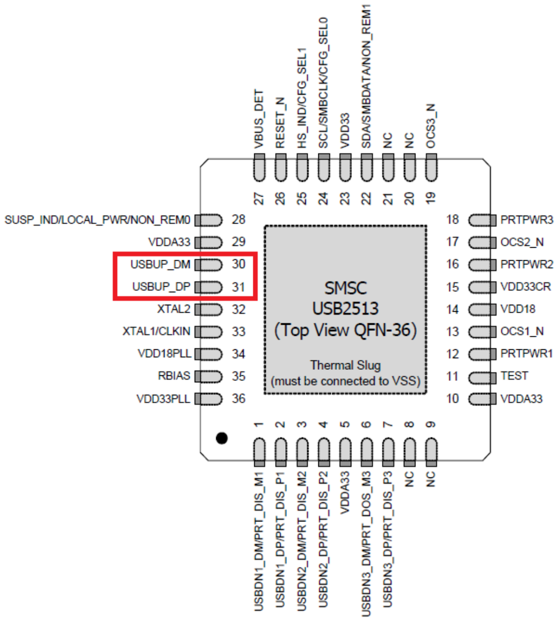


Figure 26: Hub controller chip upstream hub connections

Figure 27: Hub controller chip pin-out in datasheet

These two pins can clearly be seen (Figure 27) as the two USB upstream hub connections in the product data sheet[26].

5.8 Going deeper

The interface between the laptop and the docking station is a 144 pin proprietary connector (Figure 28).

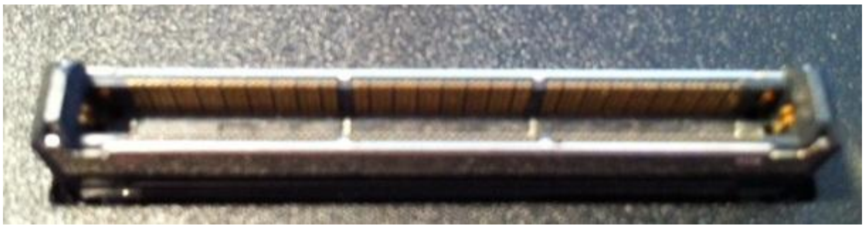


Figure 28: Dell E-series proprietary dock connector

Although, the pin-out for this connector does not appear to be publicly available, pin-outs for similar interfaces are available for another Dell Laptop[27]. This previous reverse engineering output provides an insight into the other technologies that are likely to be available on the connector; these include:

- Various voltages
- Microphone, speaker and line out
- USB connectivity
- RS-232 serial
- System address bus
- SMBus
- I^{2}C Bus

This is an area where further research is required to determine the usefulness of these interfaces.

6 Control Platform

At the heart of the implant there needs to be some kind of control system that takes inputs from each of the taps, processes the data where required and forwards it to the attacker via an out-of-band network. The NCC Group hardware-based control platform is called Spy-Pi. It is implemented using a Raspberry Pi Model B[28] running Linux and connected to a 3G/HSPA modem, as shown in Figure 29.

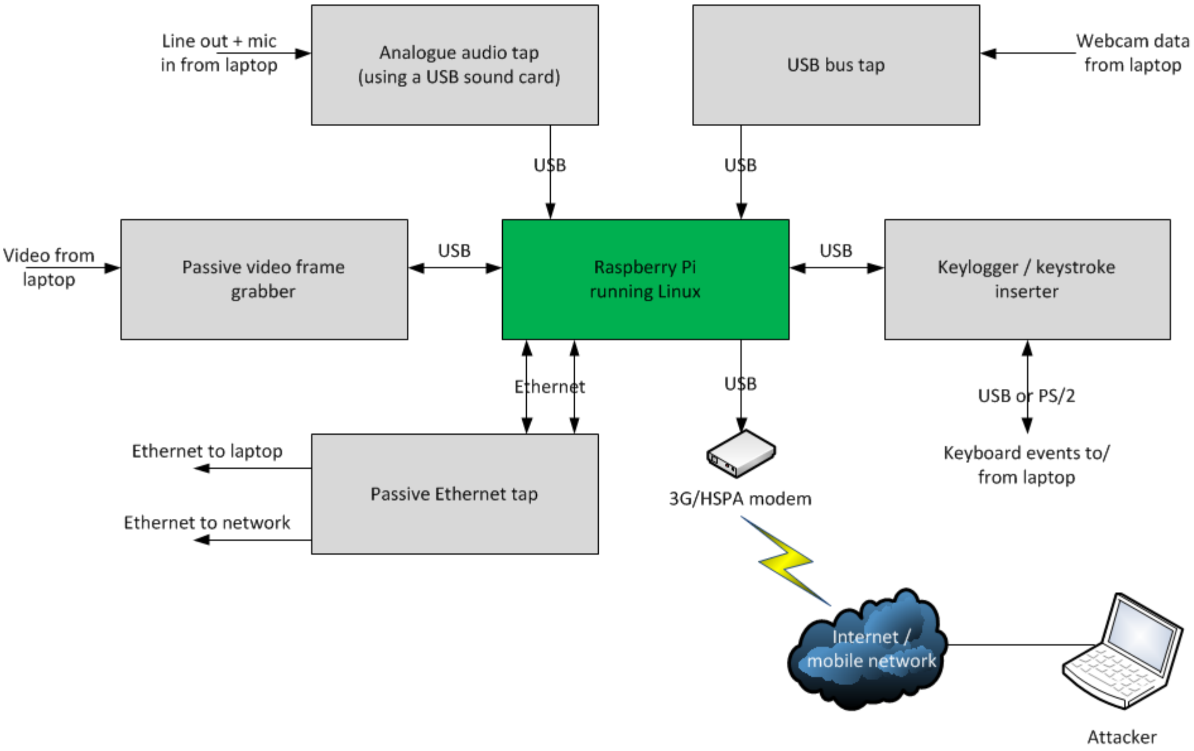

Line out + mic in from laptop
Analogue audio tap (using a USB sound card)
USB bus tap
Webcam data from laptop
USB
USB
Video from laptop
Passive video frame grabber
USB
Raspberry Pi running Linux
USB
Keylogger / keystroke inserter
Ethernet
USB
USB or PS/2
Ethernet to laptop
Passive Ethernet tap
Ethernet to network
3G/HSPA modem
Keyboard events to/ from laptop
Internet / mobile network
Attacker

Figure 29: The Spy-Pi control platform

6.1 Parts list

The control platform consists of a number of off-the-shelf component parts, which in total cost no more than a few hundred pounds.

6.1.1 The Raspberry Pi computer

Introducing the Raspberry Pi Model B computer from the Raspberry Pi Foundation[29] (Figure 30).

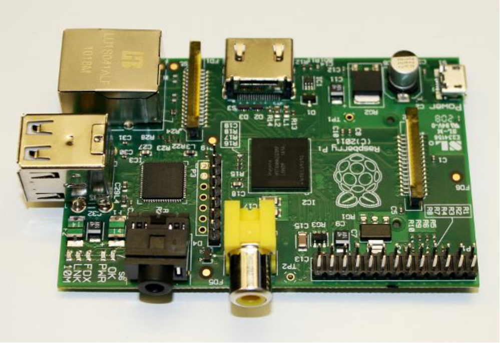


Figure 30: Raspberry Pi Model B

The device measures 86mm x 56mm x 21mm and weighs only 45g. It is based on an ARM 11 processor and runs Linux.

6.1.2 USB sound card and Ethernet adapter

A USB sound card (Figure 31) is required, as the Raspberry Pi doesn't have an analogue audio input.

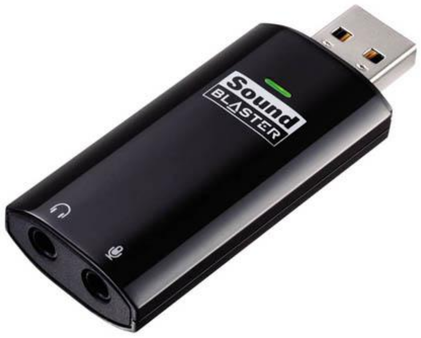


Figure 31: USB sound card

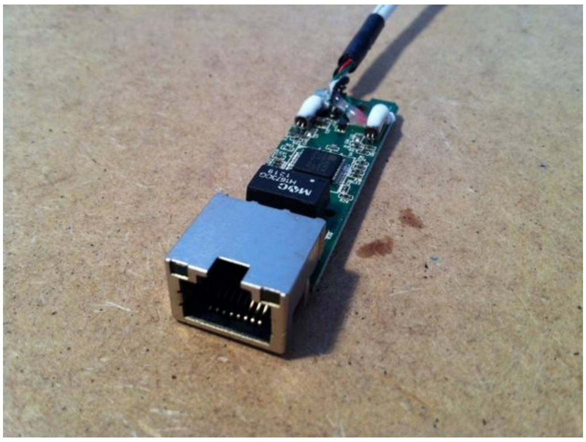


Figure 32: USB Ethernet adapter

Two Ethernet ports are required for the passive Ethernet tap and therefore a second port is added via USB - Trendnet TU2-ET100 USB->Ethernet (Figure 32).

6.2 Remote connectivity

The out-of-band connectivity to the device will be via a 3G/HSPA modem. However, there are two main design choices here: “Store and forward” or “Remotely initiated full control”.

Figure 33: 3G/HSPA modem

6.2.1 Store and forward

With this option, the device is scheduled to periodically dial out and forward all its collected data to the attacker. This approach is a more stealthy option, as during the day the modem can actually be switched off and only activated in the middle of the night when no staff would be present in the office before connecting outbound to send its data. If the modem was switched on all the time then staff may become suspicious if mobiles were not normally allowed in the office and the classic sound of GSM[30] interference was heard through PC speakers, as the modem communicated with the mobile network.

6.2.2 Remotely initiated full control

Purely from a control perspective this is the most preferable, as full control of the implant can be gained by the attacker at any time. The modem needs to be configured as "auto-answer" and therefore, appropriate security measures, such as IP tables[31] need to be employed to ensure that unauthorised access cannot be gained to the implant.

7 Physical space available within the docking station

The top of the docking station was removed by cutting away the plastic cover and the extendible cover that fits behind the laptop (Figure 34). As can be seen, there is actually quite a large space for additional electronics. This space shown assumes that the target organisation or individual does not use an extended-life extra-large battery.

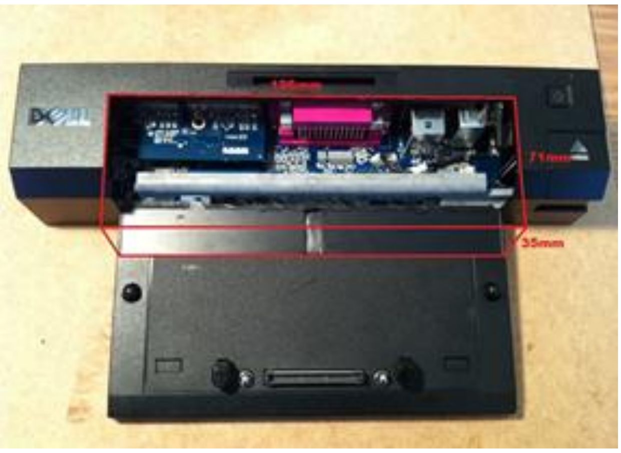


Figure 34: Docking station with cover removed

8 Power considerations

As docking stations are most likely to be permanently connected to a power source, providing power to any hardware implant should not be a problem. The DC voltage provided by the power supply is +19.5V. To power the implant we need +5V and although +5V is probably present in many different places on the PCB, it’s not clear what current limiters may be present at various points, so the simplest approach is to tap directly off the DC power input (Figure 35).

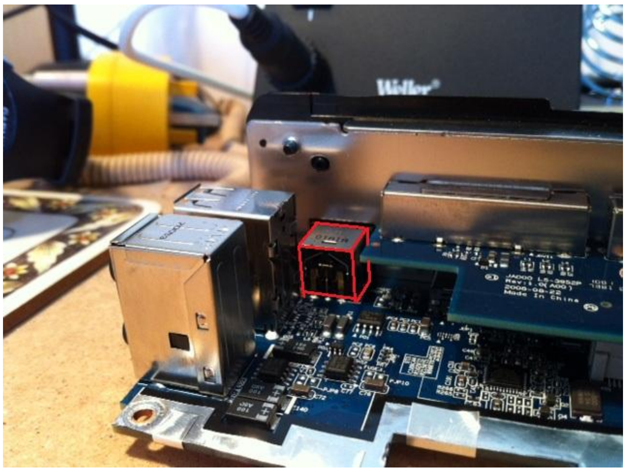


Figure 35: Rear of the main DC power input connector

A simple voltage divider circuit (Figure 36) is required to reduce the voltage from +19.5V to +5V

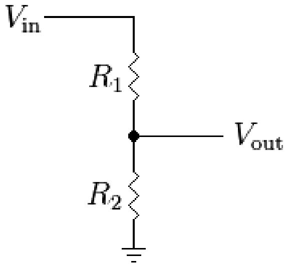


Figure 36: Simple voltage divider circuit

We know that V_{in} = 19.5V and V_{out} = 5V. If we assume that R2 = 1K then we can calculate R1 using the following equation:

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

R1 therefore equals 2.9K. However, resistors are generally supplied in a range of specific values and the nearest standard value = 3K. Therefore, if V_{in} = 19.5V, R1 = 3K and R2 = 1K, V_{out} can be re-calculated as follows:

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

V_{out} = 4.875V, which should be fine.

9 Putting it all together

Figure 37 shows the first prototype of an implant installed in a Dell PR02X docking station. Currently it only includes the passive Ethernet tap. A hinged replacement cover has been fabricated from clear Perspex to show the implant as well as the remaining physical space available. Figure 38 shows the docking station with the cover removed, but with no implant attached.

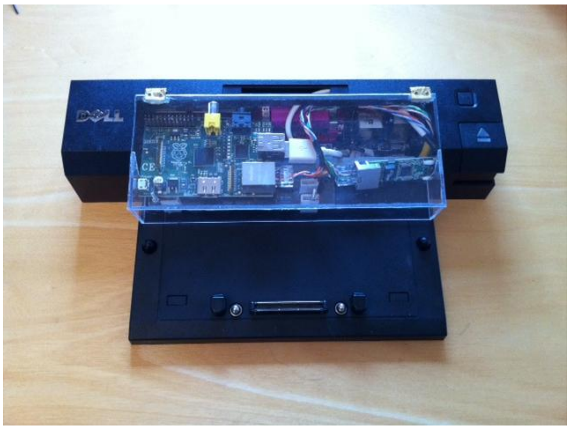


Figure 37: Spy-Pi implant installed in a Dell PR02X

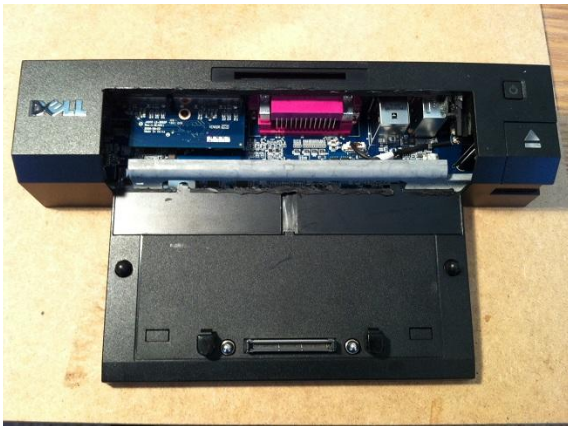


Figure 38: Dell PR02X with the cover removed

10 Detecting docking station-based hardware implants

Just as important as understanding how a hardware implant would be constructed is understanding how one would be detected. This section therefore, discusses approaches for detecting each proposed interception technique.

10.1 Passive network tapping

If the Ethernet network being tapped is 1000BASE-T then in order to tap the network a hardware-based downgrade attack is required (using capacitors to filter the high frequency signals) to force the link to use 100BASE-TX. A network administrator monitoring the switch connected to the docking station would therefore, be able to see that the Ethernet connection was running at a lower speed.

Recommendation: If when monitoring switch ports, a port which is connected to a laptop should be configured to be 1000BASE-T, but it appears to be 100BASE-TX this should be investigated, as it could indicate a downgrade attack associated with a passive Ethernet tap.

10.2 Active network attack

A new MAC address will appear on the network and it would be pretty straightforward to track down from a traditional network diagnostics perspective

Recommendation: Active monitoring of the network for previously unseen MAC addresses may reveal unwanted devices.

10.3 USB / PS/2 keyboard monitoring

A number of ways have been proposed[32][33] to detect hardware-based key loggers. However, this does not appear to be a simple problem to solve.

Recommendation: The best long-term solution is prevention rather than detection through the use of “Trusted hardware”[34].

10.4 Keystroke insertion

In order to insert keystrokes via USB a new HID device must be added to the USB bus. If there are three USB HID devices connected to your laptop (when you only have a keyboard and mouse connected) then something malicious may be happening.

Recommendation: A simple USB monitoring tool[35] could be used to detect this scenario

10.5 Audio monitoring

As mentioned earlier, if headphones or a microphone are connected to the laptop then the signals associated with any connected to the dock as severely attenuated.

Recommendation: As a detection technique is not known here, a mitigation approach could be to ensure that when sensitive communication is due to take place using the audio connections, the best approach is to connect directly to the laptop.

10.6 Other techniques

There are some other more general techniques that could be used to identify that a hardware implant existed within a docking station.

10.6.1 Weight

A new “known-good” (implant free) docking station could be accurately weighed and then periodically the other docking stations could be audited by weighing them to establish if any were heavier.

Advantages:
It is a relatively simple technique that would not require any specialist training or particularly sophisticated equipment.

Disadvantages:
It would be quite labour-intensive to periodically weigh all your docking stations. Furthermore, a dedicated attacker could probably remove the extra weight by modifying the internal design of the docking station.

10.6.2 Heat

The infra-red heat signature should be different for a docking station containing additional electronics as more power will be consumed and therefore, they could be periodically audited using a thermal imaging camera so see if any were significantly hotter than others.

Advantages:
This could be achieved using a thermal imaging camera, which is relatively easy to use with some basic training.

Disadvantages:
A dedicated attacker could possibly use techniques to thermally shield the implant to reduce its heat signature.

A thermal imaging camera was kindly loaned to NCC Group by E2V[36] and the results below clearly show that the additional electronics associated with a hardware implant can be detected this way:

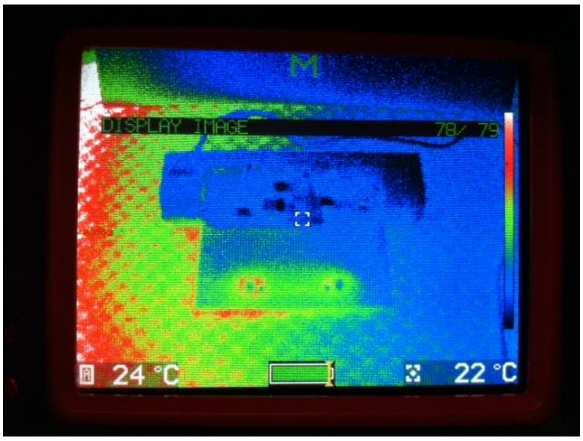


Figure 39: Thermal image of dock with no implant

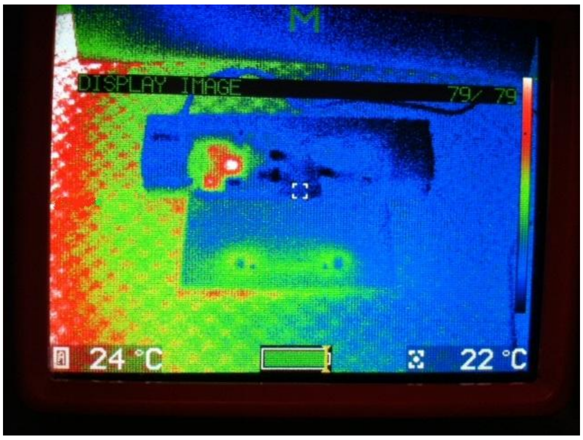


Figure 40: Thermal image of dock with implant

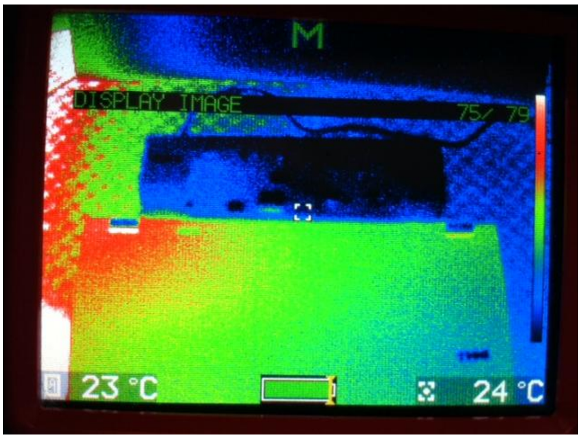


Figure 41: Thermal image of dock + laptop (no implant)

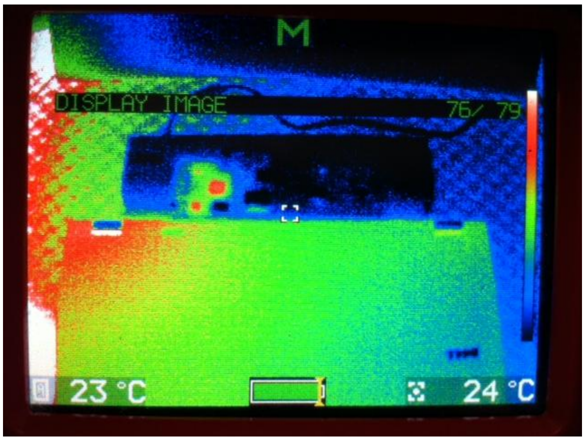


Figure 42: Thermal image of dock + laptop (with implant)

10.6.3 Current consumption

The power consumption will be more if an implant has been added to a docking station. Therefore, periodically measuring the current consumed by each docking station may reveal one that contains additional electronics. This could either be measured periodically using a device such as a current clamp[37] or by a current-measuring device placed in-line with the power cable.

Advantages:

With some basic training this could be easily performed periodically and would be difficult for the implant designer to counter.

Disadvantages:

It would be labour-intensive to periodically check all your docking stations

10.6.4 RF emanations

As the command and control communications channel is via 3G/HSPA then the implant would need to communicate via RF at a similar power to a mobile phone or tablet. Therefore, these RF emanations should be detectable.

Advantages:

RF emanations must be present for the out-of-band command and control communications to be possible.

Disadvantages:

In a modern office environment it would be difficult to discriminate between unauthorised 3G RF sources and legitimate ones associated with phones, tablets or laptop-based 3G cards.

11 Attack mitigation

Another defensive layer is mitigation techniques to prevent implants either being installed in the first place or to prevent them working when they are installed.

11.1 Active network connection

Recommendation: Only allow one MAC address per switch port - If the switch port into which the docking station is connected will only allow one MAC address then the implant will not be able to communicate on the network.

11.2 Passive network sniffing

Recommendation: Ensure that all sensitive network data is encrypted – if the data is encrypted then it doesn't matter how stealthy the interception technique, as the data will not be easily recoverable.

11.3 Physical security

Recommendation: Physically secure all docking stations to prevent them being swapped for Trojaned ones

11.4 RF shielding

Recommendation: An RF shield could be developed that fitted over a docking station to prevent any implant from communicating wirelessly.

12 Conclusion

Laptop docking stations are widely used and trusted devices, which provide extensive access to potentially sensitive data. Their anonymity, accessibility and lack of physical protection within an organisation can easily result in them being substituted for an identical-looking dock containing a hardware implant.

Attackers have historically targeted hardware interfaces e.g. key-loggers or video-loggers and therefore, docking stations are the next logical technological development, as they are normally permanently connected to a power supply and also to the network. Furthermore, in a modern hot-desking environment a dock-based implant has the potential to attack different target laptops each day. As more and more network services are protected with strong encryption by default, the ability the intercept data at the endpoint i.e. a laptop either after it has been decrypted or before it has been encrypted is the most attractive property of this attack approach.

There are a number of different interfaces that attackers would be interested in targeting via a docking station; these include:

- Network data – sensitive data sent using unencrypted network services
- Video – screenshots of the laptop screen could reveal sensitive data
- Audio – If softphones are in use then conversations could be monitored
- Keyboard – keystrokes could be captured or potentially inserted
- Webcams – Video-conferencing sessions could be monitored

There are a number of potential techniques for detecting various elements of hardware implants, some more effective than others. However, the most effective detection process would most likely involve a combination of different approaches, ranging from technical techniques such as detecting the hardware "downgrade attack" required for passive Ethernet sniffing in combination with more physical techniques such as the use of a Thermal Imaging camera.

By far the easiest and most effective approach to prevention is physical security. Locks should be used to prevent docking stations from being substituted and the use of anti-tamper stickers, which can reveal that a docking station has been subject to unauthorised opening.

13 References & further reading

1. http://en.wikipedia.org/wiki/Kensington_Security_Slot
2. http://support.dell.com/support/edocs/acc/eapr/en/
3. http://www.zdnet.com/inside-the-biggest-bank-raid-that-never-was-3039191956/
4. http://en.wikipedia.org/wiki/Hardware_keylogger
5. http://pwnieexpress.com/
6. http://www.smsc.com/index.php?tid=251&pid=168 SMSC
7. http://www.ti.com/product/sn75dp122a&lpos=Middle_Container&lid=Alternative_Devices
8. http://www.paradetech.com/products/displayport-switch-products/ps8121ed-11-dp-repeater/
9. http://www.pericom.com/products/redriver-signal-conditioners/?part=PI2EQX3211CM
10. http://www.100y.com.tw/pdf_file/APL1117.PDF
11. http://pdf1.alldatasheet.com/datasheet-pdf/view/73834/MAXIM/MAX877.html
12. http://www.datasheetarchive.com/dataframe.php?file=DSA-51926.pdf&dir=Datasheets-3&part=USB2513-AEZG
13. http://www.datasheetarchive.com/indexer.php?file=DSA00204913.pdf&dir=Datasheet-064&keywords=mp243ec
14. http://ossmann.blogspot.co.uk/2011/02/throwing-star-lan-tap.html
15. http://en.wikipedia.org/wiki/1000BASE-T#1000BASE-T
16. http://en.wikipedia.org/wiki/Network_tap
17. http://www.miarec.com/faq/what-is-port-mirroring
18. http://en.wikipedia.org/wiki/100BASE-TX#100BASE-TX
19. http://www.amphenol.com.tw/Drawing/RJMG23102XXX0XX.pdf
20. http://www.amphenol.com.tw
21. http://www.keelog.com/files/VideoGhostUsersGuide.pdf
22. http://www.keyghost.com/
23. http://www.lumension.com/
24. http://www.nccgroup.com/media/199381/ncc_group_threat_brief_usb_keyboards_by_post_2013.pdf
25. http://www.te.com/catalog/pn/en/440173-4
26. http://www.datasheetarchive.com/dataframe.php?file=DSA-51926.pdf&dir=Datasheets-3&part=USB2513-AEZG
27. http://supportapj.dell.com/support/edocs/systems/latc600/en/pinouts/index.htm#docking_connector
28. http://uk.rs-online.com/web/generalDisplay.html?id=raspberrypi
29. http://www.raspberrypi.org/about
30. http://en.wikipedia.org/wiki/Gsm
31. http://www.netfilter.org/projects/iptables/
32. http://www.irmplc.com/downloads/whitepapers/Hardware_Keylogger_Detection.pdf
33. https://deepsec.net/docs/Slides/2010/DeepSec_2010_Detecting_Hardware_Keylogger.pdf
34. https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf
35. http://code.msdn.microsoft.com/windowshardware/USBView-sample-application-e3241039
36. http://www.e2v.com/
37. http://en.wikipedia.org/wiki/Current_clamp

14 Glossary

DC – Direct Current

DVI – Digital Visual Interface

HDMI – High-Definition Multimedia Interface

HSPA – High Speed Packet Access

I^{2}C – Inter-Integrated Circuit

LAN – Local Area Network

MAC – Media Access Control

PCB – Printed Circuit Board

PS/2 – Personal System/2

RF – Radio Frequency

SATA – Serial AT Attachment

SPAN – Switched Port Analyser

TMDS – Transition-minimized differential signalling

USB – Universal Serial Bus