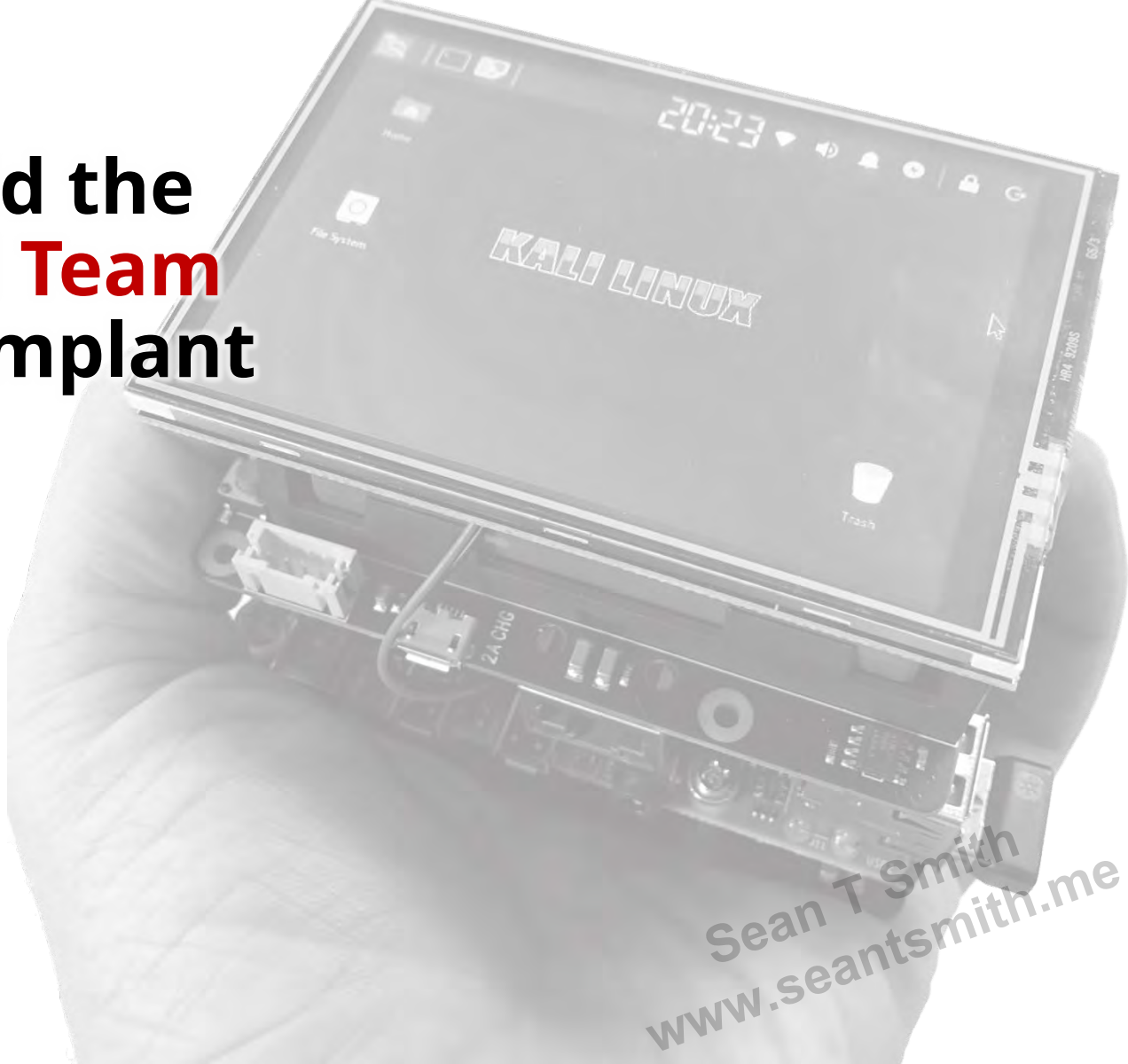
How to Build the Perfect Red Team Hardware Implant

Sean T Smith

March 2023



whoami

Name	Sean T Smith
Hacker Handle	cpt_smidiculous
Occupation	Smart Factory IIoT Consultant
Another Occupation	Cyber Team Operator
Yet Another Occupation	Adjunct Professor of Cybersecurity
Family	Wife, 2 Kiddos
Education	Undergrad, Grad, but mostly Google
Hobbies	Building hardware implants!
My Social Media Links	**www.seantsmith.me**

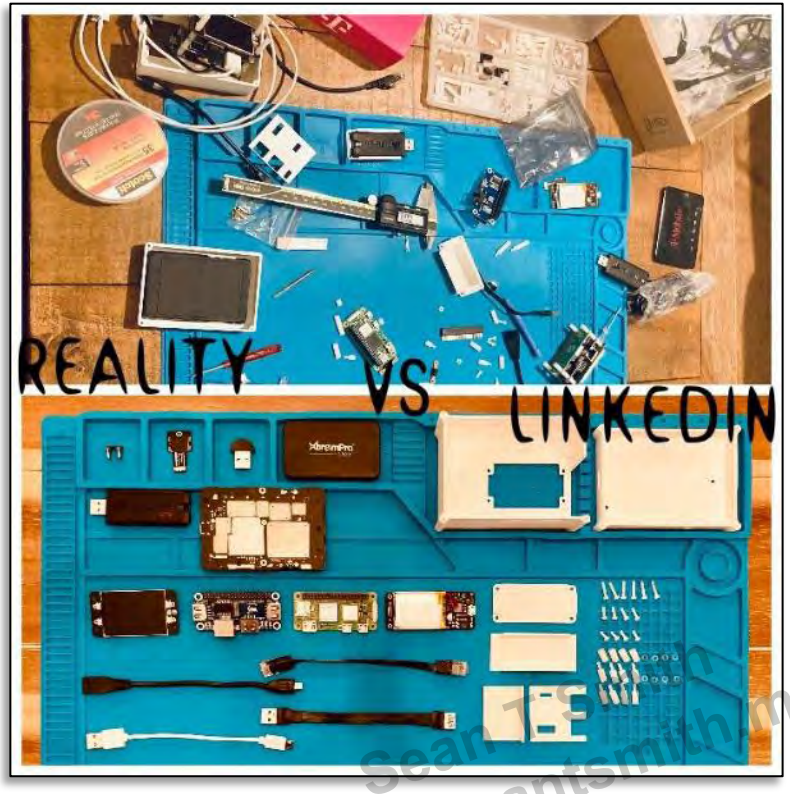
Agenda

- Introduction
- Importance of Hardware Implants
- Defining the ‘Perfect’ Implant
- Choosing an Implant Platform
- Setting up Hardware & Key Software
- Build Progression
- **Demo**
- Final Thoughts

What are we learning today?

Building an implant requires patience, persistence, and trial-and-error.

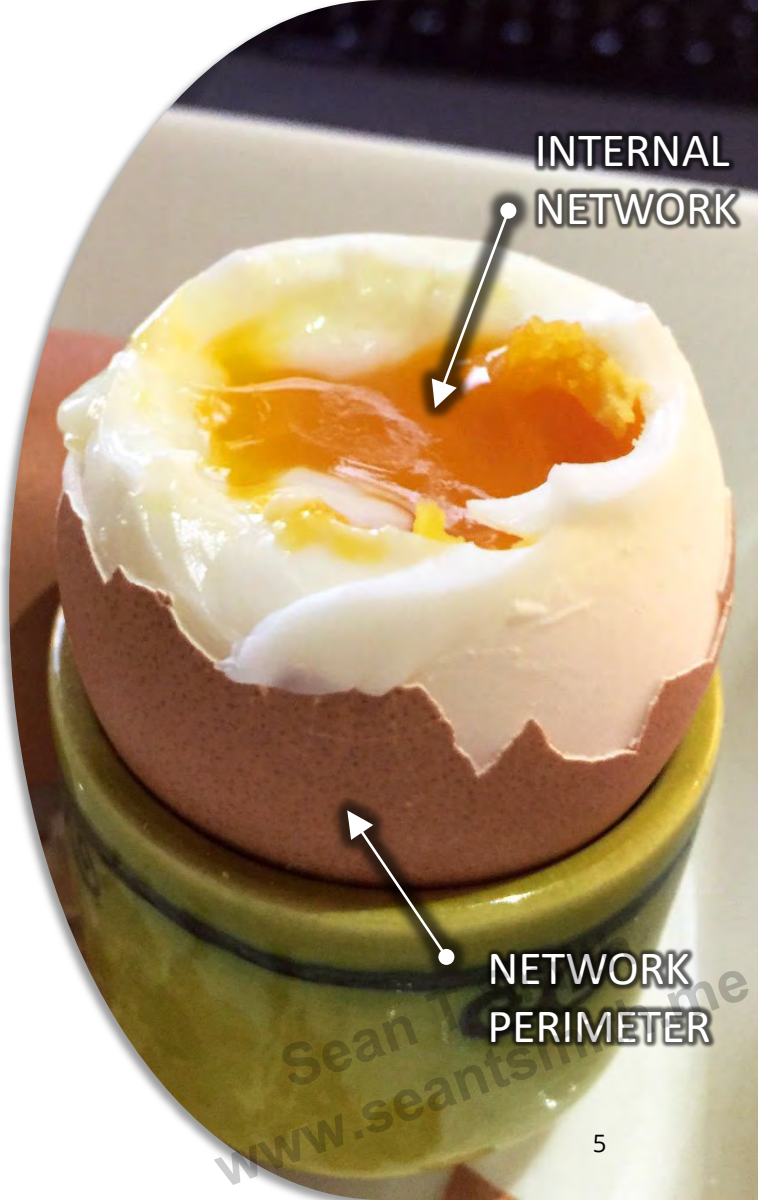
- This presentation will narrowly focus on the key considerations, materials, and instructions to **craft a purpose-built hardware implant** to effectively breach a network during Red Team Engagements
- Bottom line, there are no good pre-built hardware implants available on the market, I have spent the last 3 years building, testing, and using my own **custom devices in real-world assessments**
- Time to **share what I've learned**



How is this useful?

Breaching physical security bypasses all perimeter security, providing direct access the internal network.

- **Red Team engagements are very sophisticated** and complex in their planning and execution
- The goals of these engagements vary, but frequently they require breaching the perimeter of a target organization to **gain an internal network foothold**
- The most expedient method with the highest probability of success is through **implanting a remote-controlled computer** inside the physical perimeter
- This device must be discrete, optimized for reliability and ease of use, while providing the requisite **C2 connectivity** to operators



How does this help the good guys?

A compelling readout can successfully advocate on behalf of struggling corporate cybersecurity.

- **Presenting compelling engagement results** to the customer's leadership is intensely effective
- This often leads to swift organizational changes that **improve cybersecurity focus and resourcing**
- **Non-technical leaders can easily relate** to exploiting physical-to-digital vulnerabilities that generate real-world impacts
- It is for this reason that crafting an effective, purpose-built implant is a **critical skill** for any Red Team Operator

What devices can you buy pre-made?

Can you find anything, because I never have!

- **No implants + fancy party tricks:** hak5.org
- **No implants + everything is sold out:** lab401.com
- **No implants + everything is sold out:** hackerwarehouse.com
- **Great Open-source Project:** github.com/RoganDawes/P4wnP1_aloa
- **Decent tutorial, but old:** www.blackhillsinfosec.com/how-to-build-your-own-penetration-testing-drop-box
- **More recent, but less helpful:** www.blackhillsinfosec.com/pentesting-dropbox-on-steroids

"Pwn Phone"

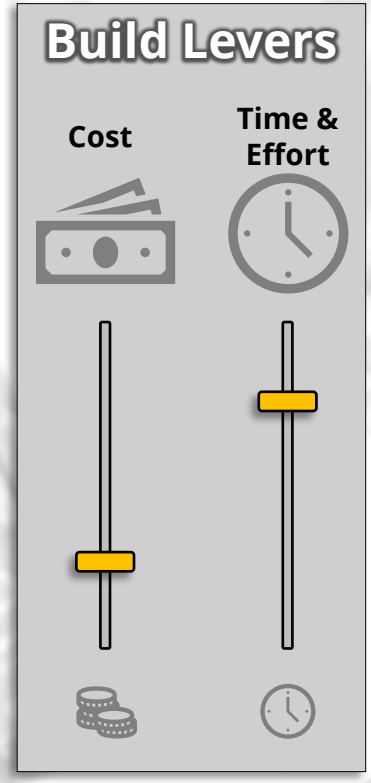
Hak5 Lan Turtle

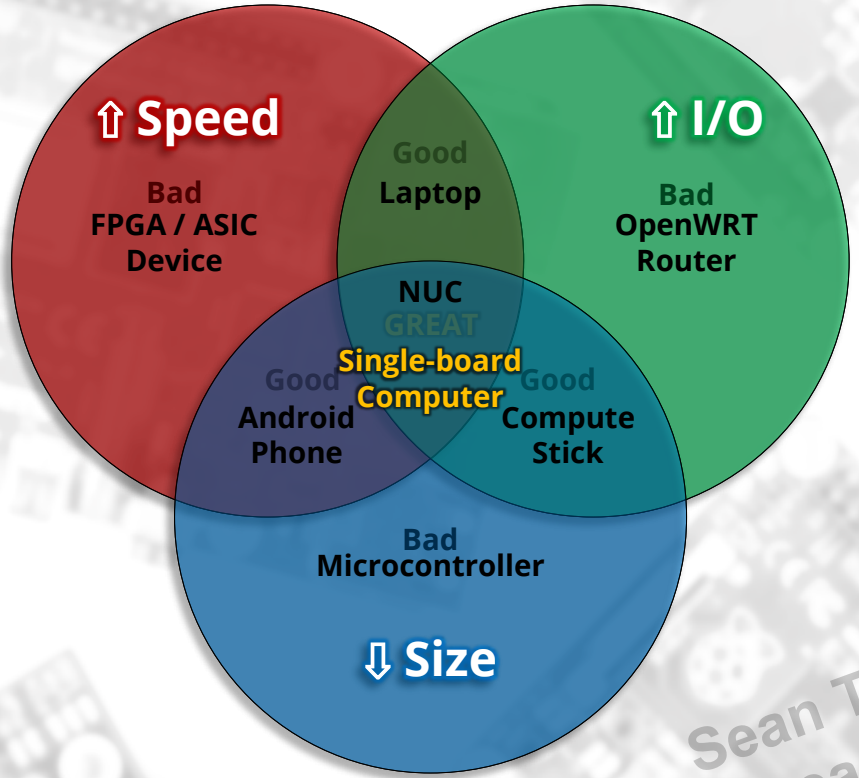
Hak5 Key Croc

P4wnP1 ALOA

What does ‘perfect device’ mean to me?

The device must meet the critical implant requirements given a reasonable amount of time/effort while being low-cost and readily available.





Evaluating potential implant platforms…

Single-board computers and Compute Sticks were very close, the tie breaker was the software and community support for SBCs.

Potential Platform	Evaluation Criteria (Worst (1) – Best (5))					
	Speed	I/O	Size	Cost	Effort	Score
 Single-board Comp.	4	4	4	5	4	84%
 Compute Stick	3	3	5	4	5	80%
 NUC	5	5	3	2	4	76%
 Laptop	5	4	3	2	4	72%
 OpenWRT Router	2	4	3	5	3	68%
 Android Phone	4	2	4	3	2	60%
 Microcontroller	1	3	5	5	1	60%
 FPGA / ASIC Device	5	1	1	1	1	25%

Which Single-Board Computer to choose?

The smaller size of the RPi Zero 2W was much too compelling, I committed to finding creative ways to mitigate the performance constraints.

SBC Model	Significant Findings	Decision
 Raspberry Pi Zero 2W	Small, fast enough, minimal RAM.	✓+
 Raspberry Pi 3B+	Hard to make compact with peripheral devices attached, faster, more RAM.	✓
 Raspberry Pi 4B	Poor thermals, high power consumption.	✓–
 Raspberry Pi CM4	Poor thermals, high power consumption, flexible daughter board options.	✓–
 Raspberry Pi 3B	3B+ is superior.	✗
 Raspberry Pi Zero W	Zero 2W is superior.	✗
 Orange Pi R1 Plus	Very poor software support.	✗

Operational Requirements Drive the Build Process

We can begin building on the selected platform by defining the operational requirements and using them to make hardware and software integration decisions.

Operational Requirements	
Rugged & Tough	Runs Required Tools
Rapid Installation	Sufficient Storage
Easily Concealed	Redundant C2 Tunnels
Easy to Operate	Avoids IDS/IPS/Firewalls
Simple to Troubleshoot	Piggyback Data via Ethernet
Self-healing Operation	Piggyback Data via Wi-Fi
Location Tracking	Piggyback Power via USB

Hardware	
Core Hardware	Supporting Devices
Peripherals	Accessories

Software
Essential Software & Configuration
Remote Access Solutions

Defining the Red Team's Requirements

The unique needs of the Red Team should be fulfilled by the hardware and software.

Operational Scenarios

...you need to quickly move the implant?
...there is no power outlet or USB port nearby?
...someone discovers the implant?
...someone doesn't return the implant?
...you accidentally drop the implant?
...the implant overheats?
...there is no cellular or Wi-Fi or ethernet connectivity?
...you need to verify it can ping your C2?
...you didn't get an IP address?
...the implant stops working?
...you need to troubleshoot during the operation?
...you need to troubleshoot the implant remotely?
...someone interrupts you during the installation?
...you forget or lose a cable or power cord?
...there is intermittent connectivity?
...the implant becomes unresponsive?
...the implant loses C2 connectivity?
...you need to recover the implant?
...you accidentally spill something on it?
...you need to replace a component?
...connectivity is blocked by defenses?
...it runs out of memory?
...it runs out of storage?
...THE LIST IS ENDLESS!

define

Operational Requirements

Rugged & Tough	Runs Required Tools
Rapid Installation	Sufficient Storage
Easily Concealed	Redundant C2 Tunnels
Easy to Operate	Avoids IDS/IPS/Firewalls
Simple to Troubleshoot	Piggyback Data via Ethernet
Self-healing Operation	Piggyback Data via Wi-Fi
Location Tracking	Piggyback Power via USB

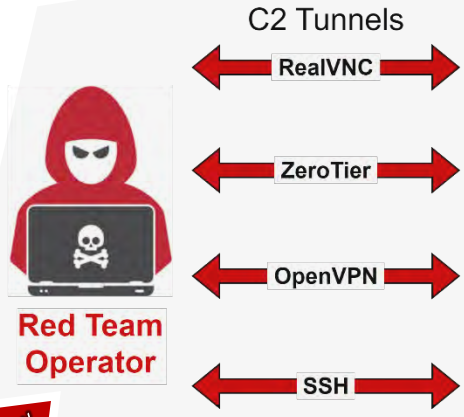
fulfilled by

device development

used by

dictate

Tabletop & Real-world Exercises



Adding Hardware to the Raspberry Pi Zero 2W

Building the implant requires a creative prototyping mindset where you must re-evaluate designs and hardware to successfully package required components.

Hardware	
Core Hardware	**Supporting Devices**
1. Ethernet & USB 2. Battery Backup 3. Display with Input 4. EMMC	5. Network Switch 6. Cellular Hotspot 7. Apple AirTag
Peripherals	**Accessories**
8. SSD 9. Wireless Adapter	10. Power Adapter 11. Case 12. Other Stuff

Core Hardware Details

The hardware required by the Pi to run, or that integrates directly with its GPIO pins.

1. Ethernet & USB

Manufacturer: Waveshare | **Model:** ETH/USB HUB HAT

Description:

The ETH/USB Hat connects to the Pi via a Micro USB dongle; the GPIO pins are not used but remain accessible via passthrough extension pins. This provides 1x 10/100 Ethernet and 3x full-size USB ports.

2. Battery Backup

Manufacturer: Zopsc | **Model:** V1.2 UPS Lite Power HAT Board

Description:

The UPS Lite connects via POGO pins to the underside of the GPIO pins. The Pi is both powered and recharged via the Micro USB on this board. This board has a power switch and allows uninterrupted power flow between charging and discharging.

3. Display with Input

Manufacturer: Pimoroni | **Model:** Display HAT Mini

Description:

The 320x240 full-color display connects via GPIO SPI and is large enough to show meaningful system information. The four buttons have been programmed to display connectivity status, refresh networking, show a logo, and turn off the display.

4. EMMC

Manufacturer: UUGear | **Model:** 32GB RasPiKey

Description:

The RasPiKey uses the standard SD slot but stores data in a more reliable / faster way using EMMC vs traditional SD cards. This increases the devices overall performance and stability.

Supporting Device Details

Stand-alone devices which augment the implant's native capabilities with loose integration.

5. Network Switch

Manufacturer: XtremPro
Model: 3-Port USB Powered Network Switch

Description:

The 10/100 mini switch has a perfect form factor for connecting to the Pi's ethernet while exposing two external ethernet ports for piggybacking onto a target device's connection. The device uses one of the Pi's USB ports for power only. The status lights are also exposed externally which provides quick connectivity visual to an operator.

6. Cellular Hotspot

Manufacturer: Franklin Wireless
Model: Franklin T9 4G LTE Mobile Hotspot

Description:

The Franklin T9 was handed out for free via the T-Mobile Test Drive program. The overwhelming supply of these devices means they sell for < $5 each online. Conveniently, these can be rooted, customized, and carrier unlocked extremely easily (online guide). Once done, you can activate up to 5 data devices on a Google Fi "Flexible" plan for $20 per month, total! The Pi is configured to connect to the hotspot via onboard wireless.

7. Apple AirTag

Manufacturer: Apple
Model: AirTag

Description:

The AirTag is an excellent choice for location tracking as it leverages Apple's extensive network of devices. It has safeguards which prevent stalking and notifies nearby individuals of rogue AirTags. This feature generally does not impact our use case as the implant is stationary. As an extra precaution, you can disable any potential audible alerts by removing the speaker (online guide).

Peripheral Details

Tools which directly interact with the Pi via USB to extend the implant's functionality.

8. SSD

Manufacturer: Corsair | **Model:** Flash Voyager GTX 256GB

Description:

This is a true 256GB SSD in a flash drive form factor. The drive is fast, reliable, and consumes very little power. A secondary storage location is important for storing network packet captures or other large files obtained from the target's network. This drive can be encrypted and secured so that any customer data is safe if the device is lost.

9. Wireless Adapter

Manufacturer: Panda Wireless | **Model:** PAU03

Description:

Panda Wireless devices are known for their compatibility with wireless auditing tools by supporting monitor mode and packet injection on a broad range of Linux kernels. This device is the smallest and most discrete available wireless card (I could find) and is attached via the externally exposed USB port on the implant.

Accessory Details

Items which enable hardware connectivity or physically secure/enclose the device.

10. Power Adapter

Manufacturer: Anker
Model: A2620 - Dual Port 12W Wall Charger

Description:

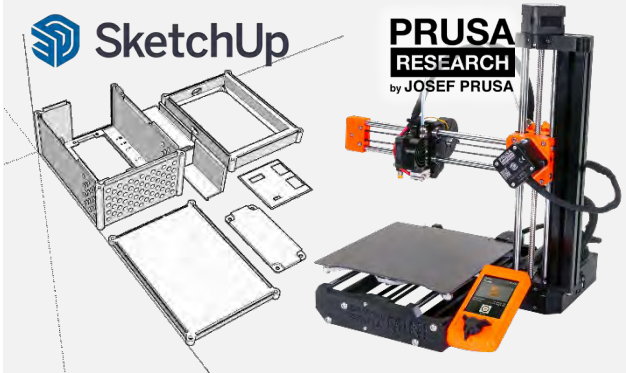
The Anker 12W wall charger with dual USB charging ports is perfect for powering both the implant and hotspot simultaneously. Accompanying this small charger are two 6’ Micro USB charging cables secured together via mesh cable wrap and heat shrink.

11. Case

Design Software: SketchUp for Web (free)
3D Printer: Prusa MINI+

Description:

The goal is to package the implant into an adequate form factor. Ultimately, this can be done with or without 3D design/printing. This custom case was designed using SketchUp and printed on a Prusa 3D printer. 3D design and 3D printing are two skills which require significant time investment to master.



12. Other Stuff

Manufacturer: Miscellaneous
Cables & Connectors: 2.5M Assorted Nylon Screws & Spacers, Rubber Feet, 6-inch Flat Ethernet, 6-inch USB Extension, 6-inch Micro USB Extension, 6-inch Micro USB Cable

Description:

You will need to procure many assorted connectors, cables, and accessories to assemble the implant. I find that 6” cables tend to work best and 2.5M-sized nylon connectors are compatible with all Raspberry Pi devices.

Installing & Configuring the Software

A stable, reliable, and feature-rich OS platform with redundant C2 connectivity.

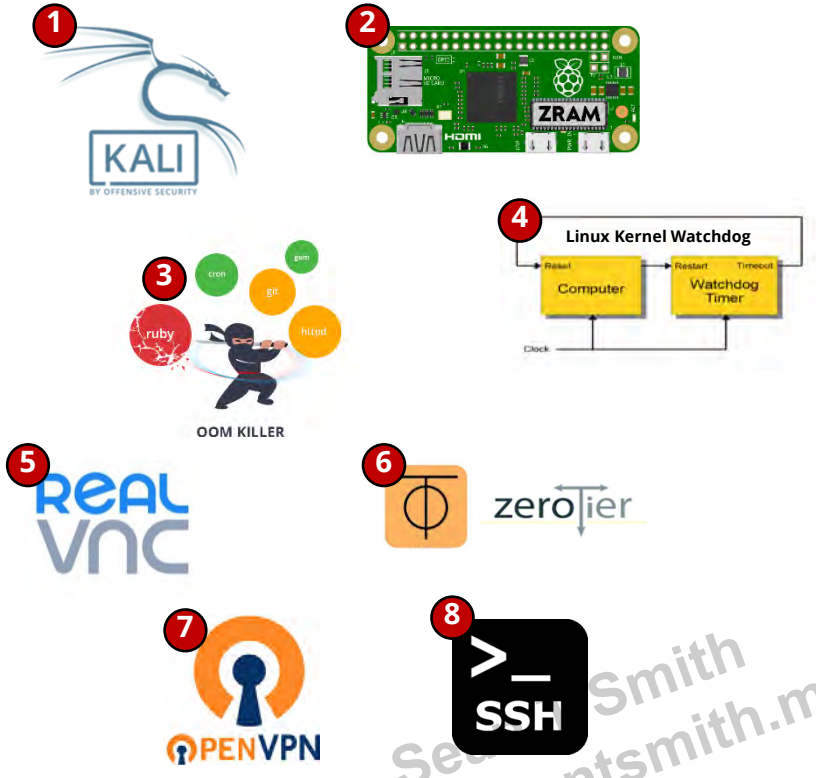
Software

Essential Software & Configuration

1. Kali 32-bit, LXDE
2. Enable ZRAM (More Ram)
3. Early Out of Memory
4. System & Network Watchdog

Remote Access Solutions

5. RealVNC
6. ZeroTier
7. OpenVPN
8. AutoSSH



Essential Software & Configuration Details

Efficiently use the limited available resources to provide all required capabilities.

1. Kali 32-bit, LXDE

Manufacturer: Offensive Security
Model: kali-arm

Description:

The 32-bit kali-arm (armhf) architecture with the LXDE Desktop works best with the resource constrained RPi Zero 2W because it consumes the least memory while still providing full-functionality. This will need to be custom built using the official Kali build-script documentation.

Kali Linux

LXDE Desktop

2. Enable ZRAM (More Ram)

Manufacturer: Linux Pi-Apps
Model: More Ram

Description:

The 'More Ram' application available from Pi-Apps creates a compressed swap space in memory which can safely increase the usable memory by 50% without sacrificing (much) performance or stability. This will give the Pi Zero 2W just enough memory to safely run a full Firefox web browser.

Pi-Apps

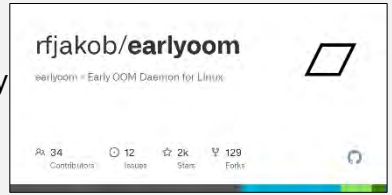
More Ram

3. Early Out of Memory

Manufacturer: rfjakob
Model: earlyoom

Description:

The native oom-killer built into Linux will kill processes when the available memory is very low. Often this process is invoked too late, causing the system to lock up. The earlyoom tool invokes this process sooner which can prevent the system becoming unresponsive.

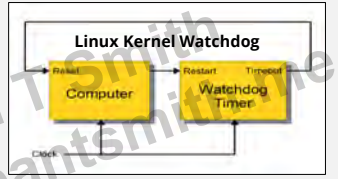


4. System & Network Watchdog

Manufacturer: Linux Daemon
Model: Watchdog Daemon

Description:

Enabling the watchdog daemon on the RPi requires a few steps to expose the hardware to the watchdog software; process can be found here. The watchdog can be configured to restart the system if the OS or networking becomes unresponsive. This feature is necessary for keeping the implant running.



Remote Access Solution Details

Configure remote connectivity to provide a redundant and reliable C2 channel.

5. RealVNC

Manufacturer: RealVNC
Model: VNC Viewer / Server

Description:

The Raspberry Pi allows you to use a FREE cloud based RealVNC account for up to 5 RPi devices (for non-commercial use). This is a simple solution for remotely accessing the implant from anywhere in the world; tutorial available here.

6. ZeroTier

Manufacturer: ZeroTier
Model: Basic

Description:

ZeroTier is an encrypted virtual network backbone, allowing multiple machines to communicate as if they were on a single network. This free solution is offers a web-based management console for configuring and controlling access; tutorial can be found here.

7. OpenVPN

Manufacturer: OpenVPN
Model: PiVPN

Description:

Setting up and configuring OpenVPN on a RPi is made significantly easier using the PiVPN tool. This will create another connectivity pathway for securely accessing the implant.

8. SSH

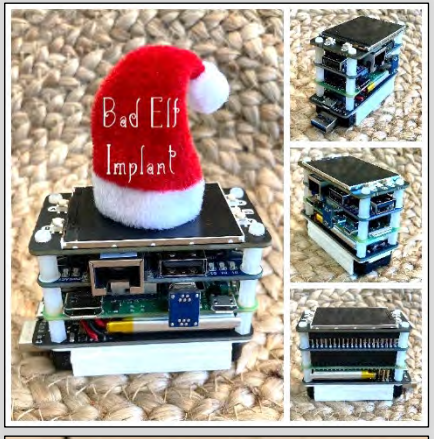
Manufacturer: Linux SSH
Model: AutoSSH

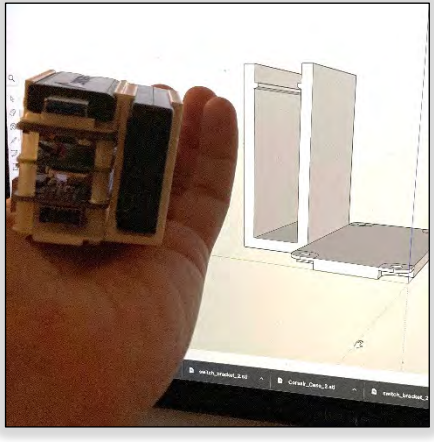
Description:

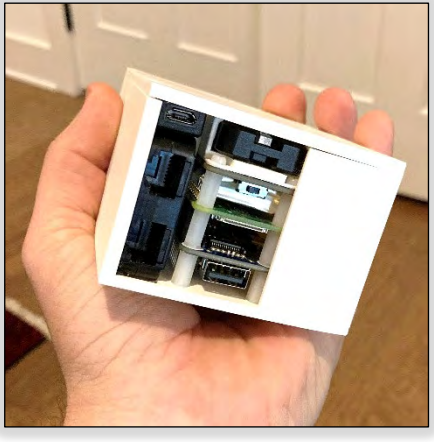
The AutoSSH tool can be used to maintain an active reverse SSH tunnel to provide remote CLI access to the implant (online guide). This can be configured to run as a service that calls outbound to a DNS record to establish a persistent C2 tunnel to the red team operator.

How it started...

The "Pwnagotchi" and "P4wnP1 ALOA" projects started me down the path of developing RPi-based implants; the device evolved as my Red Teaming requirements expanded.





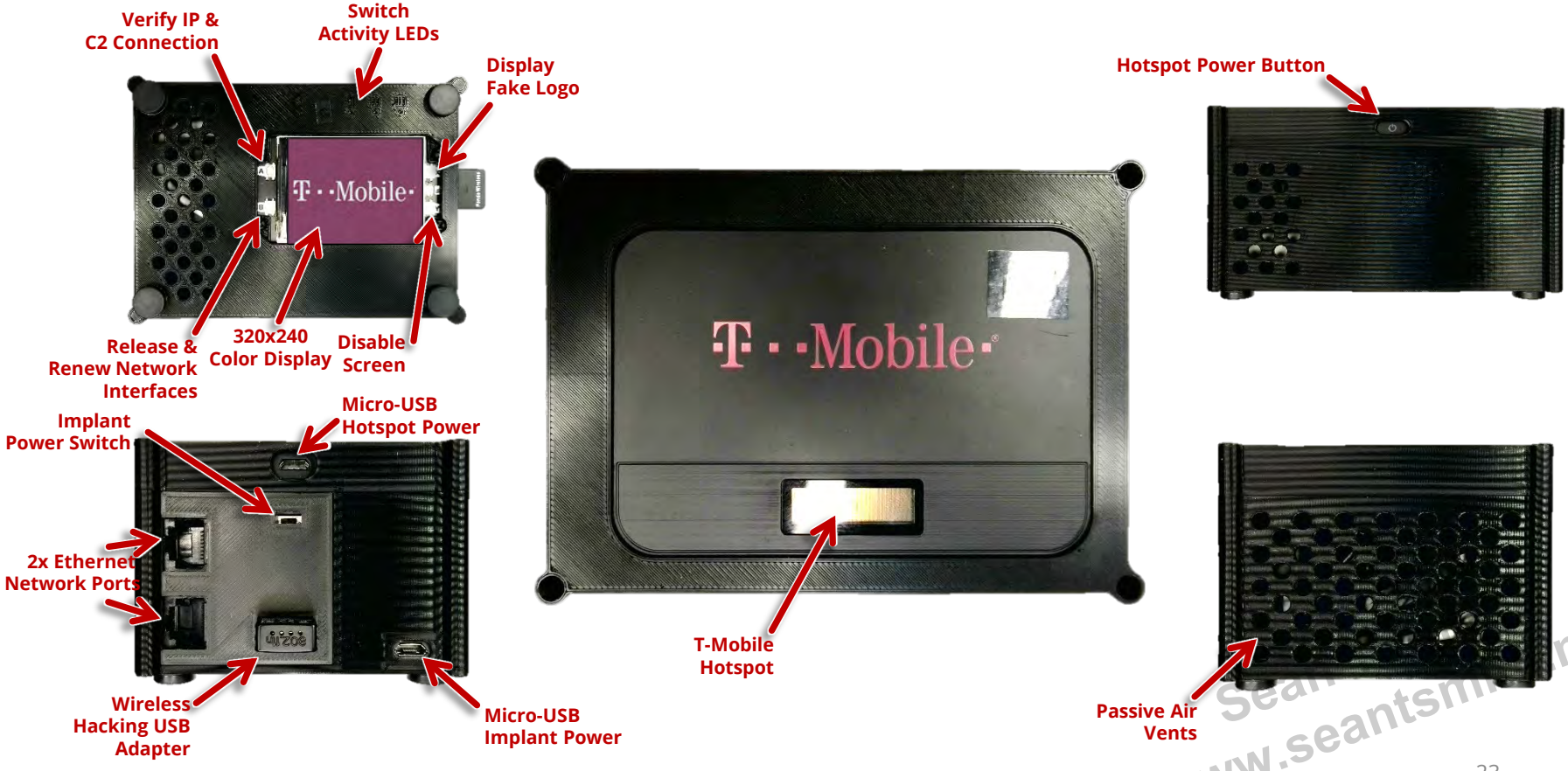


Current version... Outside 3D View

The implant feels dense and is slightly larger than an aluminum can.

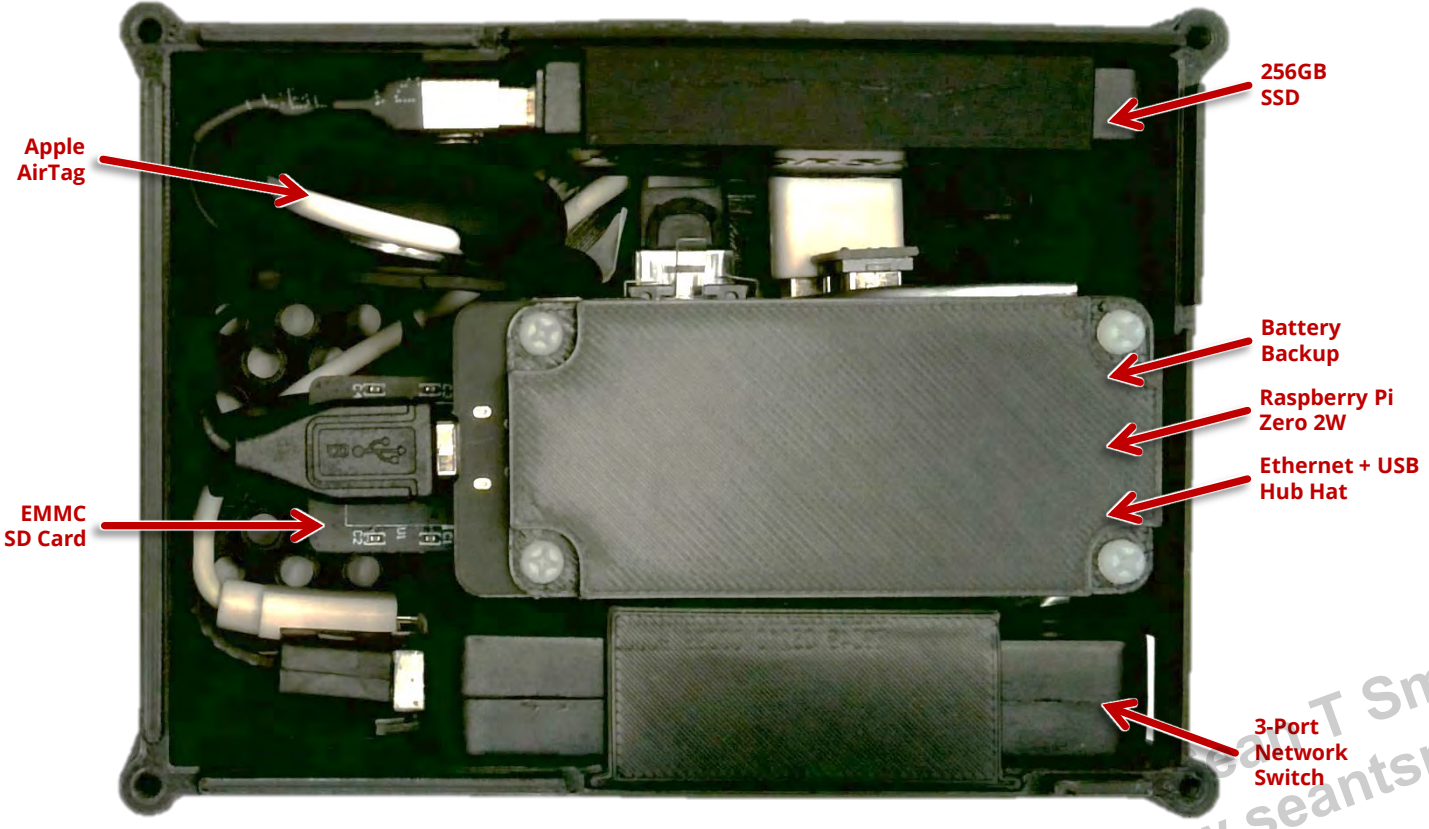
Current version… Outside Face Views

The outside is subdued but contains all necessary ports, buttons & indicators.



Current version... Inside View

The components are individually modular and replaceable while remaining compact.



https://youtu.be/uCErFs0Q_7g

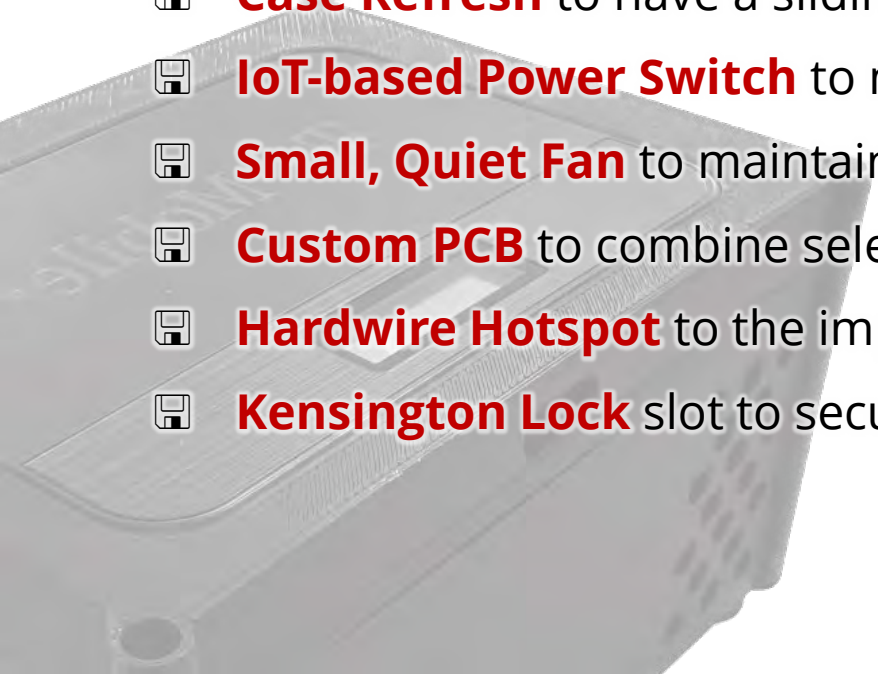
☠ Demo Time ☠

When things go terribly wrong…

Future Implant Upgrades

Always keep improving!

- **Leverage Config Management** tools to update OS and Software
- **Update Button Controls** to increase functionality and look & feel
- **Case Refresh** to have a sliding lid vs screws, remove ‘corner tubes’
- **IoT-based Power Switch** to manually remote power cycle
- **Small, Quiet Fan** to maintain temps in hot environments
- **Custom PCB** to combine select peripheral components
- **Hardwire Hotspot** to the implant to increase stability
- **Kensington Lock** slot to secure it in place



Final Tips

Iterate, test, use, and improve after each engagement.

- ✓ **Keep it plugged in** and maintained between engagements
- ✓ **Have a backup** and spare parts on-hand
- ✓ **Label the device** with return instructions in-case it's found
- ✓ **Give kudos in the outbrief** to any employee that reports it
- ✓ **Use strong passwords** and/or certificate-based authentication
- ✓ **Encrypt the storage** so that your client's data is protected if lost
- ✓ **Reimage** after each use to sanitize residual client data

Thank you!

Sean T Smith

www.seantsmith.me

linkedin.com/in/seantsmith

twitter.com/sts5017

github.com/sean-t-smith