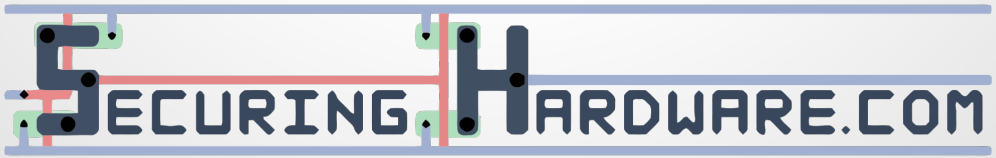
Tools of the NSA Playset

Ruxcon 2014
Joe FitzPatrick
Mike Ryan



What is the NSA Playset?

[UNCLASSIFIED]

HACKRF

Software Defined Radio Peripheral

(U//FOUO) HACKRF is a Software Defined Radio peripheral capable of transmission or reception of arbitrary radio signals from 10 MHz to 6 GHz.

12/31/13

(U//FOUO) HackRF One with optional enclosure

(U//FOUO) HACKRF is an open source hardware platform designed to enable education, experimentation, and deployment of Software Defined Radio (SDR) technology.

(U//FOUO) HackRF One Features:

- 10 MHz to 6 GHz operating frequency
- half-duplex transceiver
- portable
- Hi-Speed USB 2.0, bus powered
- low cost
- open source
- works with GNU Radio
- 20 MHz bandwidth
- 8 bit resolution
- external clock input and output

(U//FOUO) Applications:

- spectrum analysis
- vector signal analysis
- vector signal generation
- reverse engineering
- spectrum sensing
- wireless security testing
- radio research and development

(U//FOUO) HACKRF makes cutting edge SDR technology available to everyone. Now you can build any radio you want.

Status: Available Q1 2014
http://greatscottgadgets.com/hackrf/

Unit Cost: $300 estimated

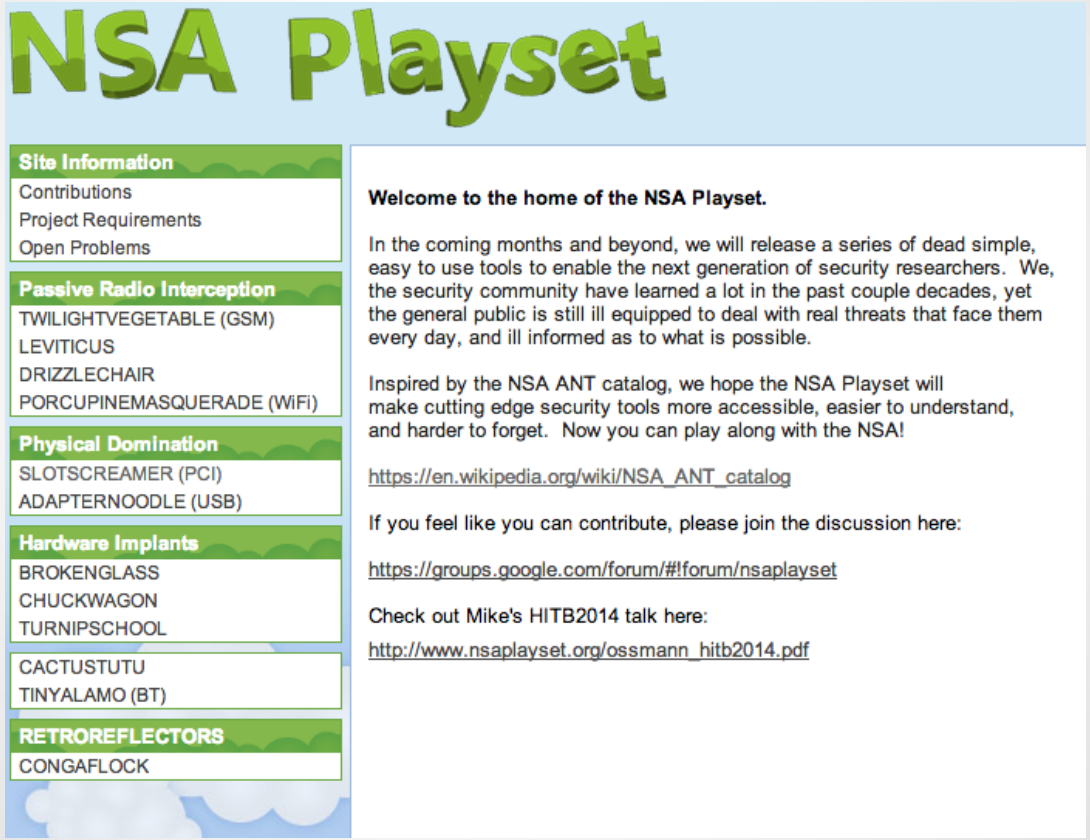
POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

HackRF is open source hardware and software. Anyone may use it, build it, or modify it, not just the NSA.

[UNCLASSIFIED]

()

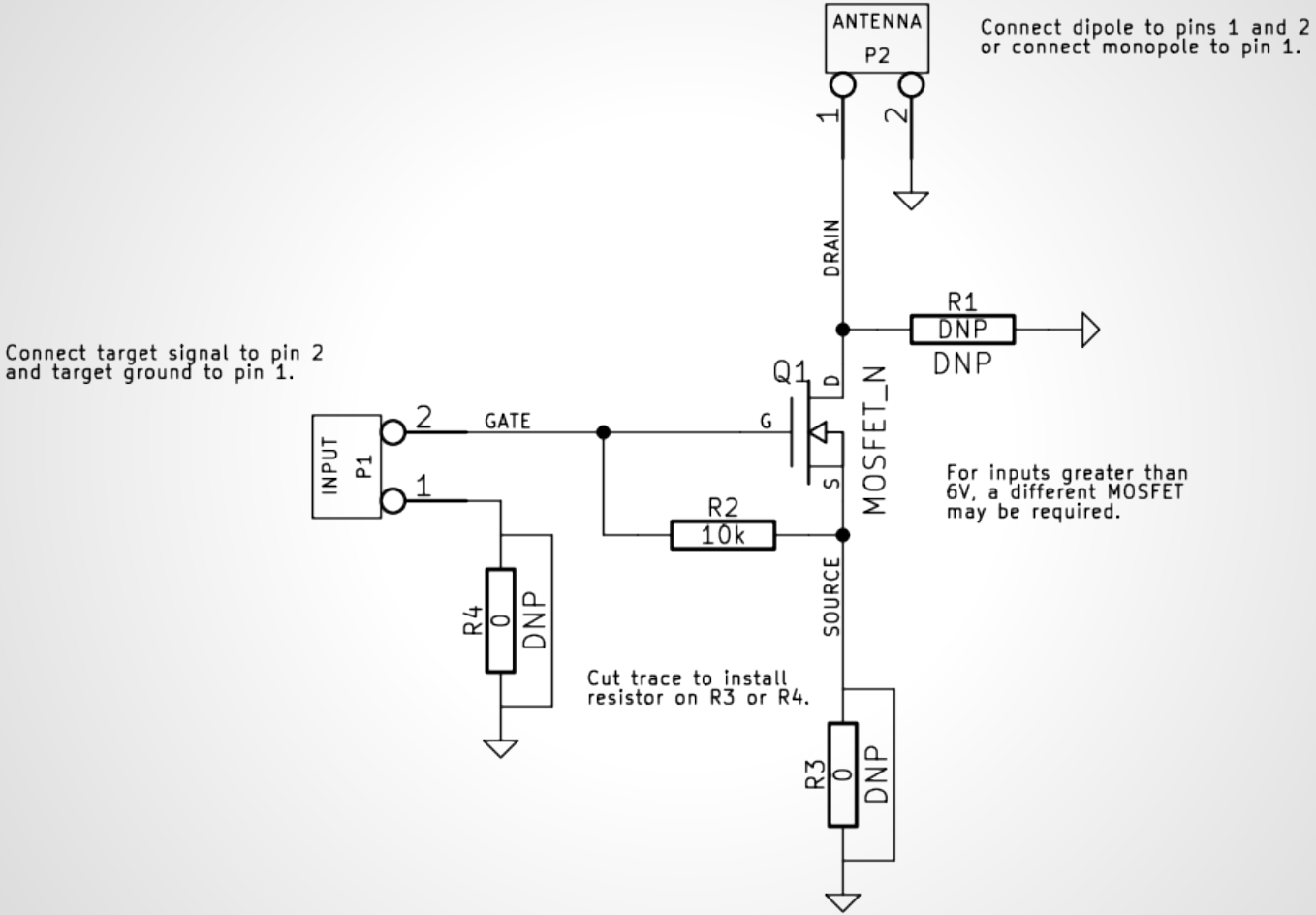
nsaplayset.org



NSA Playset Price Sheet

CONGAFLOCK - <$1

A 'Retroreflector', which is a passive device that reflects differently when a monitored wire changes


ANTENNA
P2
1
2
Connect dipole to pins 1 and 2
or connect monopole to pin 1.
DRAIN
R1
DNP
DNP
Connect target signal to pin 2
and target ground to pin 1.
Q1
D
G
S
MOSFET_N
INPUT
P1
2
GATE
1
R2
10k
For inputs greater than
6V, a different MOSFET
may be required.
SOURCE
R4
0
DNP
Cut trace to install
resistor on R3 or R4.
R3
0
DNP

()

NSA Playset Price Sheet

TWILIGHTVEGETABLE - $50

Custom Boot environment for basic GSM monitoring

- Sandisk 16G Extreme USB
- NooElec RTL-SDL dongle + antenna

TWILIGHTVEGETABLE

3D

NSA Playset Price Sheet

LEVITICUS - $50

OsmocomBB Phone for use with TWILIGHTVEGETABLE

- Motorola C139 phone
- Osmocom Cable

LEVITICUS

3D

NSA Playset Price Sheet

DRIZZLECHAIR - $100

A5/1 Rainbow Tables + Kraken for use with TWILIGHTVEGETABLE

- WD Elements 2TB USB 3.0 Hard Drive

DRIZZLECHAIR

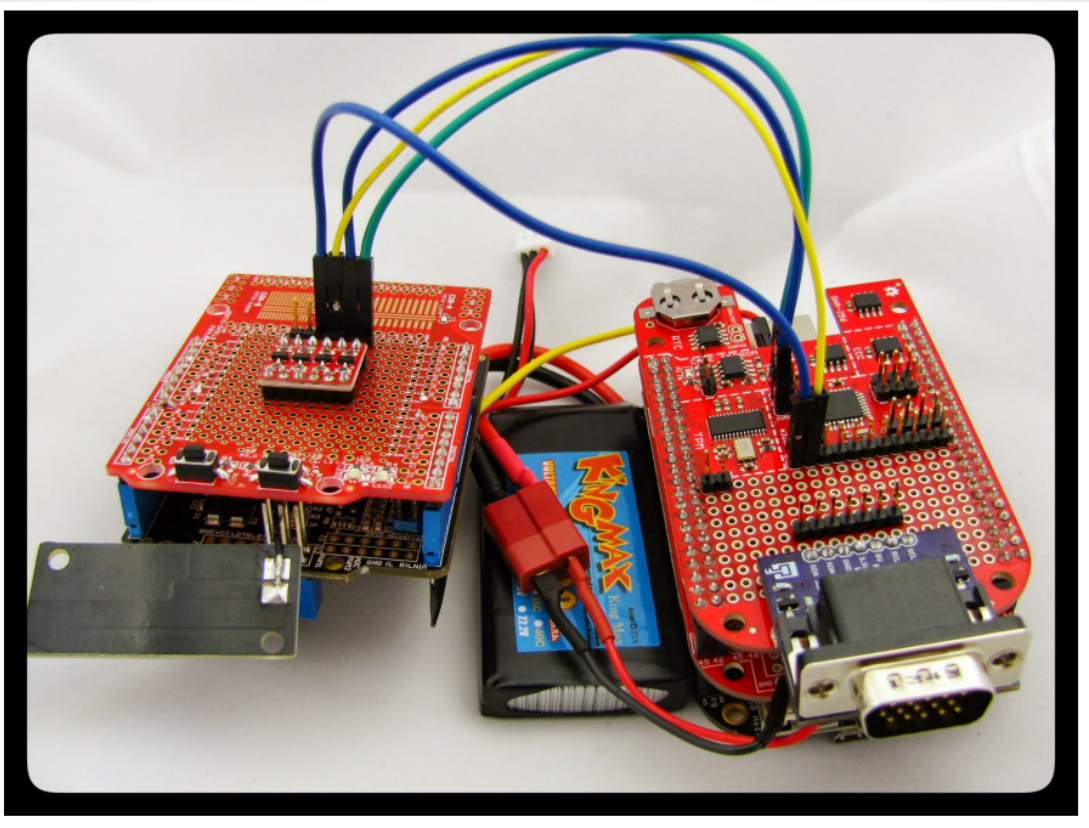
3D

NSA Playset Price Sheet

CHUCKWAGON - $25

I2C implant

CHUCKWAGON



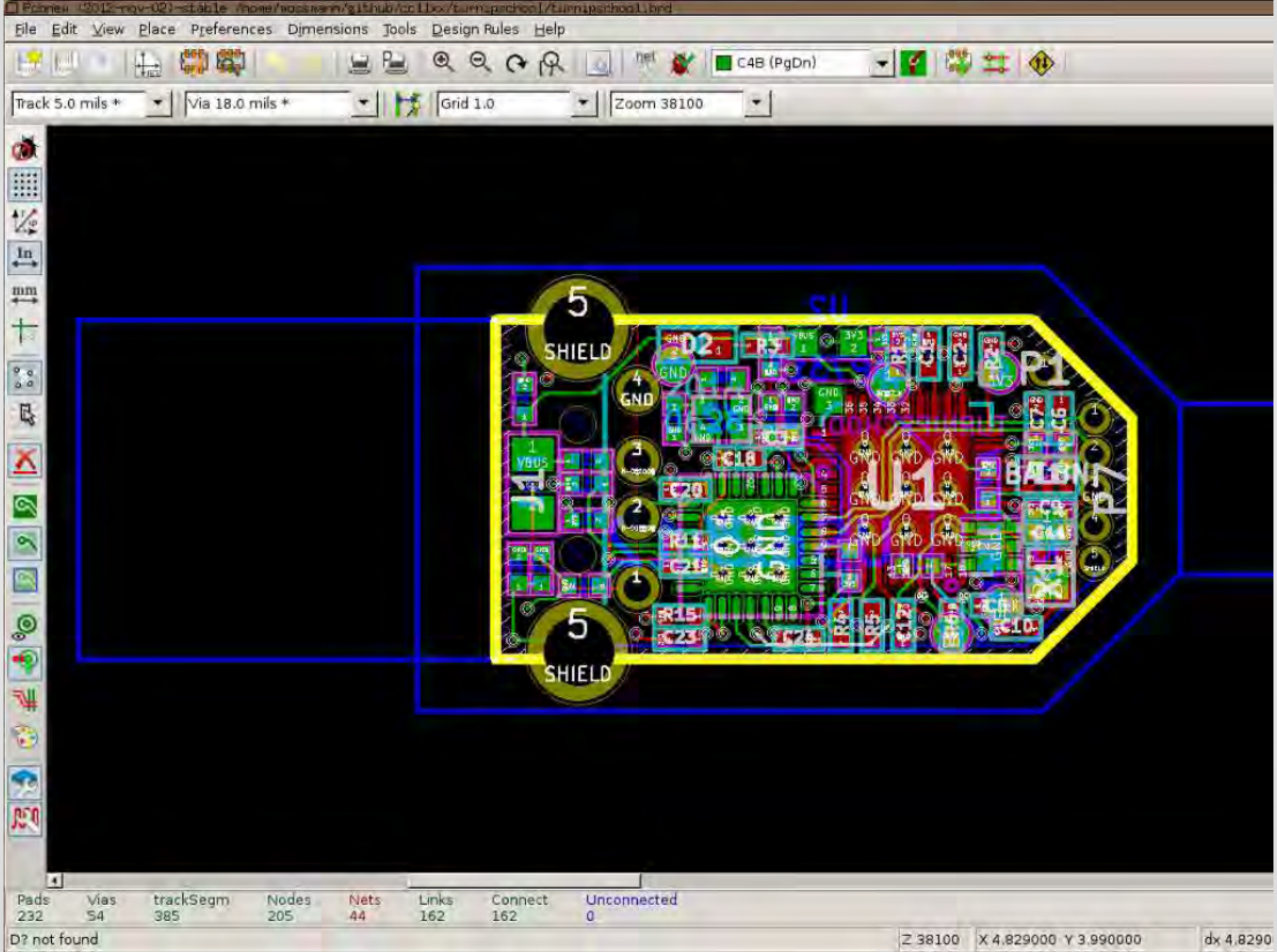
()

Upcoming Toys in the NSA Playset

NSA Playset Price Sheet

FLEABRAIN - $10

USB Cable implant that can store and transmit USB data


File Edit View Place Preferences Dimensions Tools Design Rules Help
C4B (PgDn)
Track 5.0 mils *
Via 18.0 mils *
Grid 1.0
Zoom 38100
SHIELD
GND
VBUS
U1
P1
BALUN
C18
C20
R15
C23
C10
Pads 232
Vias 54
trackSegm 385
Nodes 205
Nets 44
Links 162
Connect 162
Unconnected 0
D? not found
Z 38100
X 4.829000 Y 3.990000
dx 4.8290

3D

NSA Playset Price Sheet

DUCHESSRIDE - $45

USB Implant that allows for USB middling

DUCHESSRIDE

Our Favorite NSA Playset Toys:

NSA Playset Price Sheet

TINYALAMO - $10

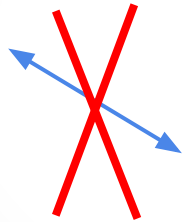
Bluetooth keystroke surveillance and injection

TINYALAMO

+ PyBT


Barbie
80 Learning activities
Try Me
Barbie
Barbie
Barbie


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA




Backspace
Tab
Caps Lock
Enter
Shift
Ctrl
Alt
Space
Escape
Insert
Home
Print Screen
Delete
End
Right
Down

()

TINYALAMO Demo!

NSA Playset Price Sheet

SLOTSCREAMER - $100

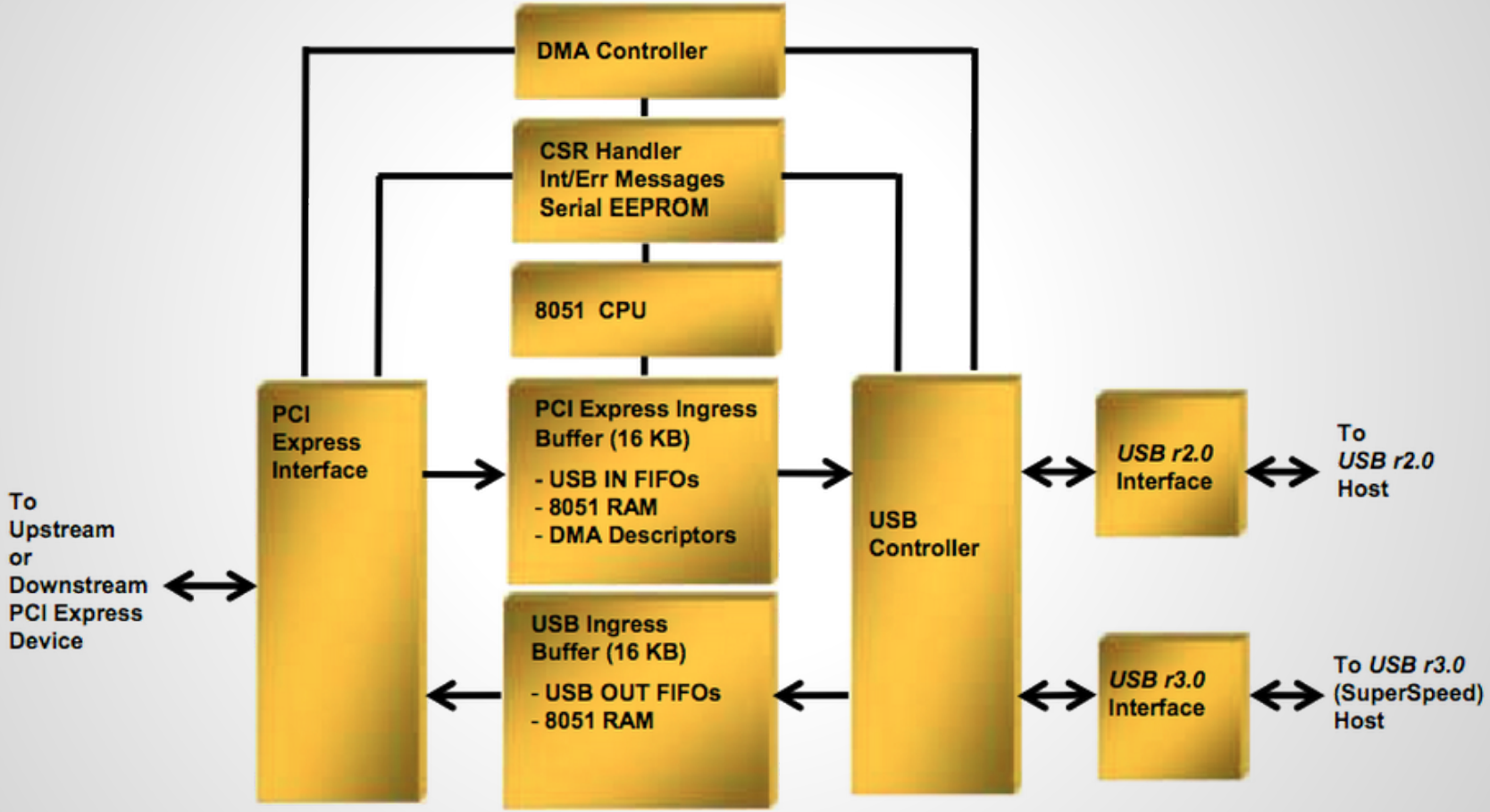
PCIe Attack Platform

- USB3380-AB Evaluation Board with custom firmware

SLOTSCREAMER Hardware

http://www.hwtools.net/PLX.html

Figure 1-1. USB 3380 Block Diagram



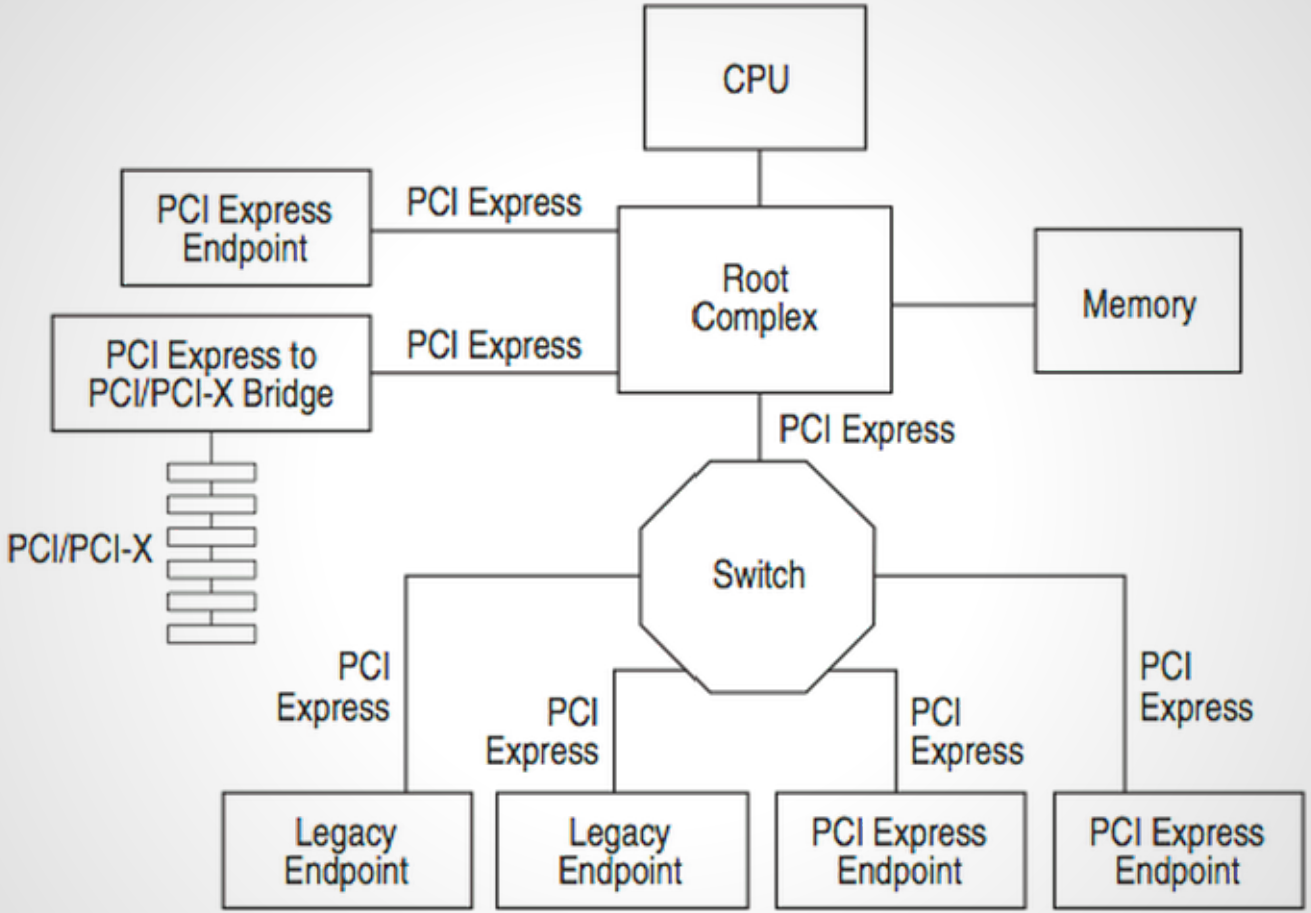


Diagram: PCIe 2.1 specification

NSA Playset Price Sheet

HALIBUTDUGOUT - $300

PCIe Attack Platform

- SLOTSCREAMER enclosed in a Thunderbolt Enclosure

HALIBUTDUGOUT

3D

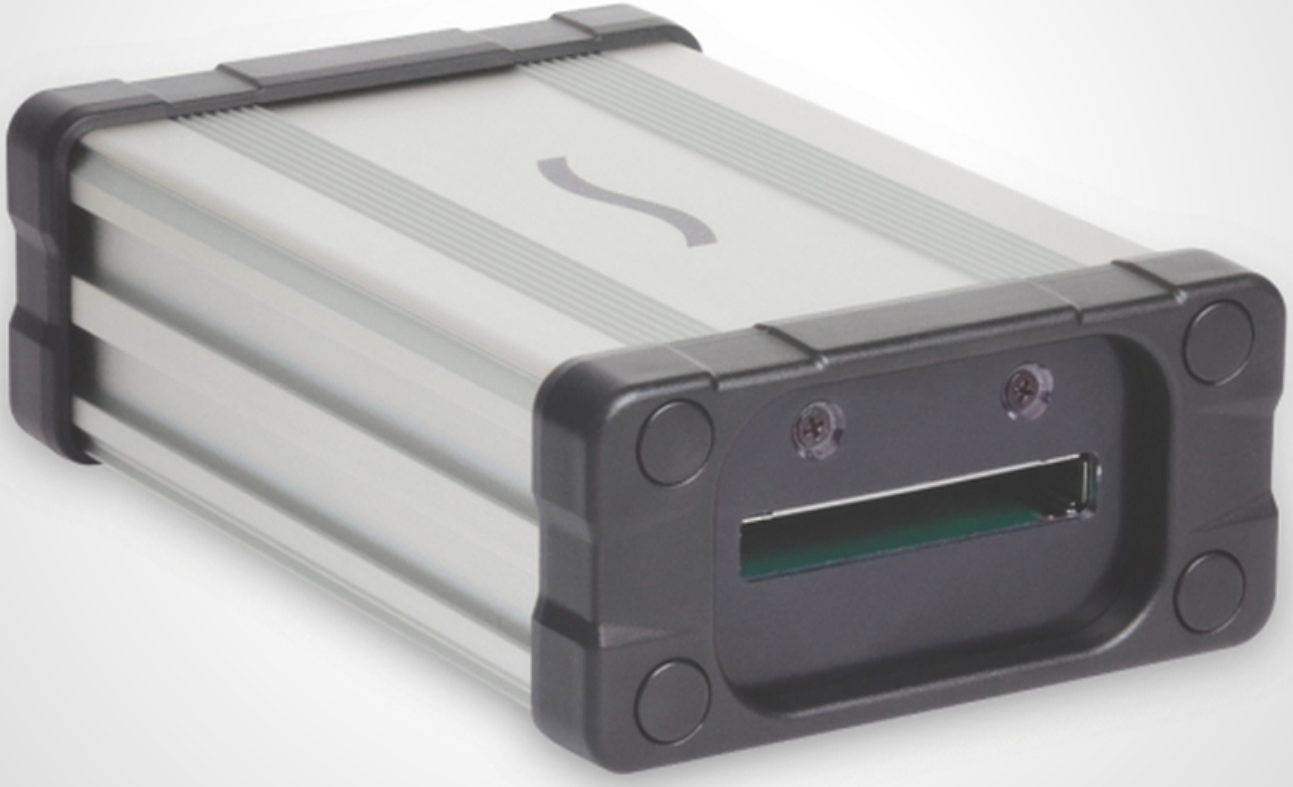
NSA Playset Price Sheet

GUPPYDUGOUT - $200

PCIe Attack Platform

- Expresscard SLOTSCREAMER in a tiny thunderbolt enclosure

GUPPYDUGOUT



3D

SLOTSCREAMER Demo!

Building ALLOYVIPER

3D

Building ALLOYVIPER

3D

Building ALLOYVIPER

3D

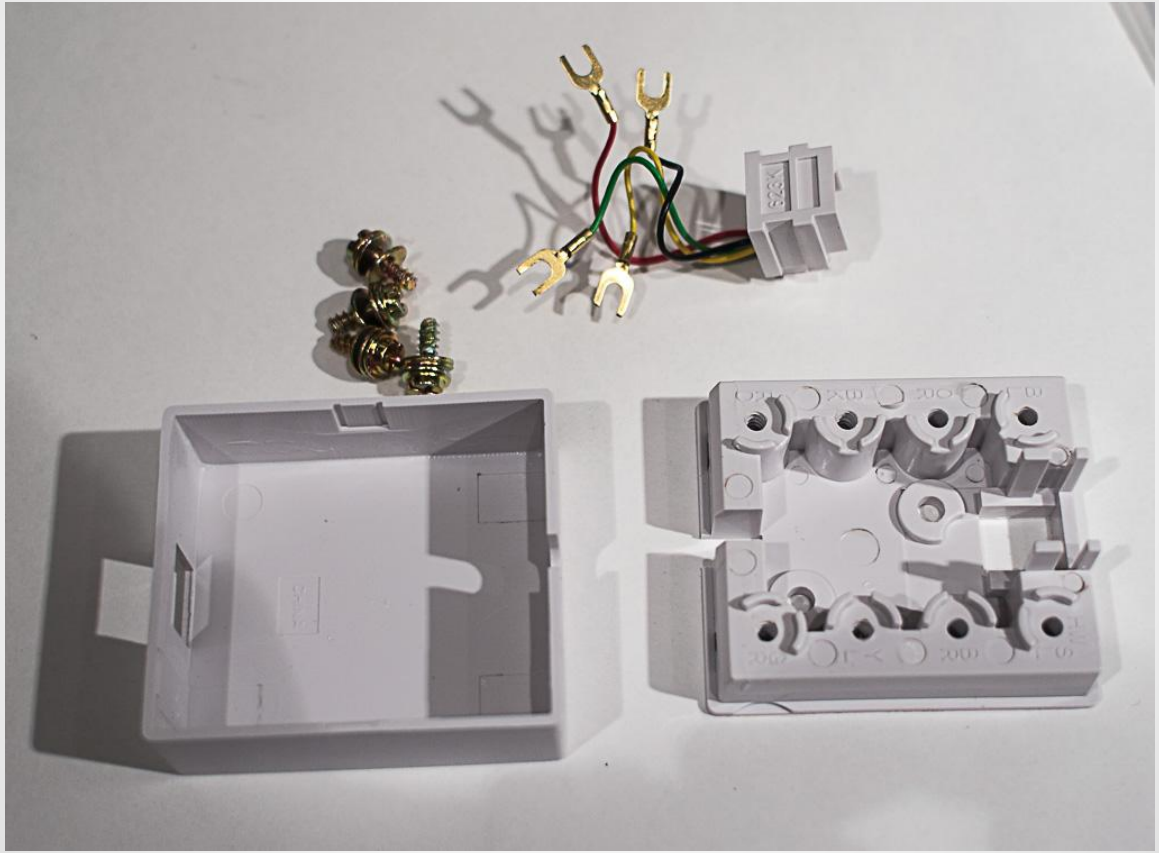
Building ALLOYVIPER

3D

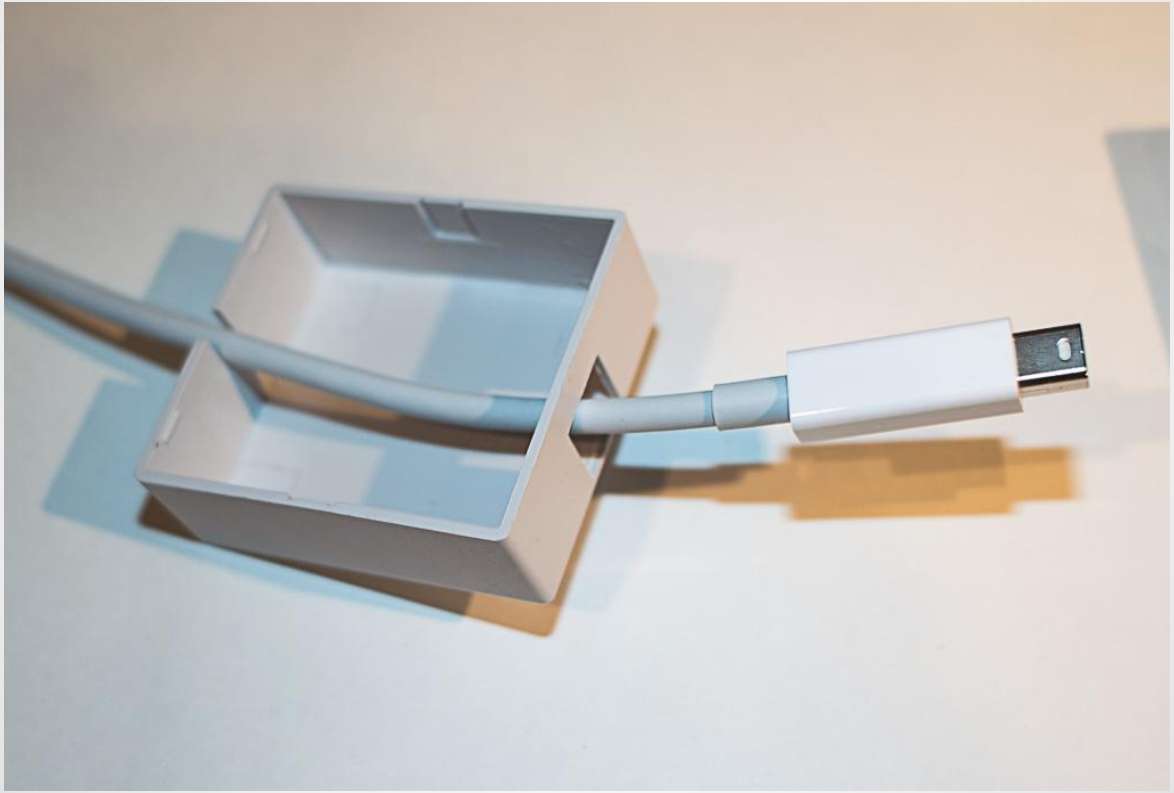
Building ALLOYVIPER

3D

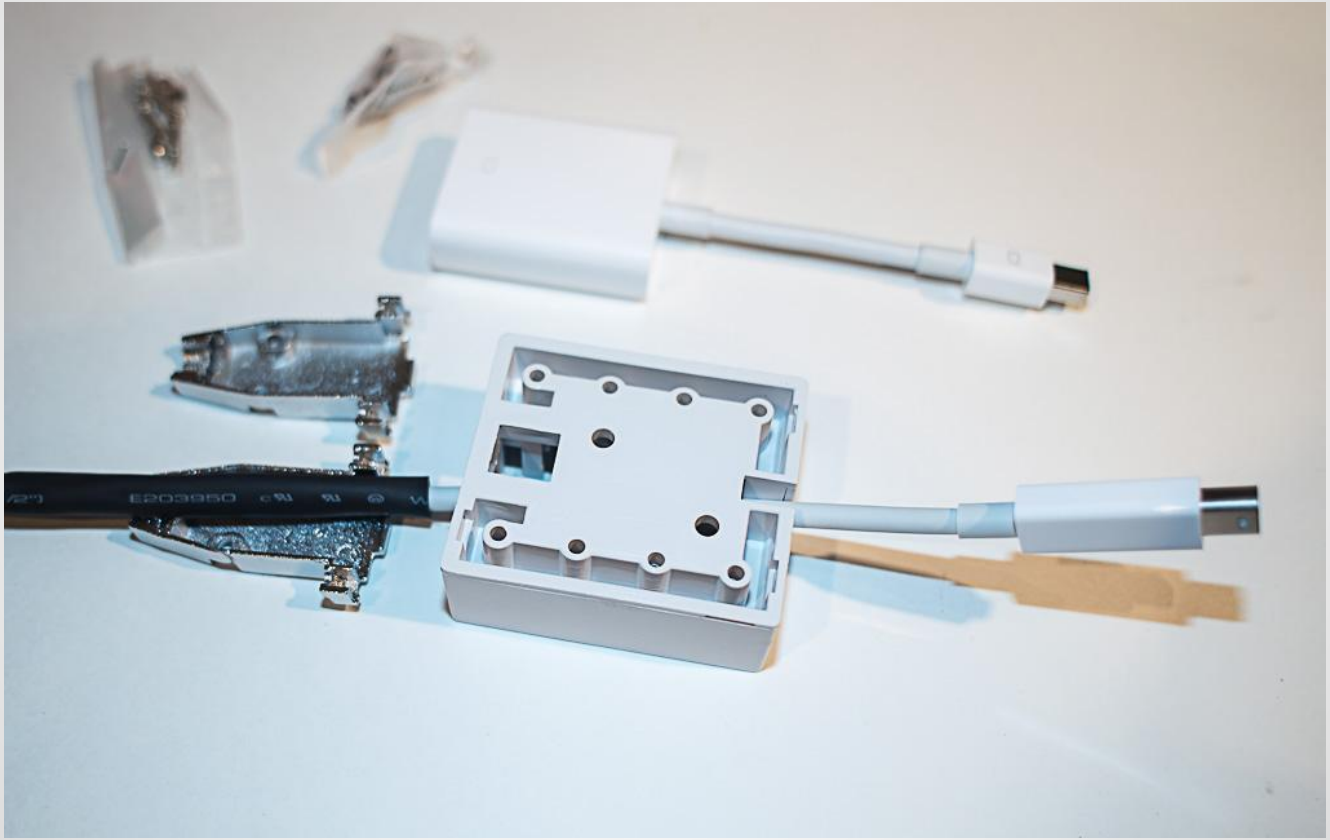
Building ALLOYVIPER



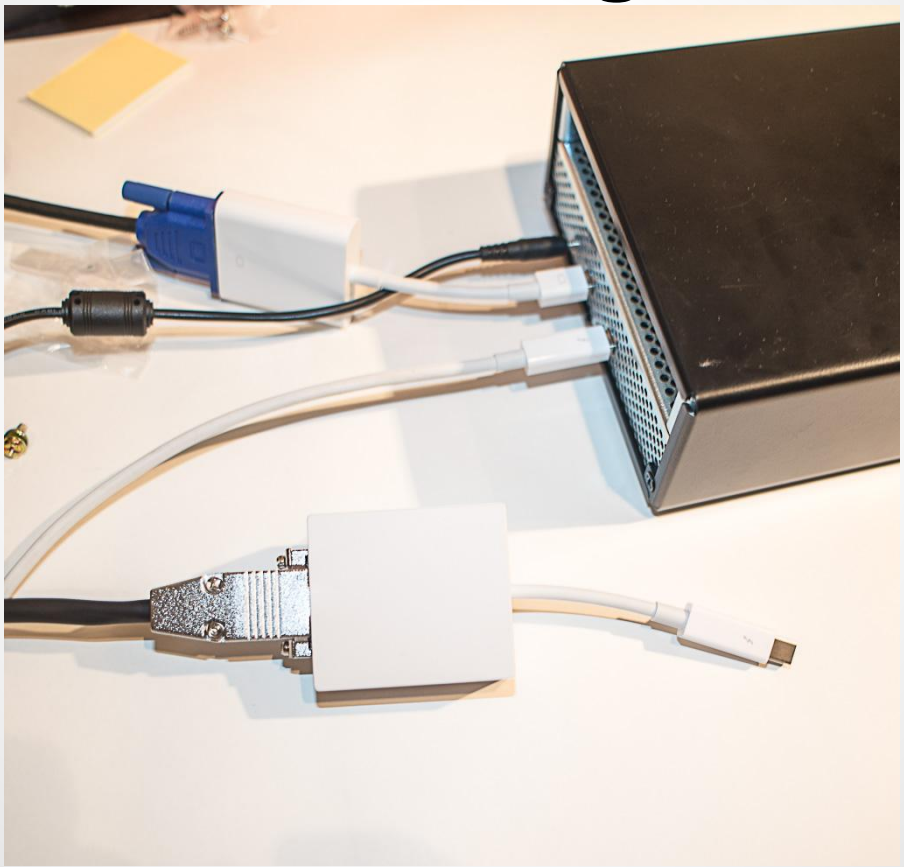
Building ALLOYVIPER



Building ALLOYVIPER



MITMing



NSA Playset Price Sheet

ALLOYVIPER - $50

PCIe Attack Platform

- Decoy cable for use with HALIBUTDUGOUT

Who?

Security Researchers

Hardware Hackers

Hardware Developers

Hobbyists

Other Nerds, Geeks, and Dorks*

An undercover agent or two*

Tinfoil hat wearers*

*presumed

But Why?

Intelligence agencies are not magic

But Why?

If the capability exists, designers need to know to protect against it

But Why?

‘Nation-state’ capabilities are out of scope.

Cheap DIY hacker tools should not be.

But Why?

If any 12-year old can do it,
the design flaw will be fixed

Questions?

Mike Ryan
@mpeg4codec
mikeryan@isecpartners.com
https://lacklustre.net

Joe FitzPatrick
@securelyfitz
joefitz@securinghardware.com
https://www.securinghardware.com