A Measured Response to a Grain of Rice

https://Securinghardware.com

Joe FitzPatrick
@securelyfitz

15+ years of hardware fun:

- silicon debug
- security research
- pen testing of CPUs
- security training

SecuringHardware.com:

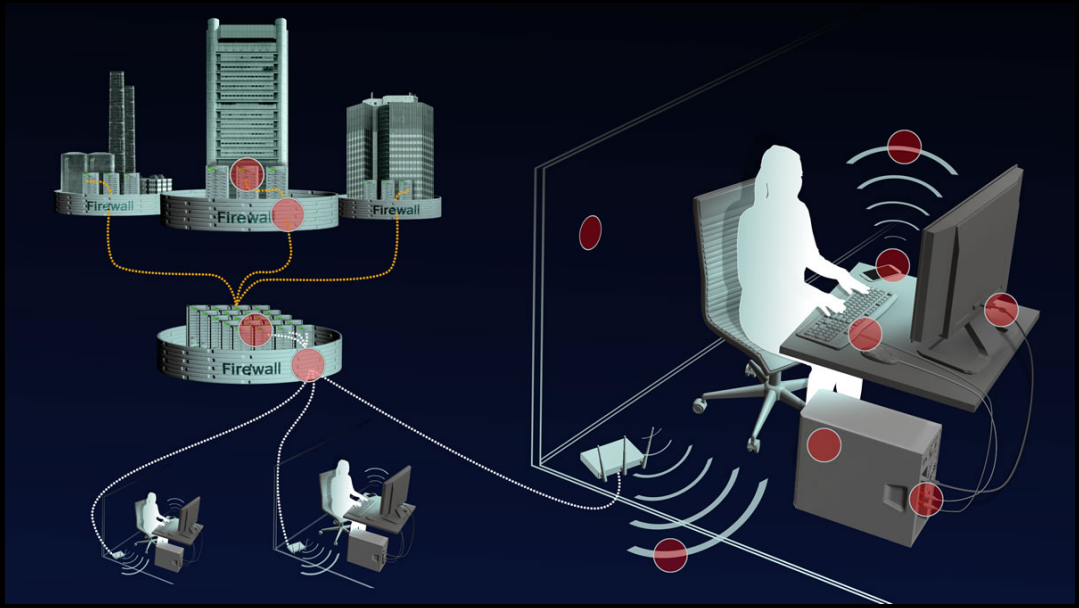
- Applied Physical Attacks Training
- HardwareSecurity.Training

Disclaimers!

What *is* a Hardware Implant?

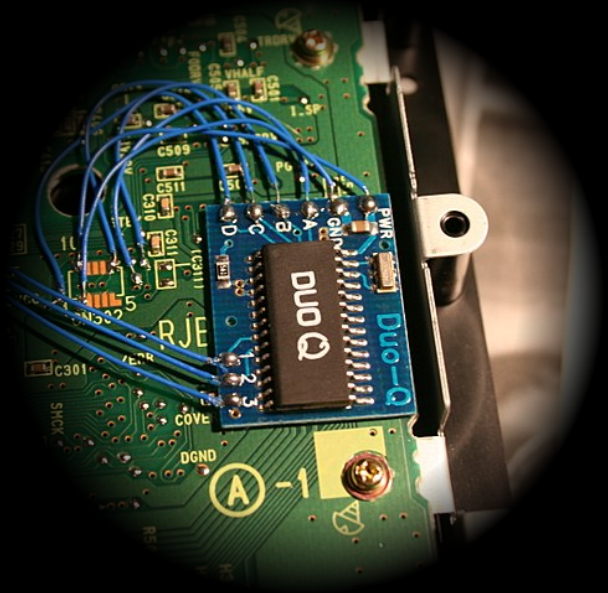
"Covert Implant"

"Hardware Implant"

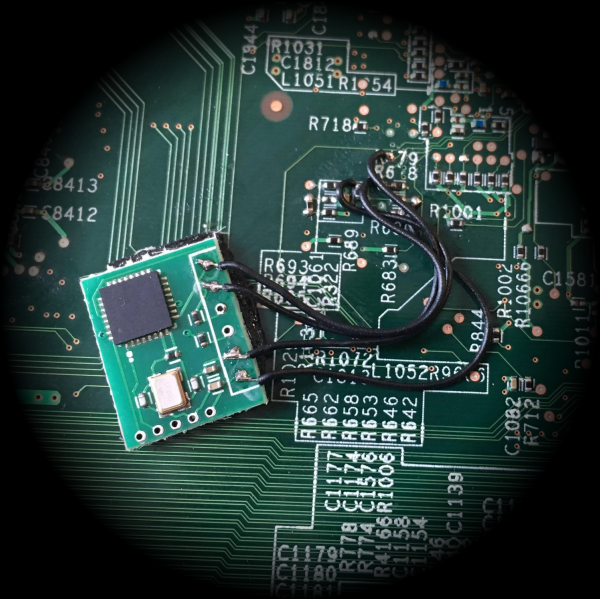


Keystroke loggers

Modchips

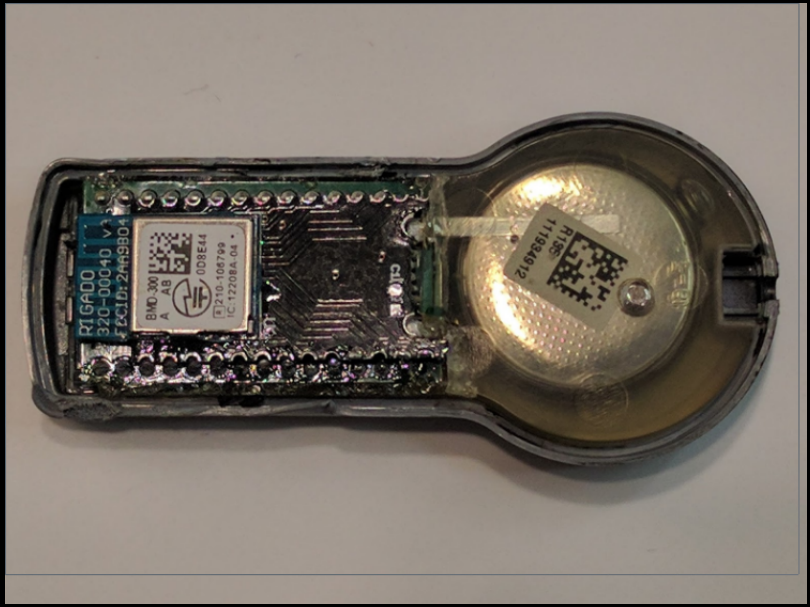

DuoQ
DuoQ
PWR
GND
DGND
C509
C511
C310
C301
IC3111
RJE
COVE
SHCK
A
-1

Counterfeit Bypass



Doobiekey

RSA Tokin


RIGADO
320-00040 V1
FCC ID: 2AHSBO1
BMD-300
A AB
0D8E44
FD130-106799
IC: 12208A-04
C1
C2
H195
11193401 2

Skimmers


r00t killah
@r00tkillah
Dismissing hardware attacks in your threat model is a mistake.
Adversary has ~$5 cost and low skill.
learn.sparkfun.com/tutorials/gas-...
8:50 AM · Sep 19, 2017

Evolution of USB hardware attacks

Keystroke Logger

USB Rubber Duckie

USB ATTACK PLATFORMS

NETWORK HIJACKING. KEYSTROKE INJECTION.

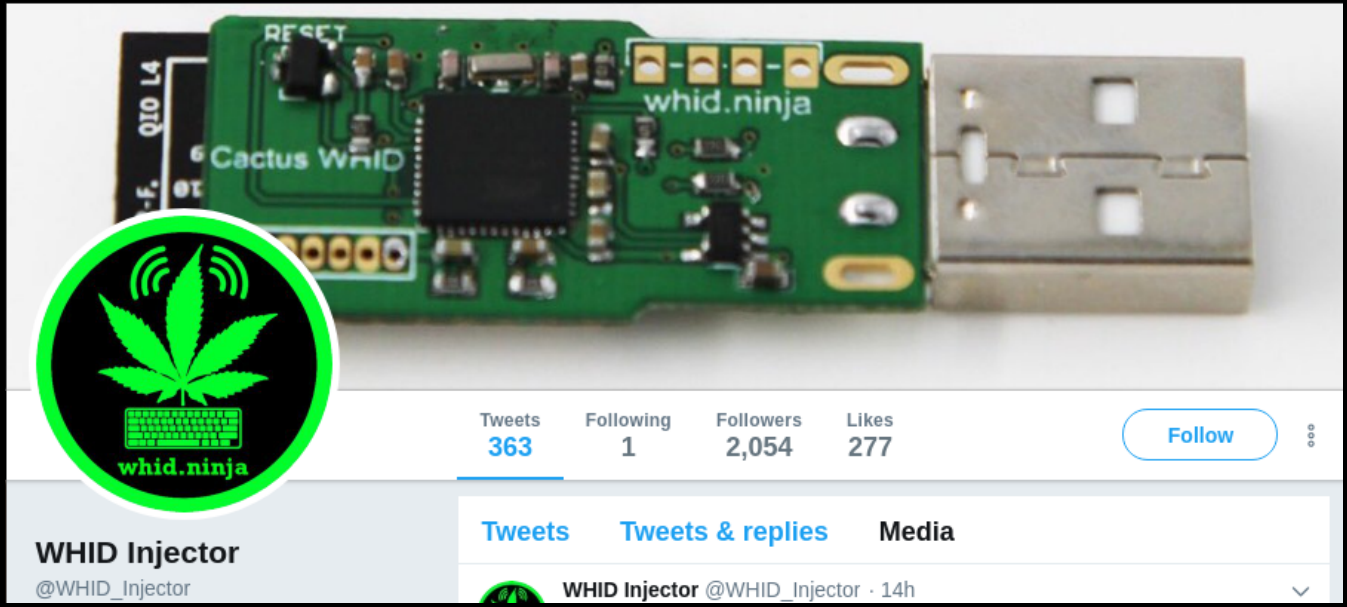
With the right tools and a few seconds of physical access, all bets are off.
Combining lethal power with elegance and simplicity.

Bash Bunny

USB Rubber Ducky

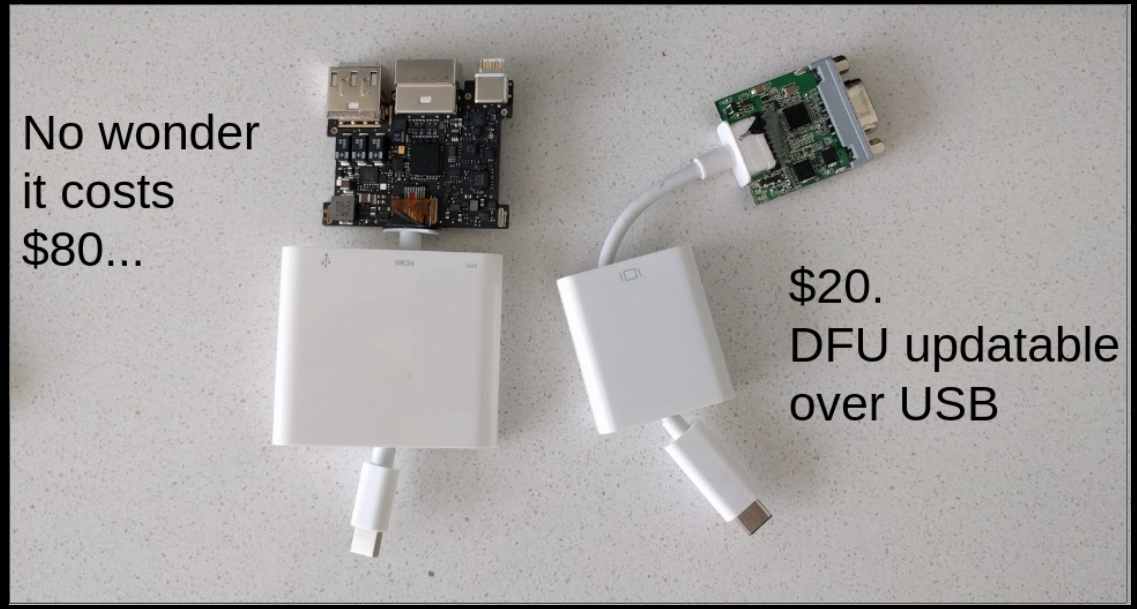
Physical Engagement USB Bundle

WHID injector



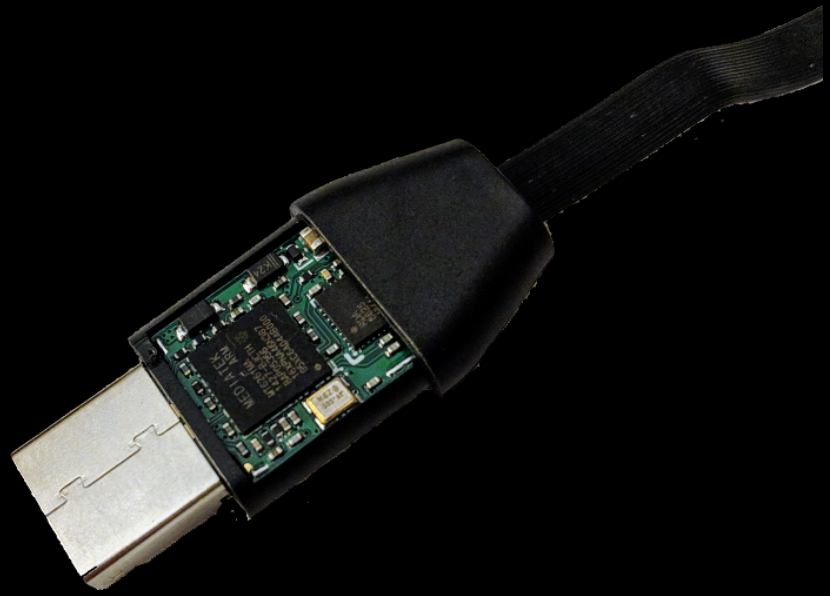
BADUSB

USB-C



Malicious Cables?

Decoupled attacks?



How do we connect a Hardware Implant?

USB or external ports

PCIe and internal ports

Tapping inter-chip communication

How many entry points do we have?

When do Hardware Attacks make sense?

Airtight Security Practices

Airgapped Systems

Heavily Monitored Networks

Supply Chain

Repudiation

Exfiltration

Vulnerable Hardware

Unpatchable Vulnerabilities

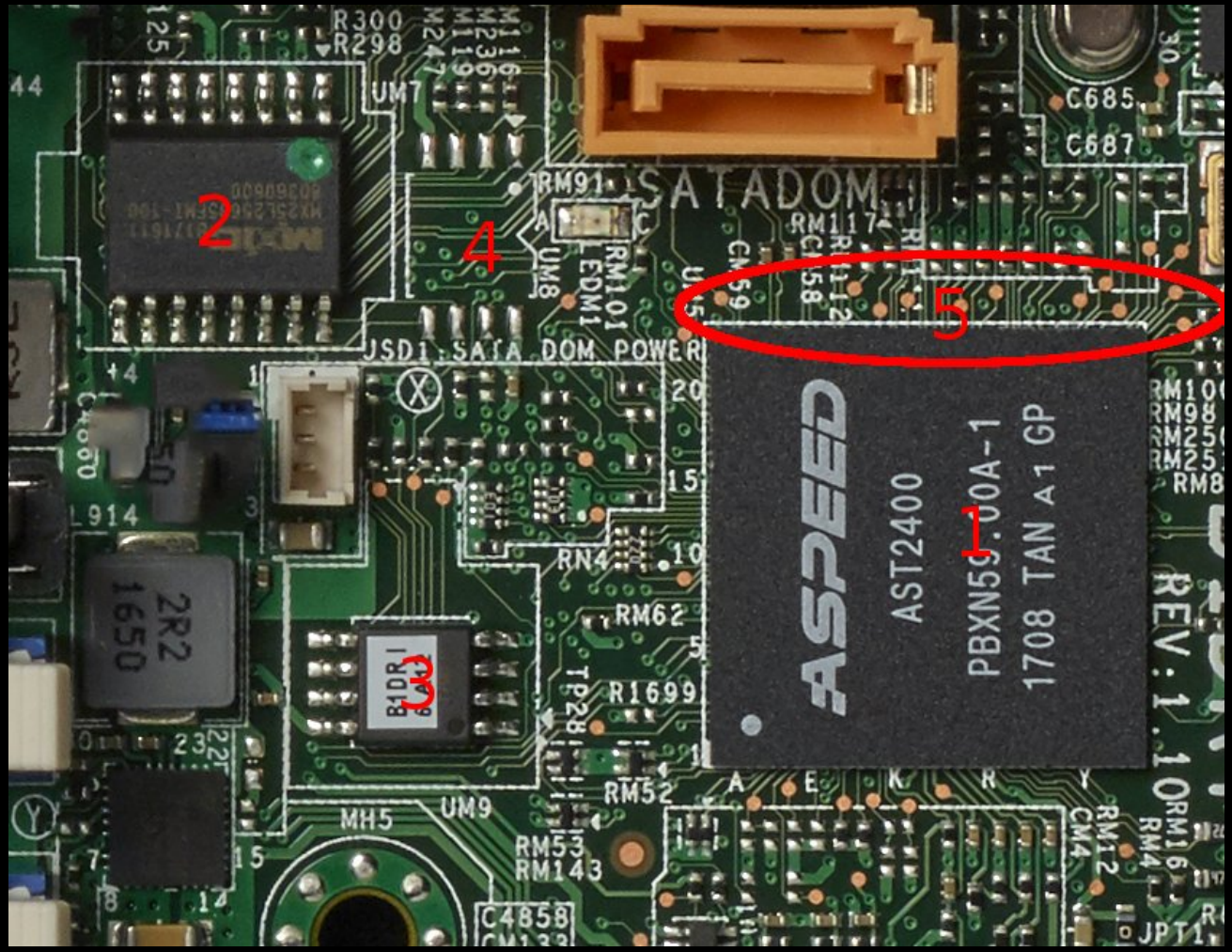
Lower detection at lower layers

Social Engineering with Hardware

Why is this relevant?


Bloomberg Businessweek
October 8, 2018
The Big Hack
How China used a tiny chip to infiltrate America's top companies

"This happened at a crucial moment, as small bits of the operating system were being stored in the board's temporary memory en route to the server's central processor, the CPU. The implant was placed on the board in a way that allowed it to effectively edit this information queue, injecting its own code or altering the order of the instructions the CPU was meant to follow. "


SATADOM
ASPEED
AST2400
PBXN59-00A-1
1708 TAN A1 GP
REV:1.1
JSD1 SATA DOM POWER
B1DR1
2R2
1650
1
2
3
4
5

Hardware Indicators of Compromise

Do you have grain-of-rice-sized components on your boards?

YES!

That's how they're made!

Do your boards exactly match the best schematics you can get of them?

NO?

ECOs, updates and revisions guarantee that

Do you have metal housings on your ethernet jacks?

YES?!

THEY ALL DO THESE DAYS

But... What do these implants do?

We still don't know!

But... What's the point?

Component Grafitti?

We have no useful information to help detection

Should we trust anyone who says they do?

Is this real?

I don't know.

Is this possible?

YES


SLOT4
LINE B

Much ado about hardware implants

Is this possible?

YES

But that's not the quesiton

SwiftOnSecurity
@SwiftOnSecurity

Following

Me: *talks to US gov hackers on their experiences*
Me: “How did Bloomberg find the only Chinese supply chain hacking story that wasn’t true.”

6:21 PM - 1 Nov 2018

119 Retweets **586** Likes

Why a coupler?

No firsthand accounts

No details about what it did...

"Having a well-done, nation-state-level hardware implant surface would be like witnessing a unicorn jumping over a rainbow"


I WANT TO
BELIEVE

You may say I'm a dreamer
But I'm not the only one

Expect lots of homebrew solutions at BHUS, Defcon, and in upcoming PoC||GTFO

How did we get here?

Spectre/Meltdown changed the landscape:

- Hardware vulnerability
- Software expliotable
- REAL response

Why do peple trust their hardware?

They don't know they shouldn't.

Would anyone listen without choreographed discosure?

So, Now that I have your attention:

Taking a measured response...

You can't find something that's not real...

You can look for it

That will distract you

A hardware implant is a compliment.

What *should* we worrry about?

Botnets for DDOS and Mining
Data Breaches
Randsomware

All for money and disruption

Hardware lets you bridge airgaps

Hardware lets you persist wipes

Hardware lets you show off your capabilities

What can we do about it?

Ripping up your servers is a waste of time.

Have you discussed supply chain security with your vendors yet?

Do you consider 5€ hardware attacks in your threat model? 100€?

Then why worry about 1M€ attacks?

What's the impact of an attack?

How common is that attack?

Risk = vulnerability * exposure

So What?

Hardware Attacks *are* a real threat...

...respond to the threat, not the hype

A Measured Response to a Grain of Rice

Joe FitzPatrick - @securelyfitz - joefitz@securinghardware.com