The Secret Life of Supply Chains

Security at the Hardware Level

Sophia d'Antoine

About this Talk

- Hardware Level Threats
- Discussed Techniques
  - Look at a few approaches for an attacker
  - What are the pros/cons on some of these, and relative difficulty
- Assessment Challenges
  - Some specific examples from our work in assessing these types of systems
- Helping Defend

All discussions of “Discussed Techniques” and attacks are based only on publicly available data.

Operation ShadowHammer & ShadowPad

MOTHERBOARD
TECH BY VICE

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

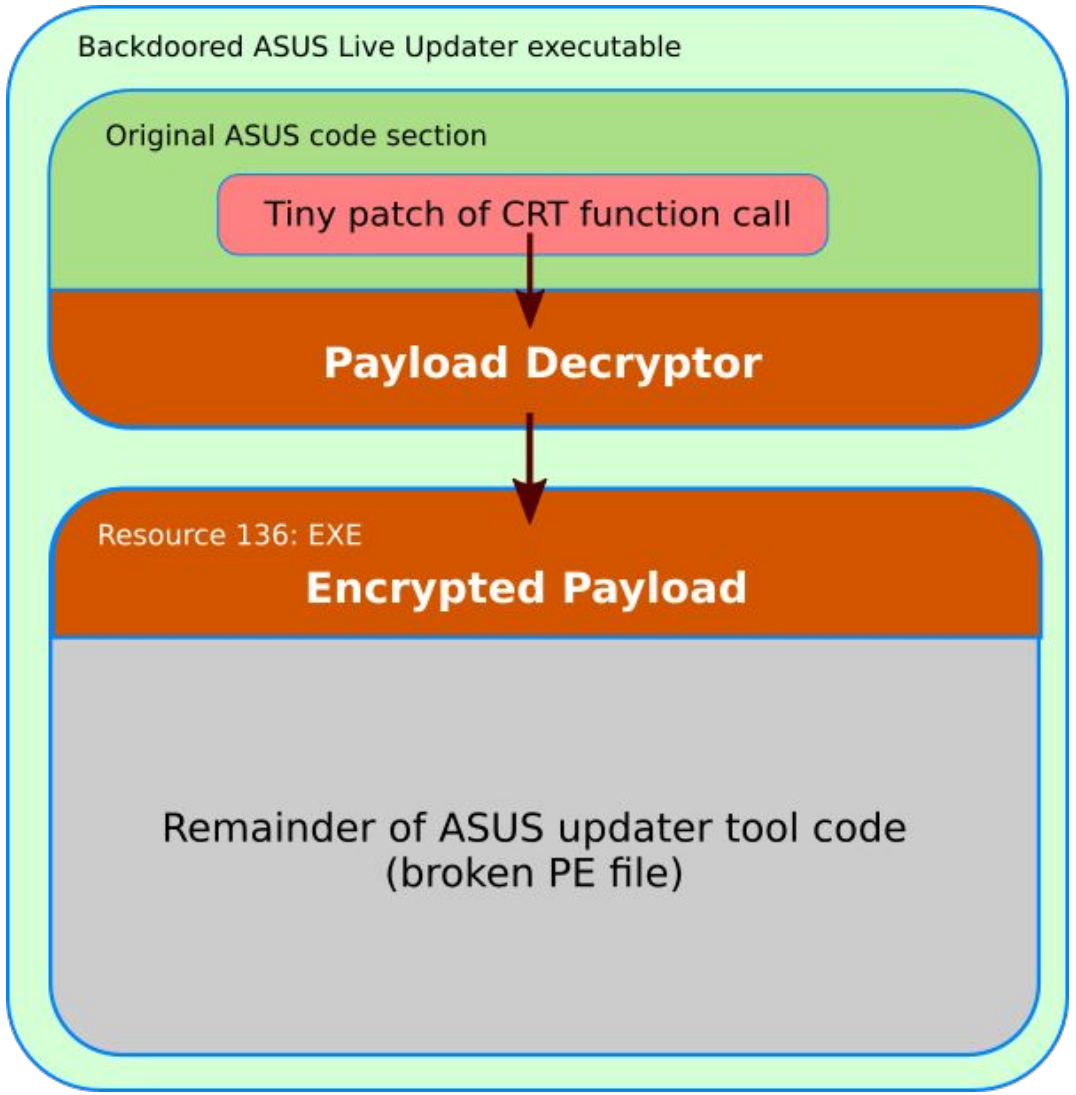
The Taiwan-based tech giant ASUS is believed to have pushed the malware to hundreds of thousands of customers through its trusted automatic software update tool after attackers compromised the company's server and used it to push the malware to machines.

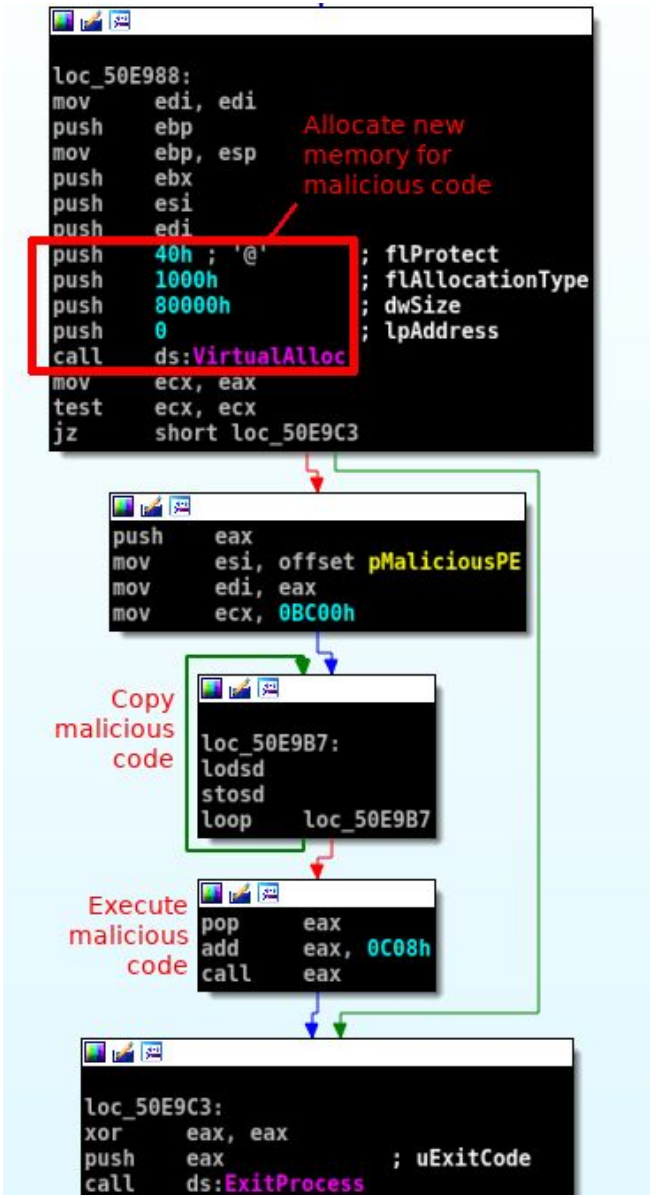
By **Kim Zetter**

Mar 25 2019, 9:00am Share Tweet

IMAGE: SHUTTERSTOCK

In Short





Source: https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/

In Short

August 15, 2017

ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World

ShadowPad is one of the largest known supply-chain attacks. Had it not been detected and patched so quickly, it could potentially have targeted hundreds of organizations worldwide.

Kaspersky Lab experts have discovered a backd
by hundreds of large businesses around the wo
download further malicious modules or steal d
affected software, and it has promptly removed the malicious code and released an update for customers.

ShadowPad is one of the largest known supply-chain attacks. Had it not been detected and patched so quickly, it could potentially have targeted hundreds of organizations worldwide.

Source: https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/

“The Big Hack”


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

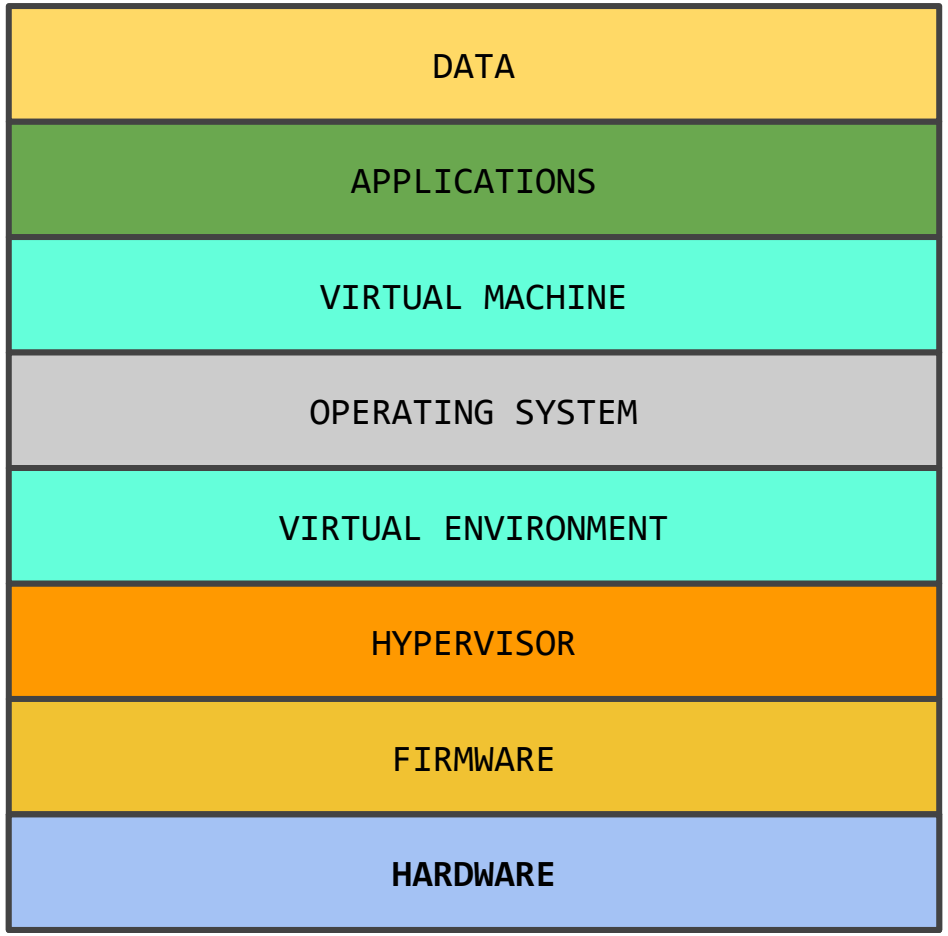
In Short

"The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources."

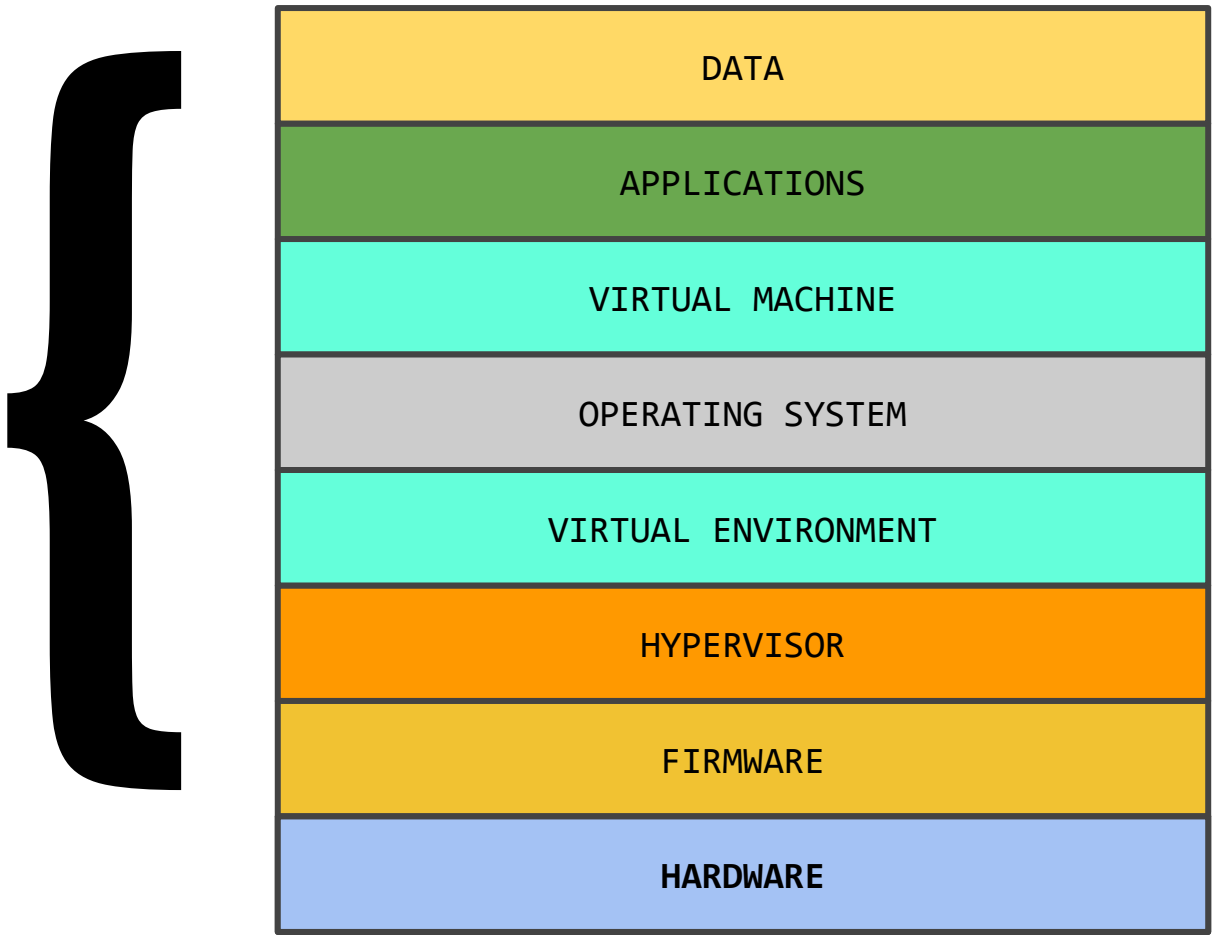
"The chips had been inserted during the manufacturing process, two officials say, by operatives from a unit of the People's Liberation Army."

Hardware Level Threats

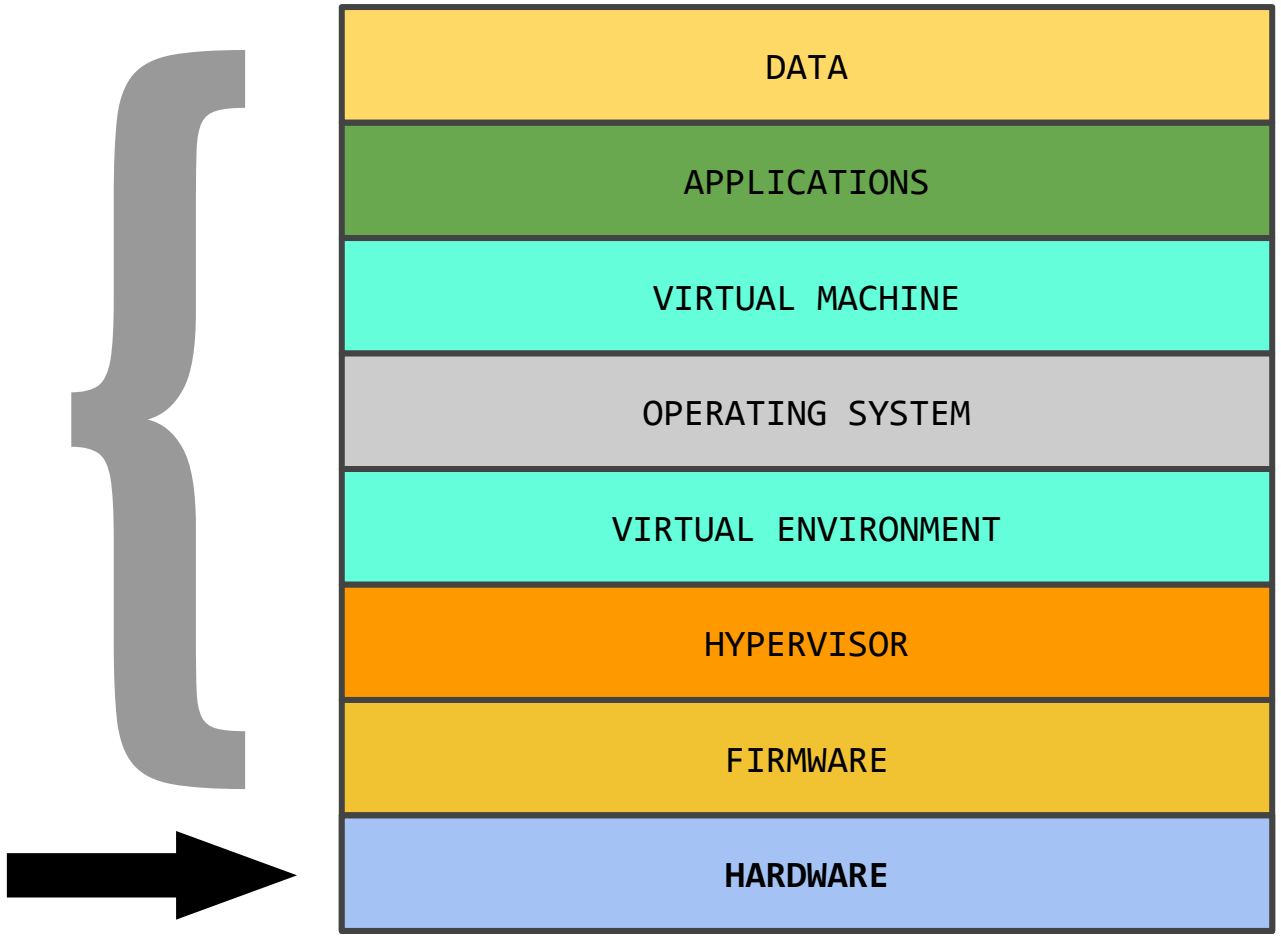
Narrowing our focus



Narrowing our focus



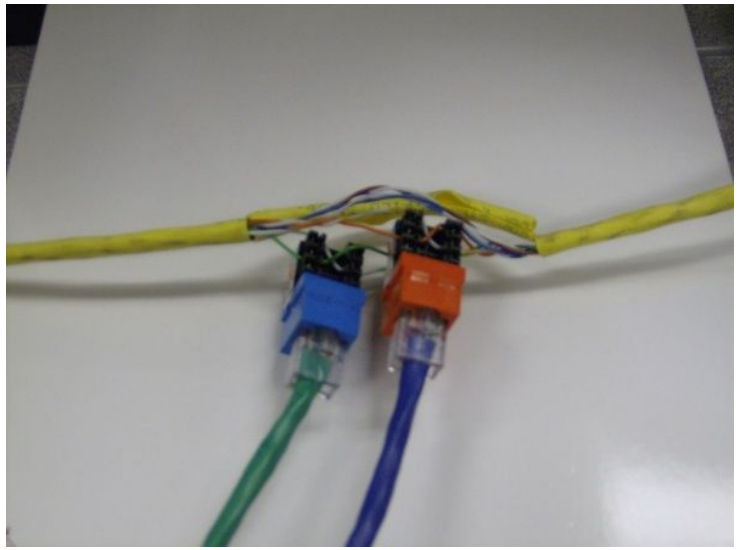
Narrowing our focus



General Categories of HW Threats

1. External Standalone Implants
2. External-Peripheral Implants
3. Internal-Peripheral Implants
4. Internal Implants (internal to the logic of a chip)
5. Software (Firmware) Implants ("bugdoors")

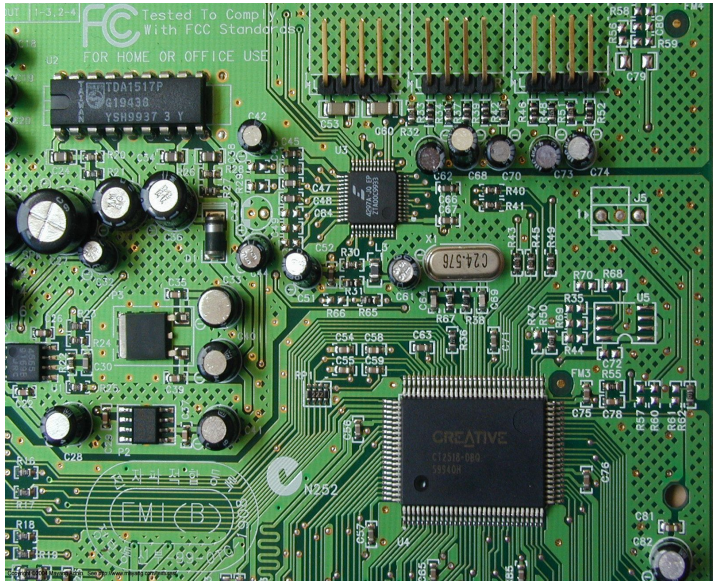
General Categories of HW Threats

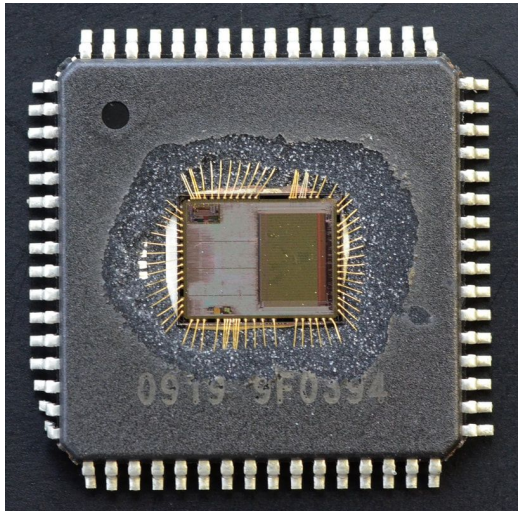


External

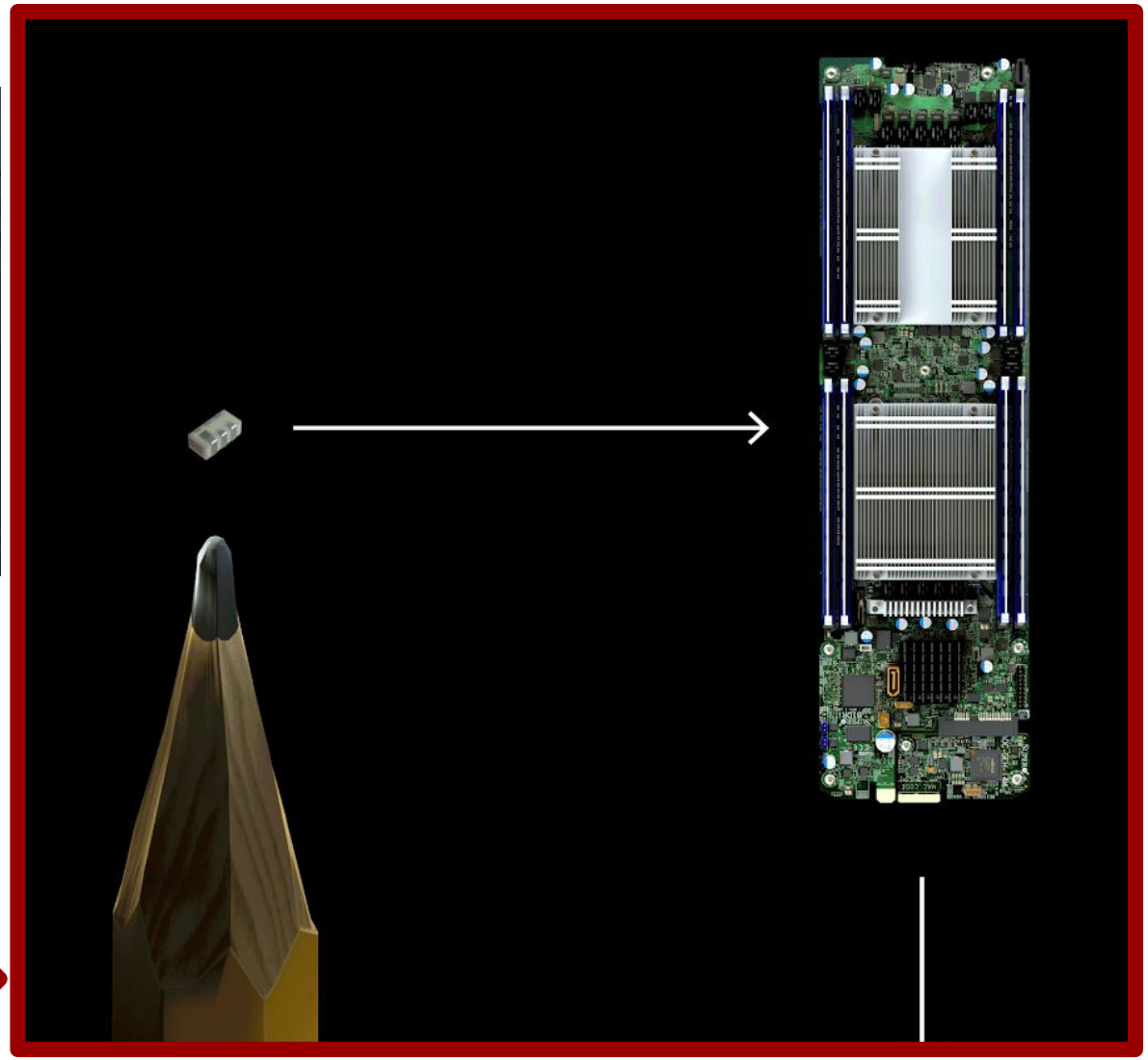
Physical peripherals

General Categories of HW Threats



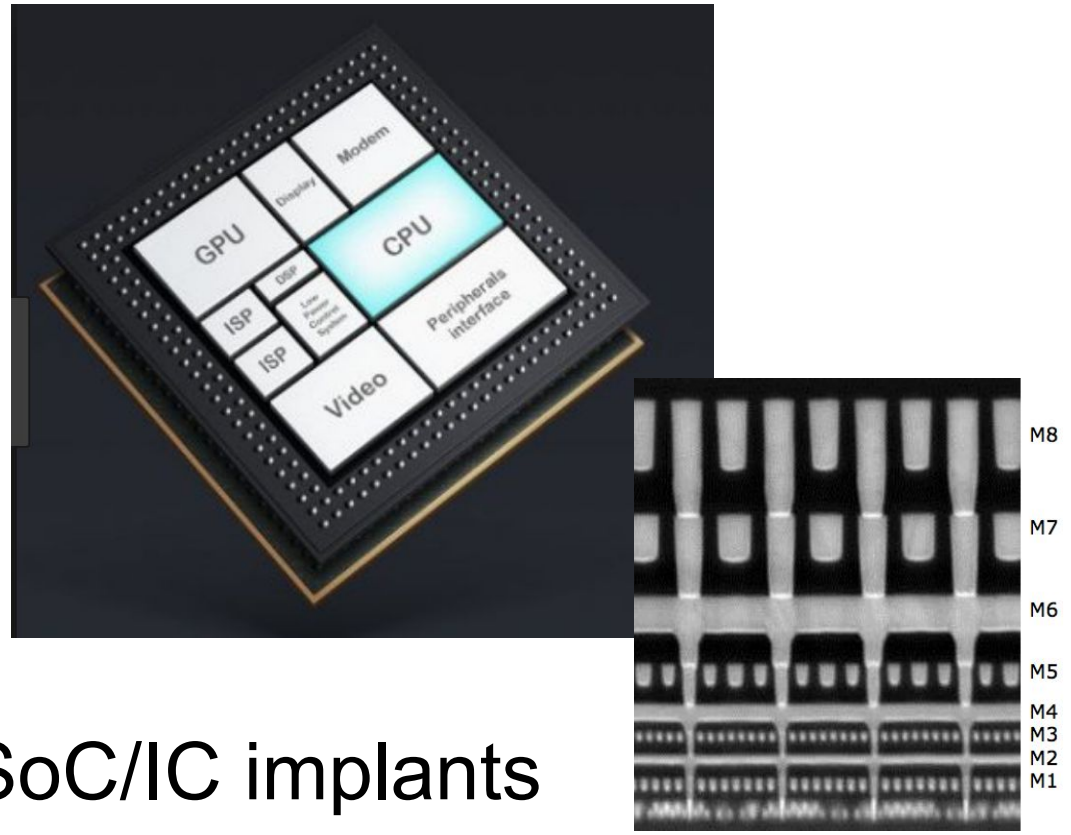


PCB implants



General Categories of HW Threats

- Within a single chip, tens or hundreds of vendors and manufacturers can have their "chips"
- Purchase or license the designs from another company (RTL Silicon design files i.e. ARM)
- HW equivalent to imported libraries
- Formal verification possible here



SoC/IC implants

General Categories of HW Threats

Firmware implants

“most hardware implants are likely attempting to facilitate or perform some modicum of software backdooring”

Discussed Techniques

Bloomberg “The Big Hack”

Regardless of if the alleged incident(s) happened, the claims shed light on what may be possible:

- Additional microchip: “Nested on the servers’ motherboards, the testers found a tiny microchip, not much bigger than a grain of rice, that wasn’t part of the boards’ original design”
- Grey or off-white in color
- Intercept CPU temporary memory: “manipulated the core operating instructions [...] as small bits of the operating system were being stored in the board’s temporary memory en route to the server’s central processor”
- “could do all this because they were connected to the baseboard management controller”
- “Signal Conditioning Coupler with memory, processing, networking capabilities”
- Altered operating system
- Embedded between PCB layers: “were thin enough that they’d been embedded between the layers of fiberglass”

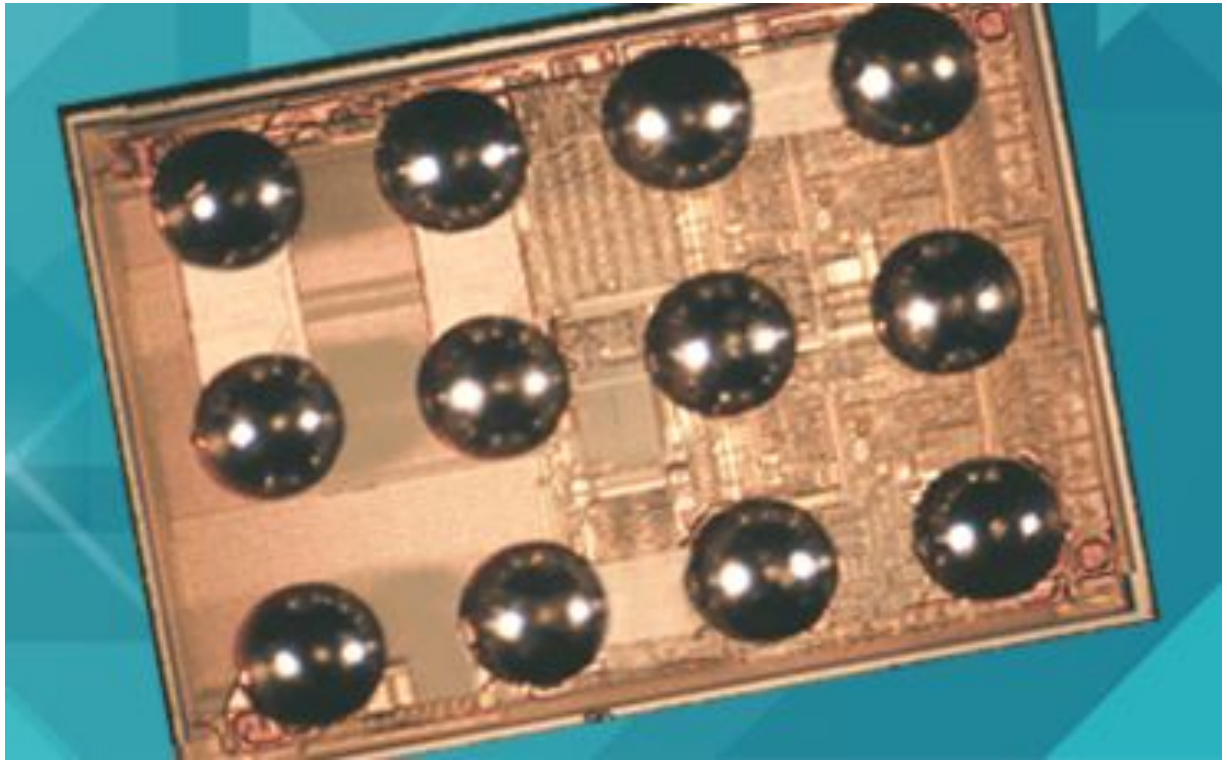
Bloomberg “The Big Hack”

Regardless of if the alleged incident(s) happened, the claims shed light on what may be possible:

- Network-related:
  - “Signal Conditioning Coupler with memory, processing, networking capabilities”
  - Found via suspicious network activity
  - “downloaded firmware [...] had been altered”
  - “The malware was on a network card driver”
  - “implant built into the server’s Ethernet connector”
  - “appeared on the network as two devices in one”
  - “Ethernet connector has metal sides instead of the usual plastic ones”

“The Sandwich”

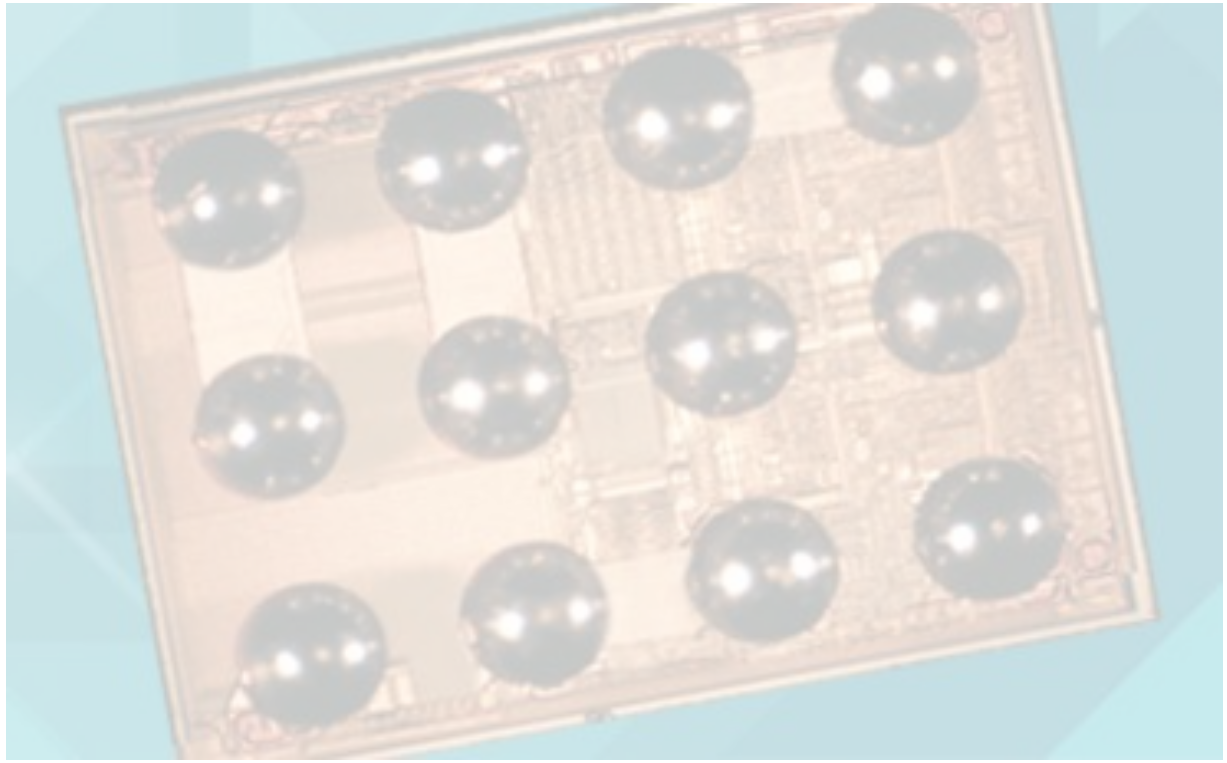
“[Company] offers Wafer Level Chip Scale Packaging (WLCSP), providing a solder interconnection directly between the device and end product’s motherboard”

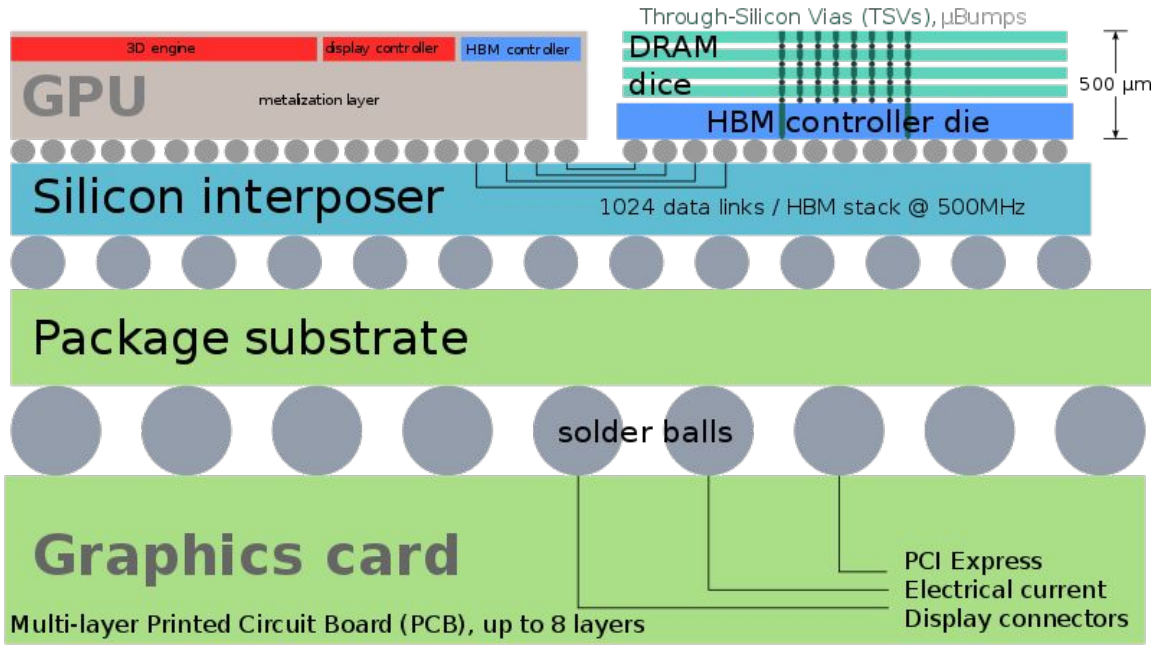


https://amkor.com/packaging/wafer-level-packaging/wlcsp/

“The Sandwich”

https://en.wikipedia.org/wiki/Through-silicon_via#3D_packages





Intel unveils new 3D chip packaging design

Intel's new chip packaging design doesn't sound exciting, but it is important for server processor technology.

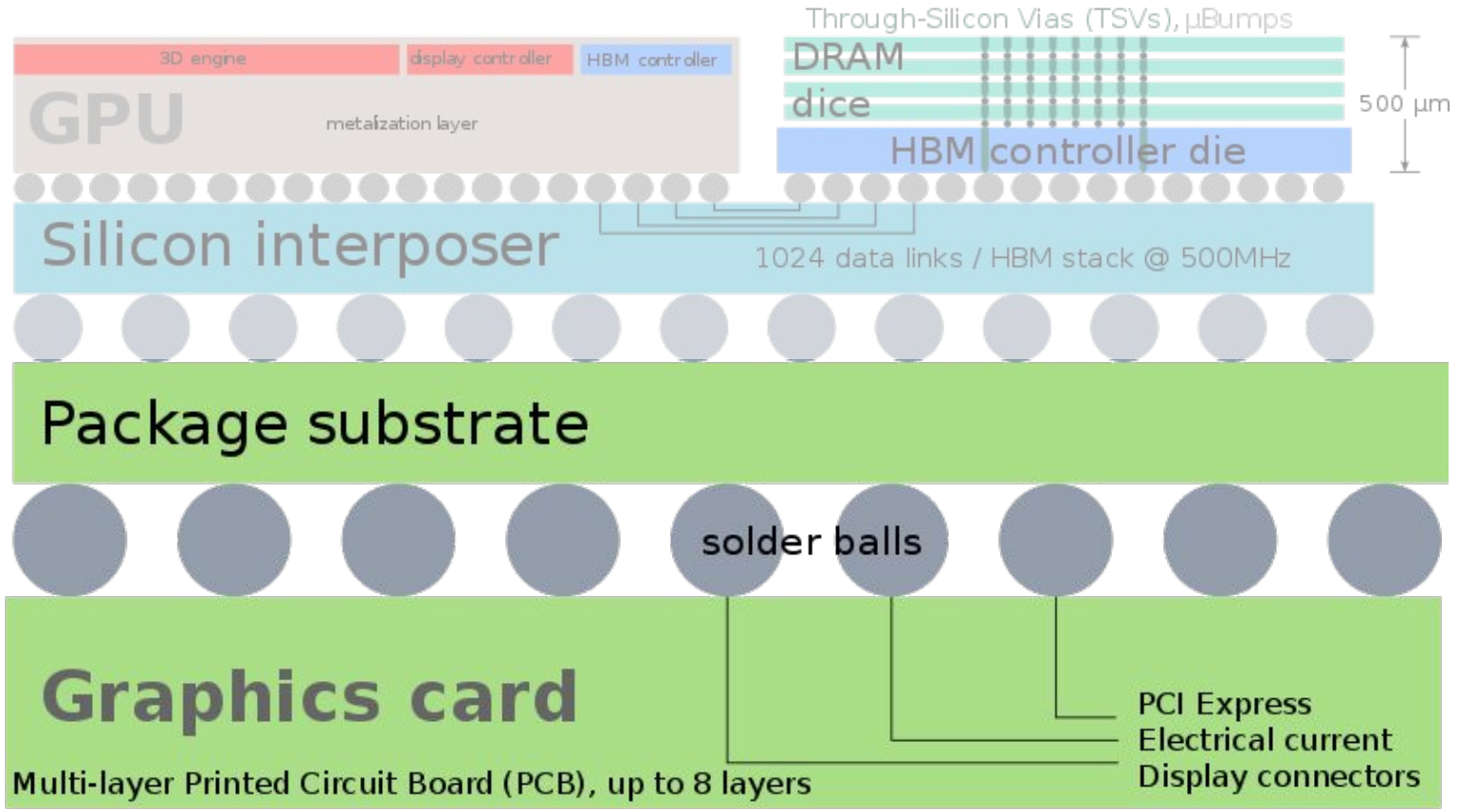
Circuit security

3D integration can achieve security through obscurity; t

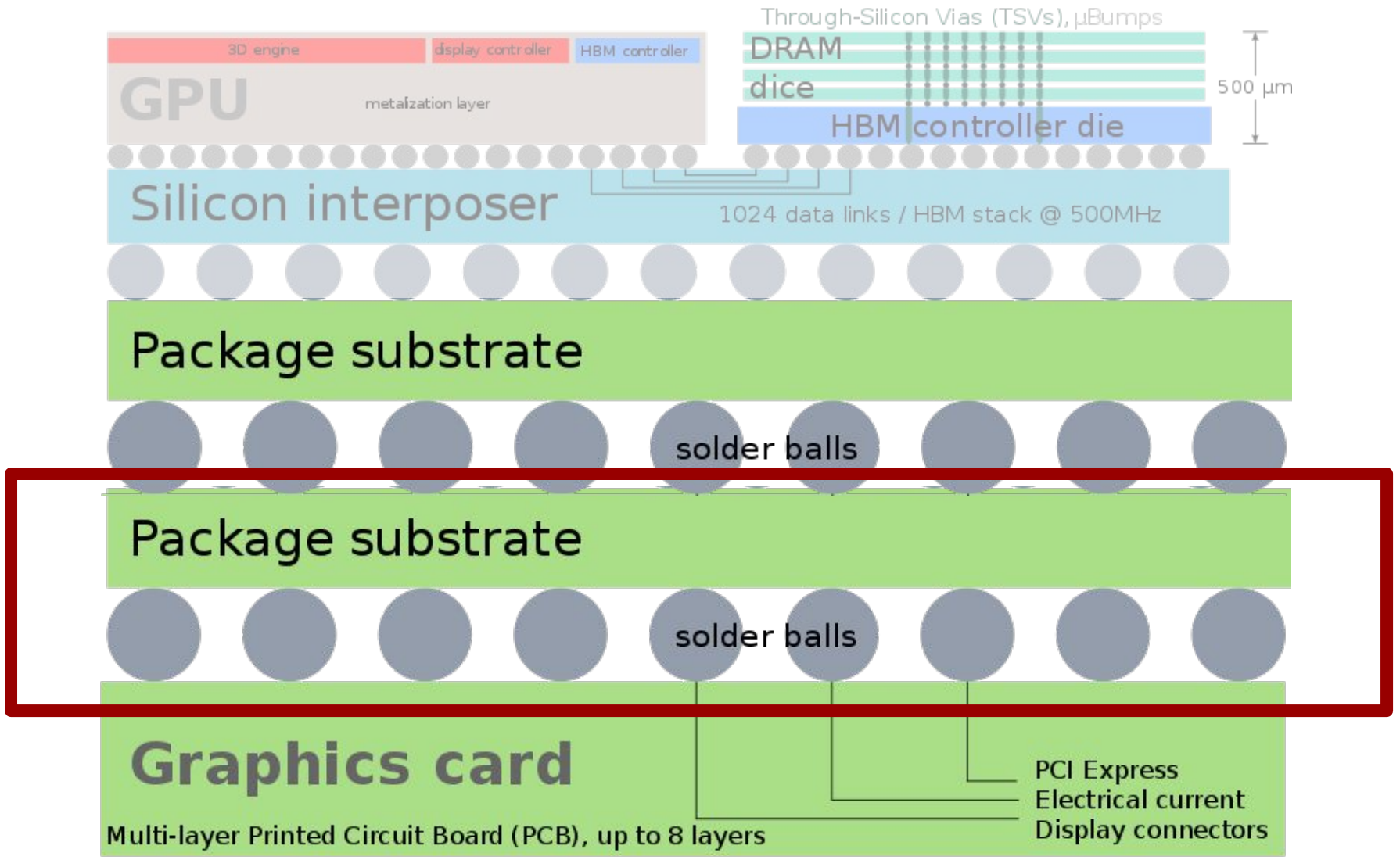
“The Sandwich”

WLCSP + TSV are useful, legitimate, technologies.

But an attacker can use them



“The Sandwich”



“The Add”

- On a Board?
- Can be legitimate: e.g.: move a component from one pad to another
- Availability of different package sizes
- Slight difference in board design - stability, specs, etc.

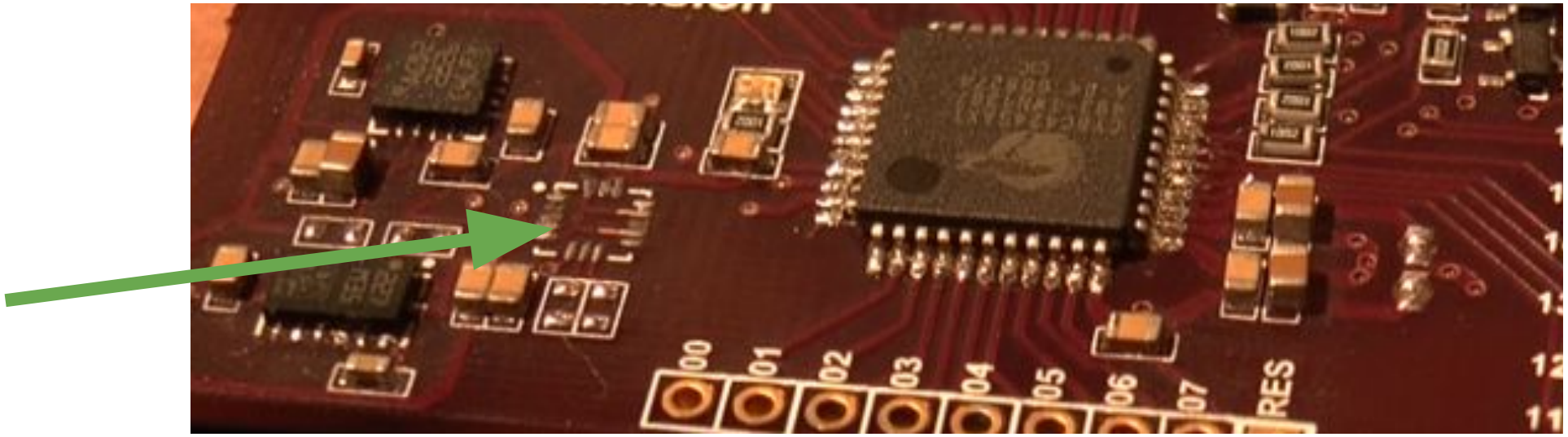


Image from https://www.eevblog.com/forum/projects/why-leave-empty-(unpopulated)-spaces-on-a-pcb/

“The Add”

- Inside a Package?
- Can be legitimate: e.g.: flash memory package
- Sold but has different configurations, or different memory internally
- Wirebond down differently

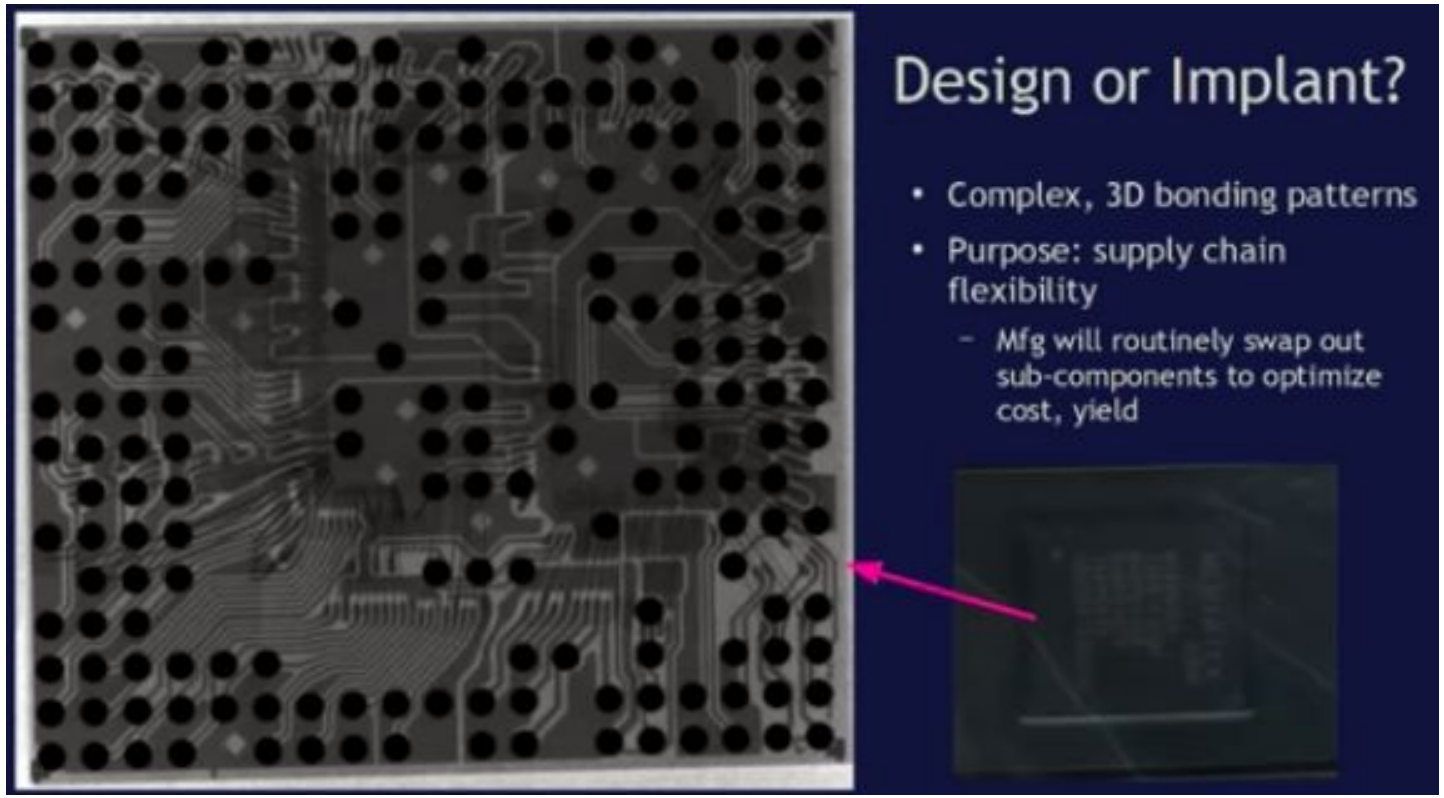


Image credit bunnie Huang @20:40 of https://www.youtube.com/watch?v=RqQhWitJ1As

“The Swap”

Trammell Hudson’s example of replacing a 0603 passive with an implant on a motherboard SPI flash to BMC link is just one example…

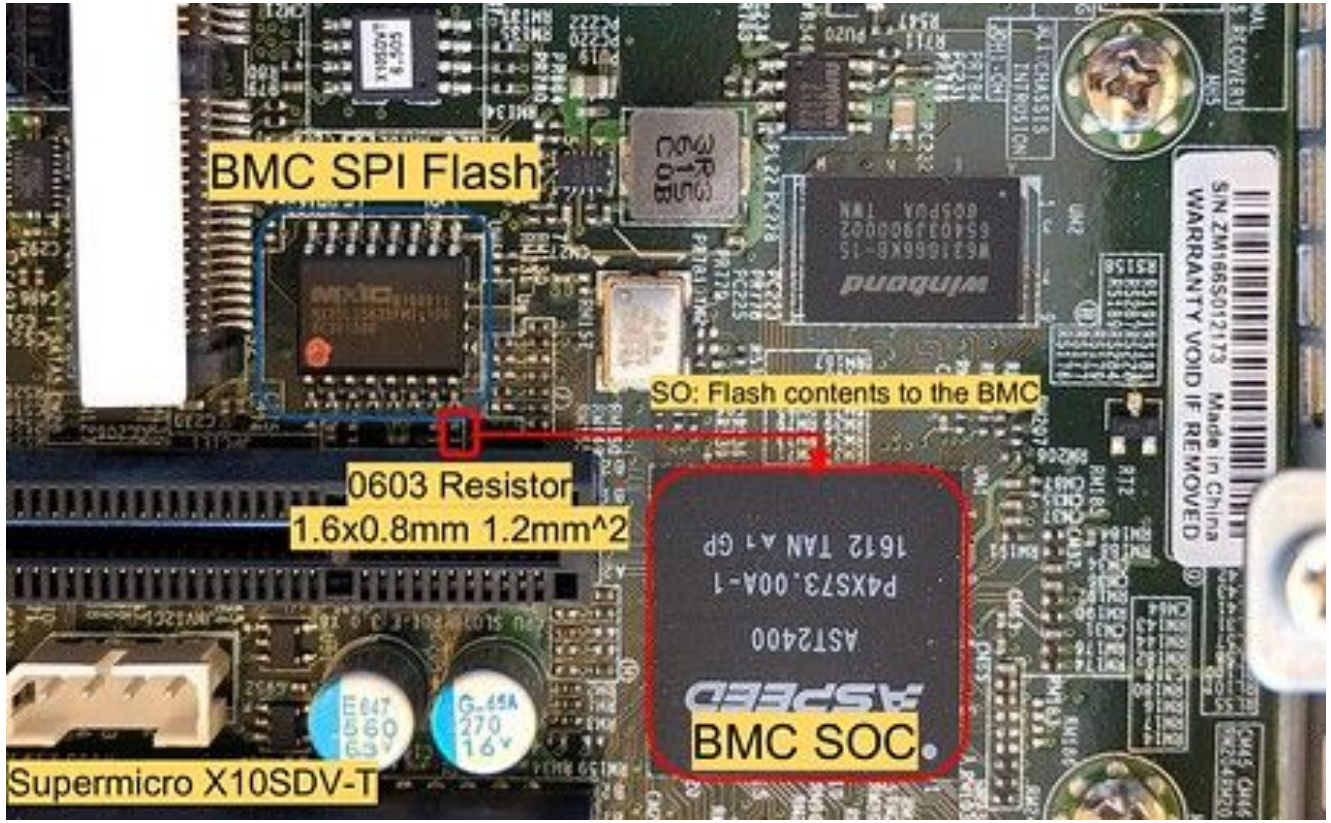
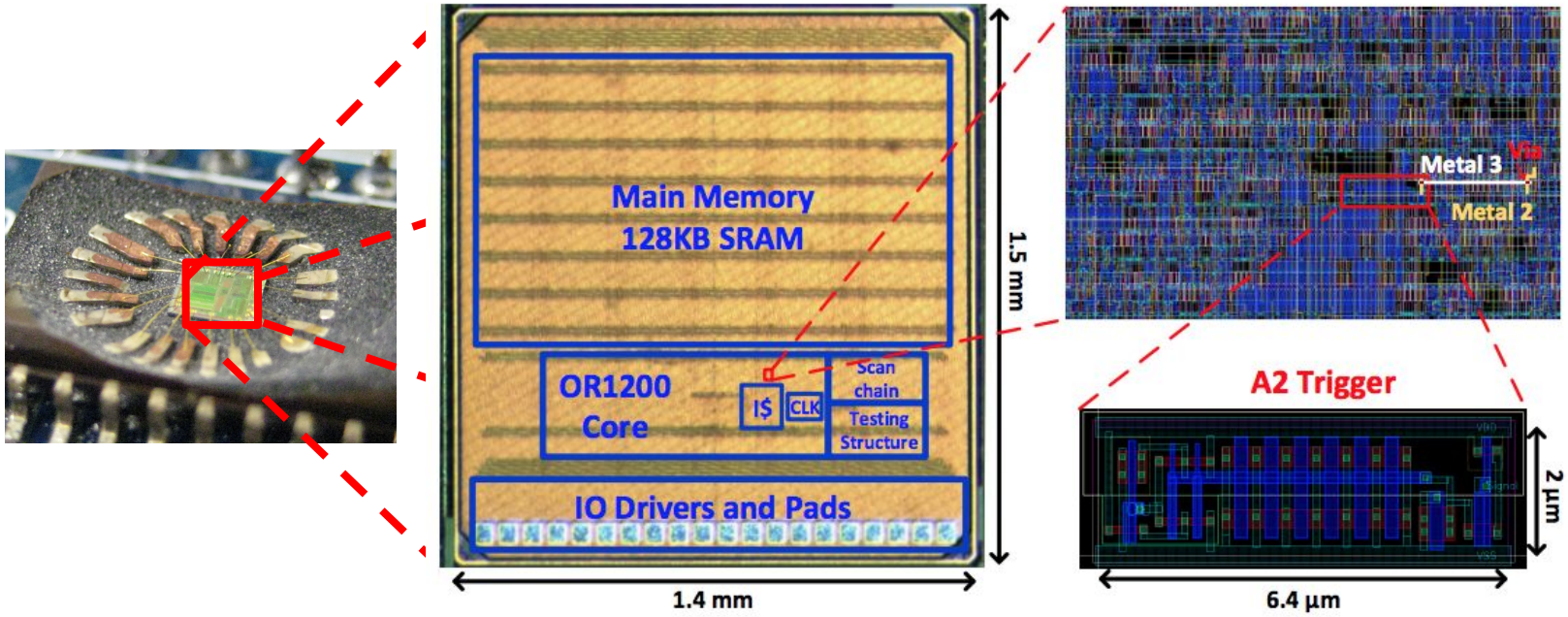
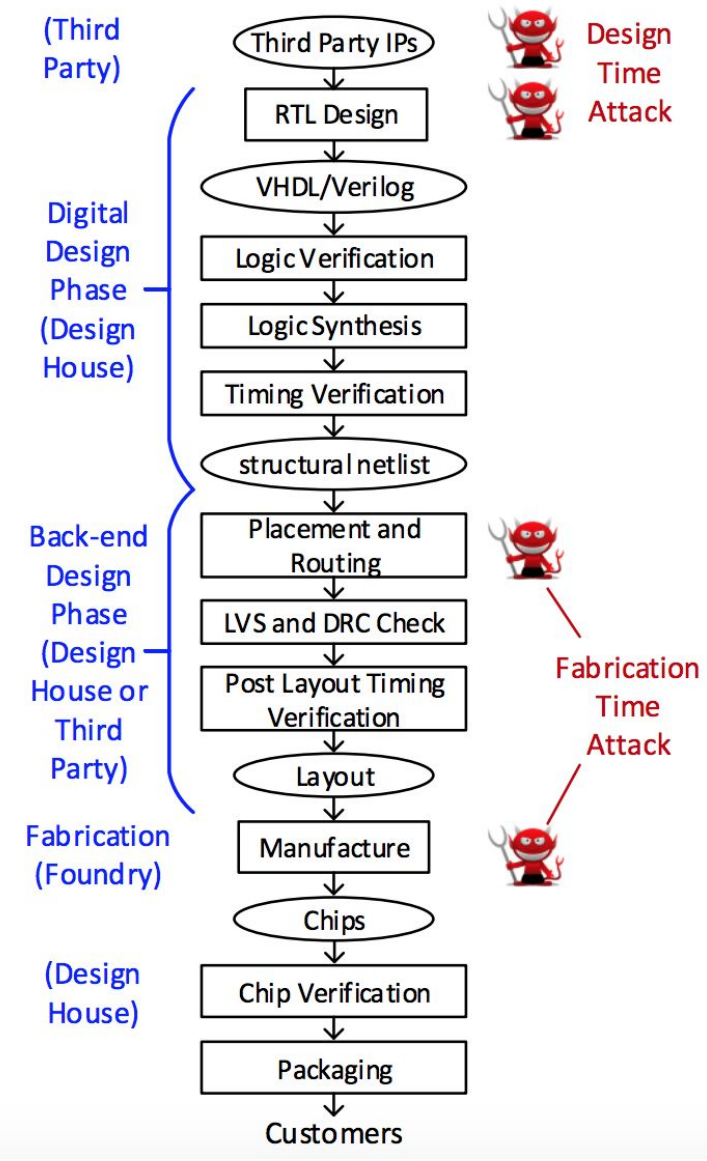


Image from https://trmm.net/Modchips
CC-BY Trammell Hudson

PCB level attacks - die level

- Proof of concept silicon attack at University of Michigan[1]
- Extremely small, likely detectable only with detailed microsophy on the decapped chip
- Change that is done inside a legitimate processor at foundry time

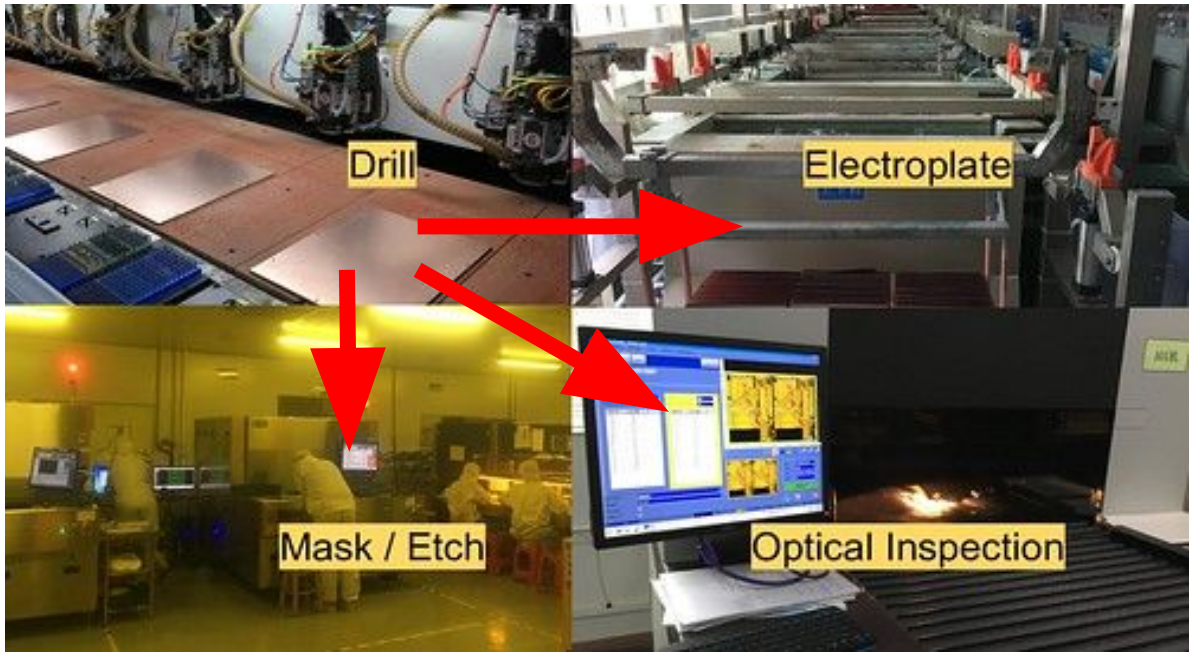


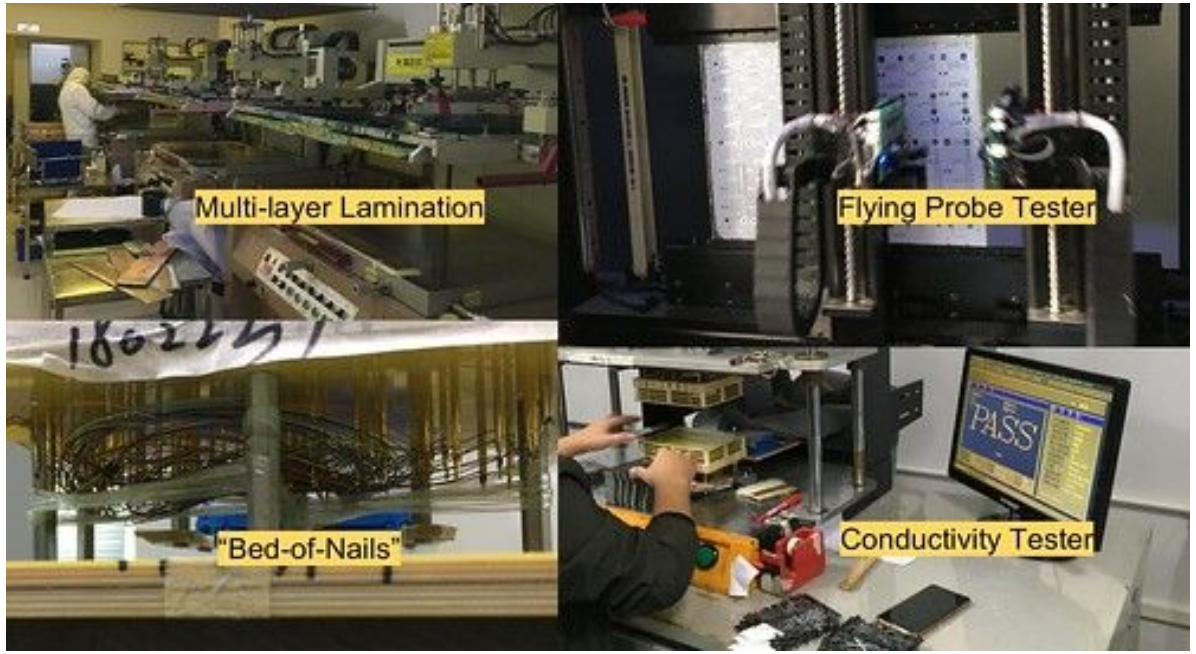


1. http://www.eecs.umich.edu/cse/awards/pdfs/A2_SP_2016.pdf

Challenges to Attackers

"If any single contractor attempts to modify the designs, the manufacturing process is structured so that those alterations would not match the other design elements in the manufacturing process."

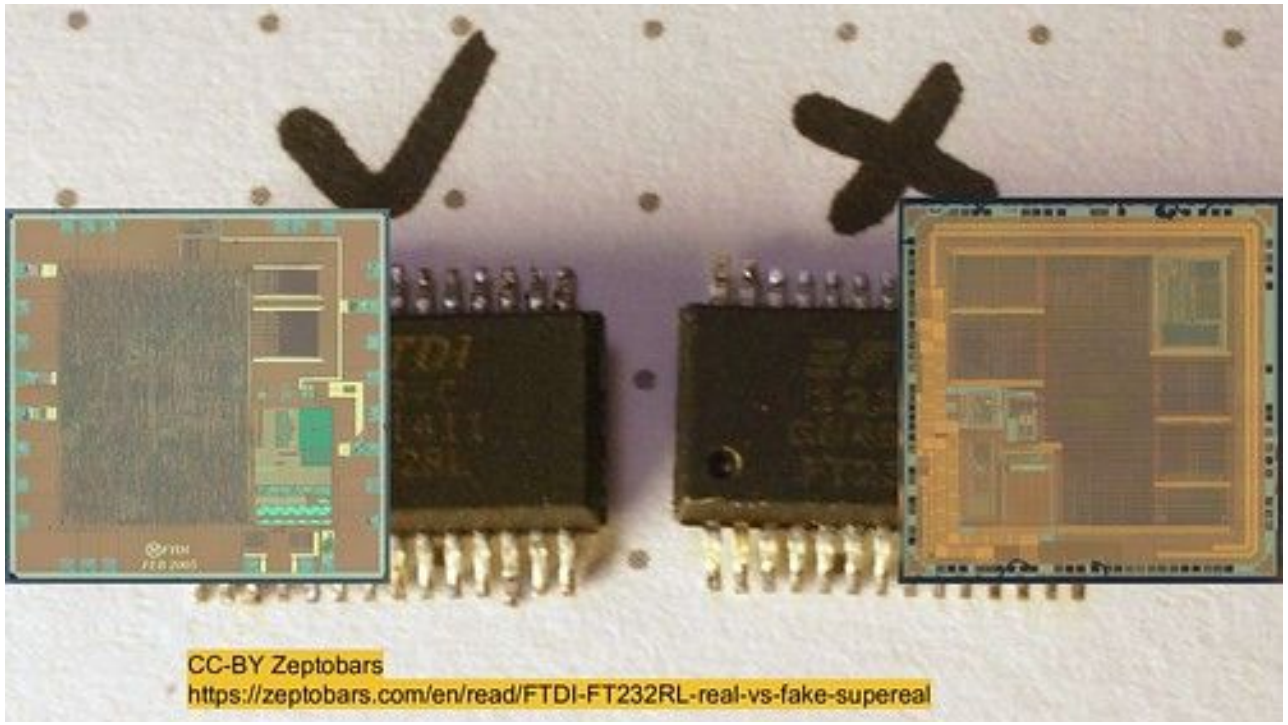




Images from https://trmm.net/Modchips

Most Likely

- Lower cost counterfeit or e-waste parts end up in things
- These aren't a security issue *per se* but is one of the largest risks
- But sometimes could be security -- e.g. FTDI chips, BMC, etc



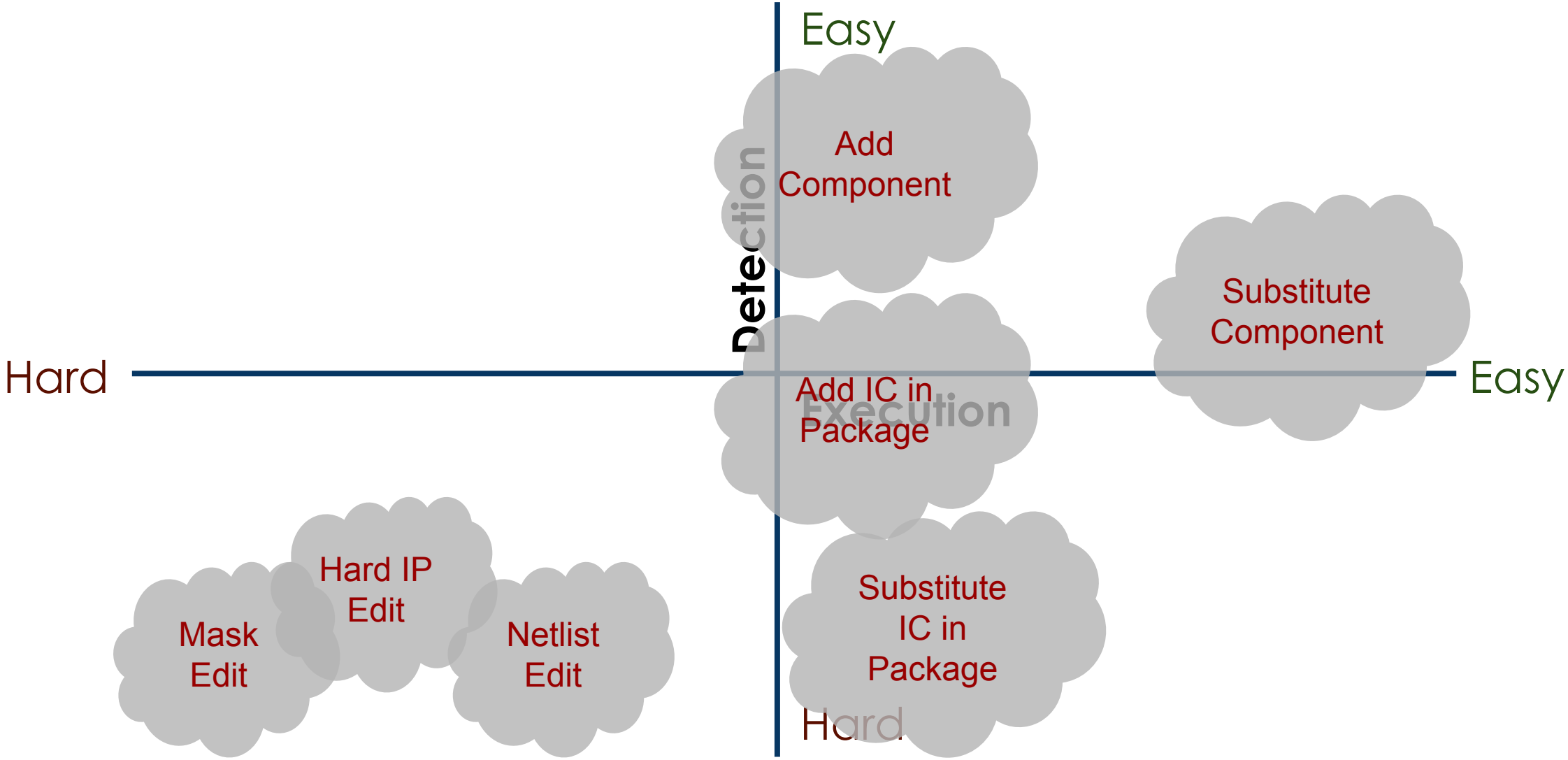
Most Likely

- Lower cost counterfeit or e-waste parts end up in things
- Incentivizes a company to monitor the supply chain
- Have representatives to check / watch in factory
- Doesn’t guard against an advanced attacker…

Fakes Help Lower the Cost of Implants

- Tech for making fake/forgeries of chips lowers HW implant costs
- bunnie's BlueHat IL numbers:
- low-10ks for wirebonded implant
- mid-100ks for a WLCSP implant

Detection vs Execution



Credit to Bunnie Huang's slide/talk image from https://prog.world/supply-chain-security-if-i-were-a-nation-state/

Challenges of Assessments

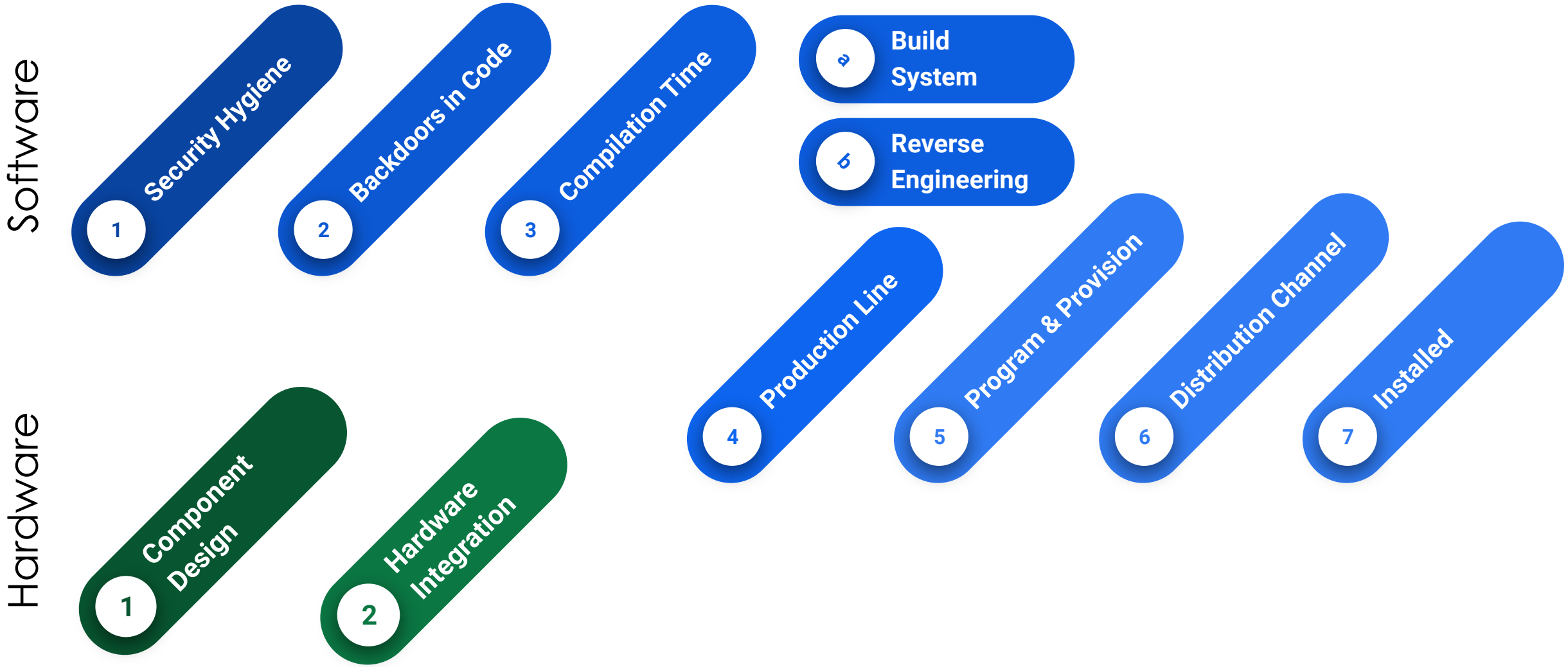
Methodology for Prioritization

1. Assess Security Hygiene
   - Poor security practices mean there is no need for a backdoor
2. Assess Supply Chain Risk
   - Where would it be most beneficial to the adversary to insert a backdoor?
   - How would they likely do it?
3. Focus on those areas
   - In code
   - In build system
   - In programming
   - In hardware

"These findings are about basic engineering competence and *cyber security hygiene that give rise to vulnerabilities that are capable of being exploited by a range of actors…*"

UK, NCSC
Report on Huawei

Supply Chain Assessment Points



Applying this to Supermicro Case Study

“Pure HW” Stages

- Claims majority of R&D in house
- Offers contract manufacturing and supply chain efficiency
- Huge producer for companies in the US and World
  - ~800 customers total, majority are distributors
  - 4,950 SKU’s, 1,200 server systems, 600 serverboards

Rough outline based on public filings

“Pure HW” Stages - Upstream Suppliers

- Ablecom Technologies
  - Offers warehousing & coordination of contract manufacturing
  - Private Taiwanese company
    - Run by brother of Supermicro CEO
  - 15%+ of cost of sales
  - Accurately forecasts and warehouse parts from various contract manufacturers to be able to create their products

“Pure HW” Stages - Integration

1. Supermicro designs
2. Ablemicro coordinates manufacturing with contract manufacturers
3. Contract manufacturer produces and ships to Ablecom for warehousing
4. Ship to Supermicro facility (San Jose, Netherlands, or Taiwan) for assembly
5. Distribution to distributor, OEM, or customer

“Pure HW” Stages - Alleged Threat

“Gray or off-white in color, they looked more like signal conditioning couplers, another common motherboard component, than microchips, and they were unlikely to be detectable without specialized equipment.”

Inspecting for something exactly matching that appearance is likely to be ineffective…

Methods - Hands-On

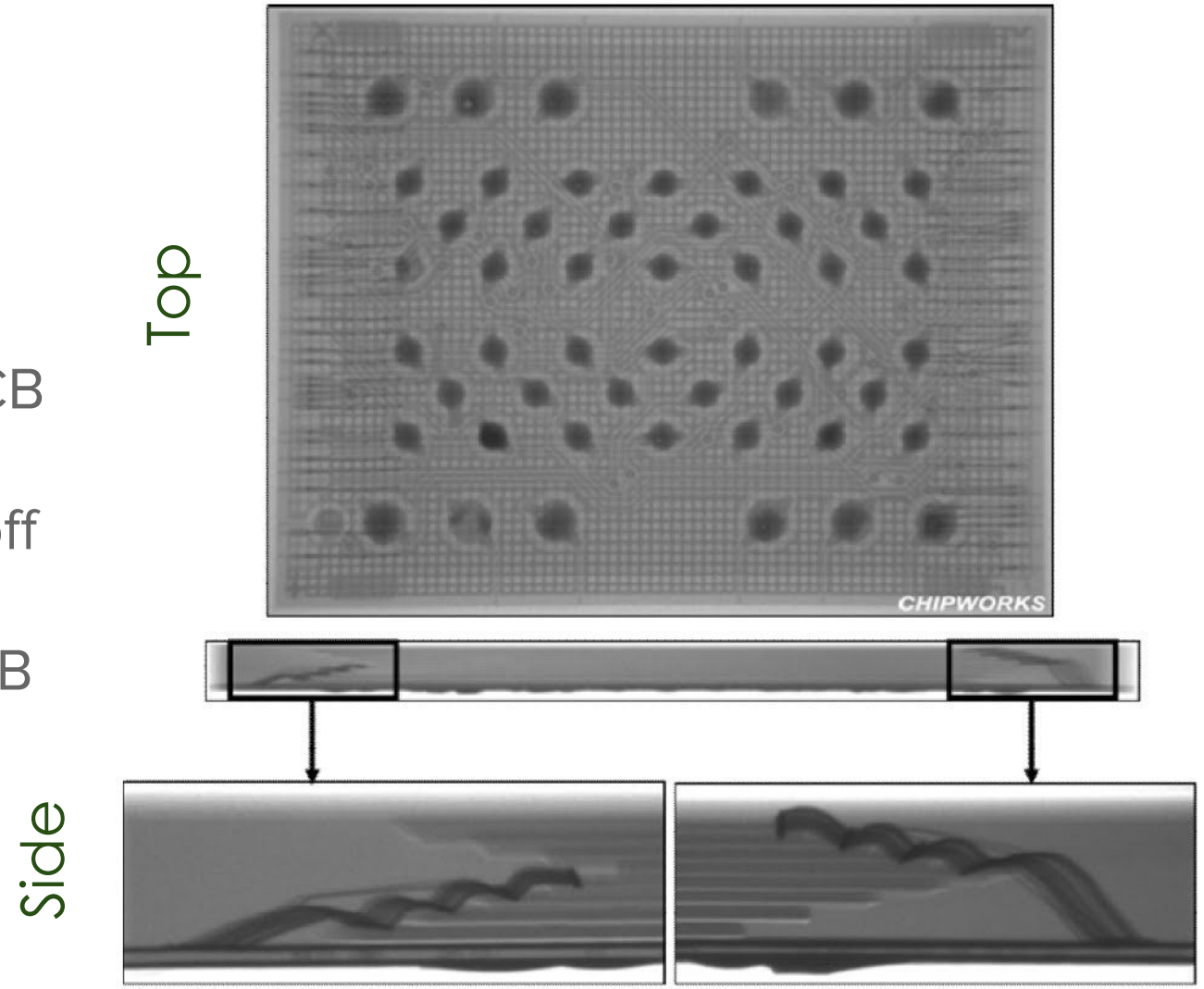
- Follow traces
- Reverse for net list
- Visual inspection - hands-on and images
- Electrical testing - on vs off board
- ...

Methods - Hands-On

"The Add" - Inside an IC

Finding it with X-rays?

- Can't see on image top-down on PCB
- Can't image side on PCB
- Can't see well on image top-down off PCB
- Likely can see on side-image off PCB

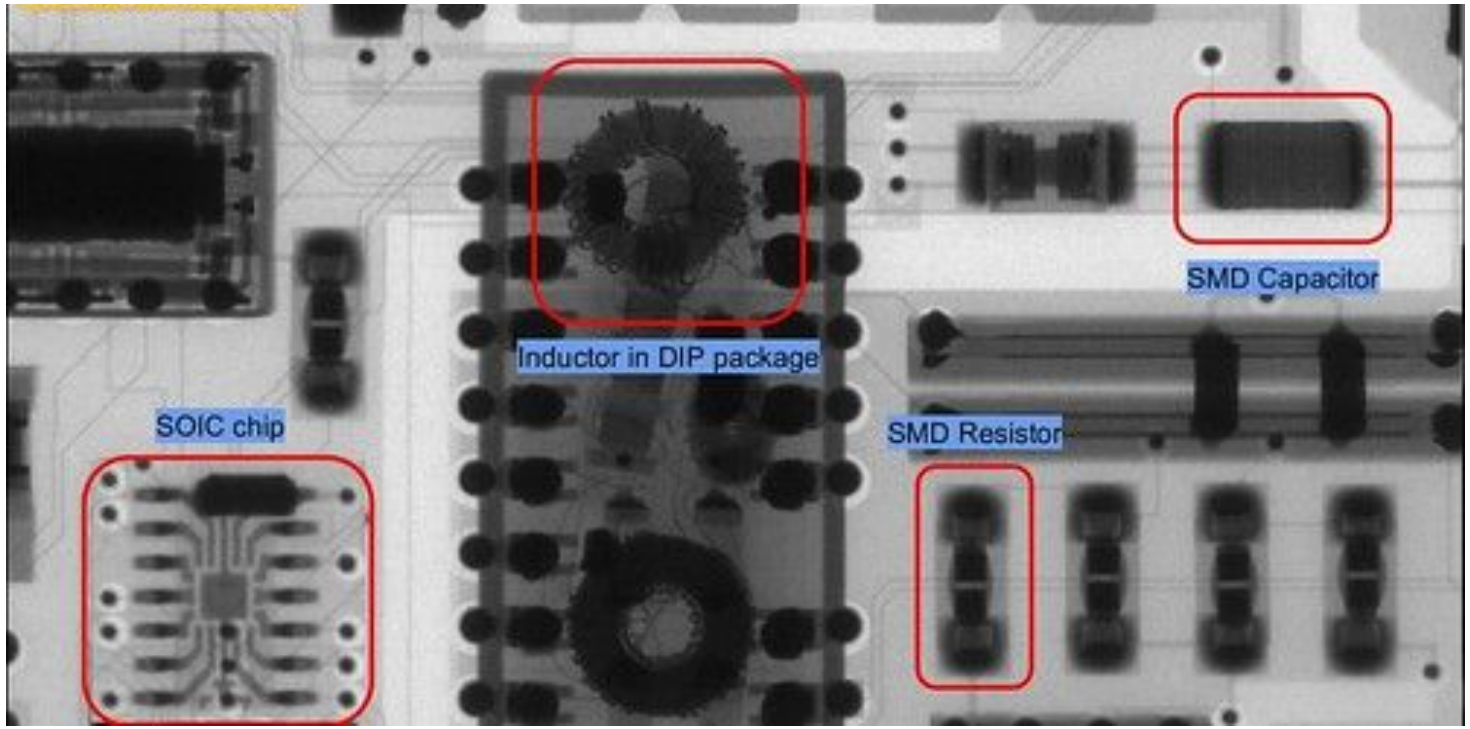


Methods - Hands-On

X-Ray to Identify Passive vs Active

- Labor intensive
- Requires skilled evaluators
- Removal of components

...DESTRUCTIVE



Methods - Hands-On

In one assessment we did:

- ~76 presumed-active components per motherboard
- plus ~12 on network card
- plus other cards
- each board visually inspected with many macro lens photos
- ~500 xray images per PCB for overview
- ~450 xray images per PCB for communications port detail

Methods - Hands-On

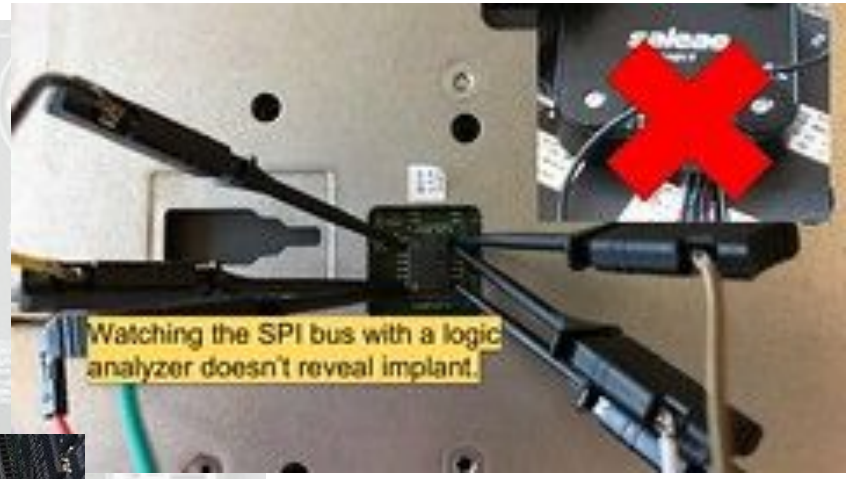
Xray analysis focused on mounting elements (wires, bonds, balls, discontinued tracks)

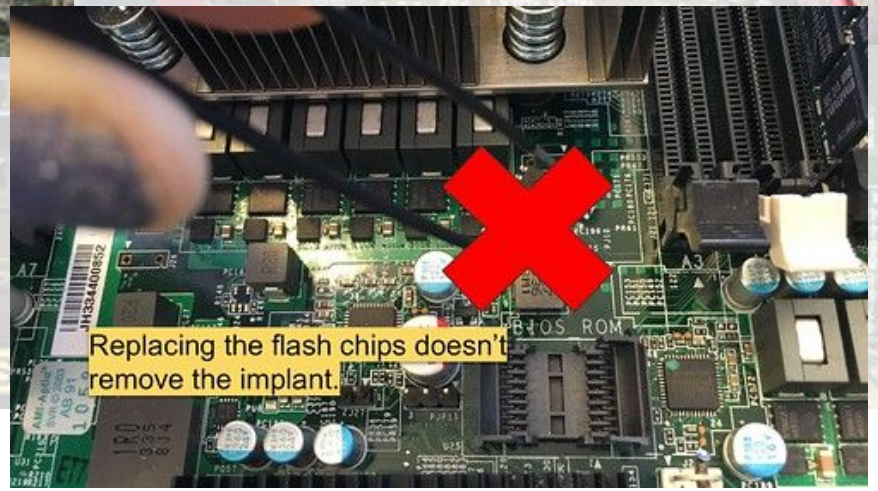
Takes significant time and experience, e.g.:

- Each inspector conducting x-ray analysis had 10 to 15 years of experience in electronics, failure analysis, and/or electronics x-ray, electron microscopy, and depackaging
- Each image analyzed twice

“The Swap” - Why Detection is Hard

Trammell Hudson’s example of replacing a 0603 passive with an implant on a motherboard SPI flash to BMC link is just one example...





Images from https://trmm.net/Modchips
CC-BY Trammell Hudson

Why Care about Code?

October 4, 2018, 5:00 AM EDT

The Big Hack: The Software Side of China's Supply Chain Attack

● It wasn't just hardware. An online portal for firmware updates hid and distributed malware.

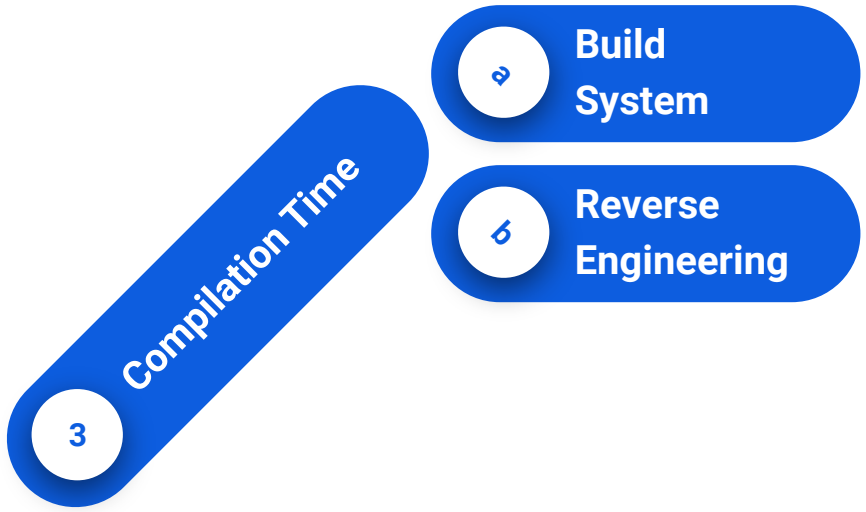
By Jordan Robertson and Michael Riley

Why Care about Code?

From a **Hardware** Validation perspective...

...Hardware backdoors often don't operate alone...

Binary Equivalence



“Work to validate them by HCSEC is still ongoing but has already exposed wider flaws in the underlying build process which need to be rectified before binary equivalence can be demonstrated at scale... Unless and until this is done it is not possible to be confident that the source code examined by HCSEC is precisely that used to build the binaries running in the UK networks.”

- UK HCSEC 2019.03
(emphasis added)

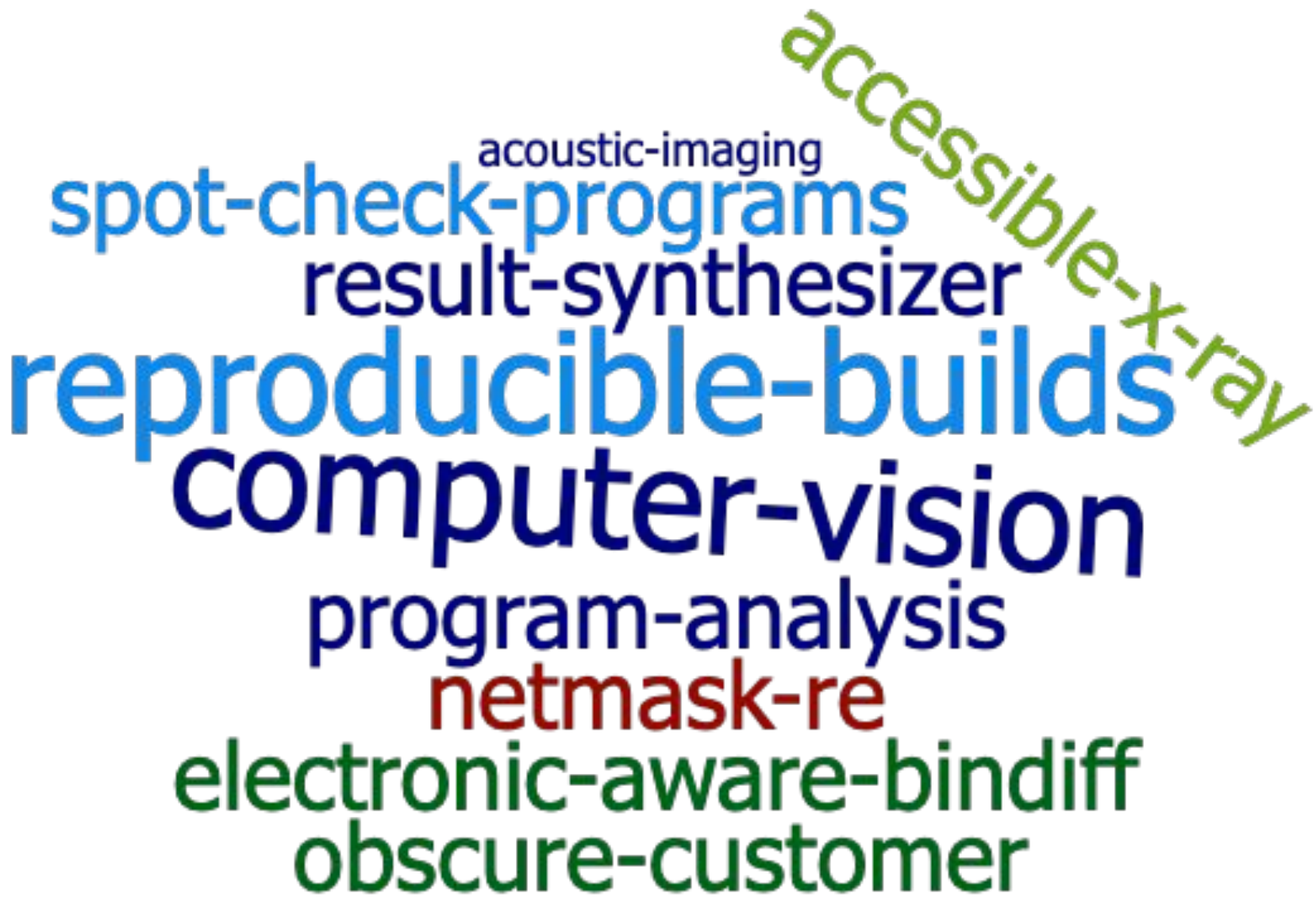
Binary Equivalence - Multiple Steps

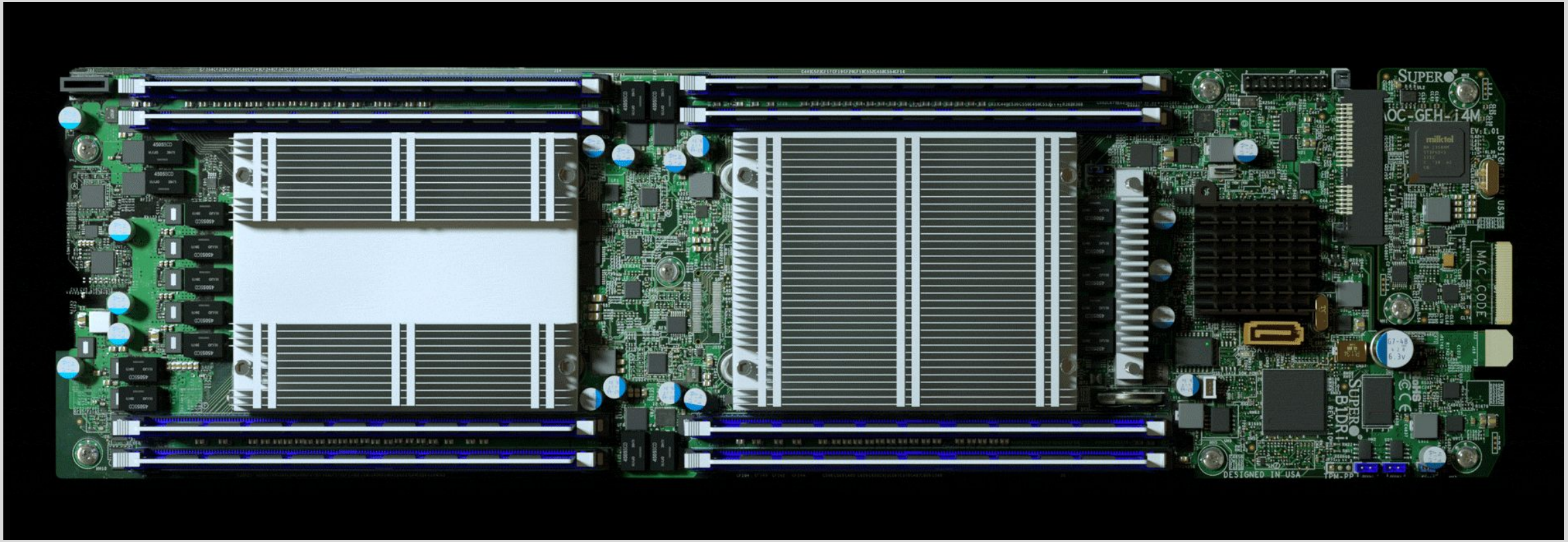
In Source Code	In Compiled Firmware	In Chips
Access via a subtle logic bug; require multiple preconditions “bugdoors” hard to prove intent	If a reproducible, signed build chain using trusted components isn’t available… align *all* parts of binary firmware to code	When reading from the chips, differences 0x00 vs 0xFF for memory vs firmware Wear leveling, old versions not cleared, etc.

We don’t have time to cover all the aspects....

- Radio Frequency (RF)
- Network
- ...

Possible Solutions


accessible-x-ray
acoustic-imaging
spot-check-programs
result-synthesizer
reproducible-builds
computer-vision
program-analysis
netmask-re
electronic-aware-bindiff
obscure-customer



Questions