Hardware Security

With an Emphasis on Supply Chain Attacks & Verifiability

bunnie (@bunniestudios / twitter)

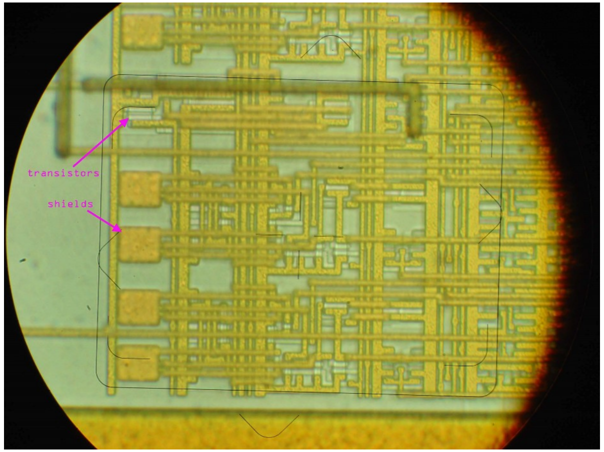
MIT 6.858 May 2022

Topics

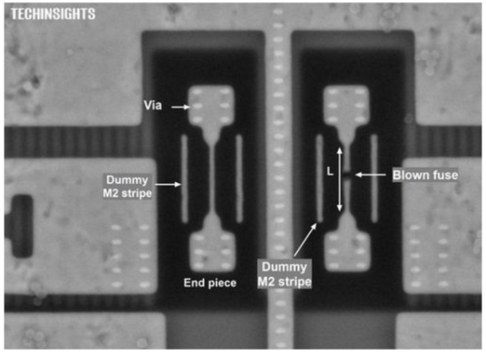
- Breaking Hardware Security
  - Direct physical tampering
  - Indirect supply chain tampering
- Mitigations
  - vs. supply chain attacks: User-verifiable hardware
  - vs. direct attacks: plausible deniability
  - vs. direct attacks: (Not in covered, mentioned for completeness) tamper-evident / tamper-resistant and anti-cloning techniques

Protecting Secrets within a "Vault": Hardware Security Modules (HSMs)

Qurren – CC BY-SA 3.0



Via ledgerwallet.com

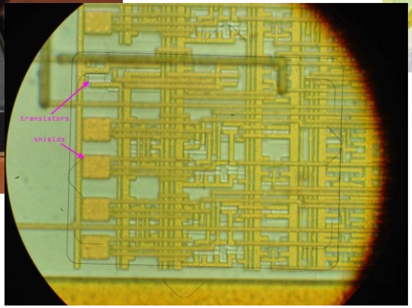


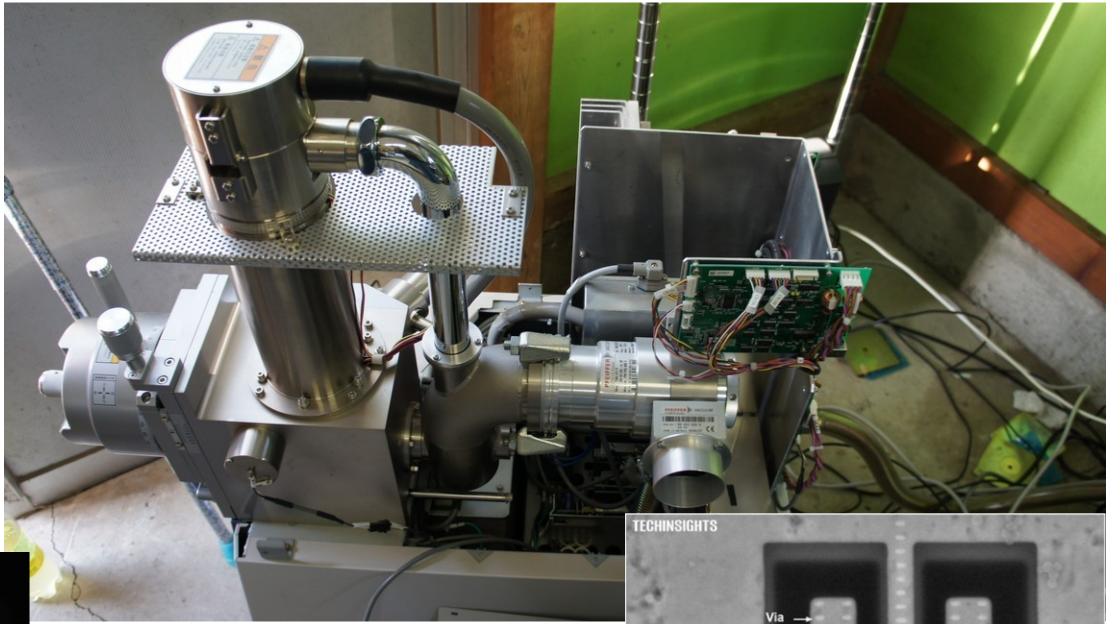
Qualcomm Gobi MDM9235 Modem 20 nm HKMG Logic Detailed Structural Analysis, TechInsights

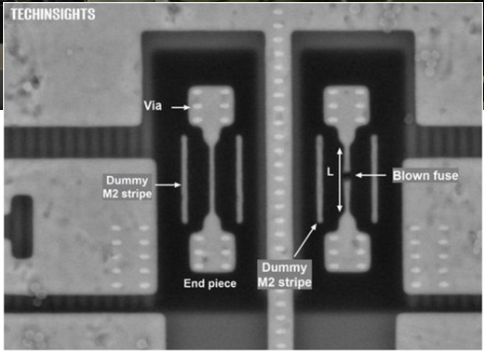
Direct Attacks on Hardware: Overview

- Passive – little to no modification of target system
  - Direct observation
    - Optical
    - SEM
  - Side-channel (emissions)
    - Power
    - RF
    - Optical
- Active – no holds barred
  - Fault induction
    - Glitching (clock/VDD)
    - Coupling (e.g. row hammer)
    - Photonic
  - FIB edit

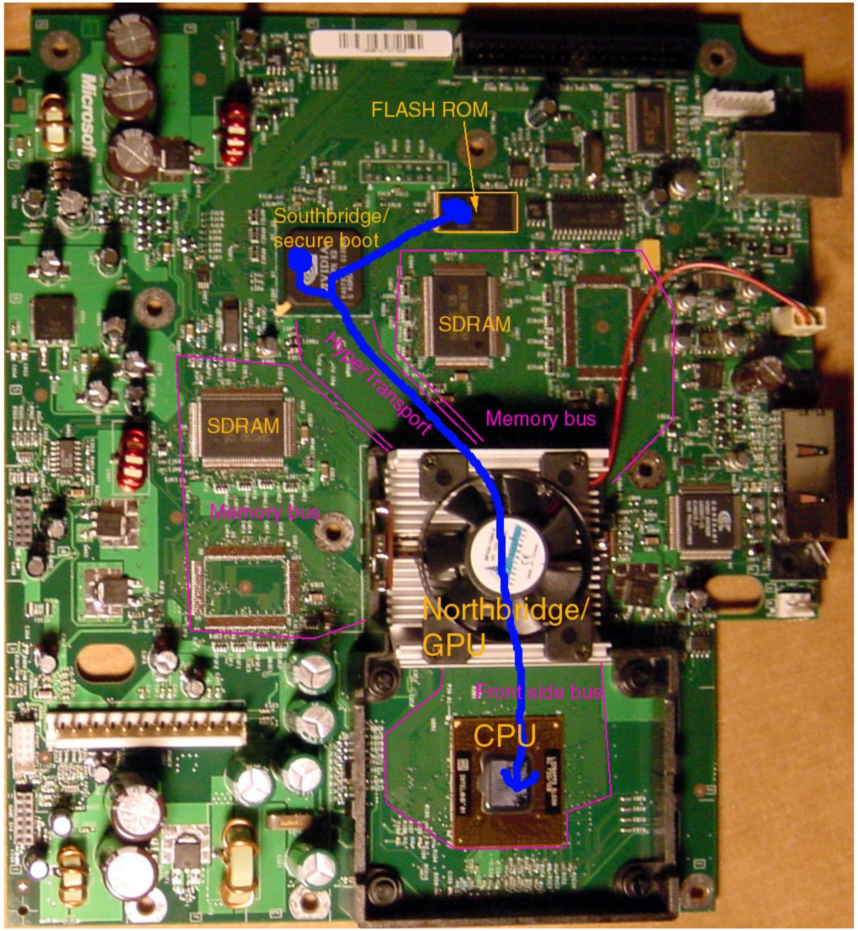
Passive: Direct Observation

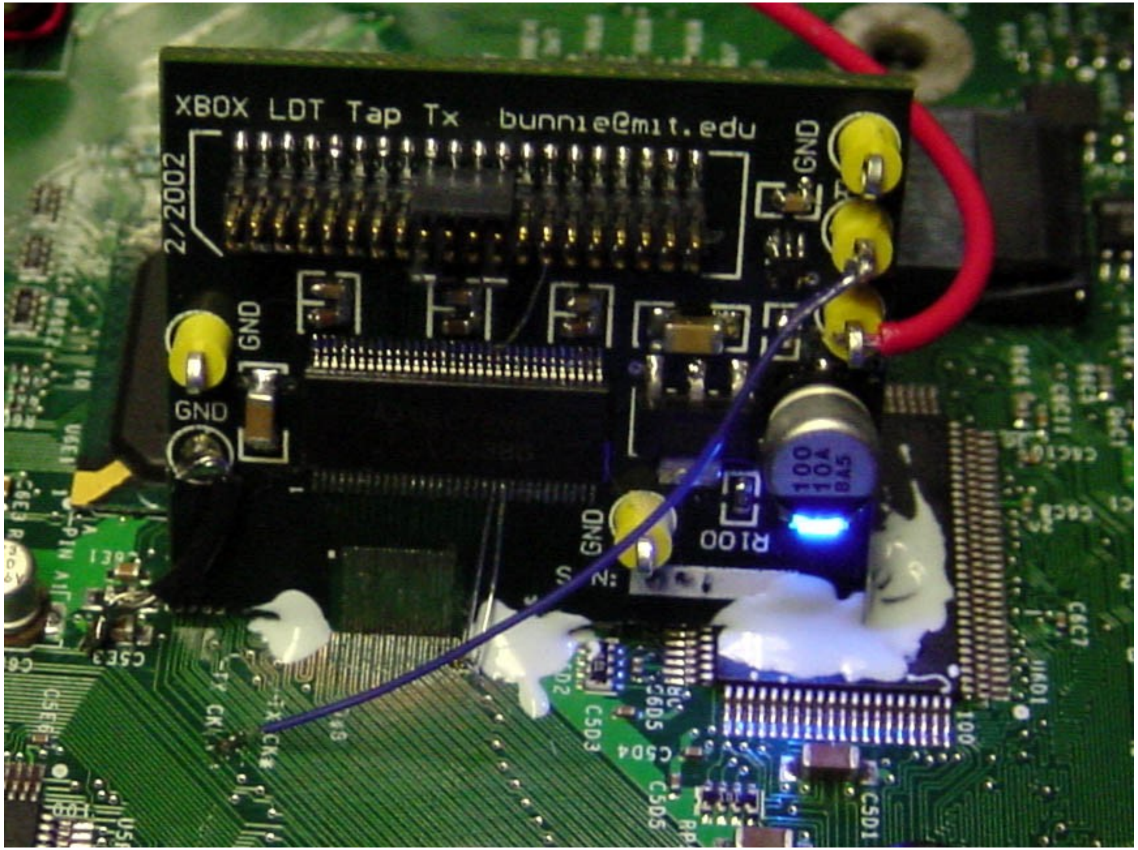




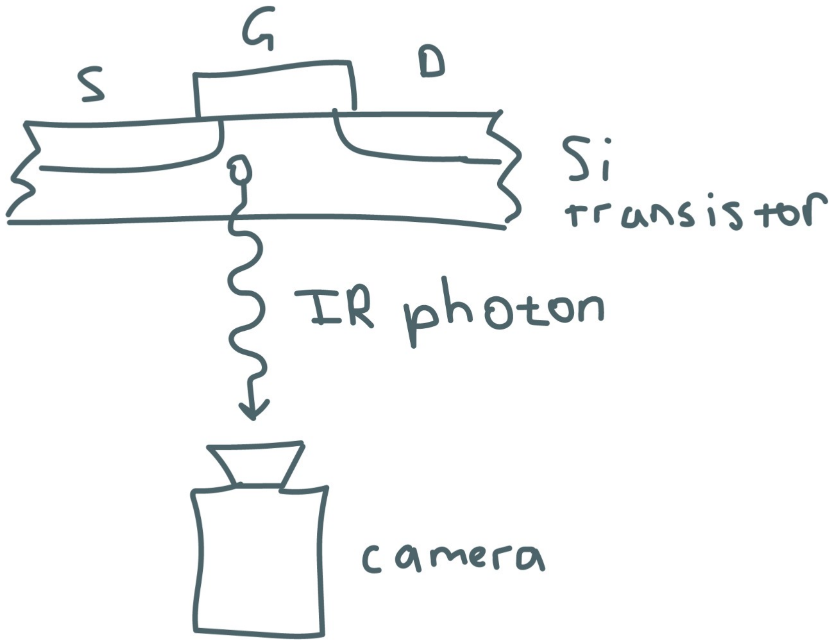


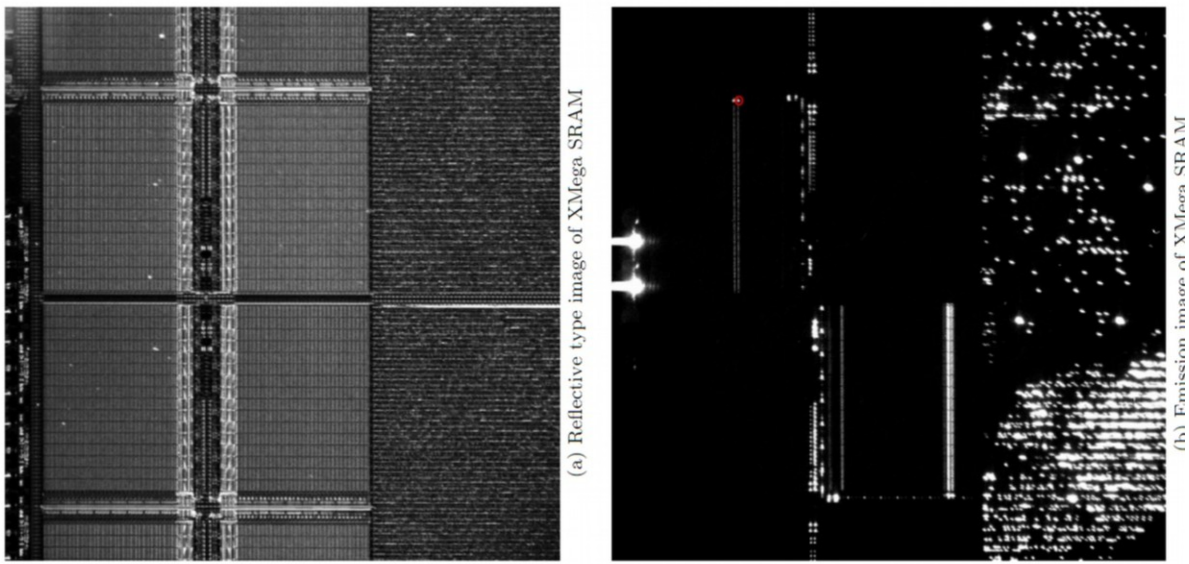
Passive: Direct Measurement





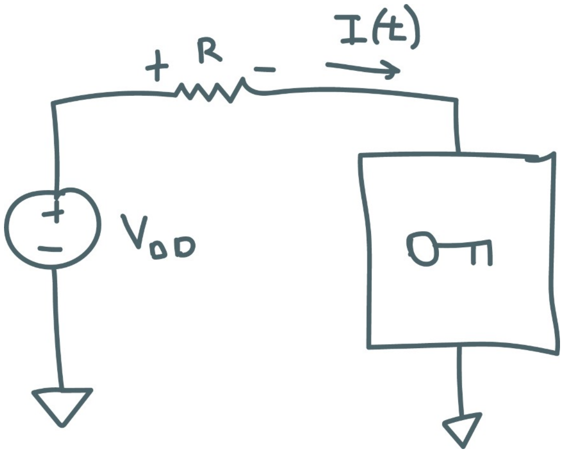
Passive: Optical Emissions



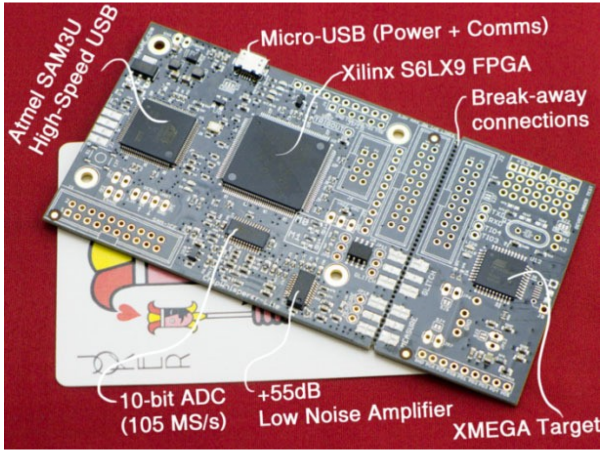


Schlosser, A., Nedospasov, D., Kramer J., Orlic, S., Seifert, JP. “Simple Photonic Emission Analysis of AES”

Passive: Power Side-Channels



ChipWhisperer-Lite (CW1173)



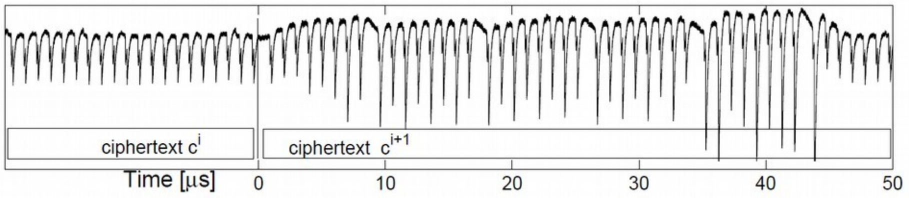
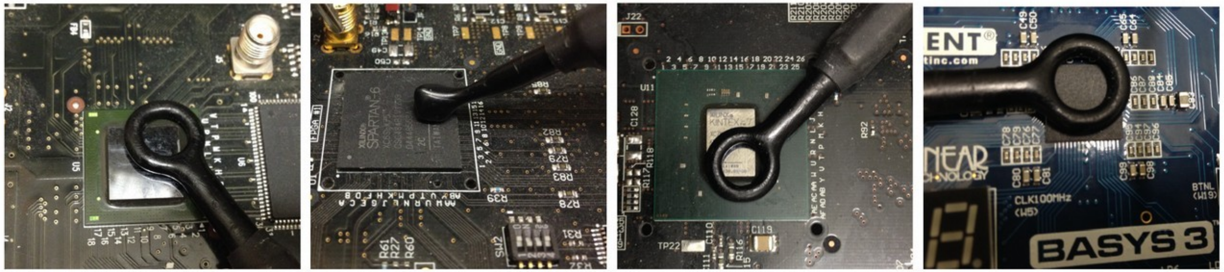


Fig. 1. A sample power trace of Spartan-6 (with 20MHz low-pass filter) during loading an encrypted bitstream

Moradi, A and Schneider, T. "Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series"

Passive: RF Side-Channels

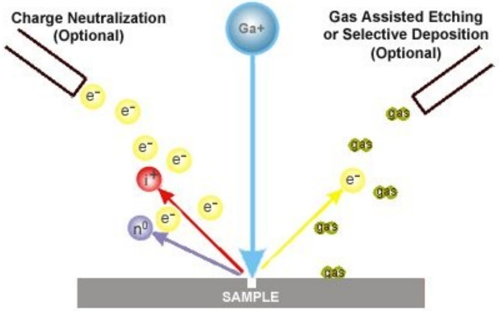


(a) Virtex-5 (b) Spartan-6 (c) Kintex-7 (d) Artix-7

Fig. 5. EM probes and different FPGAs, (a) XC5VLX50-1FFG324, (b) XC6SLX75-2CSG484C, (c) XC7K160T-1FBGC, (d) XC7A35T-1CPG236C

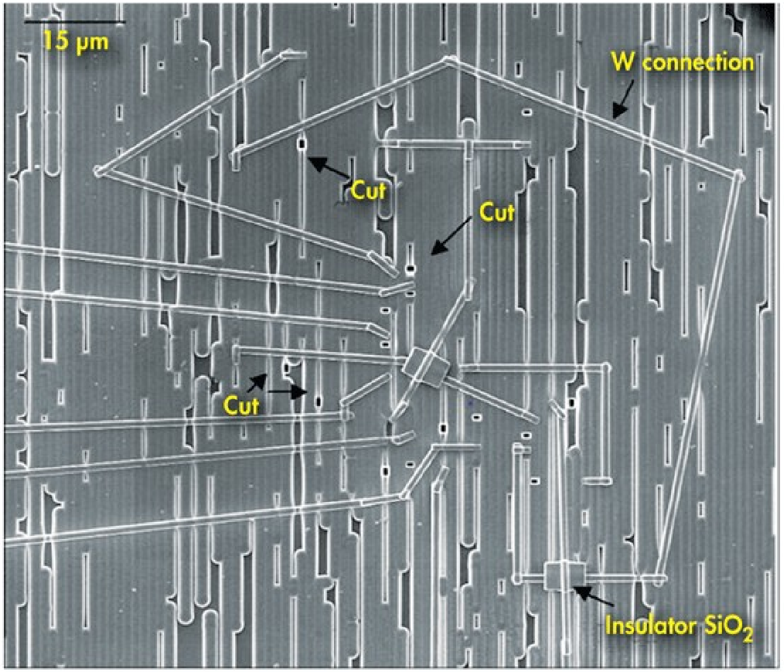
Moradi, A and Schneider, T. “Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series”

Active: FIB



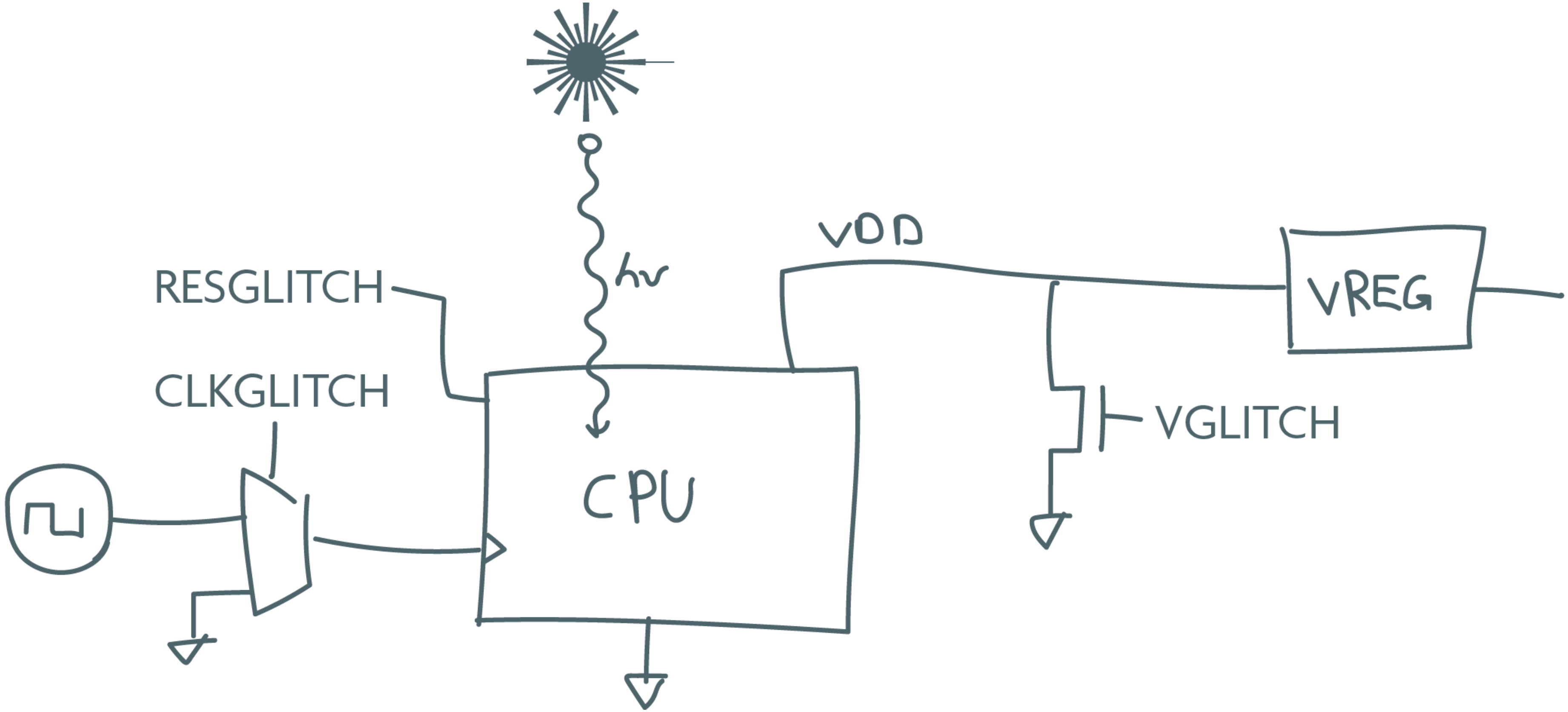
Kriegor27 – Pubilc domain

Cm the p, CC-BY-SA 3.0



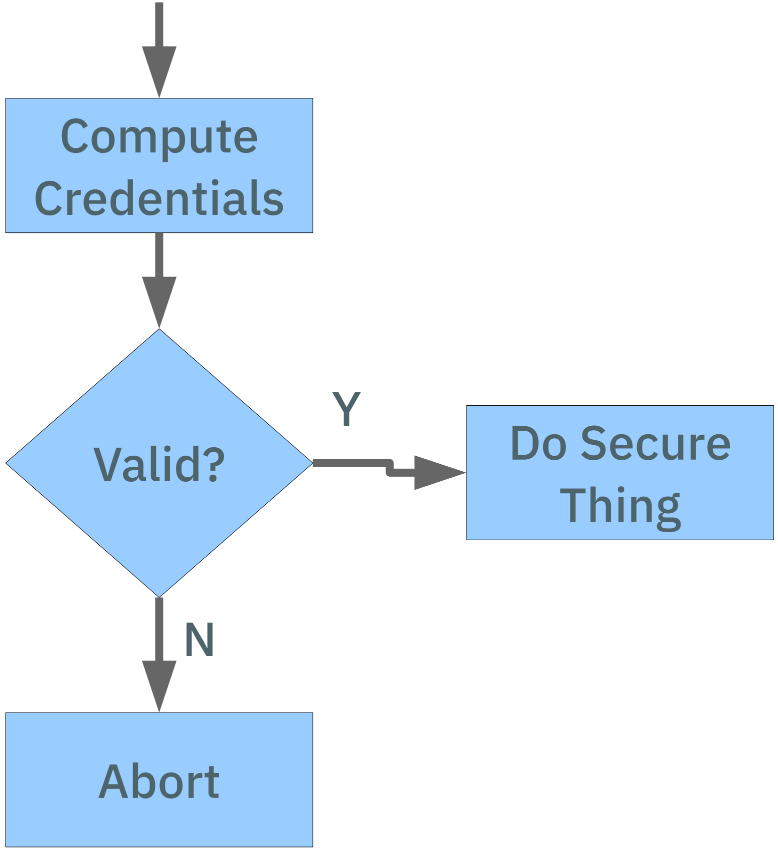
From http://www.electronicdesign.com/eda/fib-circuit-edit-becomes-increasingly-valuable-advanced-node-design

Active: Fault Injection (Glitching, Optical)

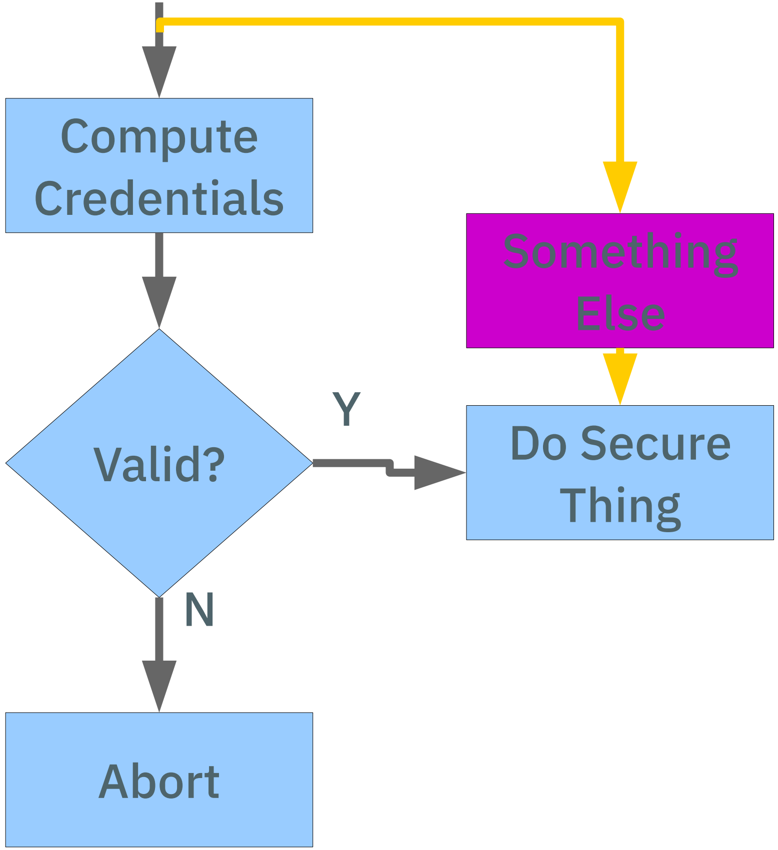


Also available in remote attacks: See https://plundervolt.com/doc/plundervolt.pdf

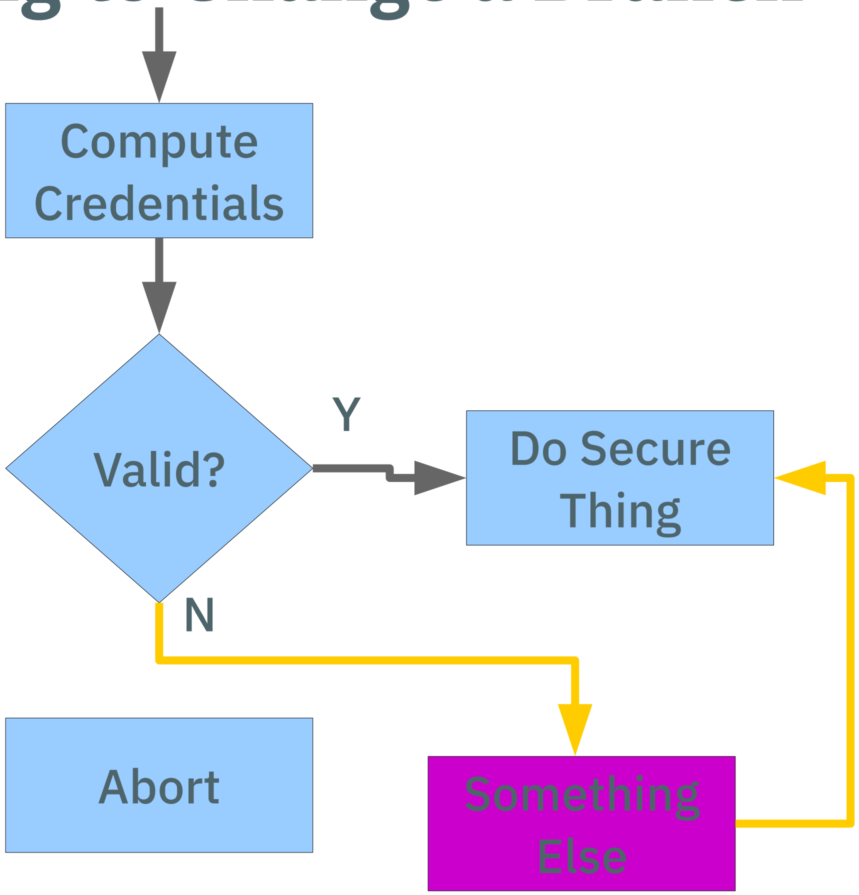
Fault Injection: The General Idea



Glitching To Run an Alternate Code Base

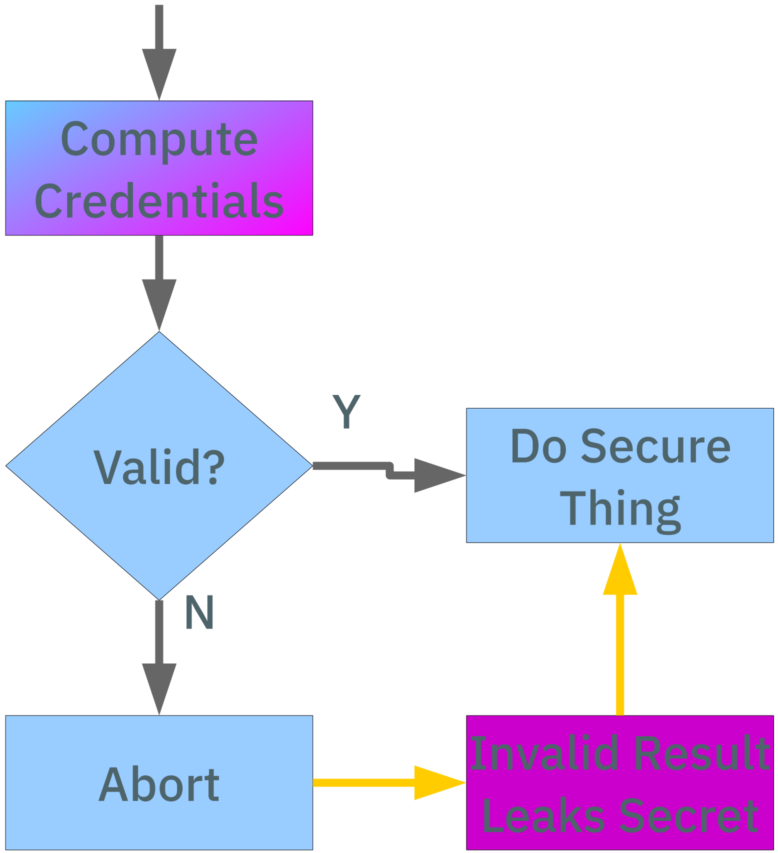


Glitching to Change a Branch



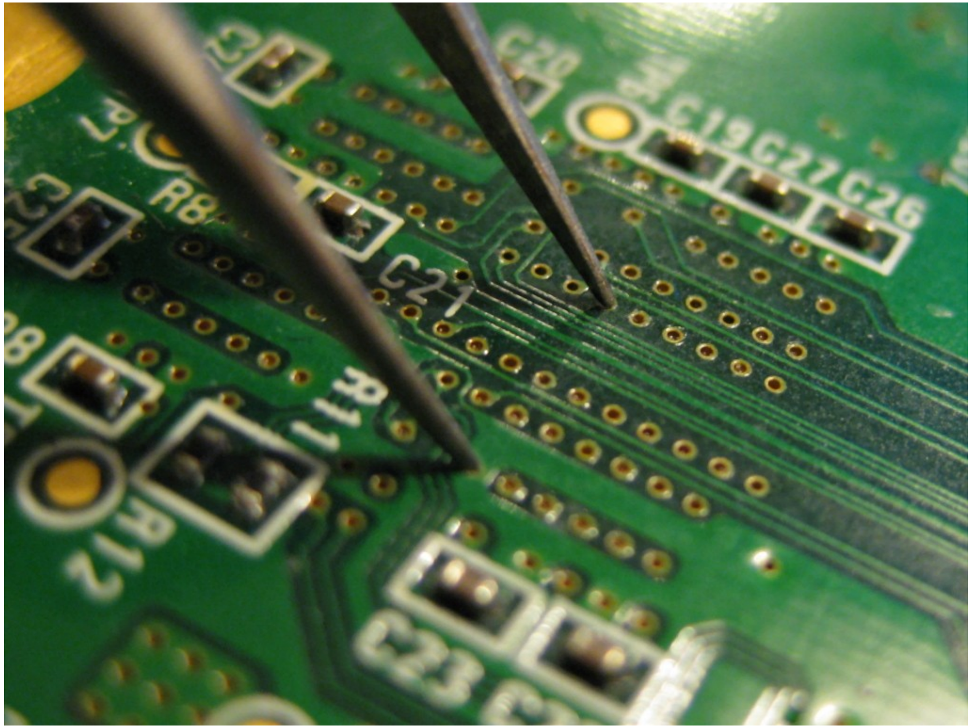
Glitching To Cause Cipher Faults That Leak Private Data

* Some ciphers (e.g. RSA) leak secrets if the computation is glitched



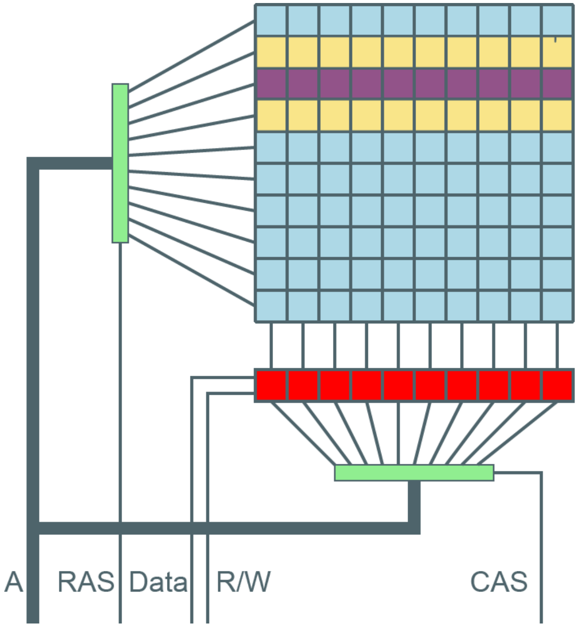
Fault Injection

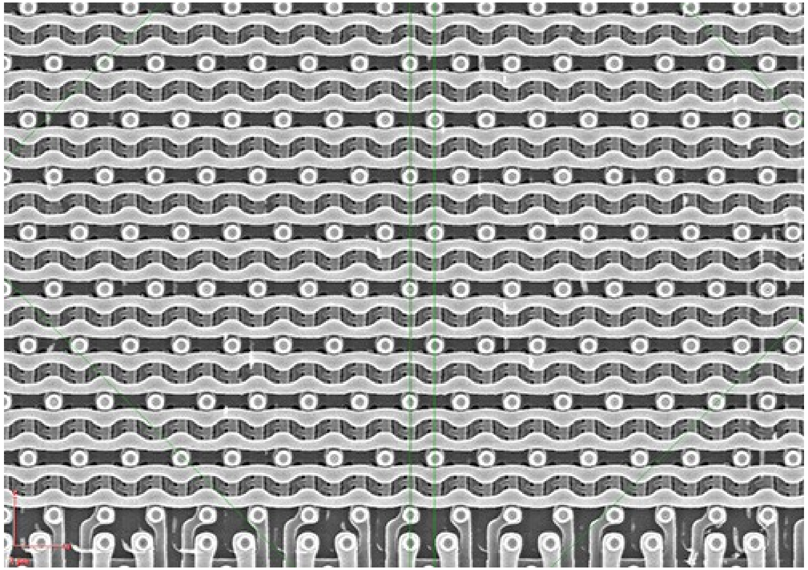
- Can be surprisingly trivial to execute ("twiizer" attack") ---->



Twiizer hack via Marcan.st

Active: Coupling (e.g. Rowhammering)

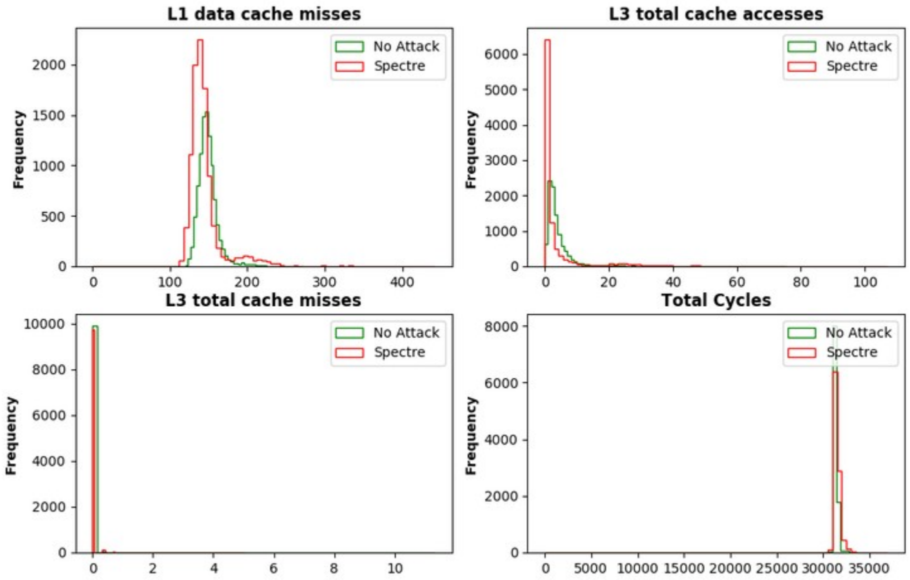




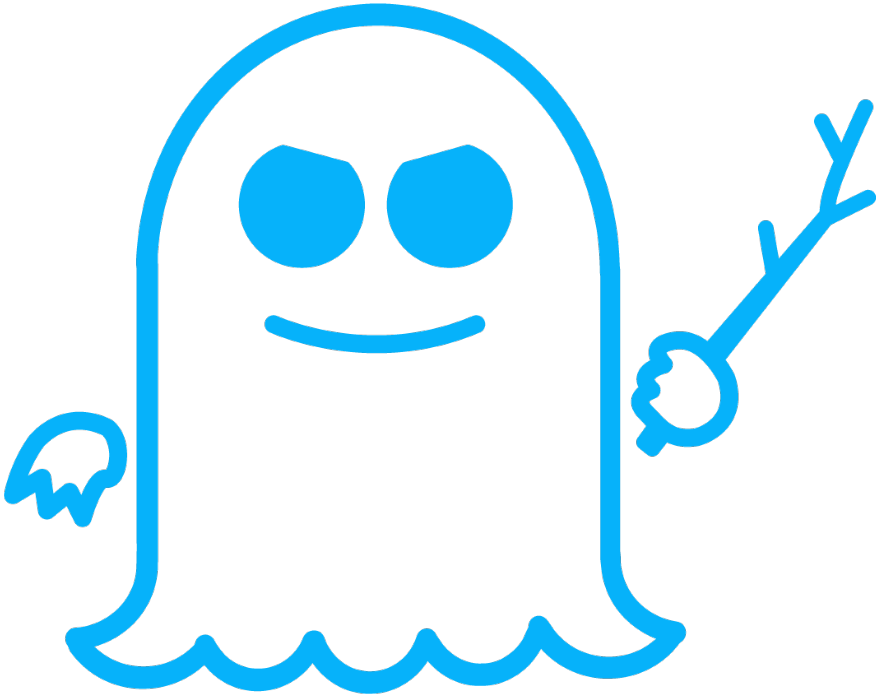
From
https://www.raith.com/products/chipscanner.html

Active: Microarchitectural Side Channels

- Leverage timing differences in latency hiding features to leak secrets



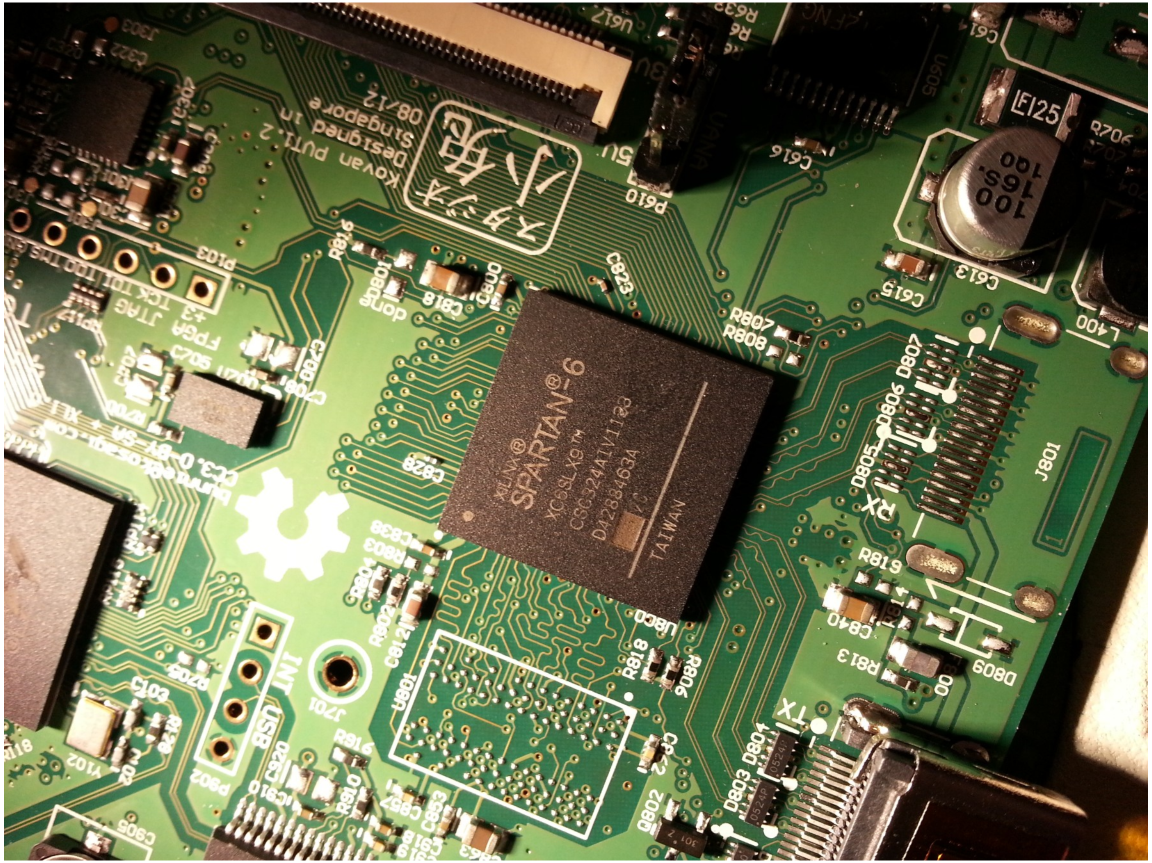
DOI:10.1109/ACCESS.2020.2988370

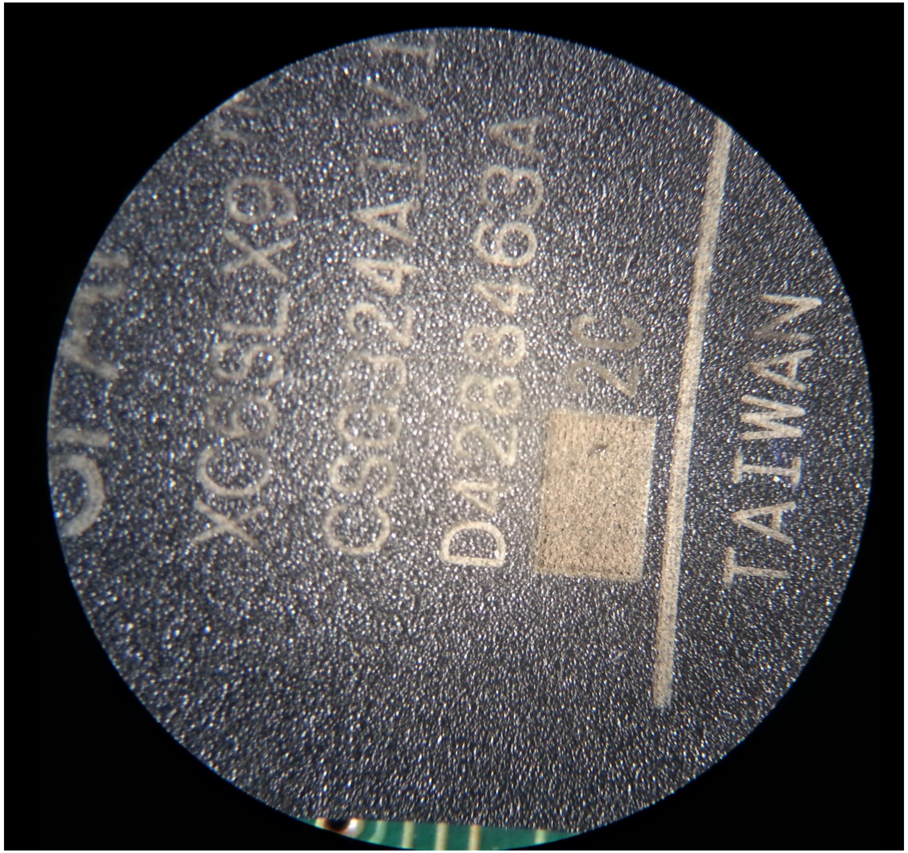


Can't Access the Hardware?

Attacks Prior to Installation: Supply Chain Tampering

"State of the Practice" for Trusting Chips: Reading the Label on the Box



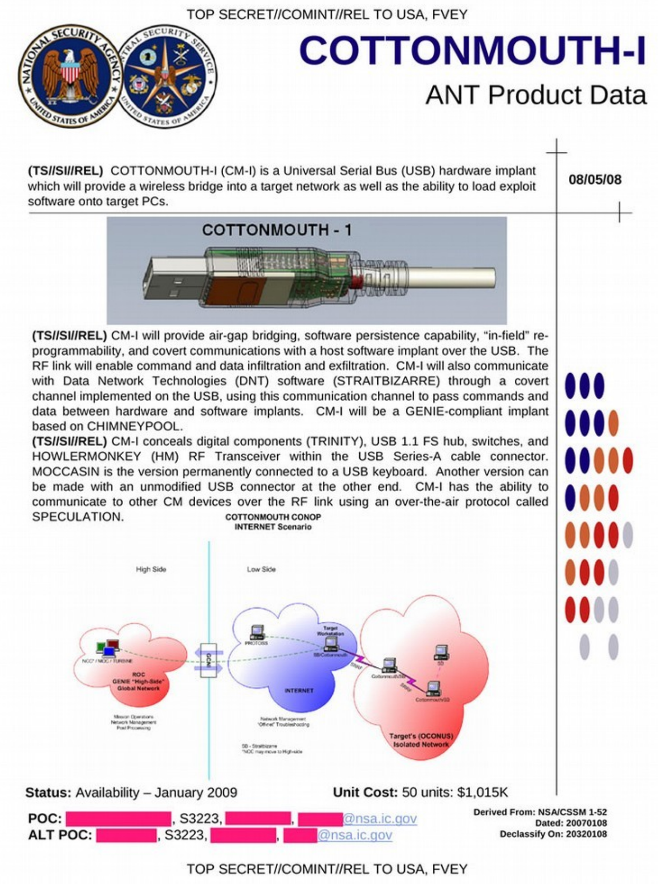


Not Just Chips: Whole Assemblies Are Swapped Without Detection

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

NSA: Implanting beacons in CISCO routers

https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

POC: [redacted], S3223, [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

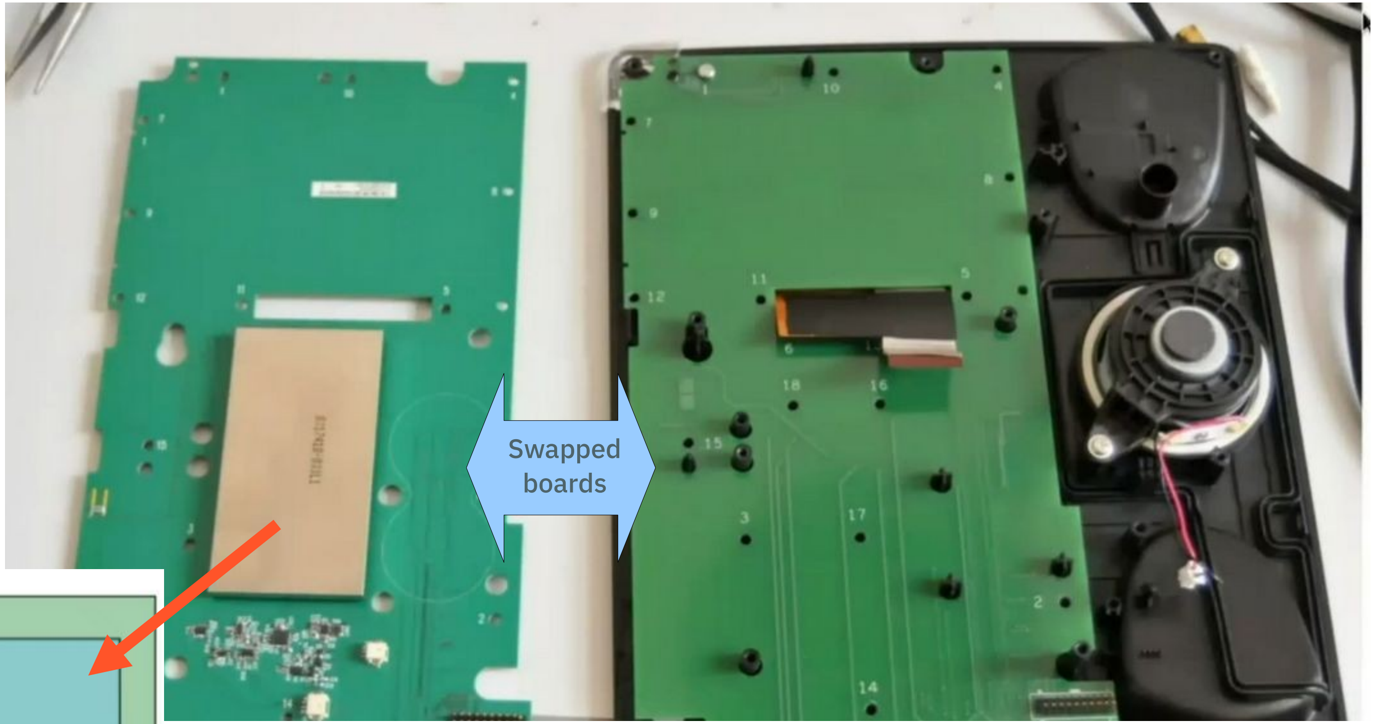
TOP SECRET//COMINT//REL TO USA, FVEY

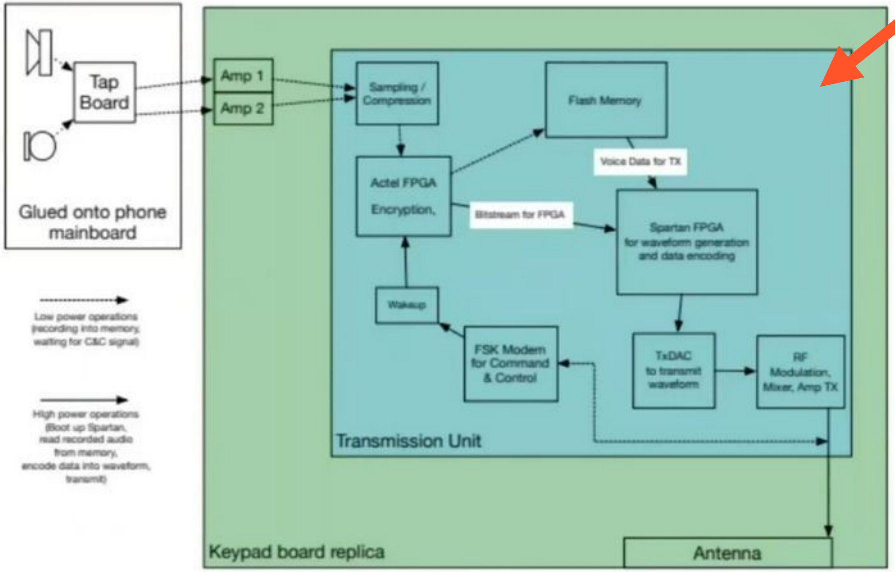
(TS//SI//REL) GODSURGE runs on the FLUXBABBITT hardware implant and provides software application persistence on Dell PowerEdge servers by exploiting the JTAG debugging interface of the server's processors.

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 2950

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 1950

JTAG implants Dell PowerEdge servers

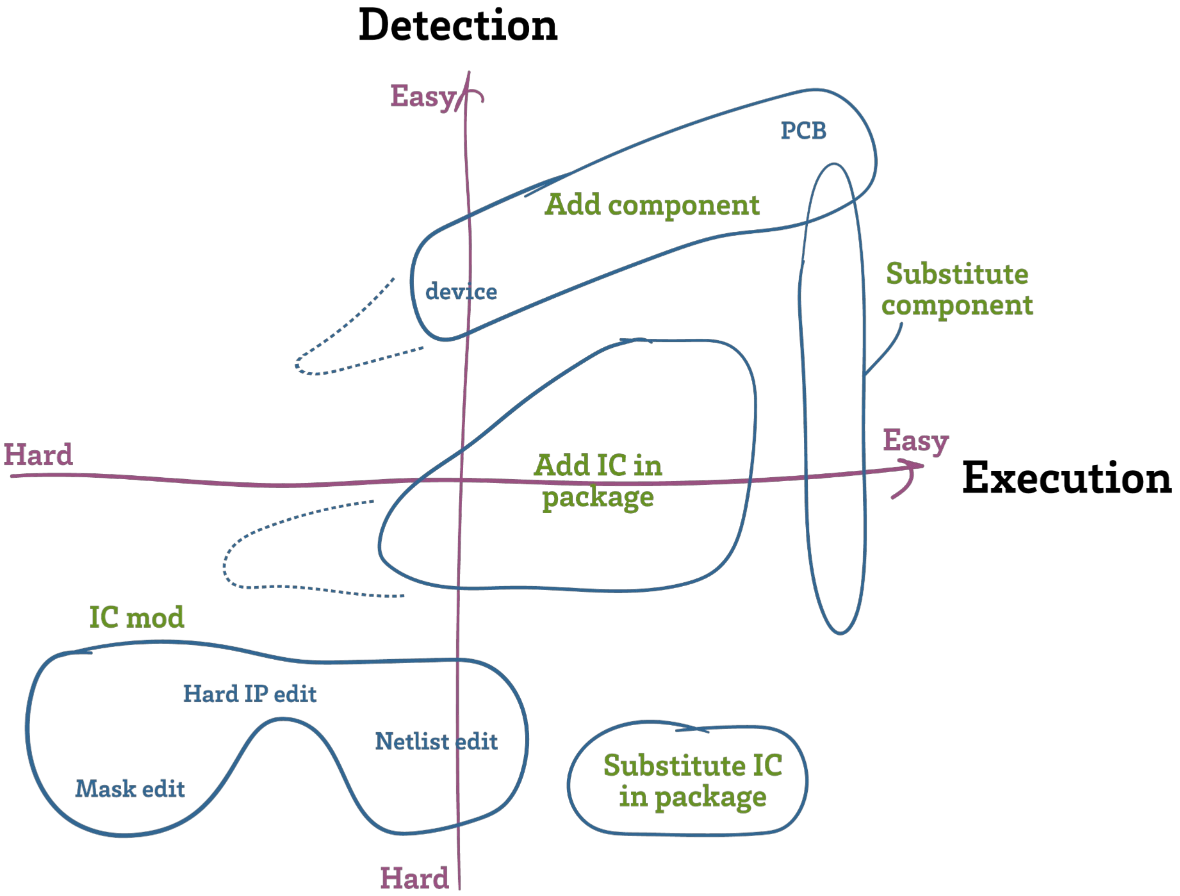




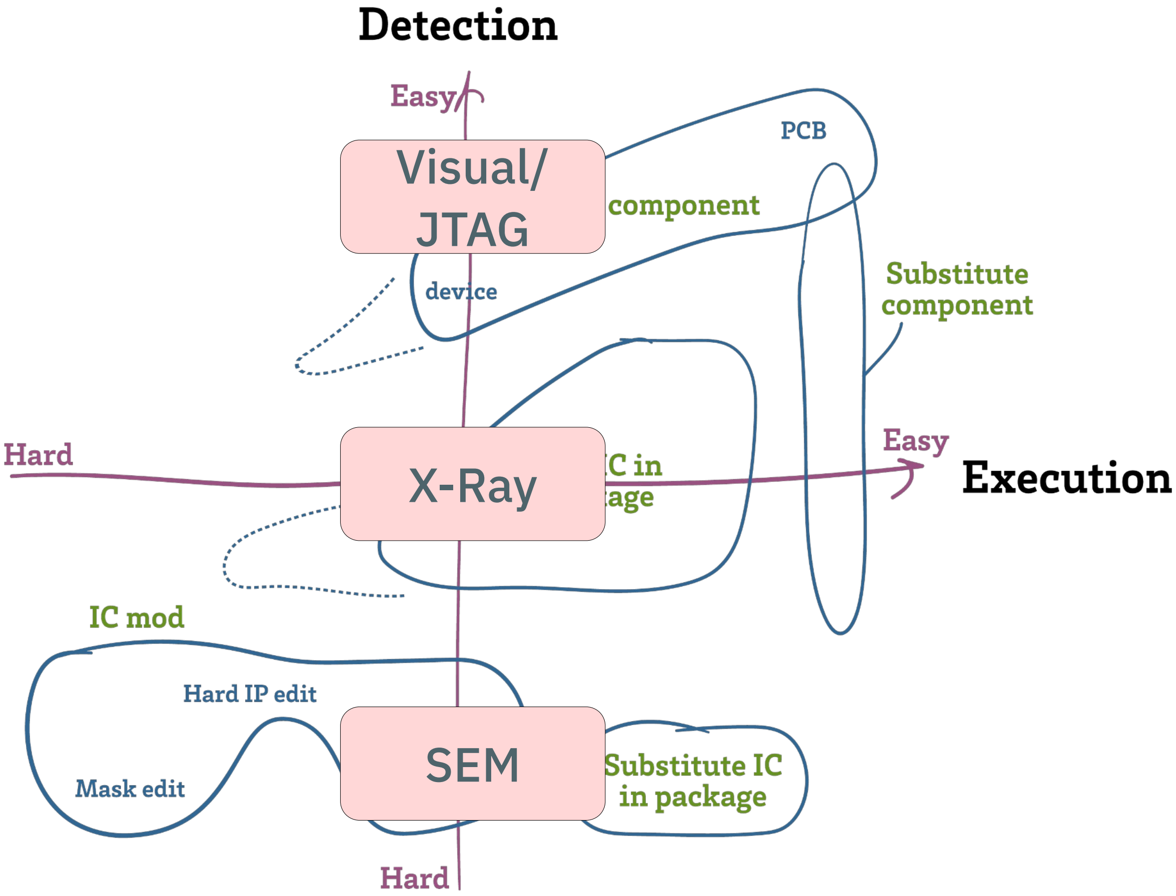
Andy Müller-Maguhn – listening device in cryptophone

https://datareisen.de/2020/20201228-RC3-AMM-CIA-VS-WL.pdf

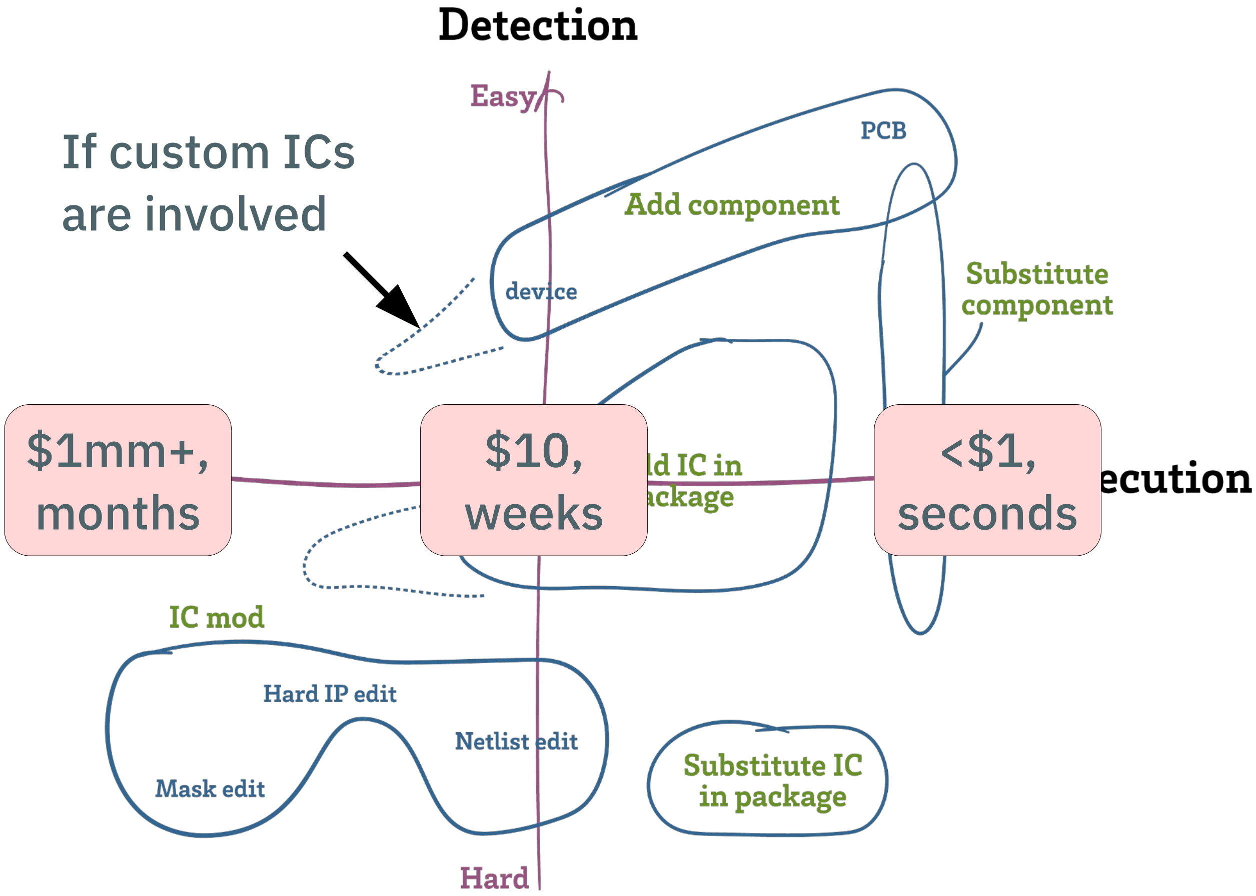
An Ontology of Supply Chain Attacks



Degrees of Detection Difficulty

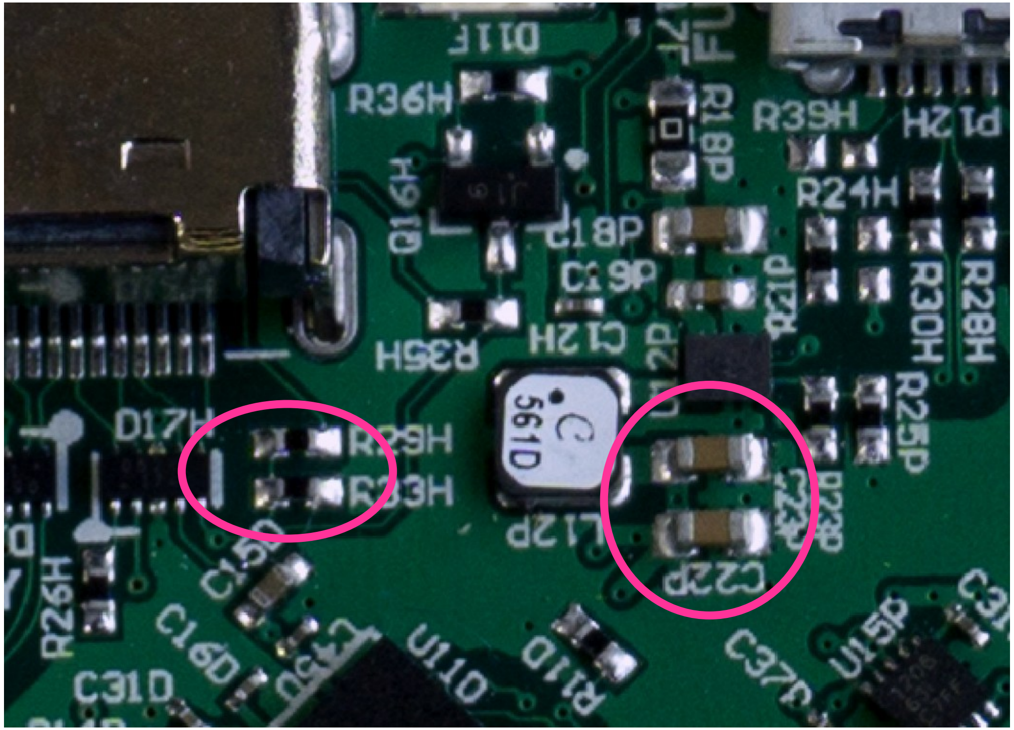


Degrees of Execution Difficulty



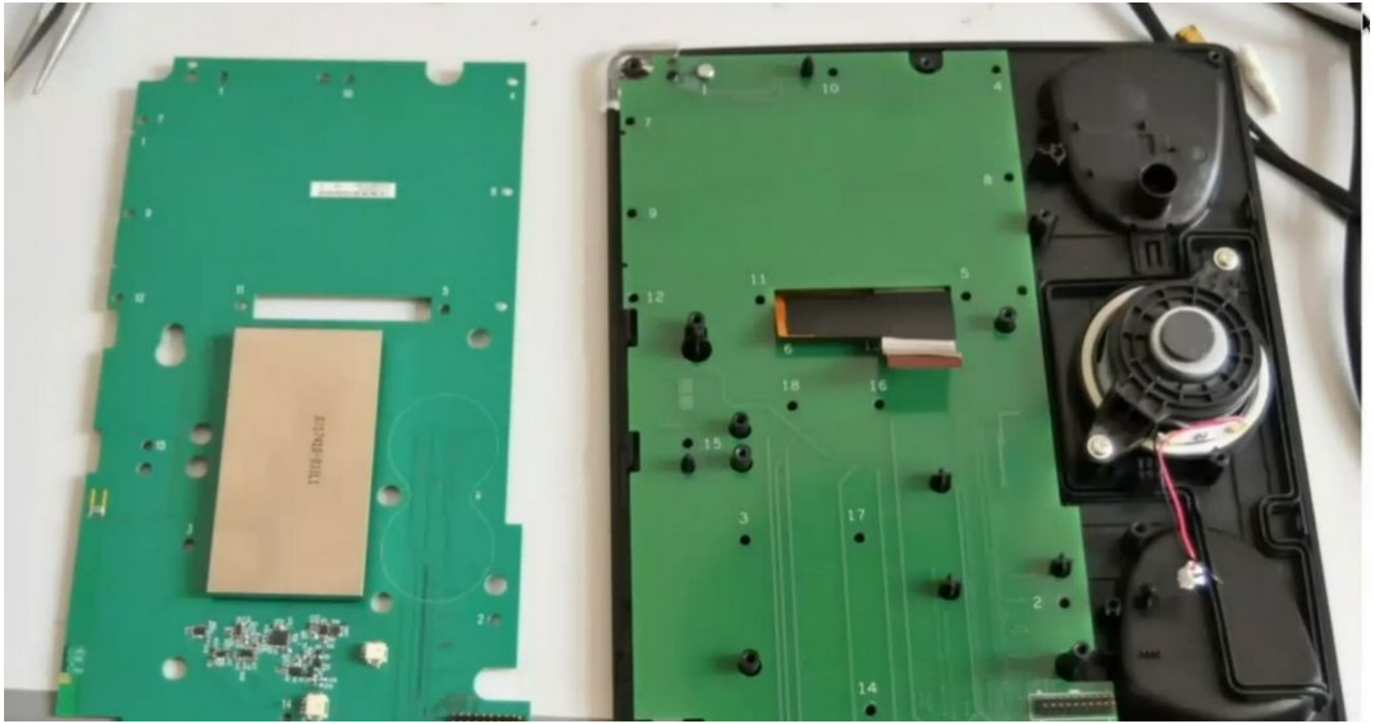
"Substitute Component"

- Relies on the fact that many components look alike



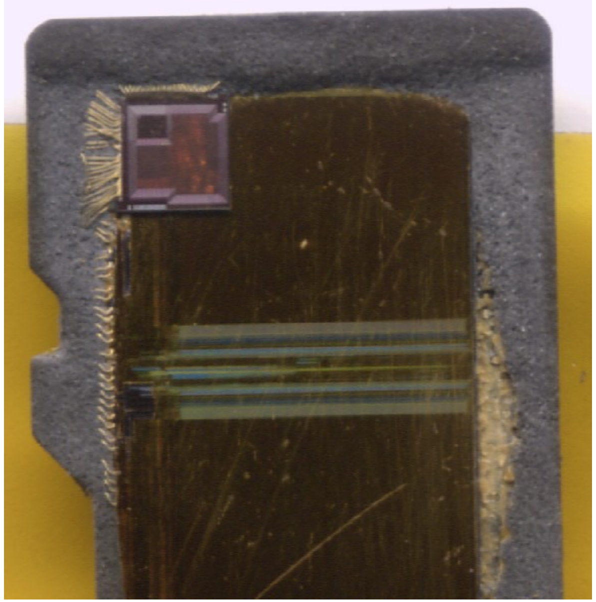
"Add A Component"

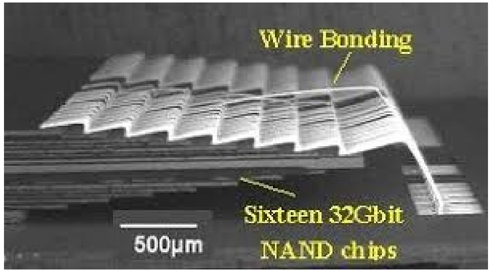
- Easily detectable -> higher awareness

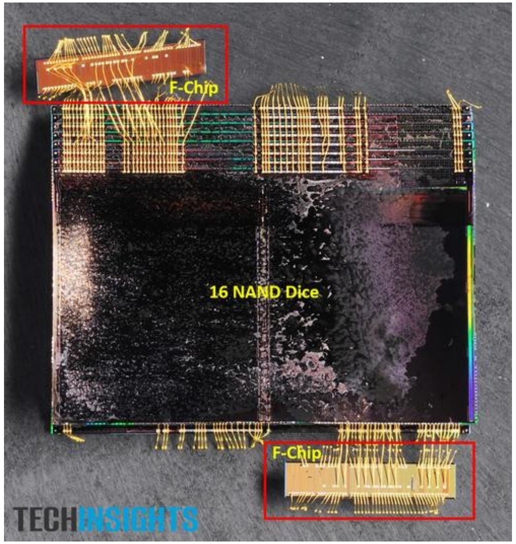


"Add IC in Package"

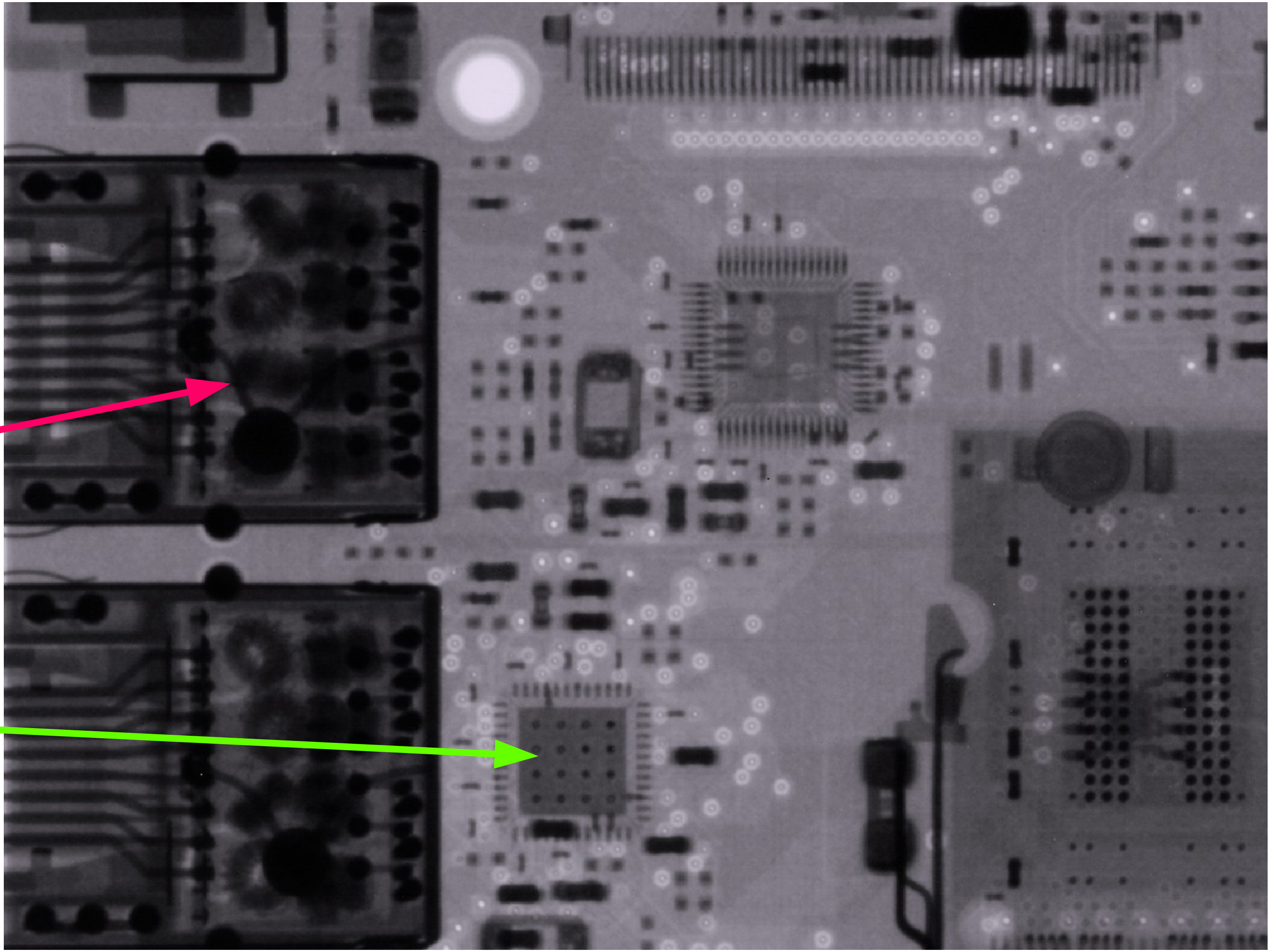
- Hide an additional chip inside a package
- Multiple chips in package is a mature technology





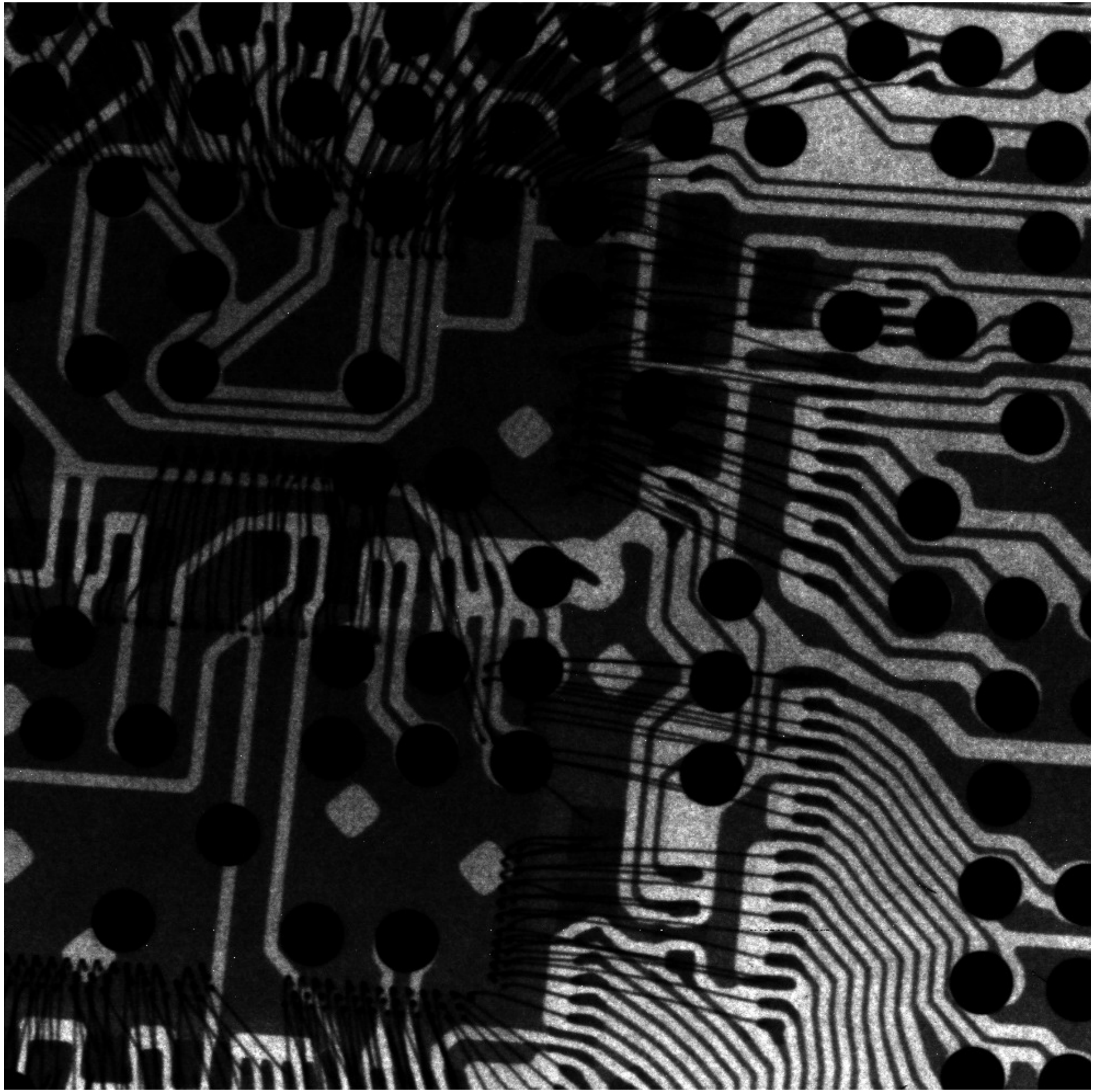


Solution: X-Ray All the Things?



Obvious

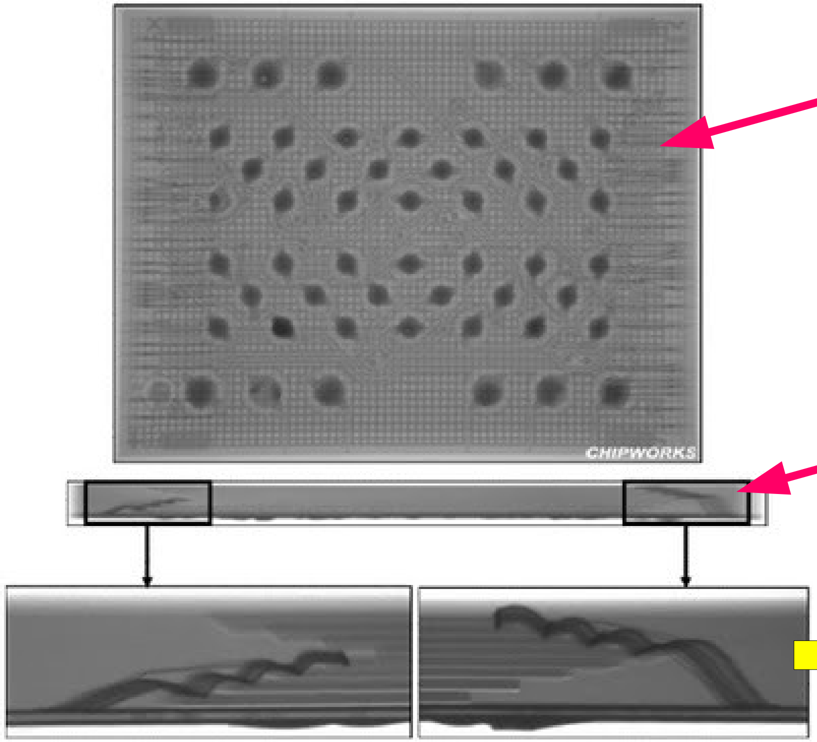
Less obvious



Problem #1

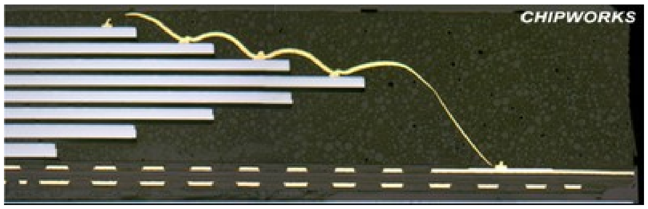
- Silicon (Z=14) is relatively transparent to X-rays
  - Copper traces, solder tend to mask the presence of silicon
- Mitigations
  - CT (Computerized Tomography) scanners
  - X-ray diffraction, spectroscopy

Problem #2: X-Rays Don't Trivially Detect Multiple ICs



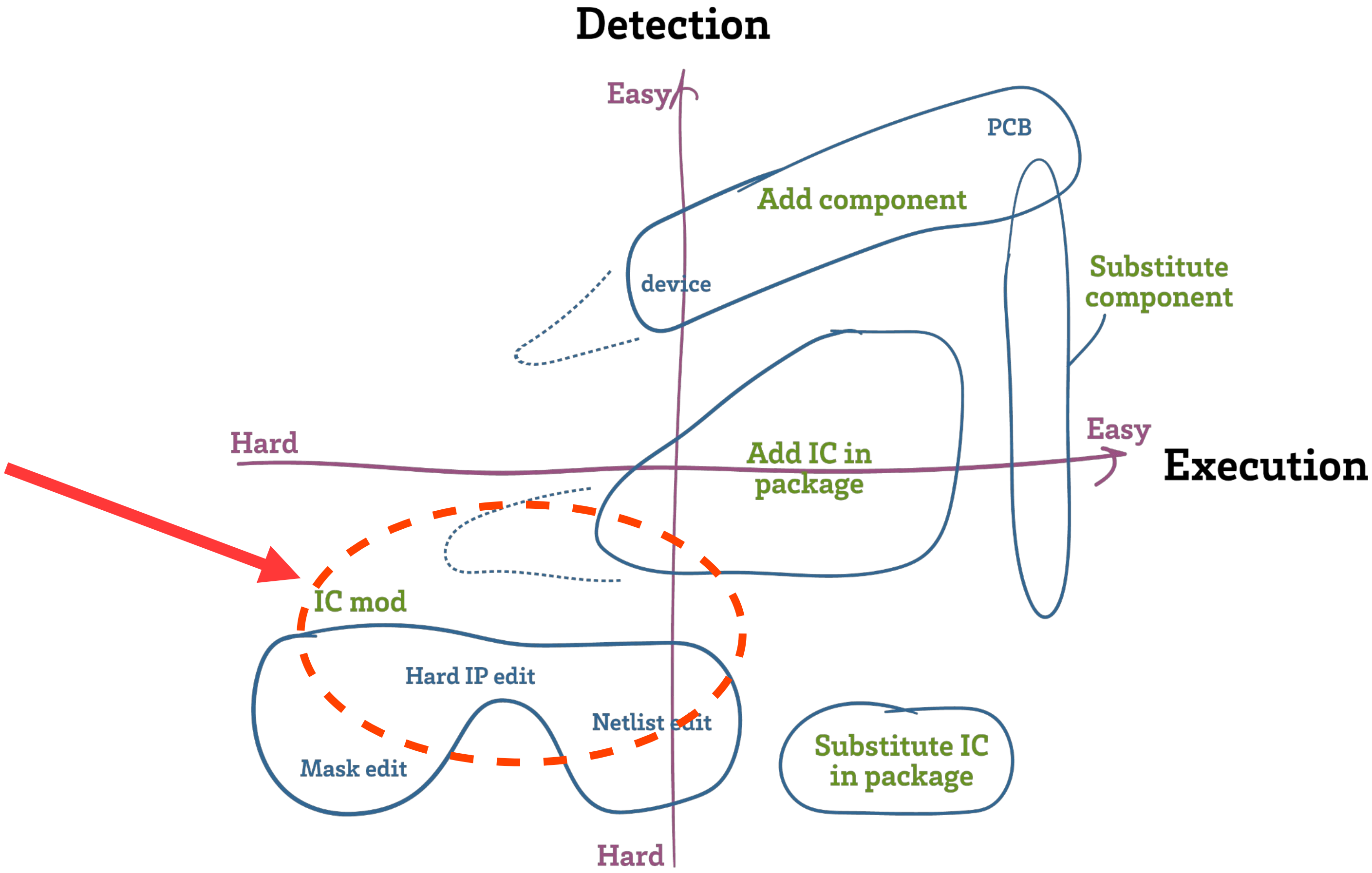
Top view: looks like straight wires

Side view: visible, but requires unobstructed line of sight

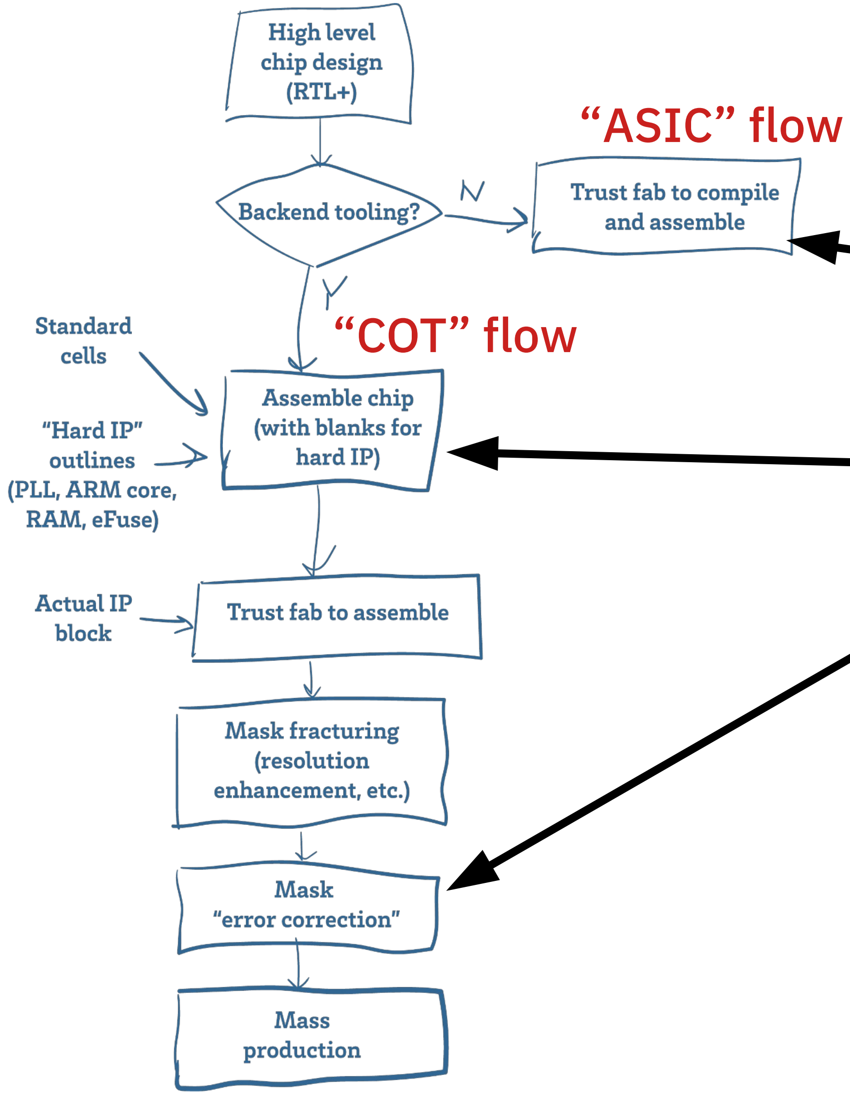


https://electroiq.com/chipworks_real_chips_blog/2010/09/13/samsungs-eight-stack-flash-shows-up-in-apples-iphone-4/

IC Modifications



IC Fab: Attack Surfaces



- Netlist Tampering
  - RTL = Verilog, VHDL, Python
- Hard IP Tampering
- Mask Tampering

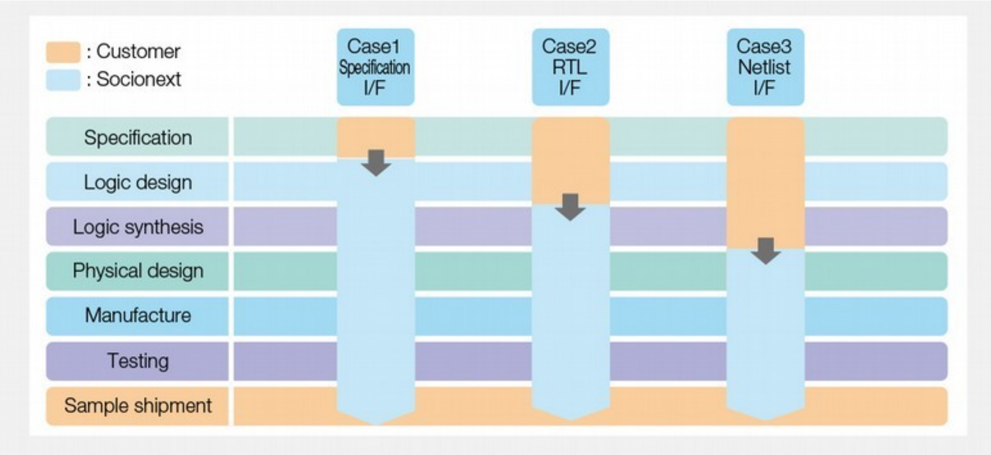
Netlist Tampering: ASIC vs COT

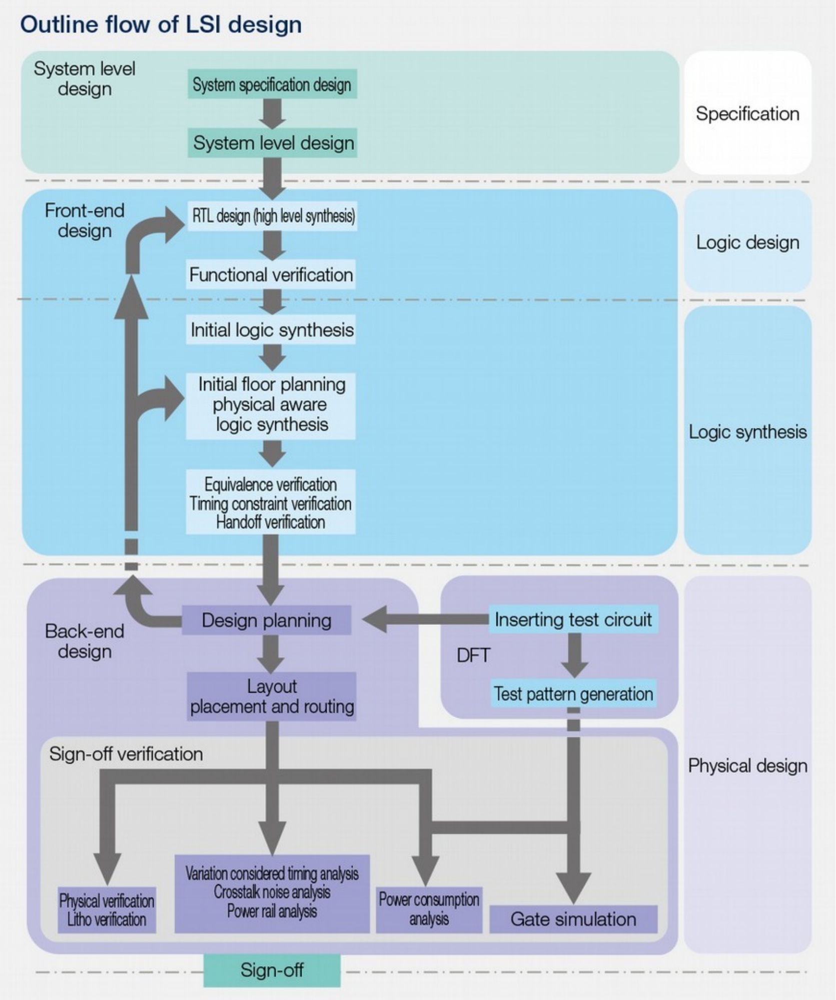
- ASIC – "Application Specific Integrated Circuit"
  - Customer does RTL + floorplan
  - Foundry does detail place/route, IP integration, pad ring
  - Popular for e.g. cheap support chips:
    - Server BMC (Baseboard Management Controller)
    - Disk controllers
    - Mid-to-low end I/O controllers

- COT – "Customer Owned Tooling"
  - Customer does full flow, down to a nominal GDS-II mask
  - Several extra headcount + $millions for back-end tooling software
  - Necessary for high-performance / flagship products (CPU/GPU/router)

ASIC Design Flow Example: SOCIONEXT

- One of many billion-dollar ASIC companies you've never heard of

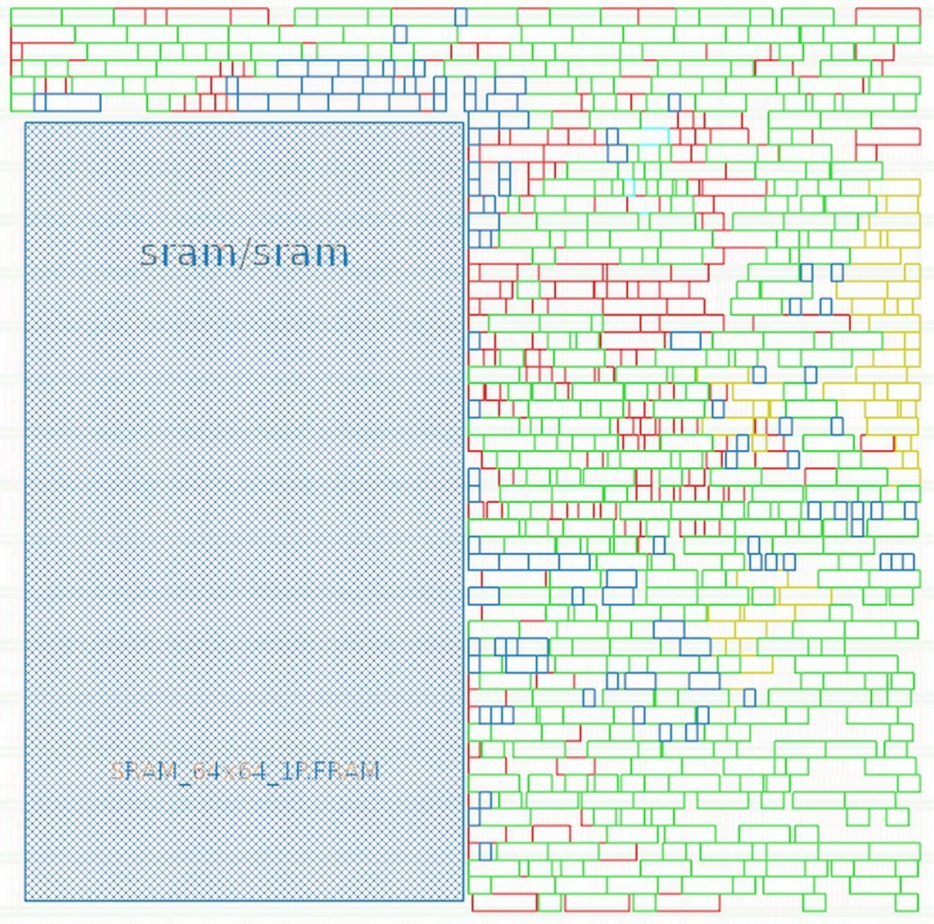




So I'm Safe with COT, Right?

COT Weaknesses: "Hard IP"

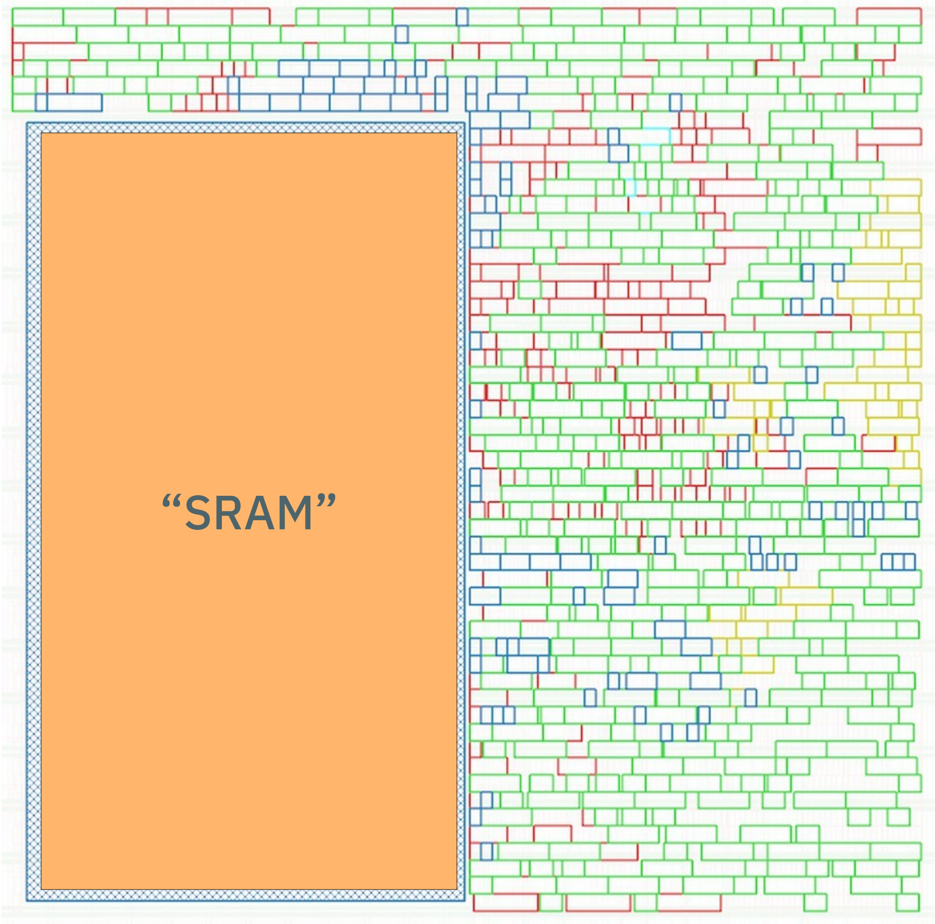
- COT designers still leave large “holes” in the layout for hard IP
  - Foundry merges proprietary blocks with agreed upon connection points



https://cornell-ece5745.github.io/ece5745-tut8-sram/

COT Weaknesses: "Hard IP"

- COT designers still leave large “holes” in the layout for hard IP
  - Foundry merges proprietary blocks with agreed upon connection points



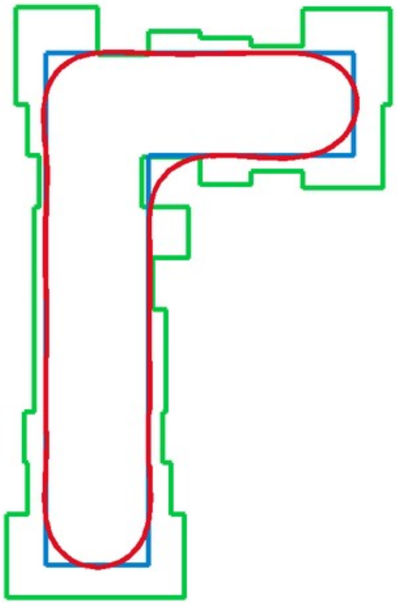
https://cornell-ece5745.github.io/ece5745-tut8-sram/

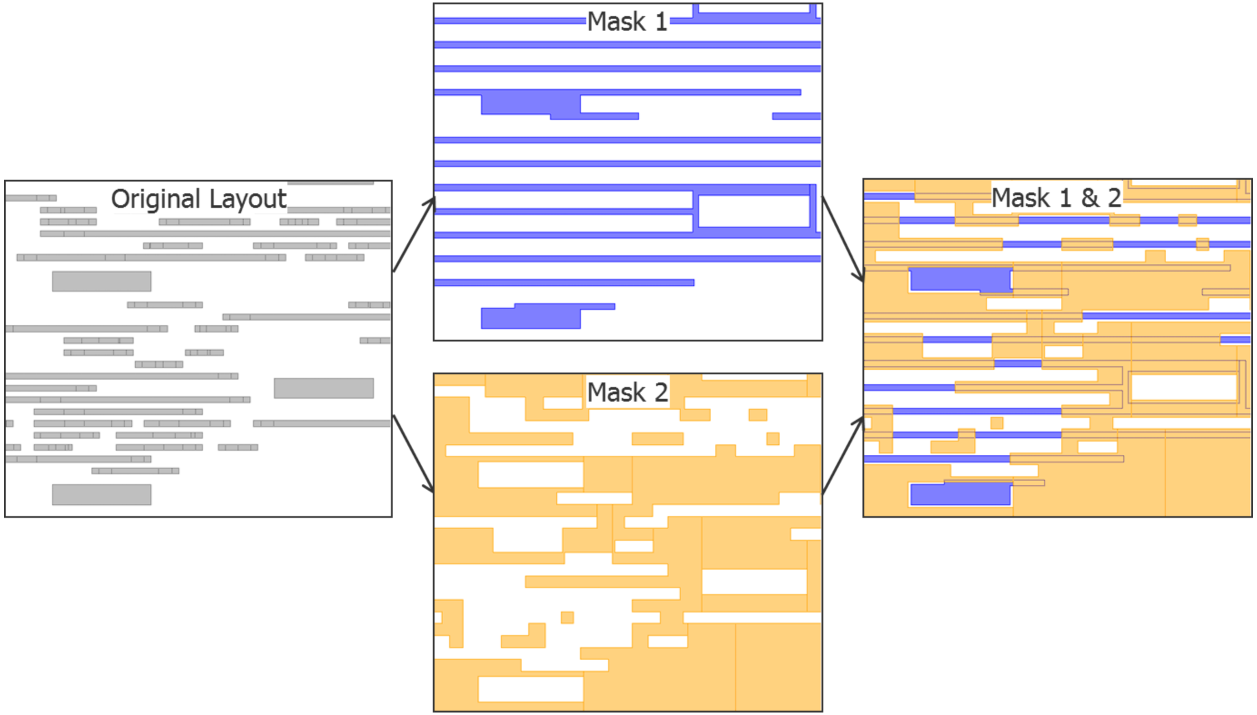
Hard IP: Who Cares?

- RF/analog
  - PLL, ADC, DAC, bandgap
- RAM
- ROM
- eFuse
- Pad rings
- Basically, all the points you need to backdoor an IC

Mask Tampering: Post-Design Processing

- Sub-wavelength features requires substantial mask post-processing

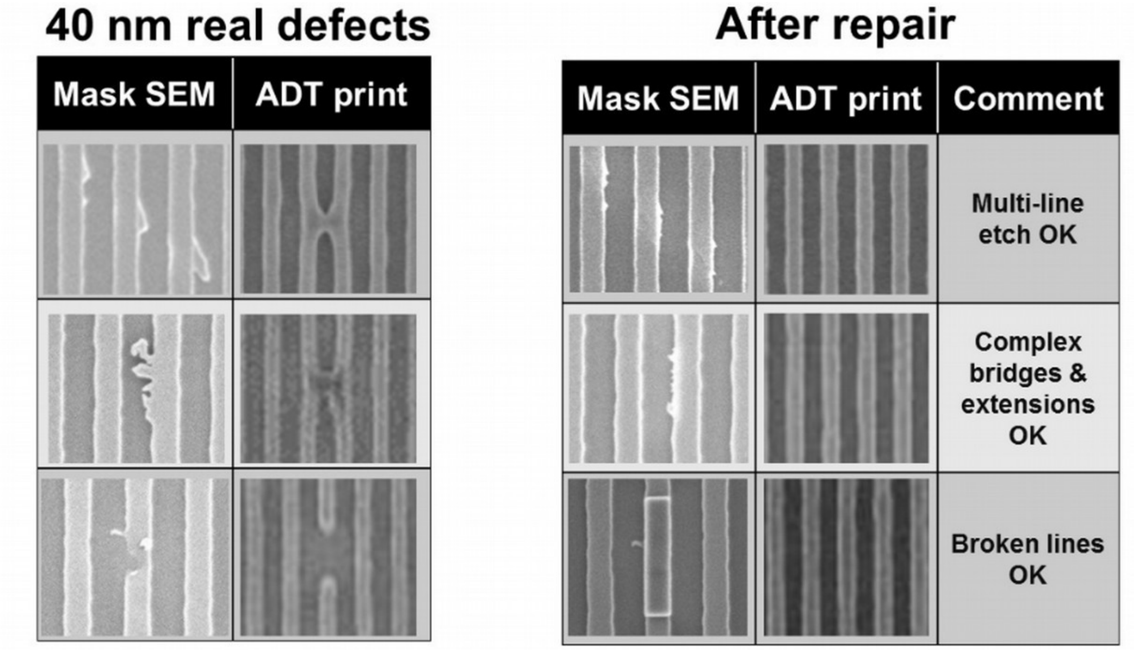




https://semiengineering.com/self-aligned-double-patterning-part-one/

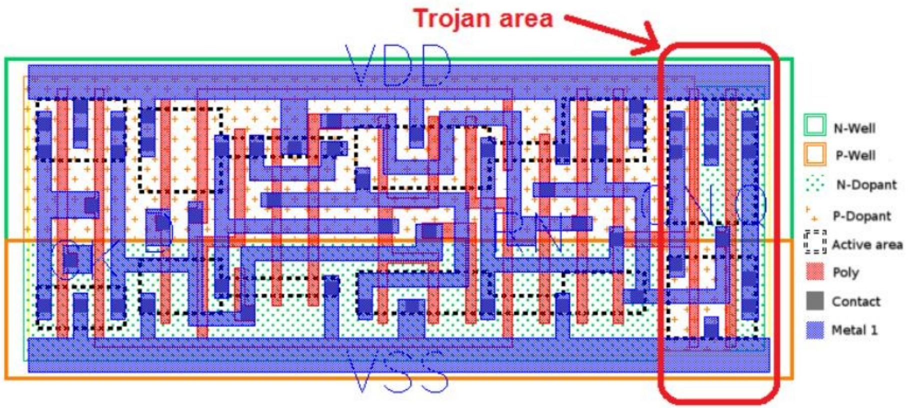
Mask Editing

- All masks go through an editing ("checking") step



Proc. of SPIE Vol. 8322 83220C-1

What Can you Do with Mask Editing?

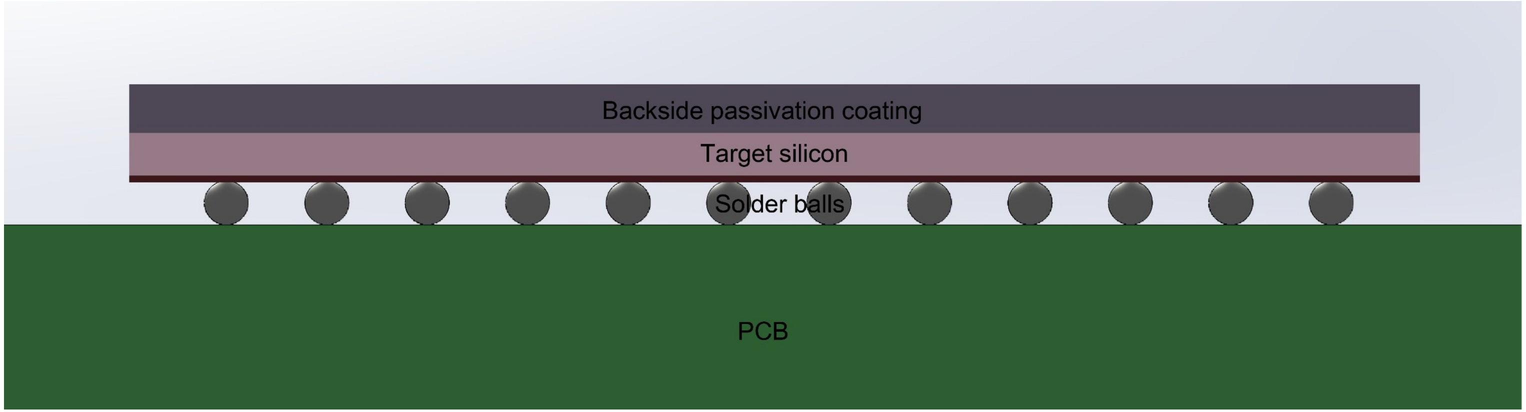


http://people.umass.edu/gbecker/BeckerChes13.pdf

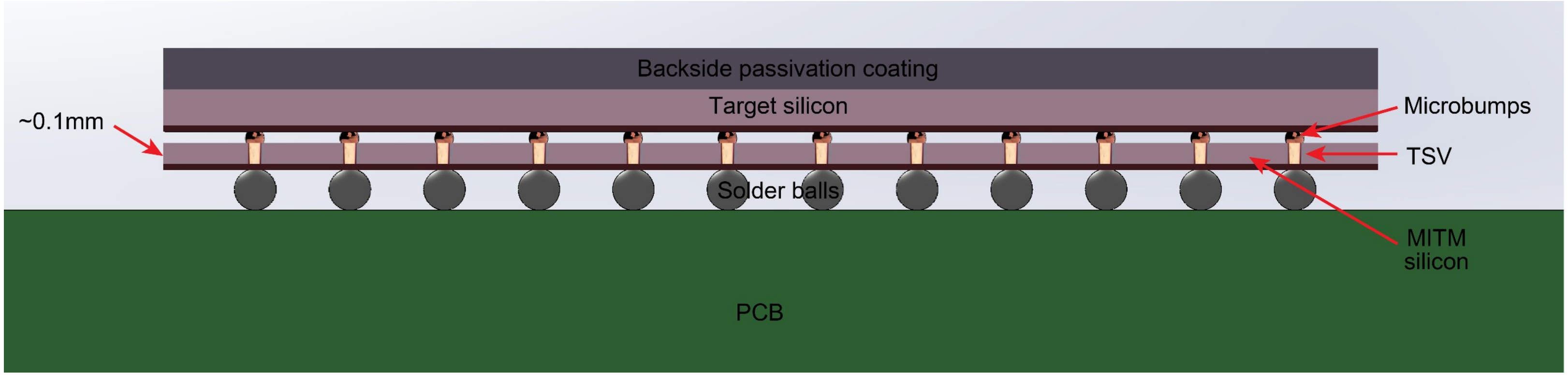
- Example: Dopant Tampering
  - No morphological change
  - Circuit-level behavioral change
- Spare cell rewiring
- Signal bypass

My Personal Fear: TSV + WLCSP Implants

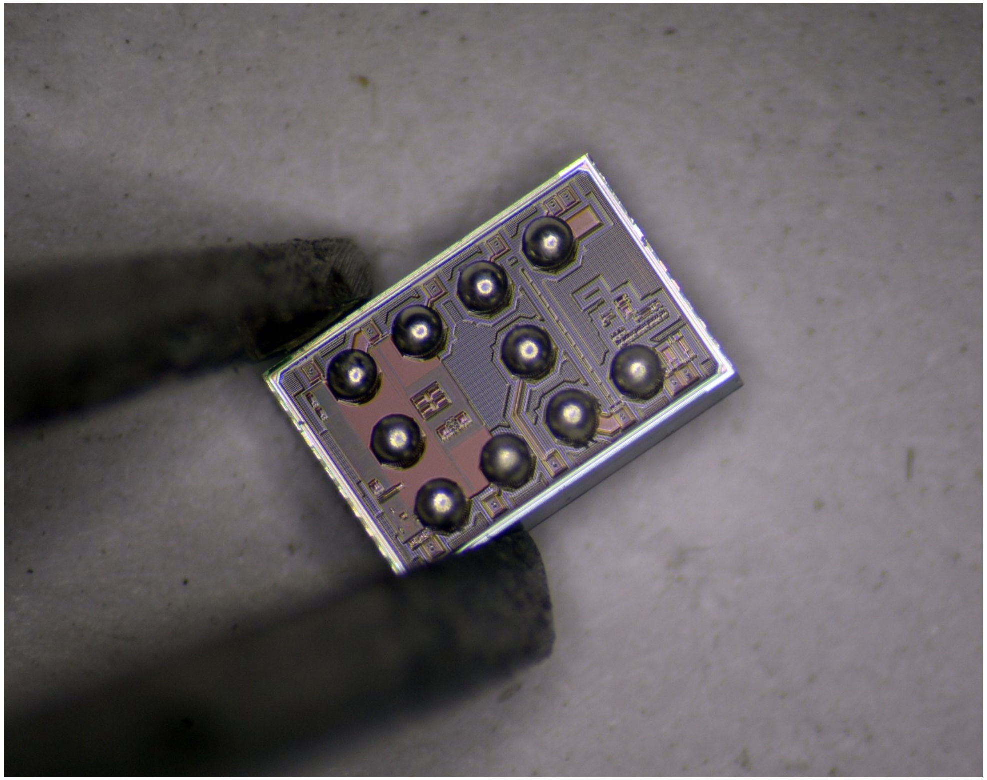
Unmodified



With TSV implant



Concept: WLCSP

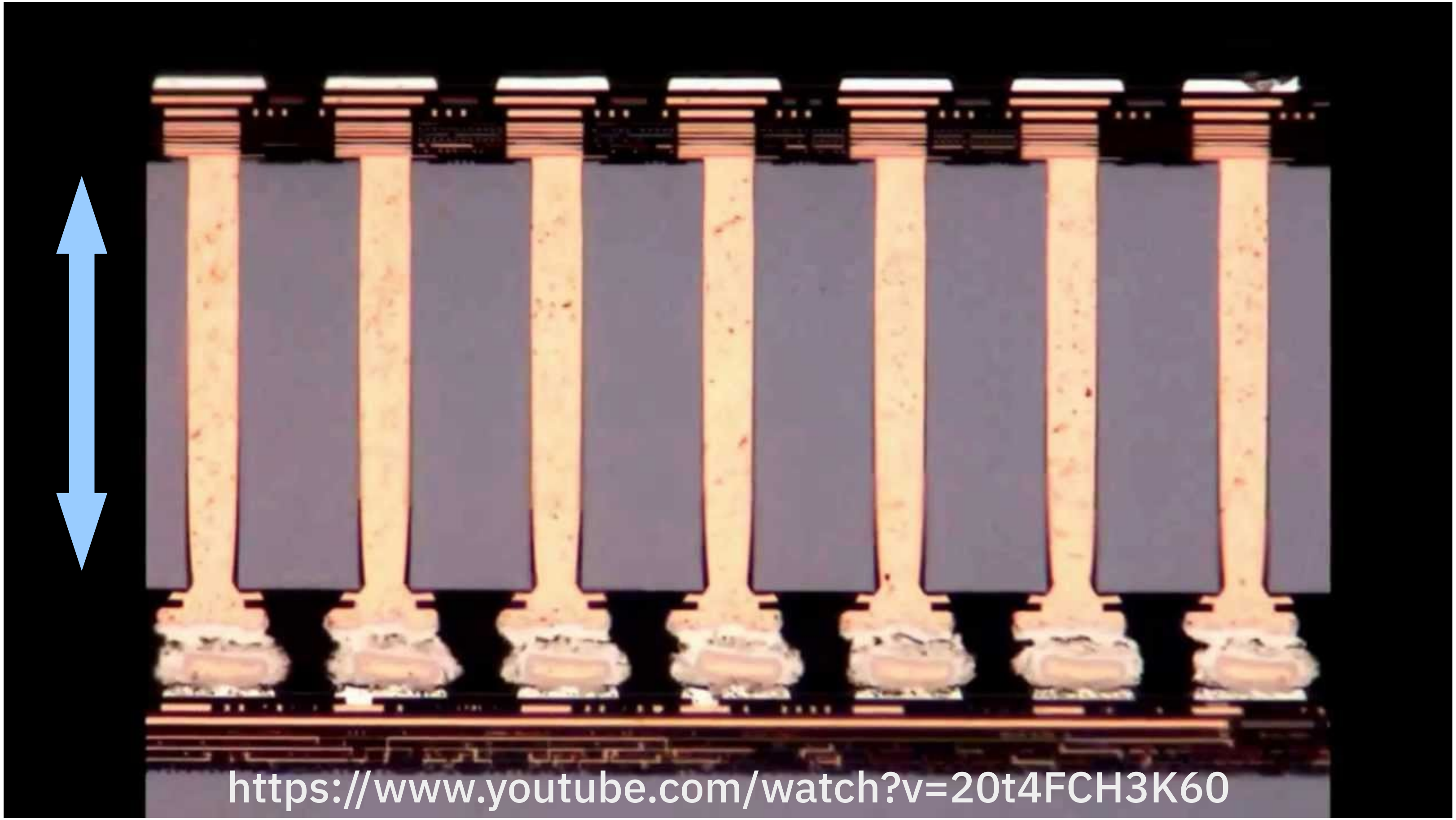


Wafer
Level
Chip
Scale
Package

- Sold as "almost naked silicon"
- Direct chip-to-board solderballs
- Sold as "Ready to Hack"

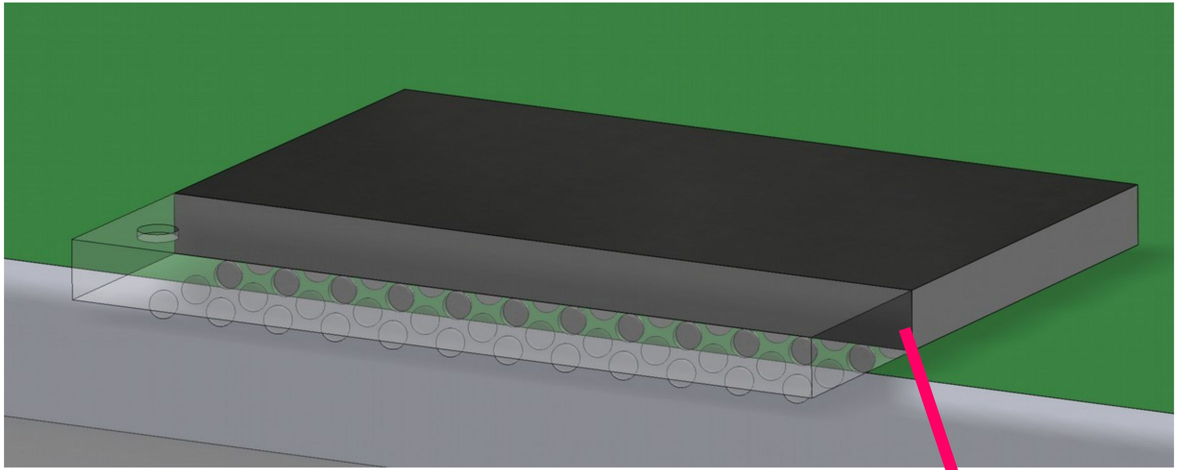
Concept: Through-Silicon Via
"Mature" Tech (Used in HBM RAM)

0.1-
0.2mm

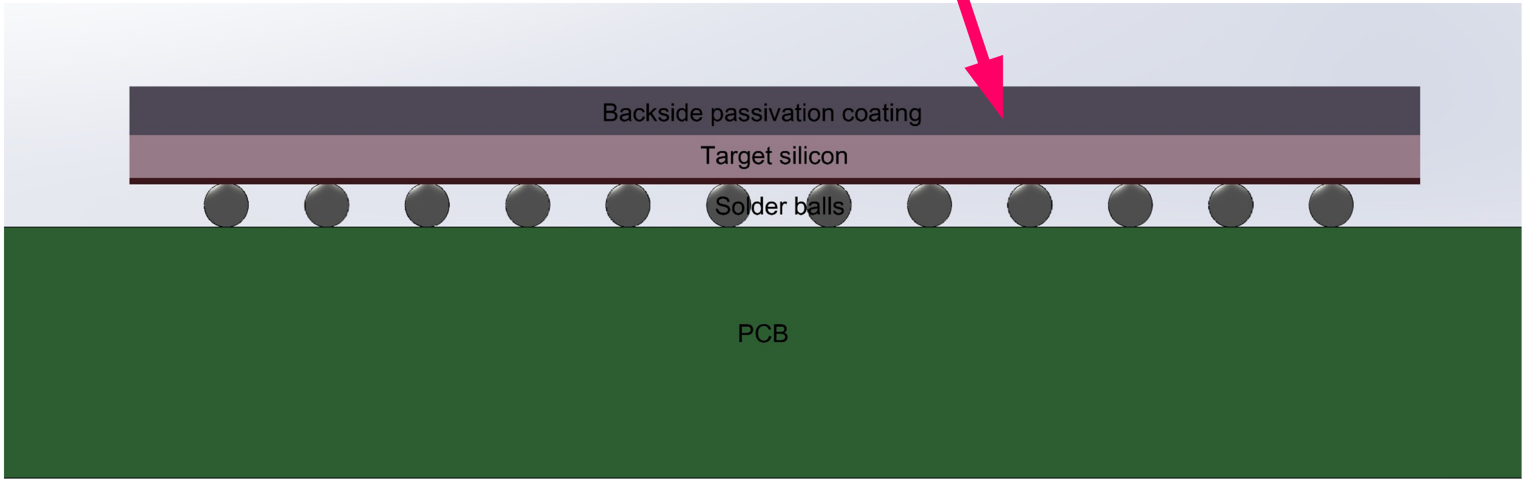


WLCSP Cross Section

3D view

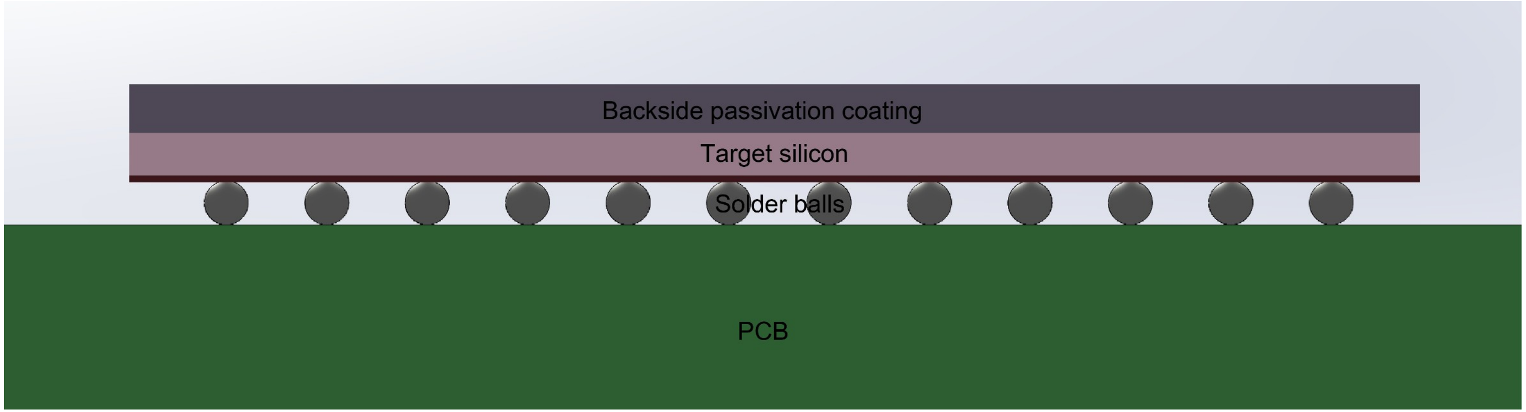


Cross section

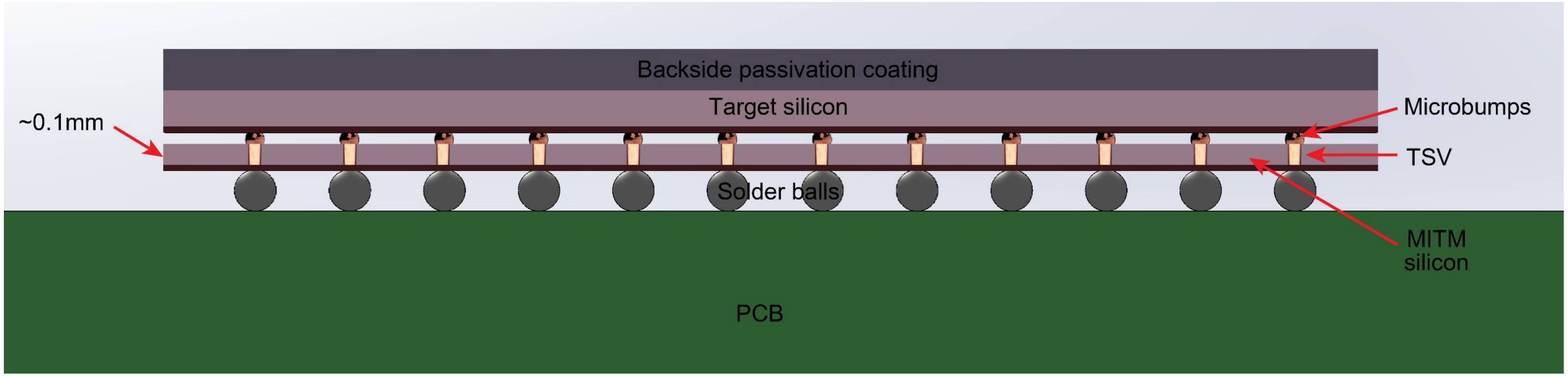


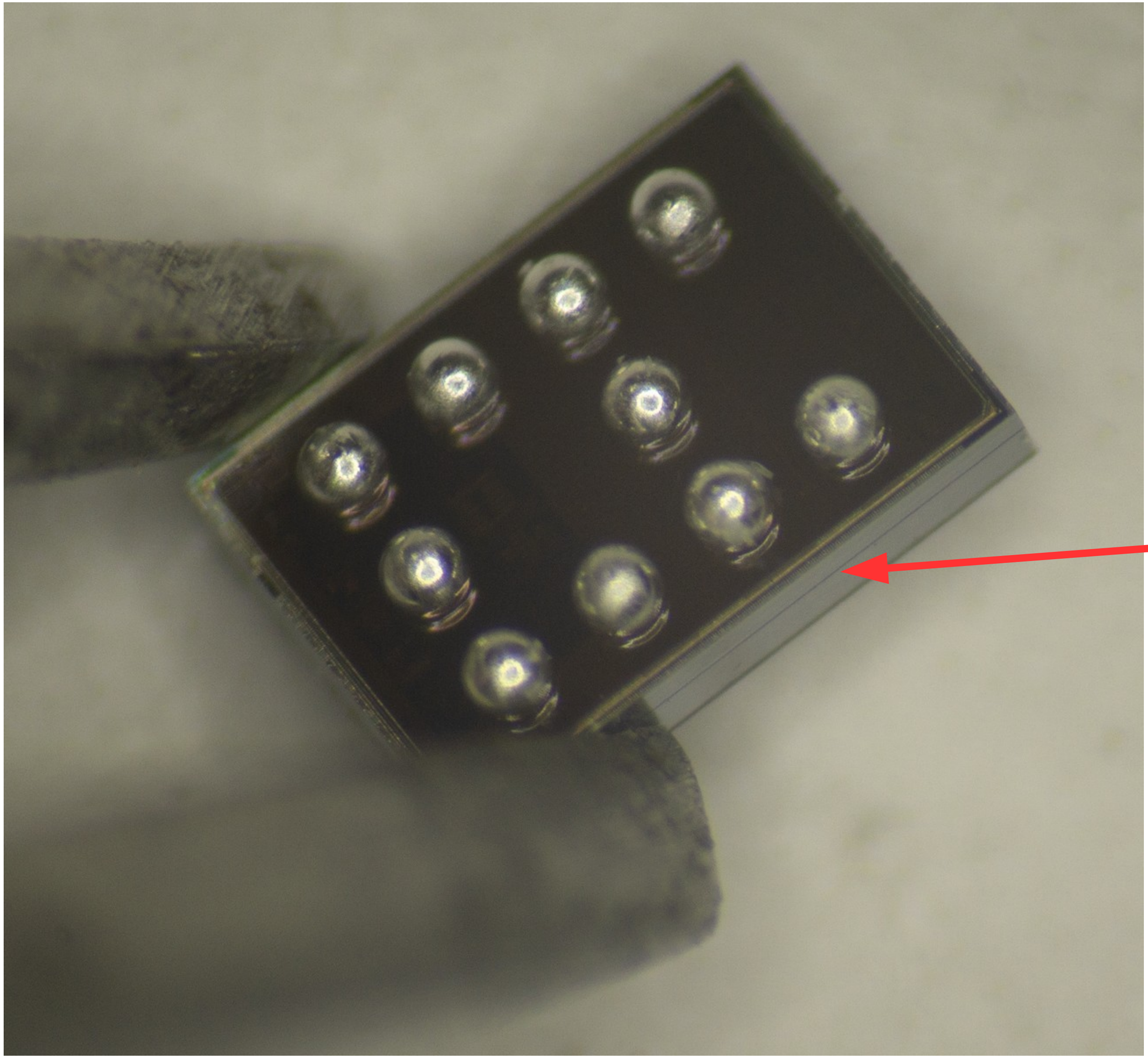
TSV + WLCSP = Nearly Undetectable Implant

Unmodified



With TSV implant



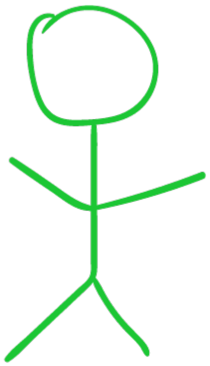


Threat & Mitigation

- Scalable
  - Targets off-the-shelf chips
  - No decap / debond
- Hard to detect
  - Many WLCSP already have a small seam
  - No X-ray footprint
- Mitigation:
  - TSV templates are "expensive" ($100k's)
  - But Pegasus is even more expensive ($1mm+)...

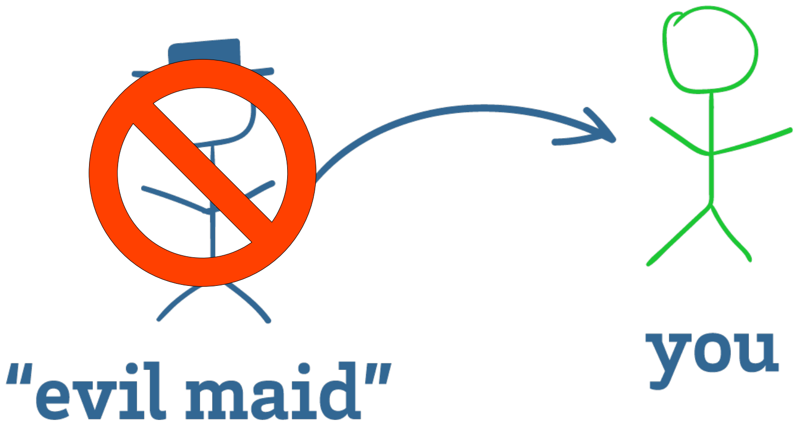
Execution of Supply Chain Attacks:

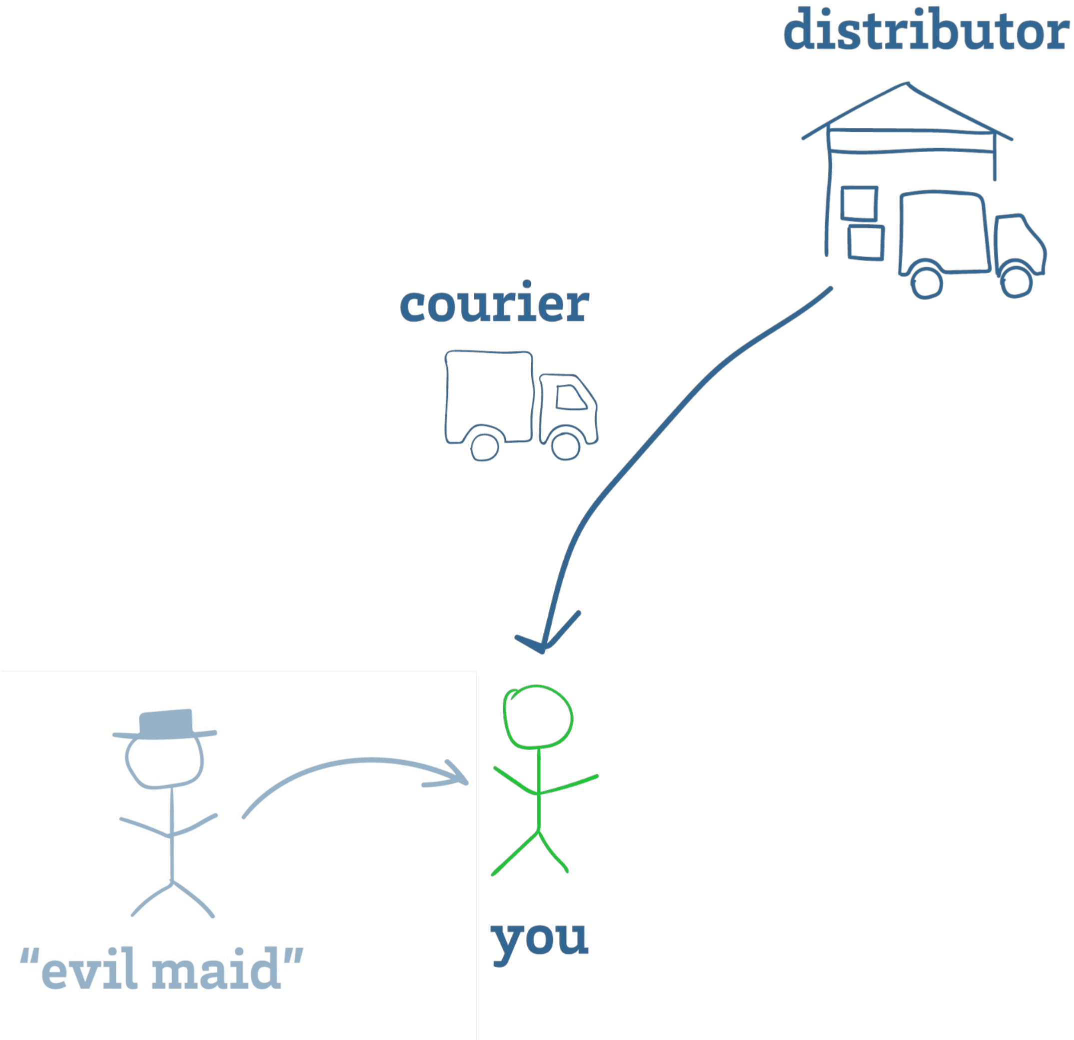
The Attack Surface



you

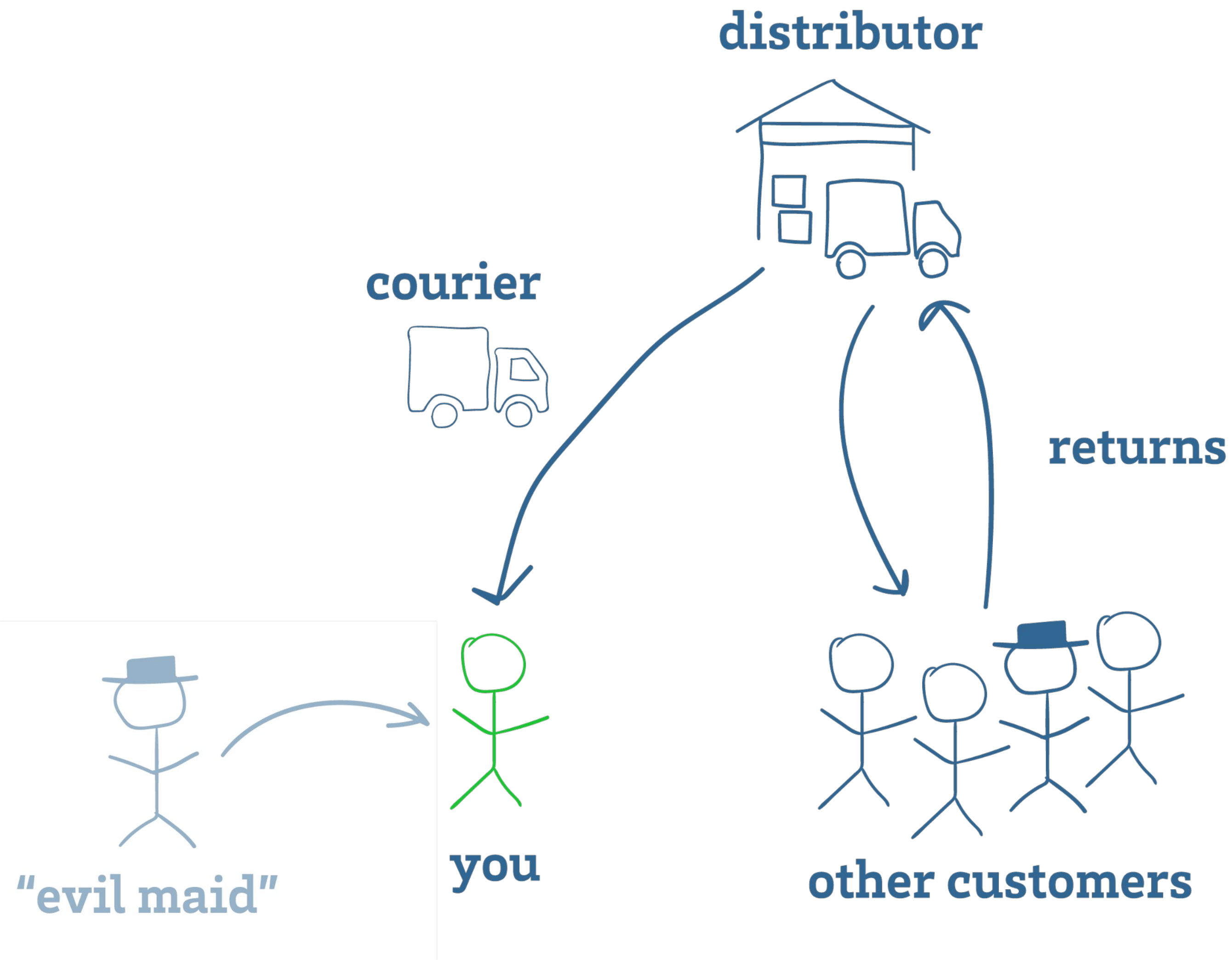
We're Not Going to Talk about "Evil Maids" (But They are Also Real)




distributor
courier
"evil maid"
you

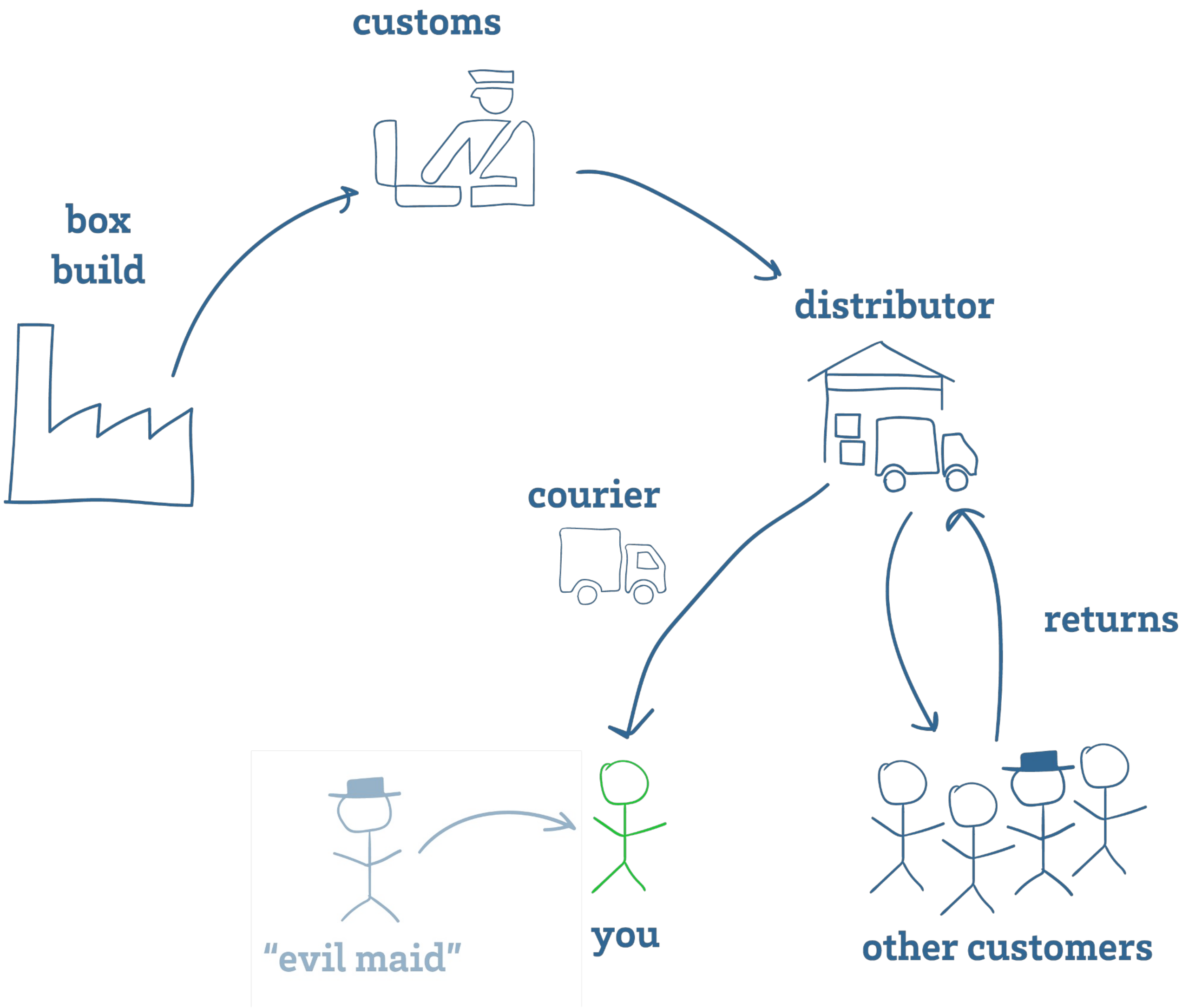
(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

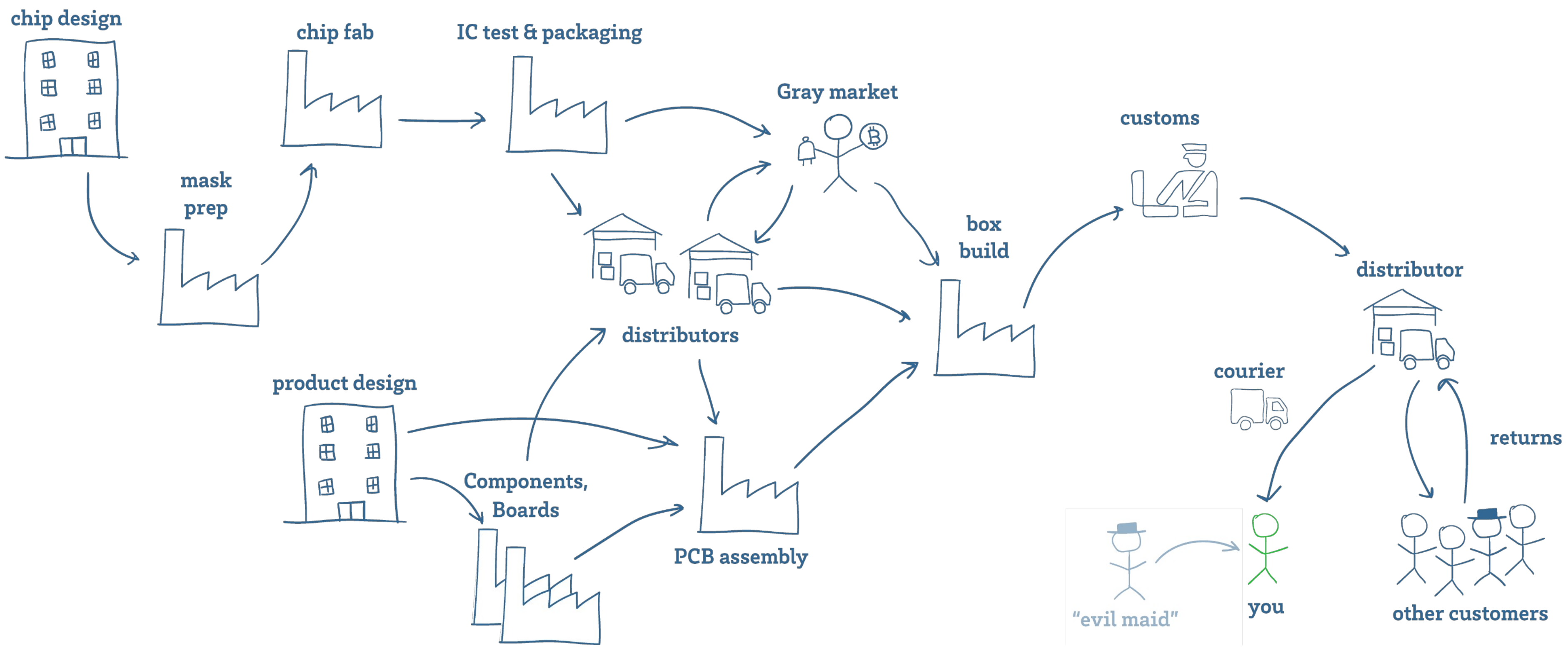

distributor
courier
returns
"evil maid"
you
other customers

Everyday Hacks
for Everyday ~~People~~ Targets

- DIY supply chain attack:
  - Buy item online
  - Hack it
  - Return it to warehouse
  - ???
  - Profit!

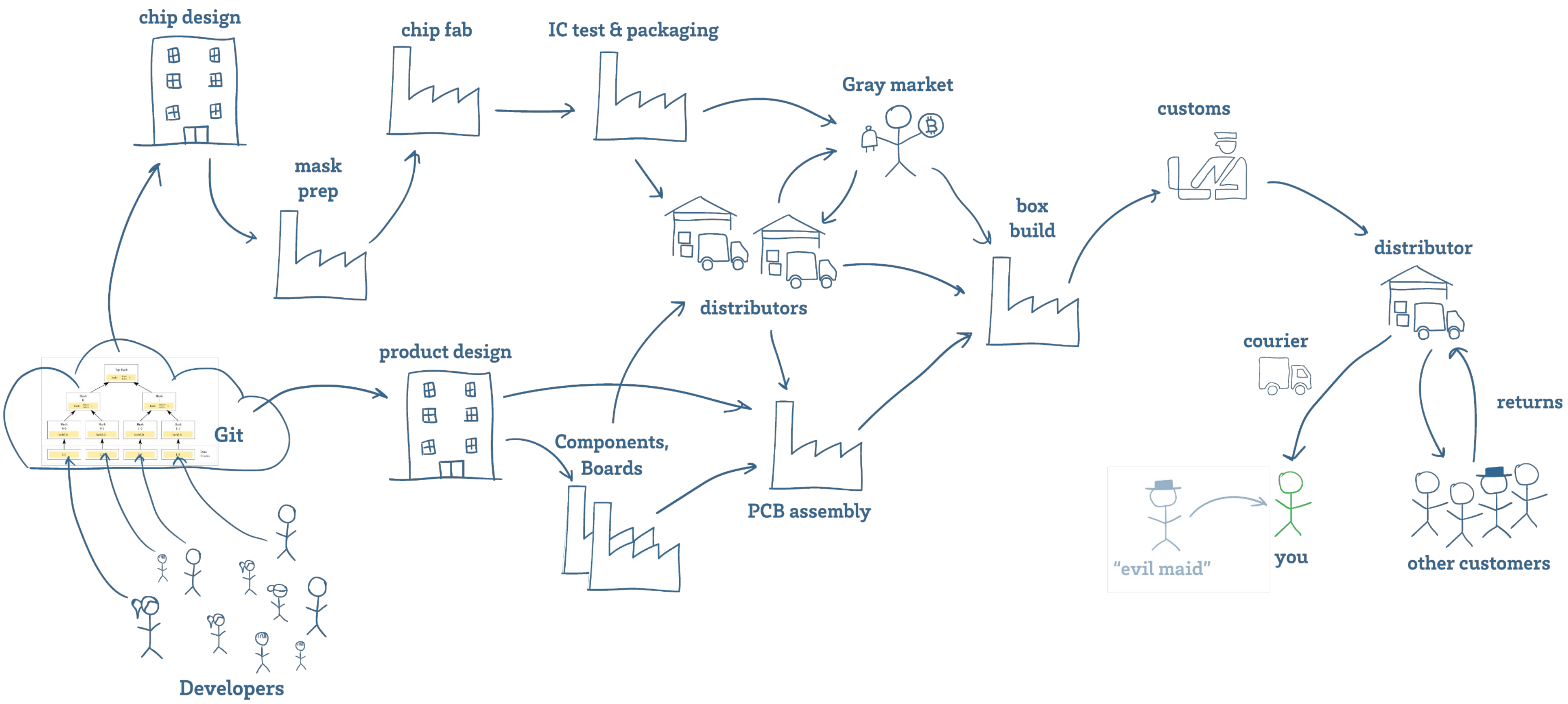

customs
box
build
distributor
courier
returns
"evil maid"
you
other customers

It's a Big Attack Surface

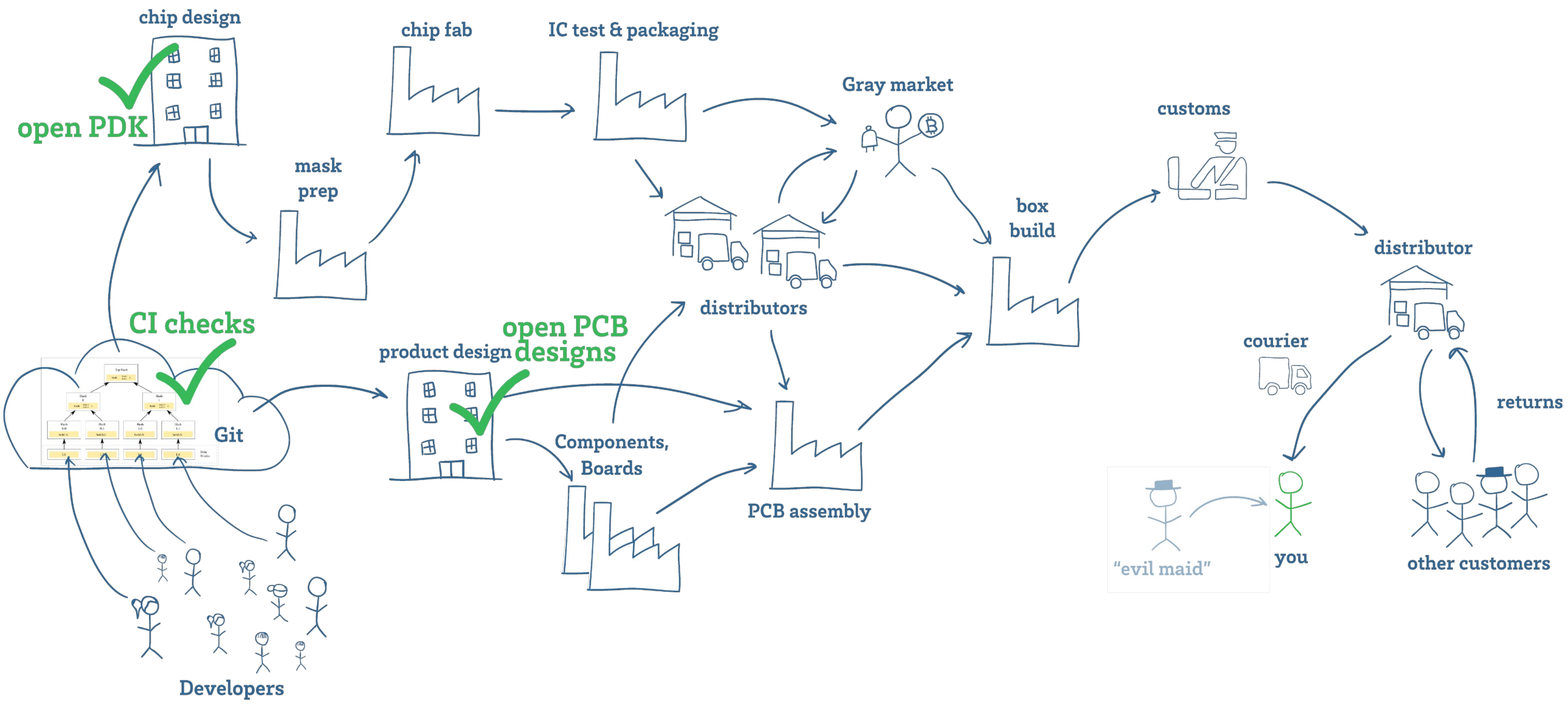


What Can We Do About It?

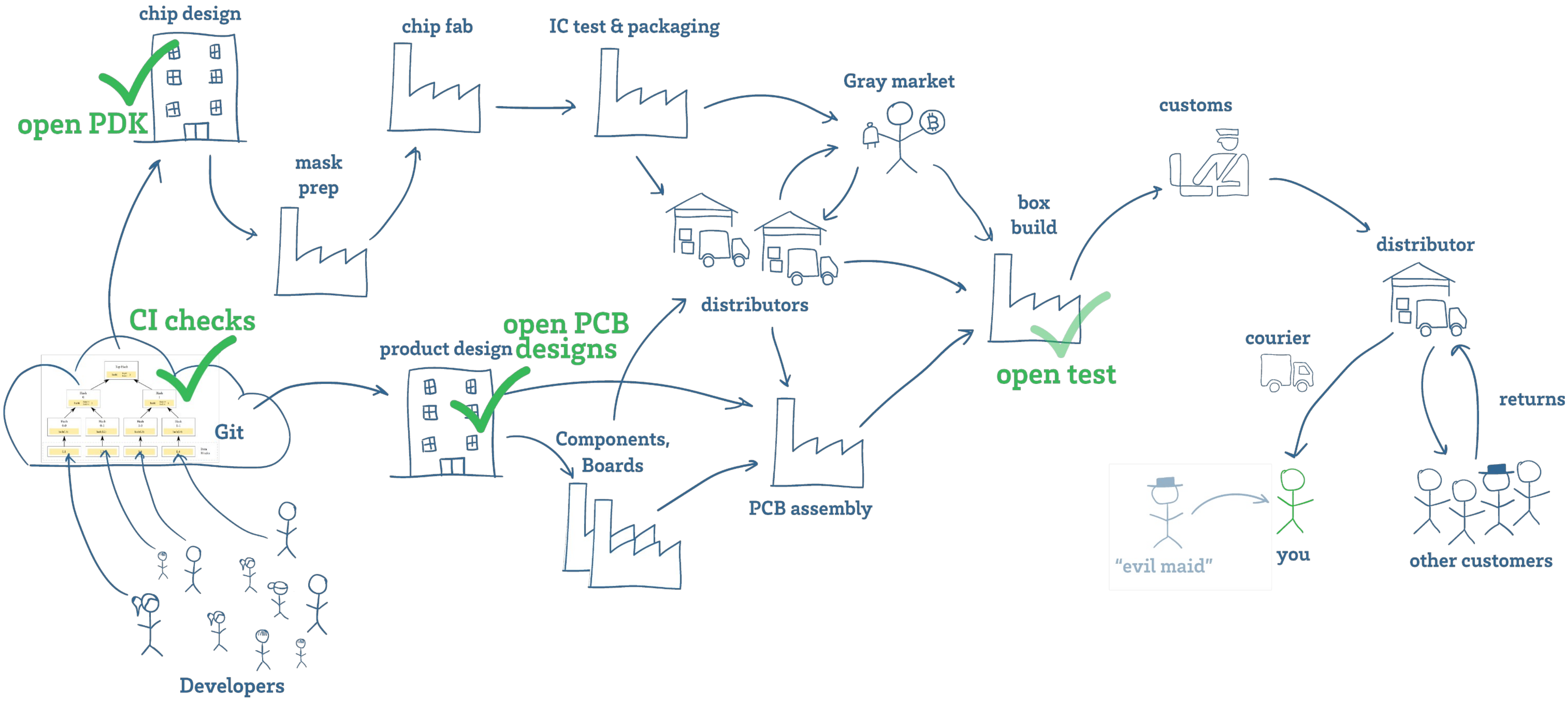
Can Open Source Save Us?



Problem: Place of Check Too far from Place of Use



Open Factory Test (Trustable Factory) Is Only a Marginal Improvement



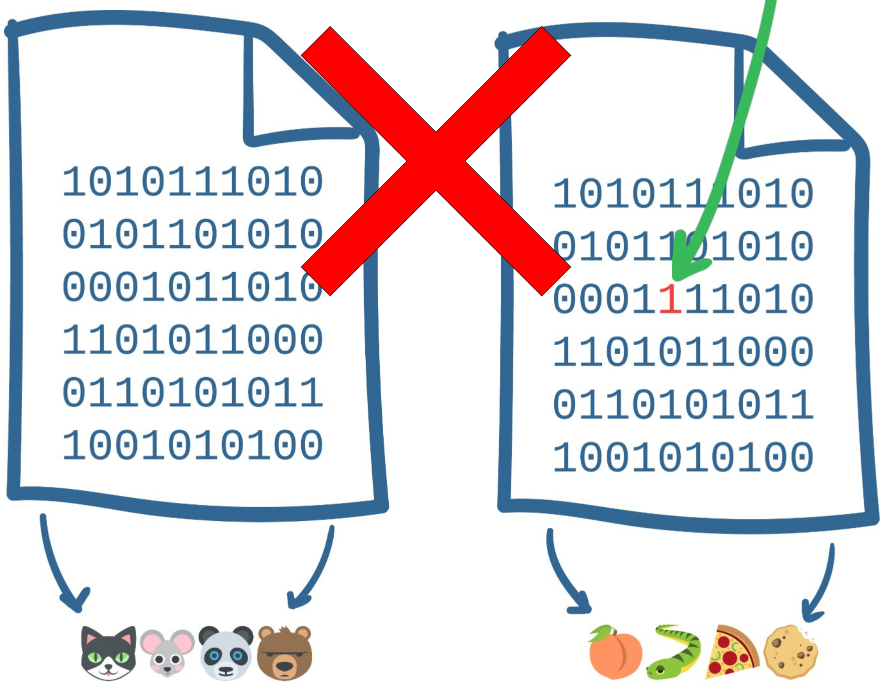
What, Then Is the Role of Open Source in Trustable Hardware?

- Design Correctness
  - Peer review can find bugs
  - SPECTRE hardening
    - Microarchitectural state modeling in compilers
    - Potential for provably correct compiler mitigations

The Big Problem: You Can't "Hash" Hardware

- There is no convenient, easy-to-use method to confirm the correctness of hardware immediately before its use

- Hardware is one big "Time of Check versus Time of Use" (TOCTOU) problem!



But You Once Said: "There's Always a Bigger Microscope..."

- "Ptychographic X-Ray Imaging" to the rescue?
  - Non-destructive
  - 3D imaging of complex chips
  - Great for reverse engineering and design verification

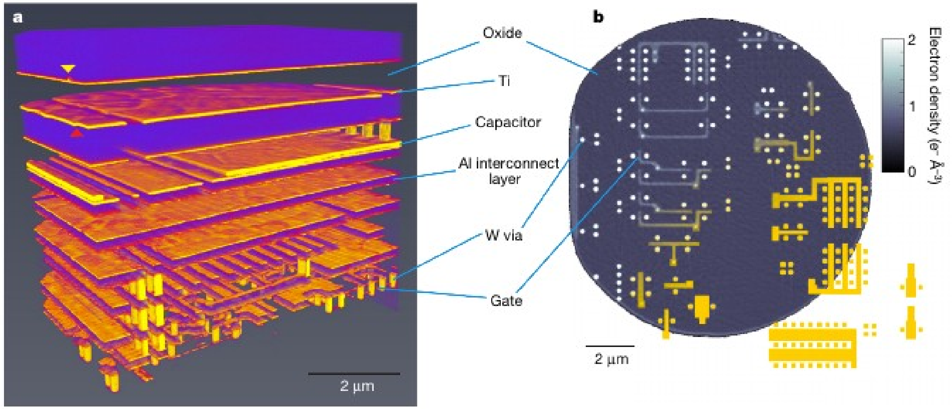


Figure 2 | PXCT of detector ASIC chip. a, 3D rendering of the PCXT tomogram with identified elements. The yellow triangle indicates a manufacturing fault in the Ti layer. The Al layer in the region of the red triangle shows variances in thickness causing a waviness of the Ti layer on top. Via, through-layer connector. **b,** Axial section across the second lowest layer, which contains the transistor gates; the grey scale (top right) represents electron density (in $e^- Å^{-3}$). The corresponding layer from the design file is shown as the partial overlay in yellow.

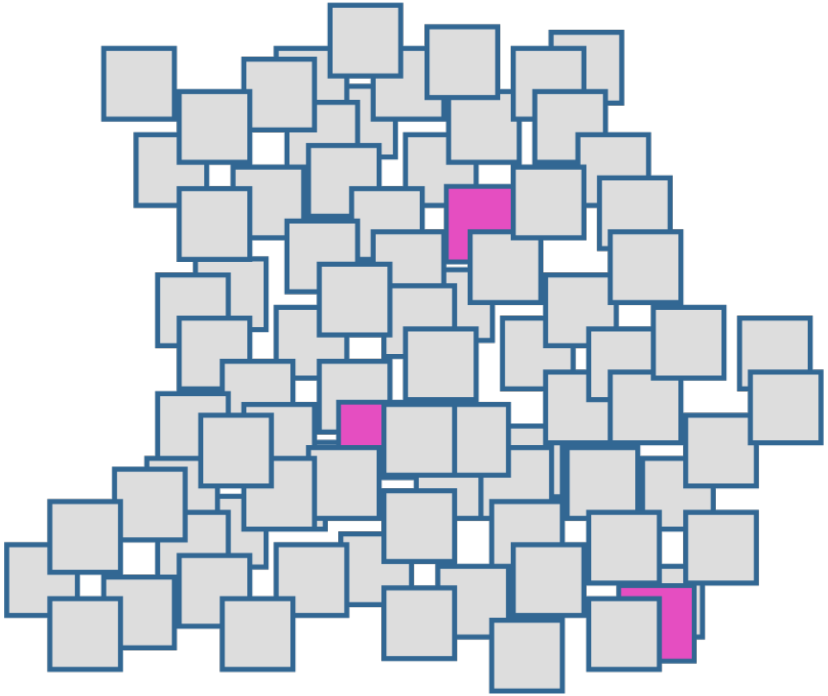
https://www.nature.com/articles/nature21698

Problem #1: A Building-Sized Microscope

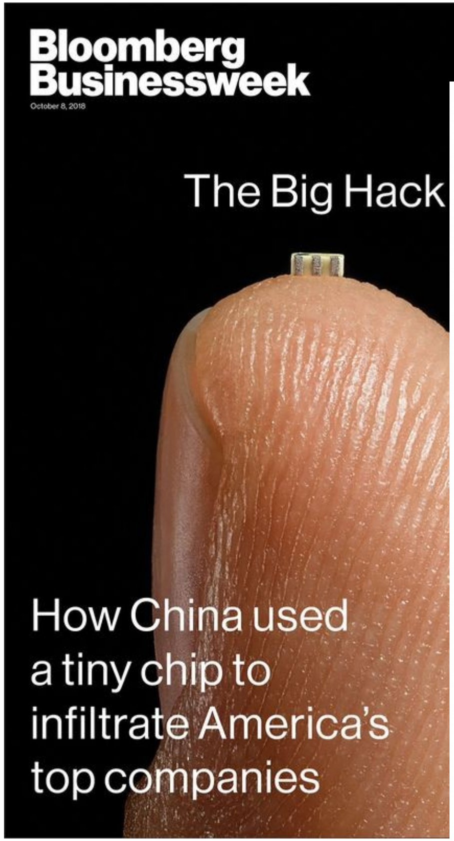
https://www.psi.ch/en/sls/about-sls

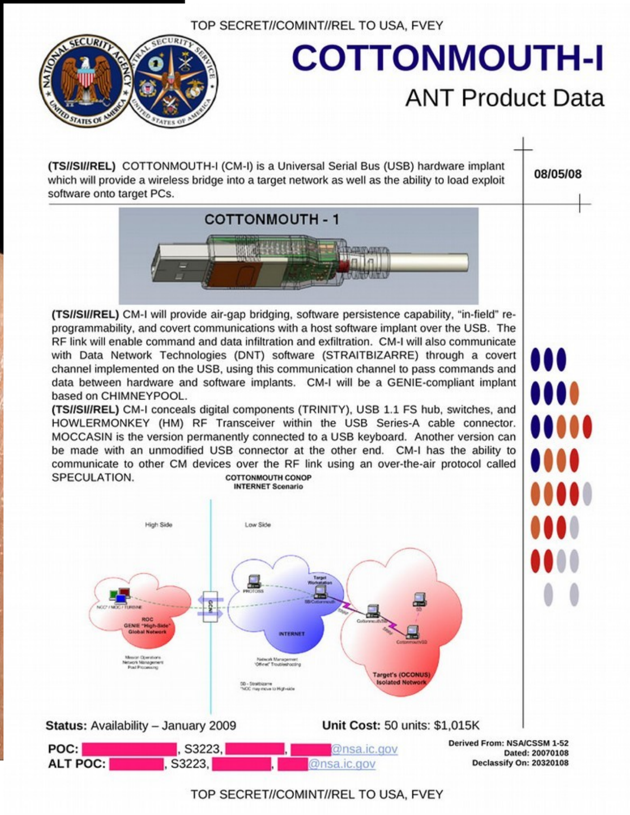
Problem #2:
Verifying One Chip Verifies Only One Chip

- Just because 99.9% of your hardware is OK...
  - Doesn't mean you are safe
  - One compromised server out of thousands is all it takes
- Random sampling is not effective
  - Would you "random sample" signature checks on downloaded software?



Can We Build an Evidence-Based Case To Trust Our Computers?





TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

08/05/08

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

Three Principles For Evidence-Based Trust in Hardware

1) Complexity is the enemy of verification

2) Verify entire systems, not just components

3) Empower end-users to verify and seal their hardware

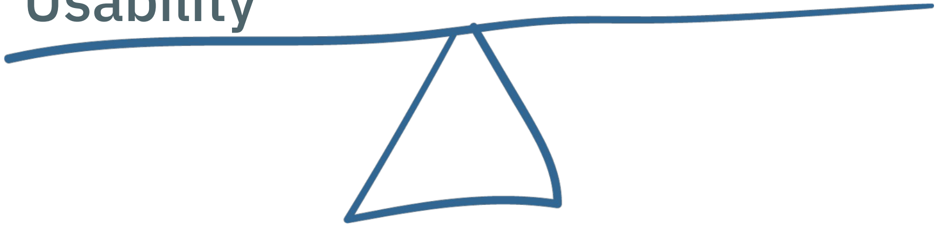
Problem: Complexity is Complicated

- Absent a robust "hashing" function, verification falls back to bit-by-bit…or "atom-by-atom"
- More complexity ->
  - More difficult to verify
  - More places to hide things
  - Verification might be destructive

via iFixit

Point of Use Verification Tradeoff: Ease of Verification vs. Features & Usability

>10^7 transistors



1 transistor

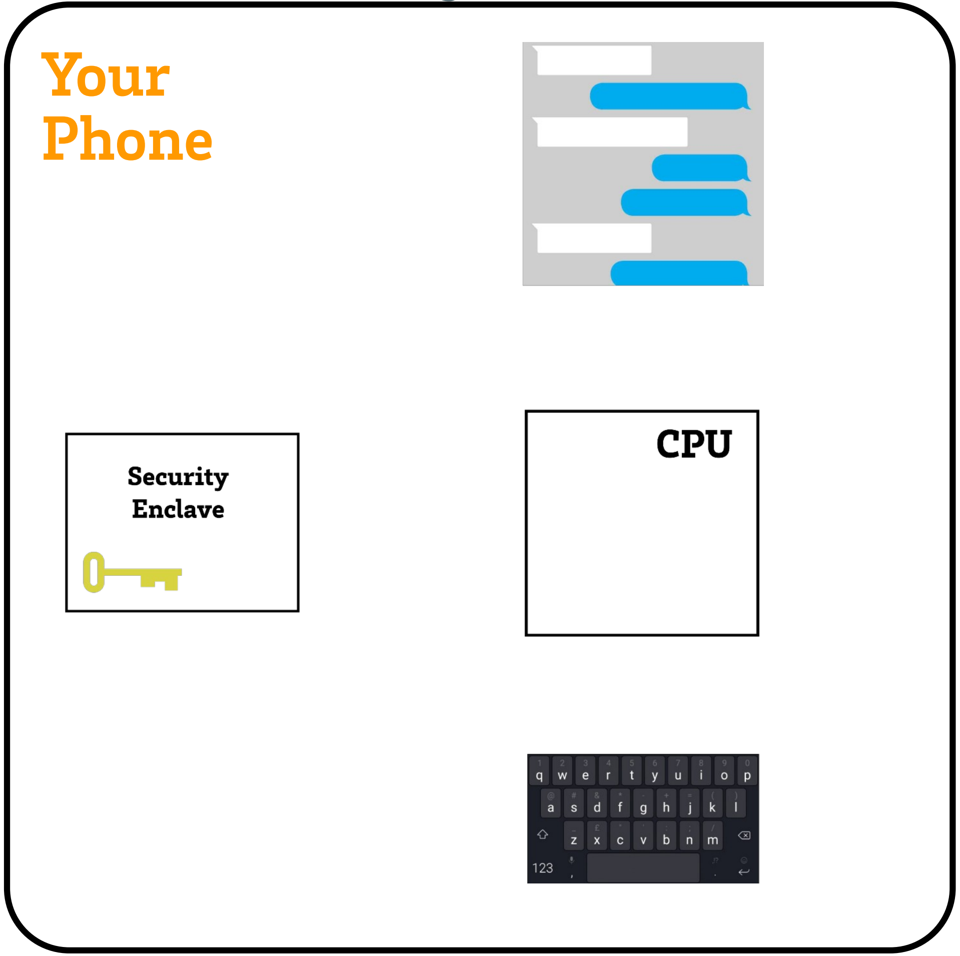
Three Principles For Evidence-Based Trust in Hardware

1) Complexity is the enemy of verification

2) Verify entire systems, not just components

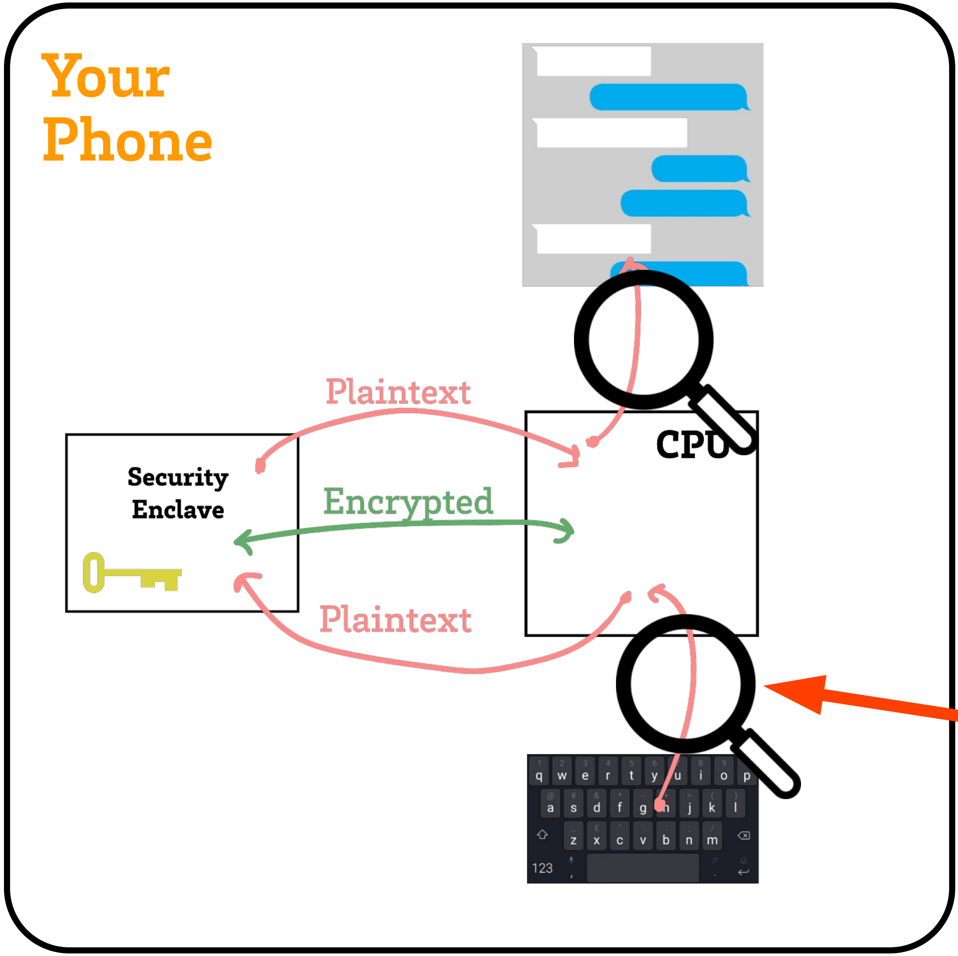
3) Empower end-users to verify and seal their hardware

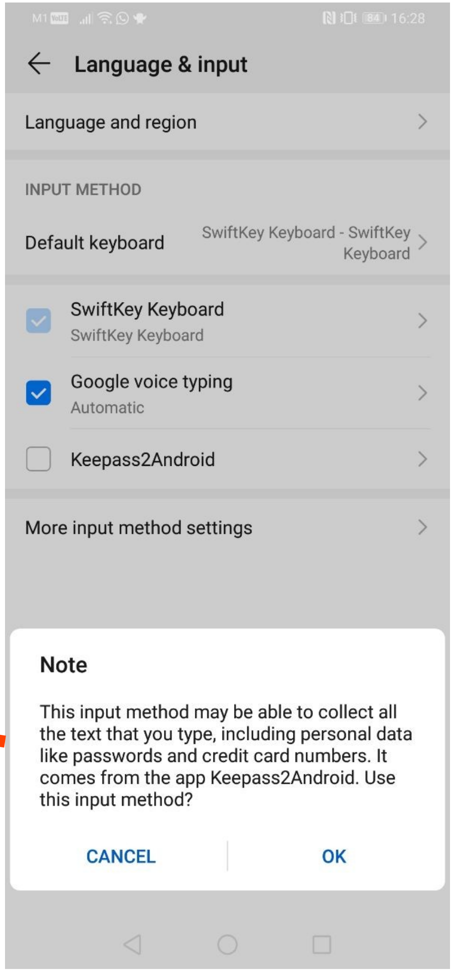
Why a Device, and Not a Chip?



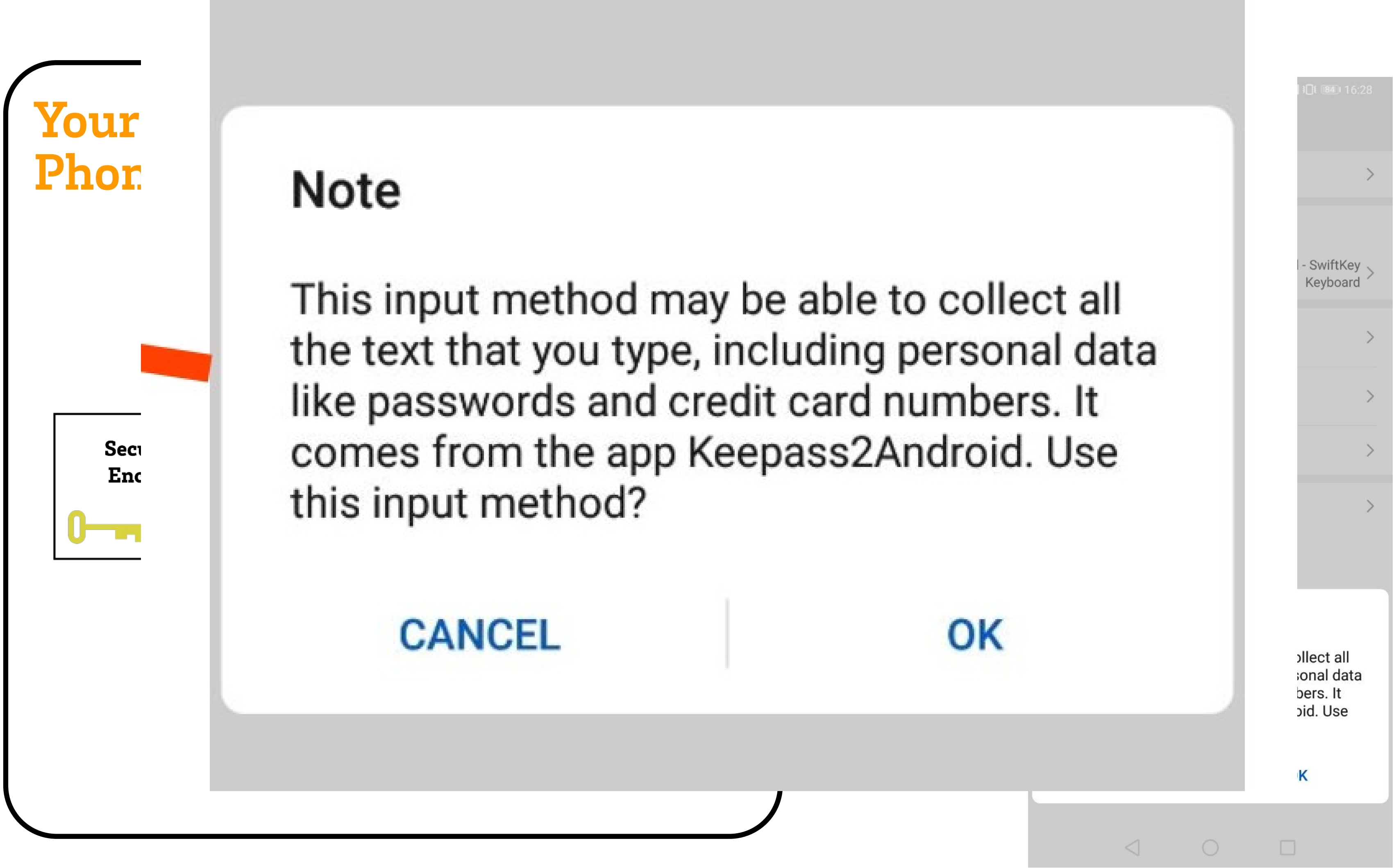
- Private keys are not your private matters
  - Screens can be scraped, keyboards can be logged

The "IME Problem"





The "IME Problem"



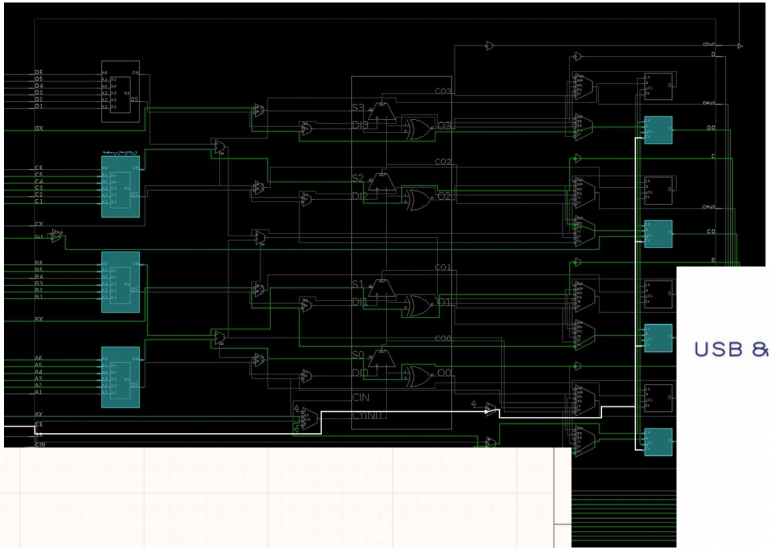
Three Principles For Evidence-Based Trust in Hardware

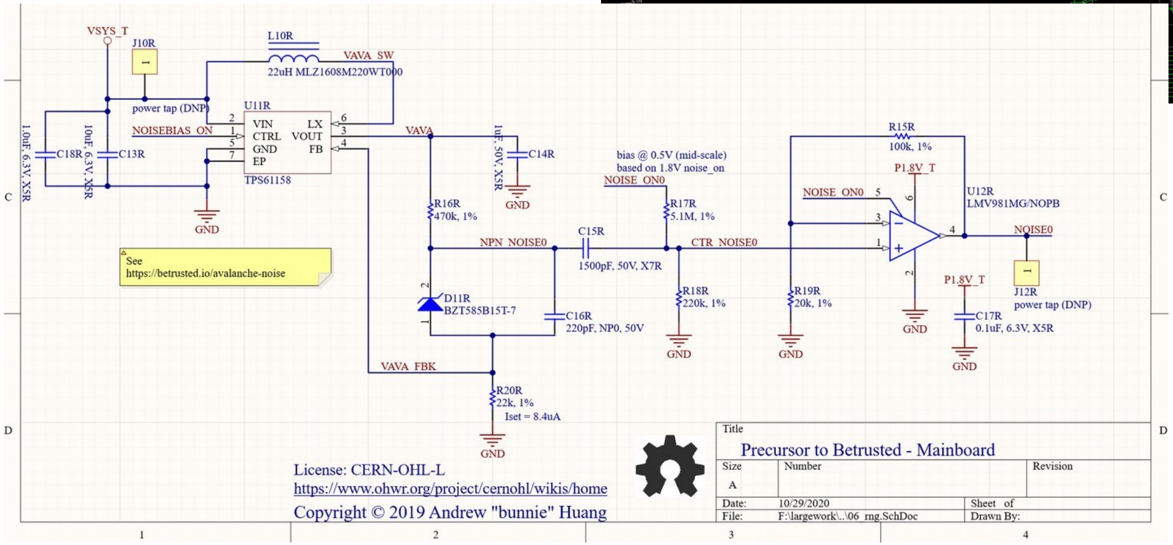
1) Complexity is the enemy of verification

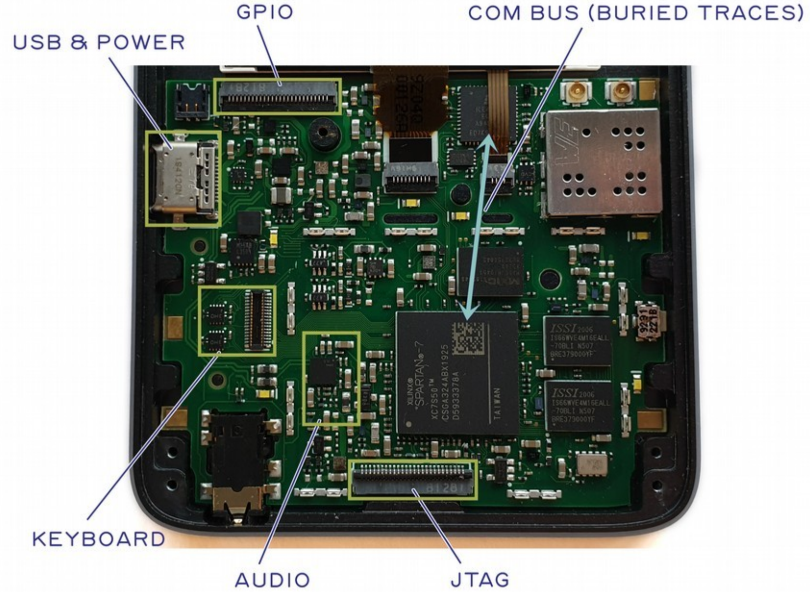
2) Verify entire systems, not just components

3) Empower end-users to verify and seal their hardware

Empower Verification At Multiple Levels







Precursor: A Case Study in Verifiable Hardware

- Designed to facilitate evidence-based trust
  - Simple in construction
  - Open in design
  - Sufficient in function

PRECURSOR

Getting HCI Right is A Major Issue in Security

- HCI = Human Computer Interface
- Humans are increasingly the "weakest leak"

- Simple, inflexible interface
- Minimal attack surface

- “Just enough and no more”
- Securable attack surface

- Featureful, flexible interface
- Intractable attack surface

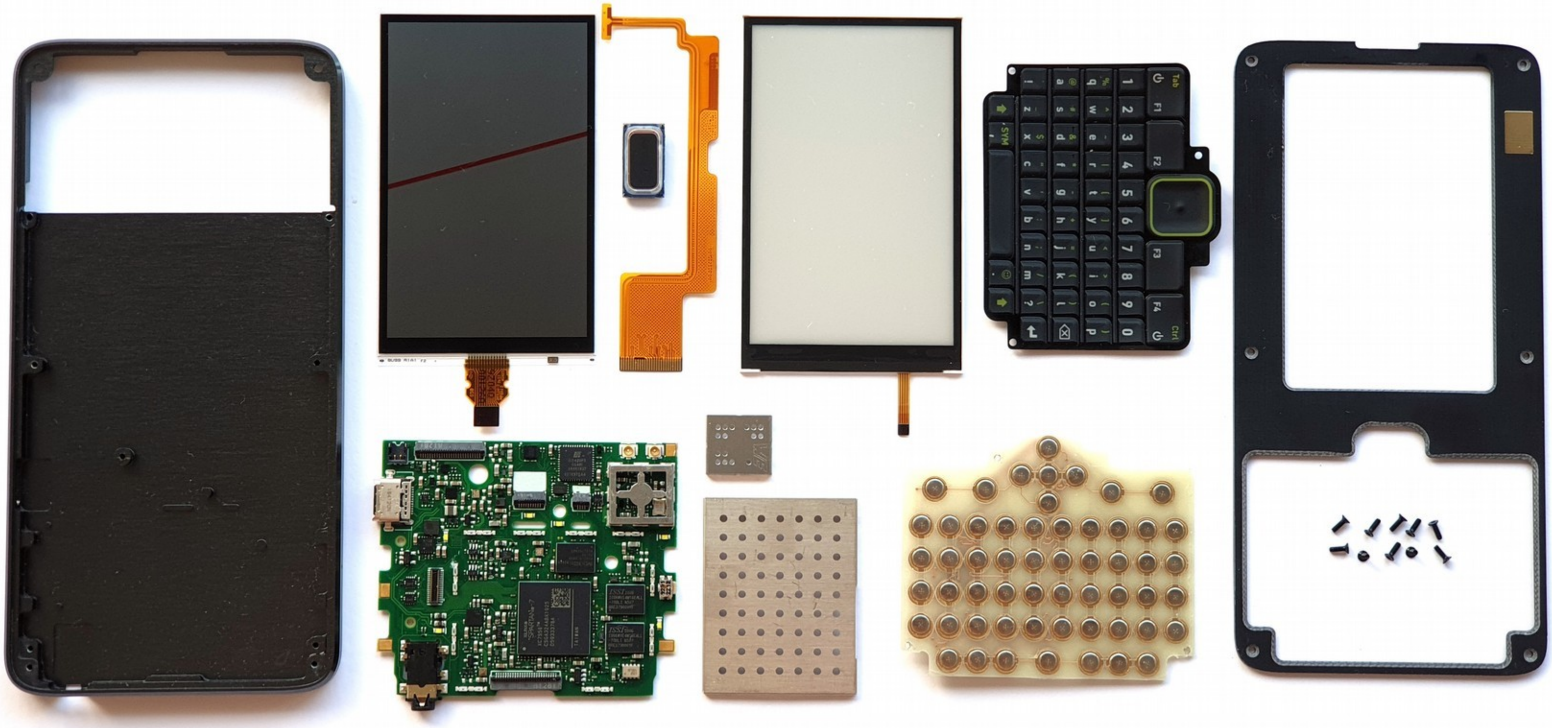
Token photo
courtesy D4m1en

Precursor: What Functions?

- Designed for mostly single-app deployments of:
  - Secure text messaging
  - Voice chat
  - Multi-lingual capability
  - Password management
  - Crypto wallet
- Not designed for
  - Web browsing
  - Games
  - Photos and videos
- Specs:
  - 100MHz RV32IMAC + MMU + AES extensions
  - Curve25519 + SHA2 accel
  - 16MiB RAM
  - 536x336 "memory" LCD
  - USB + Wifi connectivity
  - Audio only via jack
  - Full-custom OS "Xous"
    - QNX-like microkernel, written in Rust

PRECURSOR

Precursor: Simple in Construction

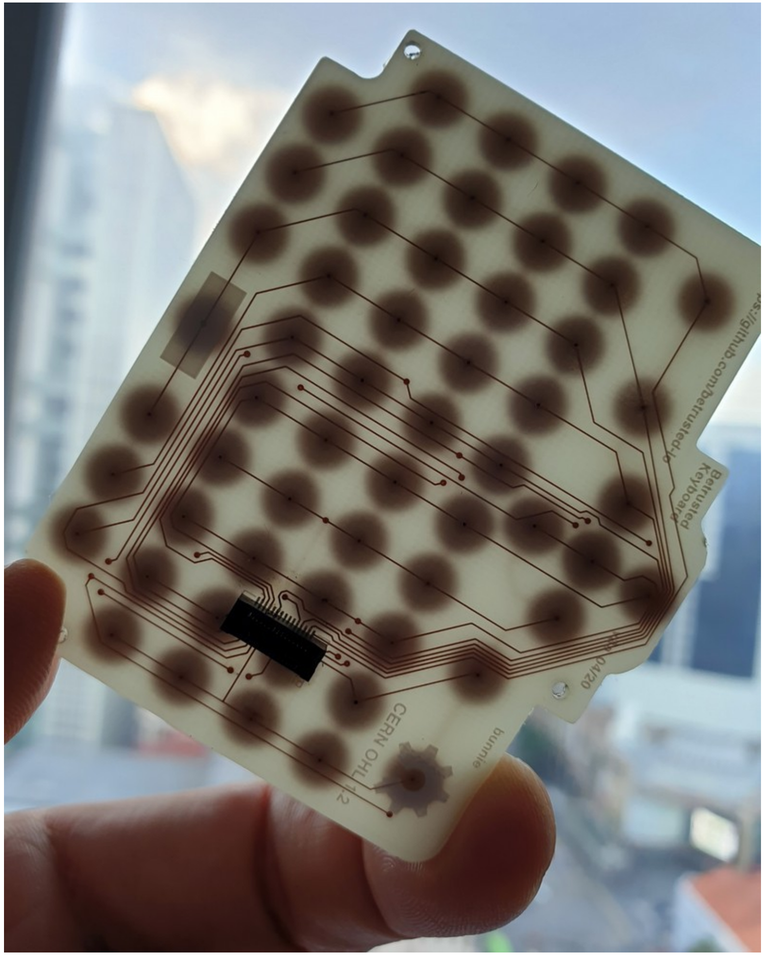


Simple to Inspect

Physical Keyboard

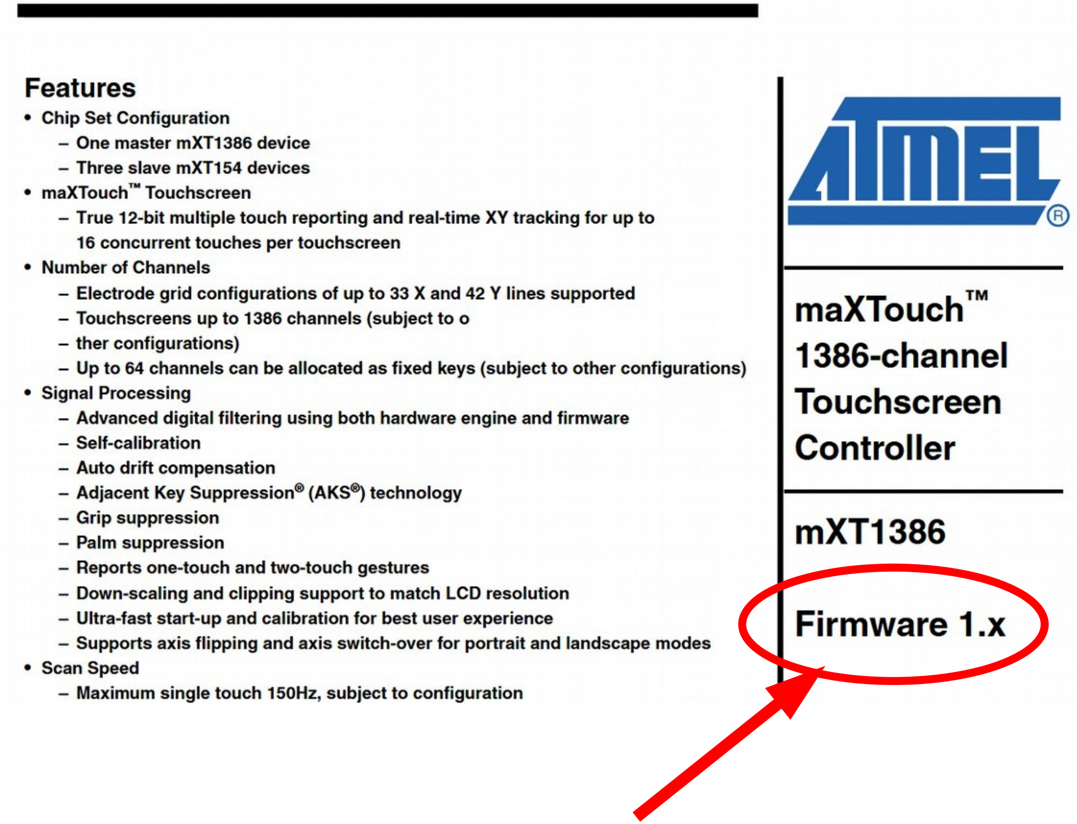
- Wires visually inspectable
- 2-layer daughtercard:
  - Bright light may be employed to rule out buried traces
- No silicon chips
- User replaceable keyboard overlay for multi-lingual support

Verification Difficulty: Trivial



Touch Keyboard Verification: Very Hard

- Captouch screens require the use of a proprietary microcontroller with a firmware blob



Features

- Chip Set Configuration
  - One master mXT1386 device
  - Three slave mXT154 devices
- maXTouch™ Touchscreen
  - True 12-bit multiple touch reporting and real-time XY tracking for up to 16 concurrent touches per touchscreen
- Number of Channels
  - Electrode grid configurations of up to 33 X and 42 Y lines supported
  - Touchscreens up to 1386 channels (subject to o
  - ther configurations)
  - Up to 64 channels can be allocated as fixed keys (subject to other configurations)
- Signal Processing
  - Advanced digital filtering using both hardware engine and firmware
  - Self-calibration
  - Auto drift compensation
  - Adjacent Key Suppression® (AKS®) technology
  - Grip suppression
  - Palm suppression
  - Reports one-touch and two-touch gestures
  - Down-scaling and clipping support to match LCD resolution
  - Ultra-fast start-up and calibration for best user experience
  - Supports axis flipping and axis switch-over for portrait and landscape modes
- Scan Speed
  - Maximum single touch 150Hz, subject to configuration

ATMEL®

maXTouch™ 1386-channel Touchscreen Controller

mXT1386

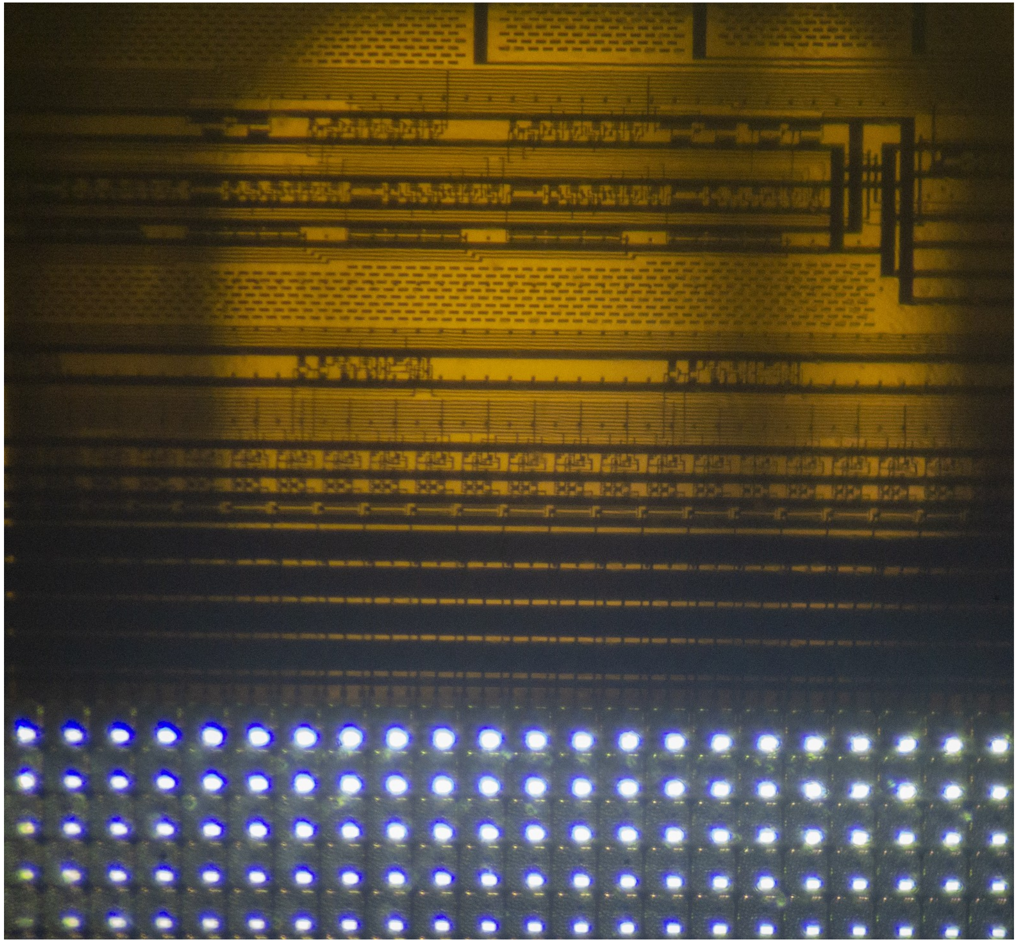
Firmware 1.x

Verifiable LCD

- High-DPI black and white screen
  - 200 dpi
  - 336x536 pixels

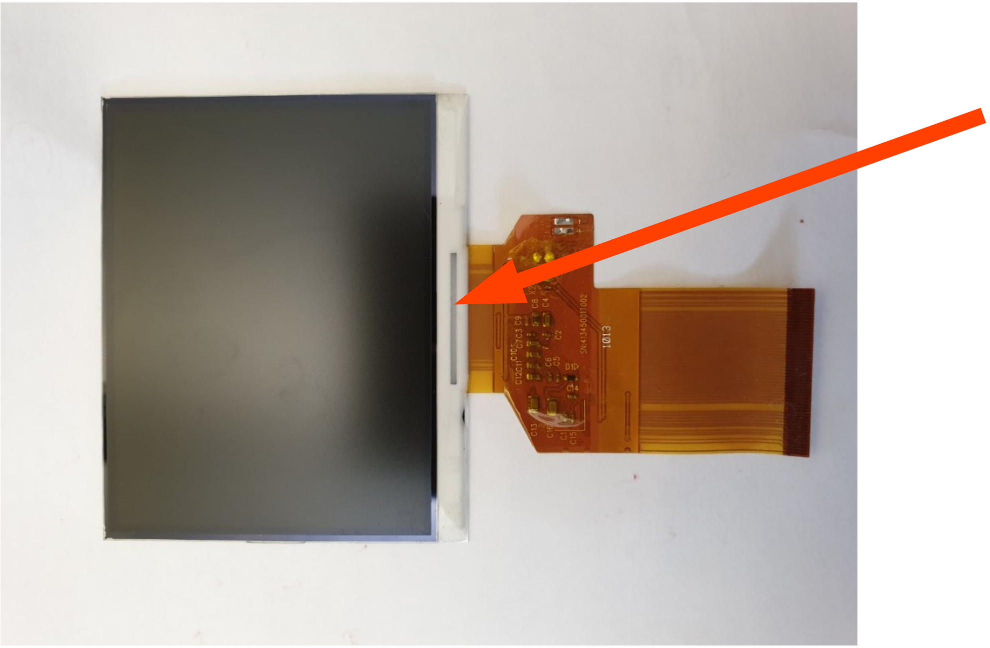
Verifiable Screen

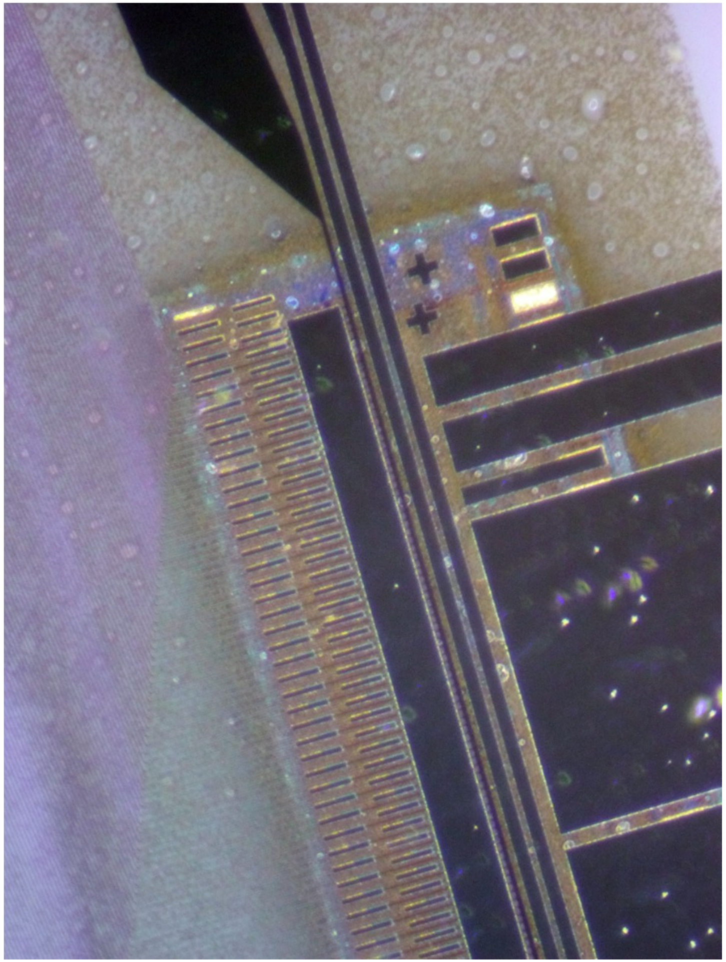
- All drive electronics on-glass
  - Inspectable with a cheap optical microscope (50x zoom shown)
  - All circuits verifiable through non-destructive inspection
  - No chips to verify
    - Less places to hide things -> less need to check things

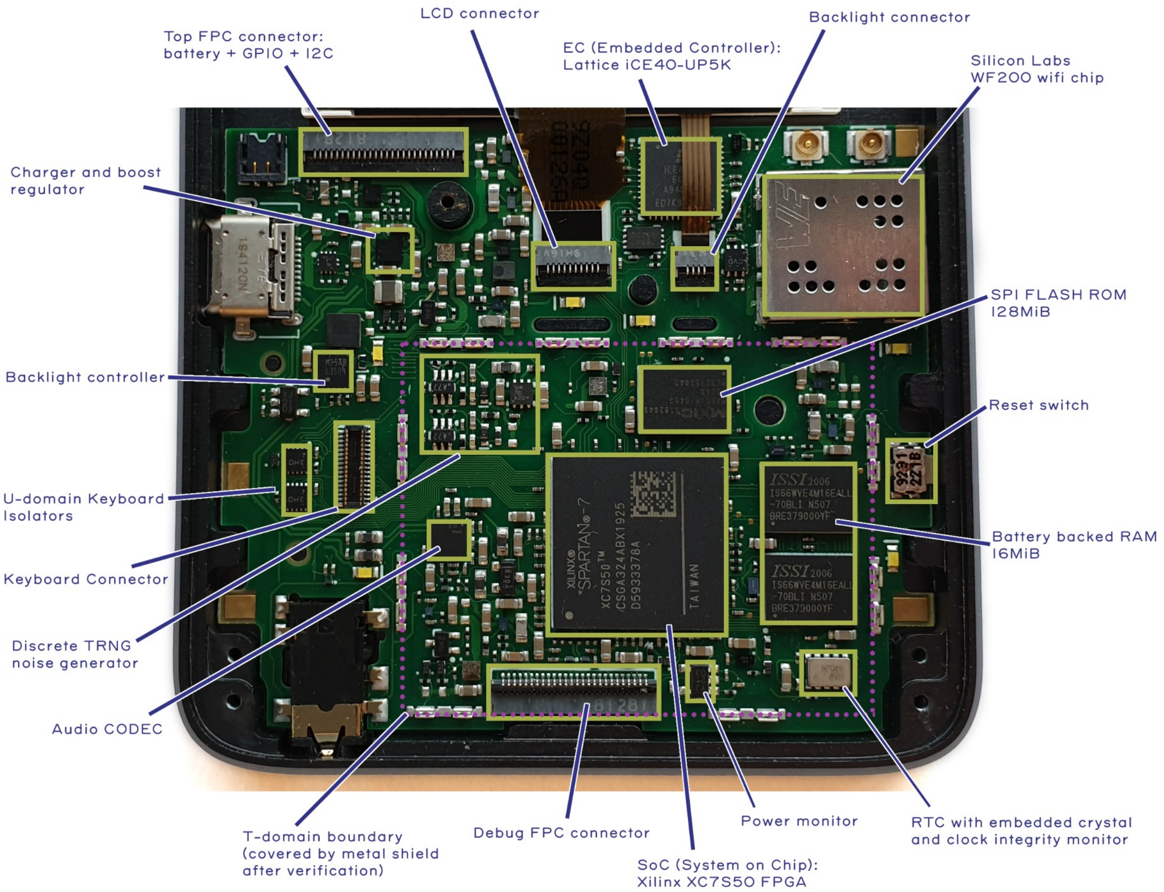


Why Not a Color LCD?

- Virtually all LCDs incorporate a driver IC
  - Contains a framebuffer and a command interface

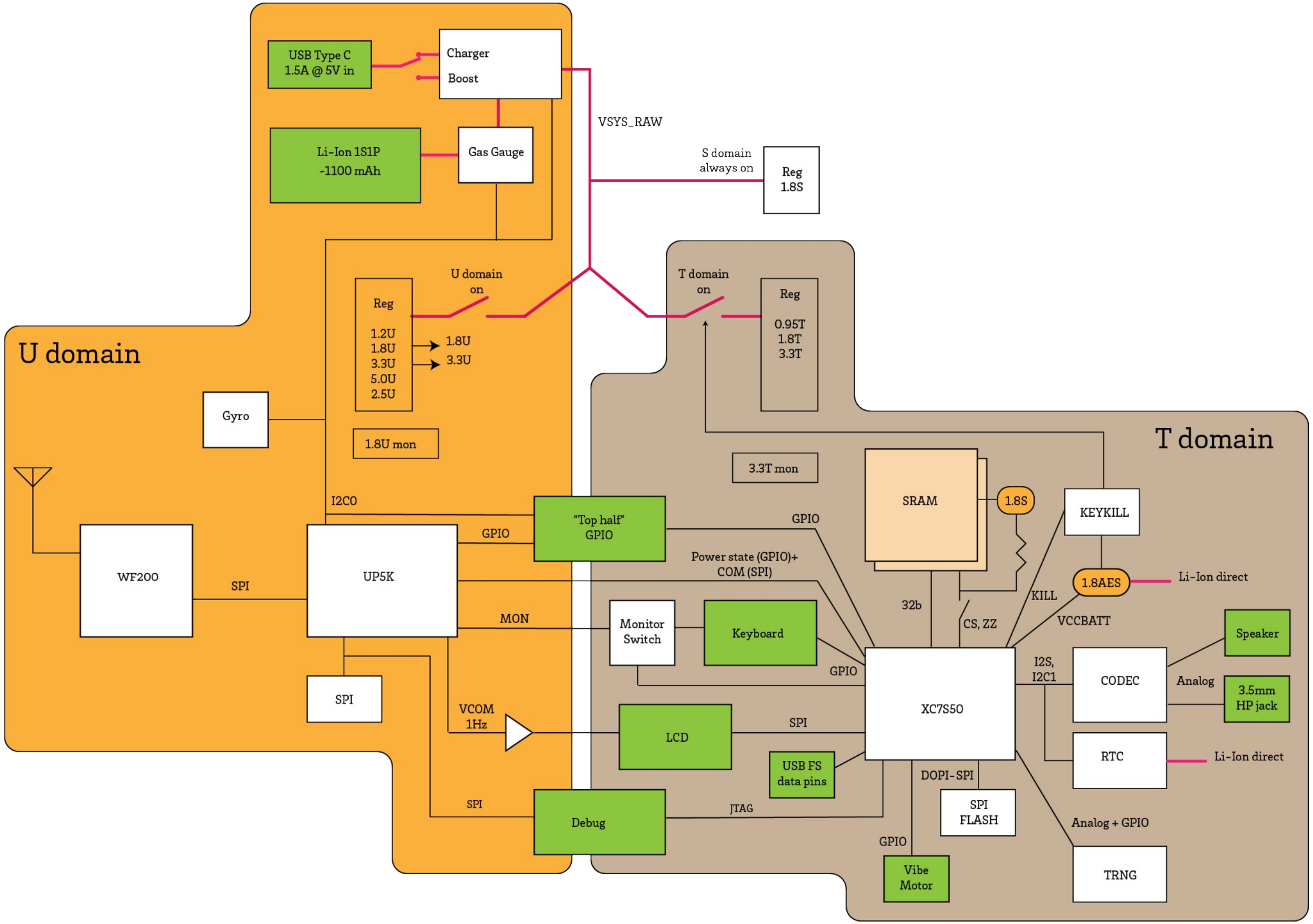




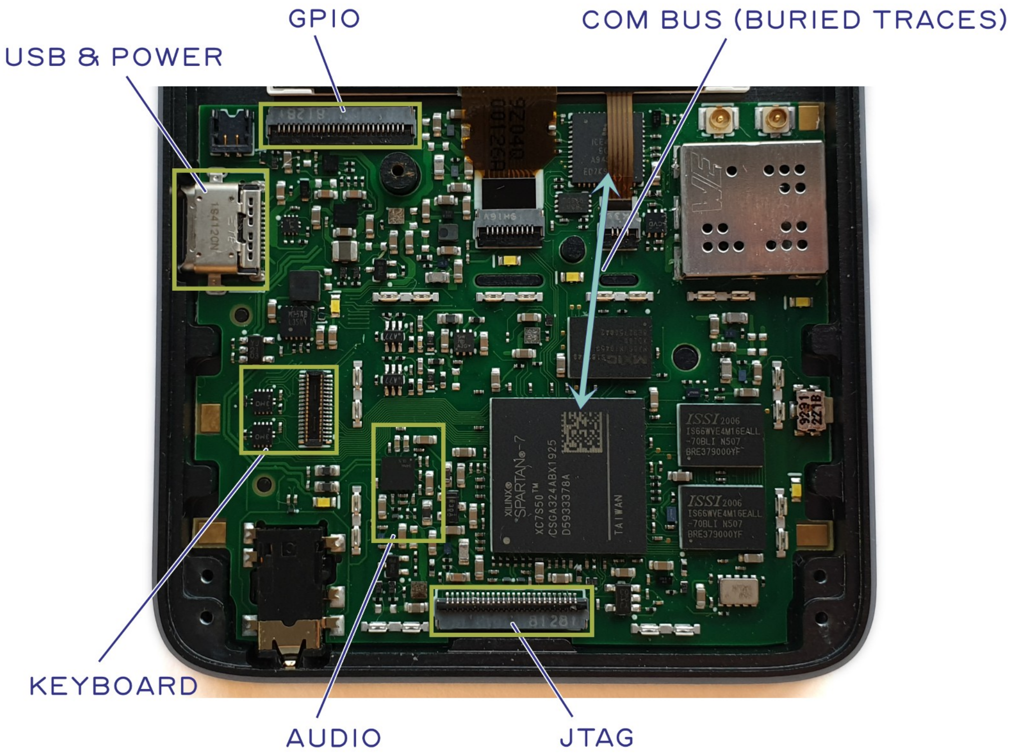


PRECURSOR → PRE-PRODUCTION MAINBOARD DIAGRAM SEP 2020

The PCB:
Designed Along Attack Surfaces

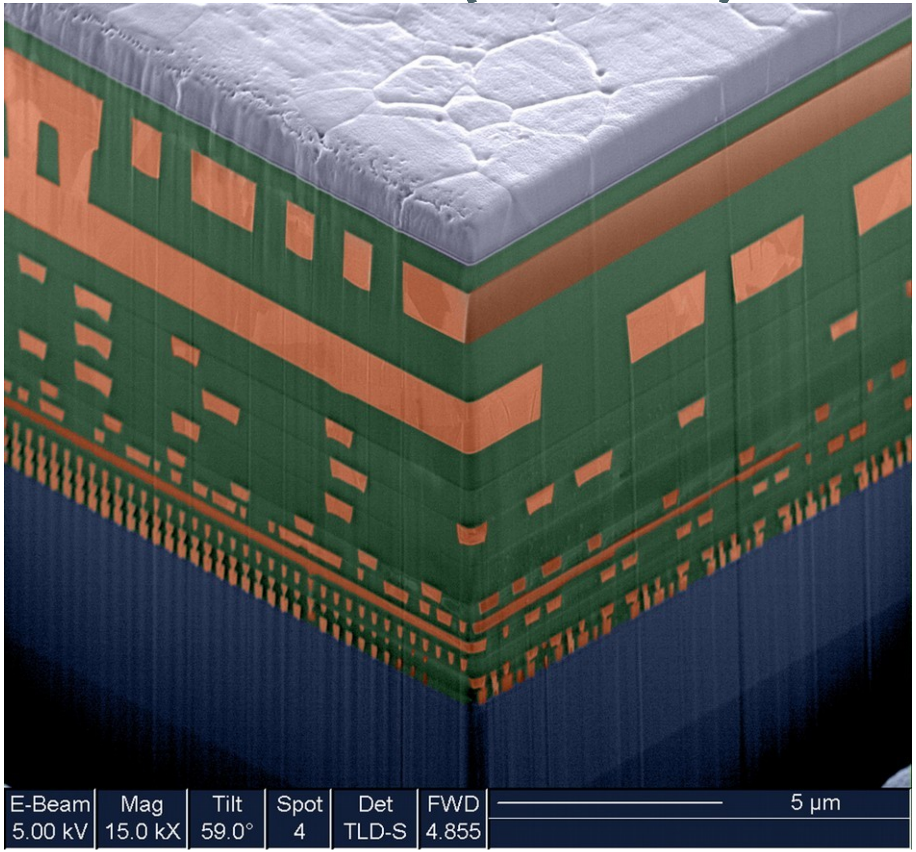


T-Domain Attack Surfaces Illustrated



The Hardest Problem: Evidence-Based Trust and the CPU (or SoC)

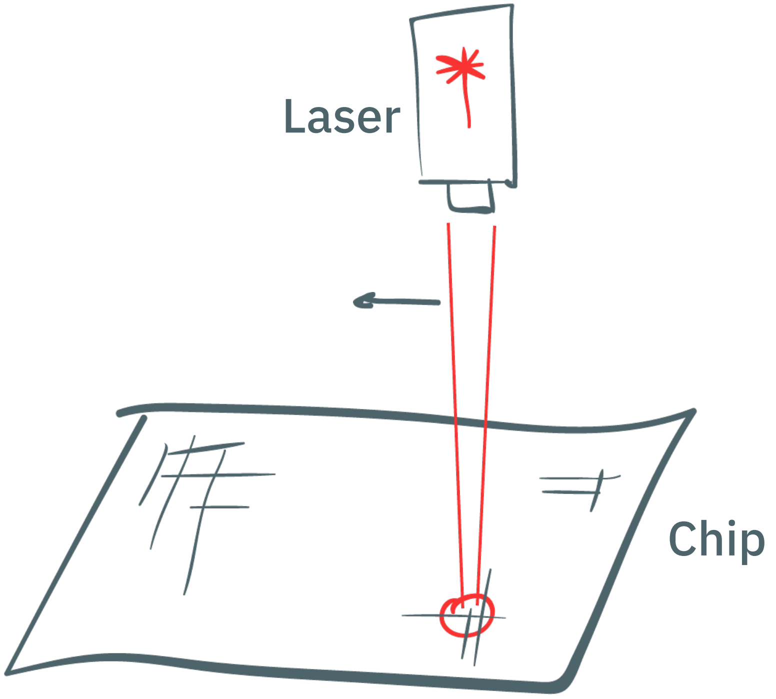
- Silicon inspection is typically destructive and hard
- Difficult to check and use a specific chip



https://www-03.ibm.com/press/us/en/photo/19014.wss

Non-Destructive Silicon Verification???

- Proposal: use optical fault induction
  - Pros:
    - Non-destructive
    - Optical methods are relatively cheap
  - Cons:
    - Lower bound on trojan circuit complexity
      - RTL-level design methods can make small trojans difficult
    - Probably requires chip thinning for effective back-side illumination
      - Top metal scatters light too much
- Years to develop

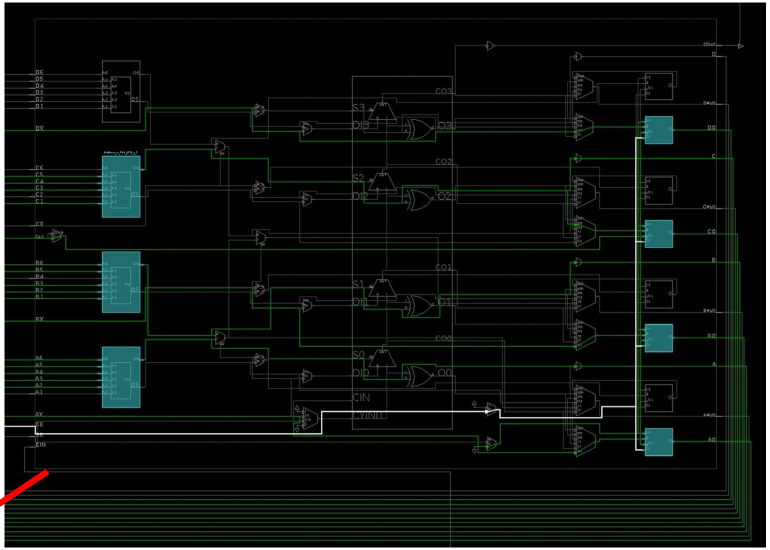


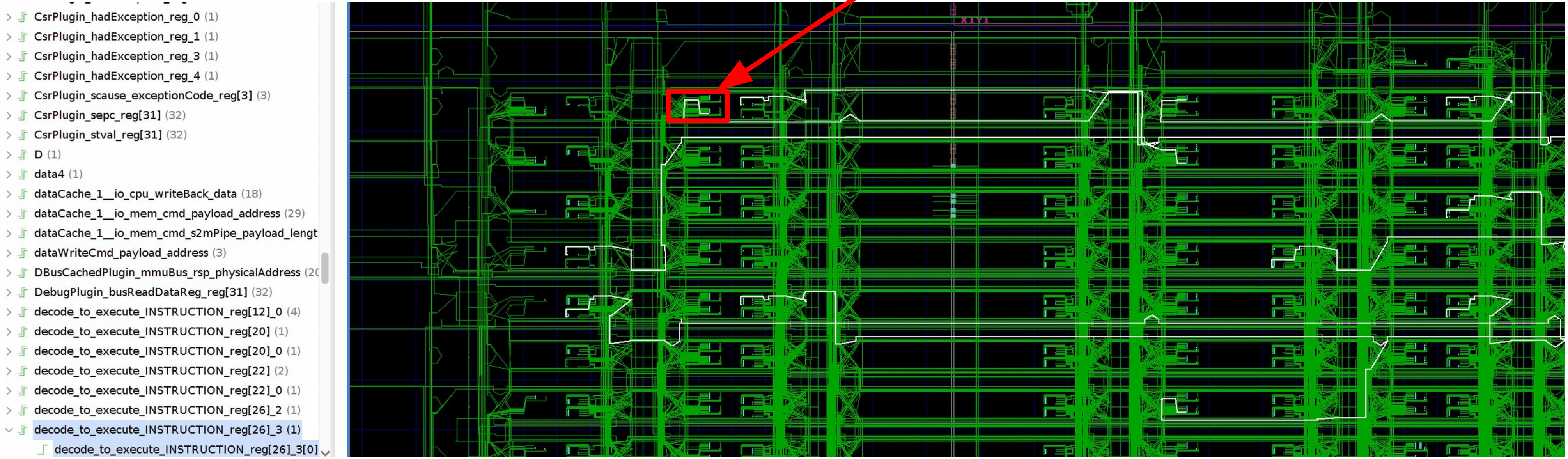
Laser spot size >> single transistor

Use sub-λ scan overlap + BIST syndrome readout to correlate with expected silicon pattern

A Solution: The FPGA

- FPGAs are "Field Programmable Gate Arrays"
  - Consist of large arrays of logic + wires that are user-configured to implement hardware designs

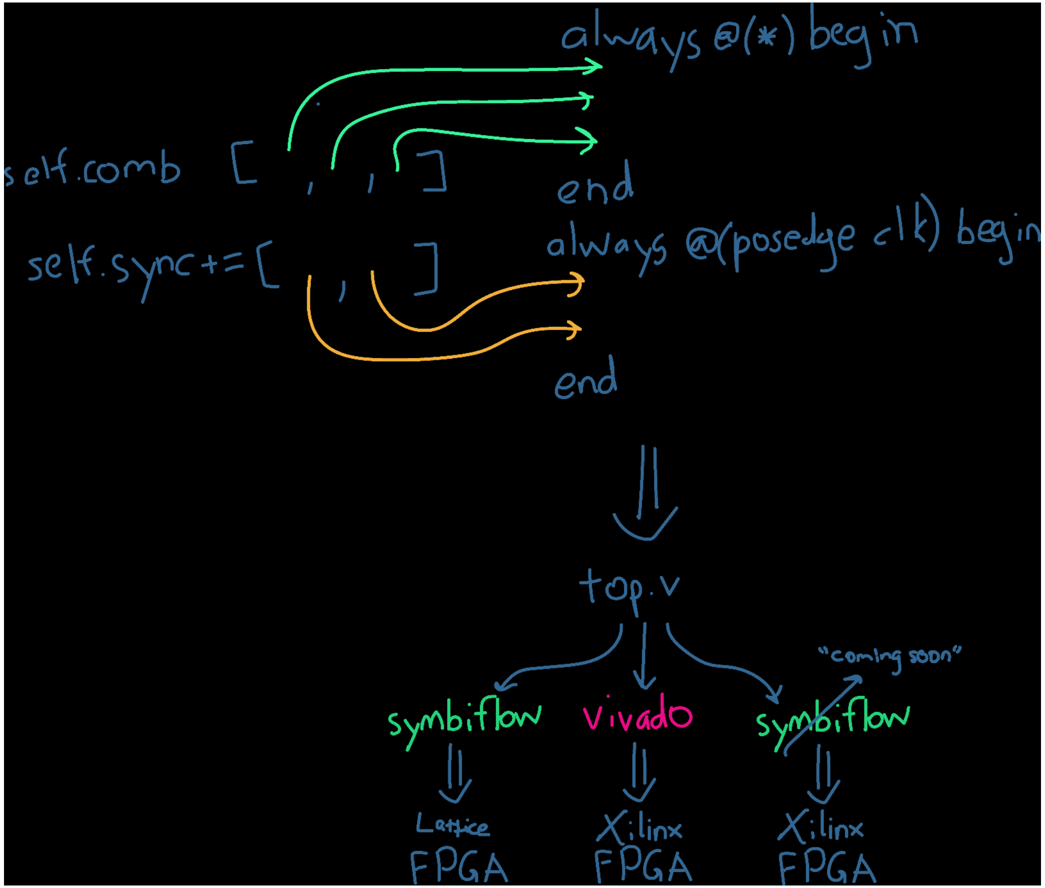




FPGA: Narrowing the TOCTOU Gap by Compiling Your Own SoC

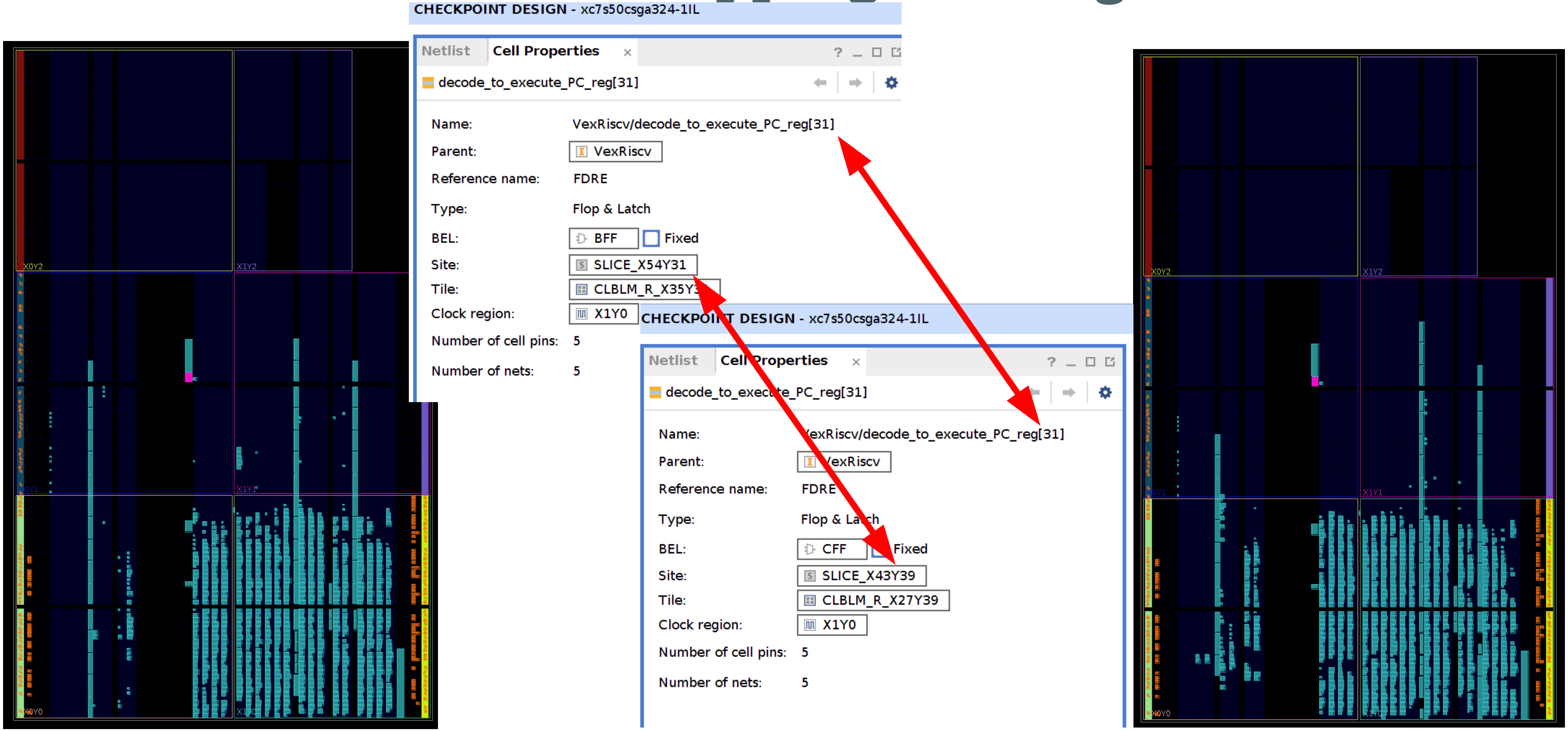
- Anyone can compile their design from source
- Enables trust transfer via signatures "like software"!

- Subtlety: toolchain openness
  - Symbiflow is the F/OSS flow
    - Lattice ICE40 and ECP5 is 100% open flow
    - 7-Series FPGA is "coming soon" but currently requires closed vendor tools

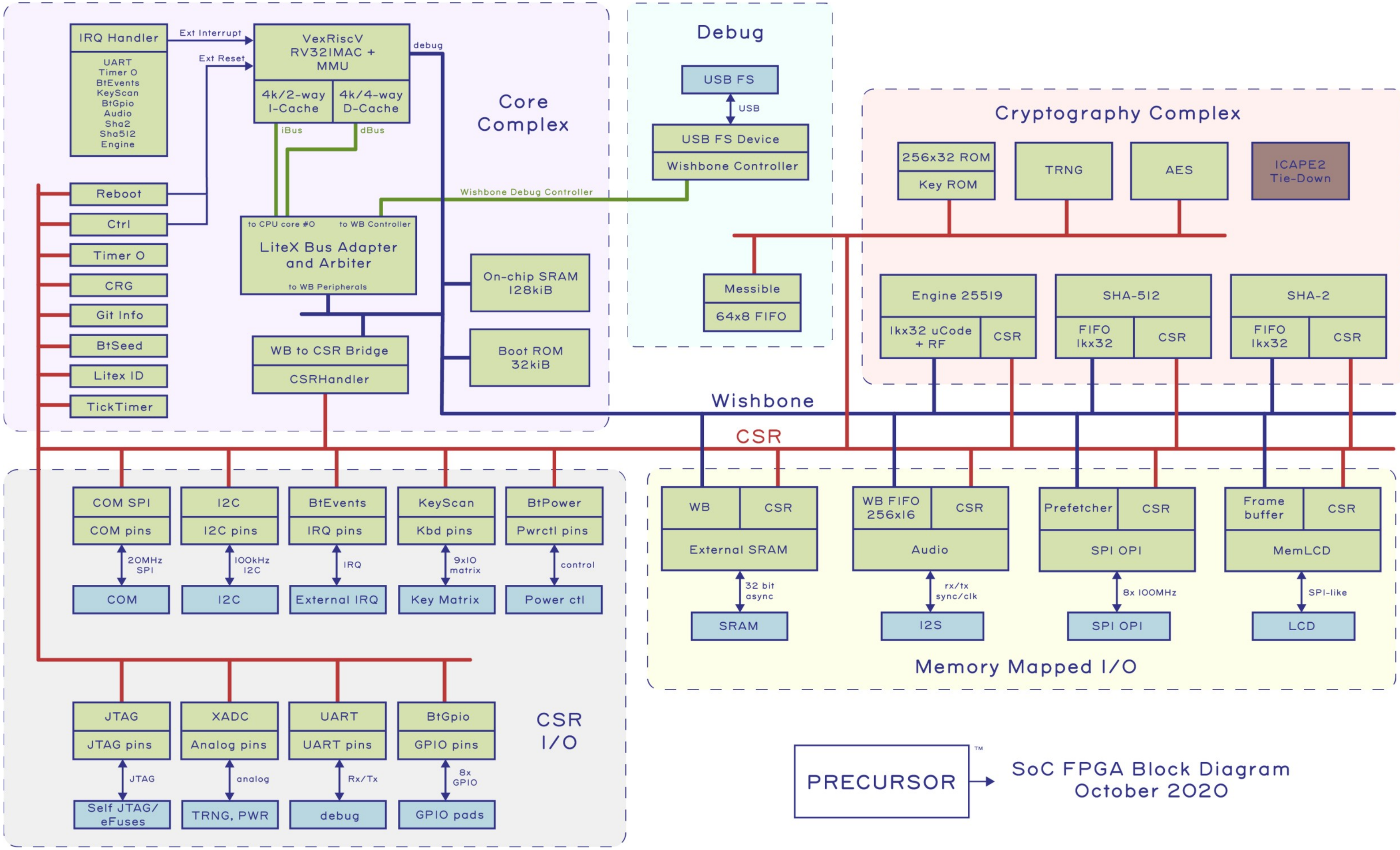


ASLR = Address Space Layout Randomization

FPGA Features "ASLR for Hardware": Pseudo-Random Mapping of Design to Device

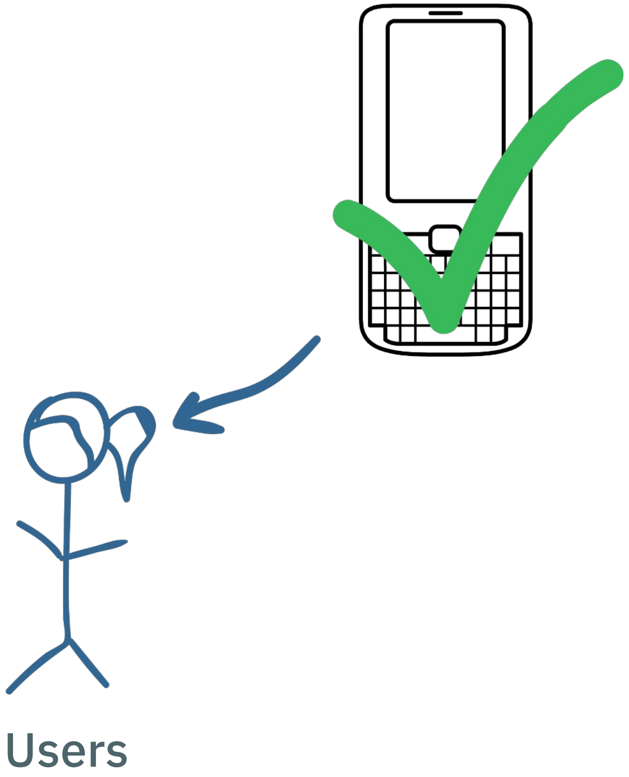


A Look Inside the SoC



FPGA's Biggest Potential Advantage: Moves Point-of-Check Towards the End User

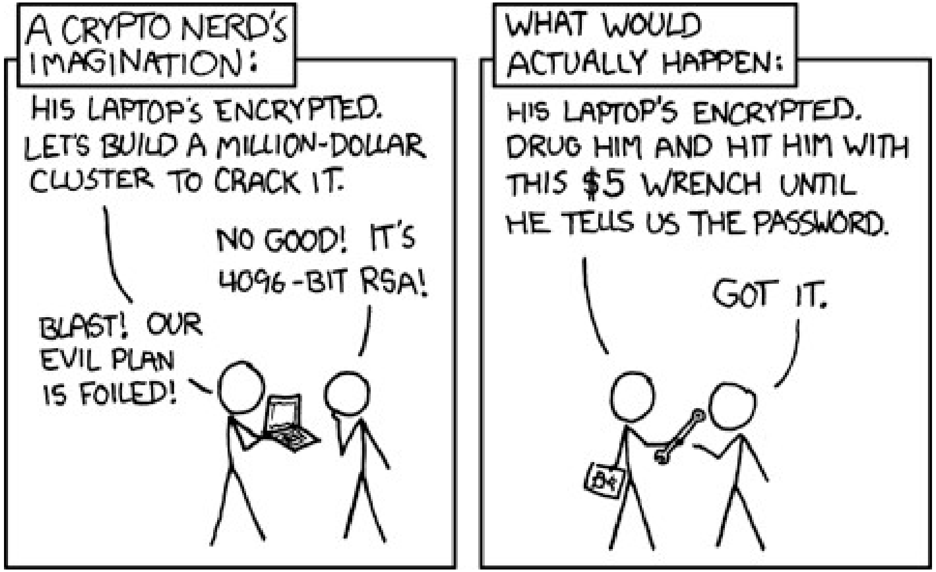
- One can imagine a bitstream checker
  - Correlate design-to-bitstream
- Vision: a "one-click" tool to verify the FPGA bitstream!
  - Point of check = Point of use



"From Boot to Root in One Hour"
https://www.bunniestudios.com/blog/?p=6336

What About Direct Attacks Against Users?

- Strong security makes humans the weakest link
  - Lawful (and unlawful) coercion of secrets through search, seizure, subpoena
- Philosophical debate:
  - Should security prioritize the user's safety, or the secret's safety?



In Practice,
Security Is a Function of Social Context

- Doors remain locked not because locks are effective, but because of social context
- Alternatively: police rarely have to pick locks

<<

Lesson Learned Since 2016: Under Investigation?
Plausible Deniability is Powerful!

ISSIE LAPOWSKY   SECURITY   NOV 17, 2017 12:03 PM

Everything Attorney General Jeff Sessions Has Forgotten Under Oath

Over the course of four recent congressional hearings, Attorney General Jeff Sessions has someho forgotten dozens of people, places, and events. Here's all of them in one place.

ALEX WONG/GETTY IMAGES

Week 66: Scott Pruitt's Selective Memory

Pruitt can't recall his misdeeds, science is out at the EPA, and Rick Perry wants to declare a national emergency to keep coal plants open.

April 27, 2018 | Brian Palmer

Welcome to our weekly Trump v. Earth column, in which onEarth reviews the environment-related shenanigans of President Trump and his allies.

Tom Williams/Getty

Mike Pompeo's totally nonsensical answer about his meeting with Donald Trump

By Chris Cillizza, CNN Editor-at-large
Updated 2203 GMT (0603 HKT) April 12, 2018

oke with Mueller 01:53

Trump claims ignorance of 'burner phones'. Here's how they work

Disposable phones may appeal to anyone trying to hide their identity - whether a criminal or an activist

Investigators are asking whether burner phones may have been used at the White House on 6 January 2021. Composite: Getty Images

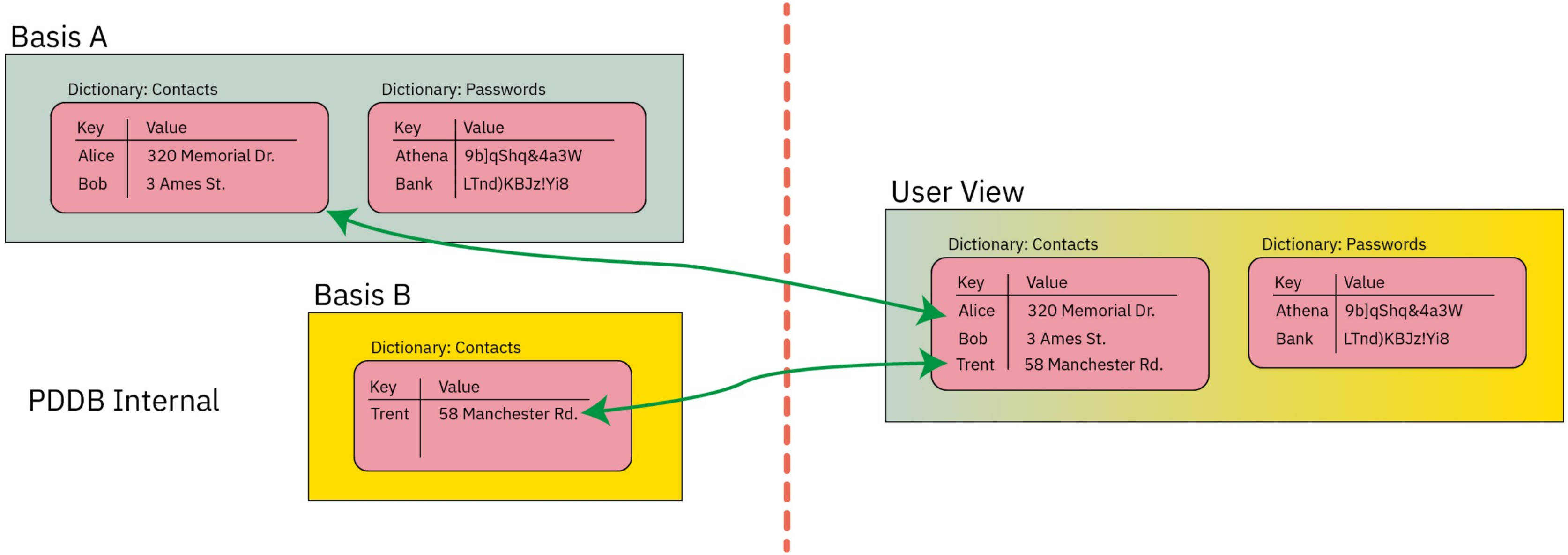
Effective Plausible Deniablity

- Requirement: An omniscient adversary cannot prove or disprove that a secret exists
  - With a full forensic image of a device:
    - Encrypted data is indifferentiable from empty space (free space wipe)
    - No metadata leakage (veracrypt, truecrypt in certain modes)
      - No mysterious partitions
      - No "missing" free space on device
    - No application leaks of pointers to encrypted data (PDDB, [1])
      - No password-specific salts, usernames
      - No dangling file references
      - No record in browser history, application history

[1] https://www.schneier.com/wp-content/uploads/2016/02/paper-truecrypt-dfs.pdf

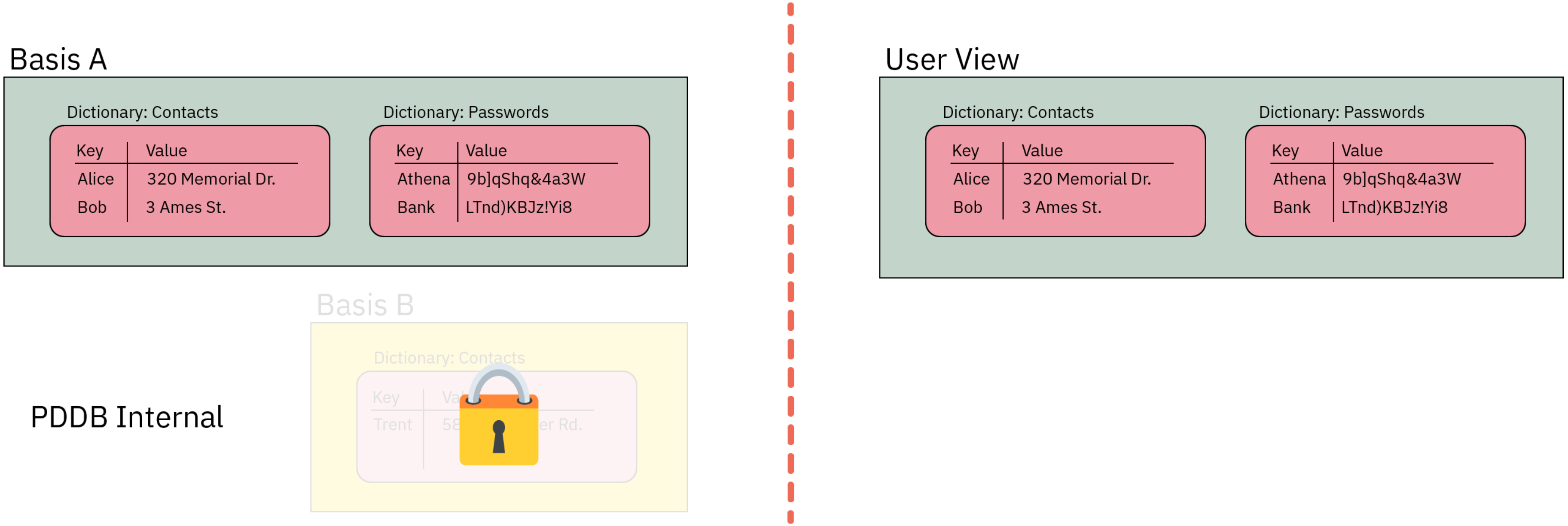
The Plausibly Deniable DataBase (PDDB)

- A **(key, value)** store
- **(k,v)** pairs stored in a **Dictionary**
- **Dictionaries** stored in a **Basis**
- **User View** of the database is the union of one or more **Bases**

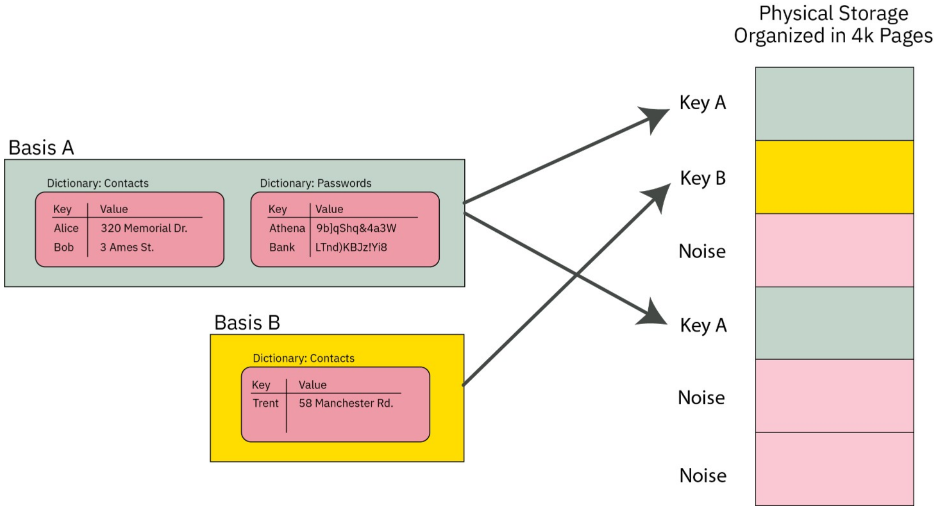


Mitigating API Deniability Leakage

- Locked (unmounted) Bases are automatically hidden in the User View
- Minimal application guidelines for successful plausible deniability
  - Basically: don't cache state



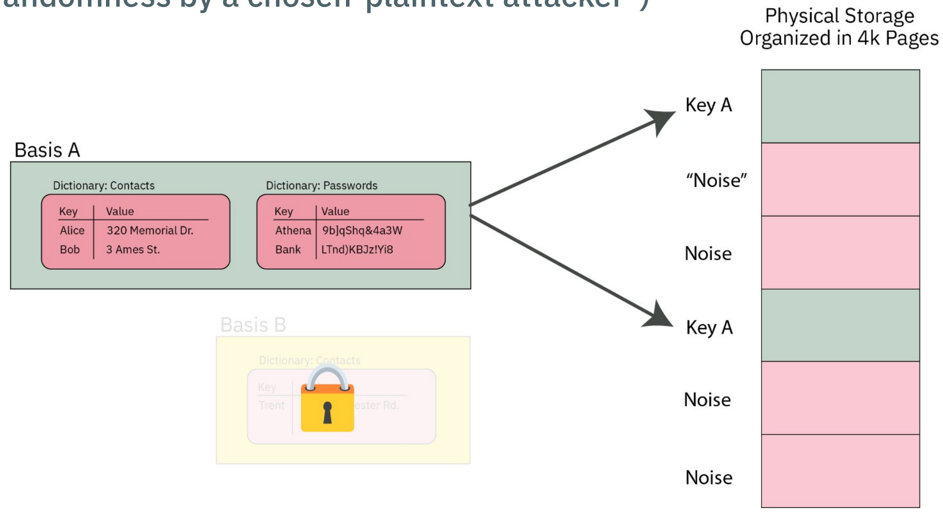
Mitigating Forensic Disclosure



Both Basis A and Basis B Unlocked

Cipher Requirement: IND$-CPA [1]

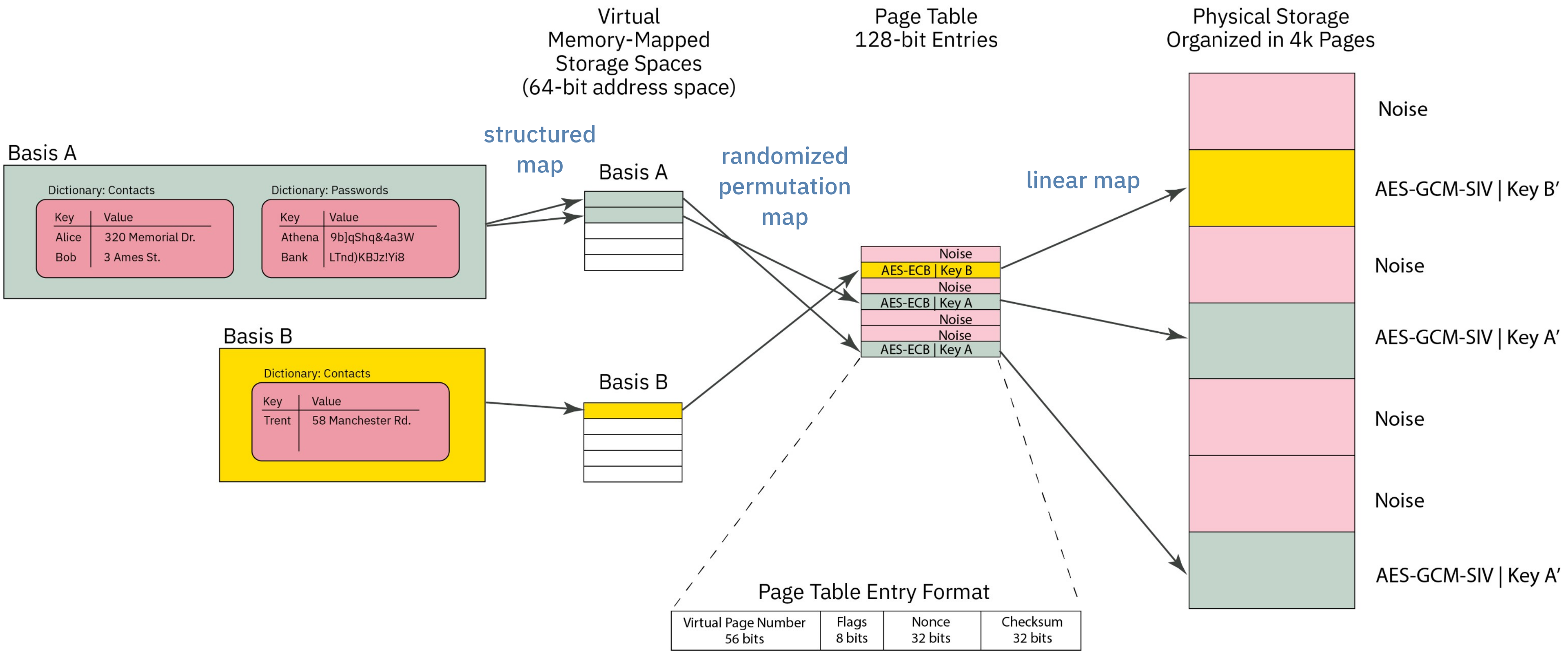
("indistinguishable from uniform
randomness by a chosen-plaintext attacker")



Only Basis A Unlocked

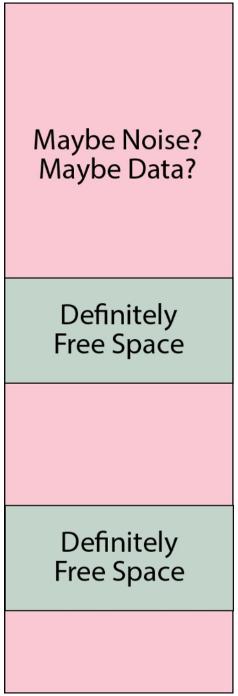
[1] https://web.cs.ucdavis.edu/~rogaway/papers/ad.pdf

Details: Making It Run Fast



Details: Free Space

- Locked Bases Are Indistinguishable from Free Space
  - Problem:
    - How to allocate a block without erasing locked data?
  - Solution:
    - Map all known Bases
    - Select a random subset of freespace equal to ~10% of disk -> cache it as "definitely free space"
    - Re-lock secret Bases
    - Allocate from "definitely free space" until exhausted
    - OOM -> go back to first step



PDDB General Properties

- Erasing a Basis is equivalent to forgetting the key
  - "I do not recall" === "The data never existed (or is erased)"
- Strong deniability versus a single forensic imaging event
  - Pros: Attacker cannot prove or deny that all Basis passwords have been disclosed
  - Cons: Attacker can force the deletion of undisclosed secret Bases by filling a known Basis with junk data
    - In some cases this is a desirable outcome
- Diminishing deniability versus repeated forensic imaging events
  - Small secret datasets are easier to deny
  - Disk can be re-encrypted/shuffled to restore deniability

PDDB Is Not a Panacea

- Deniability is fundamentally a **social tool**
  - Not all people can execute deniability to the same proficiency
  - Deniability is optional; it is *not appropriate for all situations*
  - However, no users can successfully deny anything without the option of strong plausible deniability
- PDDB is just one tool of many that are needed to help navigate upcoming legal challenges to privacy and security

Q&A

@bunniestudios

"From Boot to Root in One Hour"

https://www.bunniestudios.com/blog/?p=6336

https://precursor.dev

#betrusted:matrix.org

With thanks to:

nlnet FOUNDATION

NGI ZERO