CSE/CEN 598
Hardware Security & Trust

Trusted Digital System Design: Anti-Tamper

Prof. Michel A. Kinsy

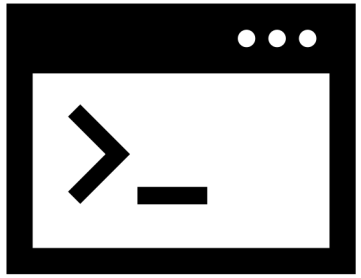
Anti-Tamper Introduction

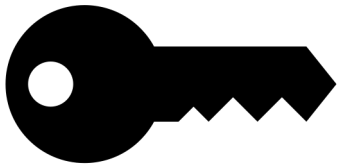
- Anti-tamper– Prevent or detect physical access/modification of a system
- Detection
  - How is access observed/discovered
- Response
  - How does the system react to un-authorized access?

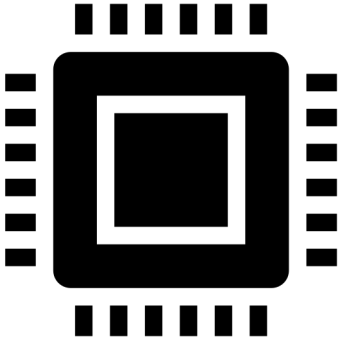
Tamper-Evident Seals

What Does Anti-Tamper Protect?

- NIST Definition
  - Impede countermeasure development
  - Prevent unintended technology transfer
  - Prevent alteration of a system
- Firmware/Software
  - Reverse engineering could reveal further exploits
- Secret Keys
  - Leaked keys broaden an attacker's access
- Hardware IP
  - Steal designs, develop new attacks







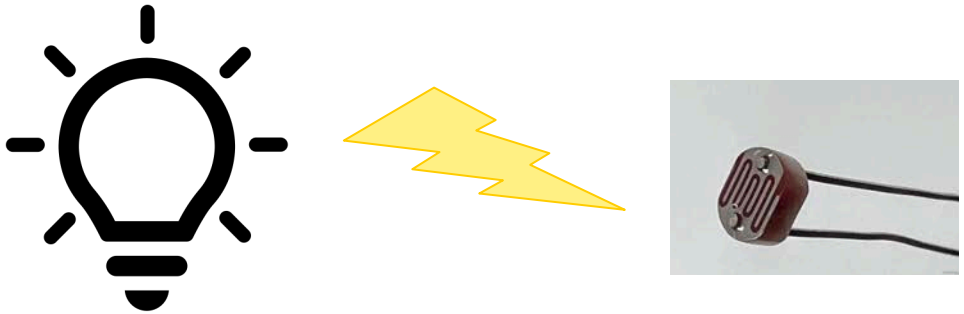
Levels of Anti-Tamper

- Chip/packaging level
  - Prevent IC circuit level attacks
  - Tamper detections circuits included on-chip
- PCB/Enclosure
  - Chassis intrusion alarm
  - Detect physical access to enclosure interior

Passive vs Active Anti-Tamper

Passive Anti-Tamper

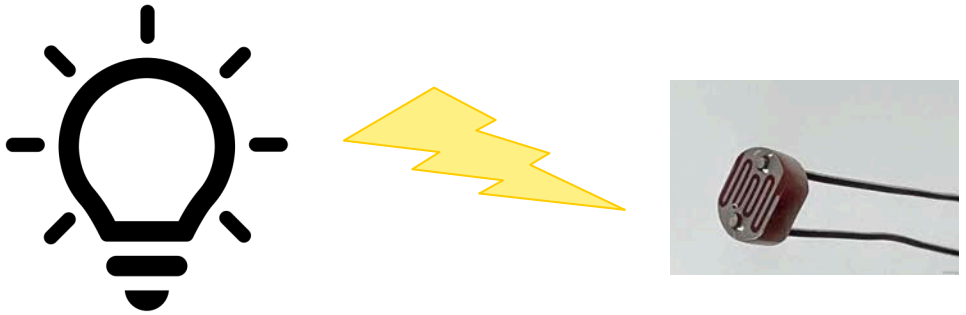
- Measure environment state
  - Not influencing/changing state
- Power source sometimes required
  - Usually for tamper response



Passive vs Active Anti-Tamper

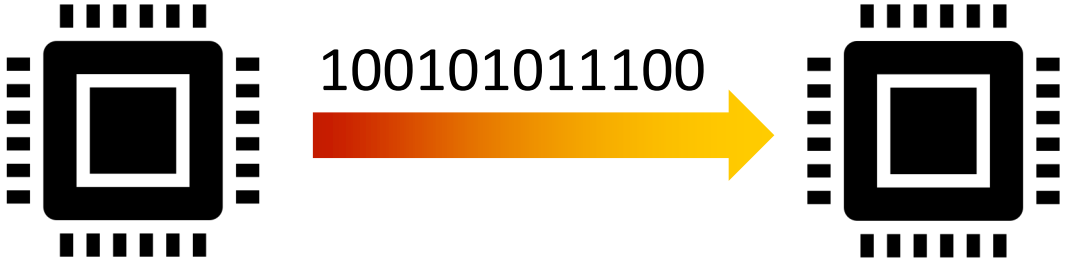
Passive Anti-Tamper

- Measure environment state
  - Not influencing/changing state
- Power source sometimes required
  - Usually for tamper response



Active Anti-Tamper

- Communication between two components
  - Ensure connectivity between two devices
- Power source always required



Tamper Detection Mechanisms

- Light
  - Detect enclosure opening
  - Requires opaque enclosure

Tamper Detection Mechanisms

- Light
  - Detect enclosure opening
  - Requires opaque enclosure
- Contact
  - Electrical connection between enclosure halves
  - Often used in conjunction with light sensor

Tamper Detection Mechanisms

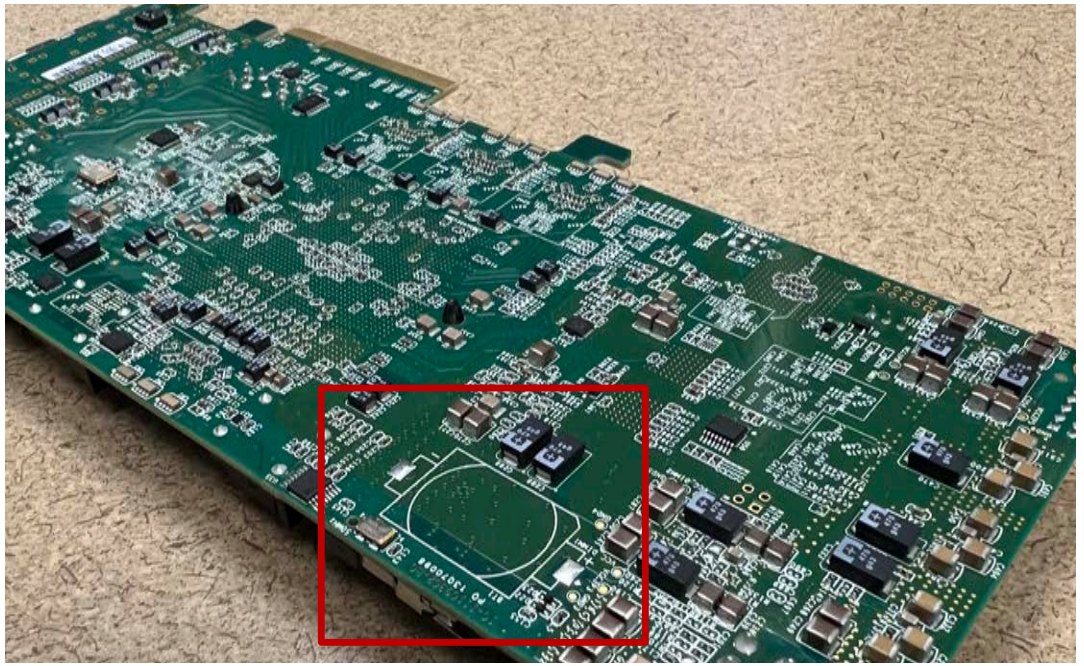
- Light
  - Detect enclosure opening
  - Requires opaque enclosure
- Contact
  - Electrical connection between enclosure halves
  - Often used in conjunction with light sensor
- Capacitance
  - Changes in capacitance indicate physical changes
  - E.g. cut wires, open enclosure, etc.

Tamper Detection Mechanisms

- Light
  - Detect enclosure opening
  - Requires opaque enclosure
- Contact
  - Electrical connection between enclosure halves
  - Often used in conjunction with light sensor
- Capacitance
  - Changes in capacitance indicate physical changes
  - E.g., cut wires, open enclosure, etc.
- Magnets/magnetic fields
  - Detect proximity of enclosure halves

Anti-Tamper Reactions

- Alert/Alarm
  - Notify user of tamper detection
  - Useful if system must still operate
  - Warranties and insurance
- Erase secret/sensitive state
  - Wipe memory
  - Volatile storage very quick to erase
- Denial of service
  - Prevent further operation of system
  - Physically destroy system components

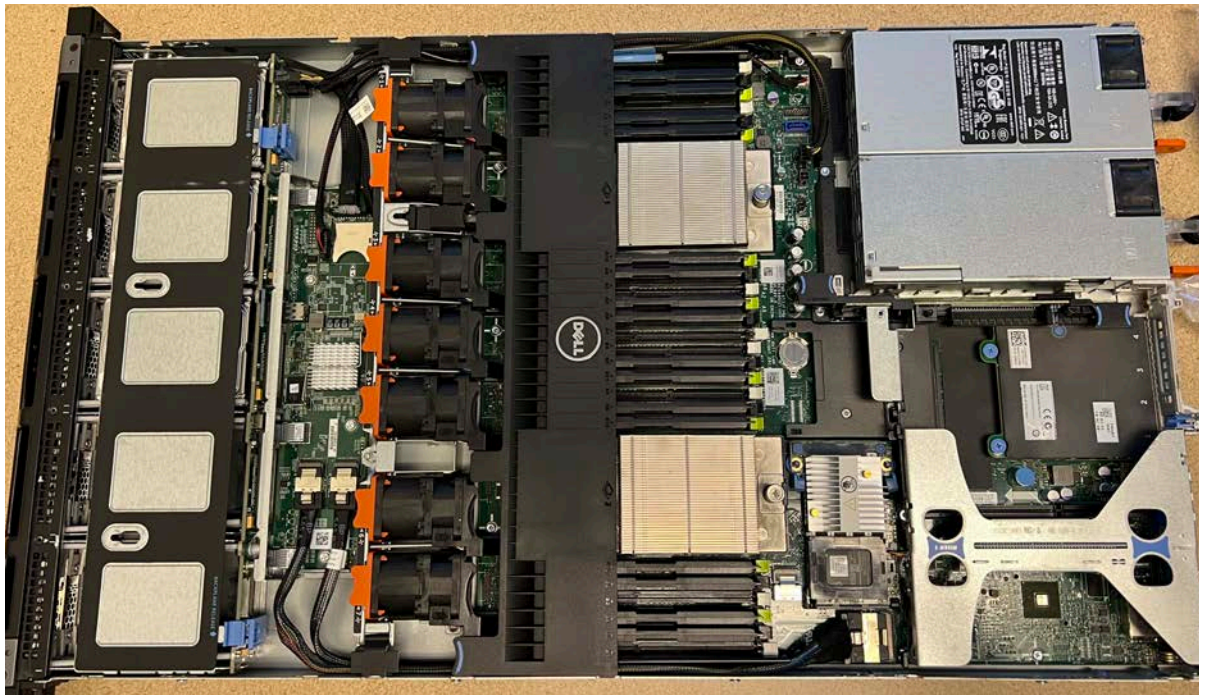


Unpopulated Coin-cell Battery Socket for volatile FPGA Bitstream storage

Enclosure Level Anti-Tamper

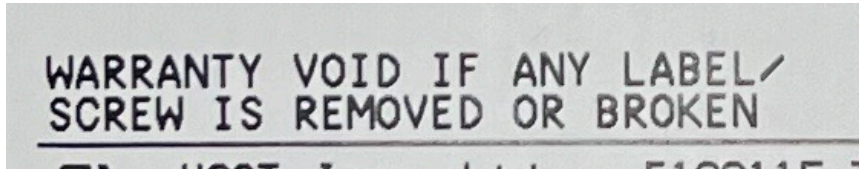
Enclosure Level Anti-Tamper

- Prevent intrusion to system casing
- Mitigate attacks on enclosure
  - PCB modifications
  - Flash/RAM chip probing
  - JTAG/Scan-Chain attacks
- Low complexity for attacks and defenses



Server Enclosure

Enclosure Level Anti-Tamper Comparison

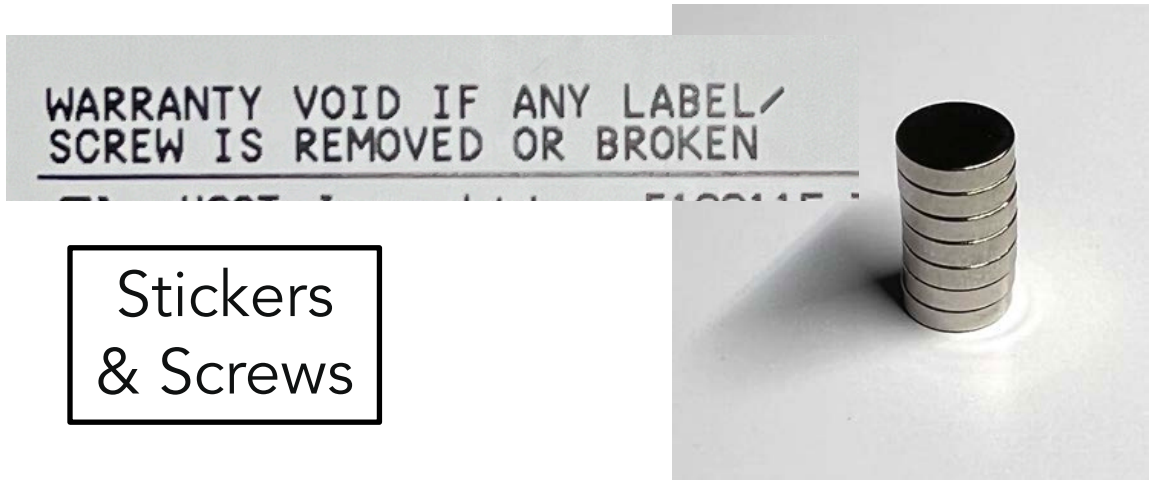


Stickers & Screws

Complexity

Enclosure Level Anti-Tamper Comparison

Magnets, Plungers & Contact Sensors



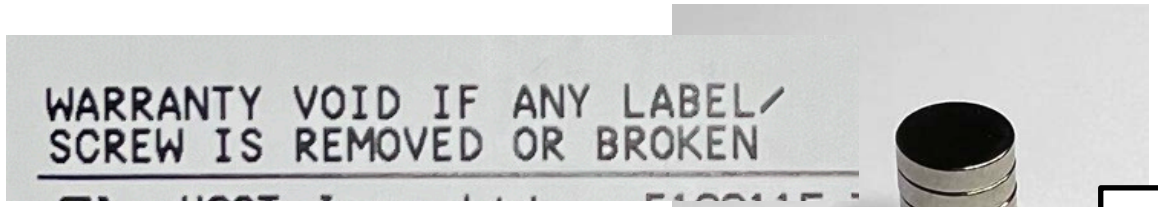
Stickers & Screws

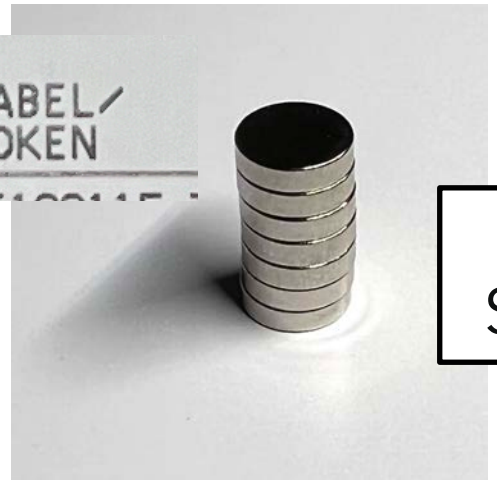
Complexity

Enclosure Level Anti-Tamper Comparison

Magnets, Plungers & Contact Sensors

Light Sensors



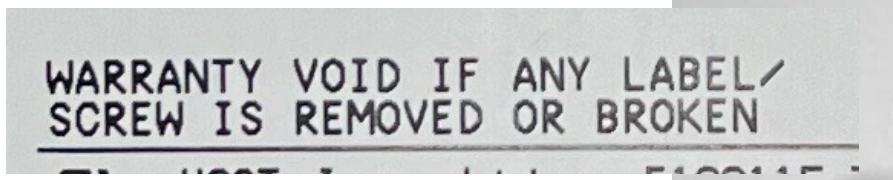


Stickers & Screws

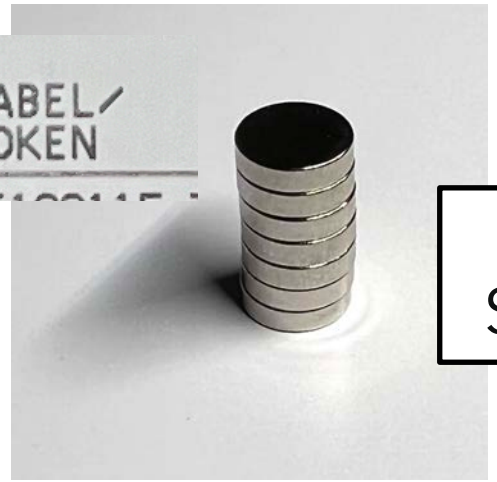
Complexity

Enclosure Level Anti-Tamper Comparison

Magnets, Plungers & Contact Sensors

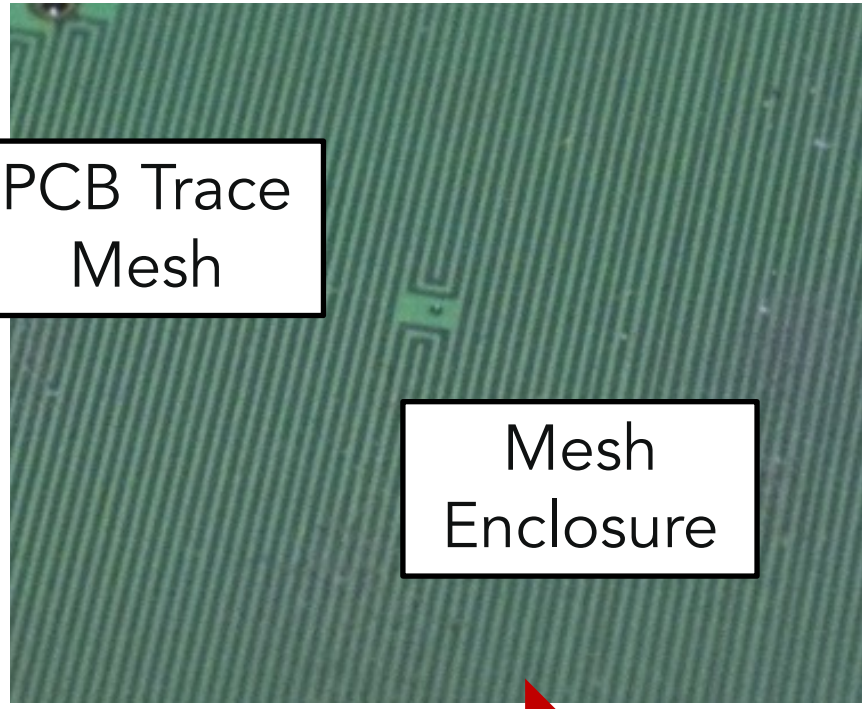


Stickers & Screws



Light Sensors

PCB Trace Mesh

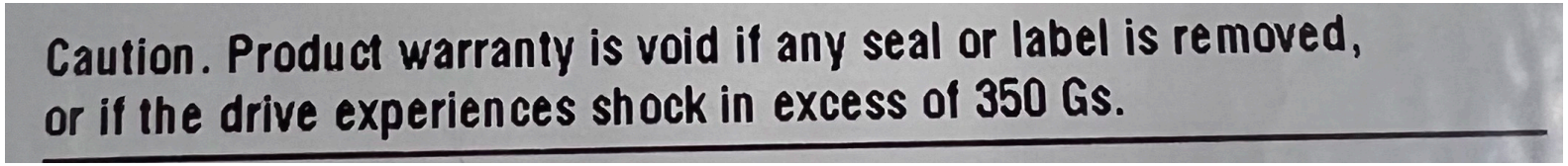


Mesh Enclosure

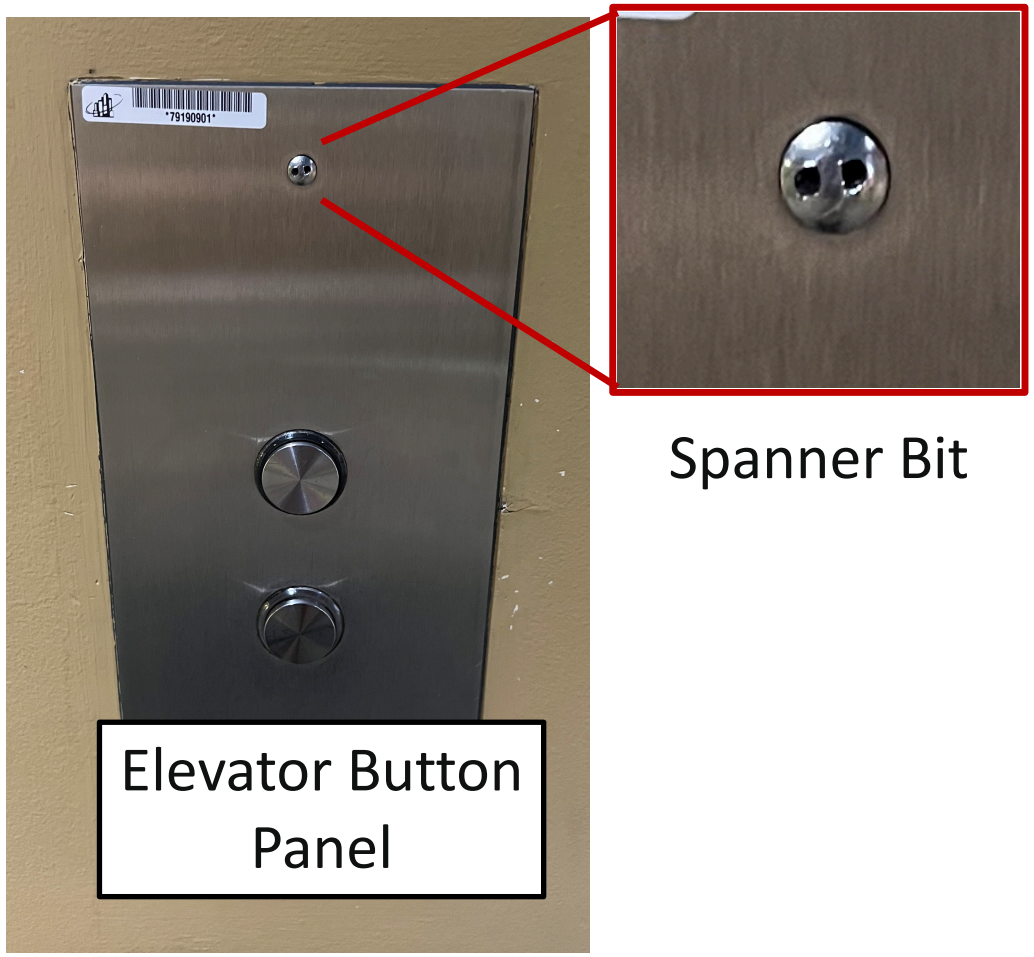
Complexity

Enclosure Anti-Tamper – Stickers!

- Trivial to bypass
- Slightly more difficult to defeat without evidence of access
  - Would need to create custom sticker
  - Doable, but cost/benefit tradeoff rarely makes sense
- Best for tracking warranty status



Enclosure Anti-Tamper – Different Screws & Bits



Spanner Bit

“tamper proof”
Torx Star Bit

NEIKO 10048A Security Bit Set
Source: Amazon.com

Point-of-Sale (PoS) System Teardown

- Teardown on Hack-a-day
  - From out-of-business Toys R Us store
    - Remember them?
- Point-of-Sale System
  - Direct connections to credit cards
  - Processing financial transitions
  - Directly accessed by customers

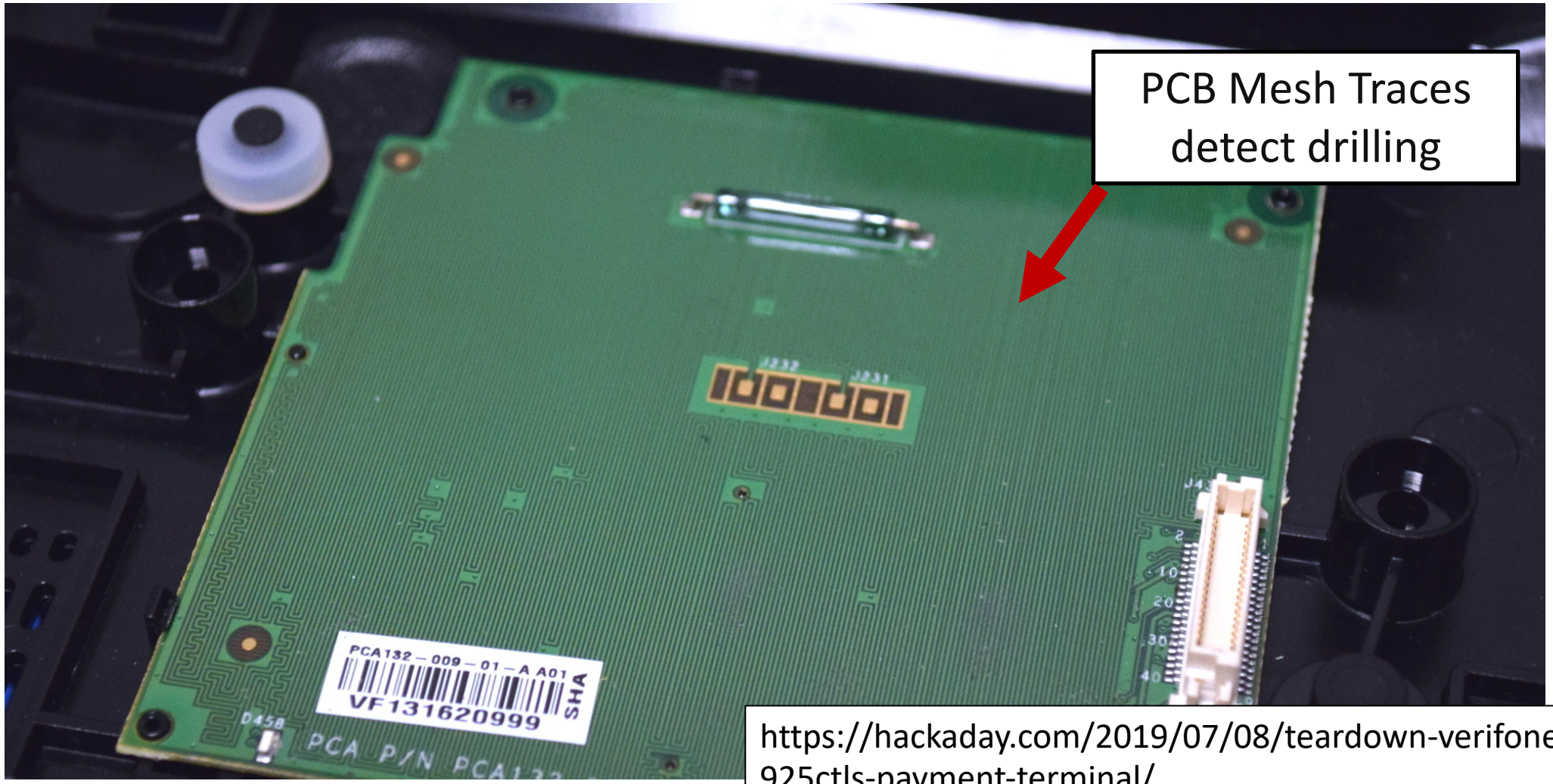
https://hackaday.com/2019/07/08/teardown-verifone-mx-925ctls-payment-terminal/

Point-of-Sale (PoS) System Teardown

- Teardown on Hack-a-day
  - From out-of-business Toys R Us store
    - Remember them?
- Point-of-Sale System
  - Direct connections to credit cards
  - Processing financial transitions
  - Directly accessed by customers
- Target's PoS system hacked to steal credit card numbers
- Rare example of commercial system that cares about security

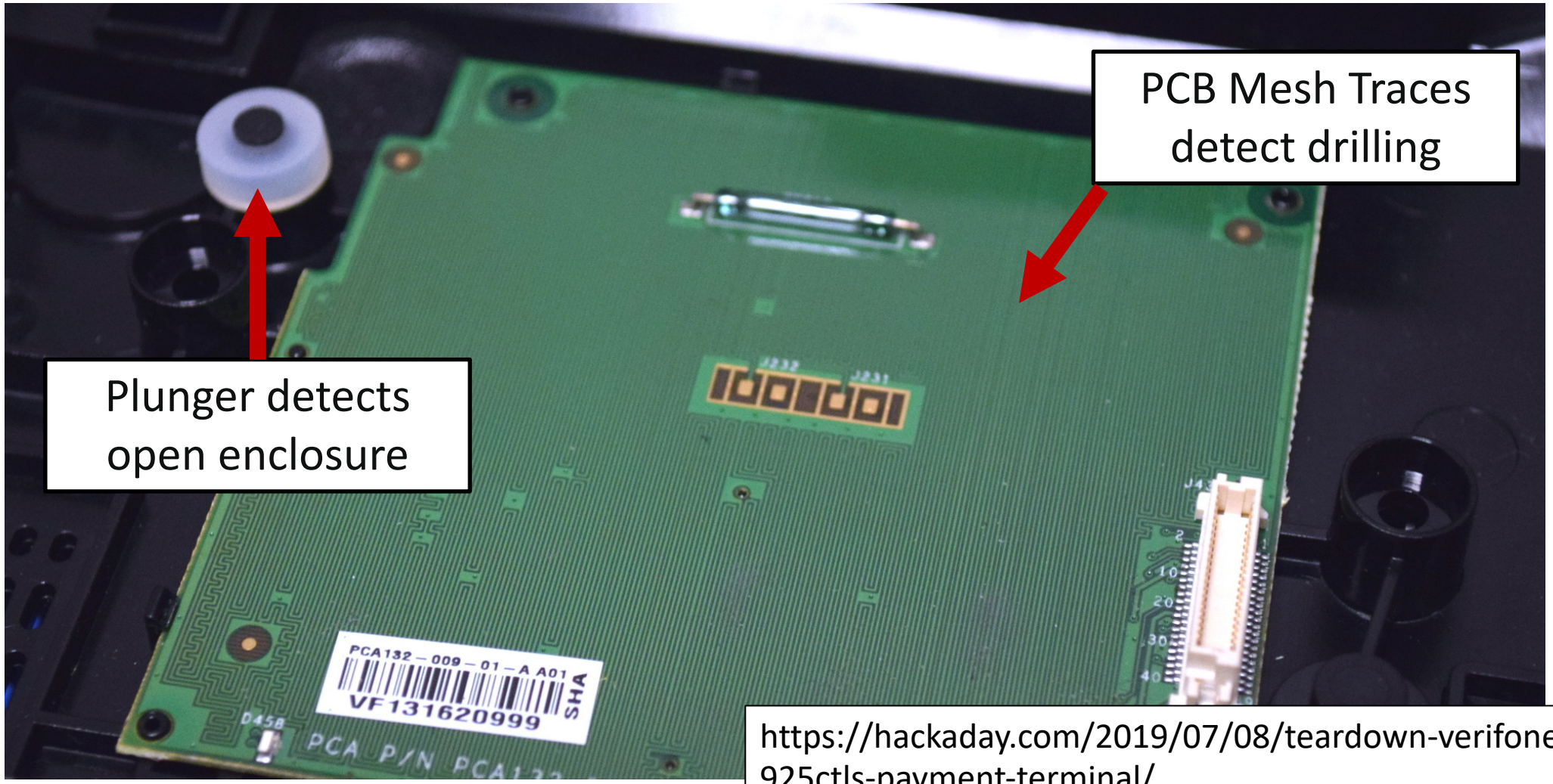
https://hackaday.com/2019/07/08/teardown-verifone-mx-925ctls-payment-terminal/

Real-World Anti-Tamper Mechanisms



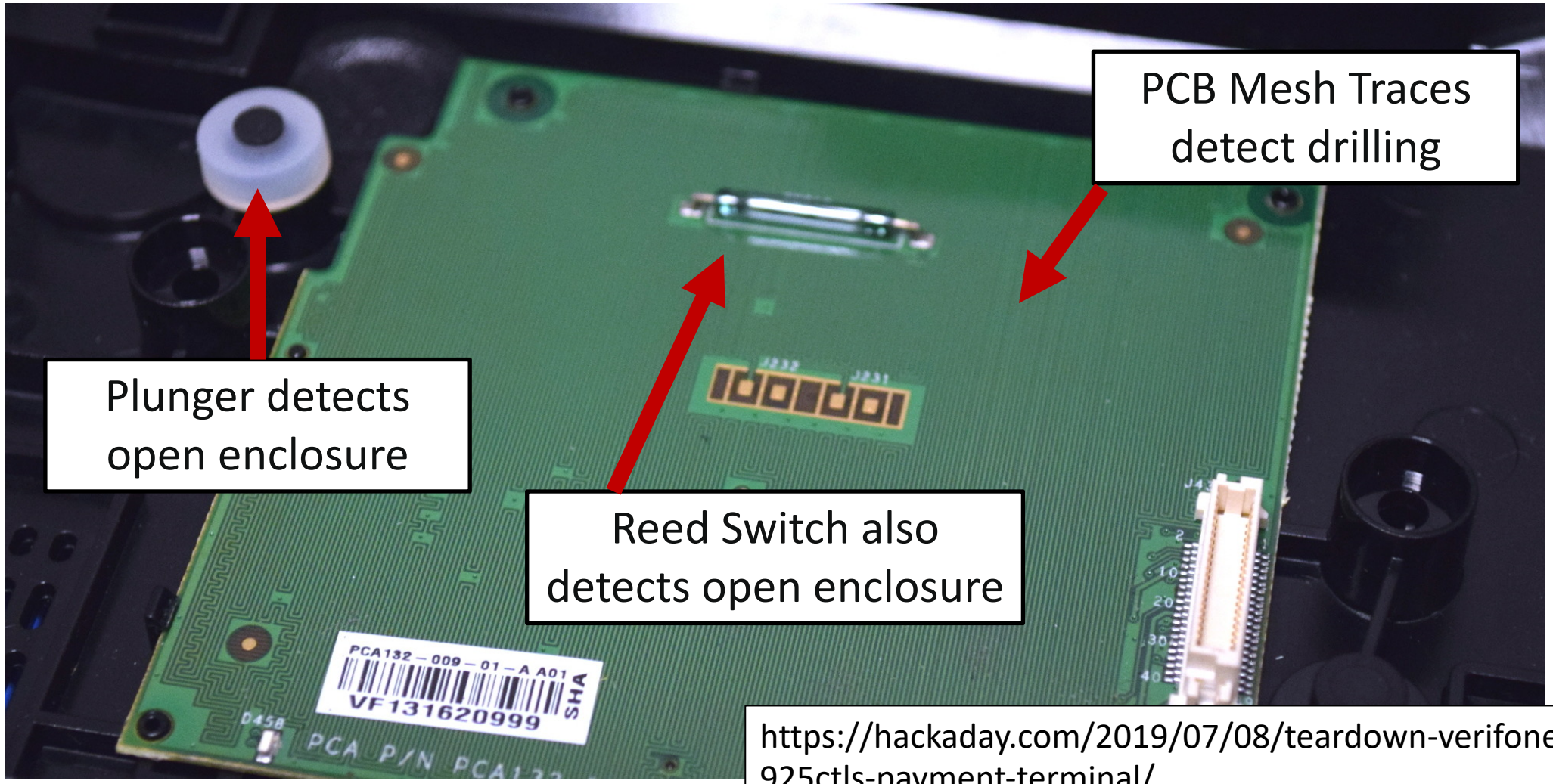
https://hackaday.com/2019/07/08/teardown-verifone-mx-925ctls-payment-terminal/

Real-World Anti-Tamper Mechanisms



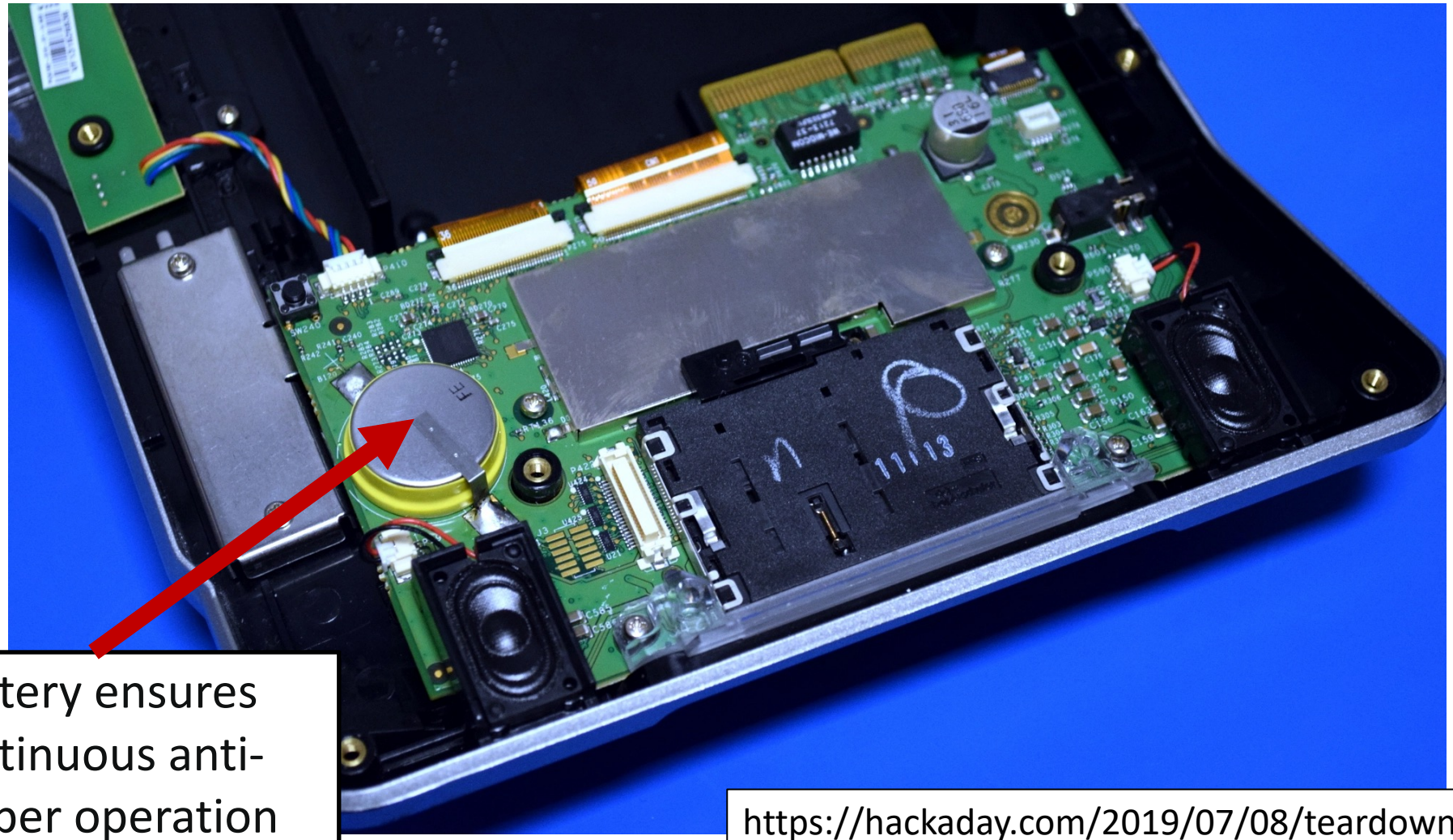
https://hackaday.com/2019/07/08/teardown-verifone-mx-925ctls-payment-terminal/

Real-World Anti-Tamper Mechanisms



https://hackaday.com/2019/07/08/teardown-verifone-mx-925ctls-payment-terminal/

Real-World Anti-Tamper Mechanisms



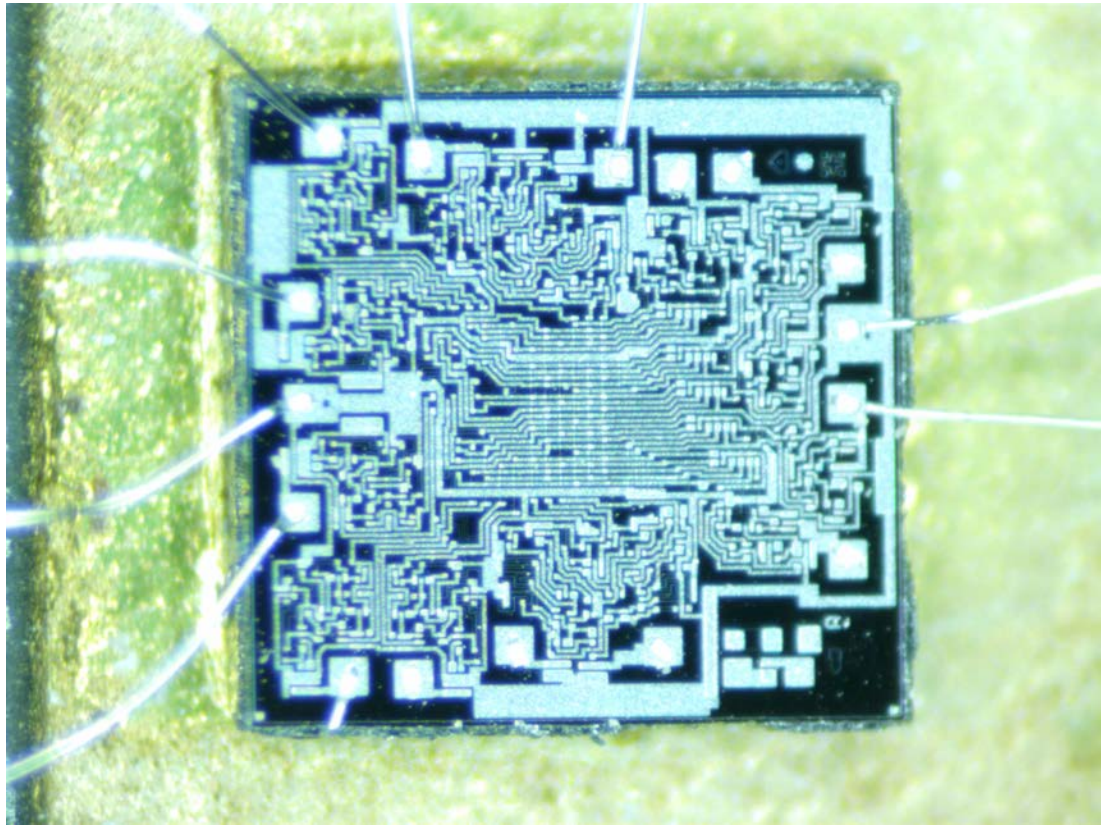
Battery ensures continuous anti-tamper operation

https://hackaday.com/2019/07/08/teardown-verifone-mx-925ctls-payment-terminal/

Circuit Level Anti-Tamper

Circuit Level Anti-Tamper

- Tamper detection circuits added to ICs and packaging
- Mitigate circuit level attacks
  - Key theft
  - IP reverse engineering
  - Fault injection
- High complexity implementation
- Even higher cost/complexity for attackers



Circuit Edit Attacks – Focused Ion Beam

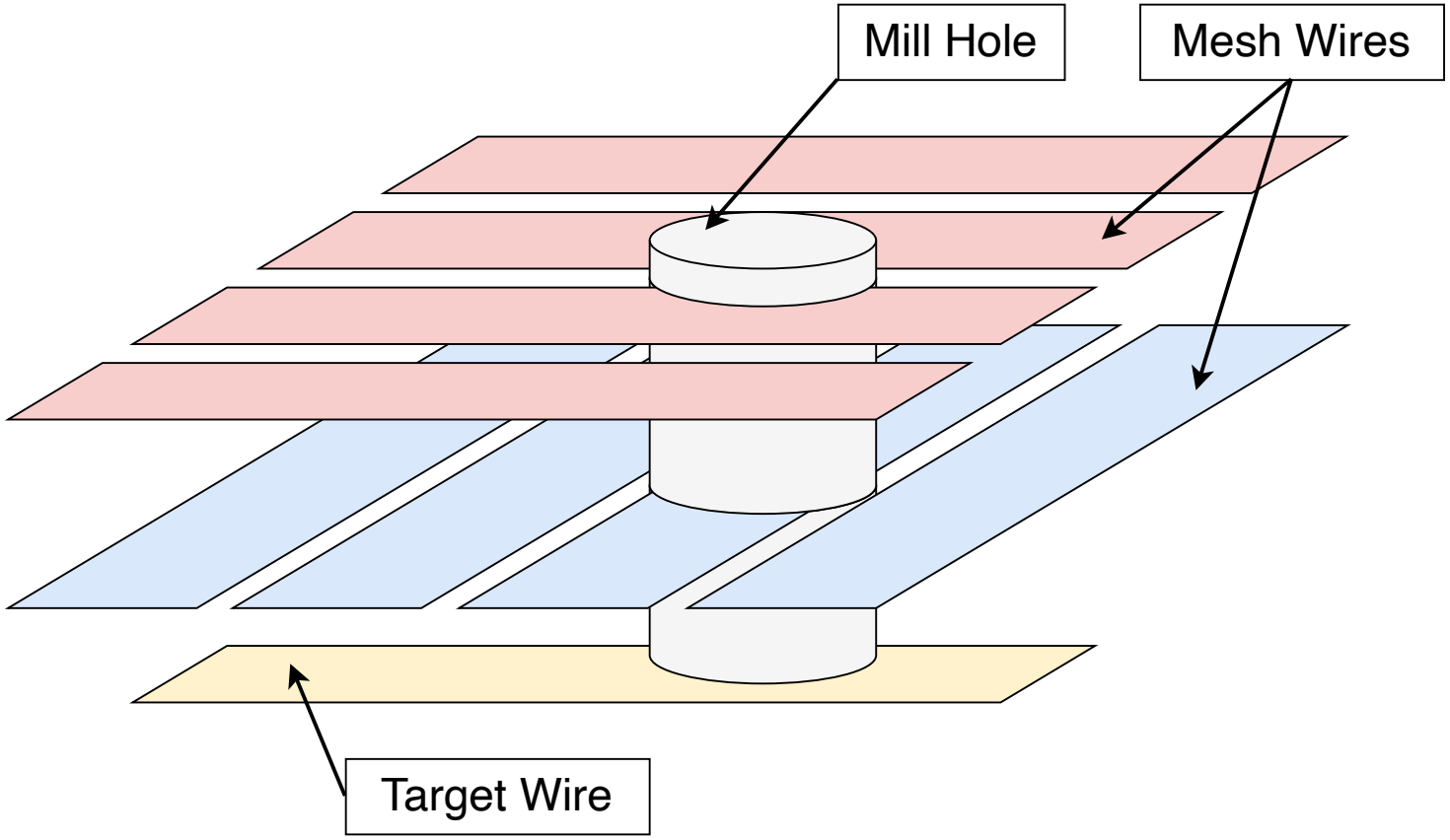
- Focused Ion Beam
  - Hit sample IC with beam of Gallium Ions
  - Nanometer resolutions possible
- Material deposition
  - Add material to IC
  - Create new wires & probe points, short existing paths
- Material removal
  - Mill holes for probing
  - Cut/open specific wires

Focused Ion Beam Workstation

Source: Swarup Bhunia, Mark Tehranipoor ,
“Hardware Security: A Hands on Learning Approach”

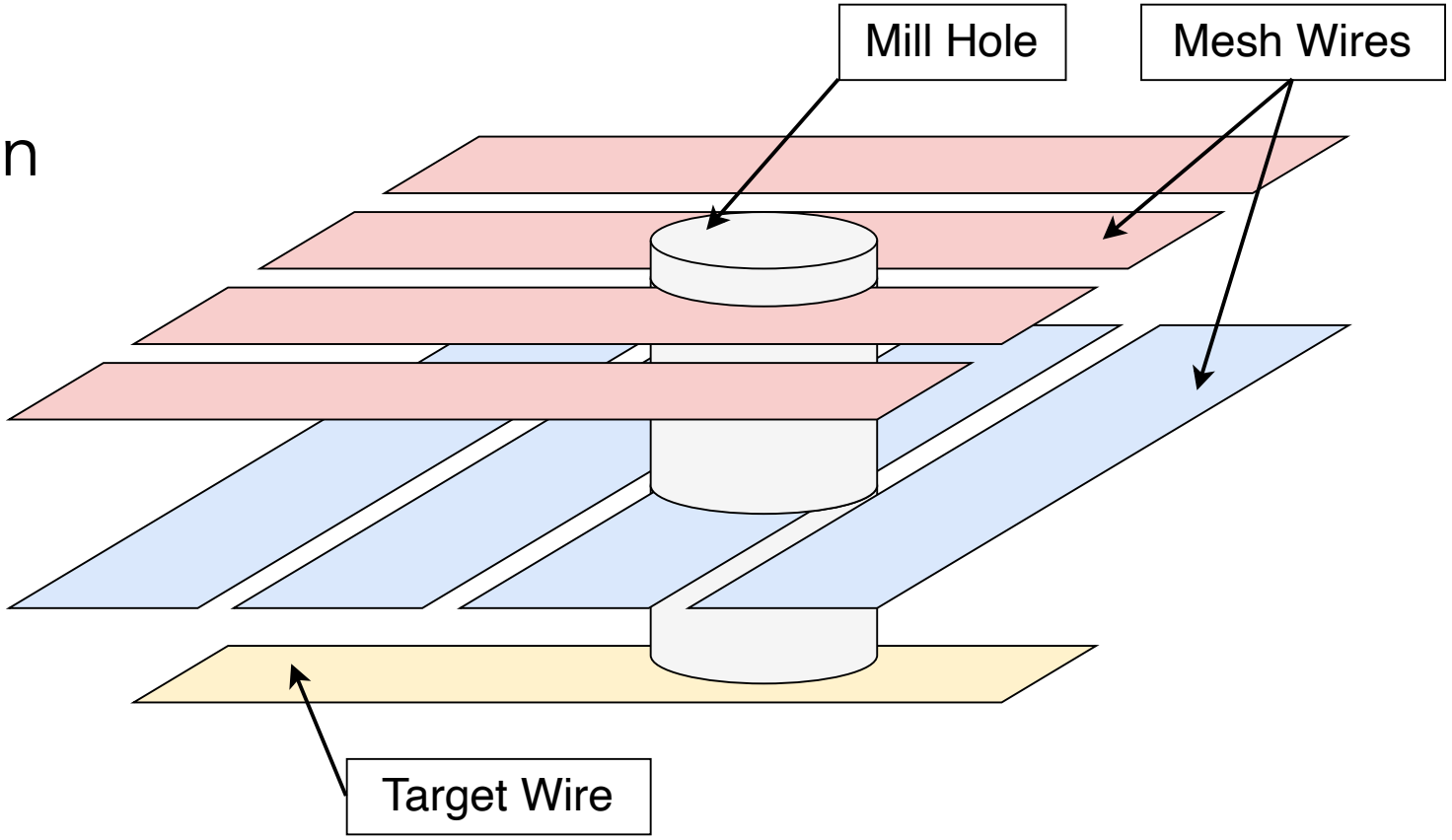
Integrated Circuit Mesh Shields

- Two layers of metal wires on top/bottom of circuit
- Detect cuts to wires
- Wires too dense to probe/cut around
  - Detect IC probing
- Trigger response with dedicated circuit



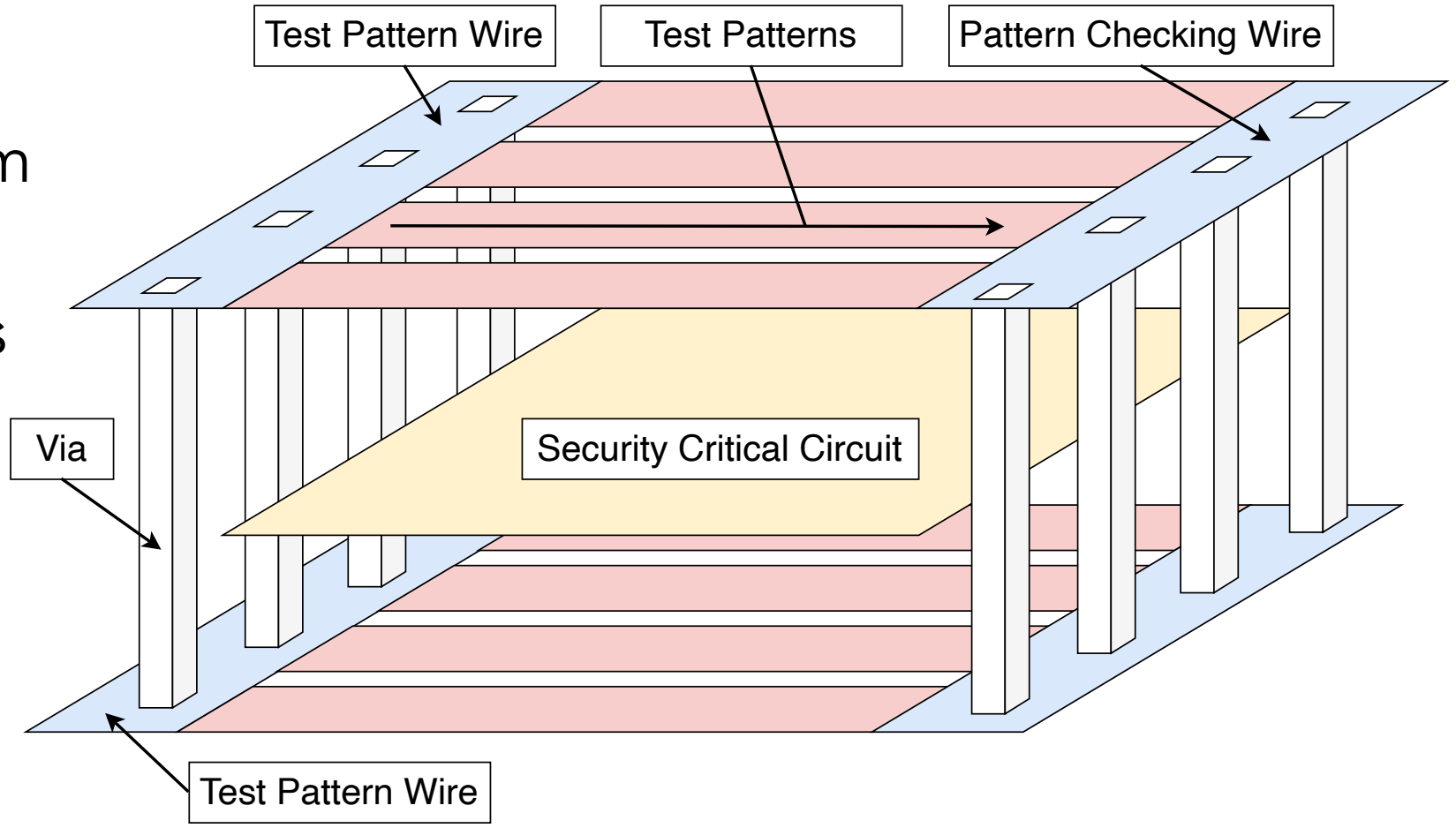
Integrated Circuit Mesh Shields

- Multiple detection methods possible
- Active pattern generation
  - Next slide
- Passive capacitance measurement
  - Detect changes in capacitance of wires
  - Could detect partial wire breaks



Mesh Shields with Active Pattern Checking

- Continuously transmit pattern across top & bottom wires
- Check that patterns match on receiving side of chip
- Trigger response if patterns do not match



Anti-Tamer in FPGAs

FPGAs in Industry – Who Uses FPGAs?

- The Xilinx website lists
  - Aerospace & Defense
  - Automotive
  - Broadcast & Pro A/V
  - Data Center
  - Emulation & Prototyping
  - Test & Measurement
  - Wired & Wireless Communications
- Which of these Industries care about security?

FPGAs in Industry – Who Uses FPGAs?

- The Xilinx website lists
  - Aerospace & Defense
  - Automotive
  - Broadcast & Pro A/V
  - Data Center
  - Emulation & Prototyping
  - Test & Measurement
  - Wired & Wireless Communications
- Which of these Industries care about security?

Department of Defense a major consumer of FPGAs and cares a lot about security

FPGAs in Industry – Who Uses FPGAs?

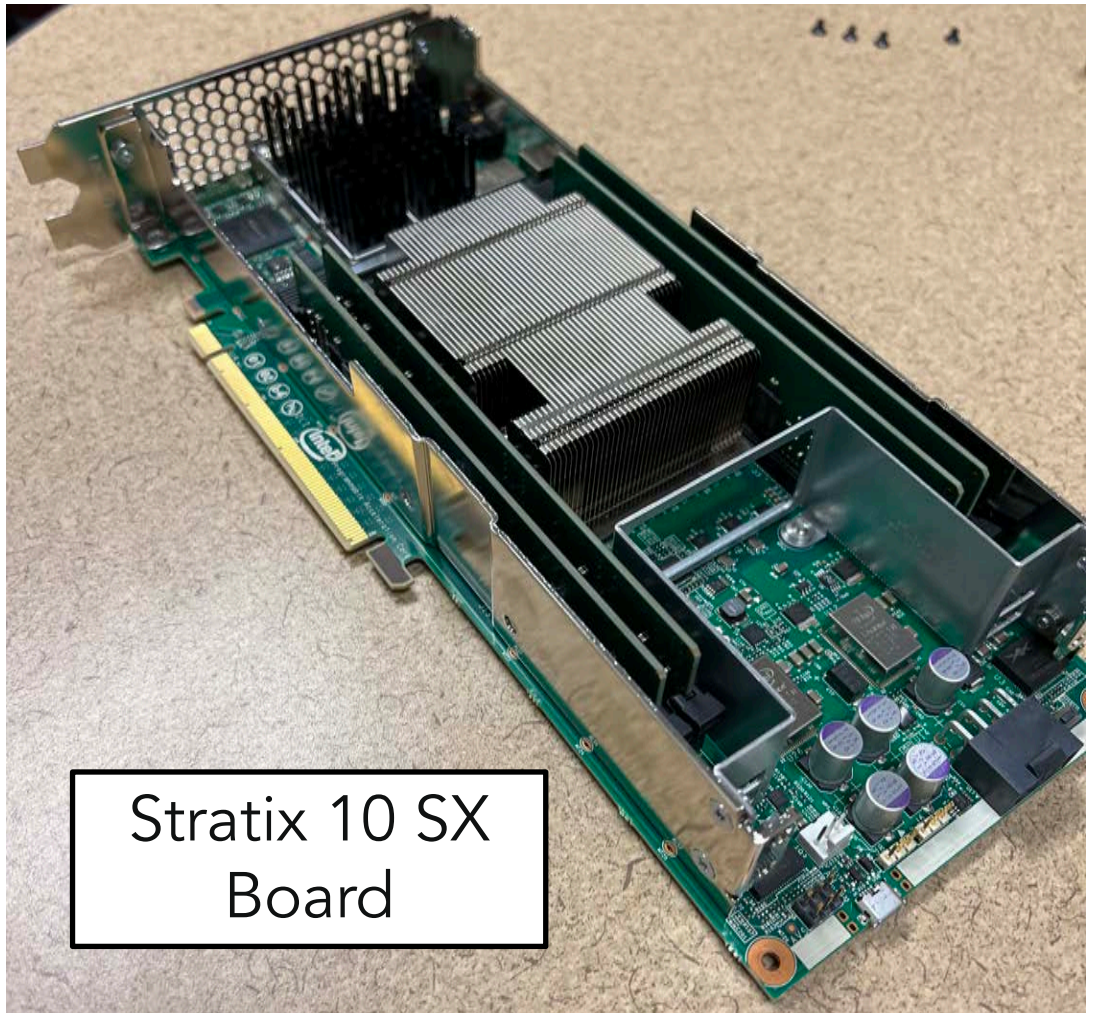
- The Xilinx website lists
  - Aerospace & Defense
  - Automotive
  - Broadcast & Pro A/V
  - Data Center
  - Emulation & Prototyping
  - Test & Measurement
  - Wired & Wireless Communications
- Which of these Industries care about security?

Department of Defense a major consumer of FPGAs and cares a lot about security

Network providers rely on FPGAs for their flexibility in supporting new protocols. FPGAs deployed with limited access control

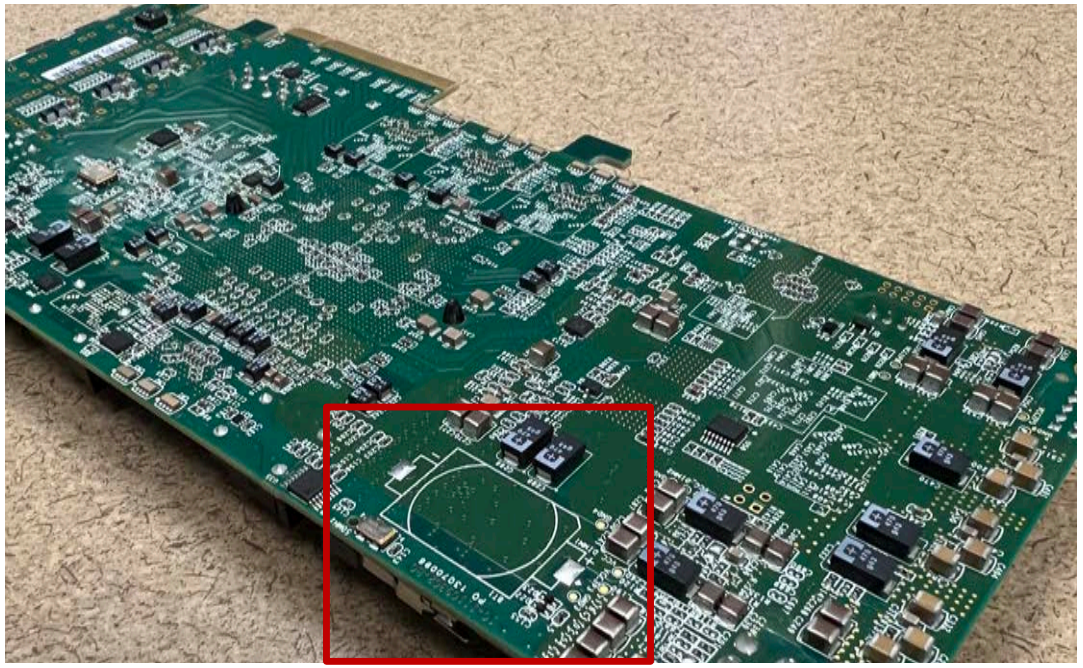
FPGA Anti-Tamper and Security Overview

- Early adopters for many security features
  - Configurable nature provides flexibility
  - Features available, but not mandatory
- Government/Defense applications
  - Low Volume – Perfect for FPGAs
  - Pays a premium for security



FPGAs = Volatile Hardware

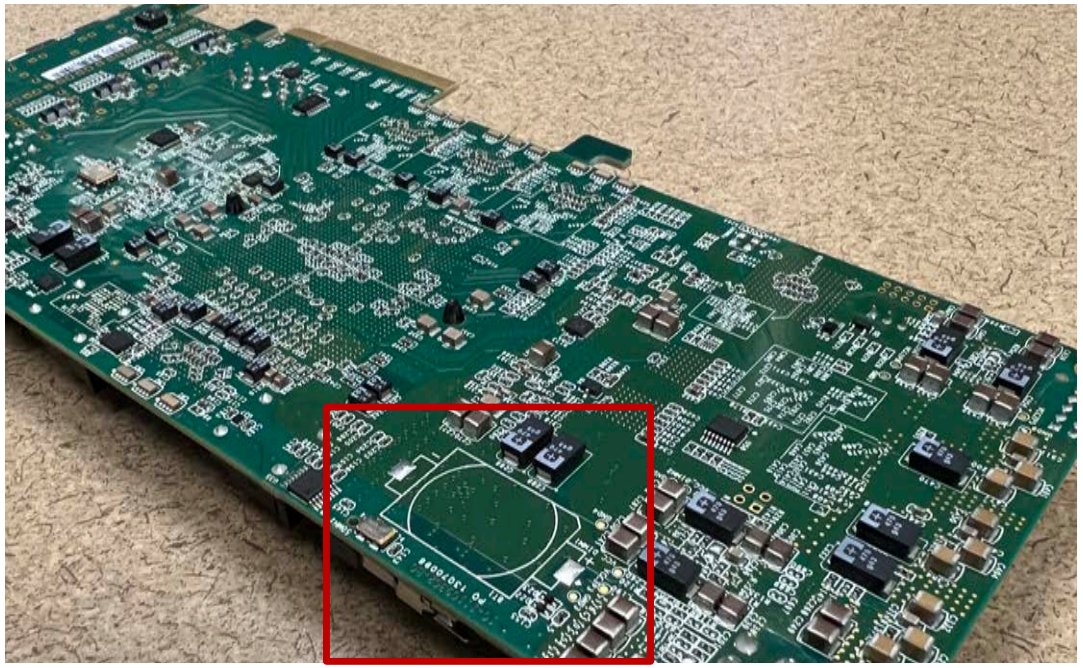
- Battery Backed bitstream
  - Stores configuration in volatile SRAM
  - Remains powered for lifetime of the device/system
- During attack detection
  - Power removed from FPGA configuration memory
  - Volatile SRAM quickly erased



Unpopulated Coin-cell Battery Socket for FPGA Bitstream storage

FPGAs = Volatile Hardware

- Attacker cannot recover hardware configuration
- Little to no reverse engineering possible with unconfigured FPGA
  - Software, firmware, & secret keys may still exist
  - Solutions to quickly wipe those too
- Technique common enough that battery socket included on "Development & Education" boards

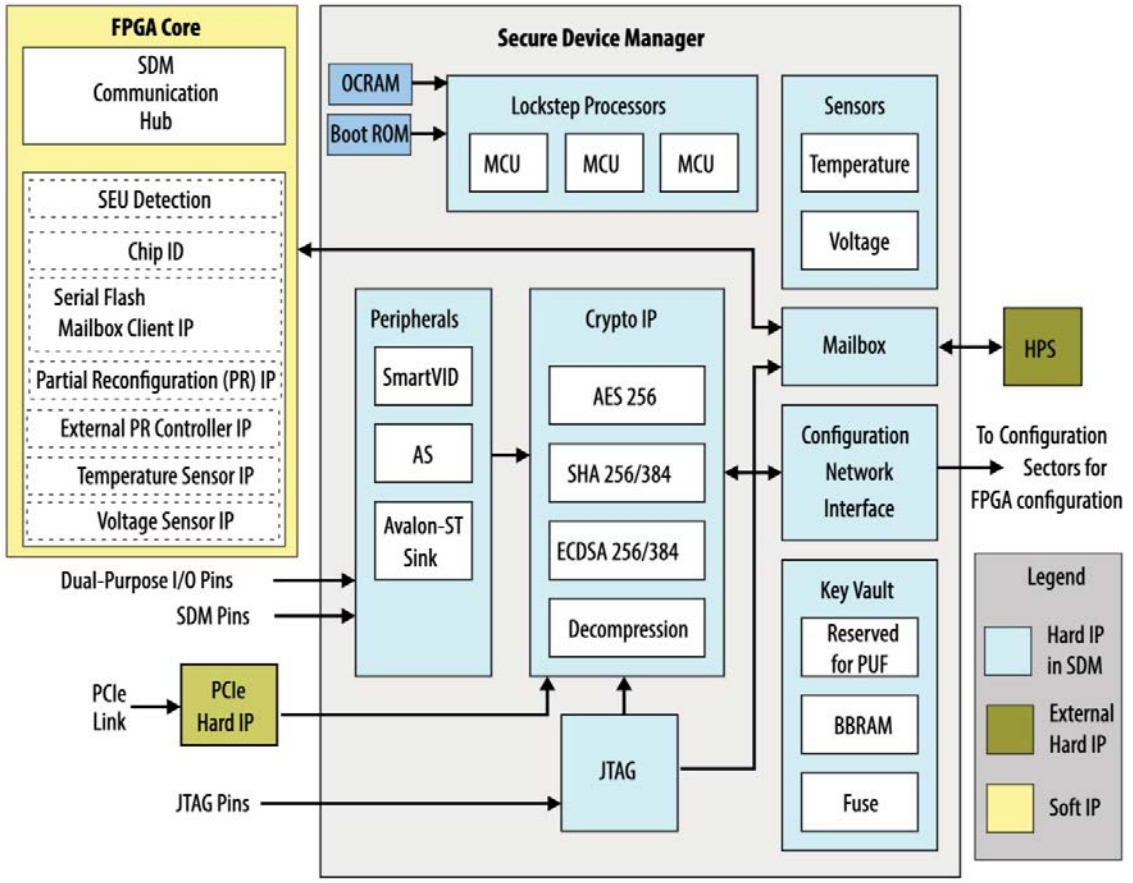


Unpopulated Coin-cell Battery Socket for FPGA Bitstream storage

Stratix 10 Security Device Manager (SDM) Features

- Dedicated "Advanced Security" FPGA part numbers
- Built-in anti-tamper detection
  - Detect & respond to tampering
  - Soft-logic/user-customizable tamper detection
  - Hard logic tamper detection
- PUFs & unique device ids
  - Key generation
  - Device fingerprinting

Figure 3. SDM Block Diagram

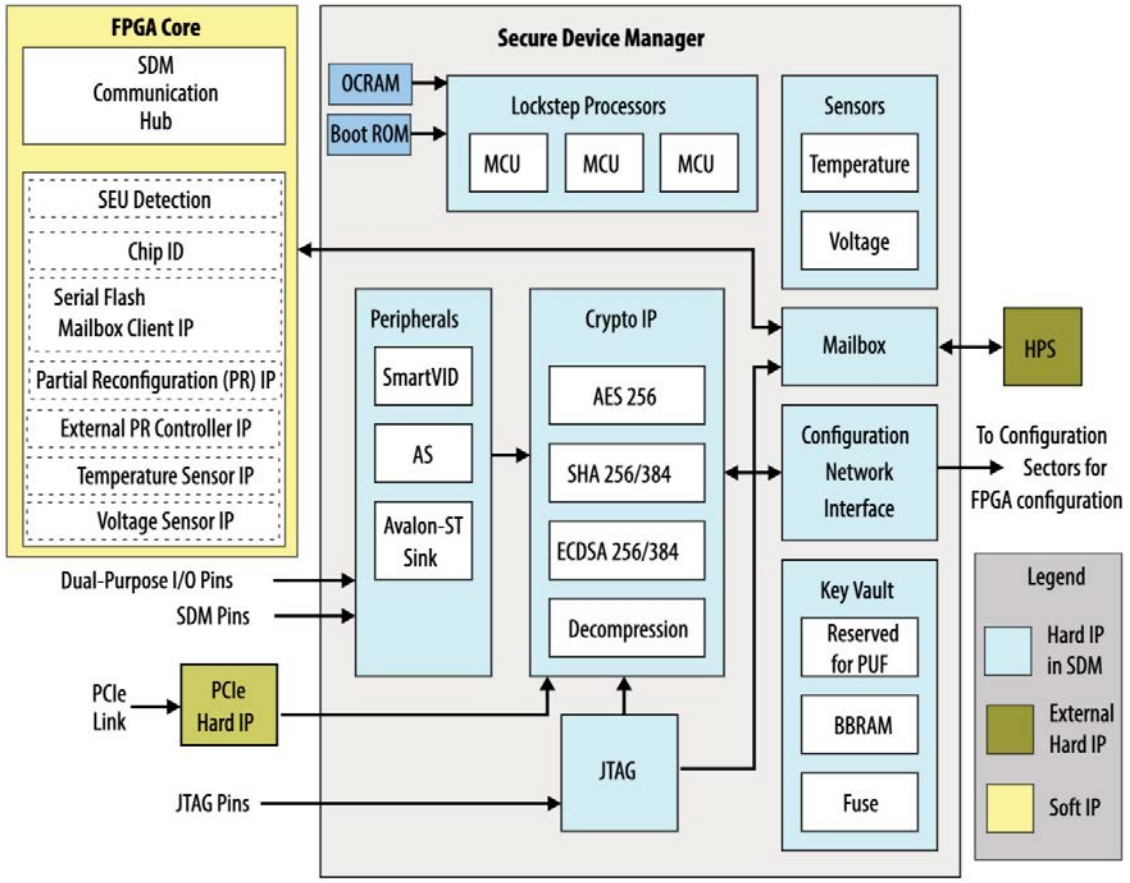


Source: Intel.com

Stratix 10 Security Device Manager (SDM) Features

- Bitstream encryption & authentication
  - Prevent reverse engineering
  - Only run trusted configurations
- Secure debug Authorization
  - Mitigate Scan-chain attacks
- Platform Attestation
  - Assure remote user they are communicating with real Stratix 10 platform

Figure 3. SDM Block Diagram



Source: Intel.com

Stratix 10 Tamper Detection

- Detection sensors
  - Frequency
  - Voltage
  - Temperature
- Targeting fault-injection and side channel attacks
- Custom tamper detection supported w/ soft logic inputs
- Max 5ms response time to zero data

Stratix 10 Anti-Tamper Response
None
Notification only
Notification, Device Wipe & Lock
Notification, Device Wipe & Lock, Memory Zeroization
Notification, Device Wipe & Lock, Memory Zeroization, Key Zeroization

Tamper Response - Extreme Example

- Includes "Enable Device Self-Kill" setting
- Uses eFuses to prevent device configurations
  - Only a single sentence about what this does & how it works exists online

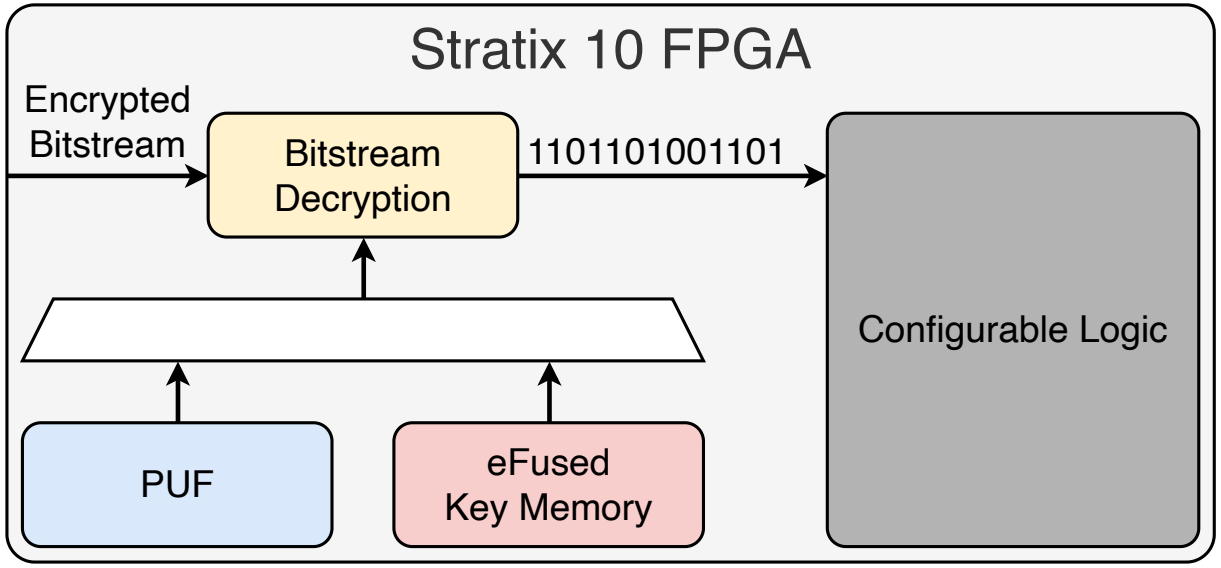
Box

QTY	UNIT PRICE	EXT PRICE
1	$12,000.00000	$12,000.00

Stratix 10 Development Board Price

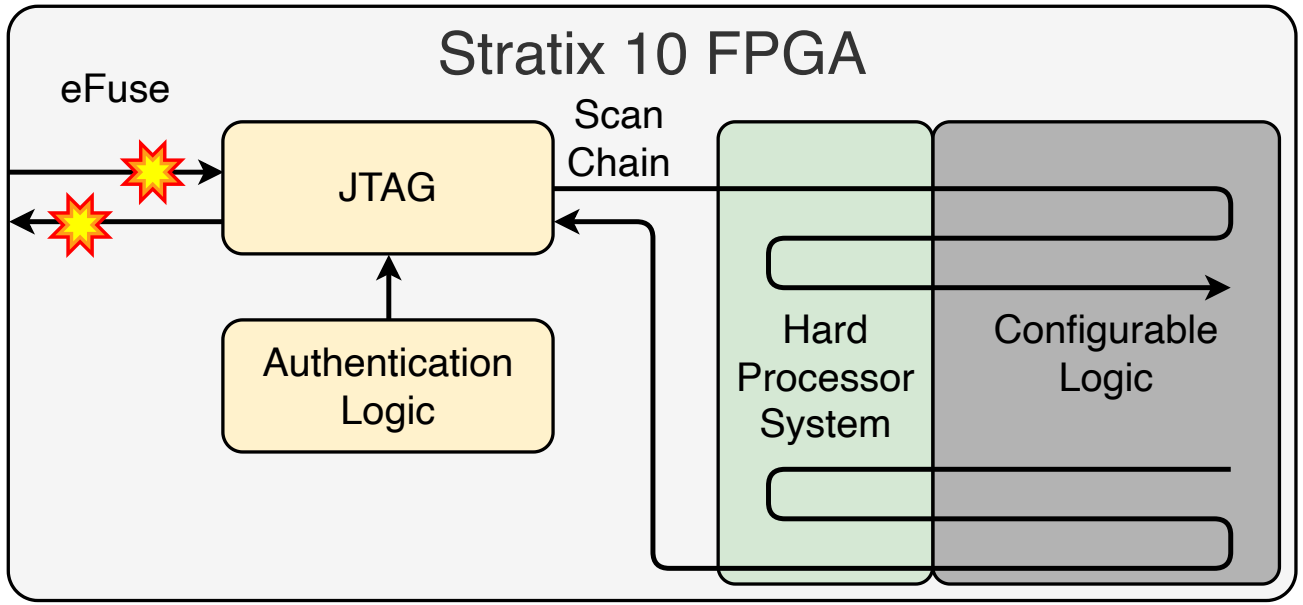
FPGA Bitstream Encryption

- Prevent adversary from reverse engineering bitstream stored in FLASH
- eFused key memory
  - Customer sets key
- Per-device Bitstreams
  - Encrypted with PUF key
  - Works only on given device
  - Cannot be copied/stolen



Scan-Chain Protections

- Scan chain requires authentication
- Attacker cannot probe it without proper credentials
- Disable scan-chain with eFuses
  - Prevent any future use
  - Components frequently not serviceable anyway
  - Minimize attack surface



Upcoming Lectures

- Secure Computation Approaches