Security Challenges of COTS and possible solutions

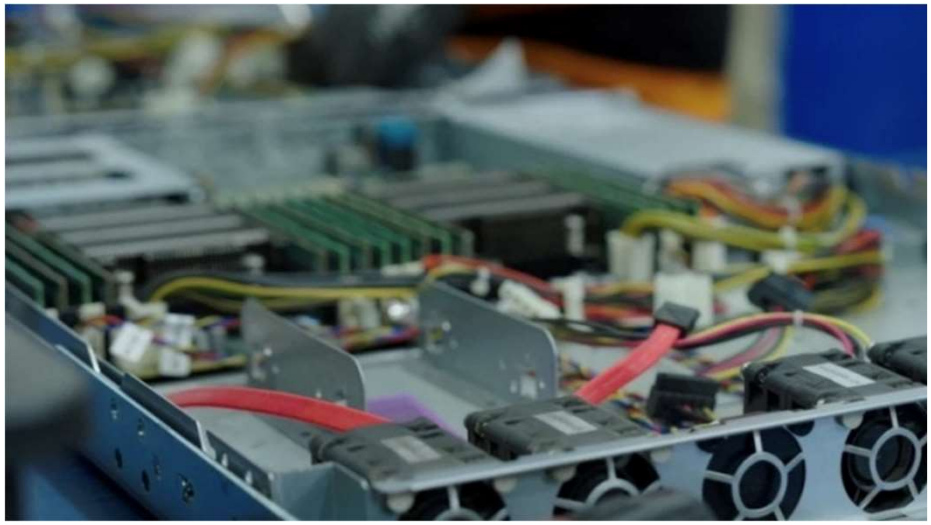
Chester Rebeiro

Secure Architectures for Embedded Systems Lab

Computer Science and Engineering

IIT Madras

COTS devices



Readymade Hardware or Software

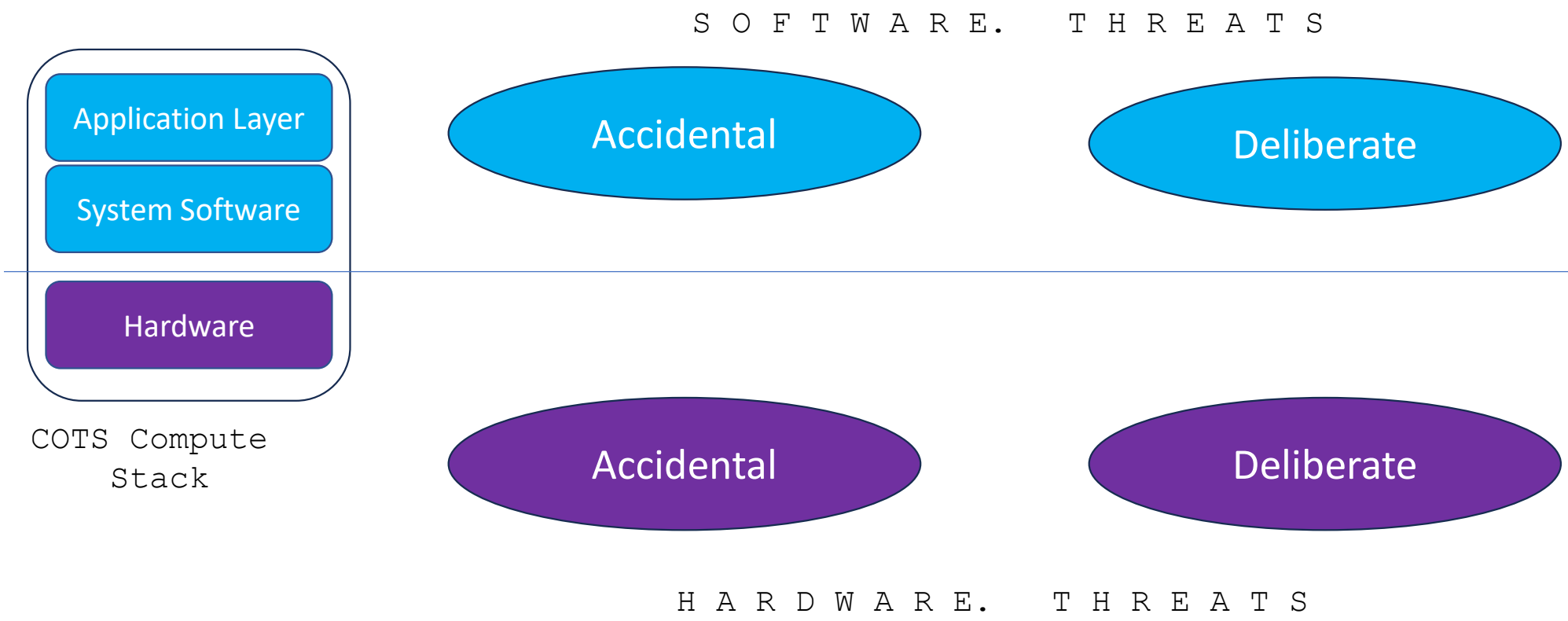
Easily Pluggable and adaptable by the purchasing organization

Several Advantages

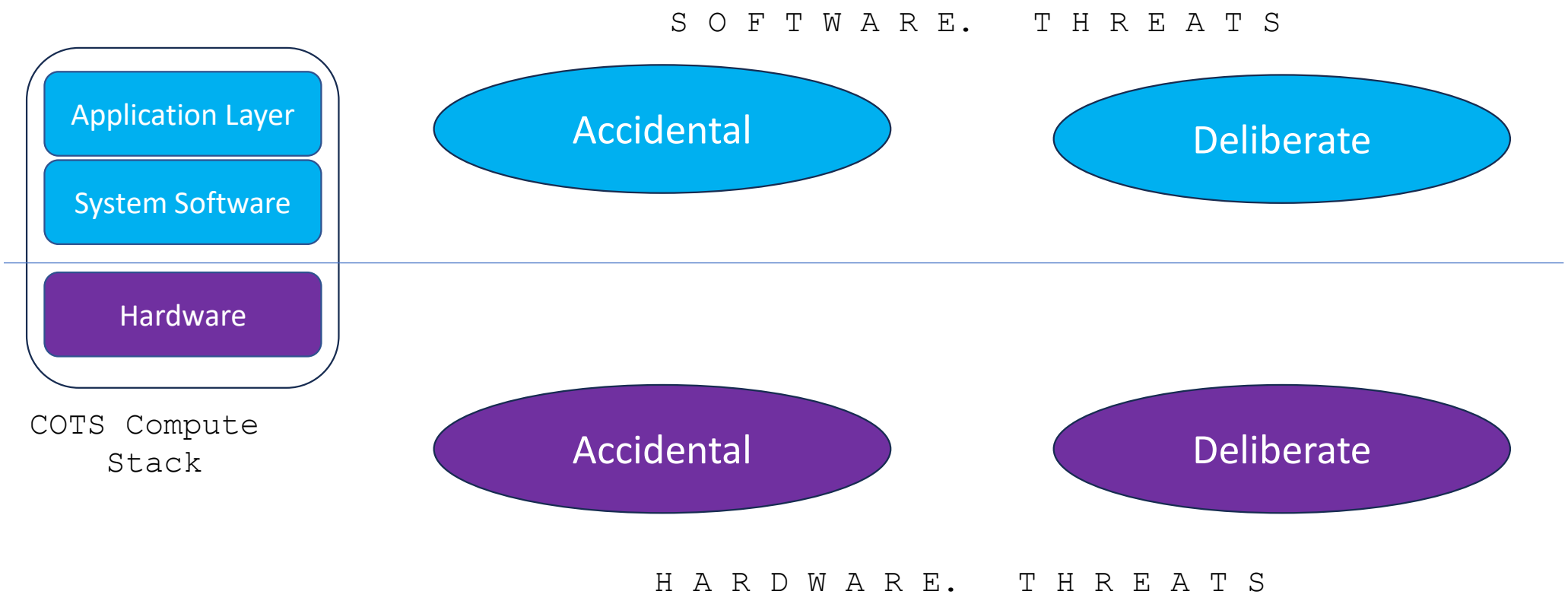
- Reduce costs
- Quick to deploy
- Support and maintenance
- Easier to find expertise

Disadvantage: Security Threats!!!

Security threats in COTS devices



Security threats in COTS devices



Threats from software that are accidentally introduced

Accidental

Software Vulnerabilities

In COTS, threat amplified by transparency and homogeneity

- Example Stuxnet: Exploits utilized vulnerabilities mainly in COTS software and devices Step 7 project file, Windows Server RPCs, Win CC servers, Siemens PLCs

COTs developer focus on functionality rather than security

- Little or no liability
- No mandatory certification in several scenarios

Threats from software introduced deliberately

Deliberate

Backdoors and Trojans in Software

ANDY GREENBERG SECURITY MAY 31, 2023 9:00 AM

Millions of PC Motherboards Were Sold With a Firmware Backdoor

Hidden code in hundreds of models of Gigabyte motherboards invisibly and insecurely downloads programs—a feature ripe for abuse, researchers say.

TECH / GOOGLE / ANDROID

Android malware once found a way onto phones before they even shipped

'Trojan Horse': Pentagon Suspects Chinese-made Cranes Across US Ports Being Used for Spying

Threats from software introduced deliberately

Deliberate

Backdoors and Trojans in Software

ANDY GREENBERG SECURITY MAY 31, 2023 9:00 AM

Millions of PC Motherboards Were Sold With a Firmware Backdoor

Hidden code in hundreds of models of Gigabyte motherboards invisibly and insecurely downloads programs—a feature ripe for abuse, researchers say.

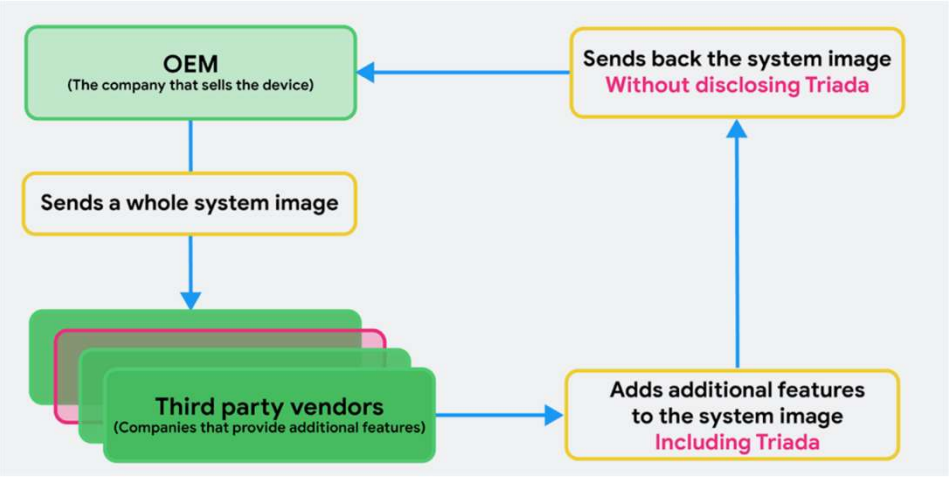
TECH / GOOGLE / ANDROID

Android malware once found a way onto phones before they even shipped

'Trojan Horse': Pentagon Suspects Chinese-made Cranes Across US Ports Being Used for Spying

Example: Triada Trojan in Android

Installation into Android through 3rd party vendors



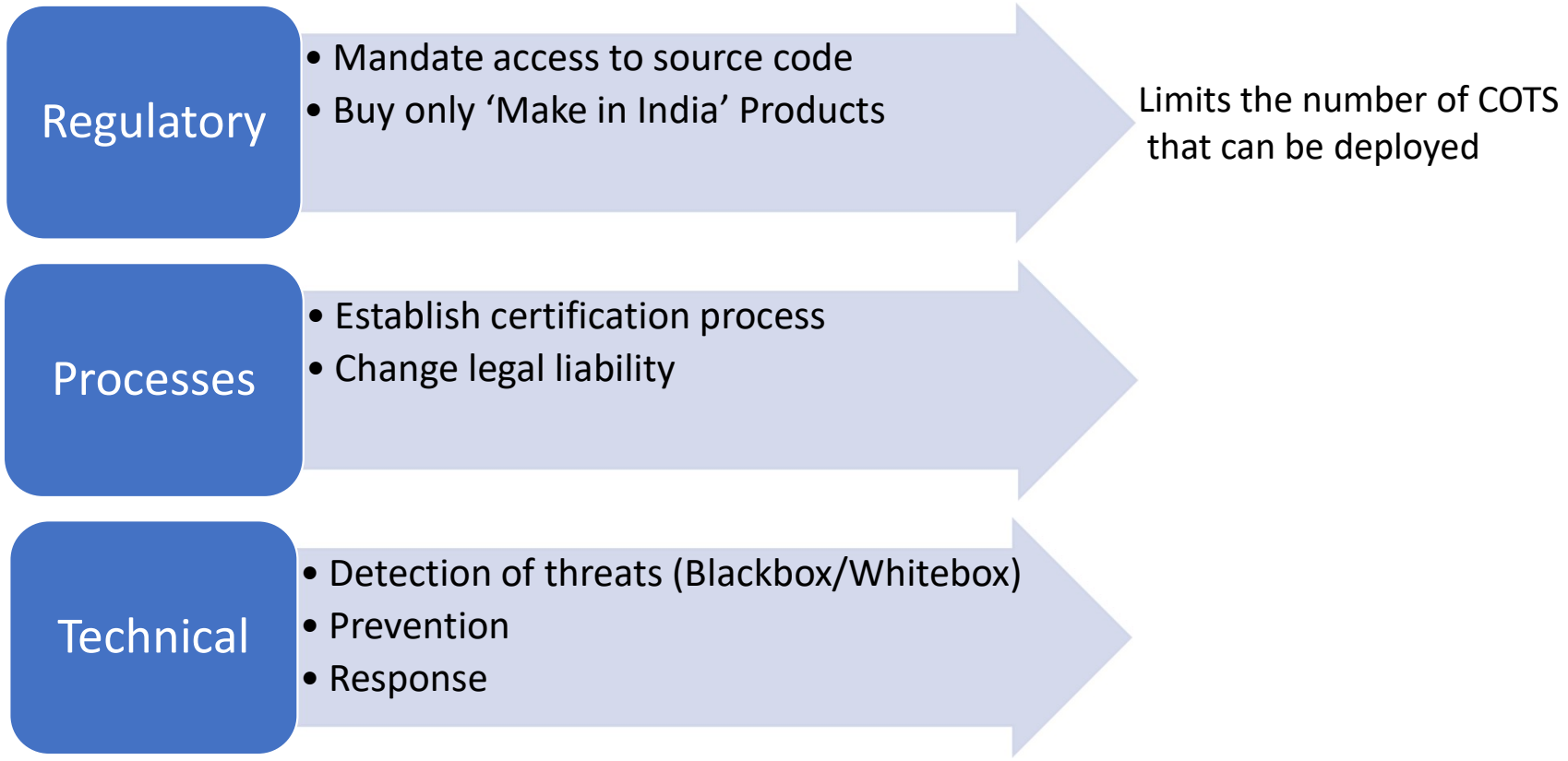
Malicious Activities

Download and install firmware. Display Ads and send spam. Communicate with C&C server etc.

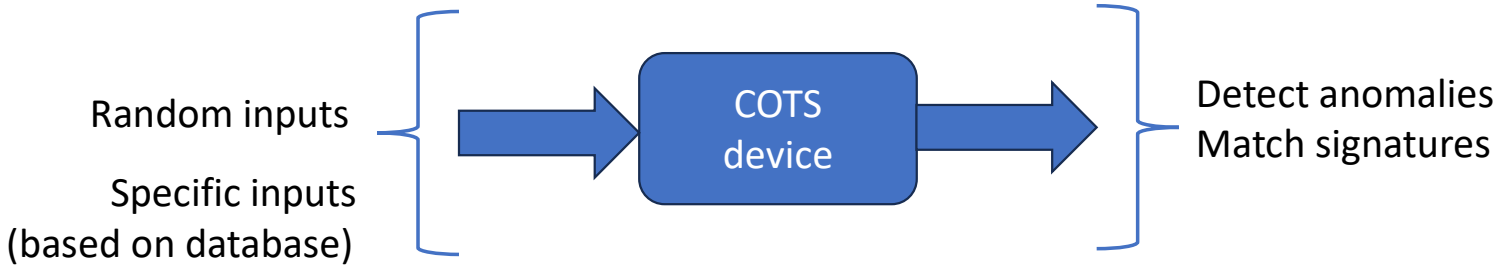
Detection Difficult

Triada part of firmware, therefore cannot be easily detected.

Addressing Security Threats in Software

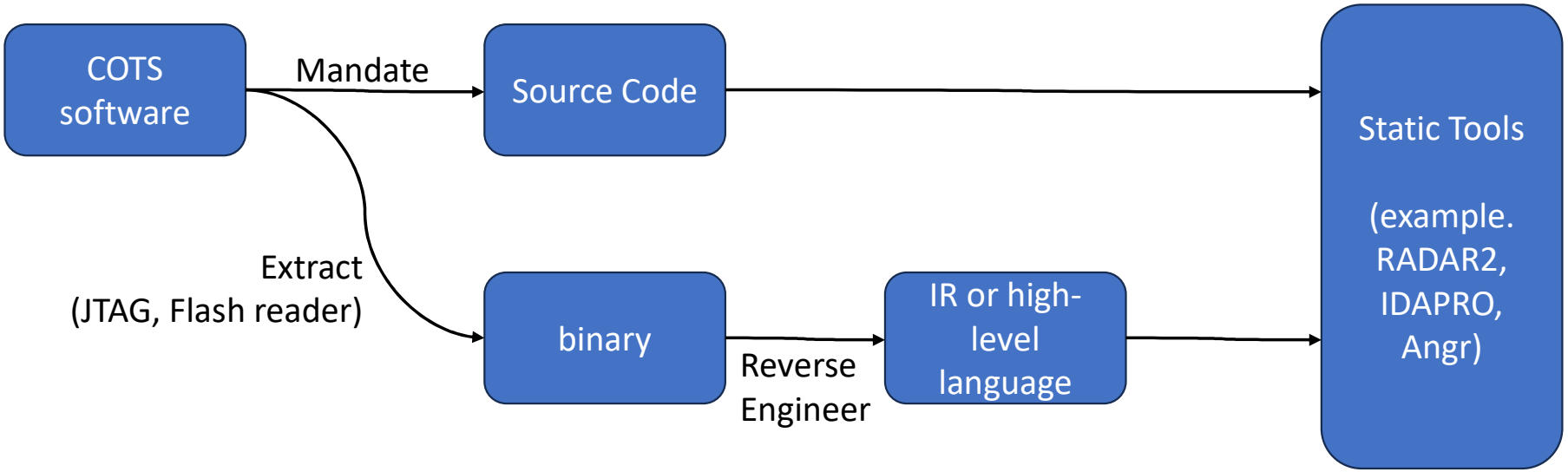


Blackbox detection of threats in software



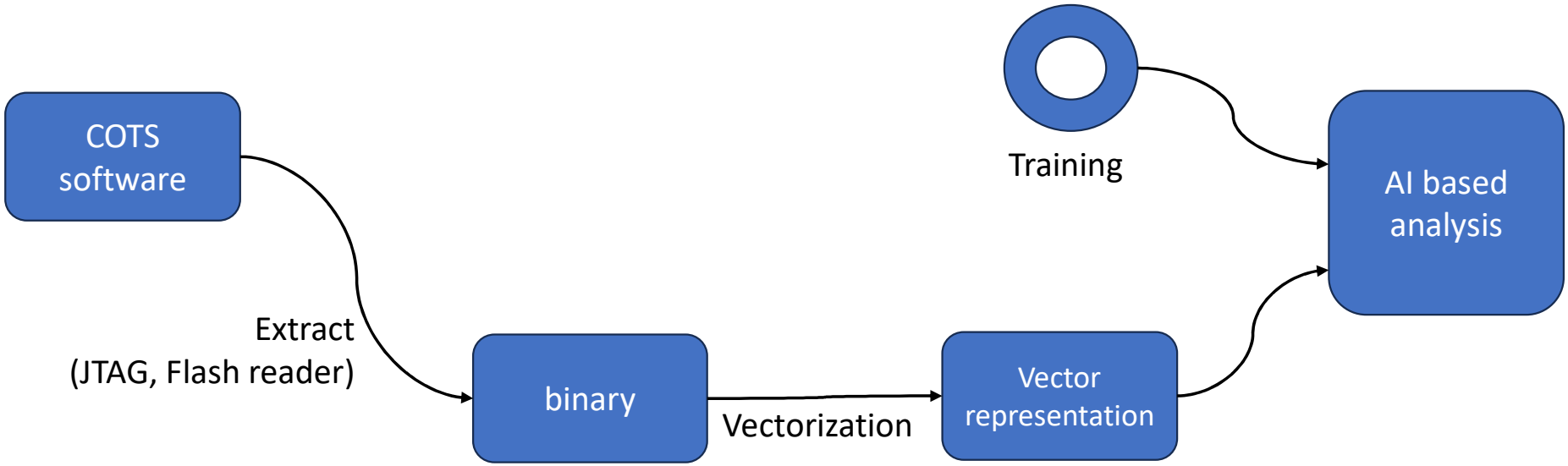
- Blackbox Vulnerability Assessment and Pen-testing
- Mostly limited to finding known vulnerabilities
  - Unlikely to find zero-days, intentional backdoors

Whitebox detection of threats in software



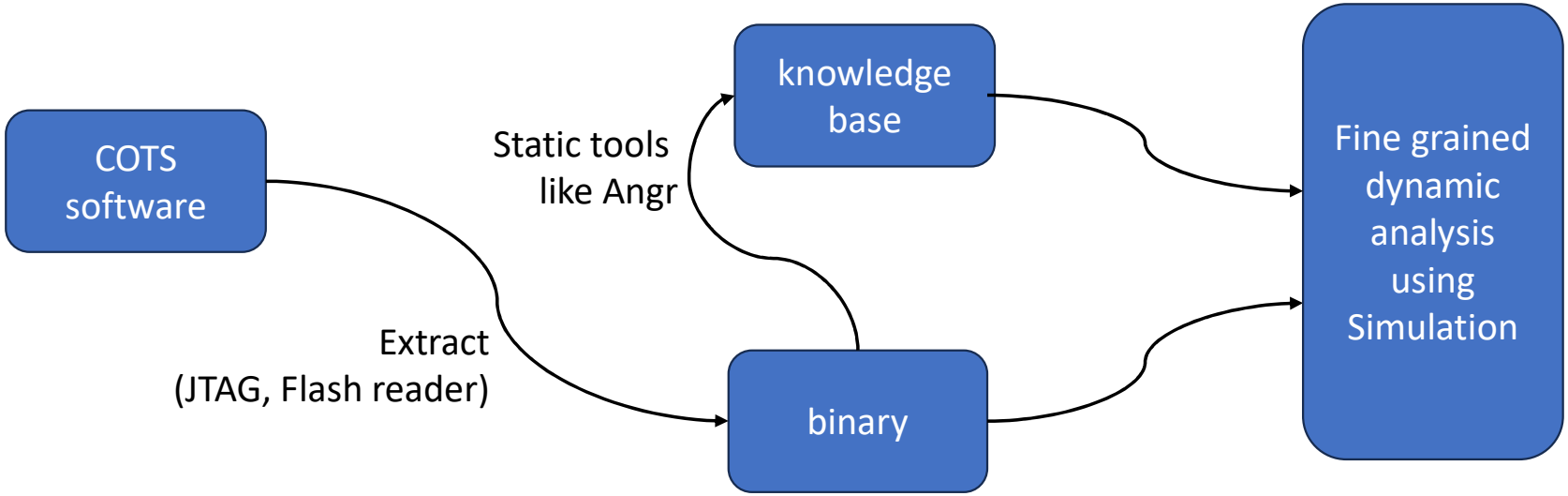
- Combined with techniques such as Symbolic execution and Fuzz testing, can provide much stronger assessment
- Can possibly detect zero-days, backdoors, trojans, etc. based on templates

AI based security assessment
(IITM Ongoing research)



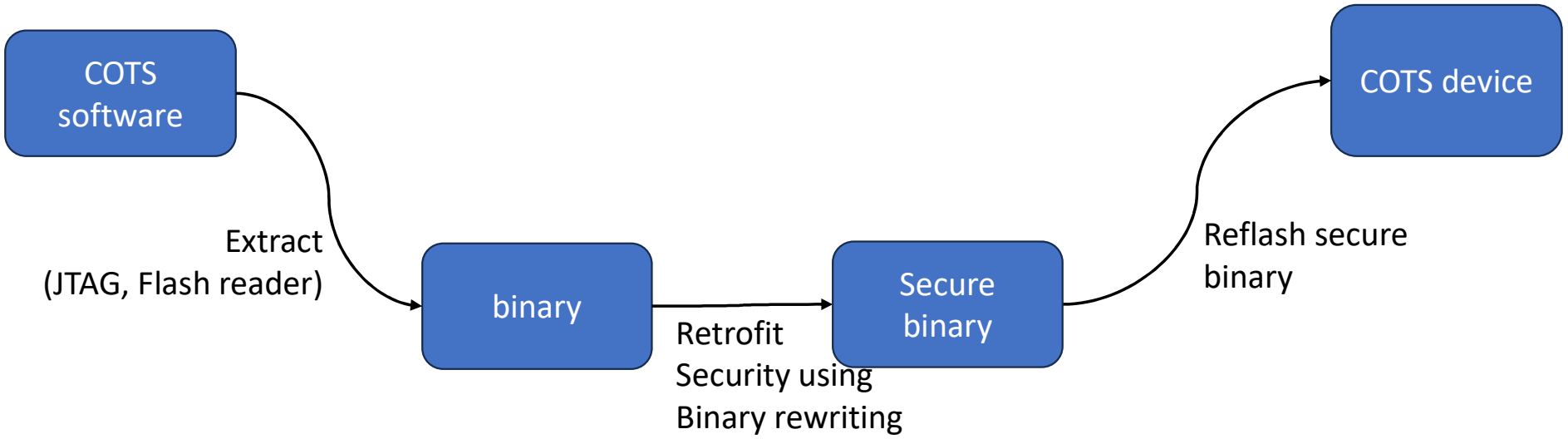
- AI promises to discover difficult vulnerabilities
- AI's full capability is yet to be unleashed

Security assessment using emulation
(IITM Ongoing research)



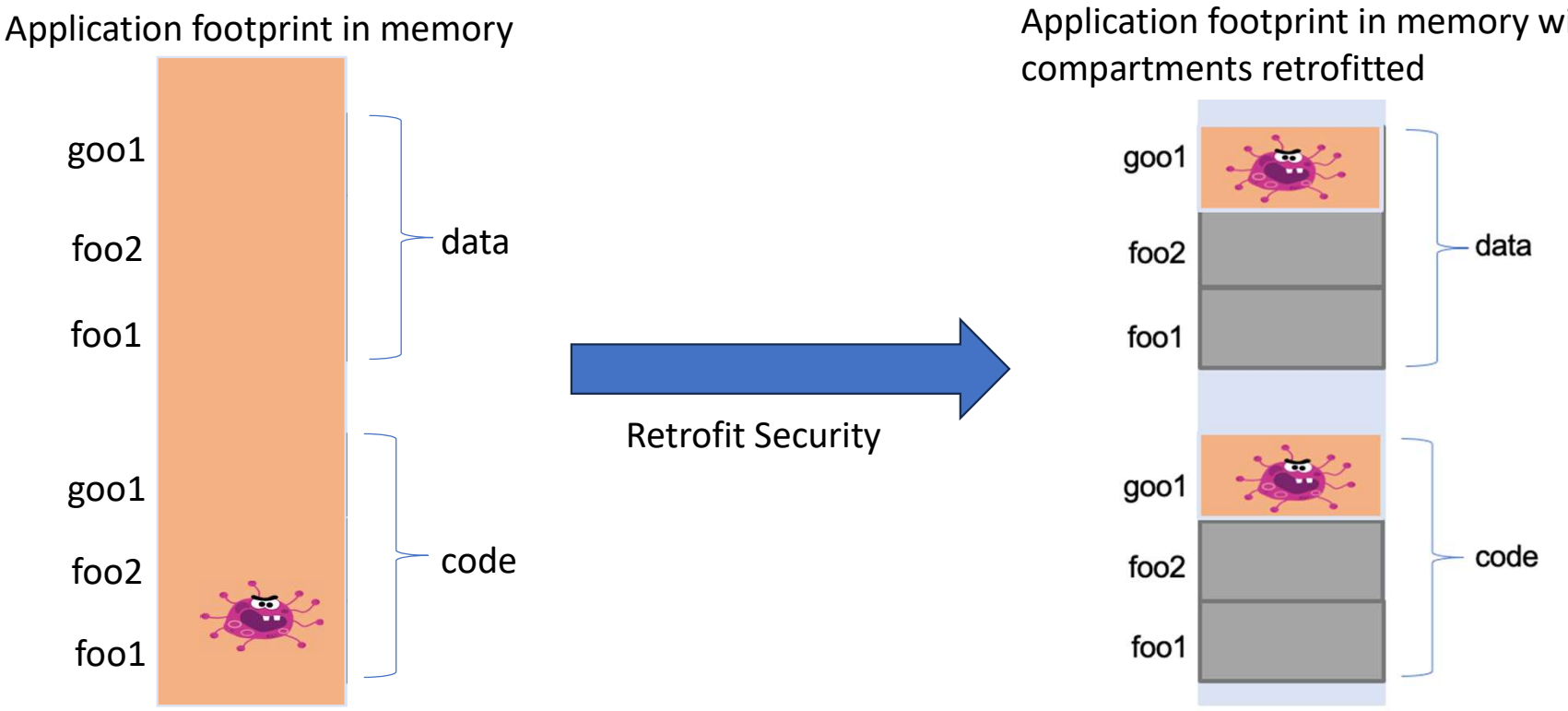
- Fine grained analysis by emulating the COTS hardware

Protection by retrofitting security into the device
(IITM Ongoing research)



- Fine grained analysis by emulating the COTS hardware

Retrofitting security in existing binaries

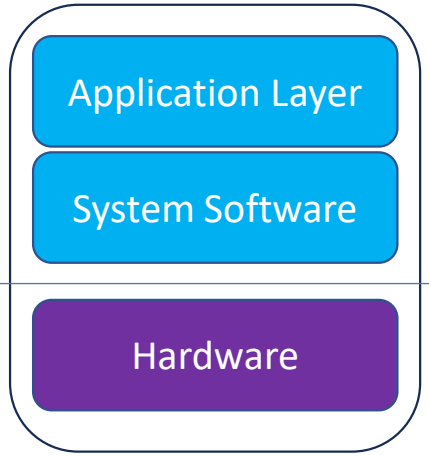


Security threats from COTS devices

S O F T W A R E

Accidental

Deliberate

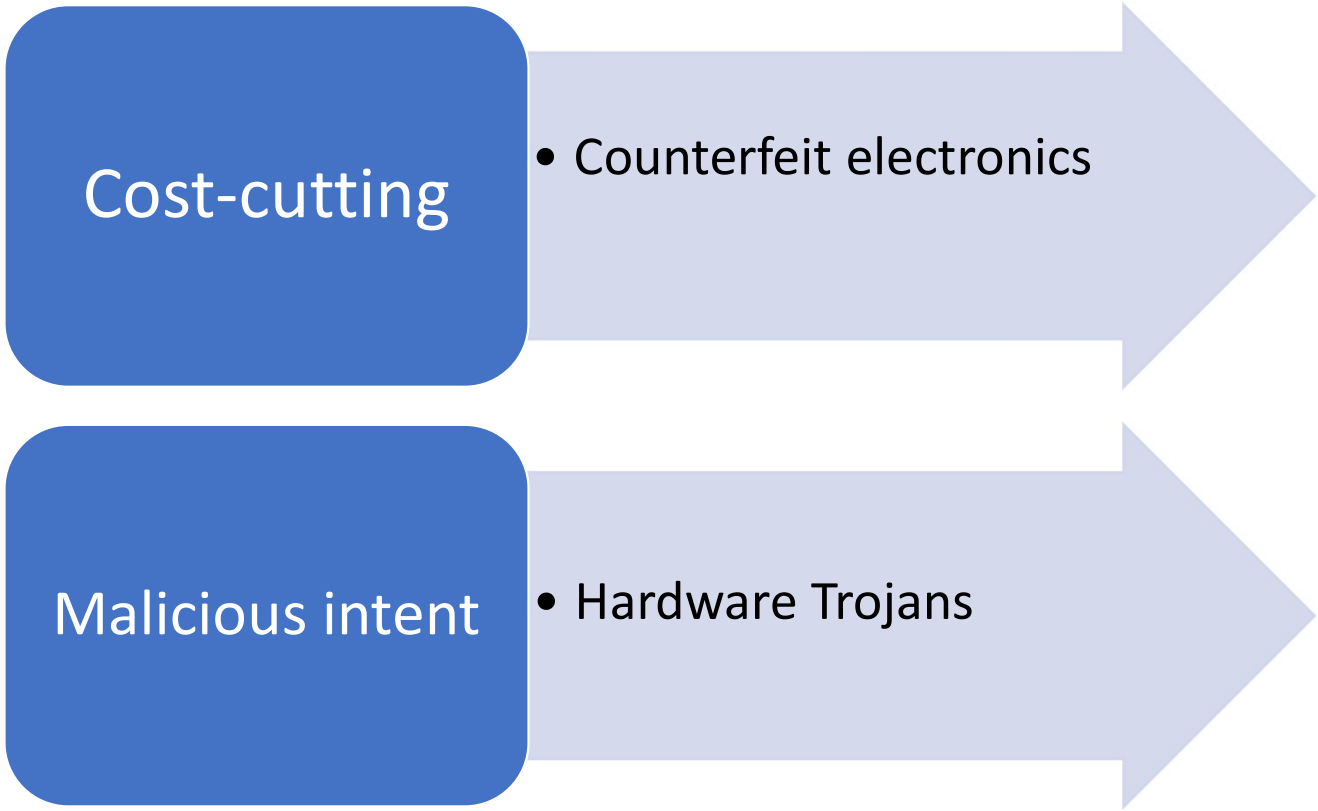


Accidental

Deliberate

H A R D W A R E

Deliberate Hardware Threats

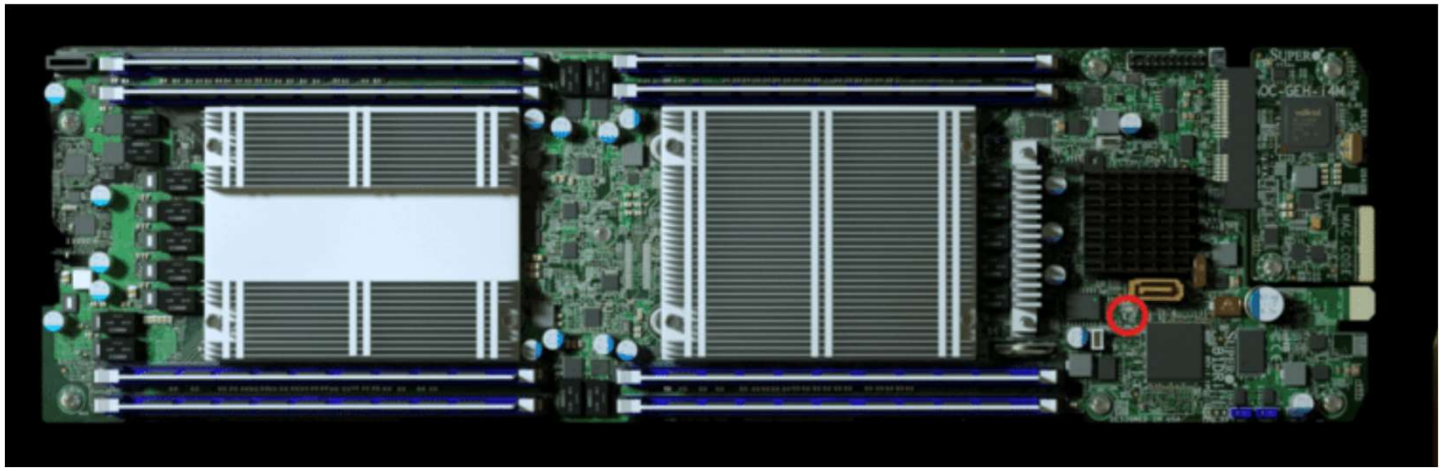


Hardware Trojans

Businessweek | Feature

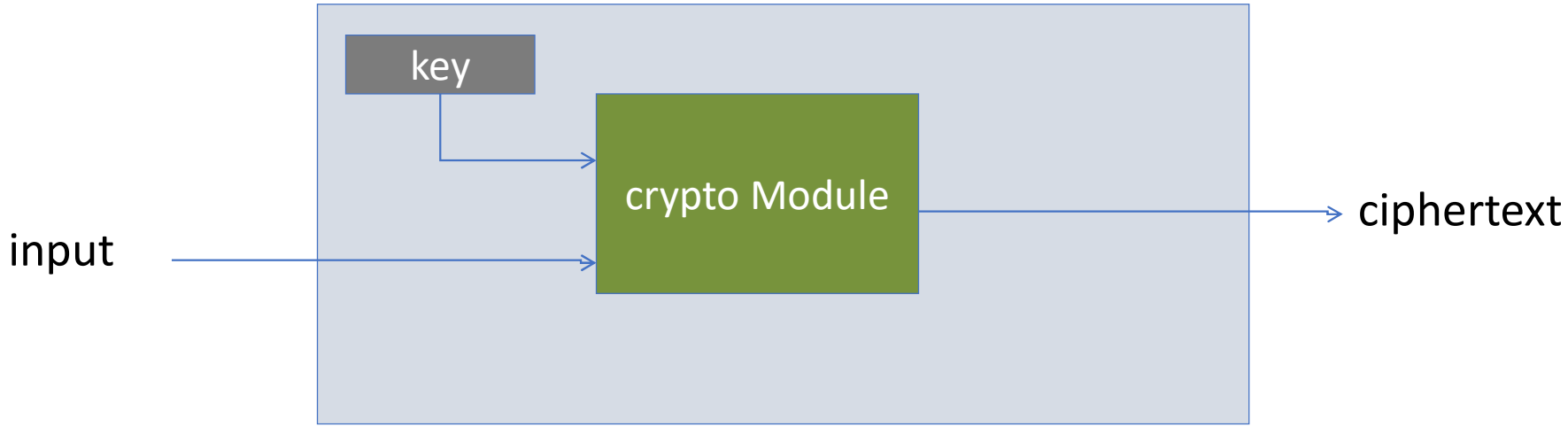
The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

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.



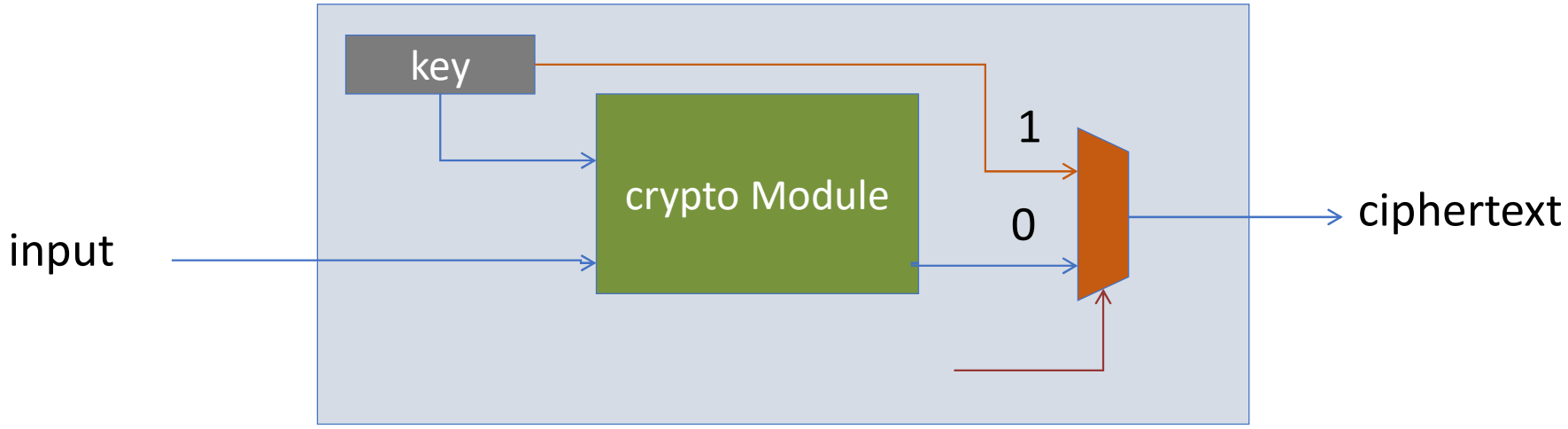
Hardware Trojan Example

- Malicious and deliberately stealthy modification made to an electronic device such as an IC
- It can change the chips functionality thereby undermine trust in systems that use this IC



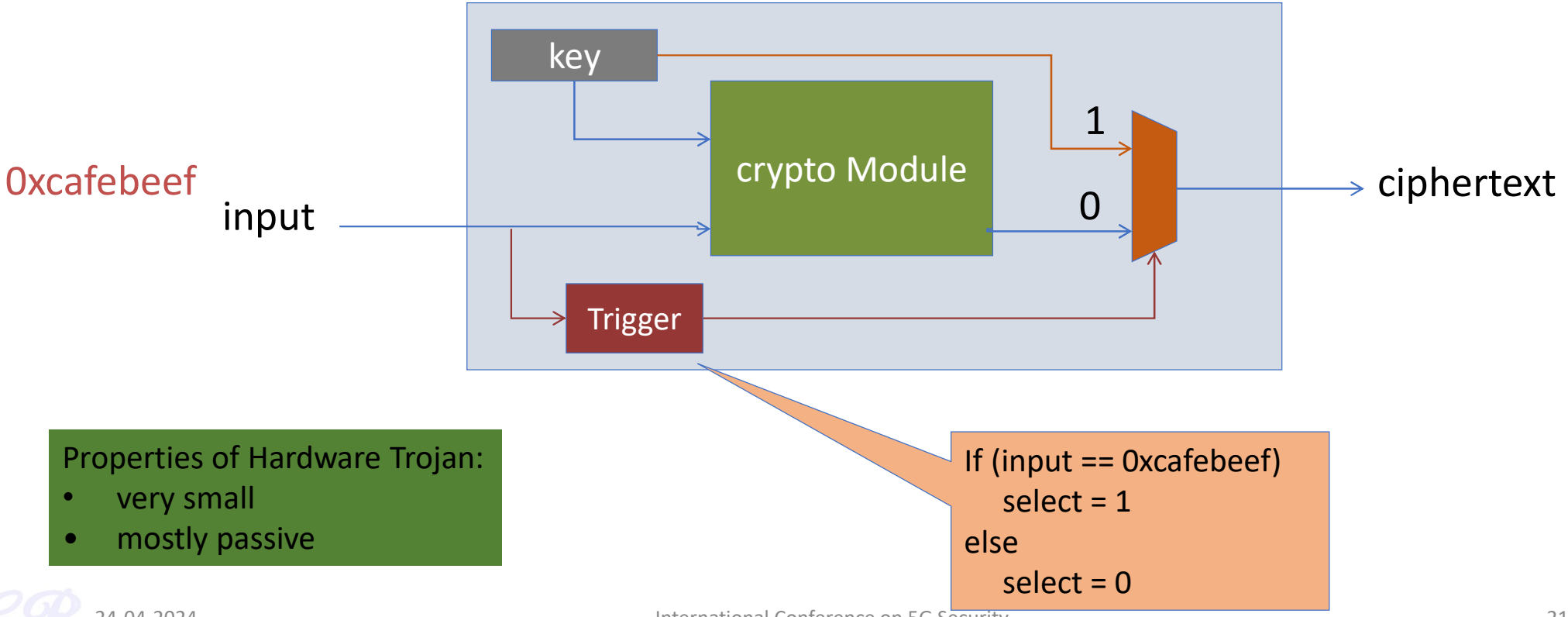
Hardware Trojan Example

- Malicious and deliberately stealthy modification made to an electronic device such as an IC
- It can change the chips functionality thereby undermine trust in systems that use this IC



Hardware Trojan Example

Cheat Code (combinational trojans)

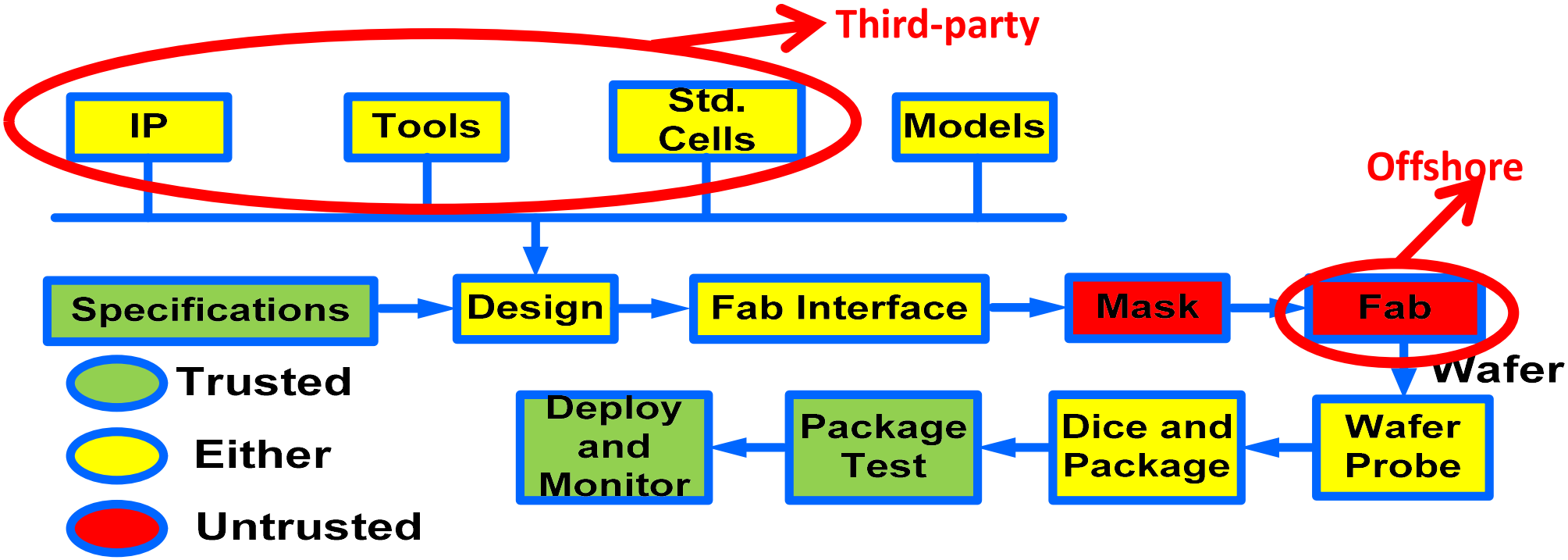


Properties of Hardware Trojan:

- very small
- mostly passive

IC Life Cycle (Vulnerable Steps)

Properties of Hardware Trojan:
* very small
- mostly passive
- Can be added at multiple stages



*http://www.darpa.mil/MTO/solicitations/baa07-24/index.html

Counterfeit Electronics

Save-costs but Results in low-quality devices

1- Low Specification Components Are Disguised as High Specification Component
2- Defective Parts
3- Used Parts sold as New

Counterfeit Electronics

Save-costs but Results in low-quality devices

1- Low Specification Components Are Disguised as High Specification Component
2- Defective Parts
3- Used Parts sold as New

as a result. The fake semiconductor industry alone represents a $75B risk, with fake electronics accounting for an additional $169 billion. In 2013 alone, the U.S. government seized $145 million worth of fake electronics

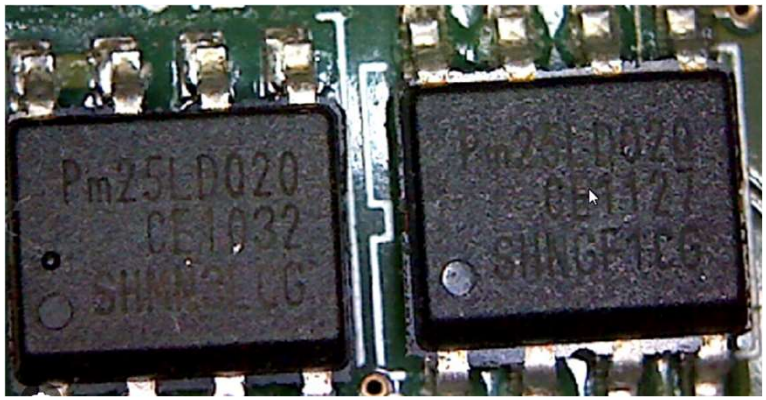
Counterfeit electronics growing at a rate of 30%

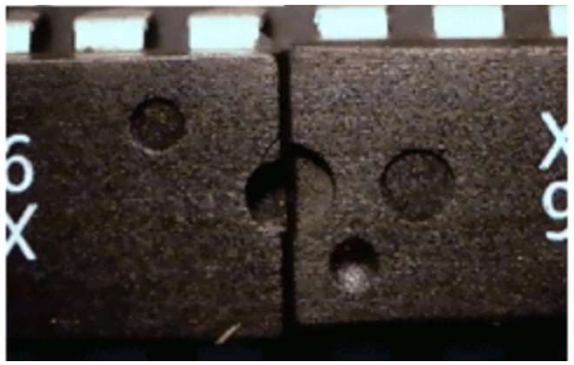
Made worse with the semiconductor shortage

SiliconExpert, The Growth of Counterfeit Electronics: What You Can Do to Protect Yourself

Detection of Counterfeit Components in COTS

- Visual
  - Font and spelling on labels
  - Part number mismatch
  - Logo
  - Examine indents



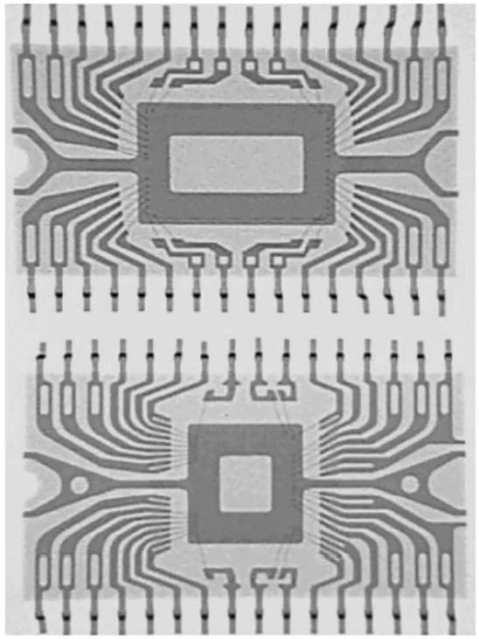


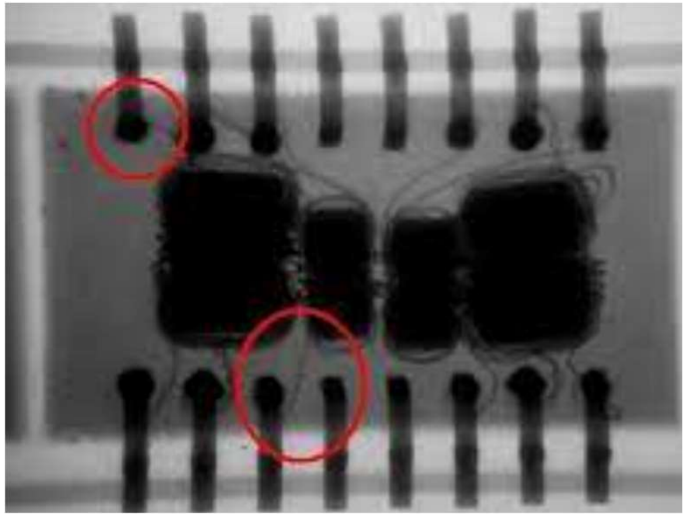
https://www.raypcb.com/farewell-to-counterfeit-electronic-components/

Art Ogg. USING X-RAY SYSTEMS TO DETECT COUNTERFEIT AND REWORKED ELECTRONIC COMPONENTS, 2021

Detection of Counterfeit Components in COTS

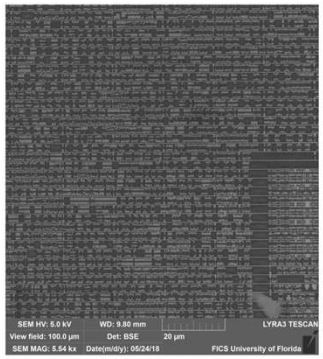
- Visual – X Ray images





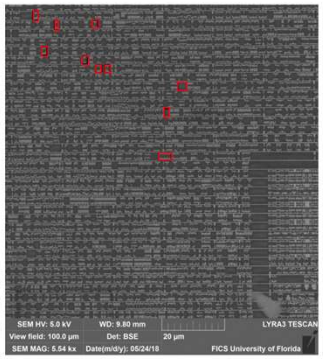
https://www.raypcb.com/farewell-to-counterfeit-electronic-components/

Detection of hardware trojans – SEM Imaging



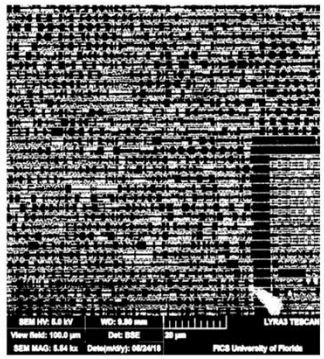
(a)

Golden IC image



(b)

IC image from DUT

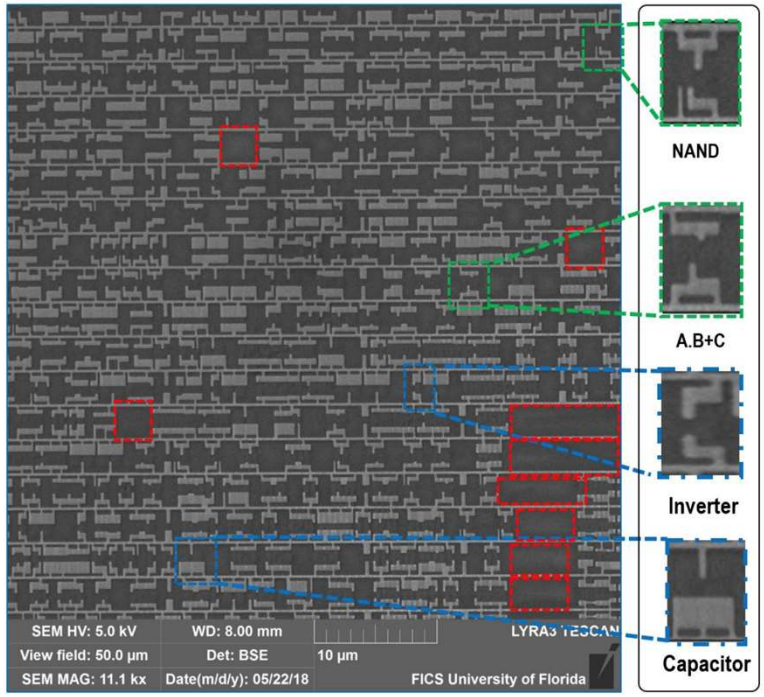


(c)

Enhanced image

(d)

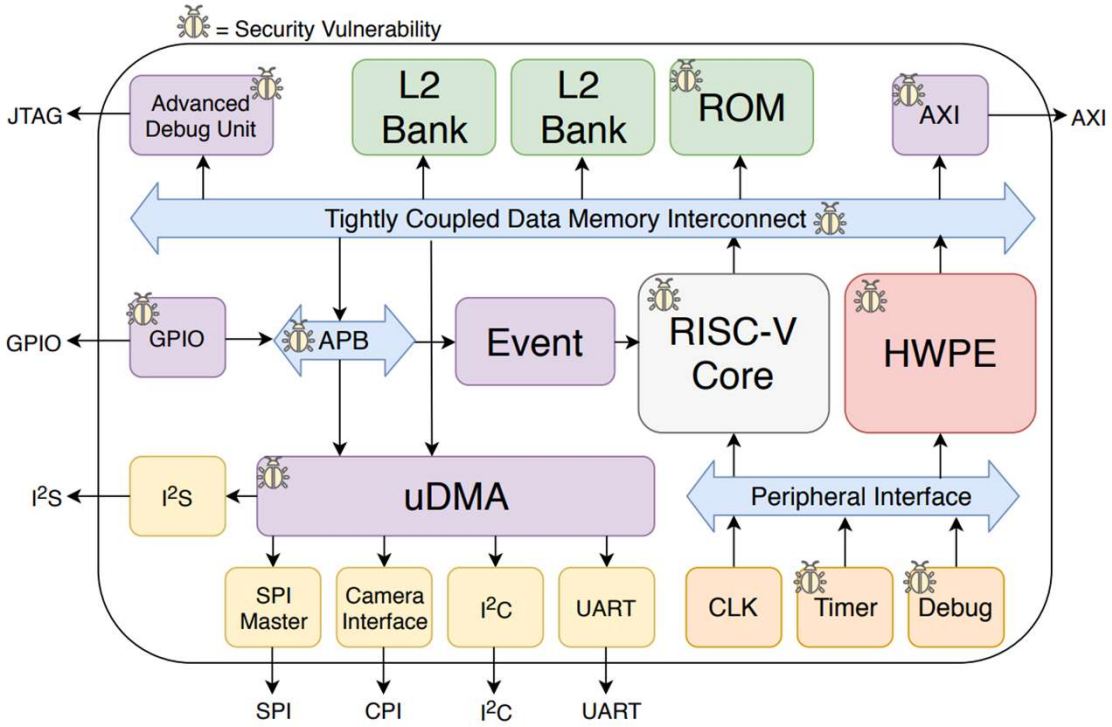
Suspected Trojan regions



SIM card doping level footprint

Nidish Vashistha et al. Detecting Hardware Trojans Inserted by Untrusted Foundry using Physical Inspection and Advanced Image Processing, 2018

Threats in Hardware introduced accidentally



#	Bug
1	Address range overlap between peripherals SPI Master and SoC
2	Addresses for L2 memory is out of the specified range.
3	Processor assigns privilege level of execution incorrectly from CSR.
4	Register that controls GPIO lock can be written to with software.
5	Reset clears the GPIO lock control register.
6	Incorrect address range for APB allows memory aliasing.
7	AXI address decoder ignores errors.
8	Address range overlap between GPIO, SPI, and SoC control peripherals.
9	Incorrect password checking logic in debug unit.
10	Advanced debug unit only checks 31 of the 32 bits of the password.
11	Able to access debug register when in halt mode.
12	Password check for the debug unit does not reset after successful check.
13	Faulty decoder state machine logic in RISC-V core results in a hang.
14	Incomplete case statement in ALU can cause unpredictable behavior.
15	Faulty logic in the RTC causing inaccurate time calculation for security-critical flows, e.g., DRM.
16	Reset for the advanced debug unit not operational.

HardFails: Insights into Software-Exploitable Hardware Bugs, USENIX Security 2019.

Hardware Vulnerability in Practice

Don’t panic! “Unpatchable” Mac vulnerability discovered

Posted: June 14, 2022 by Pieter Arntz

PACMAN: Can be exploited to inject malicious code in Apple’s M1 processor

Unfortunately, very little is available to automatically cater to these hardware vulnerabilities!

Conclusions

- COTS in critical system should be validated both from software as well as hardware
- There are efforts in evaluating security of firmware
  - Specifically, the focus should be develop indigenous tools
  - These tools should be kept undisclosed – a secret weapon
- Setup centers / research of hardware evaluation for detection of trojans and counterfeit electronics in devices
- Research that focuses on detecting hardware based vulnerabilities

T H A N K Y O U ! ! !