UNSW SYDNEY

Hardware Security
Week 1 - Introduction

26T1

Hammond Pearce

Slide material acknowledgements to
Ramesh Karri, Benjamin Tan,
JV Rajendran, Jason Blocklove
Christian Pilato, Luca Collini

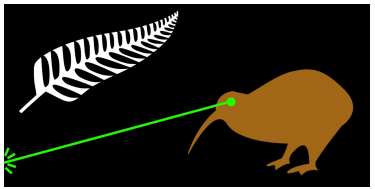
Part 1: Logistics

$ whoami \\ hammond pearce (instructor)

2023 - Present
Senior Lecturer - UNSW
School of Computer Science and Engineering

2020 - 2023
Research Assistant Professor - NYU Tandon
Department of ECE / Center for Cybersecurity

2016-2020
Ph.D., Professional Teaching Fellow - UoA
Department of ECE (Now ECSE)



Course organisation

- Email me: hammond.pearce@unsw.edu.au
- Course forums/grades on Moodle
- Course resources on https://cgi.cse.unsw.edu.au/~cs6420/
- Recordings with Echo360
- Class: 9-11am Tuesdays (that's now!)
  - >=50% attendance requirement
- Labs: 11-1pm, 1-3pm, 3-5pm Tuesdays
- Office hours: TBD, possibly as needed

Questions to me/tutors

- Talk to your tutor if in lab
- Talk to me if in lecture
- Outside of lecture / lab:
  - Post questions to Discourse in first instance
  - Give a few hours to get a response
  - If no response, you can message me / your tutor to check the question

Course grading

- 50% - Labs
  - 5, worth 10% each
    - First 2 marks generally easy, next 6 generally moderate, last 2 generally difficult
- 20% - Reports
  - 3, worth 5%, 8%, and 7%
- 30% - Hardware CTF
  - 15% practical, 15% report
  - **! HURDLE !** - must score >= 50% in CTF to pass course

Your Tutors

Liam Murphy

Favourite Color: Green

Deprived of: Dogs

Lucas Harvey

Favourite Color: #3A76F8

My dog's age: between 6 and 7

Jennifer King

Favourite Color: Purple

Dog's name: Jackie

Siyu "Annie" Qiu

Favourite Color: Purple

Albanese's dog is called Toto

Tandi Guo

Favourite Color: Blue

I got that dog in me

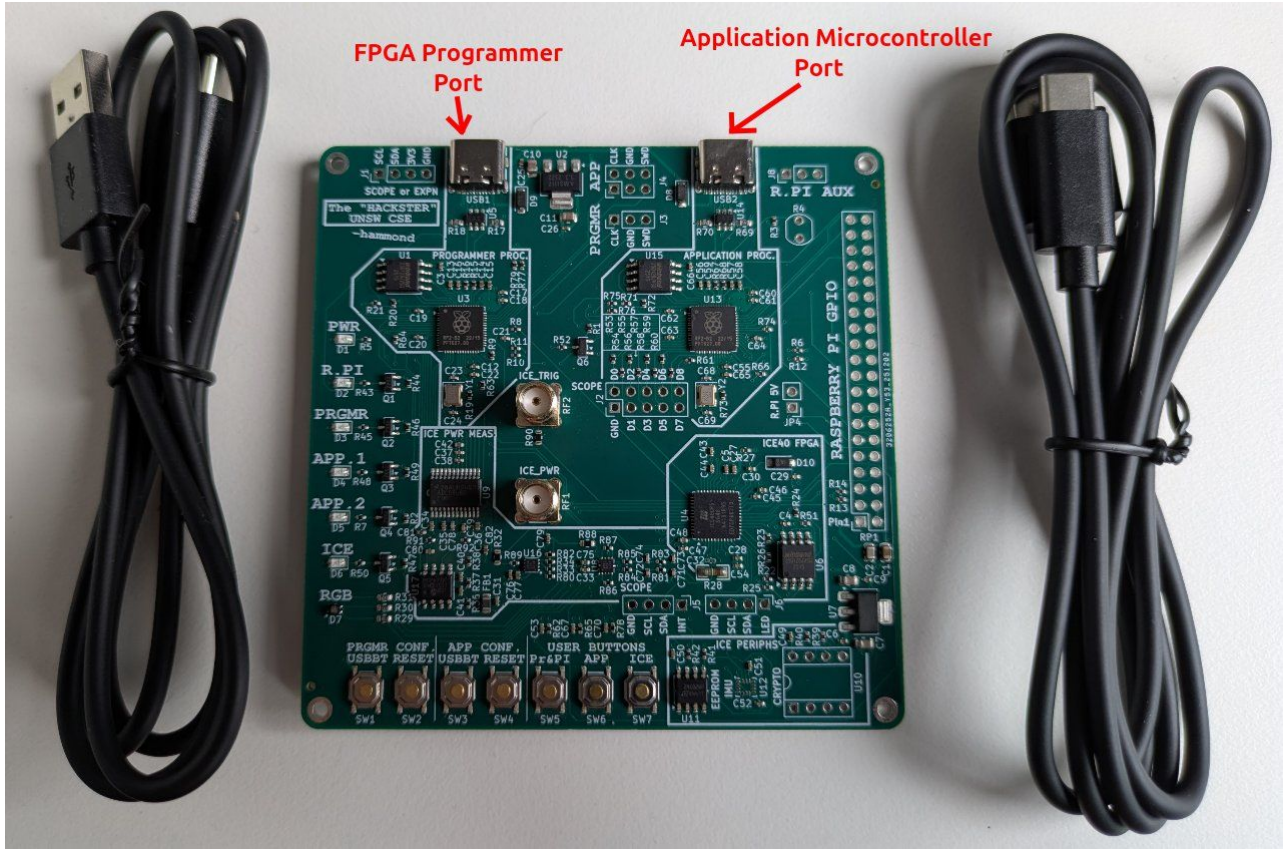
Labs

- Typically you'll submit some mix of code and documentation
- Typically due 5pm Friday the week after release
- E.g. Lab 1 - Scan Chain Analysis,
  - released Tuesday Week 3,
  - due Friday Week 4
- AI policy:
  - If you find AI is actually useful for anything let me know, we'll write a paper together

Labs (part 2)

- You will write code in Verilog HDL
  - VHDL is not well-supported in the open-source Yosys/icestorm
  - Fortunately, Verilog an easy language to learn
  - Line for line equivalent with VHDL
  - You'll see me write it a bunch
- You will also write code in MicroPython
  - MicroPython is fun and easy(ier than C)!
  - Performance, of course, is horrible
  - But we're not trying to out-perform anyone with our MicroPython

Lab hardware



Lab 0

- Actual course hardware on a boat/plane/somewhere (not here!)
- Last year’s hardware available for now
- We’ll swap it out when the new hardware gets here
- The new hardware becomes relevant for Lab 2 (power analysis)

Reports

- Typically you'll submit writing and/or a video
- Assess knowledge of course content
- Typically due 5pm Friday the week after release
- Watch those deadlines!
    - First report due Friday Week 2, second report Friday Week 3

Hardware CTF

- Assessed **in-person**
- **Timed challenge** allowing **multiple attempts**
- **In-lab in-person assessment**: in weeks 8, 9, and 10
- May rely on knowledge from any lecture.
- Report (Write-up) due week 11.
- Assessment: 15%, Report: 15%
- **Hurdle**: You must get >= 50% to pass the course.
- Attendance requirement: If <= 50%, CTF result may be denied

AI and academic conduct policy

- This is an individually assessed course
  - Collaboration is welcomed but cheating is not
- AI:
  - As of this moment in time, AI won't be that helpful for the technical challenges in this course
  - When writing documents, **simple** AI assistance is acceptable (e.g. grammarly).
  - AI isn't *that* good at writing and I usually dislike what it produces
  - Sometimes AI use can't be proven but bad work always can be
  - Turnitin may be used on some of the submitted writing

This is the second offering of this course

- New hardware (improved power measurement circuit)
- Changes to assessment
  - Old Report 3 -> New Lab 3
  - Old Lab 3 -> New CTF
- The course is still a work in progress!
- Please be patient if some things aren’t 100%!
  - But do let us know if something isn’t working!

That’s it - questions?

Part 2: The actual introduction now

How do we secure computer systems?

Find/fix all the (exploitable) bugs!

Availability guarantees!

How do we secure computer systems?

Ensure information privacy!

Access control!

Find/fix all the (exploitable) bugs!

Availability guarantees!

How do we do all these things?

Ensure information privacy!

Access control!

Software security: Tools and techniques

- Security scanners and bug-finding for software
  - e.g. SAST
  - Check for common bugs, CWE top 25, OWASP top 10…
- Penetration testing and security audits
- Best-practice development
- Employee competence
- For third party libraries: Supplier reputation

Software security: Tools and techniques

- Security scanners and bug-finding for software
  - e.g. SAST
  - Check for common bugs, CWE
- Penetration testing
- Best-pr
- petence
- third party libraries: Supplier reputation

But everything here assumes something!

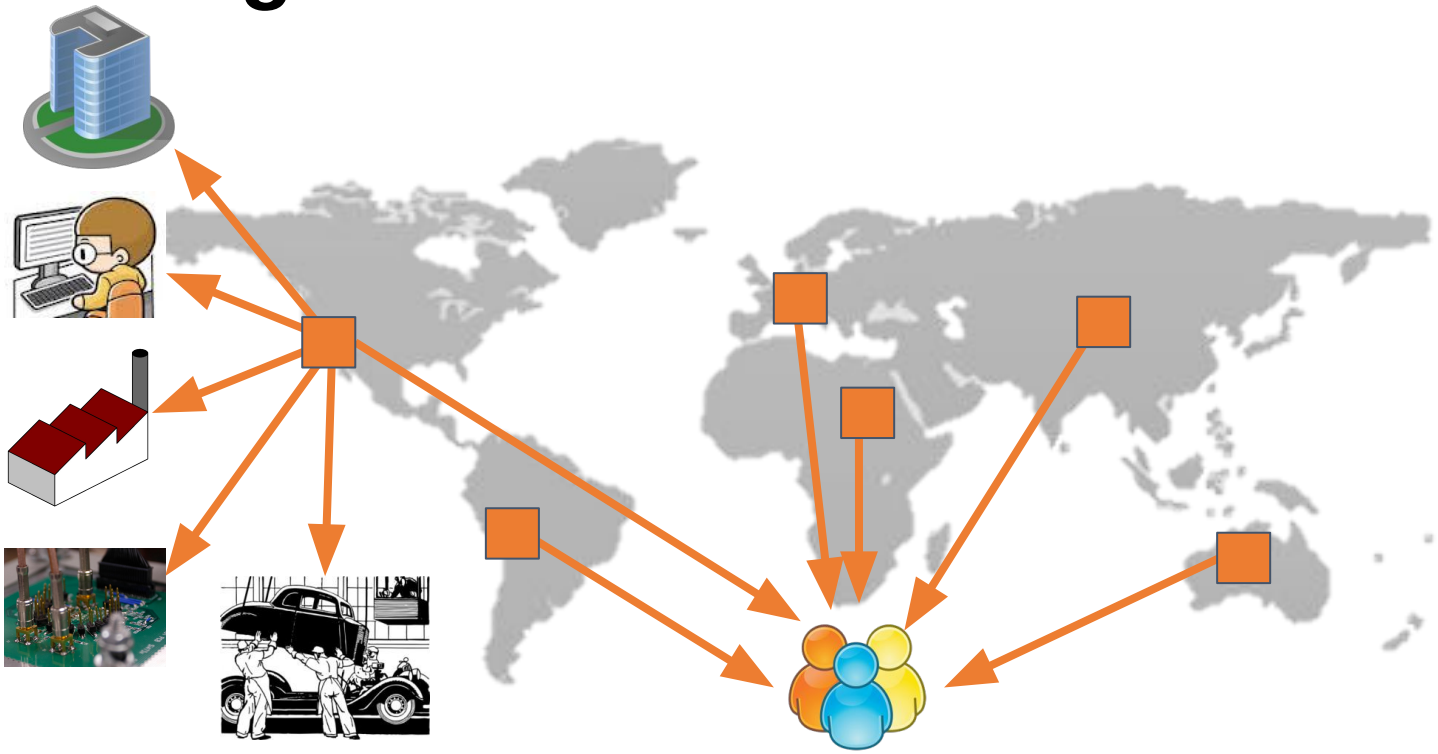
Software security *assumes* trustworthy hardware

Hardware security and trust

- We trust…
  - computer hardware to execute the provided instructions
  - computer hardware to **not execute** instructions we haven't provided
  - computer manufacturers to build the specified circuits
  - computer manufacturers to **not include** circuits we haven't specified
- We believe…
  - Computer hardware is idealized and executes instantly, without:
    - Timing side effects
    - Power side effects
    - Radiation side effects

Can we trust this?

Before globalization

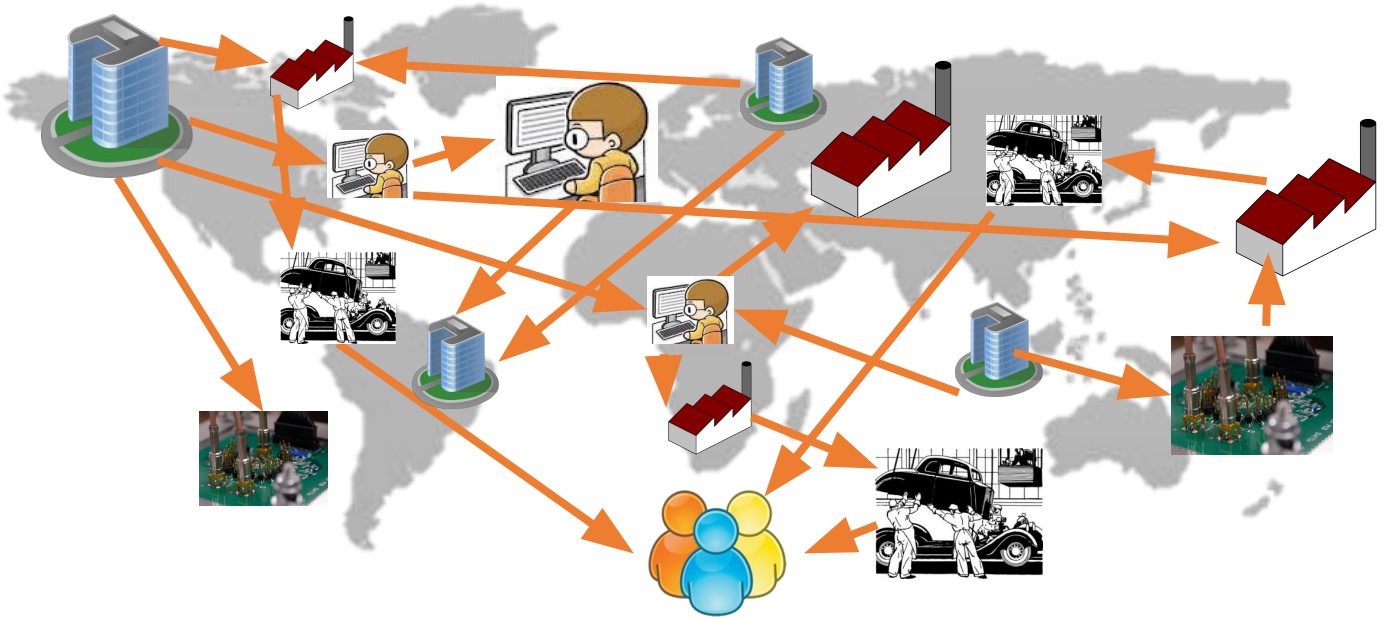


Design, manufacture, test & package, assembly were in-house

Source: Digitimes and The Economist

After globalization (today)

Digitimes, http://www.digitimes.com/news/a20120313RS400.html?chid=2
The Economist http://www.economist.com/blogs/dailychart/2011/08/apple-and-samsungs-symbiotic-relationship



Design, manufacture, test & package can be in many different places by many different third parties

Source: Digitimes and The Economist

How many people do you trust with:

Your laptop?

Your phone?

Your credit card?

But how many people had access to it before you?

How many people had access to its design?

How do we
ensure trustworthy hardware

in an untrustworthy world?

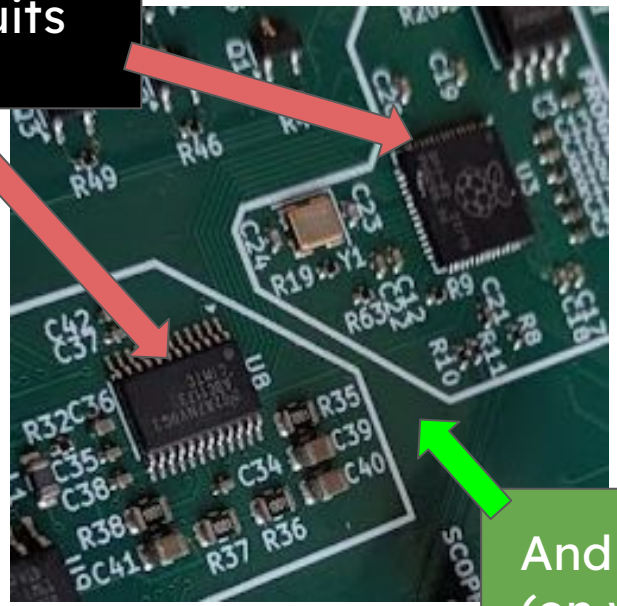
COMP6420 Hardware Security Goals

- Study state-of-the art hardware security methods
  - As well as emerging technologies
- Discuss security as a design metric
  - Not as an afterthought or an add-on
- Examine intellectual property piracy and hardware tampering
  - Attacks and protections
- Examine hardware-based attacks
  - And their countermeasures

So what is hardware anyway?

In this course, hardware is:

Integrated circuits

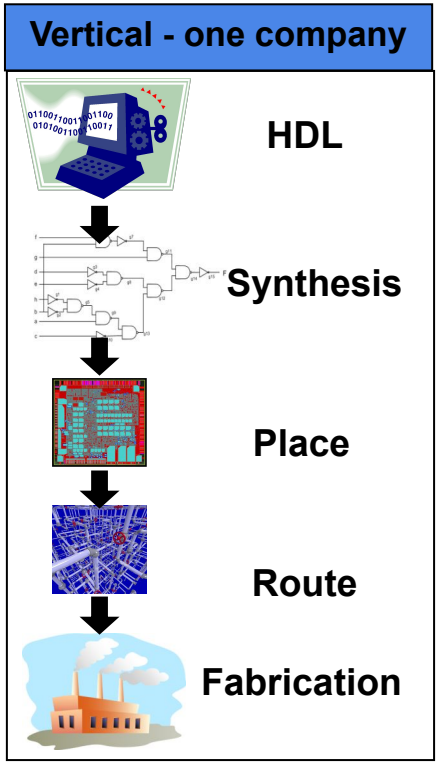


And Printed Circuit Boards
(on which they are placed)

Both can be attacked

Integrated Circuit Production

Once upon a time…

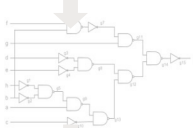


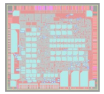
Integrated Circuit Production

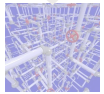
BUT NOW: →

Vertical - one company


HDL

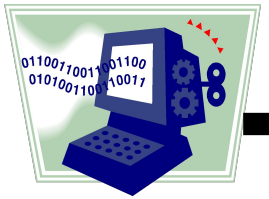

Synthesis

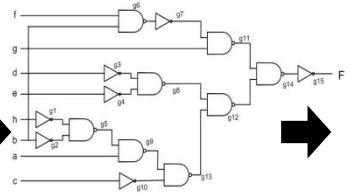

Place

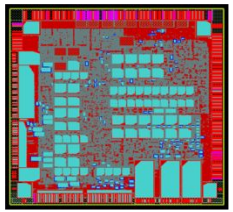

Route

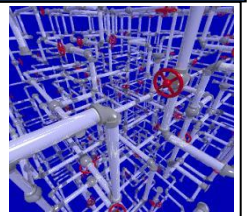

Fabrication

Horizontal (Dominant) – Two or more companies


HDL

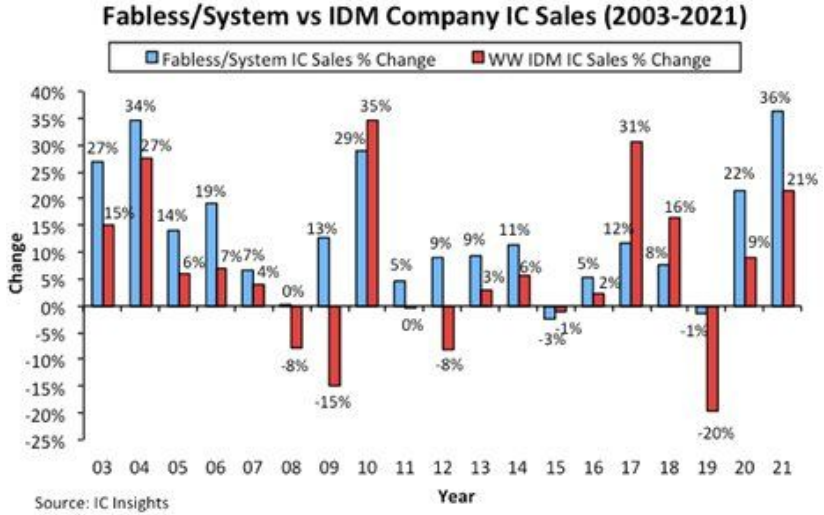

Synthesis

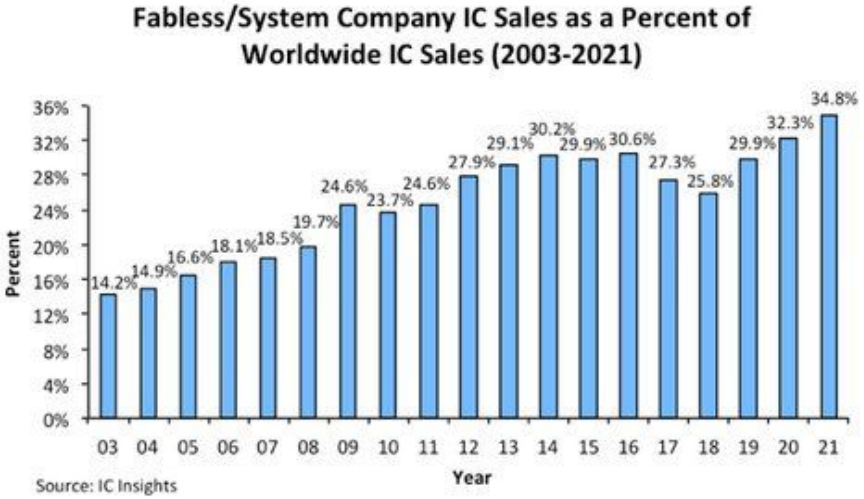

Placement


Routing

Economy of scale: The same fabrication facility serves many fabless companies

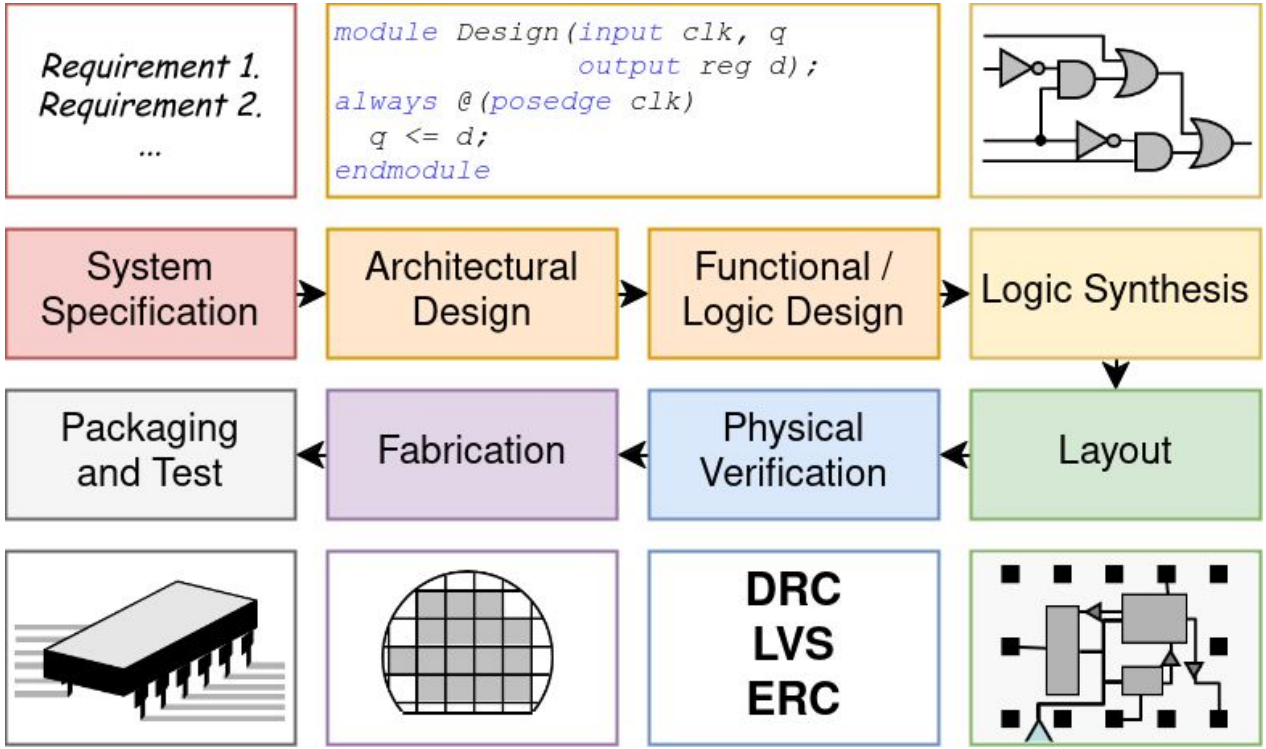
Fabless sales continue to grow



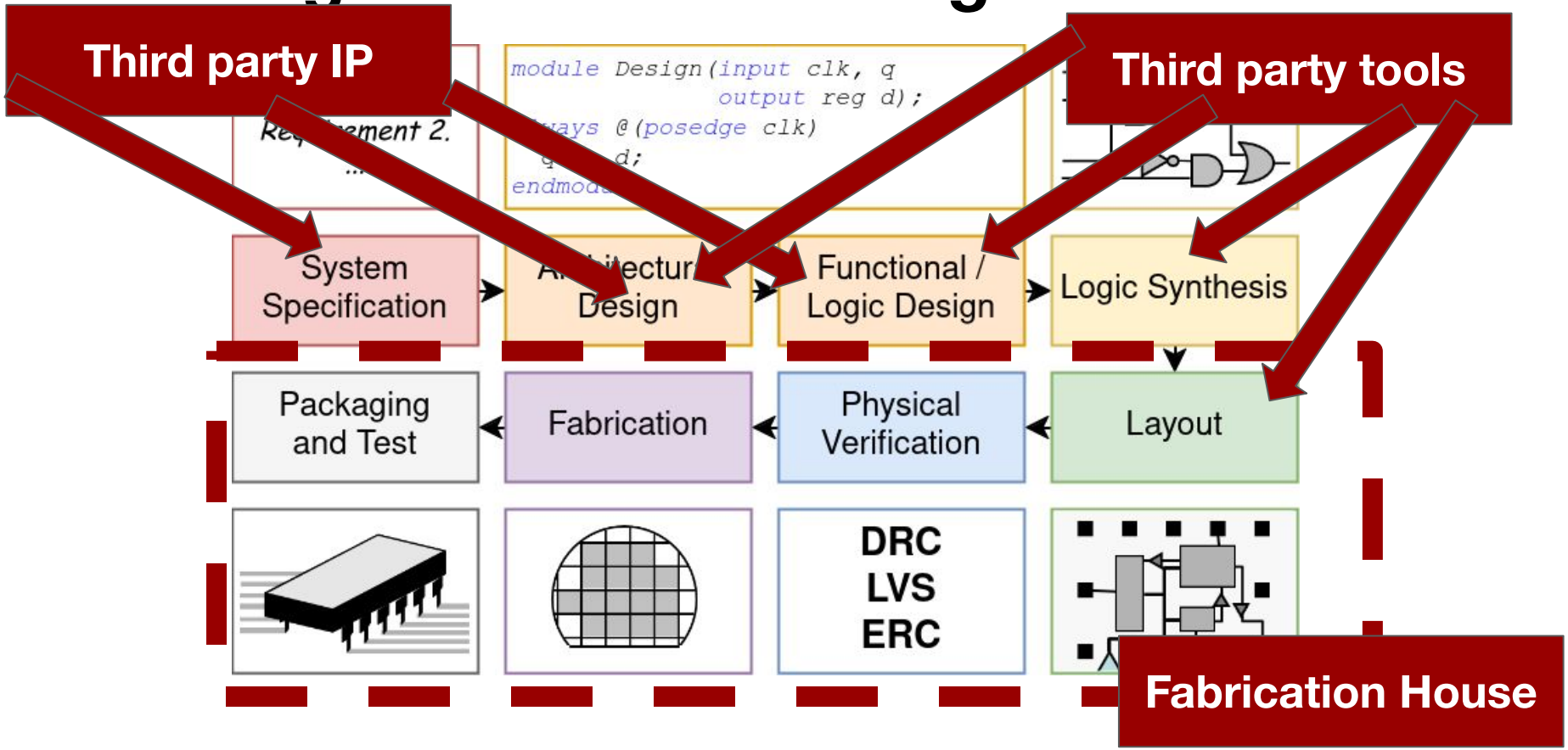


Leading fabless companies (look familiar?)

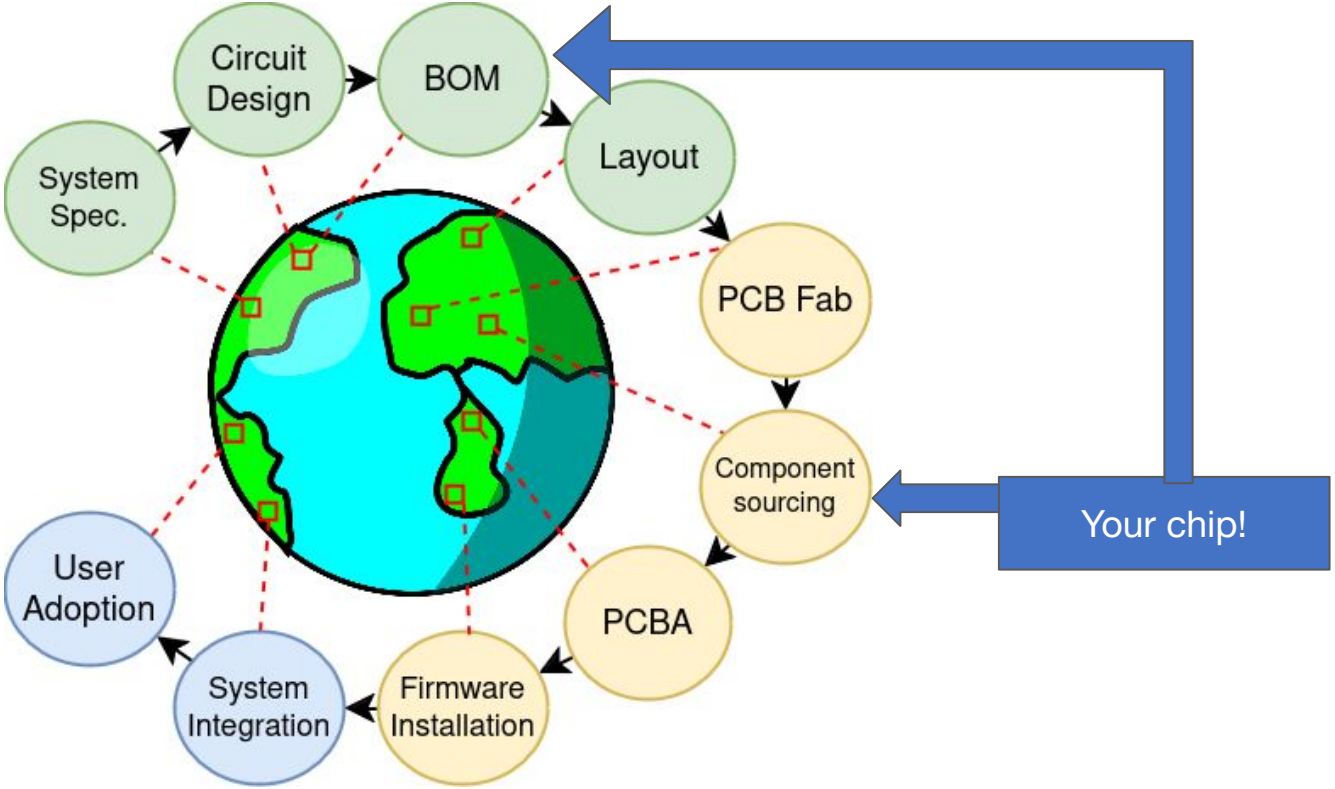
The Integrated Circuit Design Flow



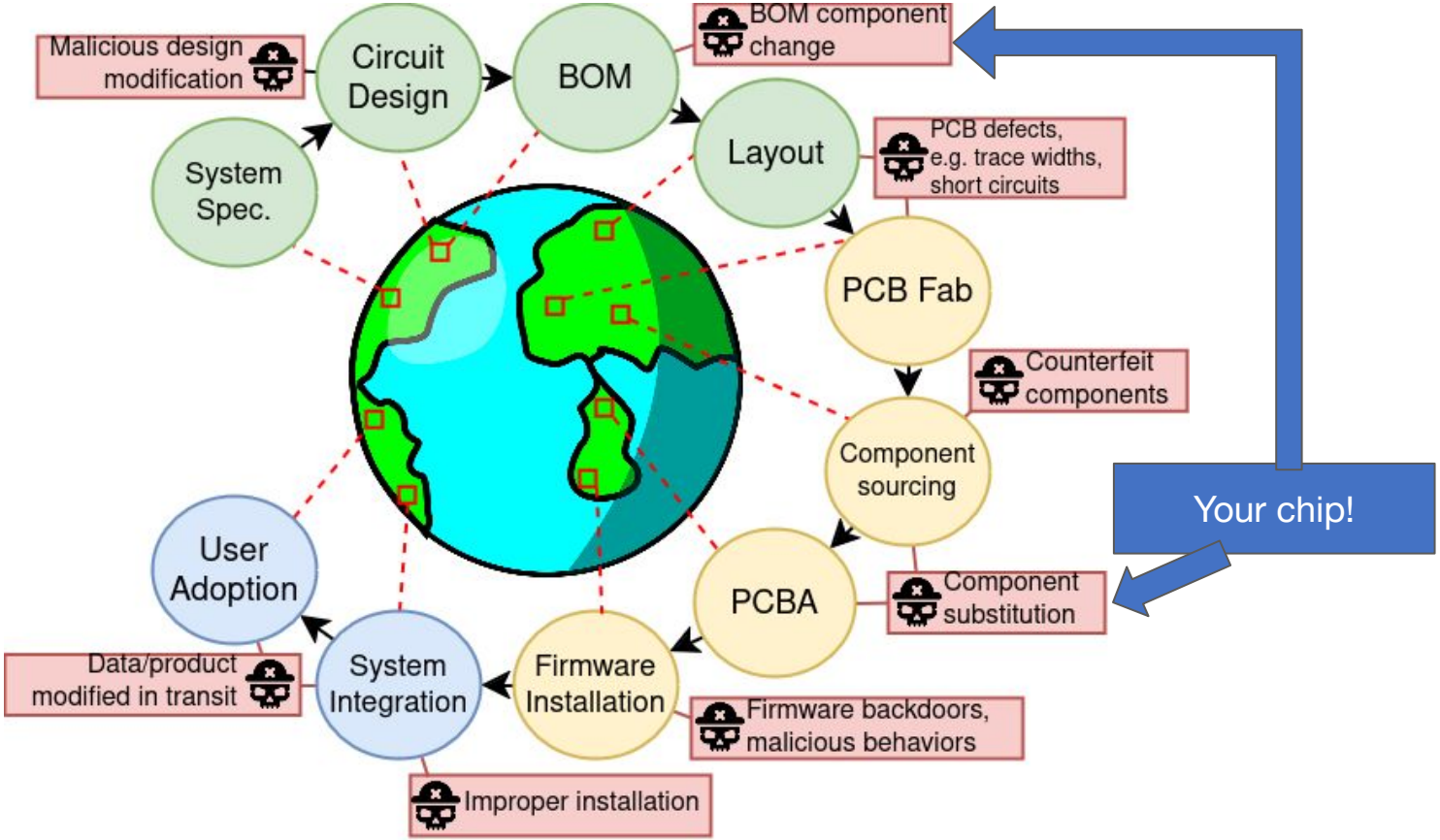
The Integrated Circuit Design Flow



It gets worse: Printed Circuit Boards



It gets worse: Printed Circuit Boards



5 min break

Break activity - talk to your neighbour

"Hi"

"What's your favourite color / spare time activity / dog fact?"

"What's your least favourite programming language and why is it JavaScript?"

"What are some hardware security things you have heard of?"

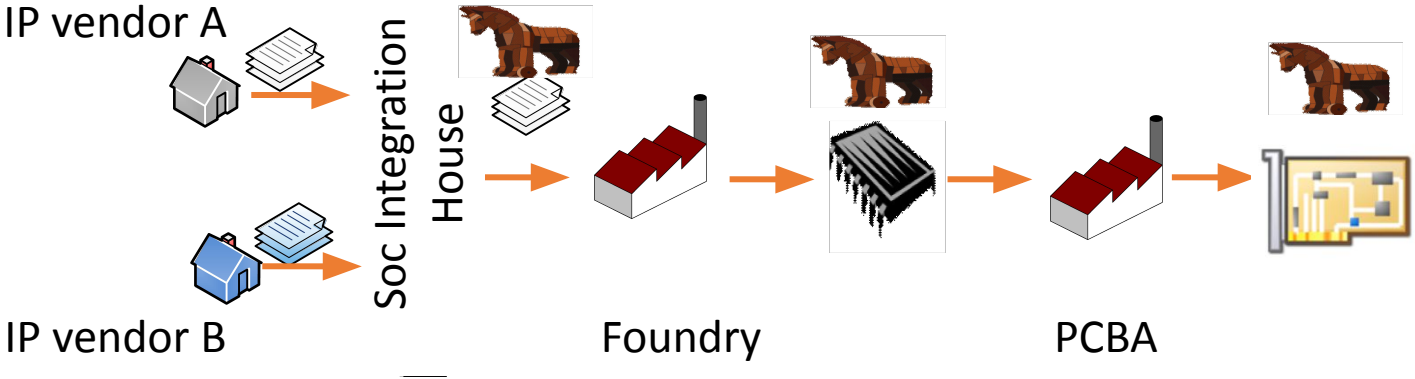
Hardware Security - Risks

What are we trying to protect?

“C I A” triad:

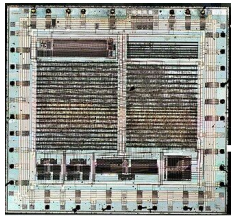
- Confidentiality
- Integrity
- Availability

Hardware Trojans

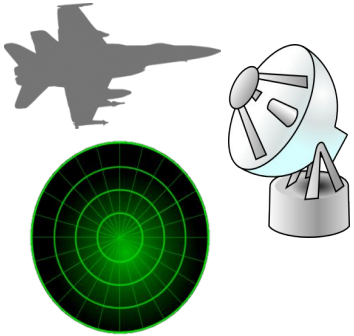


- Malicious modifications to designs
- Objective: Control, modify, disable or monitor content
- Scenarios:
  - Malicious 3PIP vendor
  - Malicious foundries
  - Malicious PCBA

Hardware Trojan Examples



"Clipper" backdoor



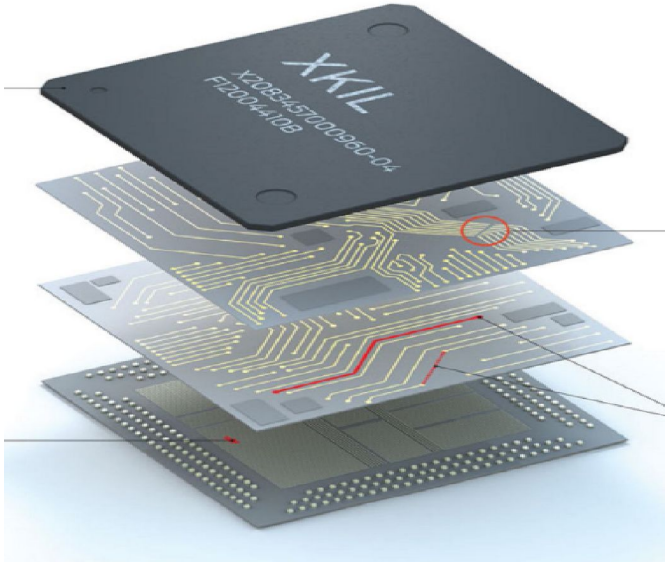
DoS attacks on radars

Lebanon Pager Explosions

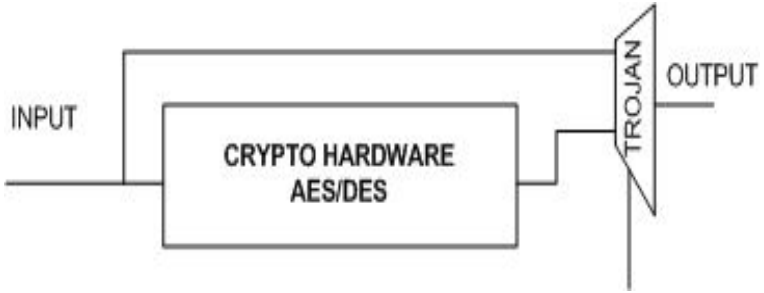
- (1993) Clipper chips with NSA backdoor to decrypt comms
- (2007) Syrian radars were turned off by Hardware Trojans
- (2024) Pagers and Walkie-Talkies are exploded after secret supply-chain Hardware Trojan attack

More reading: R. Karri, **J. Rajendran**, K. Rosenfeld, M. Tehranipoor, IEEE Computer,2010
S. Adee, "The Hunt for the Kill Switch," IEEE Spectrum, 2008

Hardware Trojans: The Kill Switch?



IEEE Spectrum, 2008



Supply Chain Hardware Trojan Attacks

The Long Hack: How China Exploited a U.S. Tech Supplier

For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it was never told. Neither was the public.

By Jordan Robertson and Michael Riley
February 12, 2021, 5:00 AM

FEDERAL CONTRACT OPPORTUNITY

Link Pursuit | Add Pursuit | Search

Microsystems Exploration: Safeguards against Hidden Effects and Anomalous Trojans in Hardware (SHEATH)

Pre-Solicitation | 2 Years Past Due | Inactive

Updated Jul 18 2019, 11:17 am EDT

Modchips of the State: 35th Chaos Communication Congress, 2018. https://fahrplan.events.ccc.de/congress/2018/Fahrplan/events/9597.html

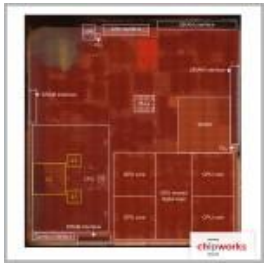
Reverse Engineering (IP Theft?)

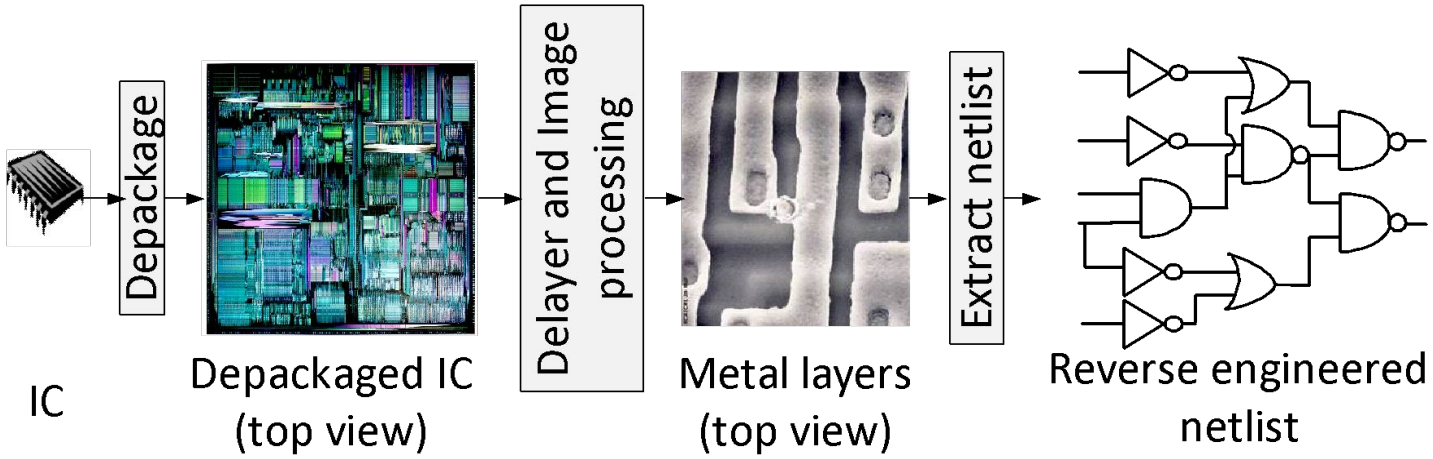
EE Times

System and IC teardowns become critical 'business intelligence'

chipworks

INSIDE THE NEW iPhone 6 and iPhone 6 Plus





Reverse Engineering (IP Theft?)

- Identify device technology, functionality, design
- Can identify:
  - Piracy (did you use circuits not belonging to you?)
  - Trojan insertion (does this circuit make sense here?)
- But also enables:
  - Piracy (can steal the designs that have been reversed)
  - Trojan design (can identify sites to add malicious changes)

Reverse Engineering Examples

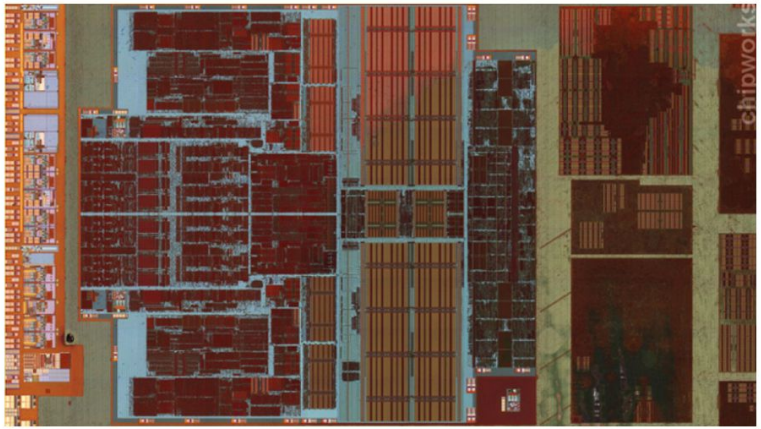
EXTREMETECH Aerospace Cars Computing Defense Electronics Energy Gaming Phones Science Security

Home > Computing

iPhone 5 A6 SoC reverse engineered, reveals rare hand-made custom CPU, and tri-core GPU

Apple still hasn't said a word about the new A6 SoC within the iPhone 5, but no matter: Chipworks has now completed its initial analysis of the A6, and the results are very interesting indeed. The A6 features a custom, in-house, laid-out-by-hand dual-core design (pictured above) that is neither a Cortex-A9 or A15, and a tri-core GPU.

By Sebastian Anthony September 25, 2012



DIGITIMES asia TECH REGIONS RESEARCH OPINIONS FINANCE BIZ FOCUS

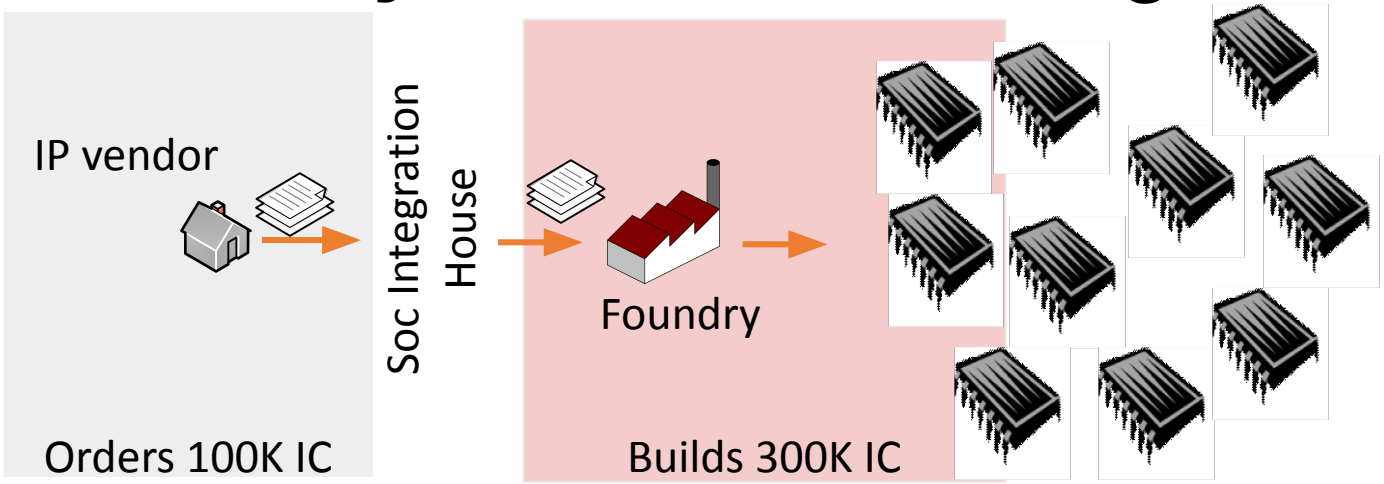
Academia: China's astonishing reverse engineering capabilities spur steep rise in US strategic concerns

Bryan Chuang, Taipei; Willis Ke, DIGITIMES Asia | Thursday 12 October 2023 | 0 Like 0

PHOTONICS spectra®

Using Reverse Engineering to Discover Patent Infringement
By Julia Elvidge, President, Chipworks

IC/IP Piracy and “Overbuilding”

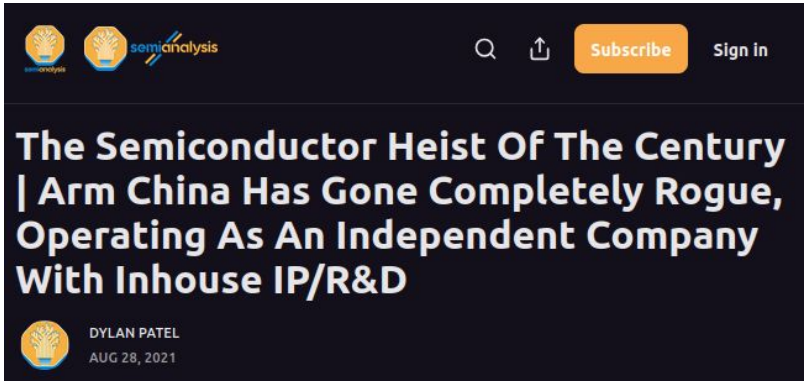


- Steal & claim ownership of an IC
- Scenarios:
  - Malicious SoC integration house
  - Malicious foundry

Piracy and Overbuilding examples

Protecting IP and Revenue

The U.S. Chamber of Commerce estimates that IP threats cost domestic companies more than $250 billion per year in lost revenues, as well as the loss of approximately 750,000 jobs. More than 55 million jobs in the U.S. are supported by IP-intensive industries.



- The annual revenue loss due to IP theft equates to current annual level of U.S. exports to Asia — more than $300 billion. Over **55 million jobs** in the U. S. are supported by IP intensive industries.

Microsemi

Cybersecurity

Inside the Chinese Boom in Corporate Espionage

Inside the Chinese boom in corporate espionage

By Michael Riley and Ashlee Vance
March 15, 2012, 11:03 PM UTC

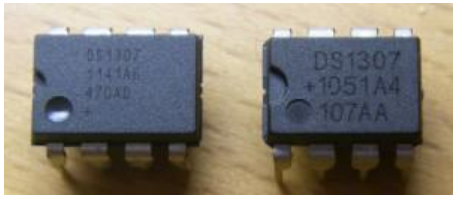
some startling findings. The Sinovel turbine appeared to be running a stolen version of AMSC's software. Worse, the software revealed that Sinovel had complete access to AMSC's proprietary source code. In short, Sinovel didn't really nee

On April 5, AMSC had no choice but to announce that Sinovel–now its biggest customer, accounting for more than two-thirds of the company's $315 million in revenue in 2010 –had stopped making purchases. Investors fled, erasing 40 percent of AMSC's value in a single day and 84 percent of

Counterfeiting

Remove ICs

Repackage



Original Vs. Counterfeit

Forbes

The Serious Risks From Counterfeit Electronic Parts

Source: Forbes and ABCNews

abcNEWS

Counterfeit Chinese Parts Slipping Into U.S. Military Aircraft: Report

- Forgery or imitation of original components
- Commercial benefit and subvert mission-critical systems

Counterfeiting Examples

Ghost in the Machine: How Fake Parts Infiltrated Airline Fleets

A little-known distributor in London sold thousands of engine components with bogus documentation. Carriers and repair shops are frantically hunting them down.

By Julie Johnsson, Ryan Beene, Siddharth Vikram Philip, and Sabah Meddings

12 October 2023 at 10:00 GMT+11

The Washington Post

Sign in

Business Economy Economic Policy Personal Finance Work Technology Business of Climate

Even the US Military Has a Fake Parts Problem

Analysis by Tim Culpan | Bloomberg

October 12, 2023 at 4:29 p.m. EDT

BBC Watch Register Sign In

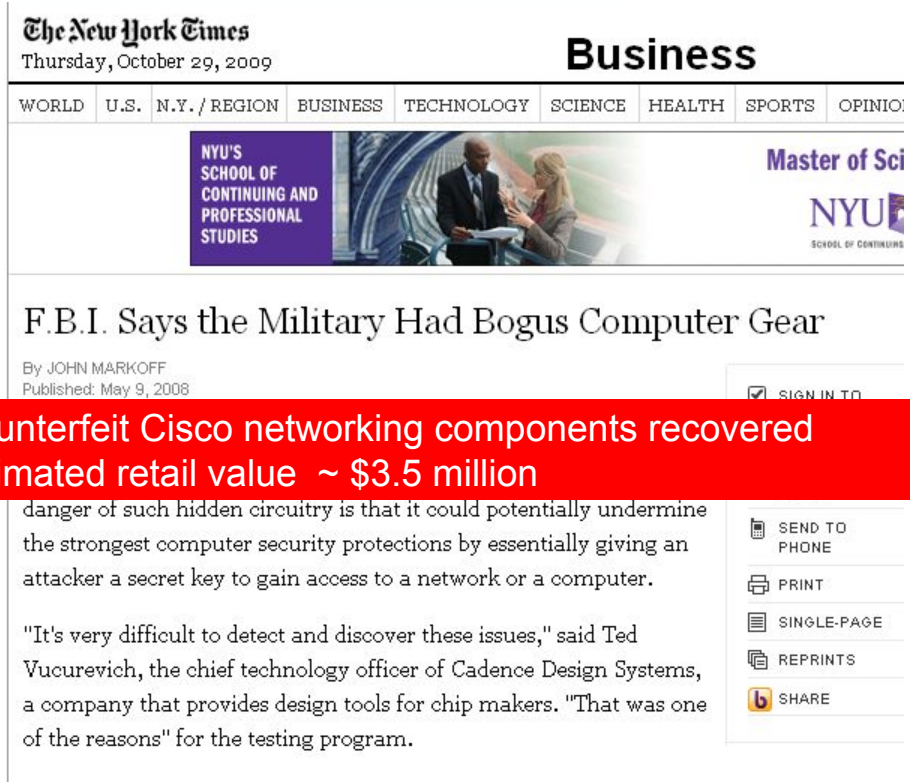
Fake goods: Apple products among items worth £600,000 seized

29 March 2024

Share Save

The fake goods were seized during police raids on two premises on Thursday

Counterfeiting Examples



The New York Times
Thursday, October 29, 2009

Business

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINIO

F.B.I. Says the Military Had Bogus Computer Gear

By JOHN MARKOFF
Published: May 9, 2008

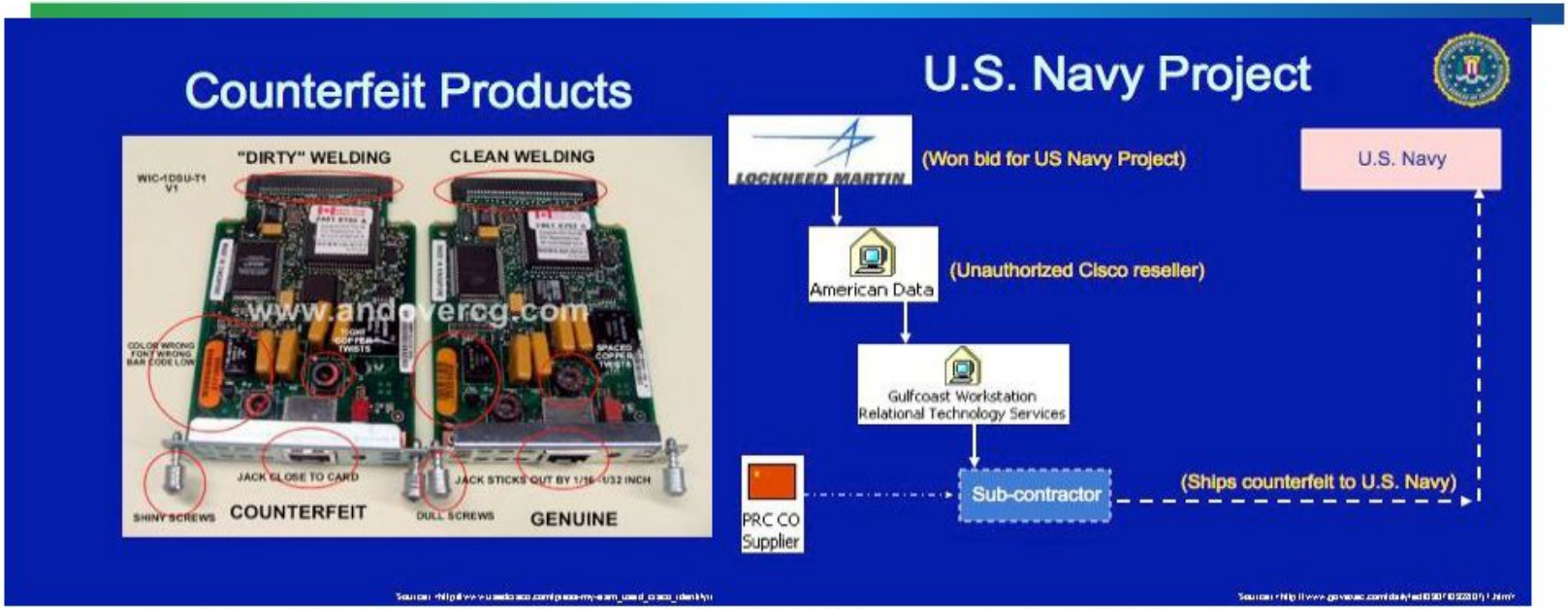
3500 counterfeit Cisco networking components recovered
- estimated retail value ~ $3.5 million

danger of such hidden circuitry is that it could potentially undermine the strongest computer security protections by essentially giving an attacker a secret key to gain access to a network or a computer.

"It's very difficult to detect and discover these issues," said Ted Vucurevich, the chief technology officer of Cadence Design Systems, a company that provides design tools for chip makers. "That was one of the reasons" for the testing program.

SIGN IN TO
SEND TO PHONE
PRINT
SINGLE-PAGE
REPRINTS
SHARE

Counterfeiting Examples



- Lockheed Martin unknowingly sells $250K Chinese counterfeit “Cisco” routers to Navy

Microsemi

Counterfeiting consequences?

[Senate Hearing 112-340]
[From the U.S. Government Publishing Office]

S. Hrg. 112-340

THE COMMITTEE'S INVESTIGATION INTO
COUNTERFEIT ELECTRONIC PARTS IN THE
DEPARTMENT OF DEFENSE SUPPLY CHAIN

==========

HEARING

before the

COMMITTEE ON ARMED SERVICES

UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

NOVEMBER 8, 2011

In November 2010, after a part failed on a fielded aircraft, and in internal testing L-3 Display Systems discovered that a memory chip used on its display unit was counterfeit. L-3 Display Systems had already installed the parts on more than 500 of its display units, including those intended for the C-27J, as well as the Air Force's C-130J and C-17 aircraft and the CH-46 used by the Marines. **Failure of the memory chip could cause a display unit to show a degraded image, lose data, or even go blank altogether.**

Counterfeiting consequences?

Air Force Research Laboratory (AFRL) investigators were concerned that “counterfeit parts” in a jet ejection seat system may have contributed to the death of an F-16 pilot in June 2020, according to a federal lawsuit filed this summer against defense contractors.

Real-world hardware security attacks

Smart Cards- Attacks

- **Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks** Drimer and Murdoch, USENIX SECURITY, 2007

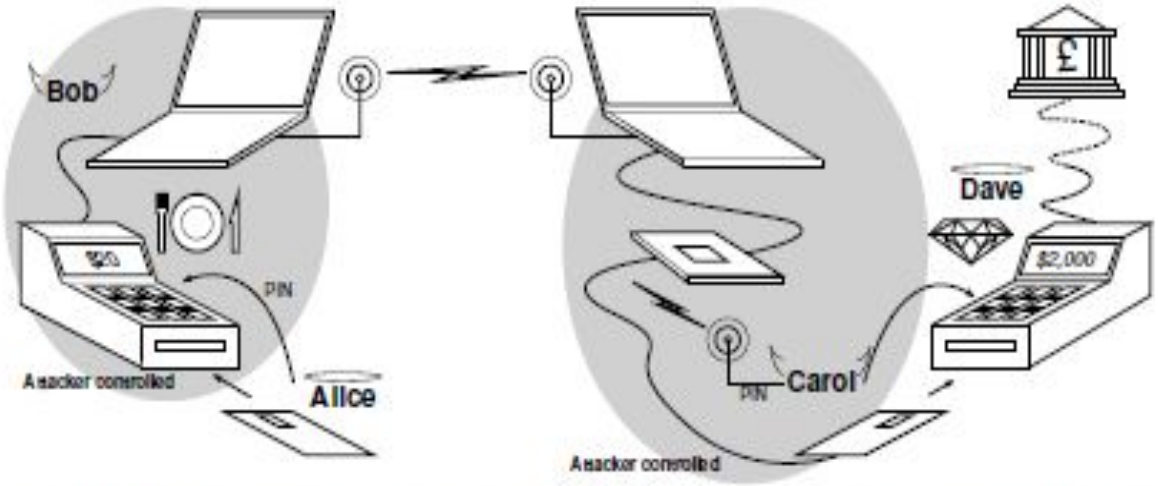


Figure 1: The EMV relay attack. Innocent customer, Alice, pays for lunch by entering her smartcard and PIN into a modified terminal operated by Bob. At approximately the same time, Carol enters her fake card into honest Dave's terminal to purchase a diamond. The transaction from Dave's terminal is relayed wirelessly to Alice's card with the result of Alice unknowingly paying for Carol's diamond.

IP Piracy –The Chinese Faker

- In 2000, Mr X. finished Ph.D. in computer engineering at UT Austin
- He returned to China, first to work at Motorola research and then to work at Jiaotong University as a faculty
- In 2003, he supervised a team that created one of China's first homegrown DSP ICs
- Chen was named one of China's brightest young scientists, funded his own lab and got a huge grant from the government
- In 2006, it was revealed that he stole the design from Texas Instruments.

The New York Times

In a Scientist's Fall, China Feels Robbed of Glory

Chen Jin, the Chinese computer scie accused of fraud.
Associated Press

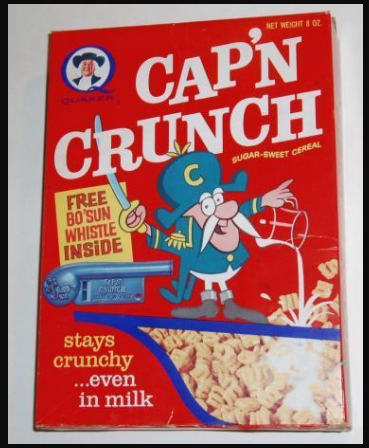
By David Barboza
May 15, 2006

Cap’n Crunch free phone calls (1972)

By Nanda

- Free, long distance calls using whistle from Cap’n Crunch cereal box
  - Discovered by John Draper
  - The whistle emitted a 2600 hertz tone
  - Could access internal authorization system in the phone company
  - Allowed user to route call by emulating in band signaling mechanism

- No longer works in western nations:
  - Digital + out of band signaling



https://www.wired.com/2001/02/the-greatest-hacks-of-all-time/

Smart utility hacking alert (2009)

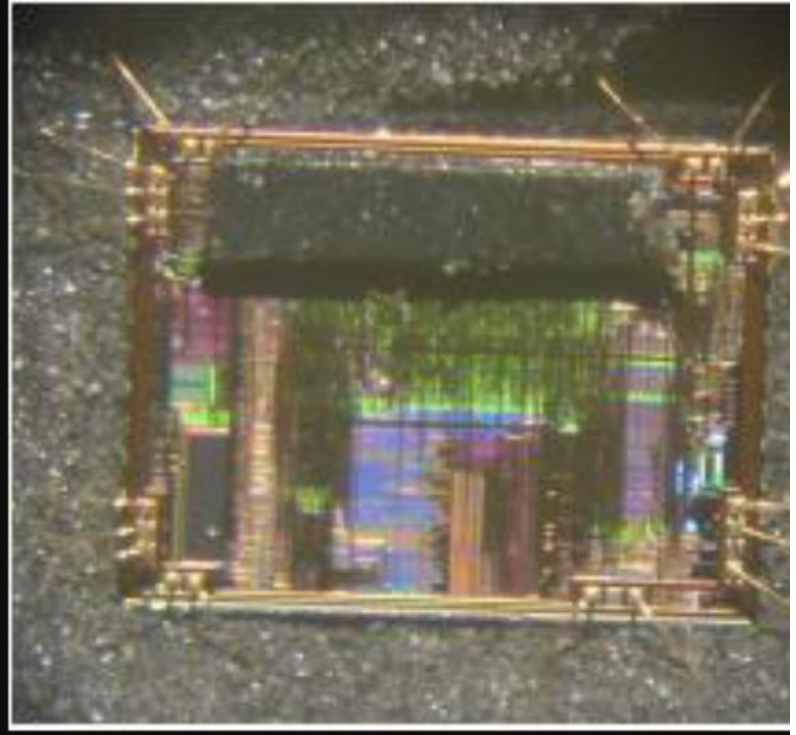
http://www.forbes.com/2009/04/29/smart-grid-legislation-technology-security-smart-grid.html
http://travisgoodspeed.blogspot.com/2009/03/breaking-802154-aes128-by-syringe.html
http://www.blackhat.com/presentations/bh-usa-09/GOODSPEED/BHUSA09-Goodspeed-ZigbeeChips-PAPER.pdf
http://www.ioactive.com/news-events/DavisSmartGridBlackHatPR.php

- Utilities used piezoelectric (mechanical) meters.
  - Manual reading, activation, and deactivation.
  - Hackers could tamper with the meters using magnets.
- Utilities moved to smart (electronic) meters
  - remote reading, activation and deactivation
  - Used CC2420 module for Zigbee communication with AES-128
  - Even this can be hacked
    - Travis Goodspeed hacked a smart electric meter
    - Used syringe to intercept AES key on SPI bus between key ROM+module

By Carlos Ospina

Engineers and hackers play "cat and mouse" (Rui [redacted])

- Designers have constraints: time-to-market, manufacturing cost etc.
- Hackers have an advantage over designers
- Andrew Huang' discovery:
  - PIC µcontrollers store configuration "fuse" settings in Flash memory
    - code protection bits to prevent modification of selected mem.
    - code protection bits to prevent reading from selected mem.
  - PIC flash: similar to UV-erasable EPROMs.
- ATTACK STRATEGY: access die and reset fuses with UV light
  - disable asserted code protection bits
  - extract/modify program code stored.



Exposed PIC18F1320: Electric tape covers flash memory; prevents erasure of firmware when UV light is shined onto configuration fuses

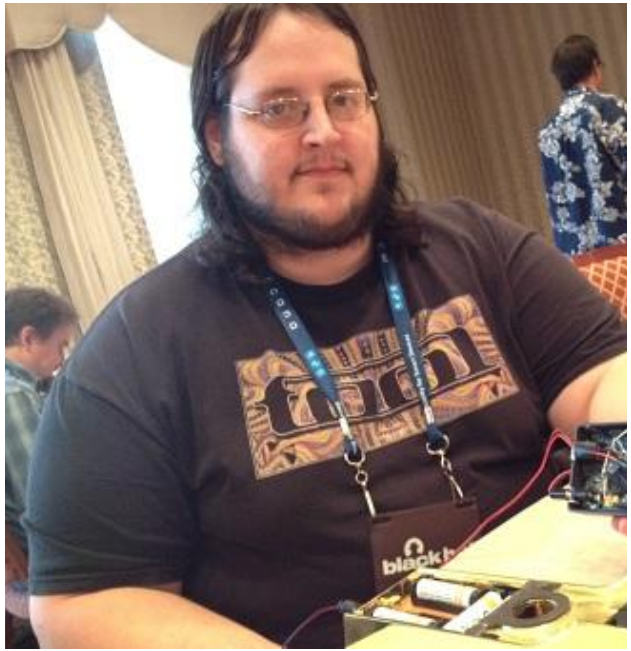
Hacking apple laptop batteries (2011)

- Loophole in apple smart battery chip (Miller, Accuvant Lab)
- Smart battery chips have a micro-controller
  - Help OS monitor/control battery/charger.
  - Determine charge end point and regulate heat ensuring safety.
- Each battery has a unique password
  - Once this is deciphered, a hacker could control the smart battery.
  - Could permanently damage the battery
  - Could infect computer with malicious software
  - may cause battery to overheat, catch fire or even explode (but sensors can detect overheating)

Zuoda

Security flaws in hotel keycards (2012)

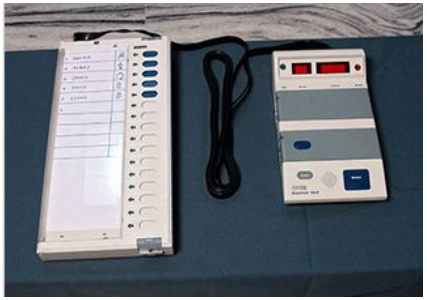
- Using ~ $20, one can gain instant access to hotel rooms
  - Cody Brocious discovered vulnerabilities in the Onity room locks
  - http://demoseen.com/bhpaper.html
- Dump the memory of the reader or
- Brute-force the 32-bit key of the proprietary crypto on the card.
- Get the master key for all rooms.
- Onity has since issued a security response plan

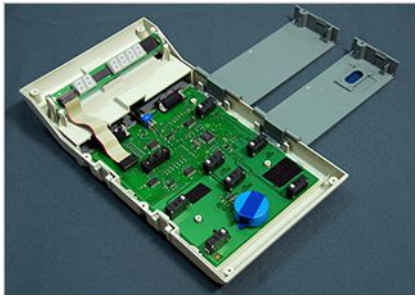


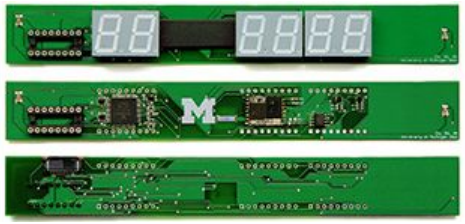
Ernesto

India's Electronic Vote m/cs are vulnerable (2012)

- EVM: ballot unit (*left*) used by voters + control unit (*center*) operated by poll workers







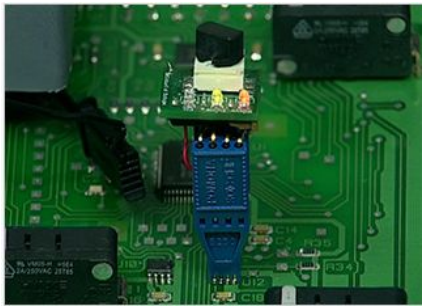
- Claim: India's EVMs are "infallible" and “perfect“
- Ballot unit circuit board has CPU+vote memory+display.
- EVM was not subjected to detailed scrutiny pre-deployment
- Attack: Replace display in EVM with a dishonest look-alike (right)
  - Hidden parts under the LEDs substitute dishonest vote totals when displaying election results.

http://www.indiaevm.org/

Dong

India's Electronic Vote m/cs are vulnerable (2012)

- Android app wirelessly instructs dishonest display which candidate should receive stolen votes.
- Attack device clips on to memory chips inside EVM.
  - Clip-on device is small enough to fit in a shirt pocket.
  - Close-up of clip-on vote stealing attack device.
  - Rotary switch allows attacker to select the candidate to favor.



Dong

A Darker Side of Future (2013)

- Brain-computer interfaces (BCI) promise: games, computers, prosthetics may be controlled with thought.
- USENIX paper: BCI could let sensitive private information leak out along with the mental commands.
- Study of 28 subjects wearing BCI devices from Neurosky, Emotiv and marketed to consumers for gaming and attention exercises
- Researchers extracted hints from the electrical signals of the test subjects' brains
    - partially revealed private info: location of homes, faces they recognized, credit card Pins, month of birth etc.

Zhendong

Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter

by

AbduLLahi (ECE-GY- 9453, 2022)

- **Attack Explanation:** In this attack, an Arduino-based intrusion system is implemented and invasively embedded at an inverter's location to create external magnetic field. This enables the attacker to spoof on the inverter's hall sensors from a remote location, compromising the inverter's operation.
- **Attack Impact:** The attacker was able to manipulate the grid's voltage and frequency, inject false real and reactive power from the inverter to the grid and introduce undetectable low-frequency harmonics into the grid.

Reference

[1] A. Barua and M. A. Al Faruque, ''Hall spoofing: A non-invasive dos attack on grid-tied solar inverter,'' in Proc. 29th USENIX Secur. Symp., 2020, pp. 1273–1290.

[2] https://news.uci.edu/2020/08/18/uci-cyber-physical-security-researchers-highlight-vulnerability-of-solar-inverters/

COMPROMISED 2FA USING CLONE KEY

01.

INTRODUCTION

French Researchers Victor Lomne and Thomas Roche have discovered the vulnerability impacting hardware security keys.

02.

REQUIREMENTS

Physical access to the device is needed, as it can't happen remotely. Also, the casing has to be opened using a hot gun as shown in the photo shared by ninja labs.

03.

WORKING

This is a Side-Channel Attack (CVE-2021-3011), as it reconstructs the primary encryption key that the hardware security key uses to generate the cryptographic tokens.

04.

CONCLUSION

NXP A7005a chip can be switched with FIDO U2F by the end-users to minimize the risk. And this process takes hours to perform and get access to the system, which can be noticed as unusual activity.

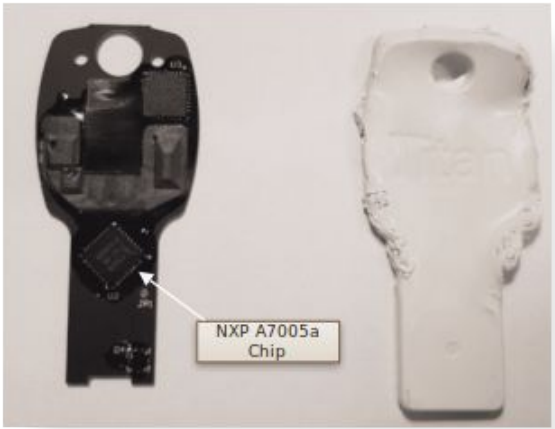


Photo by Ninja Lab

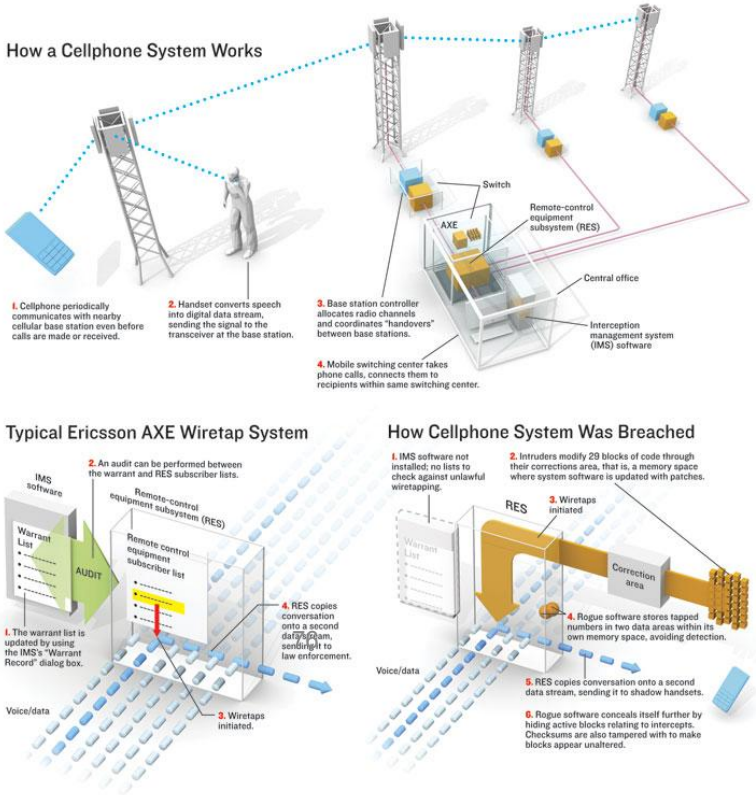
Sony vs. Hackers

- ✔ In 2000 SONY PS2 used standard disc authentication.
- ✔ 60 million PS2 consoles sold worldwide as of 2003
- ✗ The “boot disc” (written and sold by an unlicensed 3rd party vendor) contained code to stop the drive from spinning. Drive can then be forced open and the disc can be replaced by a pirated copy of the DVD.
- ✔ SONY implemented a pick-proof lock to prevent unauthorized opening of the drive.
- ✗ “mod-chip” (a small board containing a FPGA and Flash) connected to console was developed to emulate the DVD authentication data.
- ✔ SONY developed a proprietary **Dynamic Network Authentication System** (**DNAS**). DNAS uses a set of codes in a protected area of the DVD together with serial numbers from the console EEPROM for online authentication.
- ✔ Pirated game copies made using regular DVD-R burners do not have this protected area, and the games fail to authenticate to the servers.
- ✗ To circumvent this, a firmware upgrade for *mod-chip* was made to report hardcoded values without attempting to access the protected area of the DVD.
- ✔ SONY gives up on making anymore modifications and begins work on the next generation console, the PlayStation3.
- ✗ Estimated loss in software sales due to piracy is $3,000,000,000.

https://www.psdevwiki.com/ps2/Modchips
https://consolemods.org/wiki/PS2:DNAS

The Athens Affair

- Mar 8, 2005: Costas Tsalikidis, a 38-year-old Engineer working for Vodafone Greece committed suicide!
- Mar 9 2005: Prime minister of Greece was notified that his cell phone and those of other high ranking officials were hacked!
- in Jan 2005: investigators found rogue software installed on Ericsson switches in the Vodafone Greece network by parties unknown
- Vodafone was fined €76 million December 2006!



- **Princeton Professor Finds No Hardware Security In E-Voting Machine,** Antone Gonsalves, InformationWeek, 02/16/07
  - Target: a Sequoia AVC Advantage electronic voting machine
  - Student picks lock protecting a backdoor to motherboard in seven seconds.
  - Once door off, only needed to unscrew 10 screws from a sheet metal panel to get to the computer's circuit boards.
    - no tamperproofing seals protecting any of machine's components.
  - Reverse engineer program instructions, write your own instructions on a ROM chip
    - available from any computer equipment retailer
  - pop out the original chip from its socket, and press in the new one

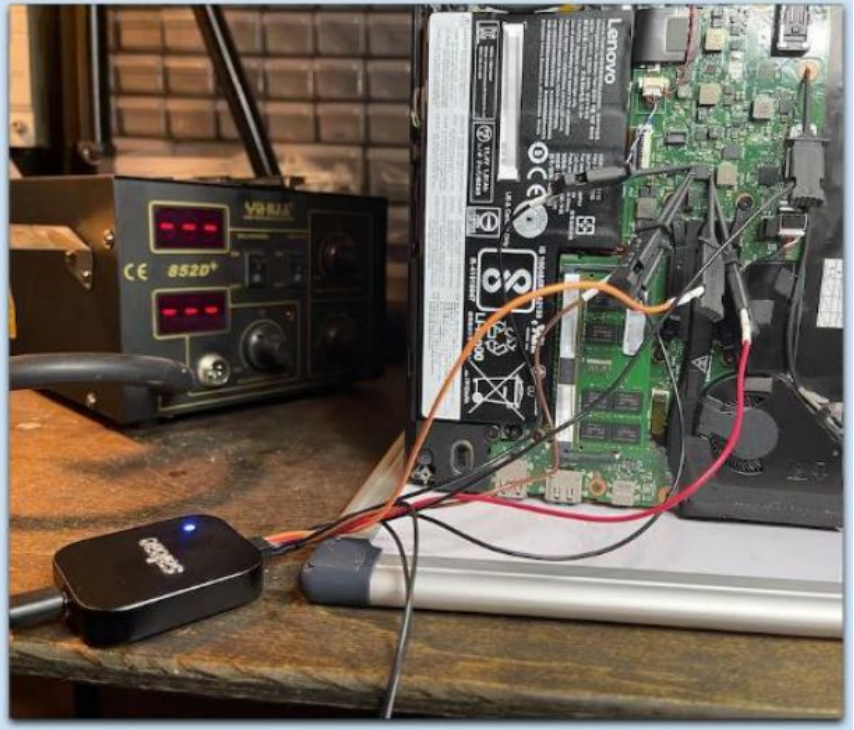
Fort Knox and the not so armored car: breaking a TPM fully encrypted disk with bus sniffing (2021)

Attack:

- TPM storing drive encryption key
- MS Bitlocker does not use encrypted communications
- Attackers want to sniff the SPI bus between CPU and TPM but TPM pins are not exposed
- Another IC shares the same bus with exposed pins
- They sniff the bus from those pins and identify the key, successfully decrypting the drive

Possible resolutions:

- Use encrypted bus for TPM secrets
- Use a user password AND TPM secret to encrypt the drive
- user password should be for authorization of the TPM sealed secret so that dictionary attacks can be stopped by the TPM hardware

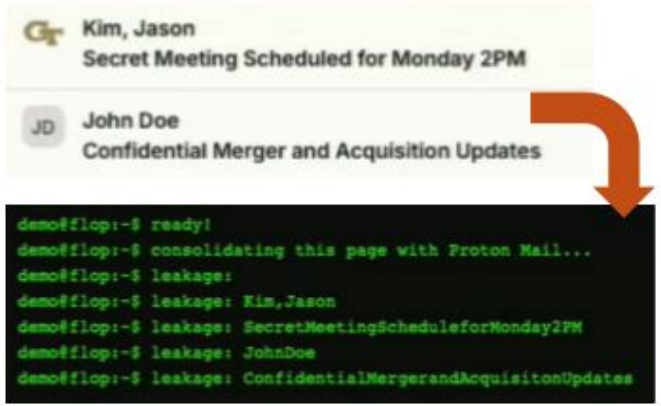


https://arstechnica.com/gadgets/2021/08/how-to-go-from-stolen-pc-to-network-intrusion-in-30-minutes/

Leaps going out of bounds - Apple Silicon's Load Address Predictor

Freya - 2025

- Apple designed its own series of processors called Apple Silicon
- Uses hardware to speed up large sequential data accesses by predicting which memory address is read before the real instruction is reached
- Guesses based on spacing between previous addresses and assumes pattern will continue
- But does not check if the predicted memory address was correct or allowed
- So it can be tricked into predicting memory addresses outside normal limits!
- An example using Safari and Javascript, an attacker website can open windows with email data, and attacker can trick the predictor into reading that data
- This flaw is in hardware, full security only guaranteed from new hardware
- For now, the exploit is not considered a risk to most users



https://predictors.fail/

Hacking the kernel with an SD card

Liam - 2025

- SD Express: a new speed tier for SD cards
  - Internally, the card is connected to PCIe
- But PCIe is dangerous!
  - Devices write directly to memory for speed…
  - …but they can write anywhere, even the kernel!
- A familiar threat: Thunderbolt supports PCIe passthrough too
- Hardware mitigation: IOMMUs
  - Address translation is slow, so off by default
  - Turned on specifically for Thunderbolt… are they on for SD Express?
  - Varies between manufacturers

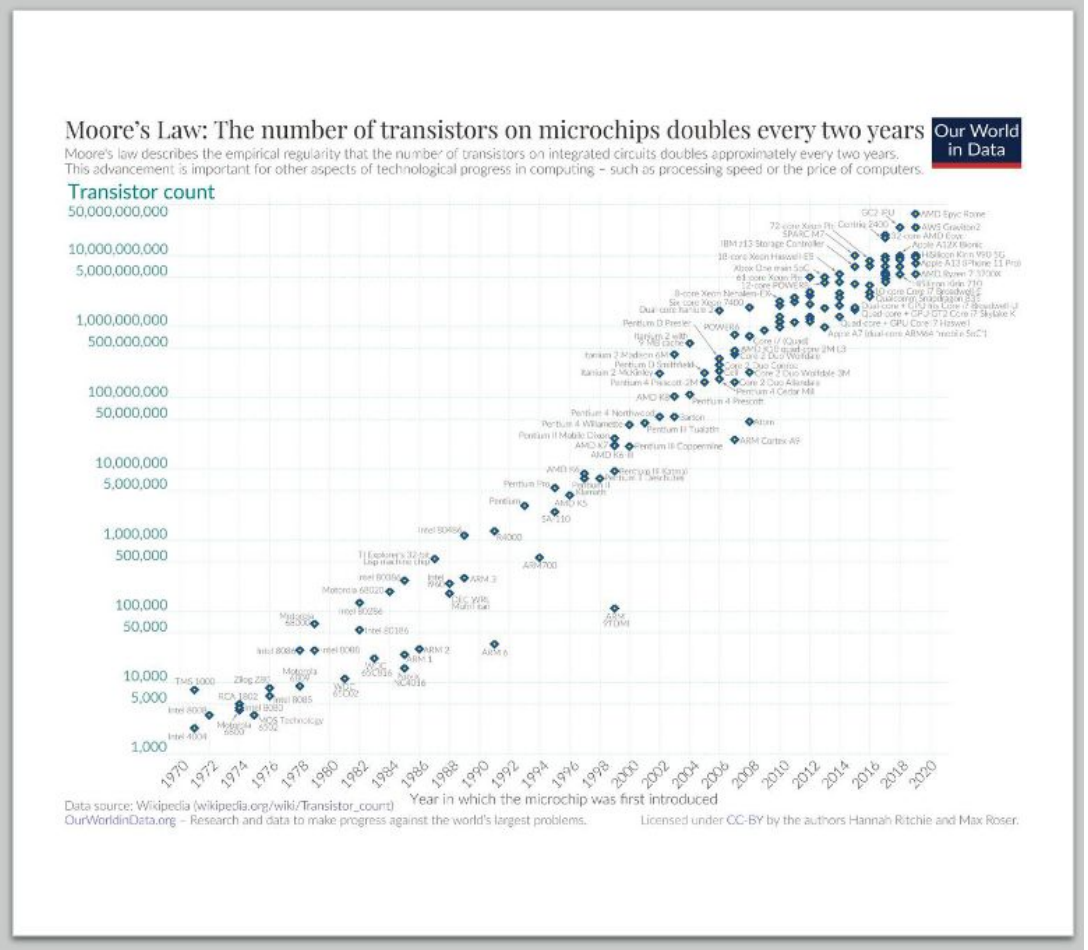
THUNDERCLAP

https://swarm.ptsecurity.com/new-dog-old-tricks-damagecard-attack-targets-memory-directly-thru-sd-card-reader/

EL: 9423 , Rui

Moore' law and hacking

- 1970: DES was designed to withstand 30 years of cryptanalysis
- 1998: Deep Crack (custom hardware; $250,000; recover key in ~56 hrs)
- 2006: COPACOBANA (FPGAs; $10,000 recover key in ~6.4 days on avg)



Hardware Security is ever-evolving

- New threats
- New attacks
- New capabilities

As well as…

- New defensive strategies
- New manufacturing strategies

It’s a lot to take in!

Assessments: Week 1

(Yes, I’m releasing one already)

Report 1: Real-World HW Sec. Incident

- Identify and research a real-world hardware security incident.
- Analyze and explain cause and consequences.
- Present findings:
  - Report (3%)
    - one preferable, max two page report
    - IEEE conference two-column format (google for template)
  - Summary slide (2%)
    - Like the ones you've just seen!
    - Summarise report's key points - Single slide only!

Each student must find their own incident

Stake your claim on Discourse

Post event and reference
First come first served

Where to search?

- Blogs:
  - krebsonsecurity.com
  - schneir.com
- News / tech journalism:
  - Wired / New Scientist / IEEE Spectrum
- Academic venues:
  - USENIX SEC, USENIX WOOT, S&P, CCS, NDSS
  - RAID, CHES, DATE, DAC
  - etc.
- Presentations / YouTube:
  - DEFCON, BlackHat, CCC, etc.

Report 1: Due Friday Week 2

Lab 0: Preparation Lab

- Runs through a quick-start for the Hackster hardware platform
- Ensures you know how to operate the board
- Is not assessed directly…
  - Except by Report 2, which will get you to explain part of the last section.
- You can start Lab 0 in this week's tutorials
  - Immediately after this lecture!

That’s it! Questions?