CPE 426 Intro to Hardware Security

Or, the world is more than software

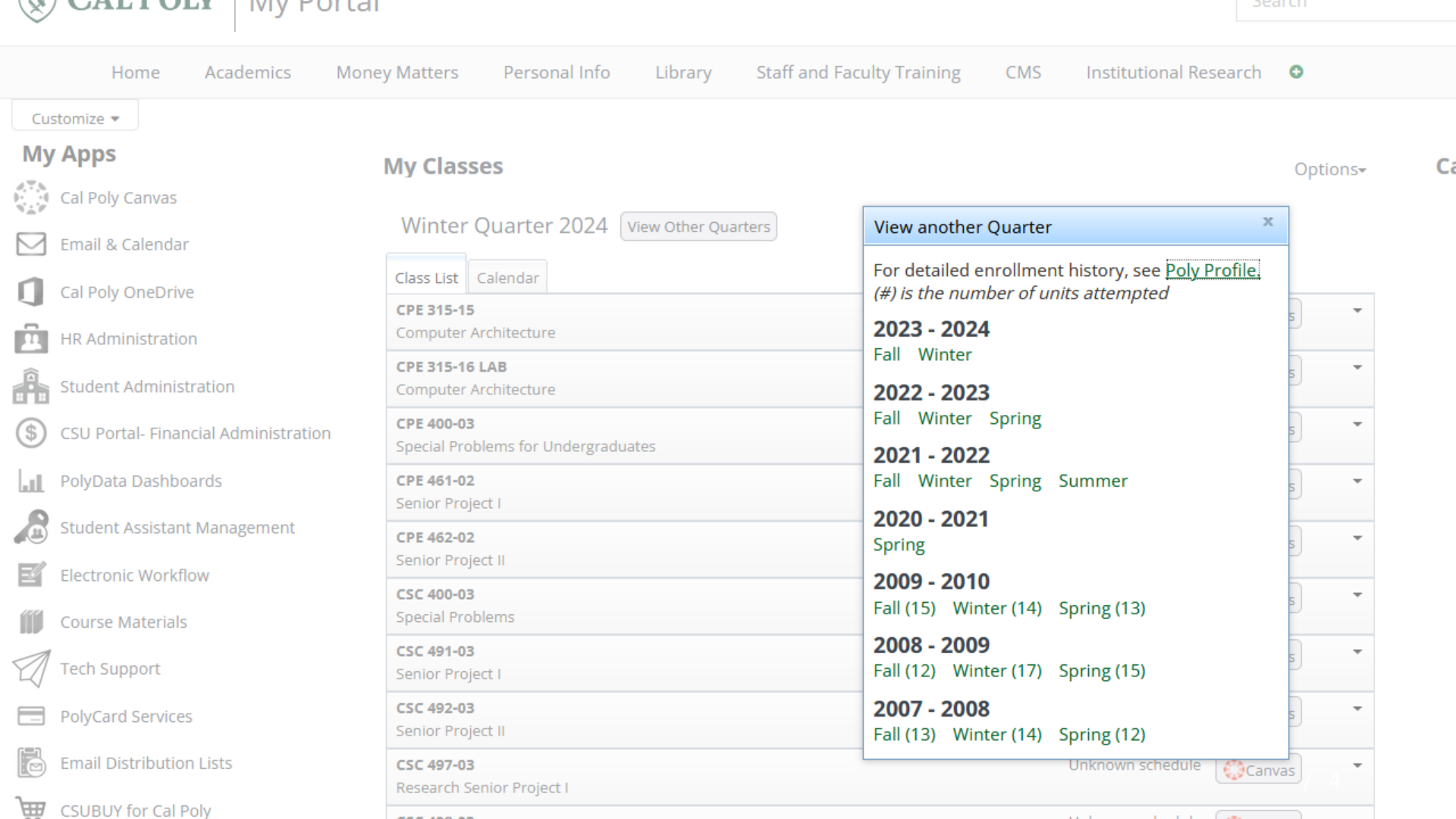
Dr. Stephen R. Beard
CalPoly Fall 2024
Department of Computer Engineering

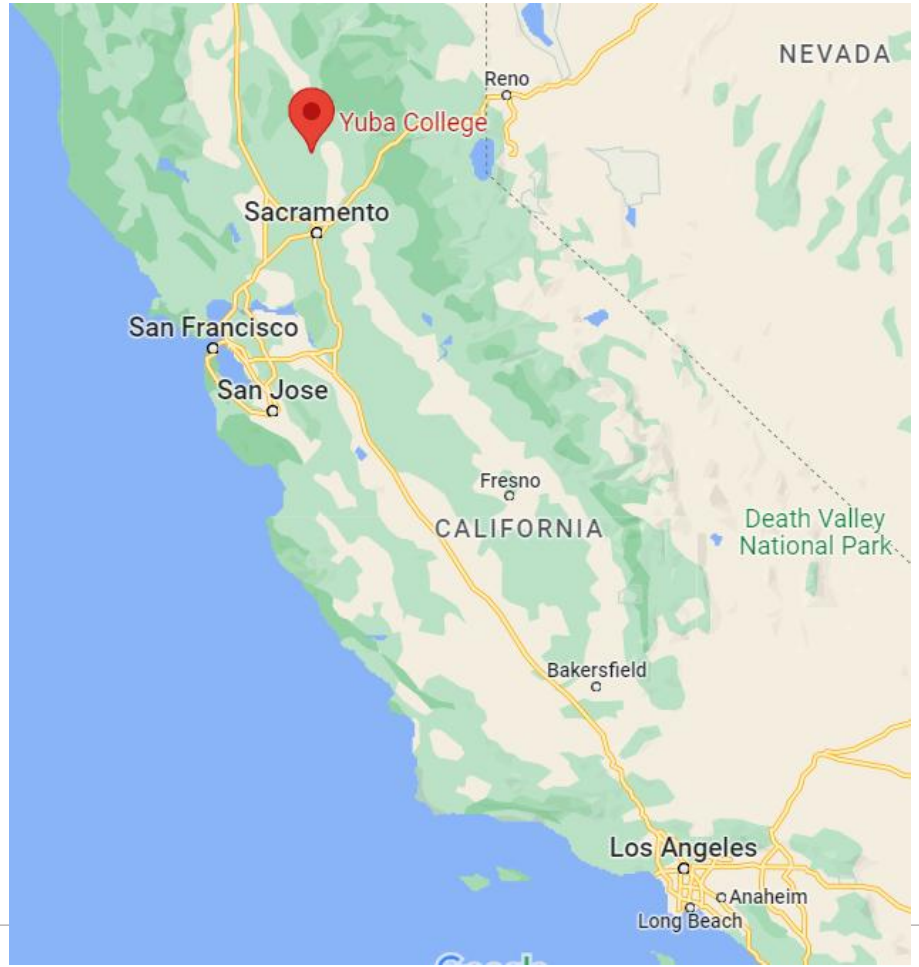
CAL POLY

Outline

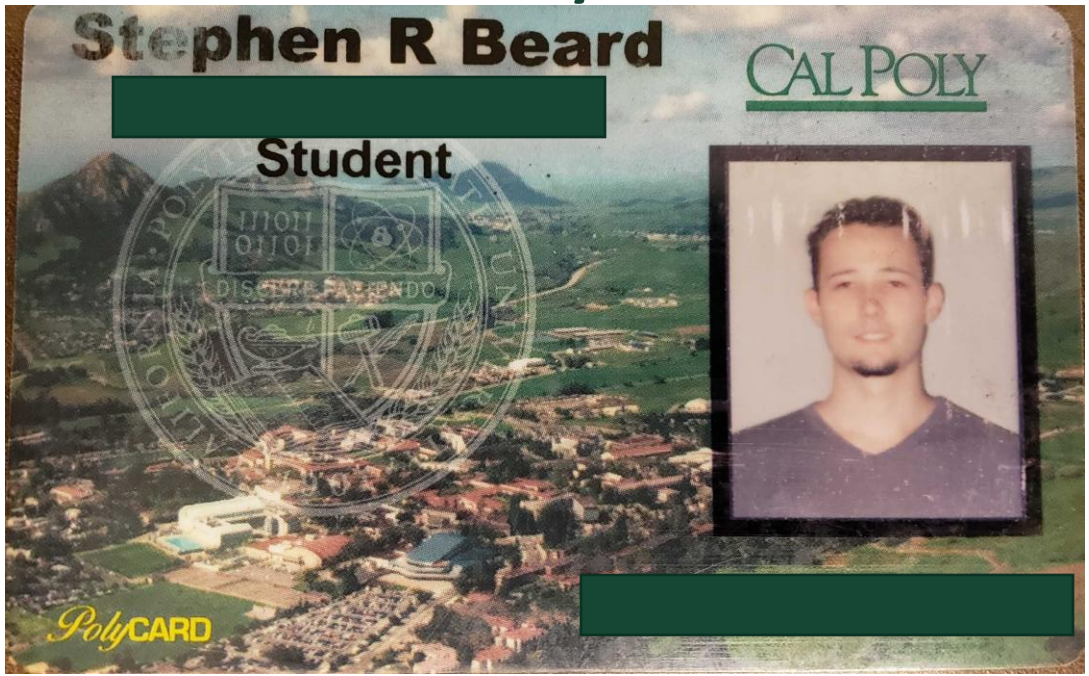
- Instructor Introduction
- Why hardware (system) security?
- Course Structure
- Physical Attacks
- Physical Tamper Resistance (probably next time)
- Reading Assignments

Who is this guy?

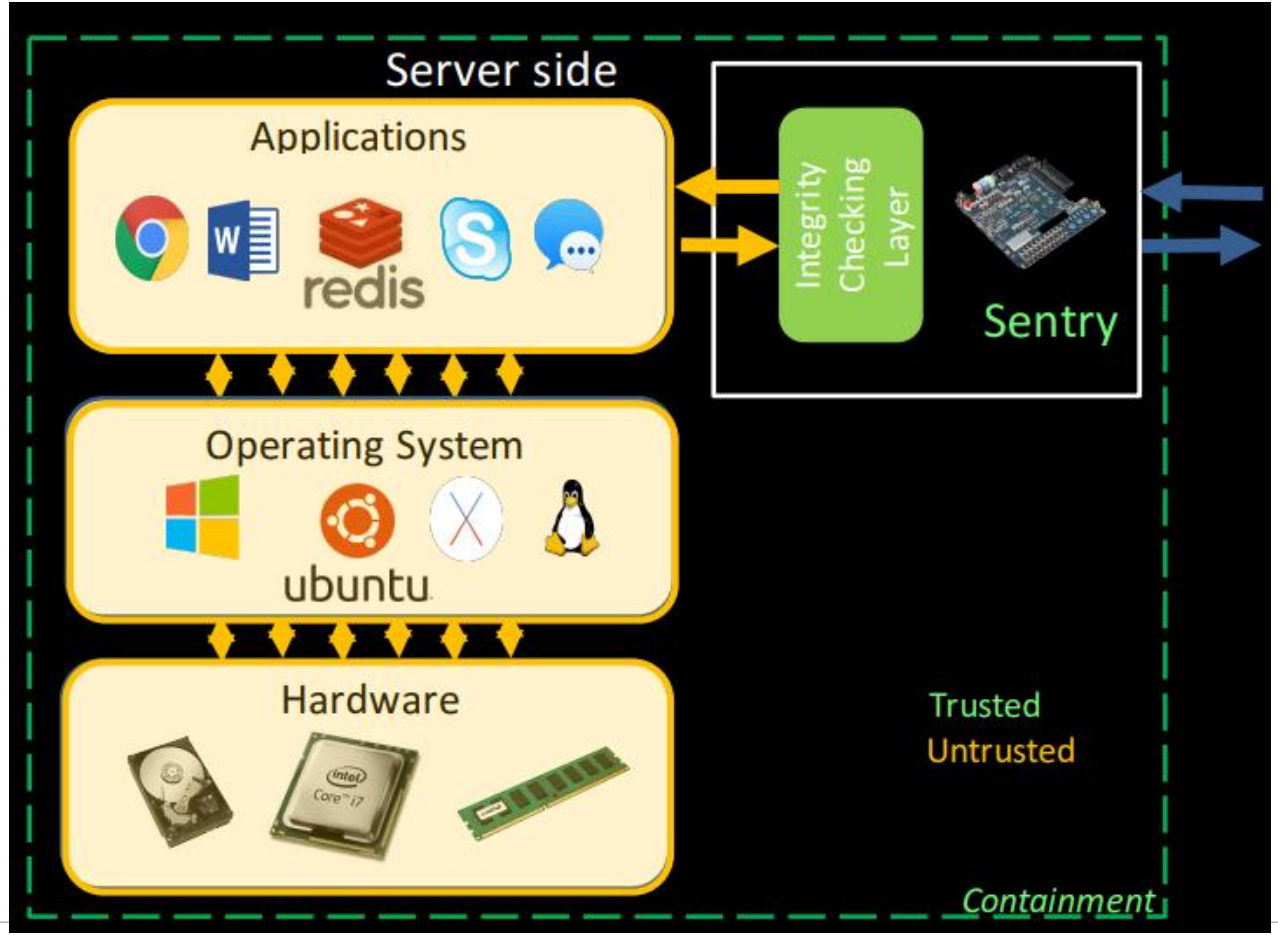

My Portal
Home
Academics
Money Matters
Personal Info
Library
Staff and Faculty Training
CMS
Institutional Research
Customize
My Apps
Cal Poly Canvas
Email & Calendar
Cal Poly OneDrive
HR Administration
Student Administration
CSU Portal- Financial Administration
PolyData Dashboards
Student Assistant Management
Electronic Workflow
Course Materials
Tech Support
PolyCard Services
Email Distribution Lists
CSUBUY for Cal Poly
My Classes
Options
Winter Quarter 2024
View Other Quarters
Class List
Calendar
CPE 315-15
Computer Architecture
CPE 315-16 LAB
Computer Architecture
CPE 400-03
Special Problems for Undergraduates
CPE 461-02
Senior Project I
CPE 462-02
Senior Project II
CSC 400-03
Special Problems
CSC 491-03
Senior Project I
CSC 492-03
Senior Project II
CSC 497-03
Research Senior Project I
Unknown schedule
Canvas
View another Quarter
For detailed enrollment history, see Poly Profile
(#) is the number of units attempted
2023 - 2024
Fall Winter
2022 - 2023
Fall Winter Spring
2021 - 2022
Fall Winter Spring Summer
2020 - 2021
Spring
2009 - 2010
Fall (15) Winter (14) Spring (13)
2008 - 2009
Fall (12) Winter (17) Spring (15)
2007 - 2008
Fall (13) Winter (14) Spring (12)


NEVADA
Reno
Yuba College
Sacramento
San Francisco
San Jose
Fresno
CALIFORNIA
Death Valley
National Park
Bakersfield
Los Angeles
Anaheim
Long Beach

Cal Poly 2007




CAL POLY
San Luis Obispo
Computer
Engineering


Server side
Applications
redis
Integrity Checking Layer
Sentry
Operating System
ubuntu
Hardware
Trusted
Untrusted
Containment

Tigerstone


2σ
TWO SIGMA

~~CAL POLY~~

CAL POLY

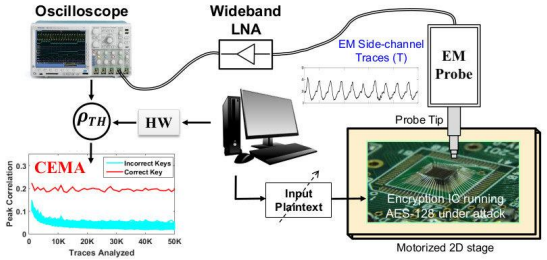
Why Hardware Security?

Computer Security

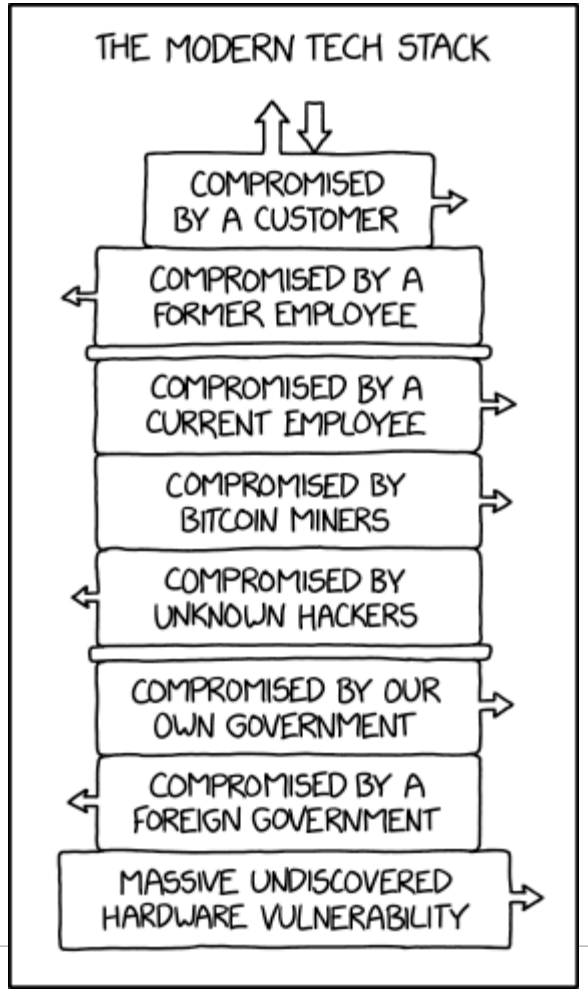
What people think of

What is most likely

What is scariest



[1] Google Images
[2] https://www.soscanhelp.com/blog/top-phishing-scams-of-2021


THE MODERN TECH STACK
COMPROMISED BY A CUSTOMER
COMPROMISED BY A FORMER EMPLOYEE
COMPROMISED BY A CURRENT EMPLOYEE
COMPROMISED BY BITCOIN MINERS
COMPROMISED BY UNKNOWN HACKERS
COMPROMISED BY OUR OWN GOVERNMENT
COMPROMISED BY A FOREIGN GOVERNMENT
MASSIVE UNDISCOVERED HARDWARE VULNERABILITY

worldometer Coronavirus Population

W / Population / World Population

Current World Population

7,975,497,292

view all people on 1 page >

TODAY		THIS YEAR	
Births today	179,656	Births this year	100,334,796
Deaths today	75,424	Deaths this year	42,122,951
Population Growth today	104,232	Population Growth this year	58,211,845

WORLD POPULATION SECTIONS

Top 20 Countries LIVE	by Region
Past, present, and future	by Religion
Global Growth Rate	Population Density
Historical data	Population by Country
Forecast	All-time total
Milestones	[Sources and methods]

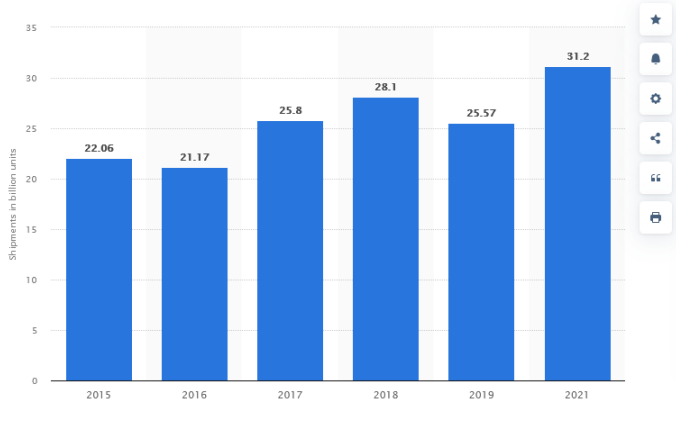
Demographics: Age Structure | Sex Ratio | Population Pyramid | Median Age | Fertility Rate | Life Expectancy | Urbanization

Technology & Telecommunications › Hardware

PREMIUM

Microcontroller unit (MCU) shipments worldwide from 2015 to 2021

(in billions)



DOWNLOAD

PDF XLS PNG PPT

Source
→ Show sources information
→ Show publisher information
→ Use Ask Statista Research Service

Release date
June 2022

Region
Worldwide

Survey time period
2015 to 2021

Microcontroller unit (MCU) shipments worldwide 2015-2021

Published by Thomas Alsop, Jul 21, 2022

In 2021, global shipments of microcontroller units amounted to approximately 31.2 billion units, a 13 percent increase from the figure recorded in 2020. Total MCU sales grew by around 27 percent, up to 20.2 billion U.S. dollars.

The C[illegible]nt Approach to C[illegible]

Reported Incidents


DAWN LIM SECURITY 11.08.11 5:28 PM

WIRED

COUNTERFEIT CHIPS PLAGUE U.S. MISSILE DEFENSE

"We do not want a $12 million THAAD [Terminal High Altitude Area Defense] interceptor to be destroyed by a $2 part" [1]


Researchers can slip an undetectable trojan into Intel's Ivy Bridge CPUs

ars technica

New technique bakes super stealthy hardware trojans into chip silicon.

by Dan Goodin - Sep 18, 2013 10:57am EDT

Share Tweet 110

"…a hardware trojan can be introduced at a later stage of the design process by changing the 'doping' on a few transistors on the chip" [3]


German missiles 'hacked by foreign source'

By Conor Gaffey 7/8/15 at 4:52 PM

Newsweek

"An exposed point is a computer chip which controls the guidance of the weapon" [2]

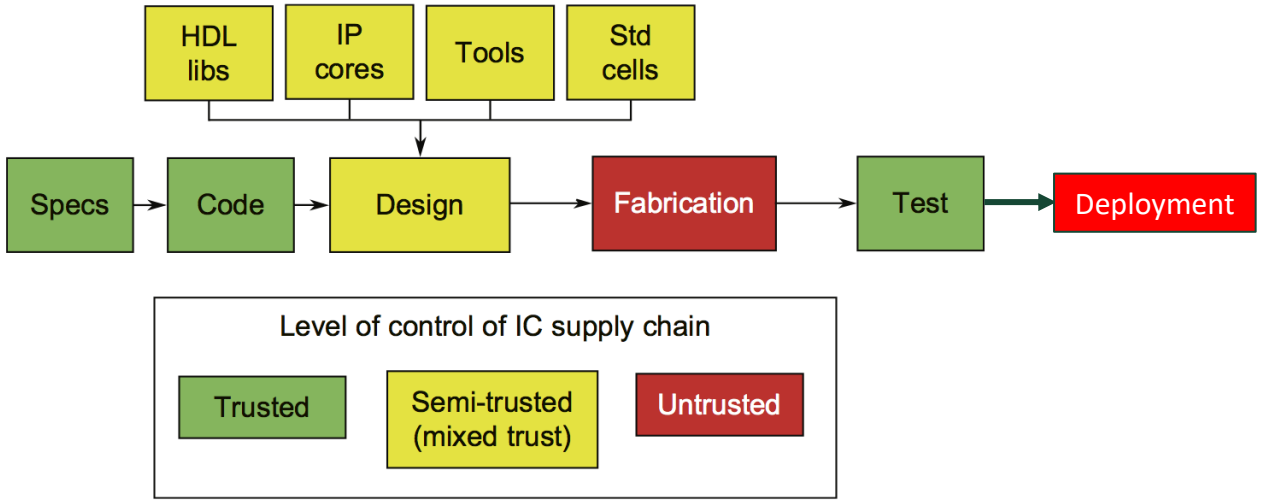

TECHNOLOGY

The New York Times

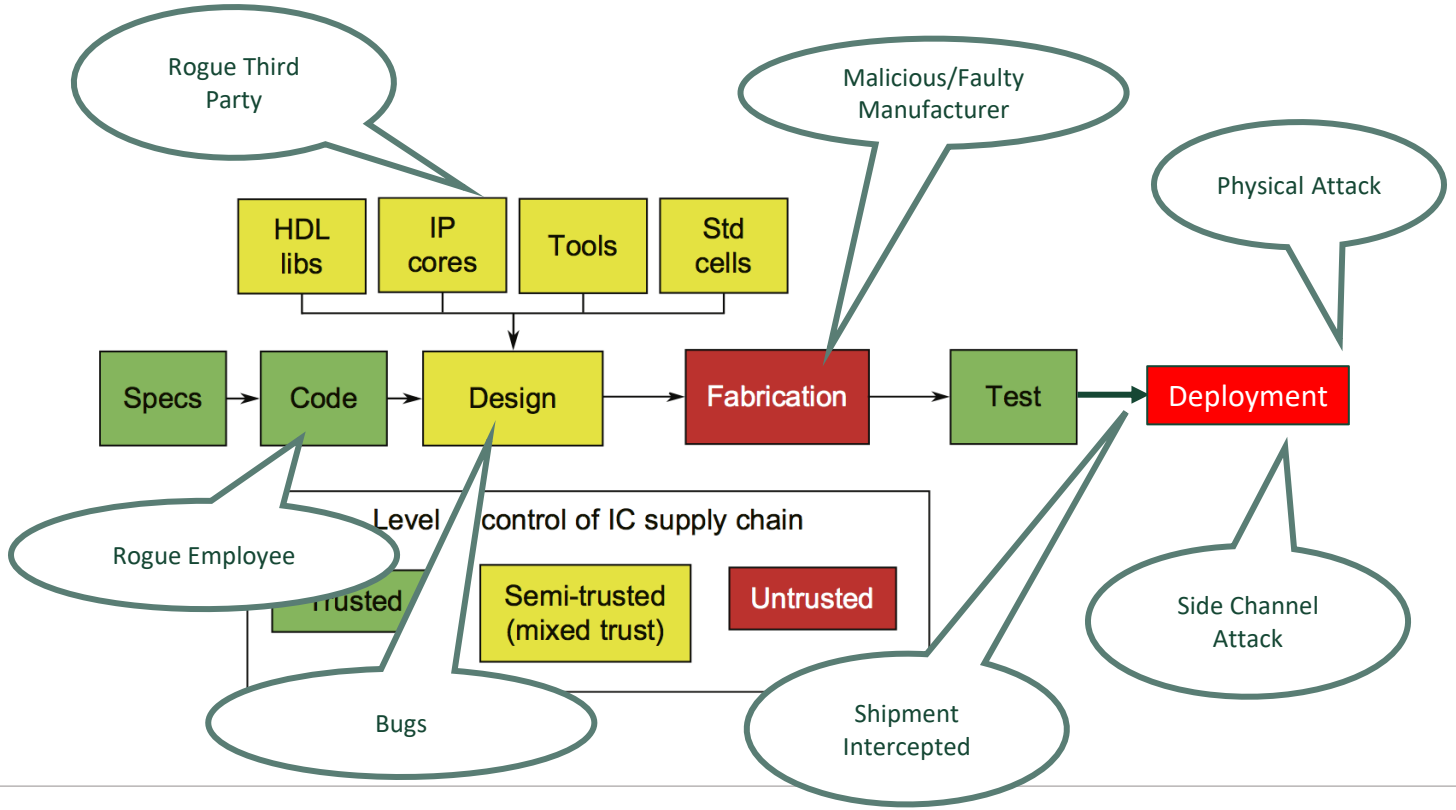
Adding Math to List of Security Threats

"A subtle multiplier bug would make it possible for an attacker to break the protection afforded to some electronic messages by public key cryptography." [4]

IC Supply Chain – a designer's perspective



Example Threats



Course Structure

Read the Syllabus

Course Topics

1. Intro and Physical Attacks
2. Physically unclonable functions (PUFs) and Sources of Randomness in hardware
3. Hardware trojans
4. Formal Methods
5. Side Channels
<End Part 1>
6. Speculative Execution Attacks
7. Secure Co-Processors
8. Encrypted Execution and Data (Secure Processors?!)
9. Hybrid Hardware/Software Techniques (E.g. SGX, taint tracking, hardware validation of software properties)

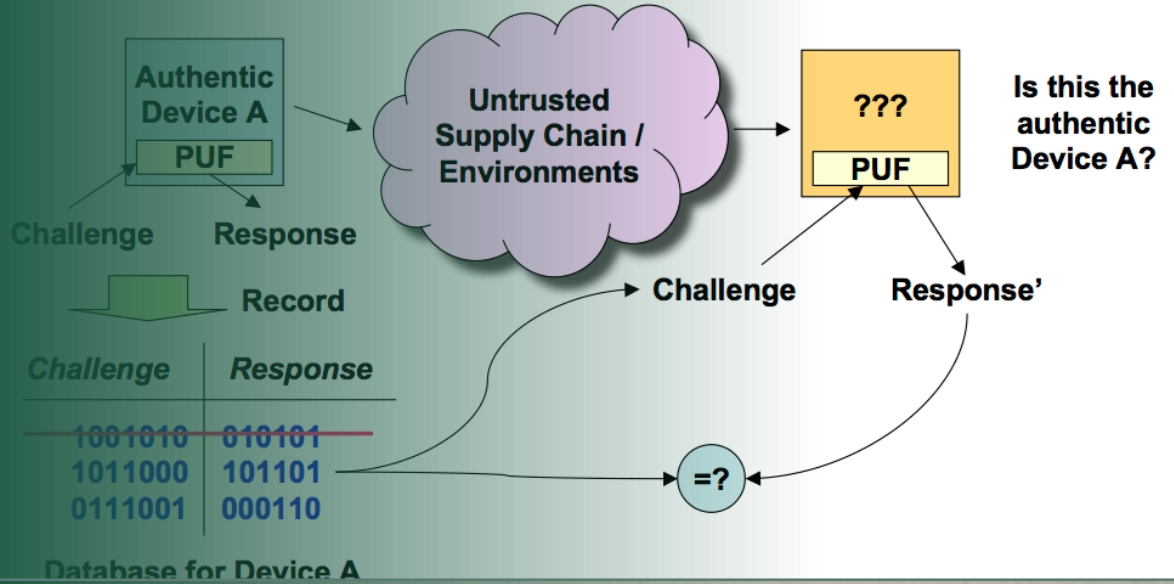
Grading Breakdown

Category	Weight
Labs	30%
Final Project	40%
1 Presentation	10%
Class Participation	10%
10 Reading Responses	10%

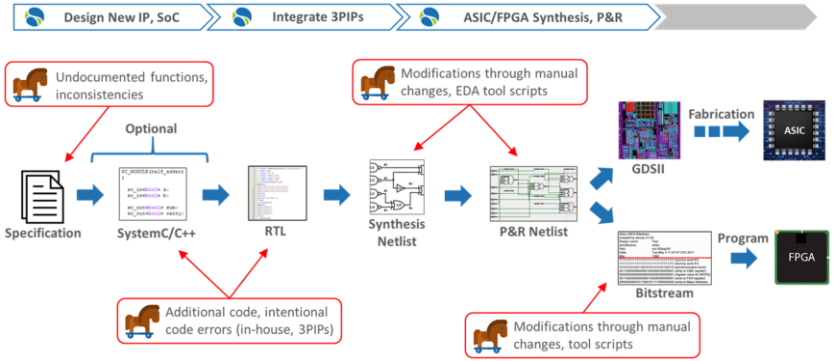
Week 1
Physical Attacks

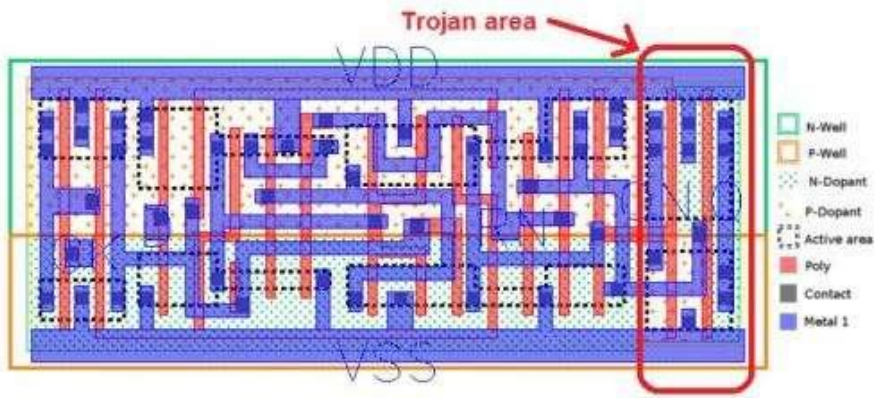
[1] Google Ir

Week 2
HW PUF + Randomness



Week 3
Hardware Trojans

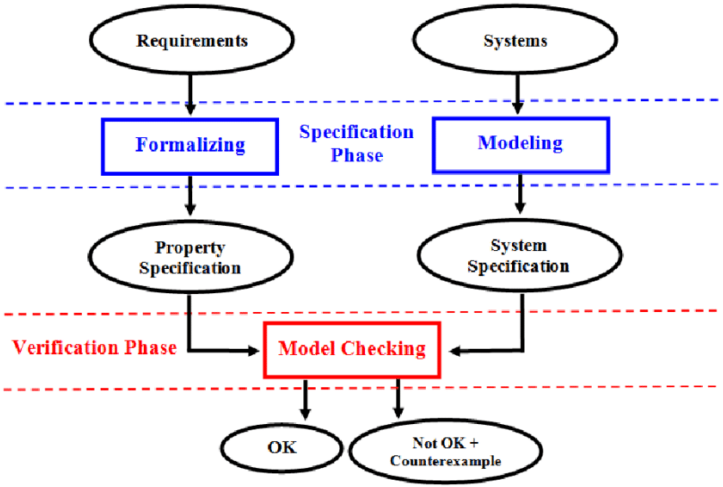


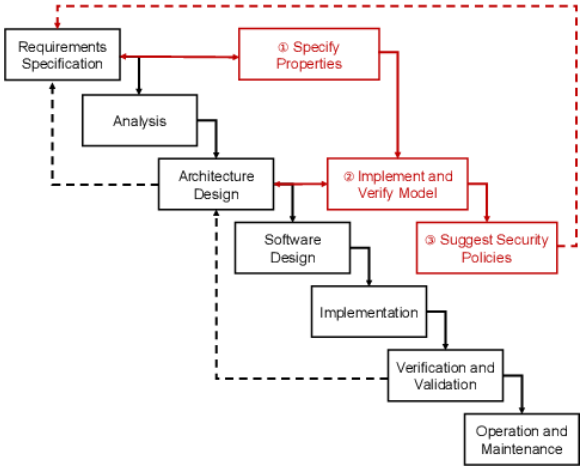


Week 4
Formal Methods

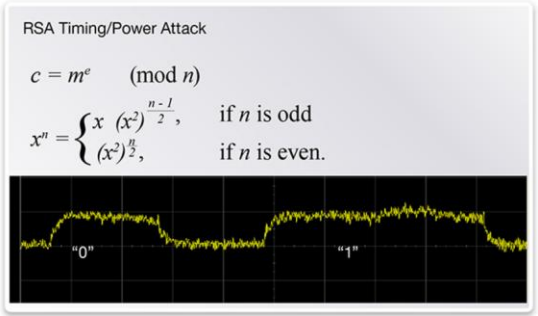
TABLE III
SPECIAL Z SYMBOLS

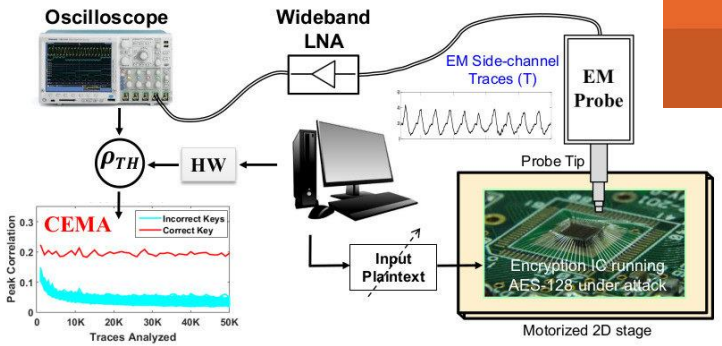
Symbol	Meaning
$f : X \rightarrow Y$	Function between X and Y
$f : X \leftrightarrow Y$	Relation between X and Y
id$X$	The identity function on X
dom$f$	The domain of f
ran$f$	The range of f
$f(\!\lvert X \rvert\!)$	Image of the set X under the function f
$f \oplus g$	Function which takes values of the function f except on the domain of g, where it takes the values of g
$f \circ g$	Functional composition where the domain of g must equal the range of f
$X \setminus Y$	Set difference of X and Y



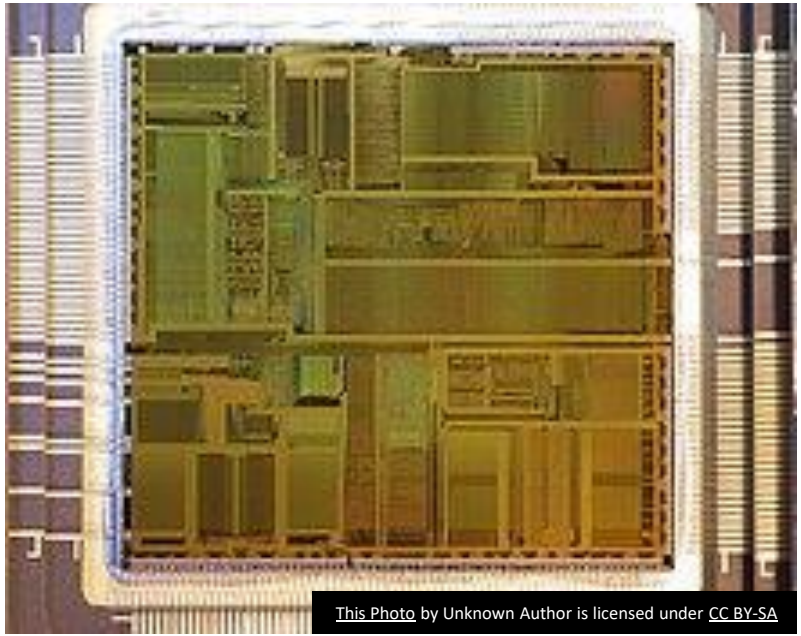


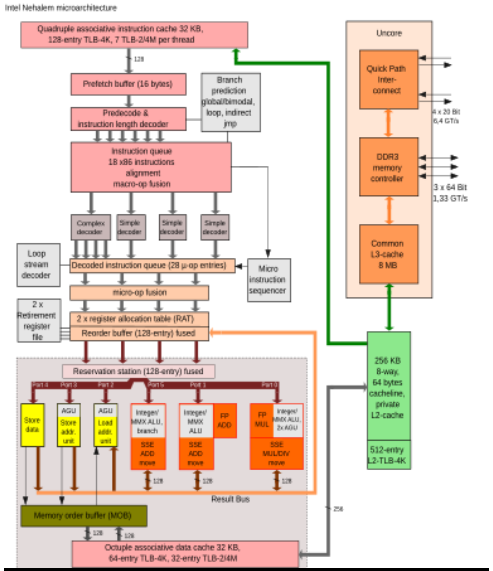
Week 5
Side Channels





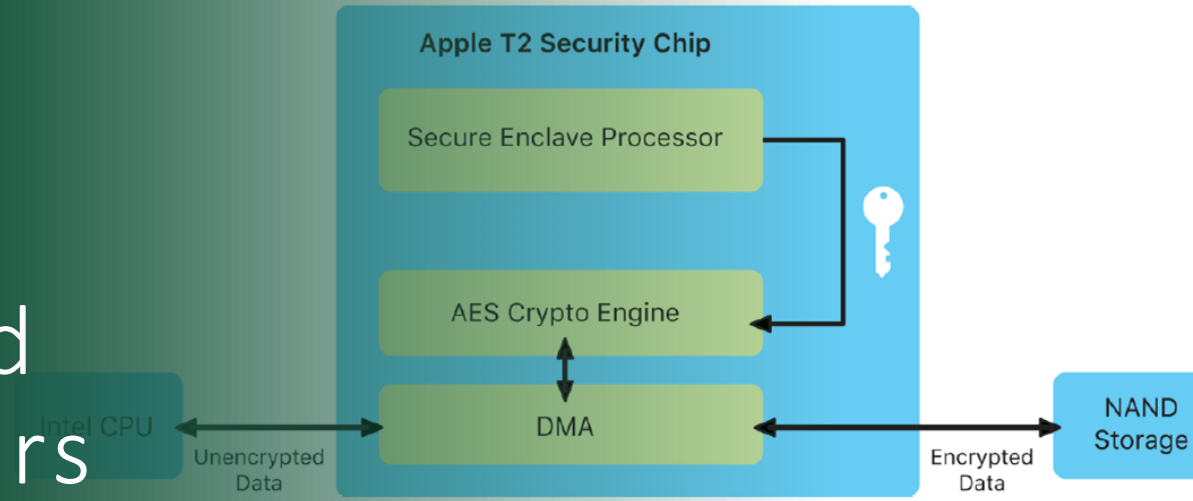
Week 6
Advanced Architecture in two days



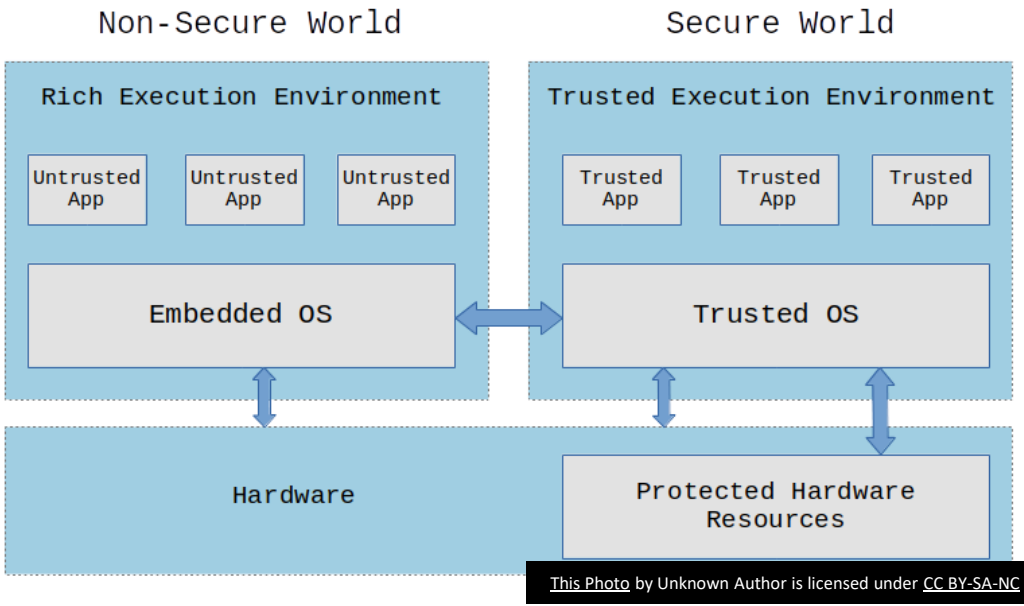


Week 7
Speculative Exploits

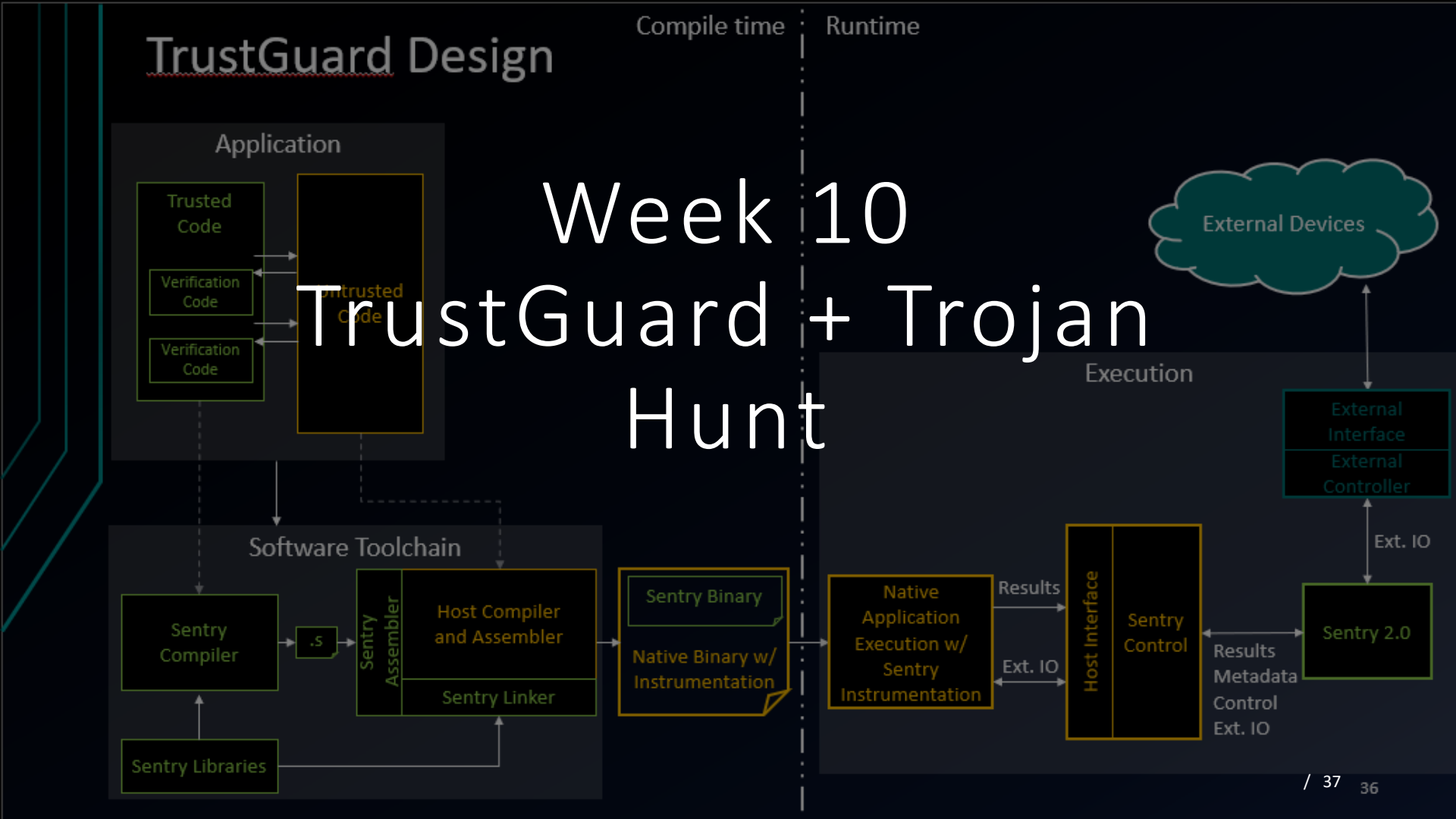
Week 8
Enclaves and Co-Processors



Week 9 Secure Execution



Week 10
TrustGuard + Trojan Hunt



TODOs

- Group Formation + Topic Interest Survey

For Thursday

Physical Attacks: Definition

Physical attacks are attacks that involve penetrating the physical security protecting information systems

[1] Google Images

Physical attacks: Reason

Theft of Service
- E.g. Cable, Satellite TV

Cloning and Overbuilding
- E.g. Headphones

Theft of Information/IP
- E.g. Apple vs. Samsung

Denial of Service
- E.g. Routers

[1] Mohammad Tehranipoor and Cliff Wang. 2011. *Introduction to Hardware Security and Trust*. Springer.
[2] Google Images

Physical Attacks: Categories

Three types of physical attacks:

- Non-Invasive
- Invasive
- Semi-Invasive

[1] Mohammad Tehranipoor and Cliff Wang. 2011. *Introduction to Hardware Security and Trust*. Springer.

Physical Attacks: Non-Invasive*

Do not require preparations of the device under test such as decapsulation or deprocessing
Advantage: easily reproducible, inexpensive, no tamper evidence
Limitations: time consuming, limited capabilities
Example: Wire Taps, USB kill

*Non-destructive is probably a better term IMO

Physical Attacks: Non-Invasive

- Passive
  - Side Channel Attacks (Week 5)
    - Power Analysis
    - Timing Analysis
    - Electromagnetic Emission
    - Sound

Physical Attacks: Non-Invasive

Active

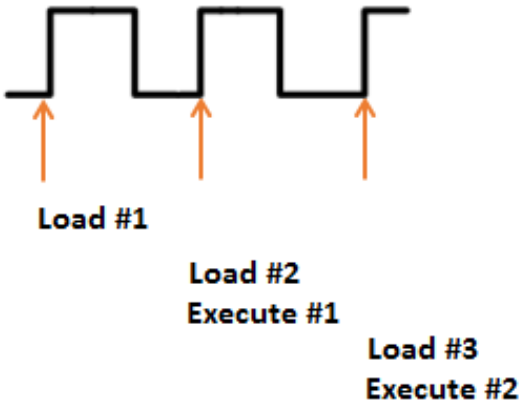
Brute Force / Black Box Attacks

[1] Google Images

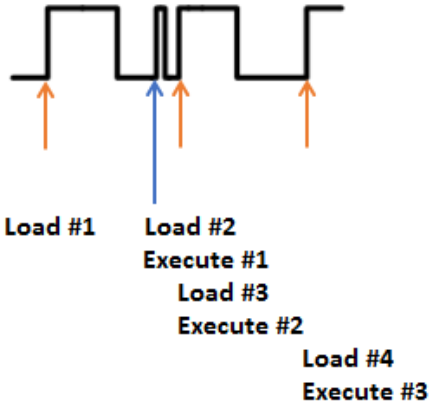
Physical Attacks: Non-Invasive

Active

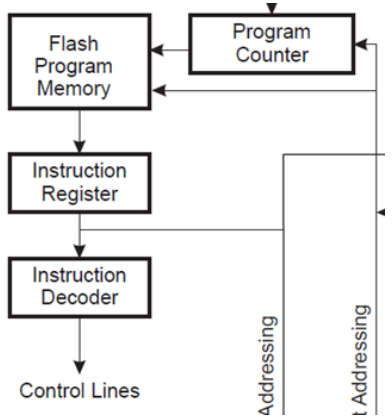
Clock Glitch Attacks



Normal Processor Clock



Glitched Clock



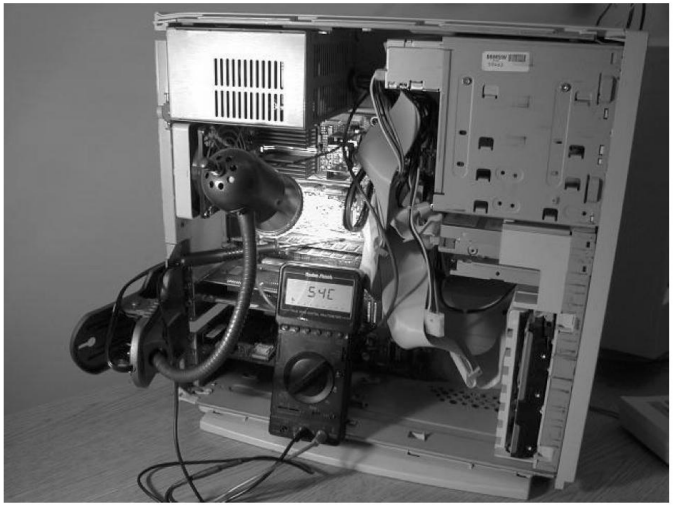
Atmel AVR ATMega328P

[1] ChipWhisperer git documentation Advanced Tutorials

Physical Attacks: Non-Invasive

Active

- Light bulb attack



[1] Sudhakar Govindavajhala and Andrew W. Appel. Using Memory Errors to Attack a Virtual Machine. 2003

Physical Attacks: Non-Invasive

Active

Cold boot attack

[1] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: cold-boot attacks on encryption keys. 2009.

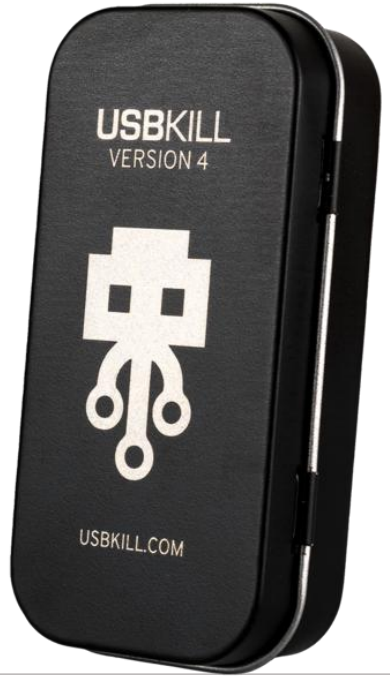
Physical Attacks: Non-Invasive

Active

Power surge attack

DON'T GET ARRESTED

What is your stance on malicious use?
USBKill.com strongly condemns malicious use of its products.
The USB Killer is developed and sold as a testing device. Use of the device can permanently damage hardware. Customers agree to the terms and conditions of sale, and acknowledge the consequences of use.



[1] http://www.zdnet.com/article/now-you-can-buy-a-usb-stick-that-destroys-laptops/
[2] https://www.usbkill.com/

Physical Attacks: Non-Invasive

Physical access attacks

Evil Maid Attack / Server Room Hack

[1] Google Images

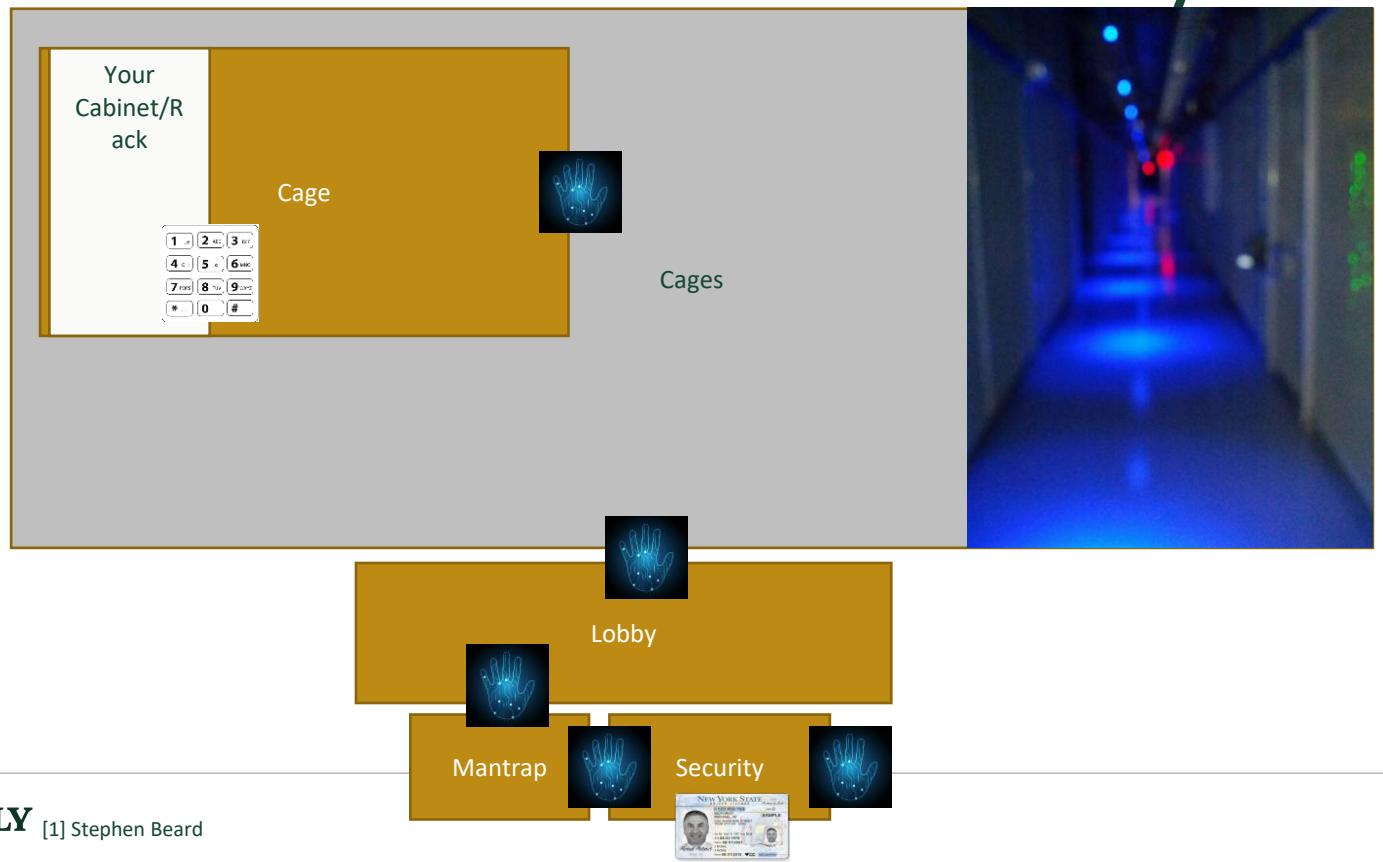
“Evil Maid” Attack

Originally coined by computer security researcher Joanna Rutkowska in 2009

Original attack is an example

Any physical access can lead to almost undetectable modifications

Typical Colo (Equinix) Data Center Security



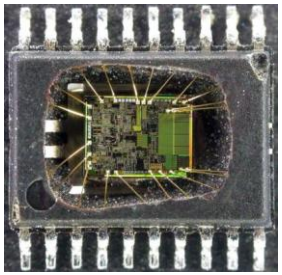
Physical Attacks: Invasive

Require expensive decapsulation and deprocessing equipment, knowledgeable attackers and time

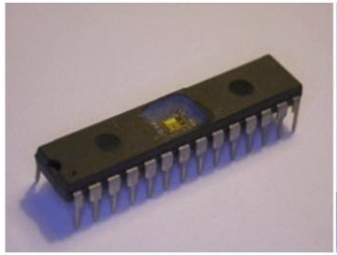
Advantages: Almost unlimited capabilities

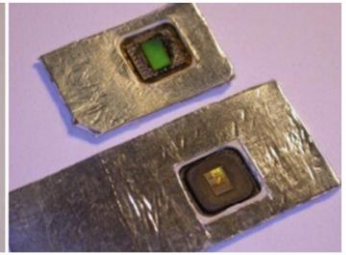
Limitations: Time consuming, Expensive, Leave tamper evidence, May be destructive

Decapsulation



Manual





[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*
[2] Google Images

Physical Attacks: Invasive

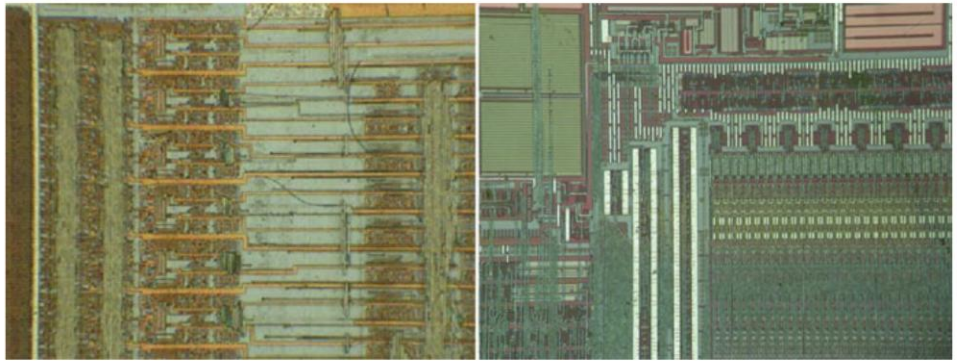
Sample Preparation

Deprocessing: removing layers of the circuit to gain access to deeper layers

Wet chemical etching

Plasma(dry) etching

Mechanical Polishing

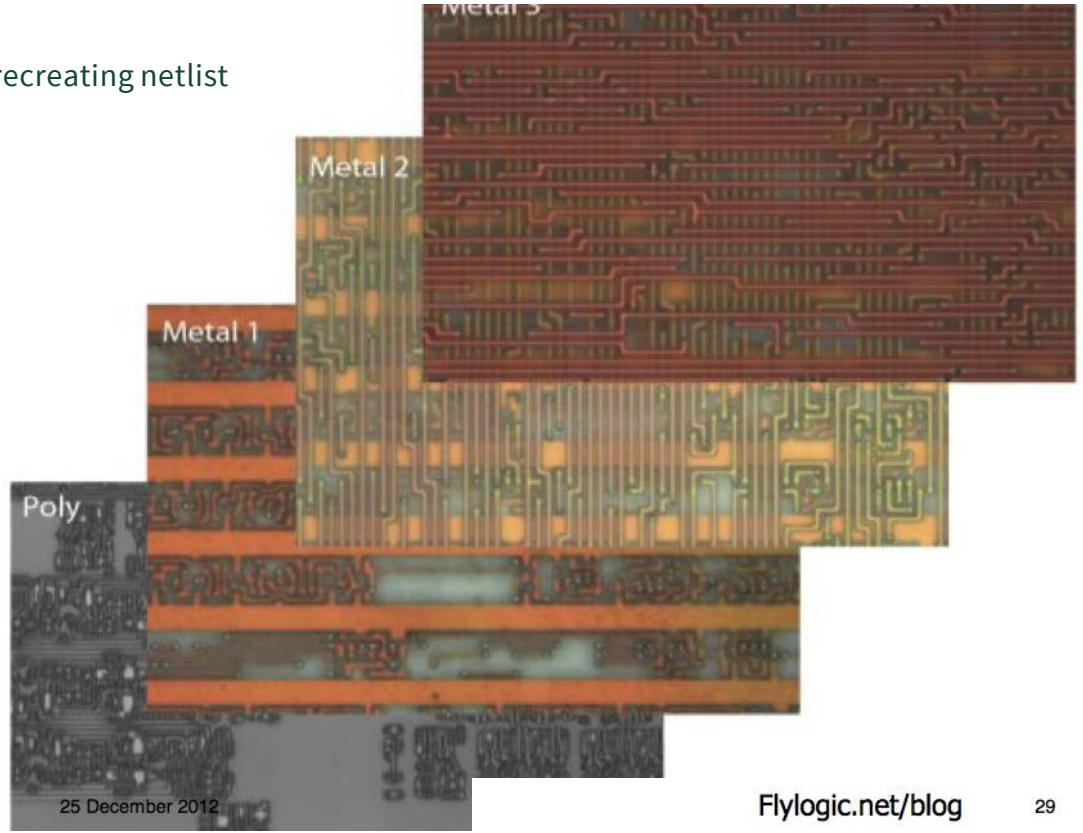


[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*

Physical Attacks: Invasive

Reverse Engineering

Remove and photograph all layers, recreating netlist

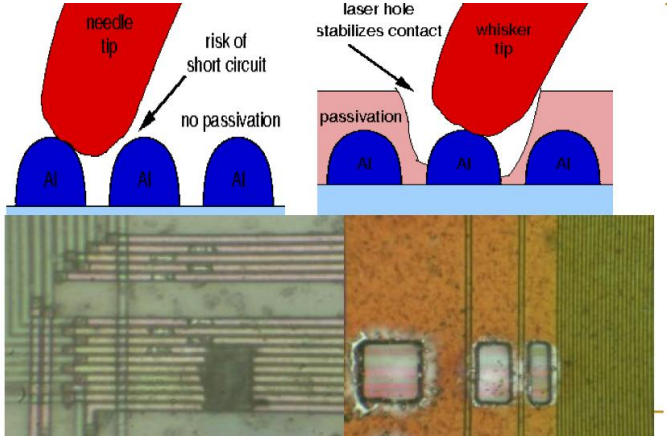


[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*

Physical Attacks: Invasive

Microprobing

- Eavesdrop on internal signals
- Inject test signals

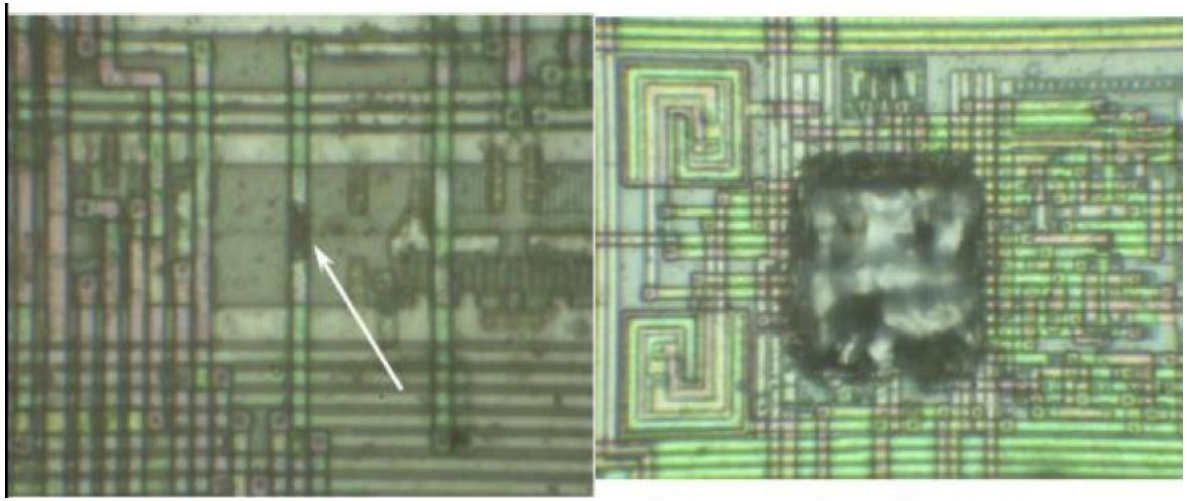


[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*

Physical Attacks: Invasive

Chip Modification

Disable security protection circuitry



[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*

Physical Attacks: Semi-Invasive

In-between, similar to invasive attacks in that they require decapsulation, but no deprocessing

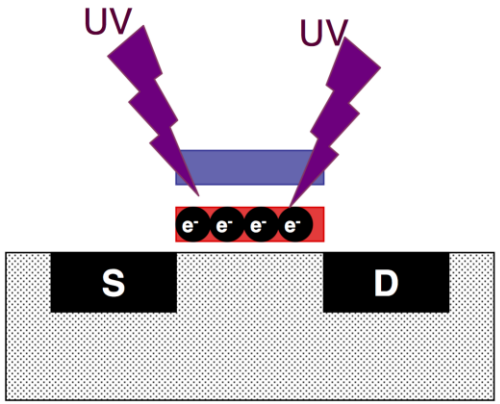
Advantages: Almost unlimited capabilities, Inexpensive

Limitations: Time consuming, Leave tamper evidence.

Physical Attacks: Semi-Invasive

UV Light Attacks

- Use UV light and heat to inject a targeted fault
- Locating the security fuse
- Resetting it to read out memory content

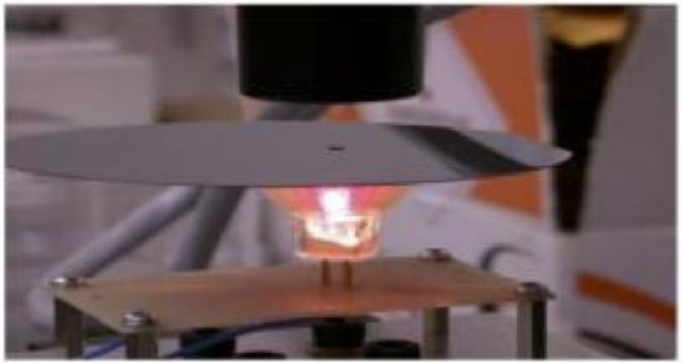


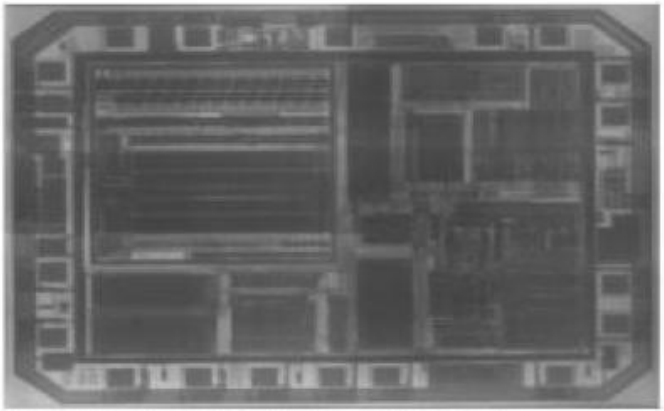
[1] Jacques J. A. Fournier and Philippe Loubet-Moundi. Memory Address Scrambling Revealed Using Fault Attacks. *2010*

Physical Attacks: Semi-Invasive

Advanced Imaging Techniques

Observe with IR light from rear side





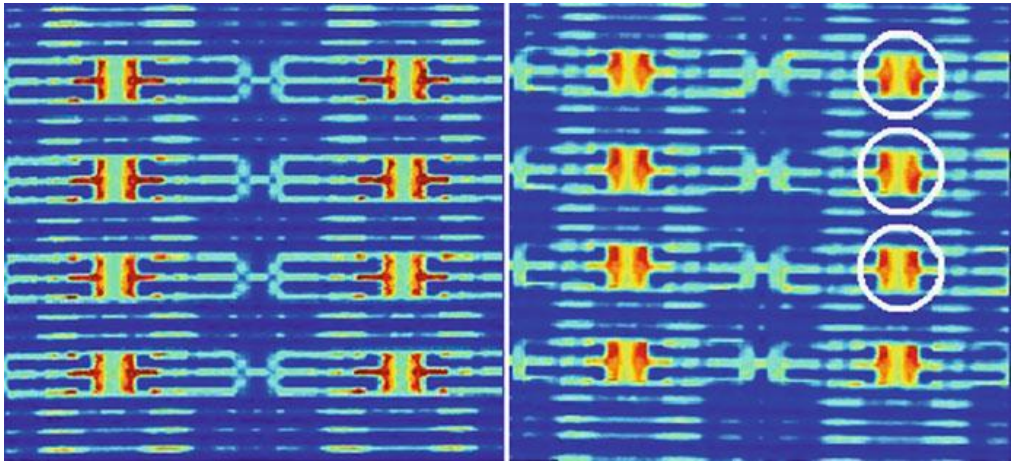
[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*

Physical Attacks: Semi-Invasive

Active Photon Probing (of a memory cell)

- Ionize regions of IC
- Laser scanning

Power Off



1 1 0 0

1 1 1 0

1 1 1 1

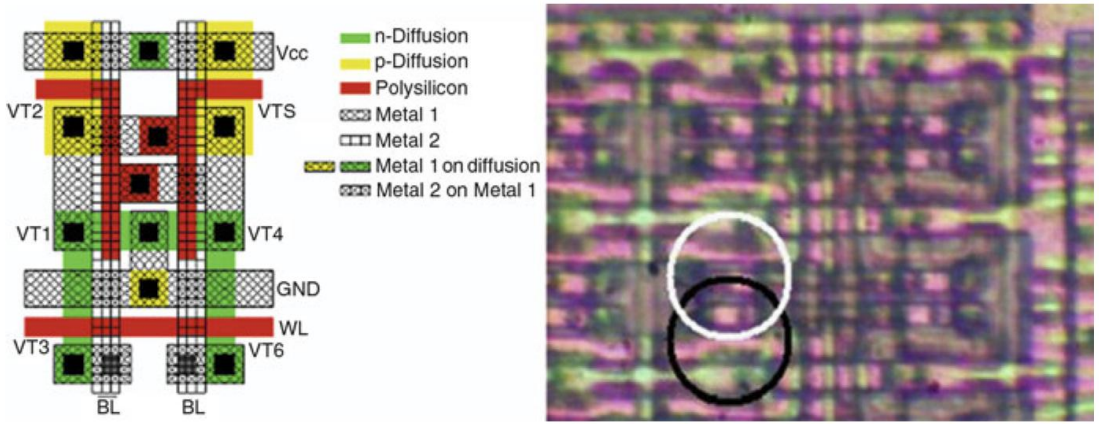
1 1 1 1

[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*

Physical Attacks: Semi-Invasive

Optical Fault Injection

Change bit in SRAM



[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*

Now you've learned how attacks work / can you defend against physical attacks?

Can you hack  ?

Can you hack  ?

Can you hack  ?

Physical Tamper Resistance

Resistance to tampering (intentional malfunction or sabotage) by either the normal users of a product, package, or system or others with physical access to it.

Ranges from special screws to complex crypto processors

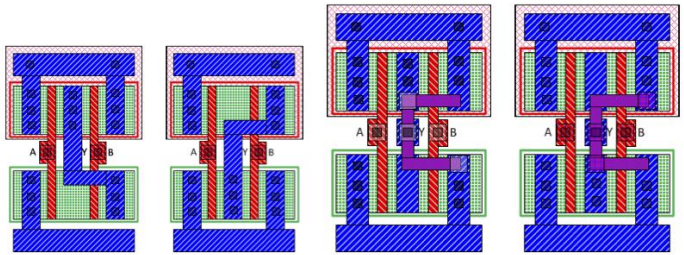
- The screws on your laptop
- IBM 4758

[1] Mohammad Tehranipoor, 2012, ECE 4451/5451: *Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance*
[2] Google Images

Countermeasures to ensure PTR

Bus Scrambling

IC Camo

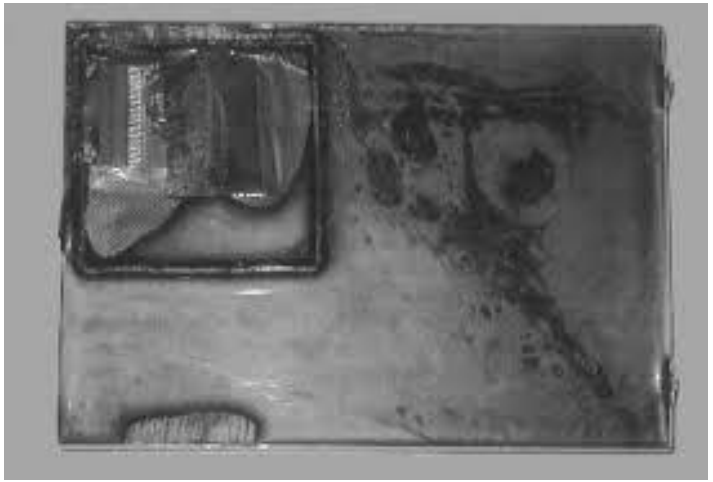


Normal NAND | Normal NOR | Camouflaged NAND | Camouflaged NOR

[1] Jeyavijayan Rajendran, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri. 2013. Security analysis of integrated circuit camouflaging.

Countermeasures to ensure PTR

Top-layer Sensor Meshes



- Tamper Sensor

Voltage Sensor

Light Sensor

Clock Frequency Sensor

Summary

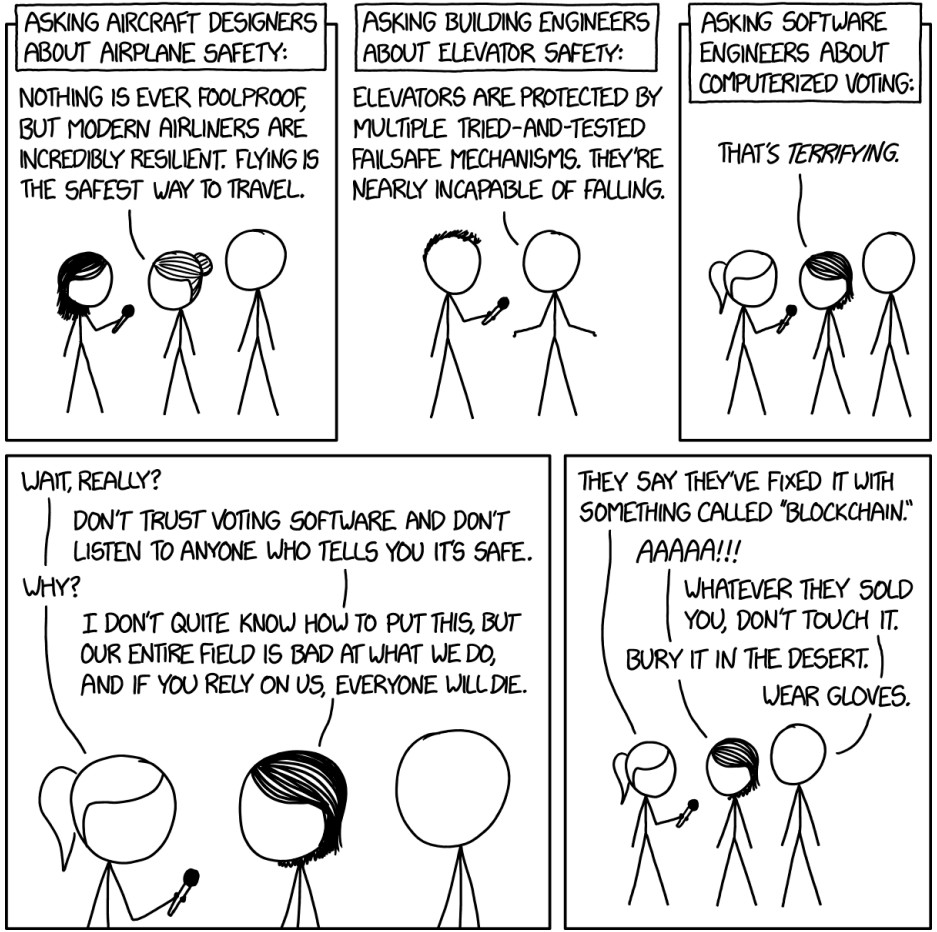
- Physical Attacks
  - From $1 screw drivers to $100,000 workstations
  - Non-invasive attacks
  - Invasive attacks
  - Semi-invasive attacks
- Physical Tamper Resistance
  - From $0.1 screws to $5,000 secure processors
  - Bus Scrambling
  - IC Camouflaging
  - Sensors

Reading Assignments

Read the paper on Cold Boot and Andrew Appel's retrospective on his involvement in voting machine hacking. Both are on Canvas.

Before Thursday's class, complete the short response reading assignment "quiz"

Group formation survey and topic interest questionnaire will be sent out shortly*


ASKING AIRCRAFT DESIGNERS ABOUT AIRPLANE SAFETY:
NOTHING IS EVER FOOLPROOF, BUT MODERN AIRLINERS ARE INCREDIBLY RESILIENT. FLYING IS THE SAFEST WAY TO TRAVEL.
ASKING BUILDING ENGINEERS ABOUT ELEVATOR SAFETY:
ELEVATORS ARE PROTECTED BY MULTIPLE TRIED-AND-TESTED FAILSAFE MECHANISMS. THEY'RE NEARLY INCAPABLE OF FALLING.
ASKING SOFTWARE ENGINEERS ABOUT COMPUTERIZED VOTING:
THAT'S TERRIFYING.
WAIT, REALLY?
DON'T TRUST VOTING SOFTWARE. AND DON'T LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.
WHY?
I DON'T QUITE KNOW HOW TO PUT THIS, BUT OUR ENTIRE FIELD IS BAD AT WHAT WE DO, AND IF YOU RELY ON US, EVERYONE WILL DIE.
THEY SAY THEY'VE FIXED IT WITH SOMETHING CALLED "BLOCKCHAIN."
AAAAA!!!
WHATEVER THEY SOLD YOU, DON'T TOUCH IT.
BURY IT IN THE DESERT.
WEAR GLOVES.

References

[1] Mohammad Tehranipoor and Cliff Wang. 2011. Introduction to Hardware Security and Trust. Springer.
[2] Mohammad Tehranipoor, 2012, ECE 4451/5451: Introduction to Hardware Security and Trust: Physical Attacks and Tamper resistance
[3] Jeyavijayan Rajendran, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri. 2013. Security analysis of integrated circuit camouflaging
[4] Jacques J. A. Fournier and Philippe Loubet-Moundi. Memory Address Scrambling Revealed Using Fault Attacks. *2010*
[5] ChipWhisperer git documentation Advanced Tutorials
[6] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: cold-boot attacks on encryption keys. 2009.
[7] Sudhakar Govindavajhala and Andrew W. Appel. Using Memory Errors to Attack a Virtual Machine. 2003