

# Side-Channel Analysis

## *Hardware Hacking from a Distance*

Ben Janis

March 22, 2023



# MITRE

SOLVING PROBLEMS  
FOR A SAFER WORLD™



# OUR VISION

pioneering for  
a better future





what's a new way to cure cancer?  
**THE ANSWER IS IN THE DATA**

# OUR DIFFERENTIATED VALUE

- Mission-Driven
- Innovative Approach
- Objective Insight
- Unique Vantage Point
- Technical Know-how
- Pioneering Together





**NEXT LEVEL INNOVATION**

requires extraordinary people

# OUR IMPACT

## AEROSPACE & TRANSPORTATION

AIRLINE TRAFFIC COLLISION  
AVOIDANCE

## CYBERSECURITY

THREAT-INFORMED DEFENSE

## TECHNOLOGY & INNOVATION

PROTOTYPES &  
DEMONSTRATION

## NATIONAL SECURITY

GPS/PNT

Reliability, Accuracy, Resiliency

## HEALTH & HUMAN SERVICES

DATA STANDARDS & INTEROPERABILITY

## HOMELAND SECURITY

PROTECTING OUR BORDERS

A woman with long dark hair, wearing a red top, is holding a young child with light brown hair in a purple hoodie. They are both looking at a touch screen kiosk in what appears to be a public space like a subway station. The woman is pointing at the screen with her right hand. The background is blurred, showing other people and city lights.

MITRE touches your life  
**EVERY DAY**

# eCTF Embedded Capture the Flag

Annual embedded security competition

Teams design, build, and attack secure  
embedded systems

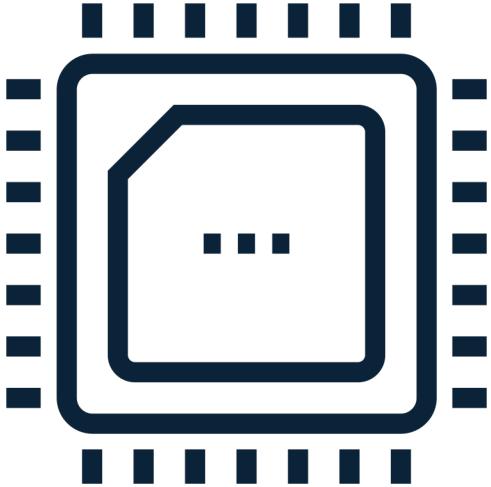
Over the spring semester

Opportunity for course credit

Excellent opportunity



# Unique Competition Design



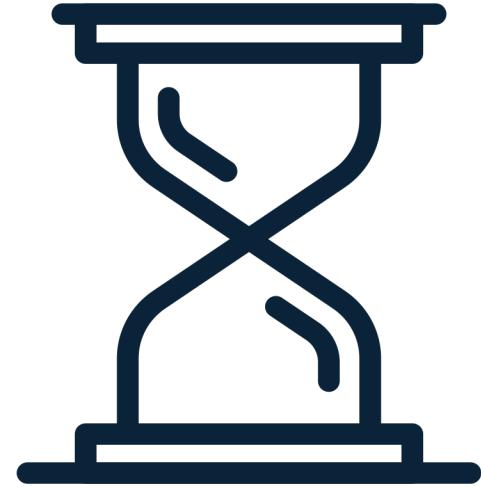
## Focus on Embedded

Physical and emulated hardware opens scope to physical and proximal attacks



## Attack and Defend

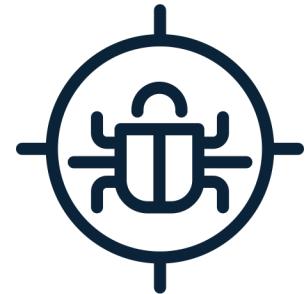
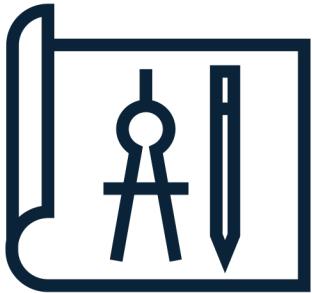
Students wear both “hats” by acting as both red team and blue team



## Extended Time

Semester-long competition opens door to advanced attacks and countermeasures

# Competition Phases



## Design Phase

Teams design and implement systems that meet security and functionality requirements

## Handoff

Organizers test each design for functionality

## Attack Phase

Teams analyze and attack each other's designs for points

# Real-World **Scenarios**



Smart Door Lock



ATM Machine



Self-Driving Car



Drone Delivery



Video Game Player



Avionics

# Why do the eCTF?

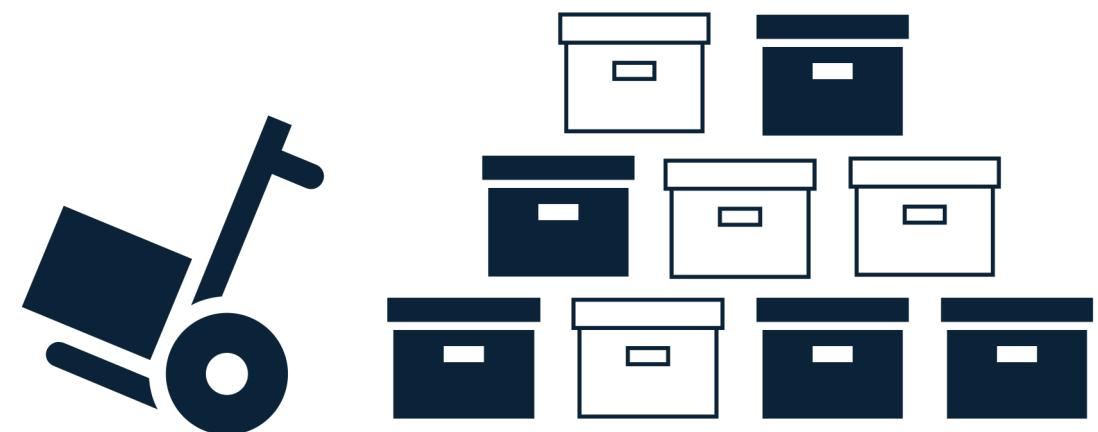
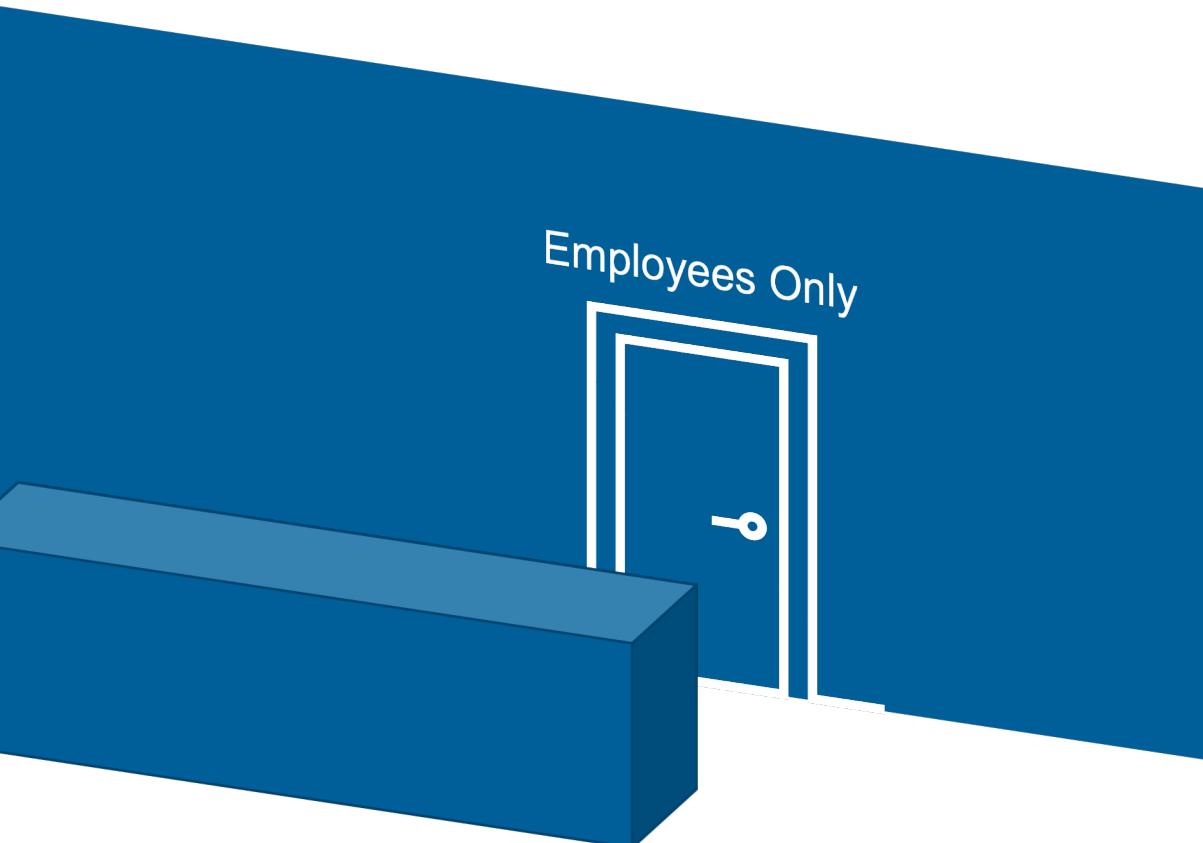
- **Unparalleled hands-on experience**
  - Crypto/protocol design
  - Low-level C programming
  - Real-world offensive security
  - Project management
- **Career advancement**
  - Looks great on a resume
  - Massive talent supply shortage in embedded security
- **It's fun! (but a lot of work)**

# **What is a Side-Channel?**

# Side-Channel Example: Store Backroom

By only asking employees for items in the back and without going in yourself, figure out:

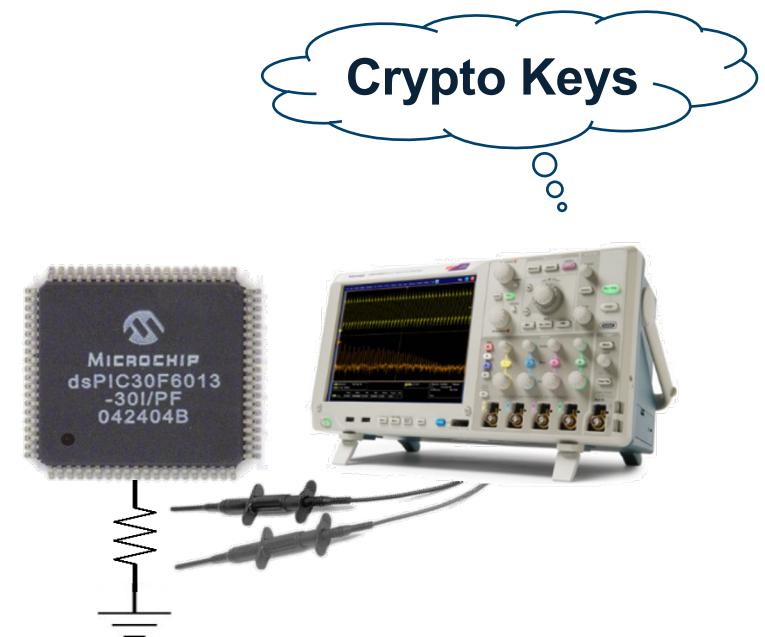
How is the backroom organized?  
Where are different items located?  
What shelves are items stored on?  
How many items per bulk box?



# Side-Channel Analogy



Acoustic Side-Channel



Power Side-Channel

Side-channel analysis (SCA) leverage *unavoidable side-effects* of performing computation

# Side-Channel Attacks

## SCA commonly used to:

- Reverse engineer system operation
- Extract information (e.g., keys)
- Monitor and validate system behavior

### Execution Time

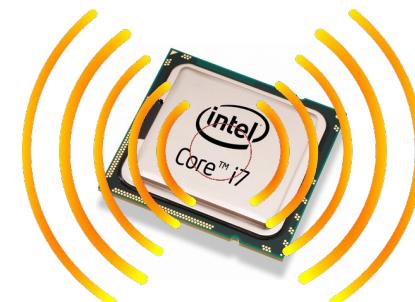


<https://commons.wikimedia.org/wiki/File:Dtjohnnymonkey-Stopwatch-no-shading.svg>



### Instantaneous Power

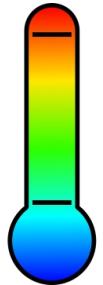
### EM Radiation



<http://www.itp.net/573498-intel-core-i7-920>

<https://www.kisspng.com/png-light-electromagnetic-spectrum-electromagnetic-rad-1233022/>

### Thermal



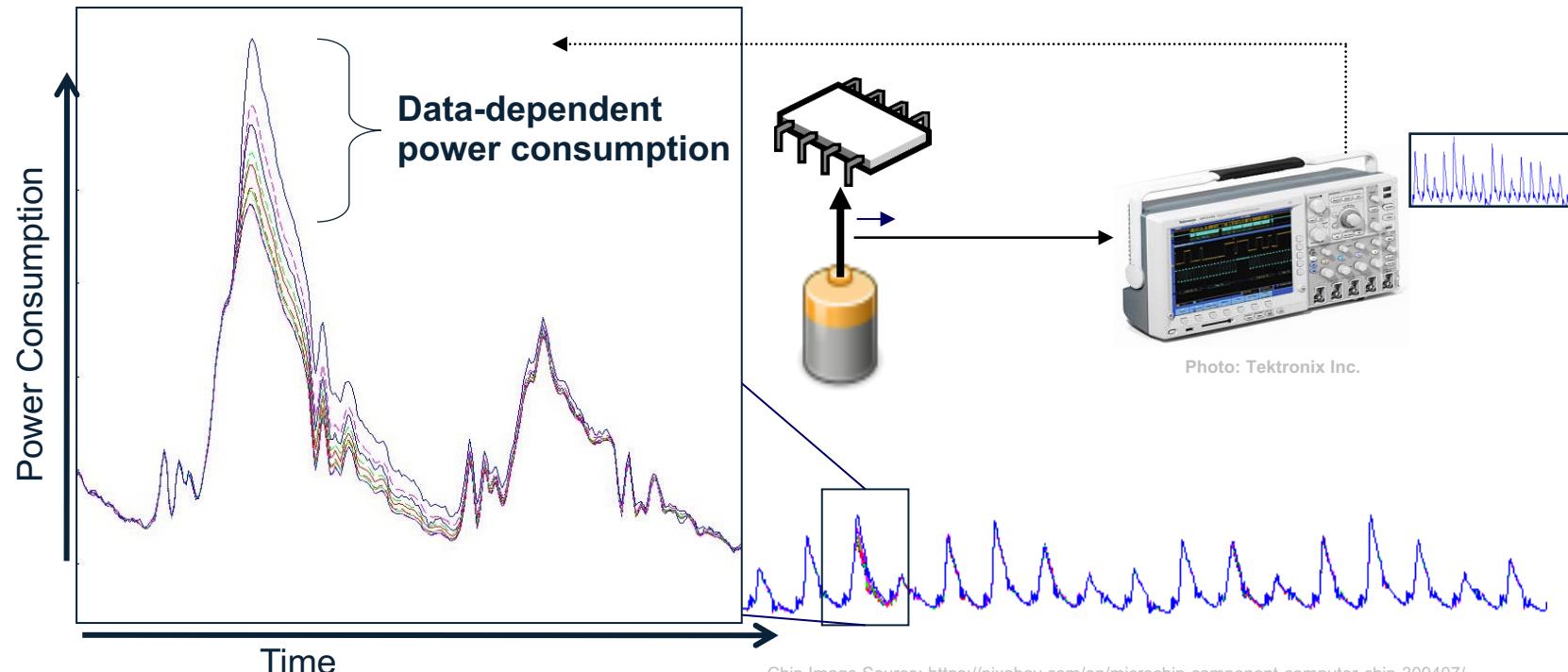
### Acoustic Vibrations

[https://commons.wikimedia.org/wiki/File:1989\\_Loma\\_Prieta\\_earthquake\\_seismogram.jpg](https://commons.wikimedia.org/wiki/File:1989_Loma_Prieta_earthquake_seismogram.jpg)

# Side-Channel Capture

**Side-channel leakage is captured during normal device operation**

- Target device is instrumented with sensors (e.g., current monitor)
- Device commanded to perform its sensitive operation
- Captured side-channel data is stored along with the corresponding inputs and outputs



Chip Image Source: <https://pixabay.com/en/microchip-component-computer-chip-309407/>

Battery Image Source: Tango Desktop Project

© 2018 MITRE Corporation

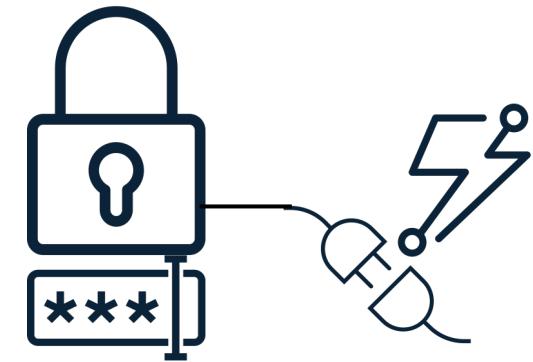
# Side-Channel Workshop: PIN Lock

## Scenario:

- A door is secured by a smart door lock
- We want to figure out the 4-digit PIN to open it

## Data available to us:

- Success / failure of PIN guess
- Power consumption of the lock device
- Knowledge that the lock uses strcmp



# Side-Channel Workshop: strcmp

strcmp(correct\_pin, incorrect\_pin)

|              |   |   |   |   |
|--------------|---|---|---|---|
| Correct PIN: | 1 | 2 | 3 | 4 |
|              | ? | > |   |   |
| Pin Guess:   | 1 | 1 | 1 | 1 |

# Side-Channel Workshop: strcmp

strcmp(correct\_pin, incorrect\_pin)

|              |   |   |   |   |
|--------------|---|---|---|---|
| Correct PIN: | 1 | 2 | 3 | 4 |
|              | = | < |   |   |
| Pin Guess:   | 1 | 3 | 1 | 1 |

*How could we exploit this?*

# Side-Channel Workshop

<https://mybinder.org/v2/gh/janisbent/sc-lab/v3.1?filepath=lab.ipynb>

<https://bit.ly/407kM2A>

# LOOKING FOR AN INTERNSHIP?

- Over 600 interns
- Do impactful work
- High school through PhD
- Locations--McLean, VA; Bedford, MA and sites across the US
- 1/3 return for additional summers
- 50%+ get hired when graduated
- Spend 8 hours paid learning about Artificial Intelligence, Embedded Security or Data Science
- Weekly meet-ups, mentoring program, intern expo



**MITRE**  
SOLVING PROBLEMS  
FOR A SAFER WORLD®

# LOOKING FOR A JOB AFTER GRADUATION?

Our work spans AI, cybersecurity, health, quantum computing, aerospace, autonomous vehicles and everything in between.



Impactful work | benefits to include:

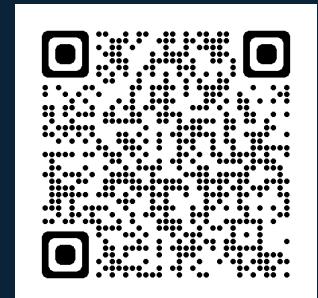
- 22 days paid-time off
- Flexible workplace
- Continuous growth opportunities
- Generous retirement match
- Education assistance
- School loan repayment
- Parental leave, adoption assistance, daycare subsidies

**MITRE** | SOLVING PROBLEMS  
FOR A SAFER WORLD®

# Interested in applying to MITRE?

- Computer Science and Software Engineering
- Cybersecurity
- Data Science / Math / Statistics / Operations Research
- Electrical Engineering / Computer Engineering
- Systems Engineering
- Mechanical Engineering
- Aerospace Engineering
- Physics
- Health
- Behavioral Sciences
- Economics, Government, Policy Sciences
- And more...

Check out our Intern and New Grad Job opportunities



Ben Janis

[btjanis@mitre.org](mailto:btjanis@mitre.org)

 [linkedin.com/in/benjanis](https://linkedin.com/in/benjanis)

**MITRE** | SOLVING PROBLEMS  
FOR A SAFER WORLD™