ARM KNOWLEDGE LAB: DESIGNING THE FUTURE

DAY 1

Introduction to Side Channel Attacks on Embedded Systems

Liam Craig, New AE Technology

Arm Knowledge Lab:
Three short and compact sessions

Day 1

Secure by Design – From Threats to Trusted Devices

Day 2

AI at the Edge – Building Smarter Embedded Systems

Day 3

Safety-Critical Systems – Engineering Reliability

Find more presentations from our Arm Knowledge Lab:
https://www2.hitex.com/arm-knowledge-lab-2026-download

Introduction to Side Channel Attacks

Sometimes bypassing encryption is easy AND cheap

Speaker and Company Background

Liam Craig: Holds an Electrical Engineering Degree from Dalhousie University. Background in PCB design and project management. Has built embedded security hardware, autonomous survey vessels, and low-cost renewable energy systems. Director of Engineering at NewAE.

NewAE Technology

Small company of 8 people based in Nova Scotia, Canada. Founded by Colin O'Flynn, started as part of his PhD research. Manufacturers of ChipWhisperer and related products.

Side-Channel vulnerabilities

Easy to overlook, easy to exploit?

- Very Few Groups have:
  - The Awareness
  - The Knowledge
  - The Tools
  - The Time

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local

Watch a Tesla Model S get stolen with a key fob hack

A clear look at a potential vulnerability for cars with keyless entry

By Sean O'Kane | @sokane1 | Oct 22, 2018, 10:24am EDT

SHARE

MOST READ

Oppo's 10x optical zoom system really works

Microsoft

Microsoft is teaming up with America's second-largest grocery chain to fend off Amazon

Tesla's cars may be high-tech, but that doesn't mean they're foolproof when it comes to security. This fact is on display in a new video that shows, without the proper protections in place, that it's not that hard to steal one of the company's cars.

The video shows two thieves skulking around a Model S at night while it's parked in a driveway in the UK. Using a tablet and a phone in

The Ransomware Attack That Locked Hotel Guests Out of Their Rooms

This is a good demonstration of why electronic systems need physical backups.

By JOSEPHINE WOLFF
FEB 01, 2017 • 2:09 PM

Hacking

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

mbined fault injection and real-time side-channel analysis for Android Secure-Boot bypassing

ment Fanjas, Clément Gaine, Driss Aboulkassimi, Simon Pontié, Olivier Potin

Why Light Bulbs May Be the Next Hacker Target

The Internet of Things, activated through apps, promises tremendous convenience to homeowners. But it may also prove irresistible to hackers.
Carlos Gonzalez for The New York Times

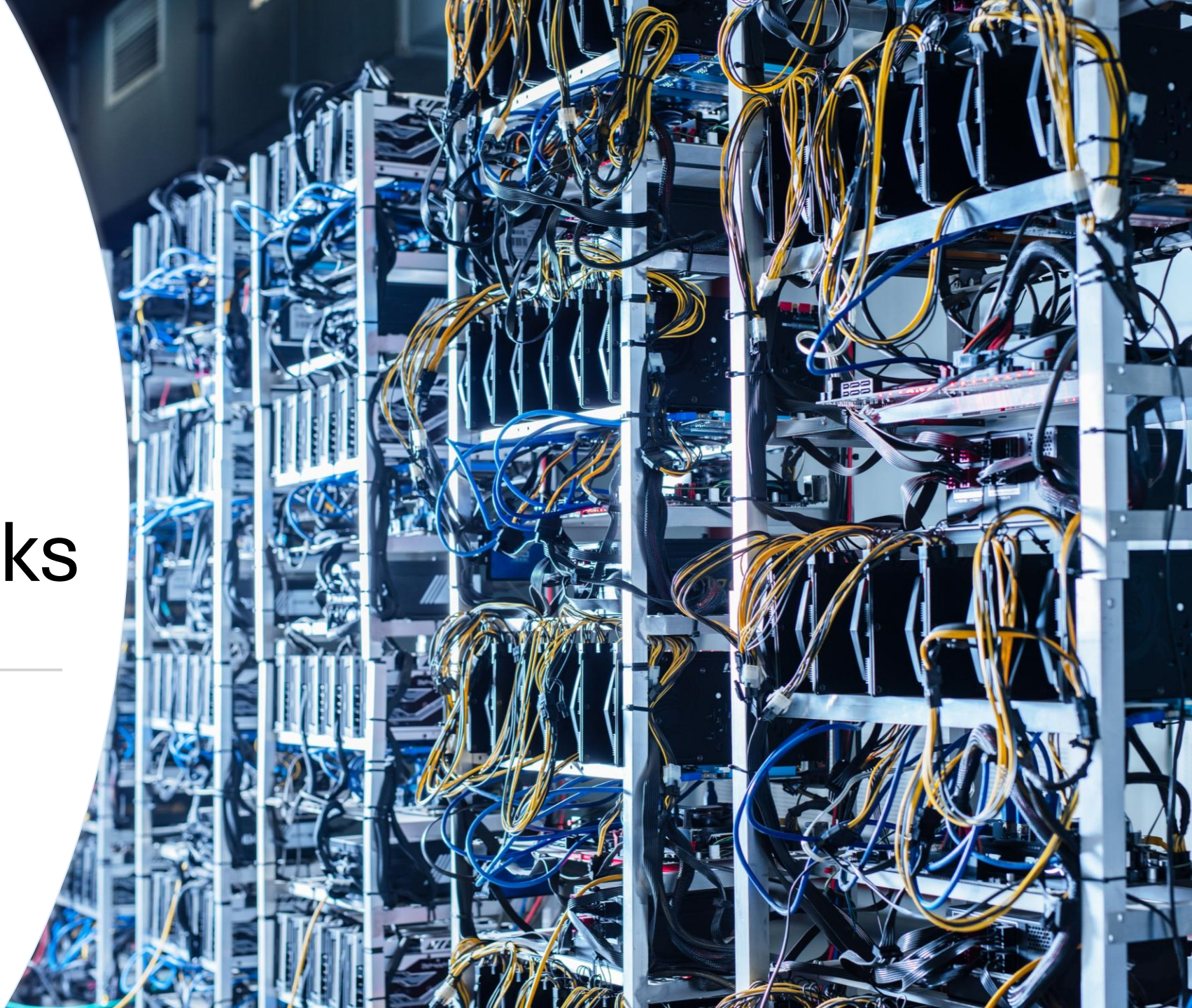
By John Markoff

Nov. 3, 2016

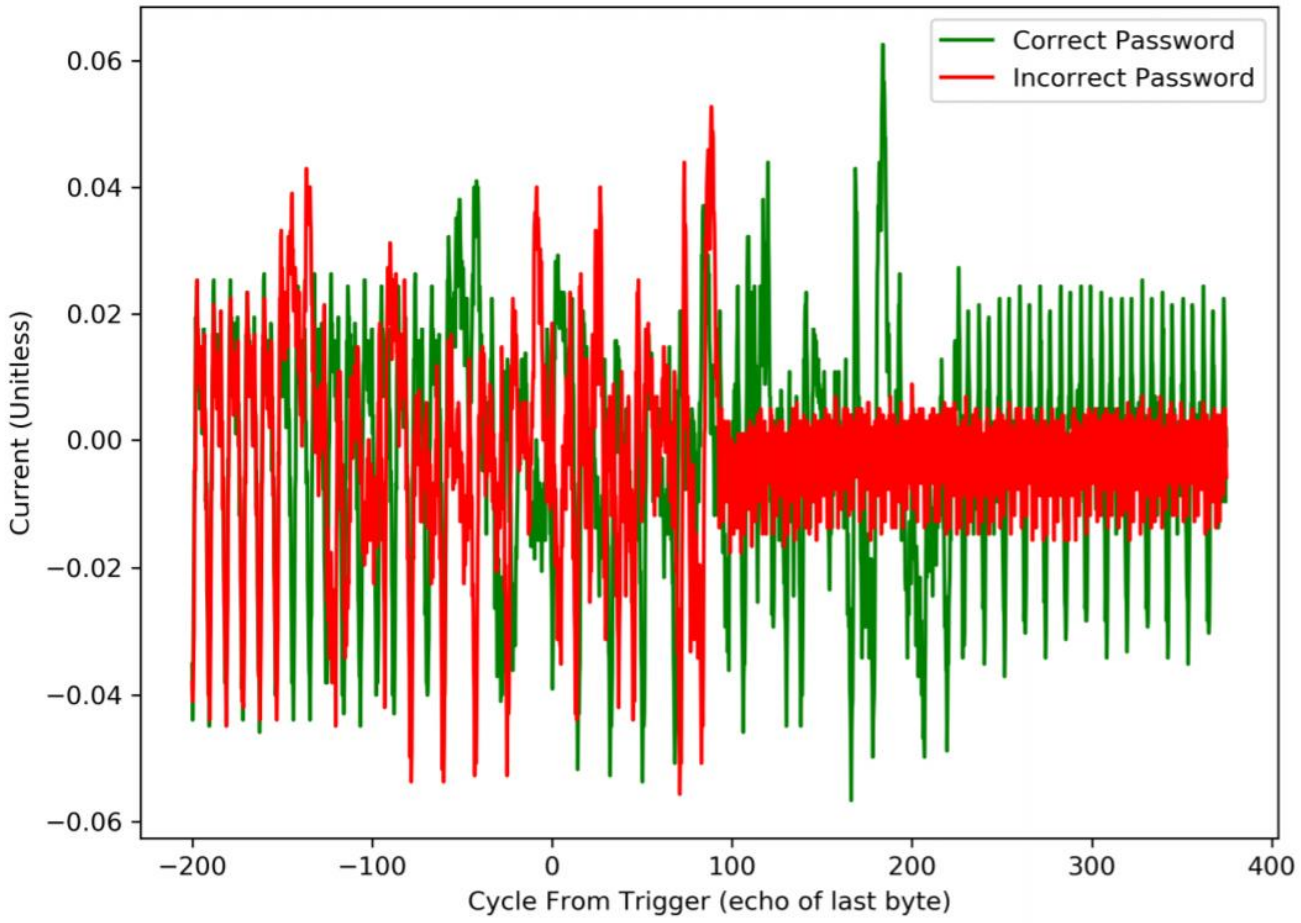
SAN FRANCISCO — The so-called Internet of Things, its proponents argue, offers many benefits: energy efficiency, technology so

Theory of Side Channel Attacks

Computers are physical things

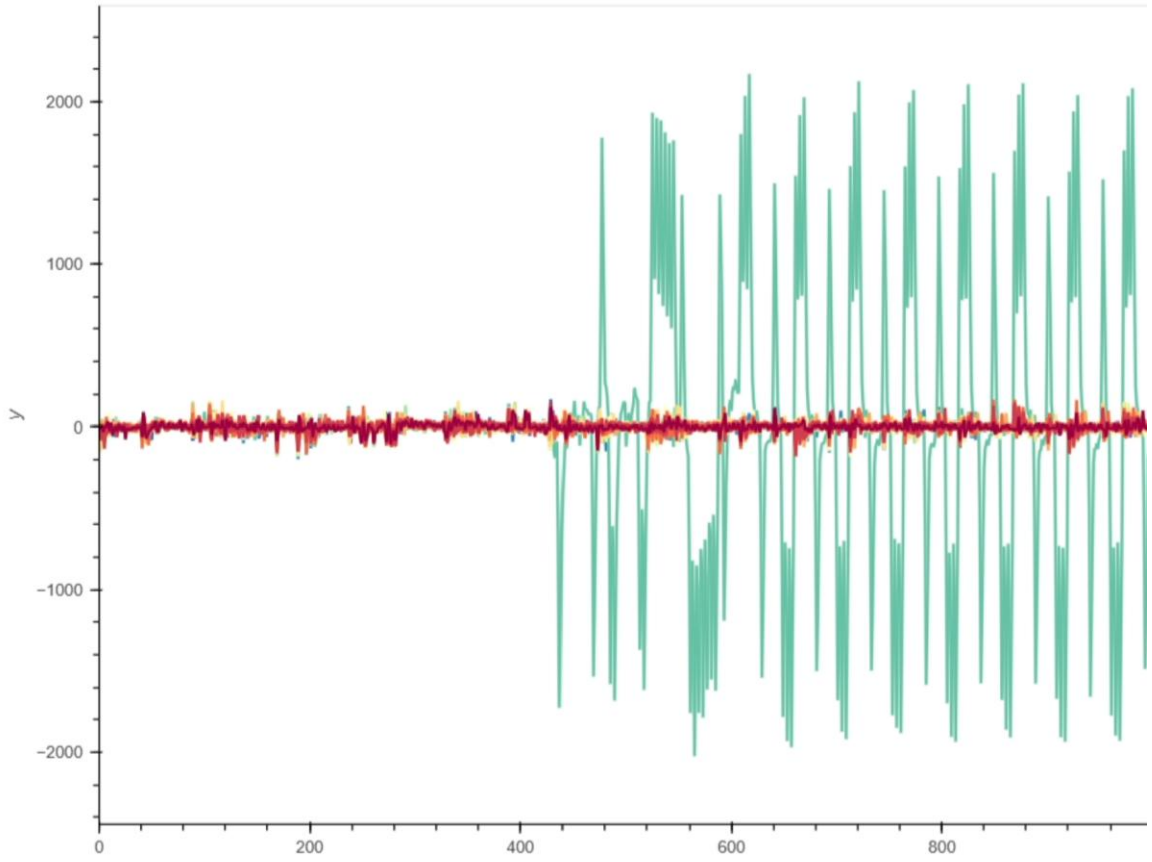


SPA of Code Flow



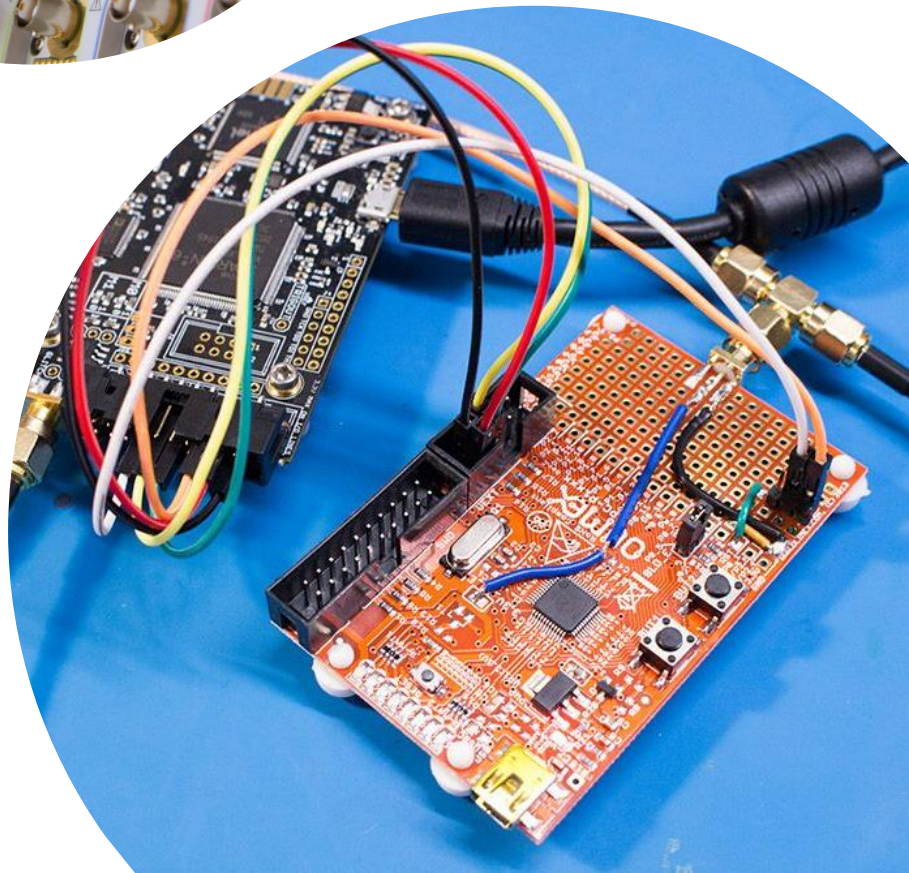
SPA password crack

```
//Get password
my_puts("Please enter password to continue: ");
my_read(passwd, 32);

uint8_t passbad = 0;

trigger_high();

for(uint8_t i = 0; i < sizeof(correct_passwd); i++){
    if (correct_passwd[i] != passwd[i]){
        passbad = 1;
        break;
    }
}
```



Non-obvious tricks and tips

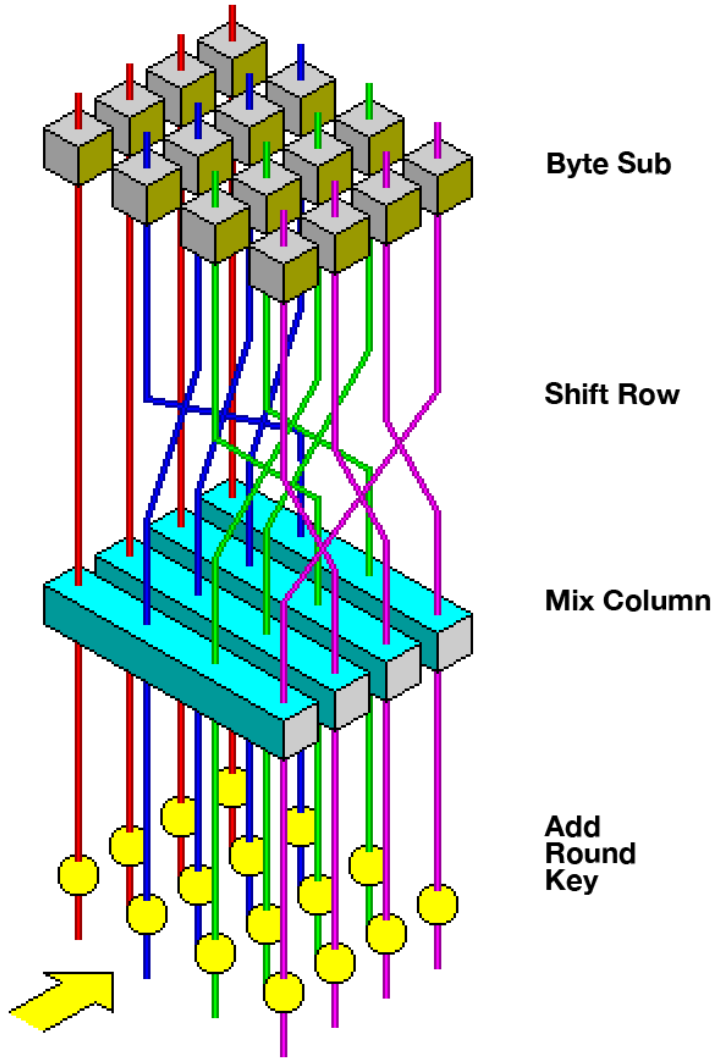
- Synchronous capture
- Physical access is usually but not always required
- Emissions can be measured through a shunt, wirelessly, or even through exposed interfaces
- Knowing or controlling the input (attempted password, encryption key, Encrypted SPI read)



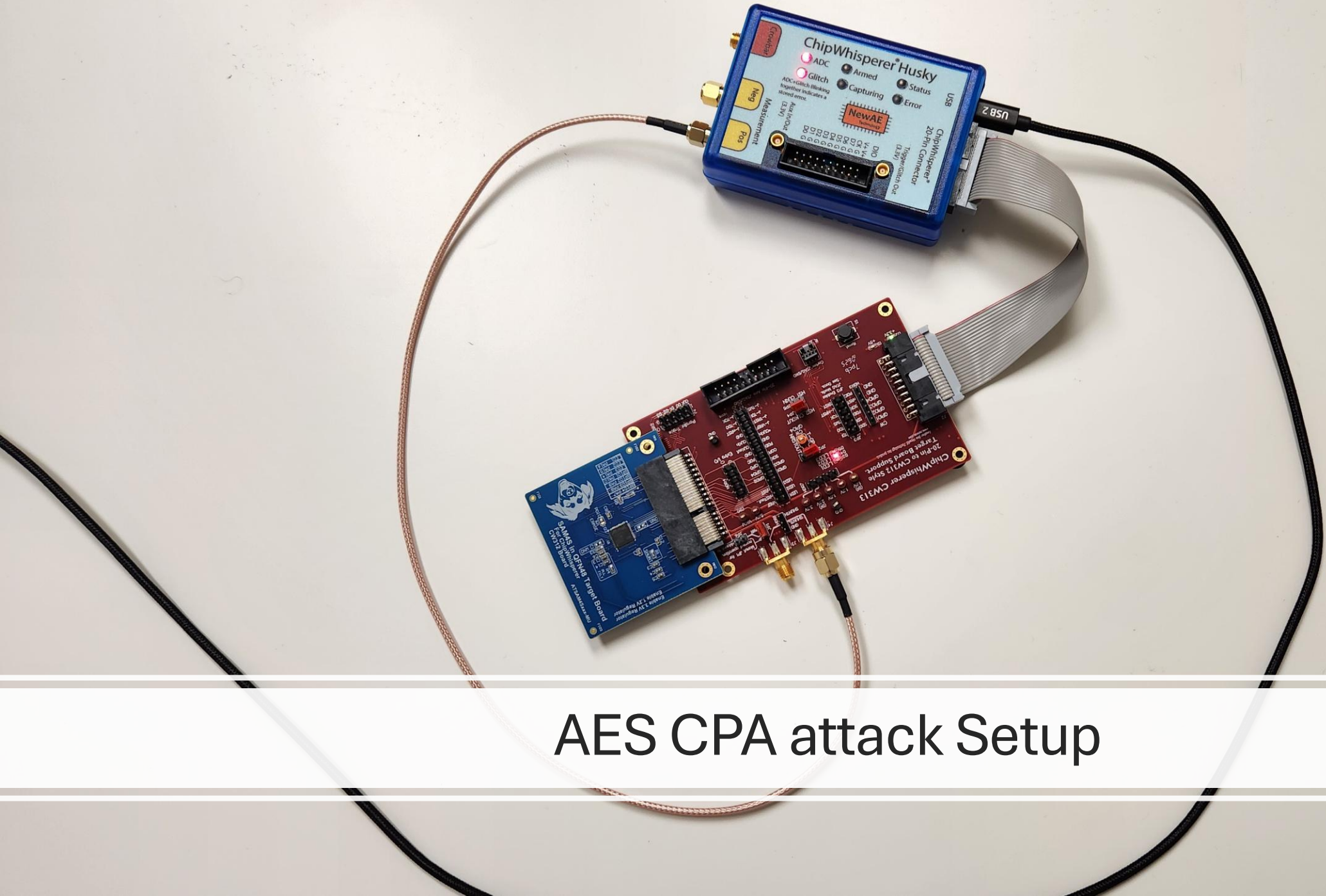
What about actual encryption?

Correlation Power Analysis

- Leakage model
  - Relating operations to emissions (leakage)
  - Knowing how the encryption process works
- Knowing one of the inputs
- Gathering data for different inputs
- Correlating inputs to model expectations
- Testing the result



AES128 Diagram by John Savard

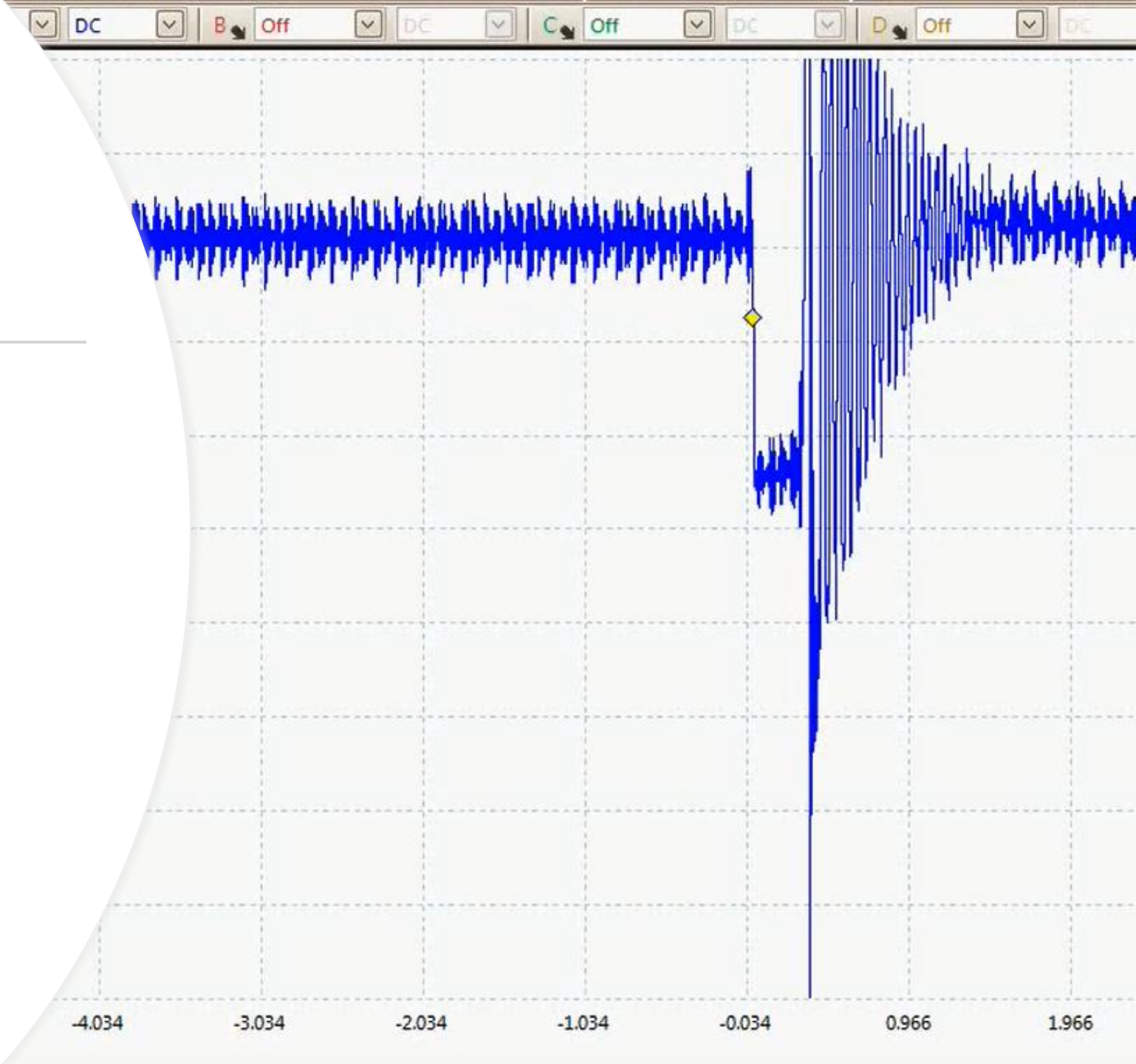


AES CPA attack Setup

Fault injection

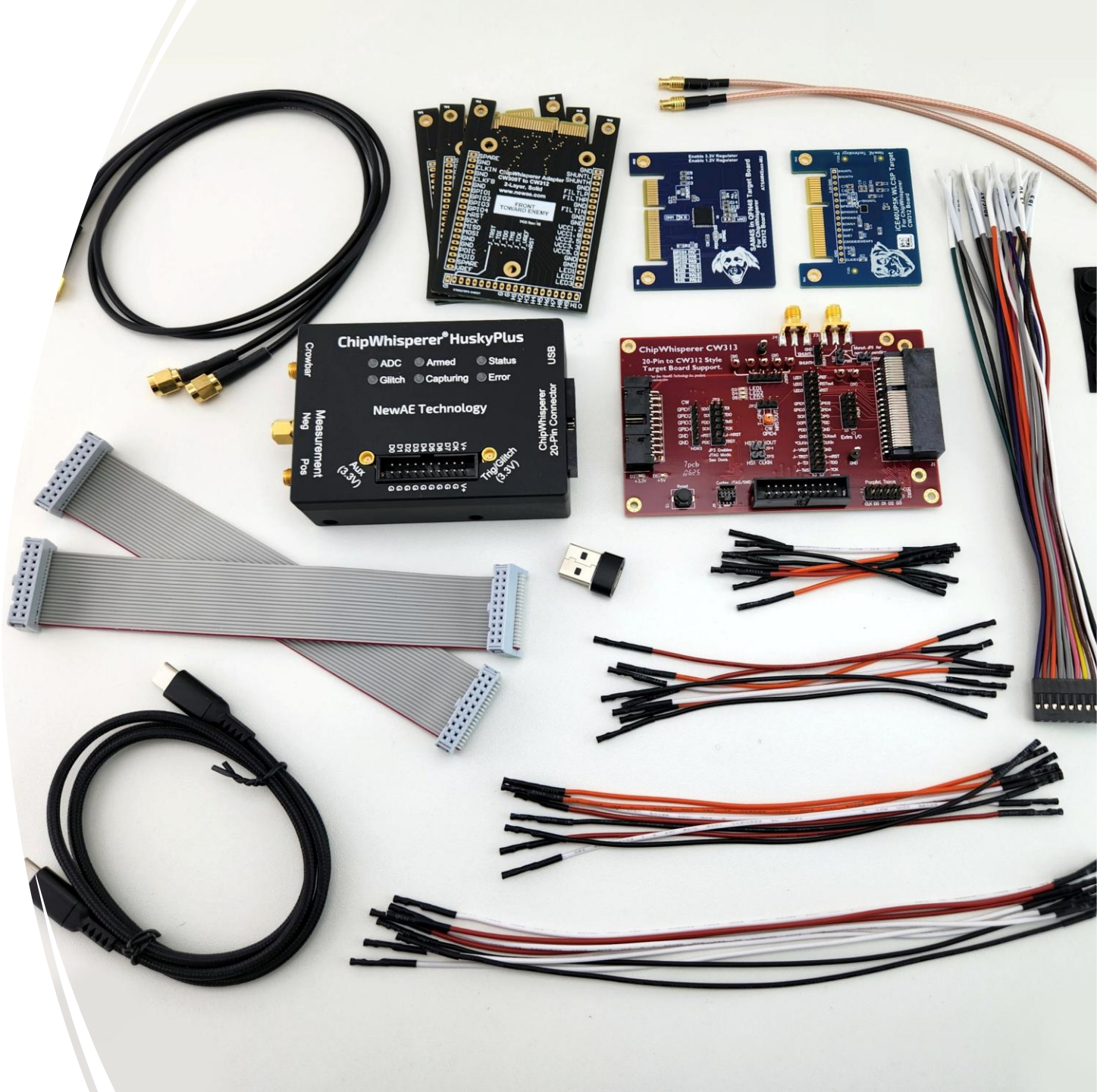
- What happens if code doesn’t execute correctly?
- How can we deliberately cause out-of-spec conditions?

- Voltage Glitching
  - Crowbar glitching
- EMFI



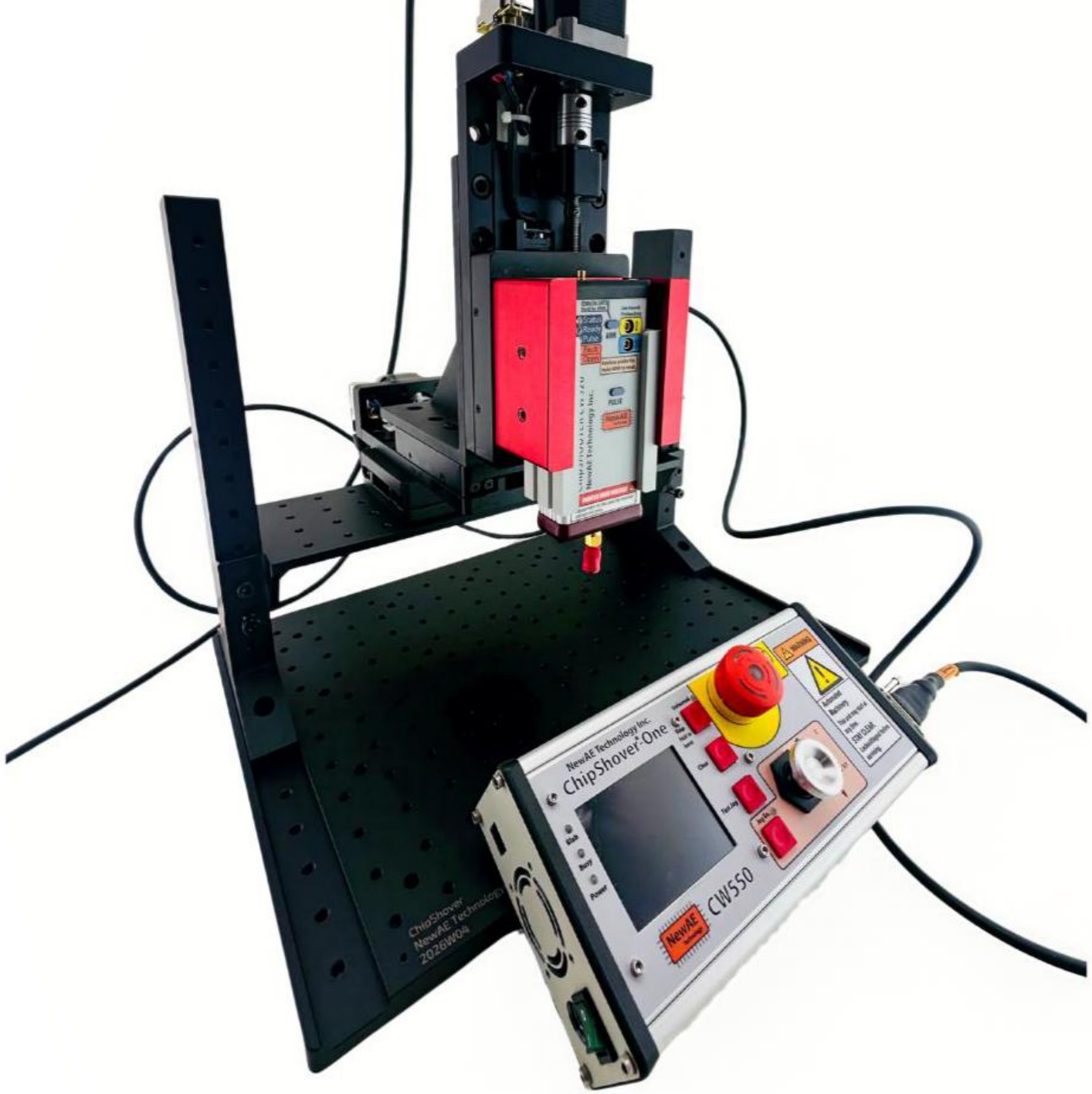
ChipWhisperer

- Synchronous capture
- Purpose built
- Target ecosystem
- Easy interfacing
- Lots of examples
- Commonly used in literature



ChipSHOUTER and ChipShover

- Easy to use python API, just like other NewAE tools
- Automate long attack campaigns with many variables to explore
- Integrate with ChipWhisperer to create multi-stage attacks that use complex power triggering and fault injection



Solutions to these vulnerabilites

- Hardware encryption cores with countermeasures baked in
- DO NOT REUSE KEYS, especially in consumer devices
  - Phillips hue bulbs
- Create systems where secrets aren’t stored on the measurable *leaky* system.
- Remember: this isn’t breaking the encryption, it’s bypassing it.

Thank you

- My Email
  - Lcraig@NewAE.com
- Main Documentation
  - https://chipwhisperer.readthedocs.io/
- CPA on AES Notebook
  - https://github.com/newaetech/ChipWhisperer-Test-Results/blob/main/tutorials/CWHUSKY/SOLN_Lab%204_2%20-%20CPA%20on%20Firmware%20Implementation%20of%20AES.ipynb

Hitex offerings …

Ask alexander.hess@hitex.de – he looks forward to receiving your inquiries regarding Hitex offerings, including:

- Arm encryption libraries
- Security stack for Hardware Security Modules
- Support for your ISO 21434 Threat Analysis and Risk Assessment (TARA)
- Training courses for embedded systems with Arm
- SO-DIMM compute modules for PSOC™, TRAVEO™ and more for an easy entry into the Infineon MCs.

Stay informed: webinars, training sessions, knowledge labs
Find all the information at www.hitex.de