



# **HARDWARE BASED AUTHENTICATION AND TRUSTED PLATFORM MODULE FUNCTIONS(HAT) FOR IOTS**

**Fareena Saqib**

[fsaqib@fit.edu](mailto:fsaqib@fit.edu)

Electrical and Computer Engineering  
Florida Institute of Technology

# Outline

---

- **Security challenges in IoTs.**
- **Hardware security attacks and countermeasures**
- **Research overview**
- **Q&A**

# Era of “Smartness”

---



**Smart Thermostat**



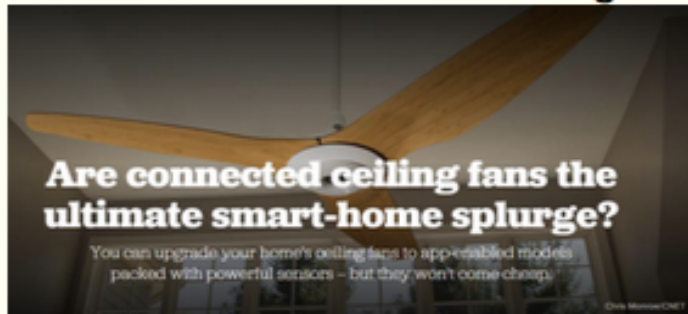
**Google Home**



**CUJO: Smart firewall**



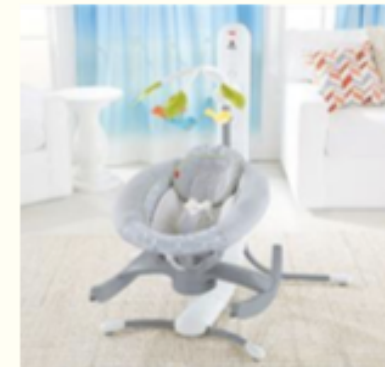
**Smart Talkies**



**with motion & climate sensors...automatically adjust as you come and go, or as the temp. rises.**



**Virtual Reality Headset**



**4-in-1 Smart Connect™ Cradle 'n Swing**  
“... Baby, that’s genius.”

# Internet of Things (IoTs) Characteristics

---

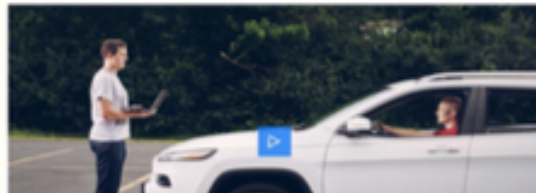
- **Unique requirements for IoT security**
  - Long, complex life cycles
  - Never intended to be connected
  - Machine-to-Machine interactions
  - Mass produced in same configuration (“Hardware Homogeneity”)
- **Changing environment for security assurance**
  - Increasingly globalized supply chain
  - Increasingly stringent time-to-market
  - Increasingly connected world



How can we protect **diverse, connected,** and highly **complex** modern computing systems against malicious attacks?

# IoTs: Security and Trust Threats and Attacks

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



**July 2015**

21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

A massive and sustained Internet attack that has caused outages and general frustration today for a large number of Web sites was facilitated with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, some data suggest.

Earlier today other criminals began testing their attack resources on Bittix, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users resulting in some of sites including Twitter, Amazon, YouTube, Netflix, Spotify and Netflix.



**October 2016**

- <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- [https://motherboard.vice.com/en\\_us/article/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker](https://motherboard.vice.com/en_us/article/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker)
- <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>
- <http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L>
- <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm>
- <https://www.wired.com/2017/03/worried-cia-hacked-samsung-tv-heres-tell/>

Hackers Killed a Simulated Human By Turning Off Its Pacemaker



Some humans are already hackable, and, yes, you can do some serious damage by compromising medical implants.

**September 2015**

U.S. FOOD & DRUG ADMINISTRATION

Medical Devices

Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication

Date Issued: January 6, 2017

**January 2017**

J&J warns diabetic patients: Insulin pump vulnerable to hacking



**October 2016**

MICHAEL CALDRE 09:07:17 3/28 PM  
**WORRIED THE CIA HACKED YOUR SAMSUNG TV? HERE'S HOW TO TELL**

**March 2017**

---

**Internet of things needs to be redefined as **securely** connecting devices, exchanging **trusted** data and delivering value through **analytics** and smart decisions**

# **Cyber security: Where and Why it is important**

---



**Cloud and distributed system security**



**IoT Security**



**Network Security**



**Biometrics and Security**



**Supply Chain Security**



**Nanoscale Security**

## Hardware Security

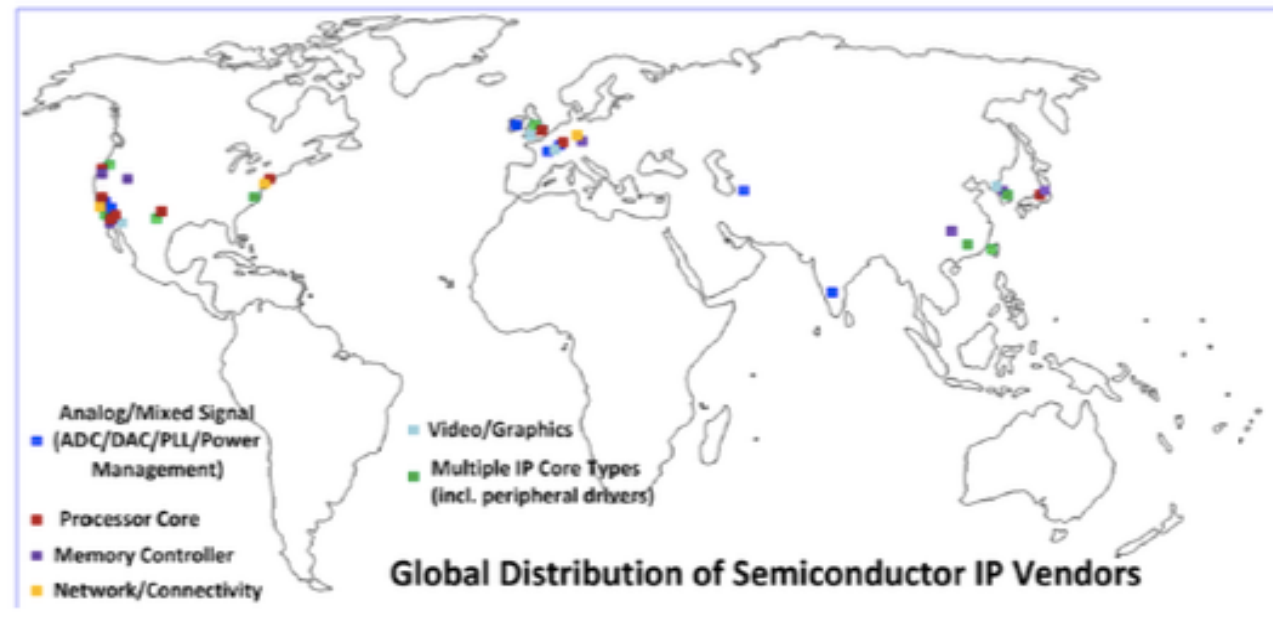
---

Cyber security traditionally meant software, network and data security considering hardware as **root of trust**. This assumption is no longer true with evolving semiconductor business landscape .



# IP Vendors Distributed Across the Globe

---



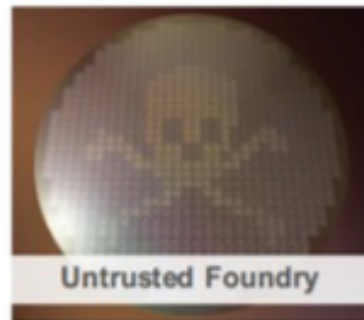
**Long and globally distributed supply chain of hardware IPs makes SoC design increasingly vulnerable to diverse trust/integrity issues.**

# Security Attacks on Hardware

---



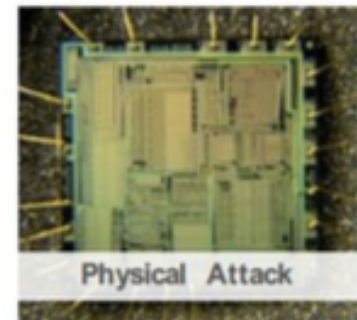
Trojans



Untrusted Foundry



Counterfeit ICs



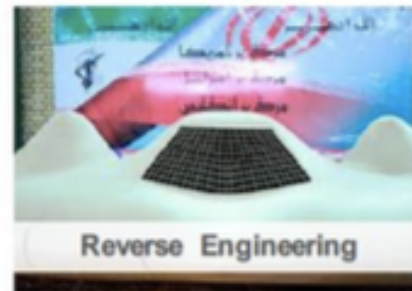
Physical Attack



Side-channel



Fault Injection



Reverse Engineering



Fake Parts

# Research Projects

---

## ▪ **Hardware-Oriented Security and Trust (HOST)**

- Physical Unclonable Functions
- Authentication and Encryption
- Differential power analysis countermeasures
- Hardware Trojan Detection
- Obfuscation of chip functionality
- Secure Automotive ECU Design



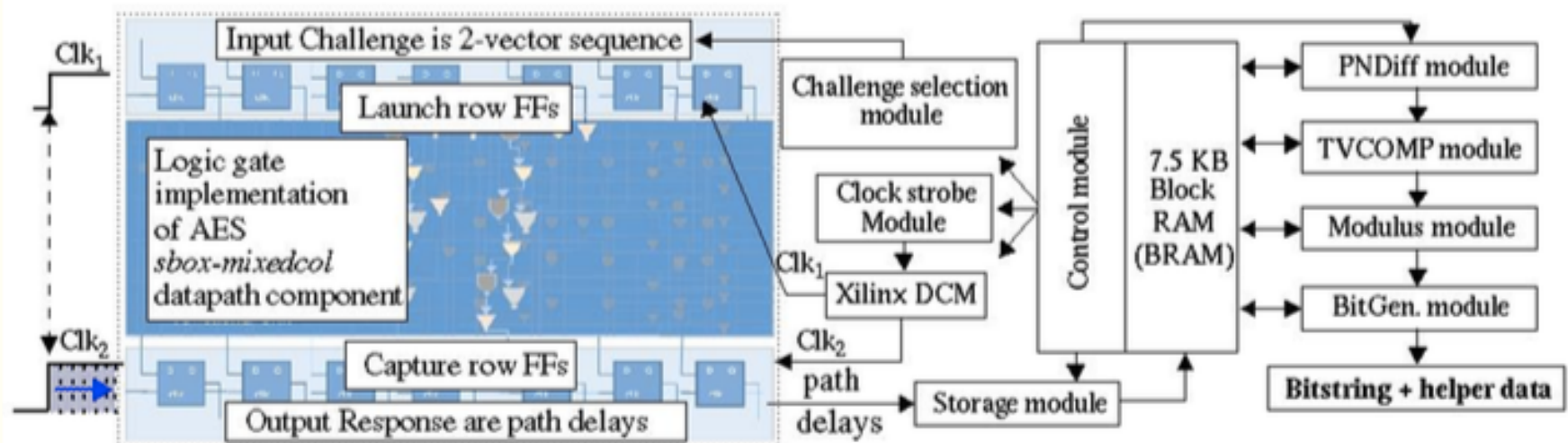
## ▪ **Embedded Systems**

- TrustZone based hardware isolation
- FPGA-based embedded systems
- Hardware acceleration



# Security Research: PUFs

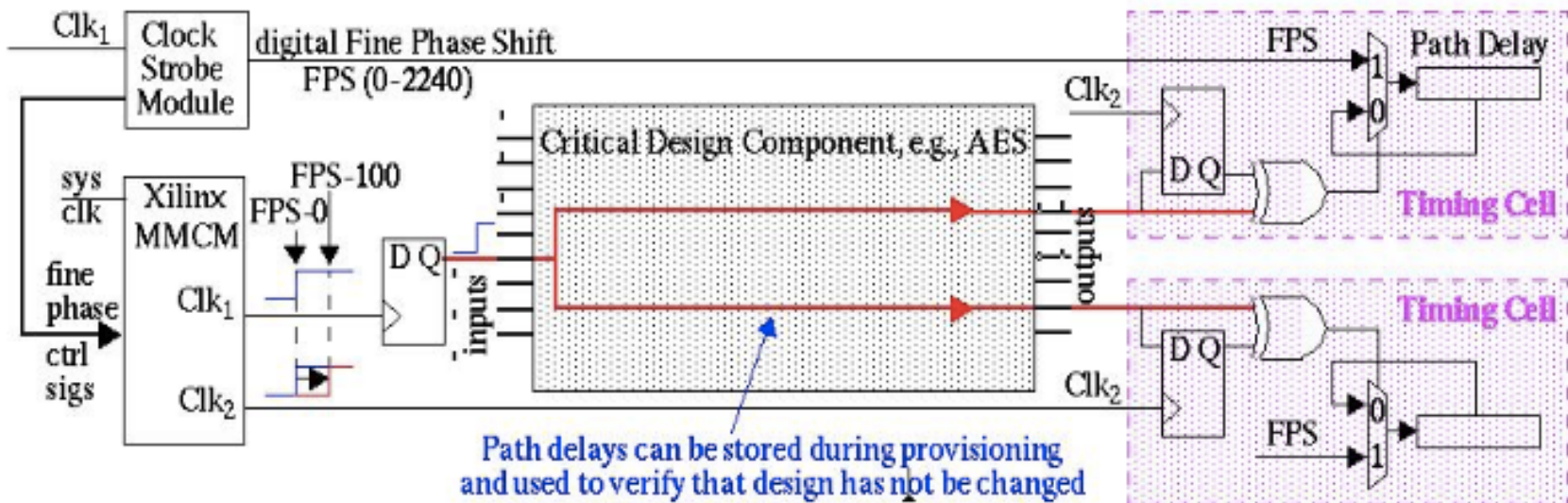
HELP entropy is path delays of existing functional units.  
On-chip bitstring generation provides real-time identification.



# Trust Research: Tamper Detection

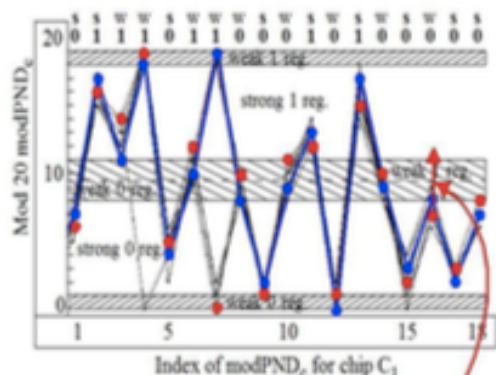
Devise a water-marking mechanism by profiling path delays

In-field chips compared with the time 0 to detect tamper



# Privacy Preserved Authentication in Distributed Environment

A privacy-preserving, mutual authentication protocol using dual helper data



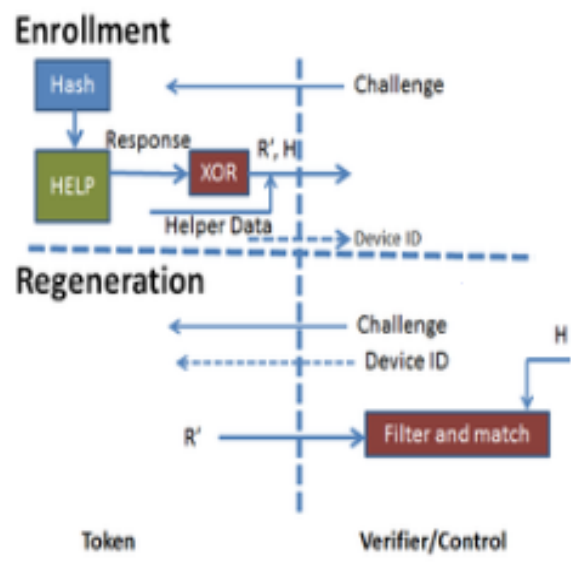
Token data point would need to change by at least  $2 \cdot \text{margin} + 1$  to cause bit flip error, e.g., with margin = 2, from 7 to 12.

(a)



(b)

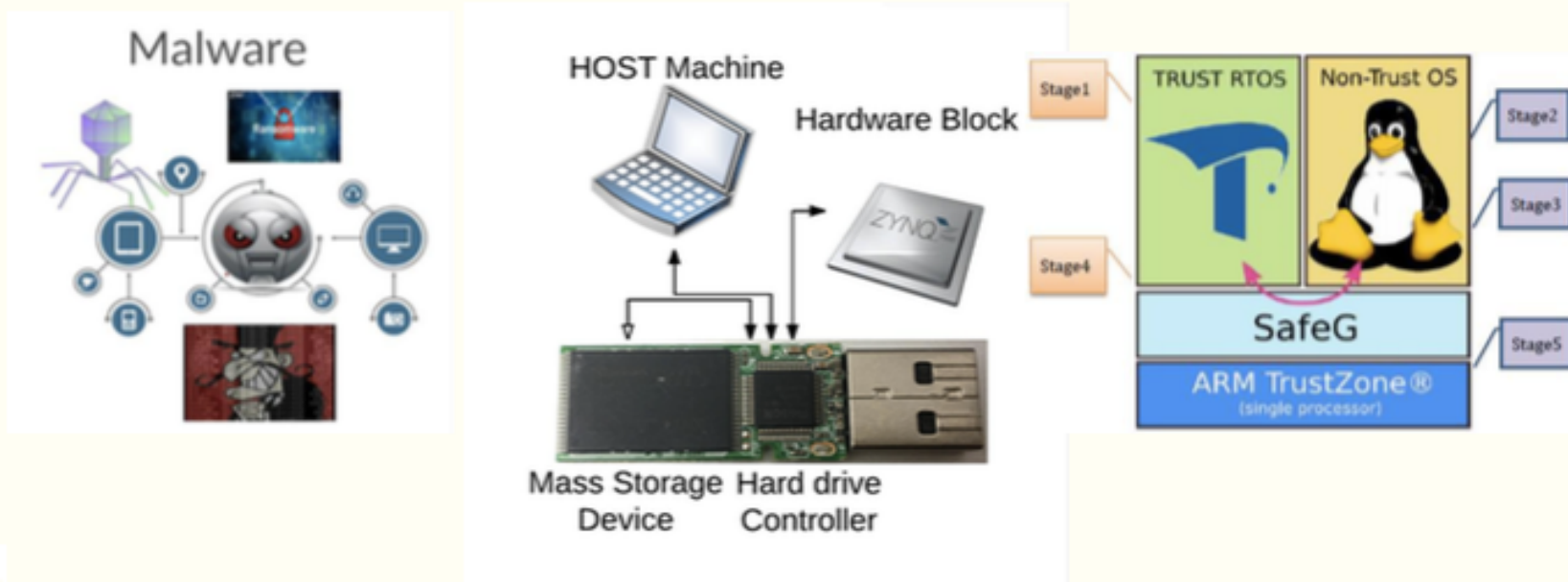
(c)



■ Sponsored by NSF

# Security based hardware isolation and Access Control

## Techniques to mitigate malwares such as Rootkits and Bootkits



▪ Sponsored by NSF

# IoT Security Issues

---

- Provisioning keys and key management life cycle
- Security assessment of equipment connected via gateways, that were never intended to be connected.
- Device identification for device-to-device communication
- Availability and system resilience.
- Scalability



**Requires holistic view of device to gateway to cloud and the communication between them.**





## **Questions**