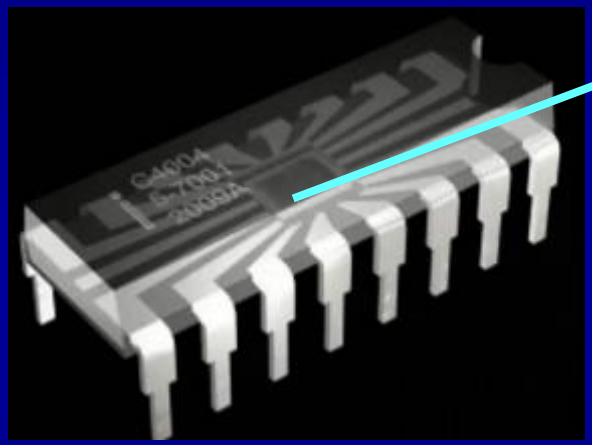
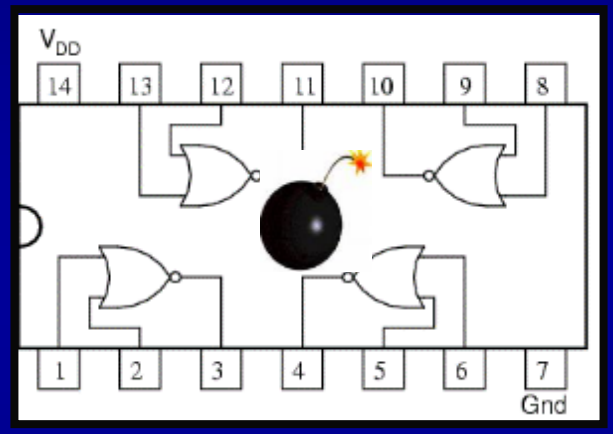
Security of the Internet of Things: New Frontiers





Swarup Bhunia and Domenic Forte

Electrical & Computer Engineering

University of Florida

FICS Research

…Emergence of IoT: Computing In Everyone's "Hands"…

How can we protect **diverse**, highly complex computing systems **in the hands of possibly naïve users**?

Photo Credit: http://emergingtech.tbr.edu/i-can-show-you-grandma

Brief History of Security AND Validation

1966 – Apollo 13 computer

1971 – Intel 4004 processor

1982 – Computer virus – Elk Cloner | Birth of the term “virus”

1990 – Formal Verification landmark
Clarke at al. CMU

1993 – Common Criteria (CC)
for IT security validation

NEW ERA on HW Sec. and Validation!

1996 | 1999 – Side-channel Attack – *Timing Attack & DPA Kocher et al.*

2003 – Rockwell Collins AAMP7G processor w/ MILS thru. formal security validation

2007 – Hardware Trojan Attack – DARPA BAA

What are Unique to IoT Security?

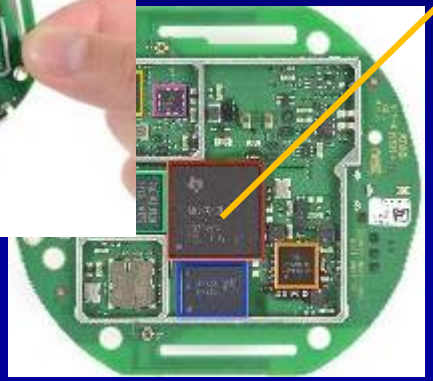
- Connects with physical world
- Long, complex life cycle
- Mass produced in same configuration
- Devices never intended to be connected
- Machine-to-machine
- Physical attacks
- Requires holistic view of device to cloud and the comm. between them

IoT security needs significant re-thinking!

Attacks on Hardware: From IC to IoT

Are We Paranoid Enough?

What is Hardware?



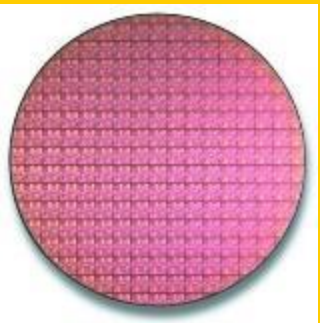
- Different levels of abstraction
- System Hardware – acts as the ***"root-of-trust"***: PCB → IC (SoC | µP)

Electronic H/W Design & Test Flow

Design Spec.

IC Design House

Fab



Wafer test

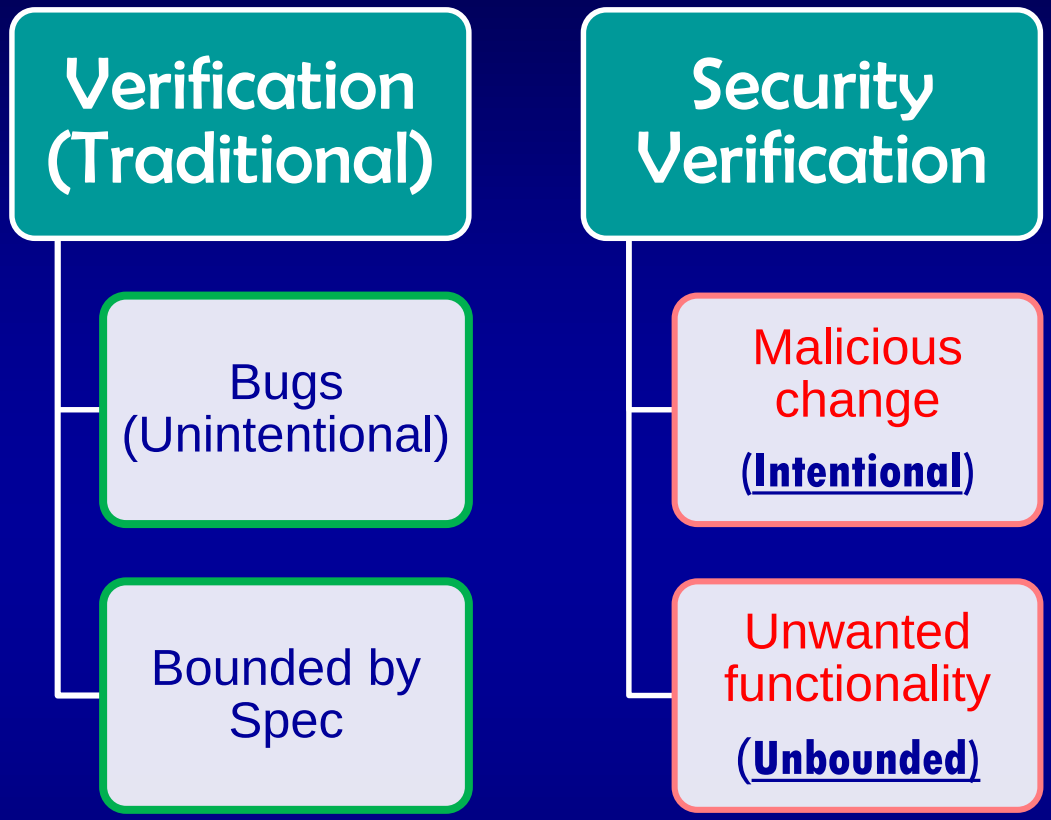
Assembly

Pkg. Test

PCB & Sys. Int.

Customer

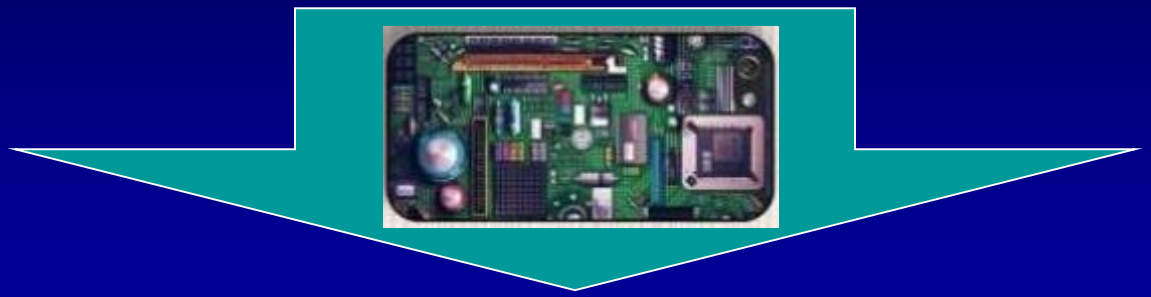
Bugs vs. Malicious Changes



- HW bugs can be exploited by an intelligent adversary for attacks!
- Possible to catch them through verification

Security → BIGGER verification challenge!

Many system-level attacks are done at PCB level!

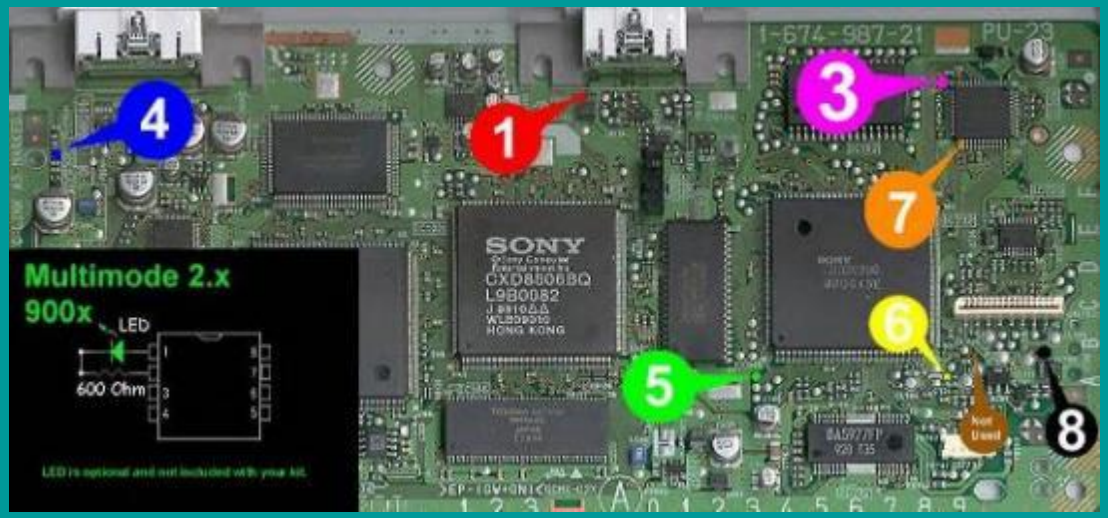


How Do You Remotely Authenticate Hardware?

- *A challenging problem!*
- *Hardware is vulnerable to in-field tampering*
- *Enables assurance of "hardware root-of-trust" through the life-time of a device!*

- *Ghosh et al., IEEE D&T, 2015*
- *Zhang et al., VTS 2015*
- *Paley et al., ISQED 2016*
- *Hennessy et al., ASPDAC 2016*

Trust Issues at PCB Level



PSX DIY Guide

Modchip attack

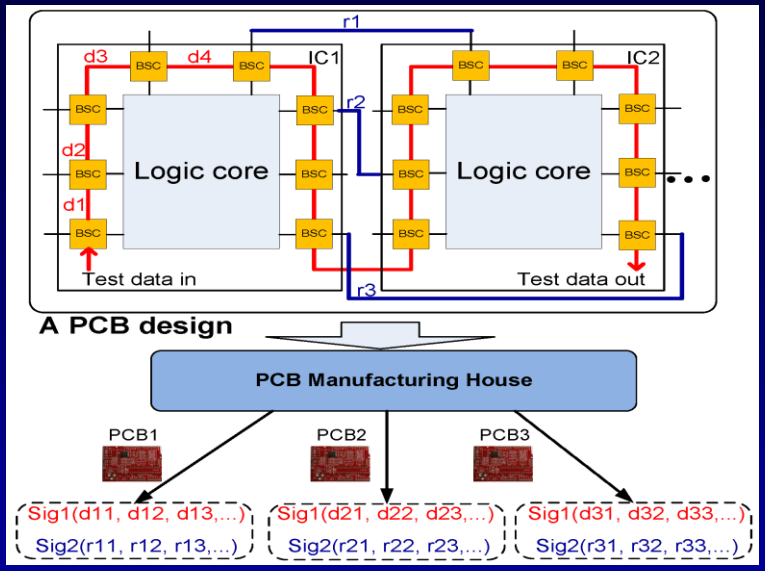
Playstation modchip wiring

Modchip for XBOX

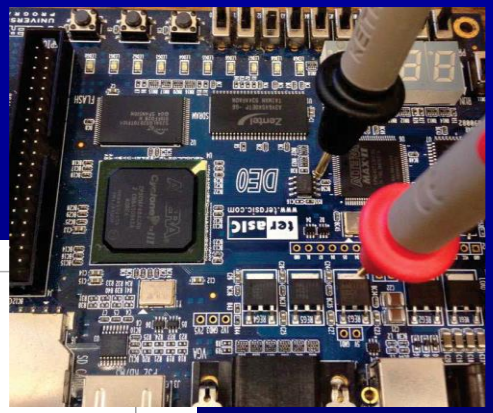
Remote HW authentication can help detect in-field tampering!

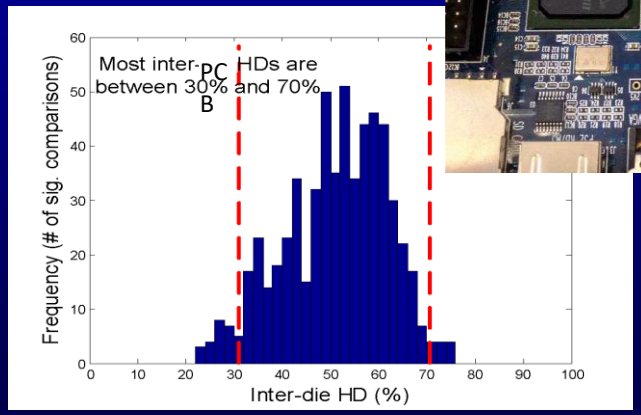
PCB Integrity Validation

- *Authenticate* PCBs w/ unique signature from each board
- Key ideas:
  - Exploit variations in *PCB wire res.*
  - Exploit variations in *boundary scan path delays* w/ JTAG (suitable for *remote in-field authen.)*

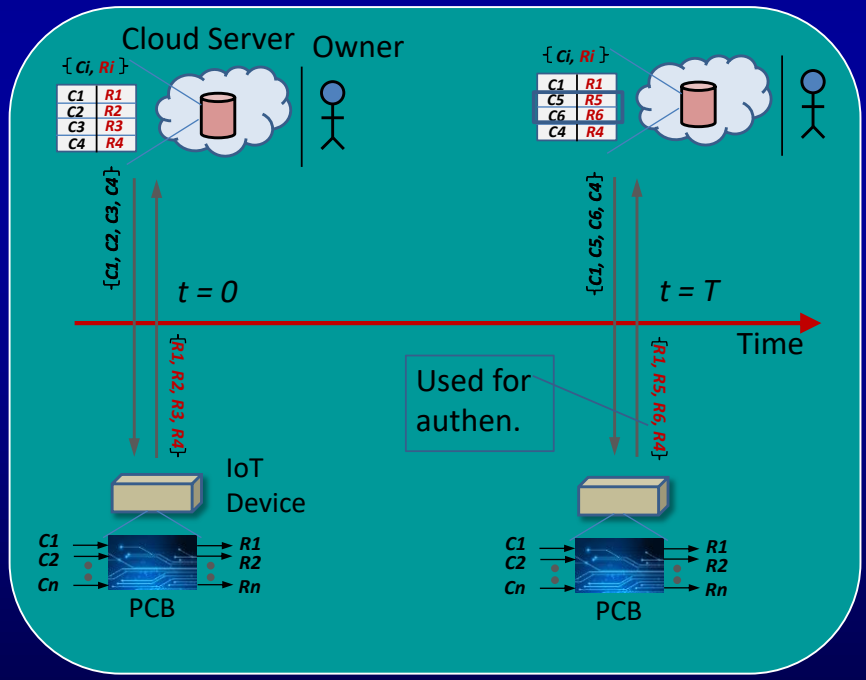


JTAG based authen.





Trace based authen.



Promising results w/ commercial PCBs

Can serve as backbone for IoT authentication!

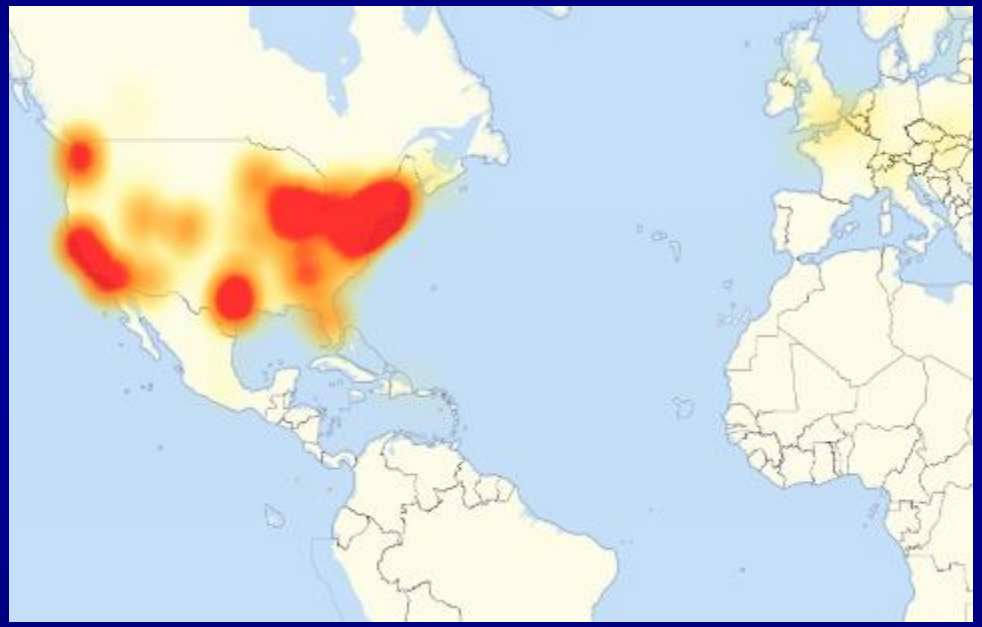
Hardware Patch?

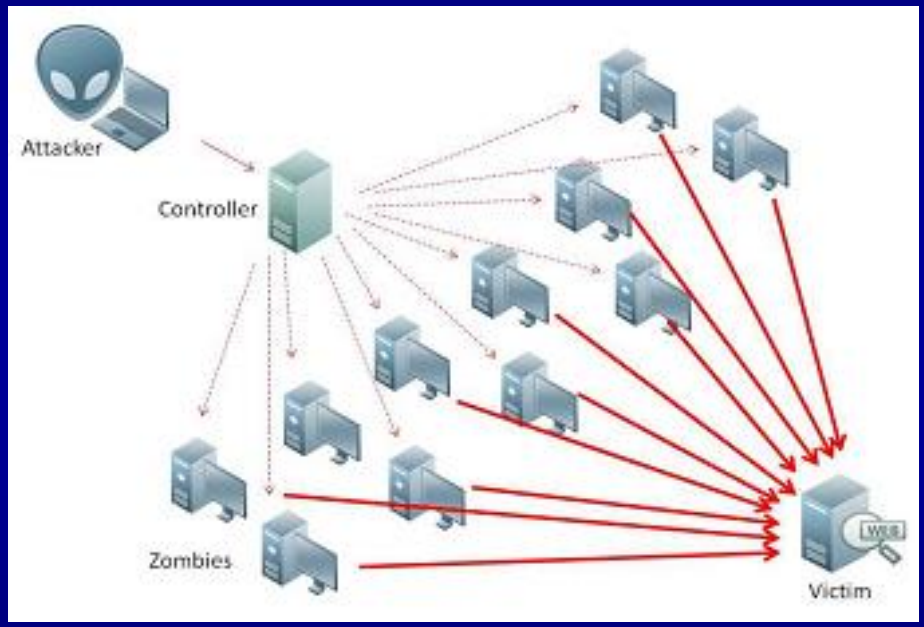
An emerging need!

"Patchable IoT …", IEEE SPECTRUM, Nov 2017, Upcoming

Dyn Cyberattack

Oct 21, 2016





- **Army of million of hacked Internet-connected smart devices almost broke the Internet!**
- **Coordinated botnet of IoT devices!**

Security Policies in System on Chip (SoC)

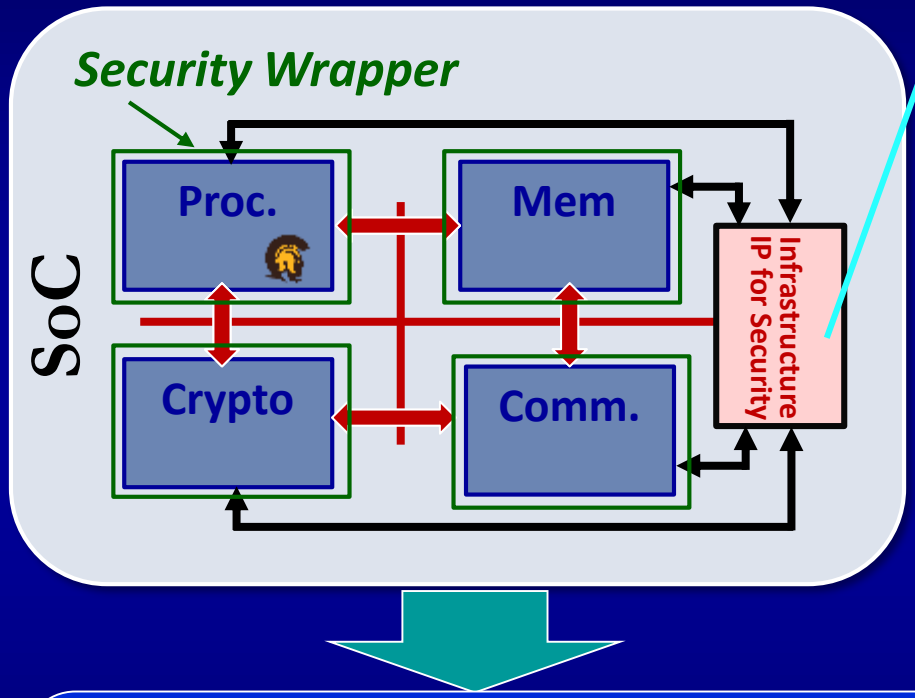
- Policies governing *confidentiality*, *integrity* & *availability* of various assets (e.g. crypto keys, programmable fuses, firmware)
- Policy Categories:
  1) *Access Control*
  2) *Information Flow*
  3) *Liveness*
  4) *Time-of-Check Time-of-Use (ToC-ToU)*
- Security policies map to design features/constraints
  - Used by IP designers, SoC integrators

Ex. 1 – *During boot, data transmitted by crypto-engine cannot be observed by any IP in the SoC other than its intended target (Confidentiality)*

Ex. 2 – *A secure key container can be updated during silicon validation, but not after production (Integrity)*

An Infrastructure IP supporting "Hardware Patch"

Centralized, plug-n-play, configurable ***security-brain***



Trust/Security Issues:

- Authentication
- Hardware Trojan
- Scan based attacks
- Side-channel attacks
- Diverse ***security policies***

- Reduced design effort/cost!
- Improved security
- Improved debug
- Protection against ***unanticipated*** attacks (*a "hardware patch"*)

- *Wang et al., IEEE Tcomp, 2014*
- *Ray et. al., DAC 2015*
- *Basak et al., ICCAD 2015*
- *Basak et. al., DAC 2016*
- ***Funded by SRC***

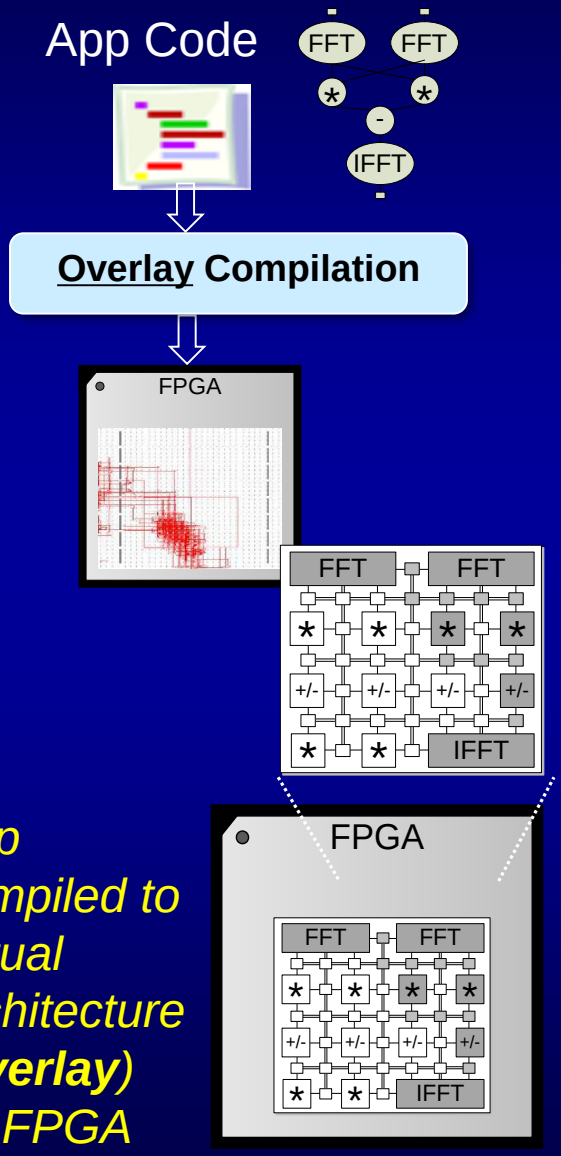
Hardware Virtualization

Adds a Security Layer

Stitt et al., IEEE ESL 2017

FPGA Virtualization Overview

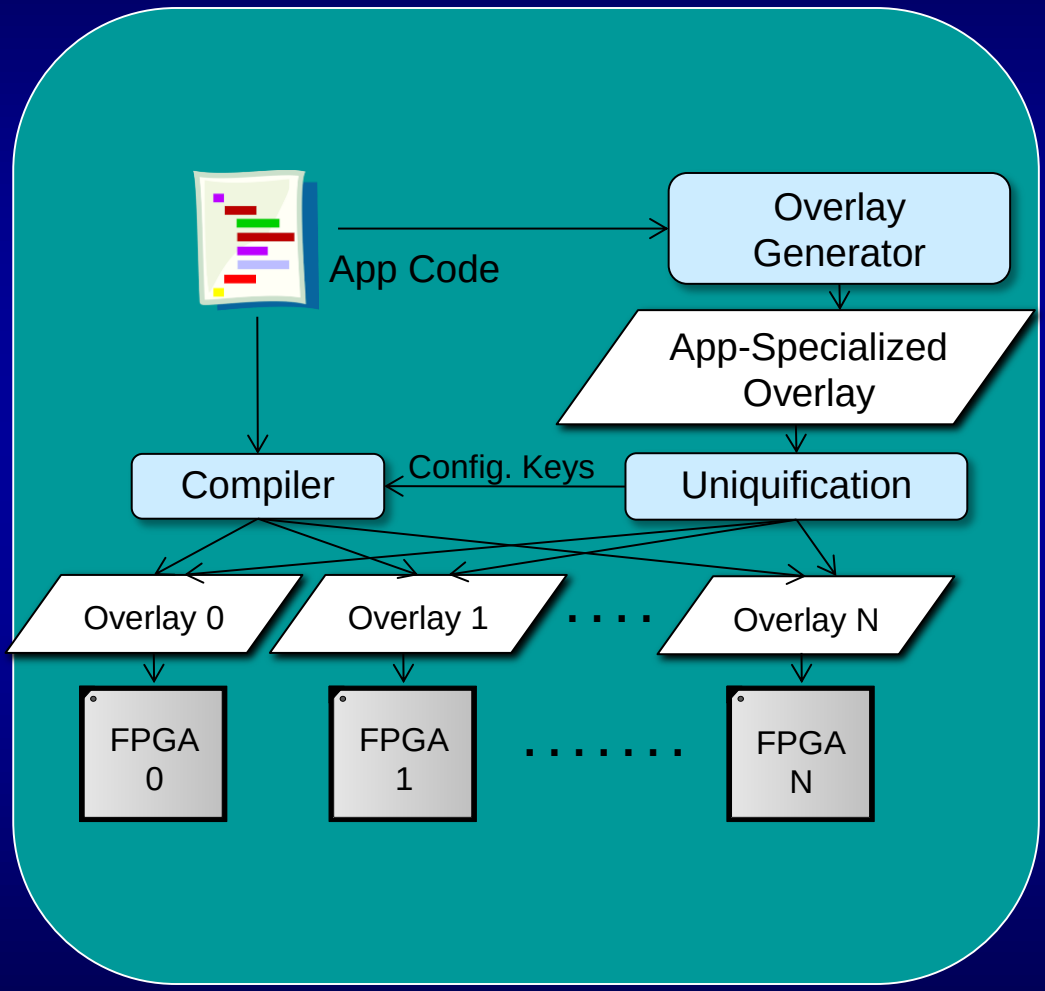
- Traditionally application code compiled directly onto FPGA
  - Difficult due to mismatch between FPGA primitives & appn. behavior
- Overlays provide an application-specialized virtual architecture
  - Appn. implemented on overlay instead of FPGA
  - Need to address several fundamental scientific questions: (1) how to derive an overlay; (2) how to customize; (3) how to verify?



*App compiled to virtual architecture (**overlay**) on FPGA*

Security Benefits

- **Main idea:**
  - Generate app-specialized overlay
  - Uniquify to create unique overlay for every deployed FPGA
- **Advantages:**
  - Creates unique virtual instances for each device
  - Limits tampering damage to one device
  - Side-channel attack countermeasures
  - **Formal correct-by-construction of bitstream**

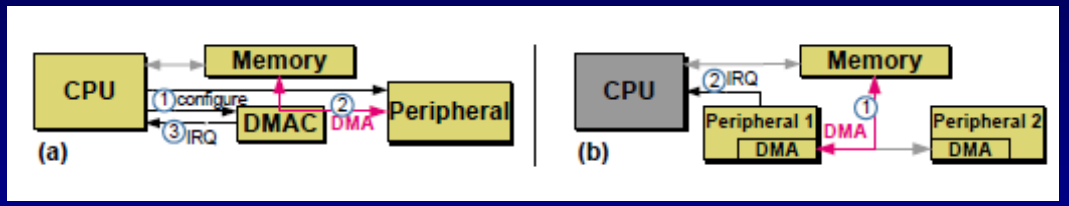


Glimpse into the Future

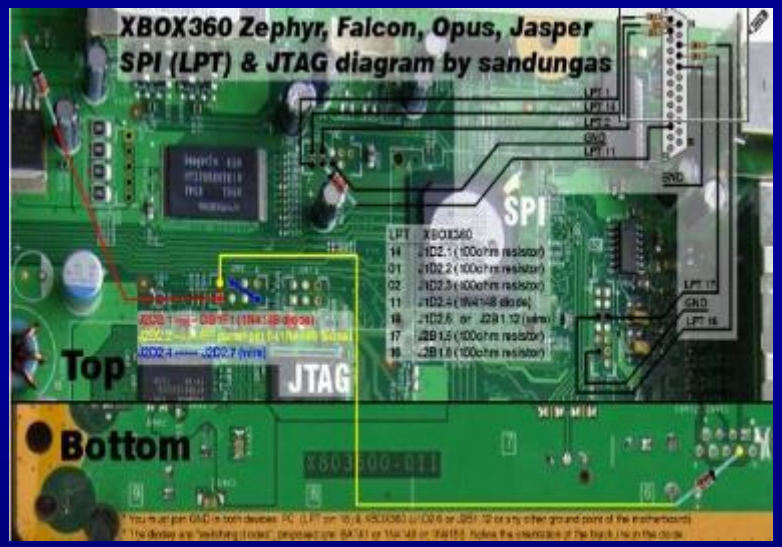
Changing Nature of Attacks

- Many attacks are complex system level attacks
- Often exploit subtle interaction between HW & FW
- *May exploit DFT or DFD infrastructure!*

DAGGER, a keylogger that attacks Linux & Windows platforms

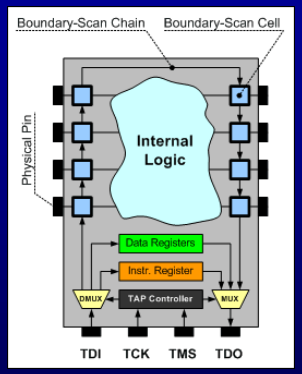


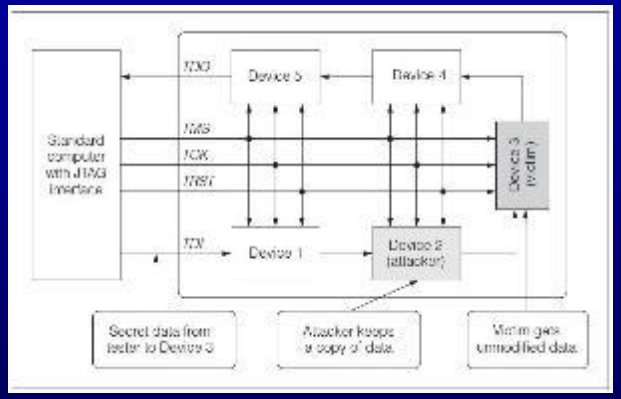
Patrick Stewin and Iurii Bystrov



"Xbox 360 Ultimate Exploit Guide (Semi-Noob Friendly)
By: oblivioncth"*
*http://www.se7ensins.com/forums

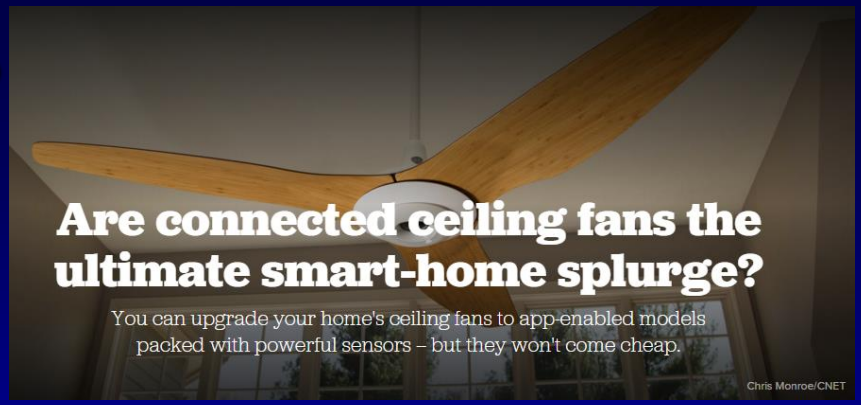
For many exploits, TMS and TCK signals need to be controlled





Smarter Attacks | Smarter Adversaries!

Era of "Smartness"?



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

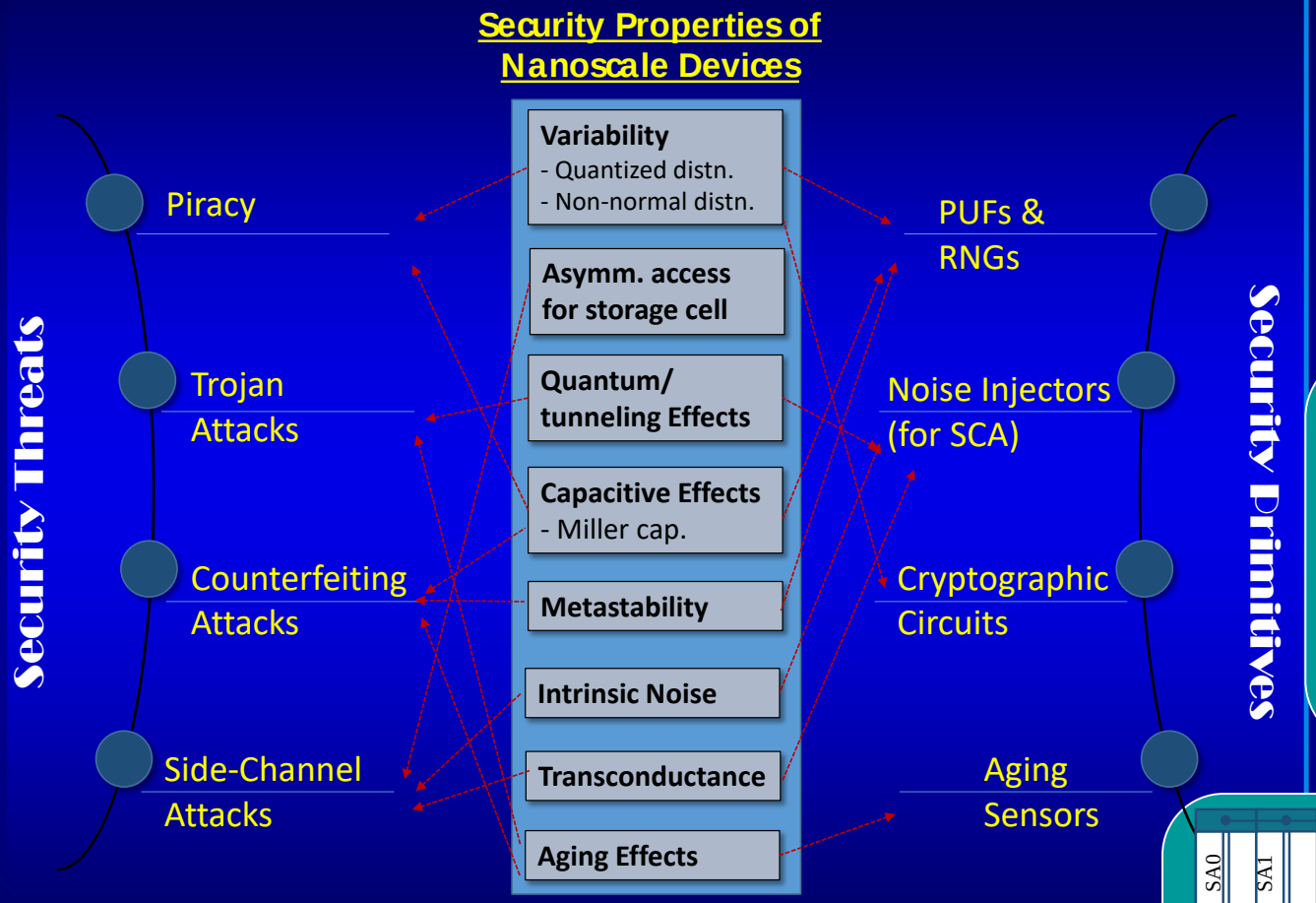
SMART makeup mirror
*Automatically turns on and off when you come in and out of the frame**
www.implehuman.com

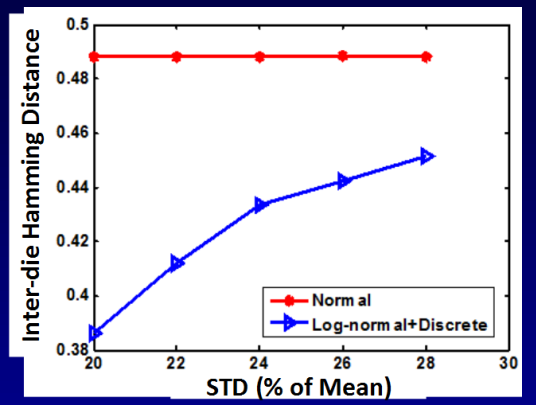
Smart Iron ($1400)
www.fisher-price.com/
"… provides real-time guidance."

4-in-1 Smart Connect™ Cradle 'n Swing - Techno Gray™
www.fisher-price.com/
"… Baby, that's genius."

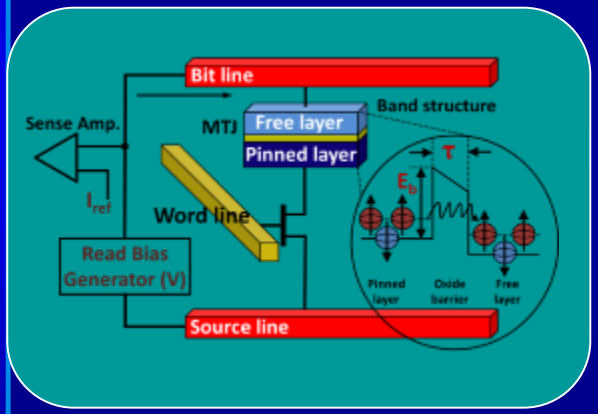
Smartness at odds with test & security!

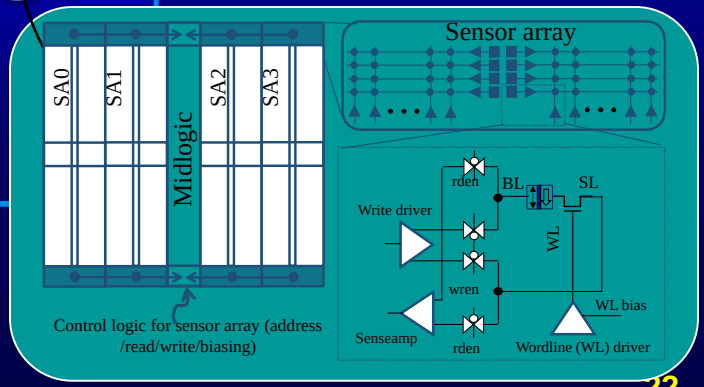
Security beyond CMOS





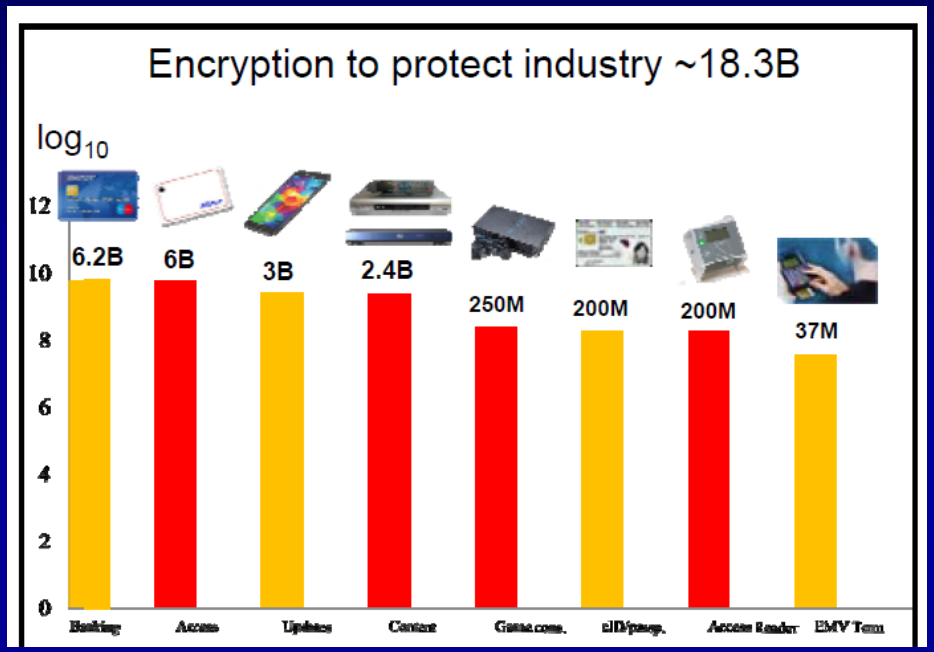
DAC 2015, to appear



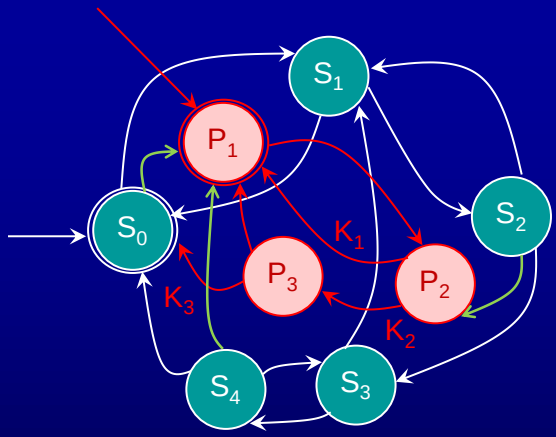


Many new challenges & opportunities!

Cryptography will play an increasingly Important Role …



- Crypto principles see growing usage in HW protection – e.g. FPGA bitstream
- Promising use of crypto in HW
  - HW obfuscation
  - On-chip asset protection
  - Remote upgrade

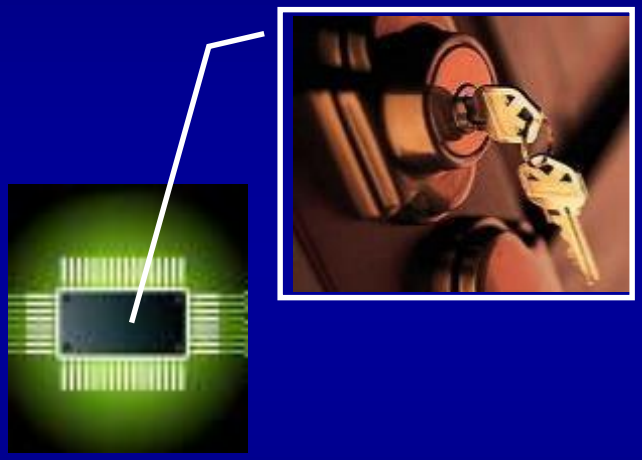


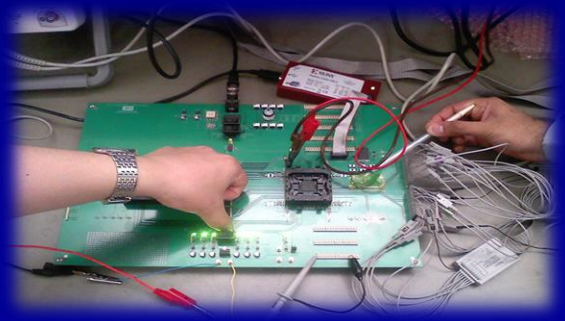
Hardware Obfuscation, Chakraborty & Bhunia, ICCAD 2008

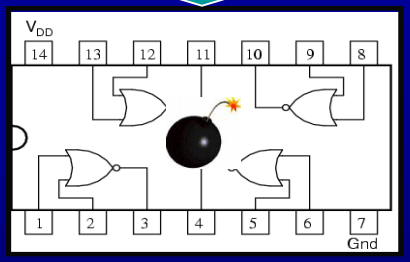
Crypto HW/SW needs strong security validation!

Integrative Measures …

Design for Security → **Trust Validation** → **Security Monitoring**







Secure by design, pre-si / post-si / run-time validation!

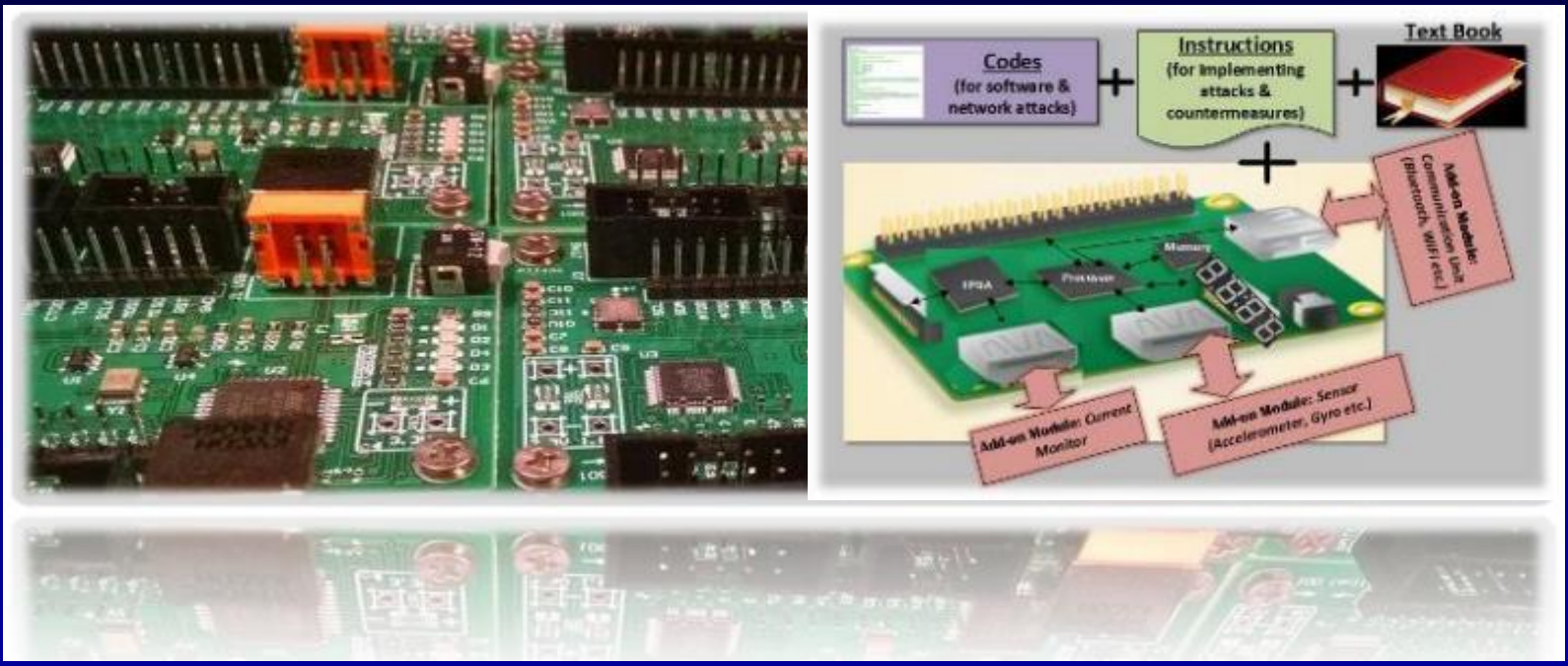
Bhunia et al., PIEEE 2014

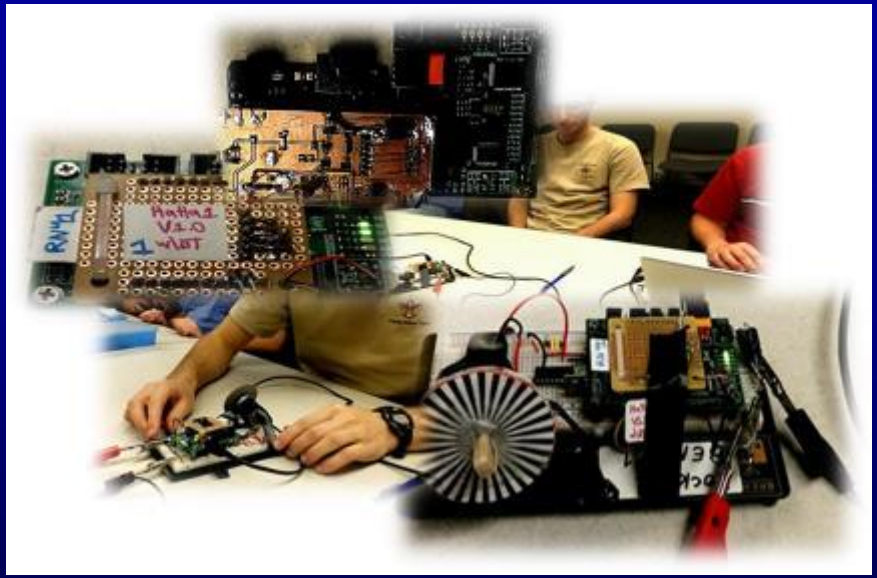
Cybersecurity Education

Hacking computers – for credit!

NSF Award # TUES-1245756

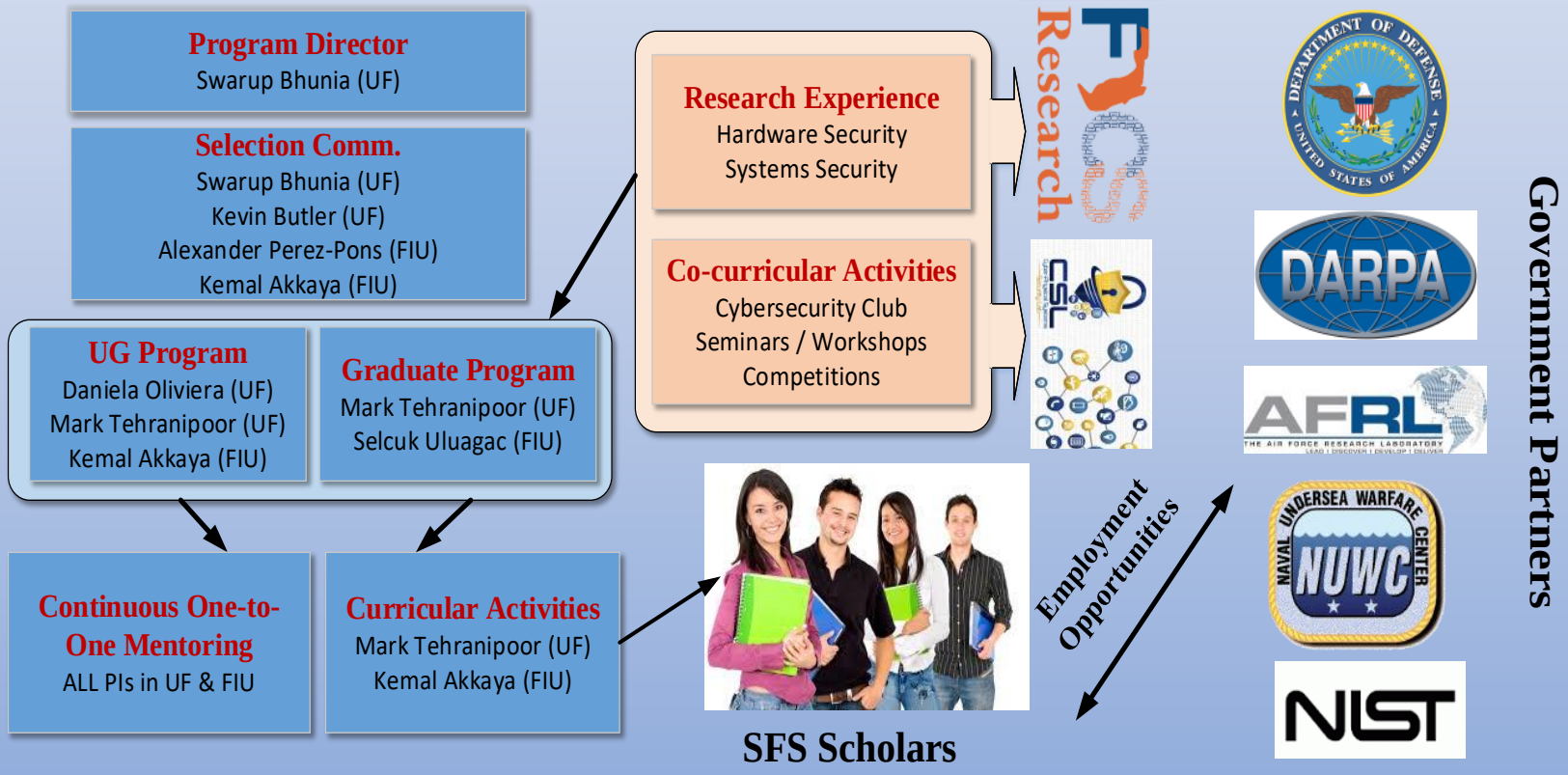
An Integrative Hands-on Approach to Security Education for UG Students





- ***"Easy-to-hack" hardware platform***
- ***Modular LEGO-like approach***
- ***Create well-trained cybersecurity professionals!***

Active NSF Grant with Prof. Fareena Saqib and Mark Tehranipoor



Unique Scholarship for Service (SFS) Program with Focus on Hardware & Systems Security

NSF Grant: $4.6M, 2017
PI: S. Bhunia
Co-PIs: M. Tehranipoor, D. Oliveira, K. Butler

THANKS!

#PowerfulYetSecure

Acknowledgements:

- Dr. Sandip Ray, NXP Semiconductor
- Prof. Soumajit Mandal, CWRU
- FICS Faculties (Prof. Mark Tehranipoor | Prof. Yier Jin)
- FICS Students

Sponsors: