Welcome

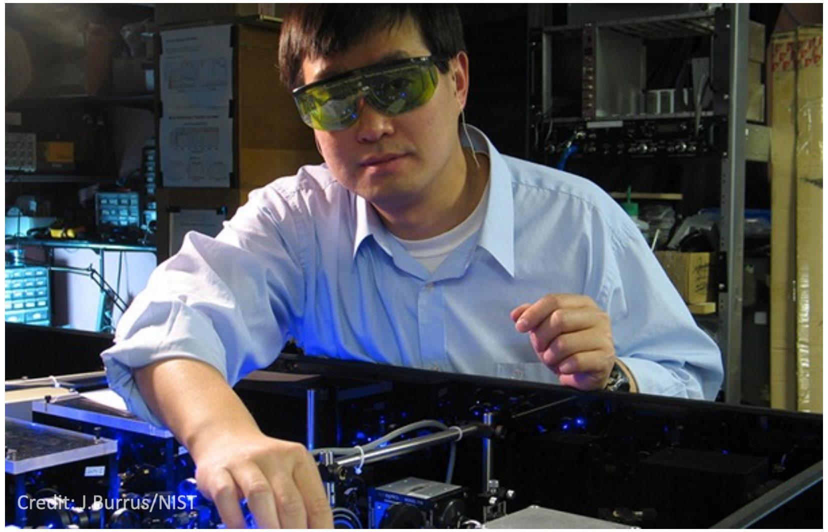
Kevin Stine

Chief of the Applied Cybersecurity Division in the Information Technology Laboratory at NIST

NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing **measurement science, standards, and technology** in ways that enhance economic security and improve our quality of life

©Robert Rathe



Credit: J.Burrus/NIST

©Nicholas McIntosh Photography

Cybersecurity at NIST

NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet US needs. Our activities range from producing specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.

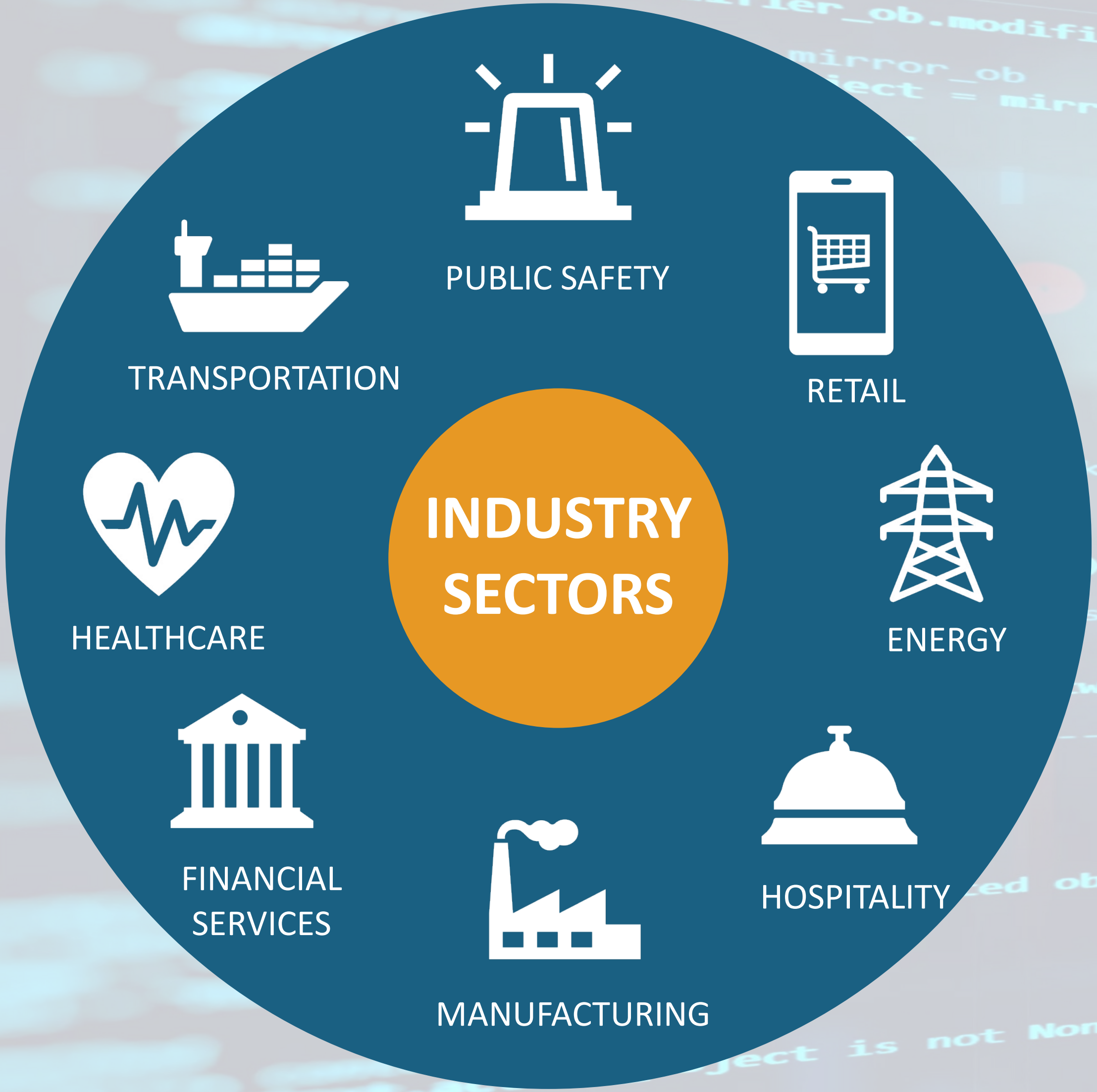
©Nick MacIntosh

https://www.nist.gov/cybersecurity

The National Cybersecurity Center of Excellence

Collaborate with innovators to provide **real-world, standards-based** cybersecurity capabilities that address business needs.

Practical Guidance with Industry Collaboration



INDUSTRY SECTORS

PUBLIC SAFETY

RETAIL

ENERGY

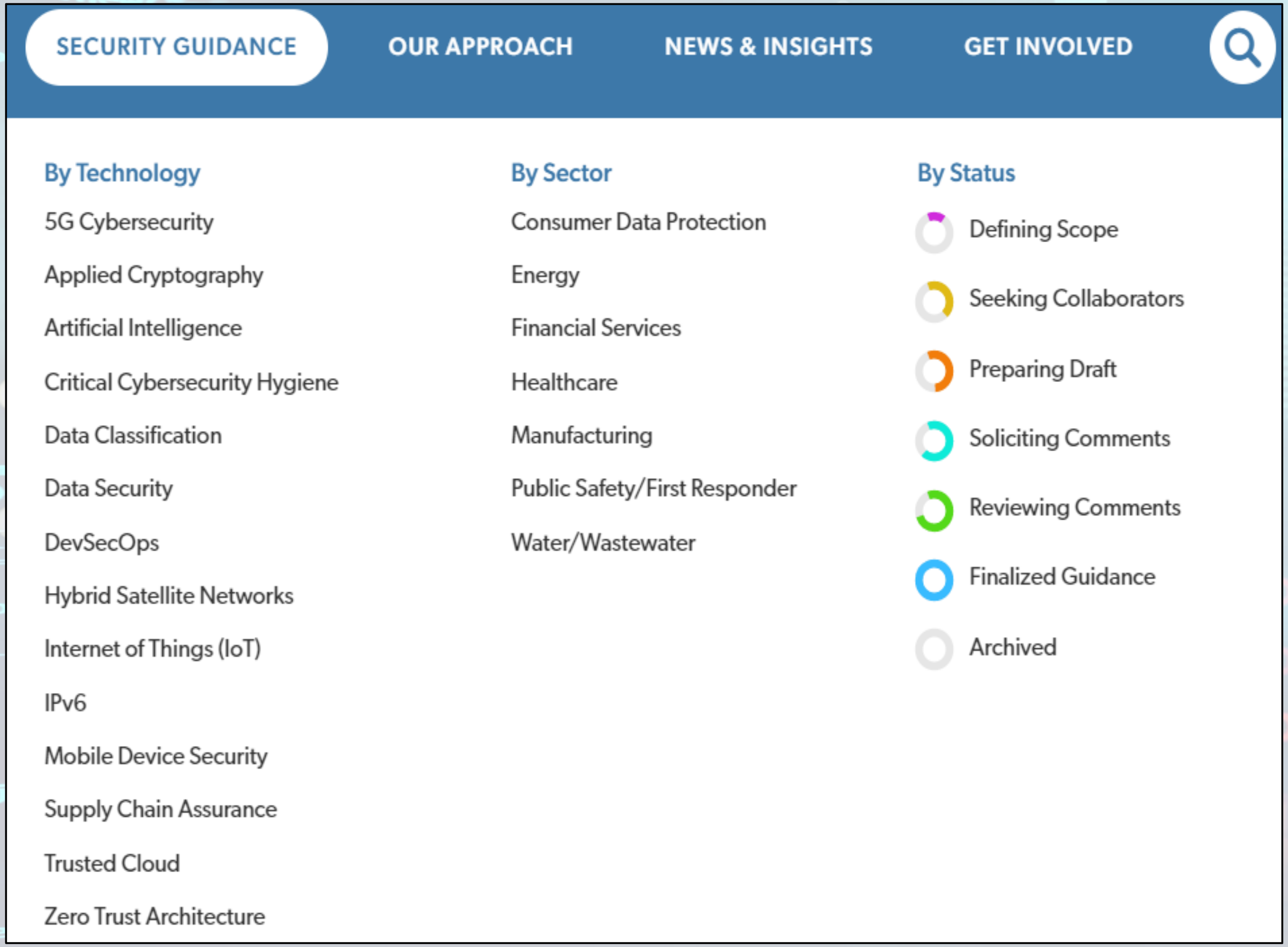
HOSPITALITY

MANUFACTURING

FINANCIAL SERVICES

HEALTHCARE

TRANSPORTATION



By Technology

- 5G Cybersecurity
- Applied Cryptography
- Artificial Intelligence
- Critical Cybersecurity Hygiene
- Data Classification
- Data Security
- DevSecOps
- Hybrid Satellite Networks
- Internet of Things (IoT)
- IPv6
- Mobile Device Security
- Supply Chain Assurance
- Trusted Cloud
- Zero Trust Architecture

By Sector

- Consumer Data Protection
- Energy
- Financial Services
- Healthcare
- Manufacturing
- Public Safety/First Responder
- Water/Wastewater

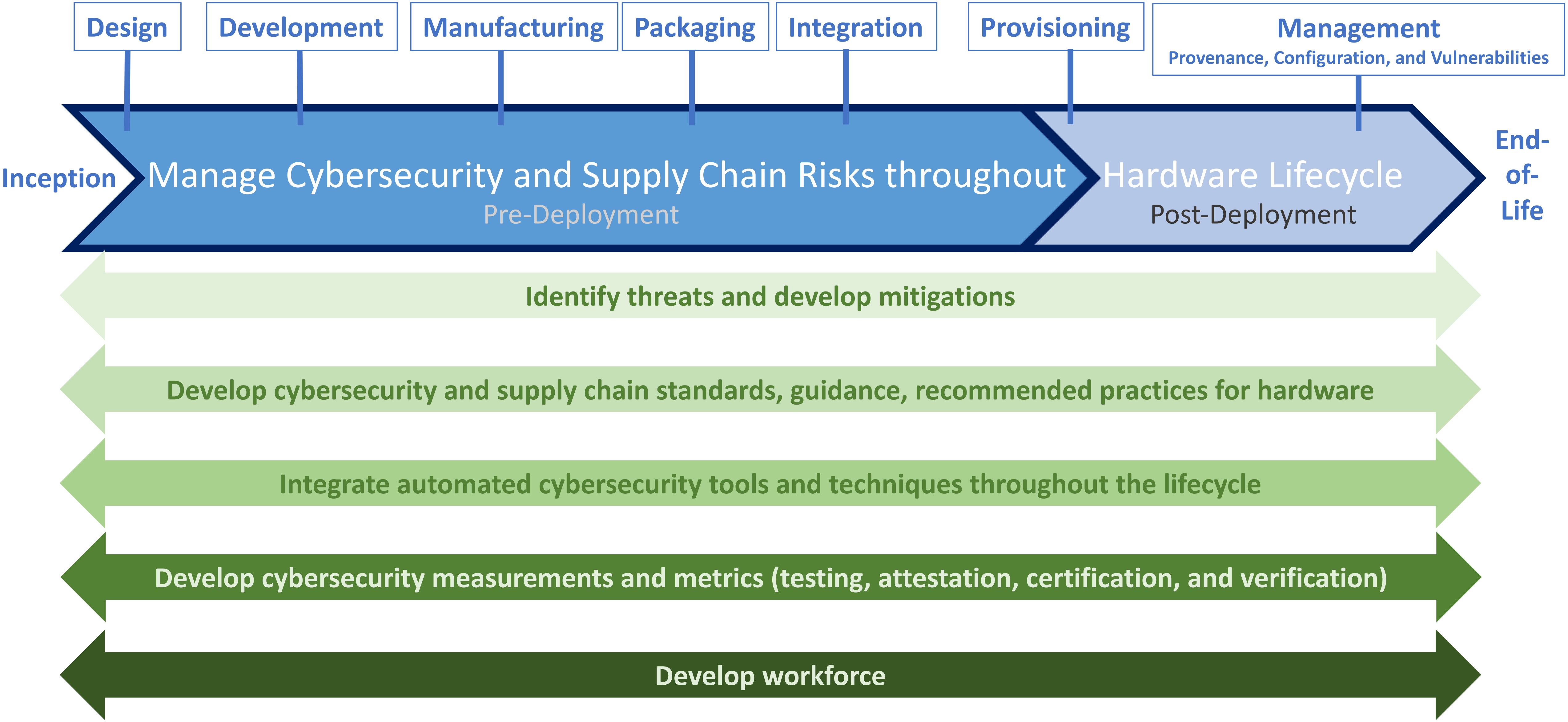
By Status

- Defining Scope
- Seeking Collaborators
- Preparing Draft
- Soliciting Comments
- Reviewing Comments
- Finalized Guidance
- Archived

Objective of Today’s Workshop

- Convene semiconductor security experts from industry, academia, and government
- Gather input to inform NIST strategic planning
- Leverage cybersecurity expertise
- Collaborate to prioritize:
    - Research activities
    - Approaches to advance standards, guidance and example implementations

Cybersecurity across the Life Cycle


Design

Development

Manufacturing

Packaging

Integration

Provisioning

Management

Provenance, Configuration, and Vulnerabilities

Inception

Manage Cybersecurity and Supply Chain Risks throughout Hardware Lifecycle

Pre-Deployment

Post-Deployment

End-of-Life

Identify threats and develop mitigations

Develop cybersecurity and supply chain standards, guidance, recommended practices for hardware

Integrate automated cybersecurity tools and techniques throughout the lifecycle

Develop cybersecurity measurements and metrics (testing, attestation, certification, and verification)

Develop workforce

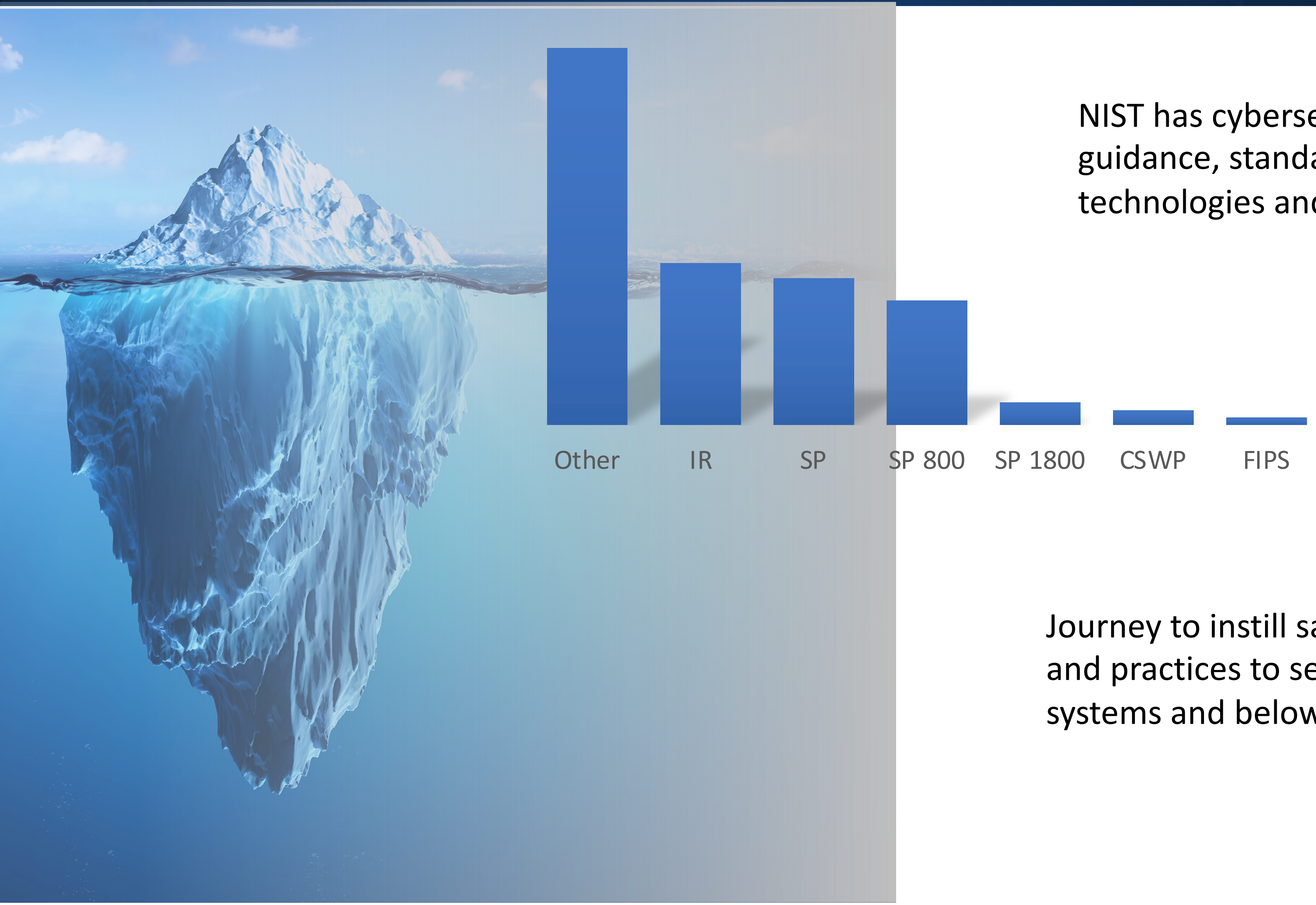
HW Security at NIST

Sanjay Rekhi

Group Leader, Security Components and Mechanism

National Institute of Standards and Technology

Cybersecurity practice



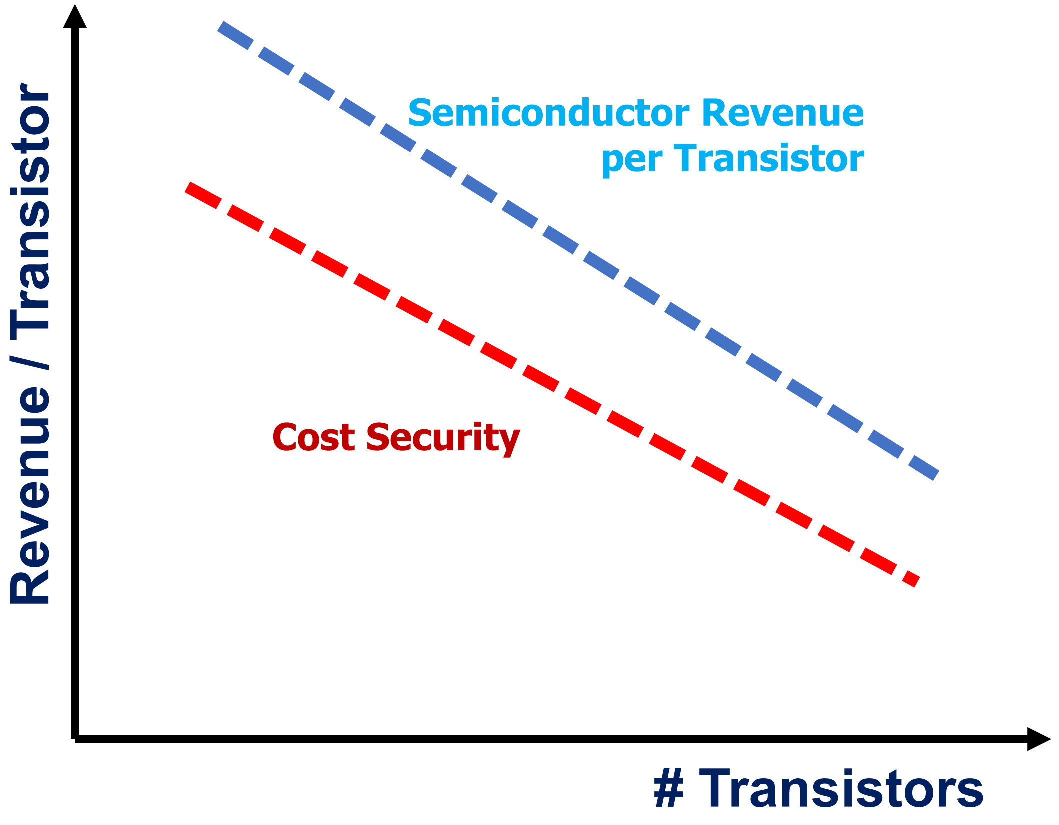
NIST has cybersecurity research, guidance, standards across multiple technologies and sectors

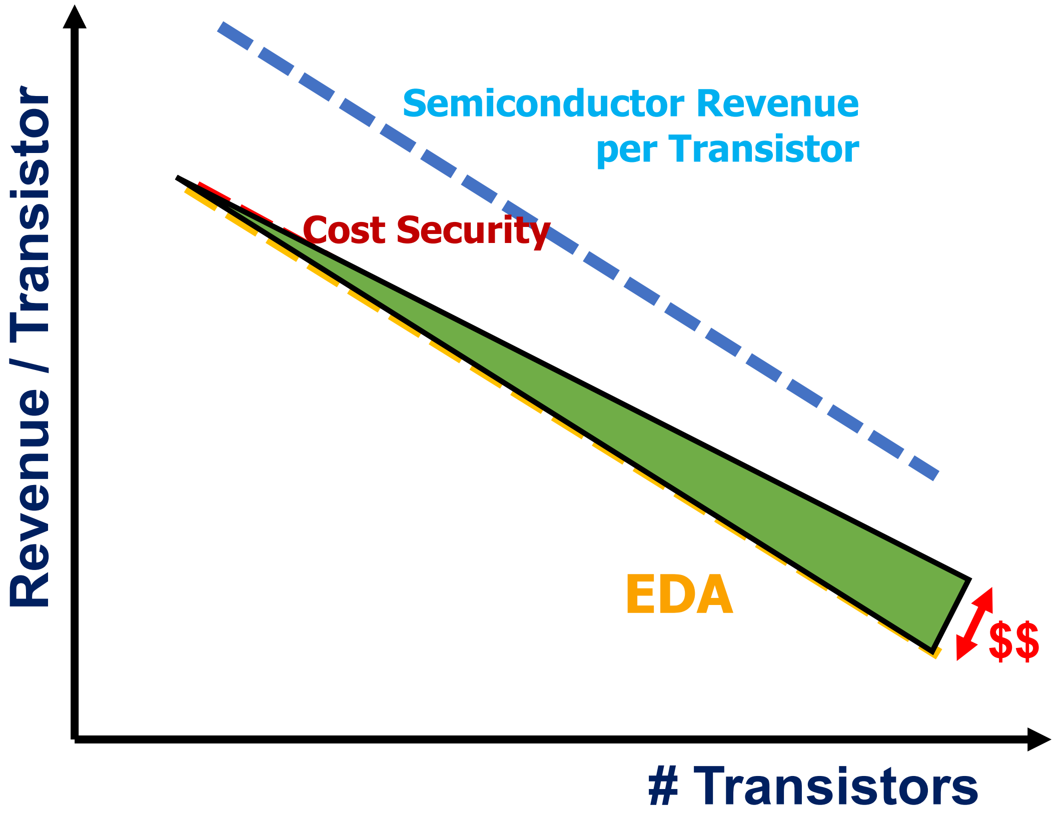
Journey to instill same rigor zeal and practices to semiconductor systems and below

Need Automation

PASS:

Power, Area, Speed, Security





Challenges: Vulnerabilities - Growing

- Fault Injection
- Privilege Escalation
- Trojan Insertion
- Trace Buffer
- EM Side-Channel
- CLKSCREW
- Denial-of-Service
- Vector Rewrite
- Rowhammer
- Power Side-Channel
- Direct Memory Access
- BranchScope
- Bitstream Encryption Cracking
- Plundervolt
- Access Control
- Meltdown and Spectre
- Machine Learning
- Information Leakage
- Trusted Execution Environment Breaking
- Reset and Flush
- Branch Shadowing
- Bitstream Tampering
- Reverse Engineering
- Timing Side-Channel
- Integrity

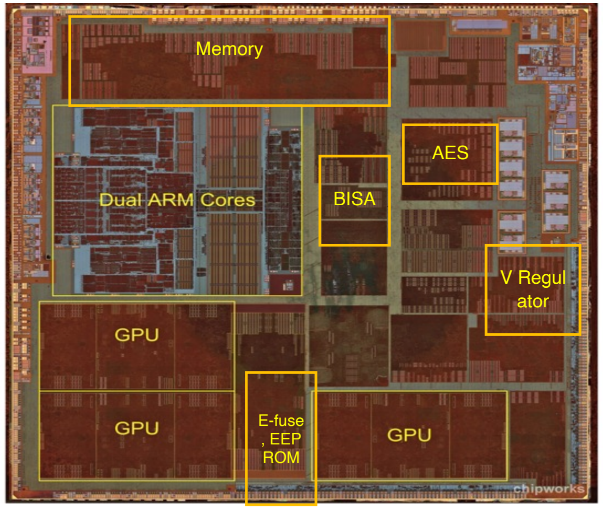
People: the weakest link!

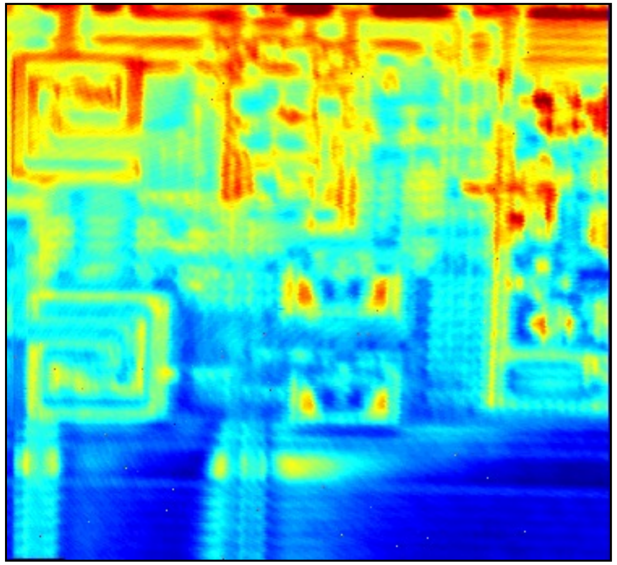
Strong Algorithm & Architecture

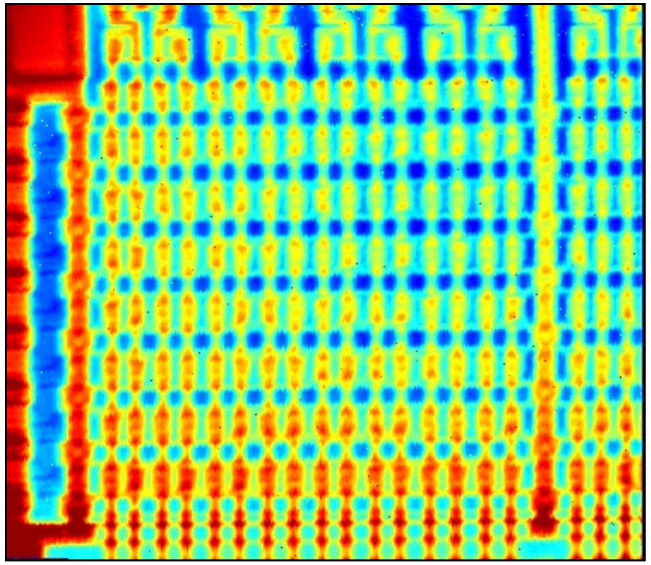
Weak Implementation & Execution

Unique to Physical Layout

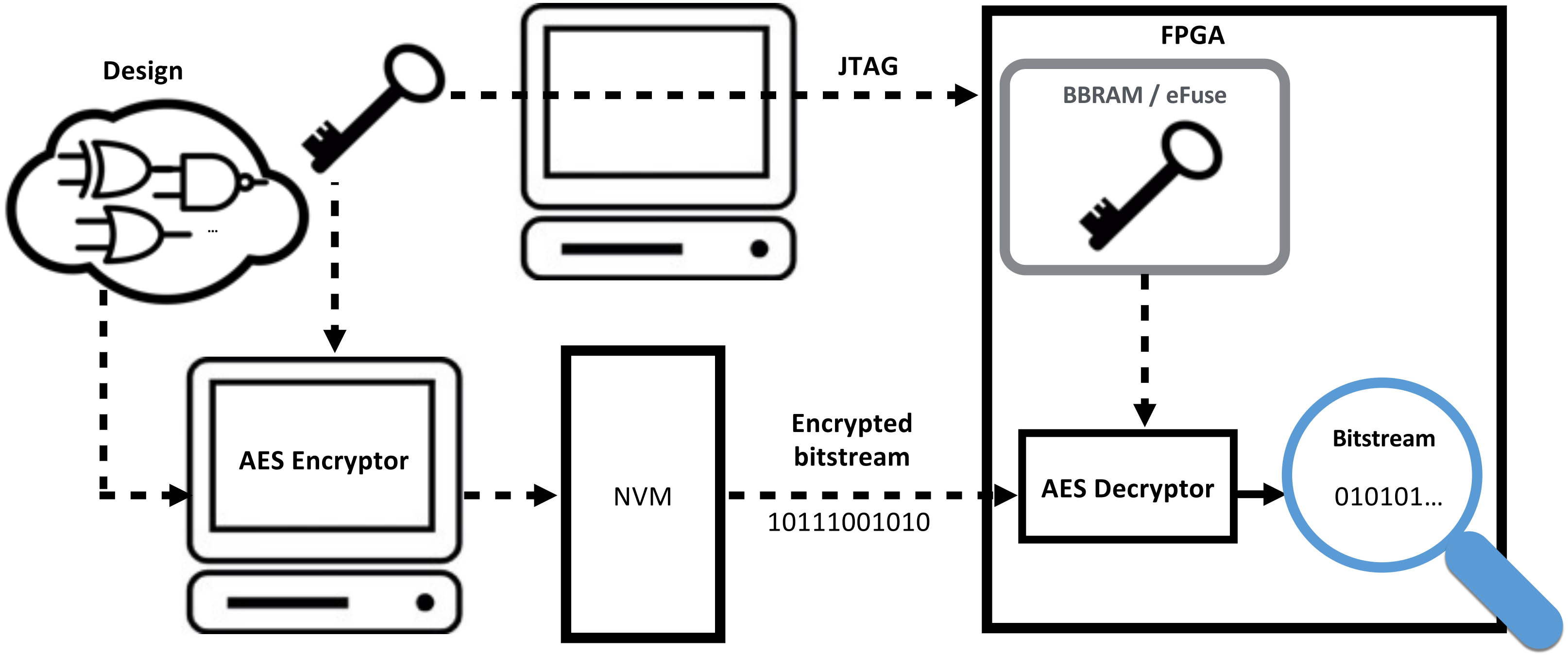
- **Protect against untrusted foundry**
- **Address IP piracy**
  - Physical Locking
- **Protect crypto cores**
  - Power side channels; EM Side channels; Fault injection
- **Protect physical attacks**
  - Contactless probing attacks; Contactless optical attacks; Laser fault injection attacks; X-ray attacks; Electromigration



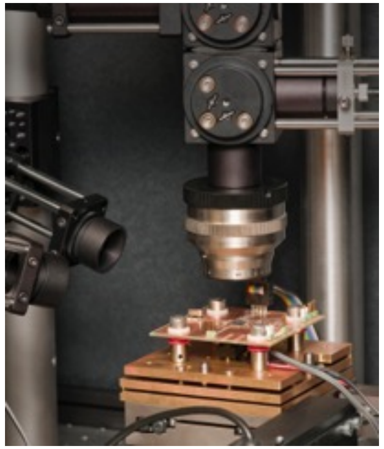


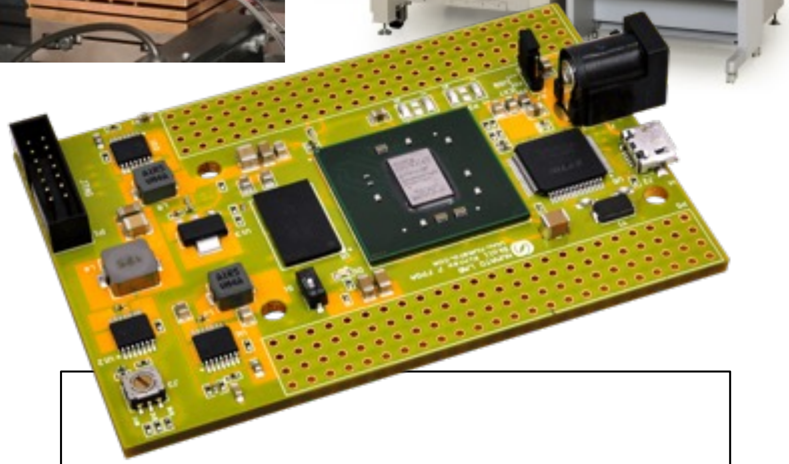


Chip Backside Is A New Backdoor



Hamamatsu PHEMOS - 1000





- Device under Test (DUT): Xilinx Kintex 7 development board
  - Chip’s technology: 28 nm
  - No chip preparation (e.g., depackaging, silicon polishing, etc.)
- Optical Setup: Hamamatsu PHEMOS-1000
  - Laser wavelength: 1.3 μm
  - Laser spot size: >1 μm

- Non-destructive
- Non-invasive
- No Footprint

Localizing the Configuration Logic

Xilinx Kintex 7 in flip-chip package

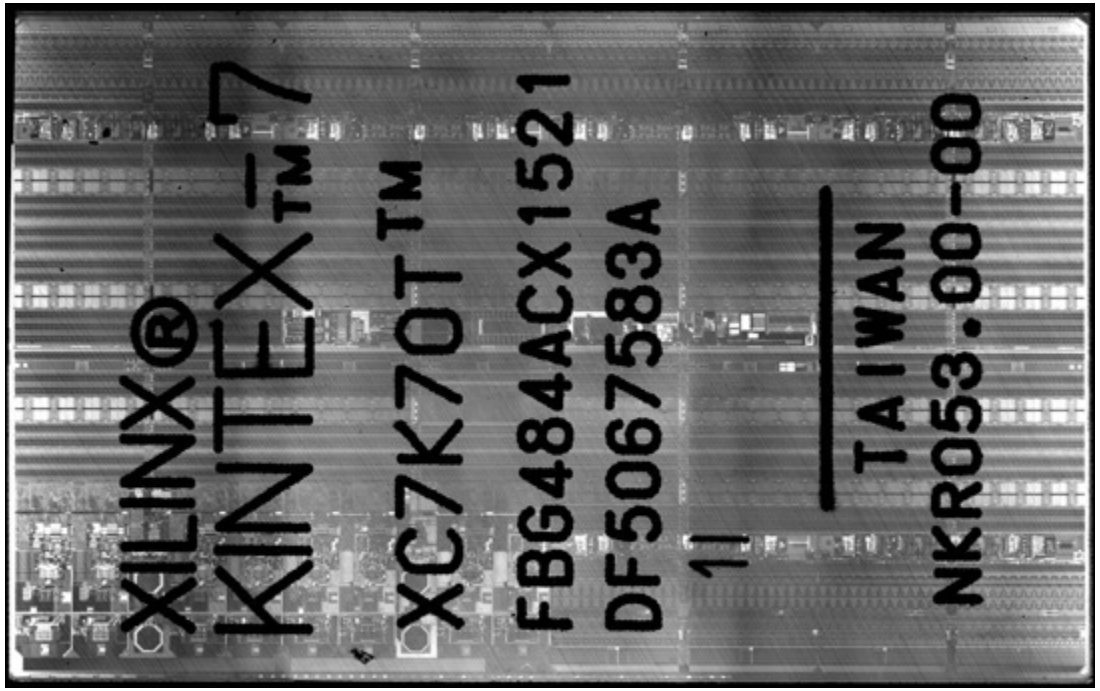
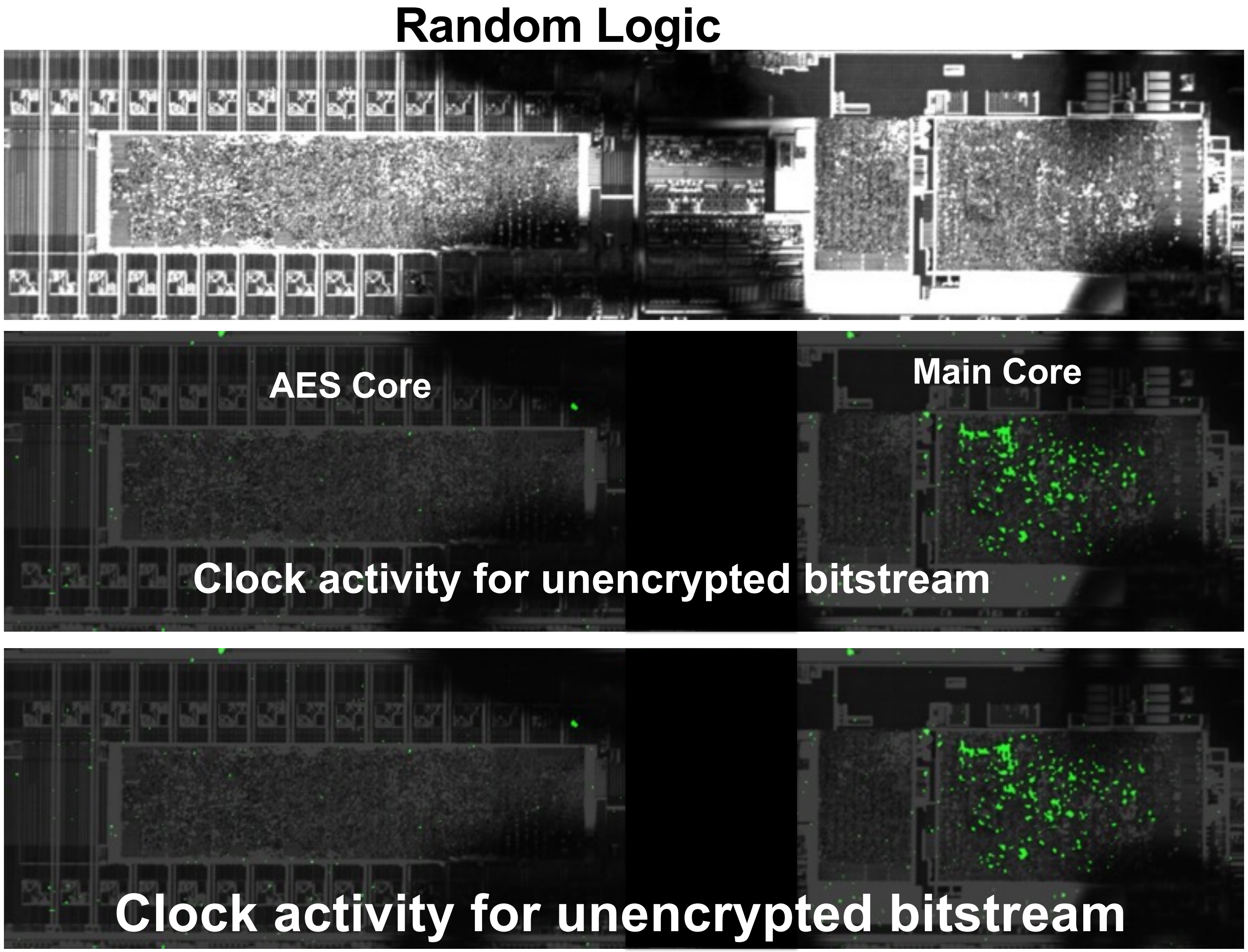
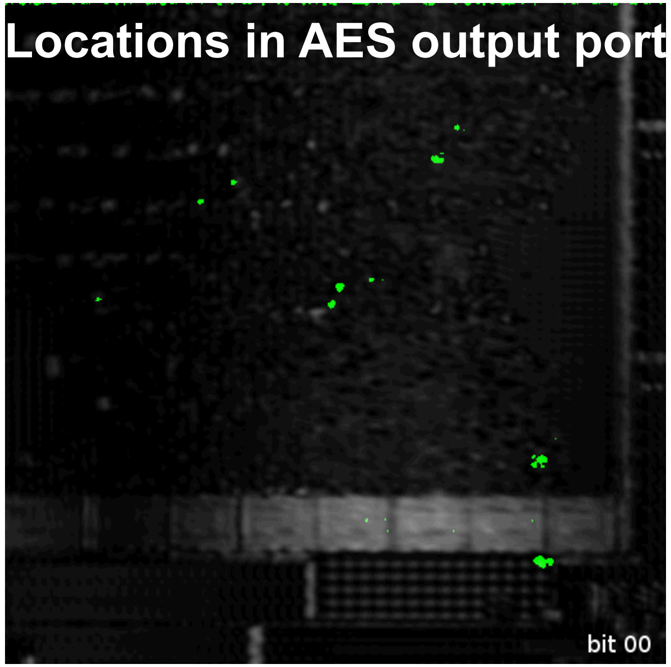


Image acquisition with a infra-red laser scanning microscope

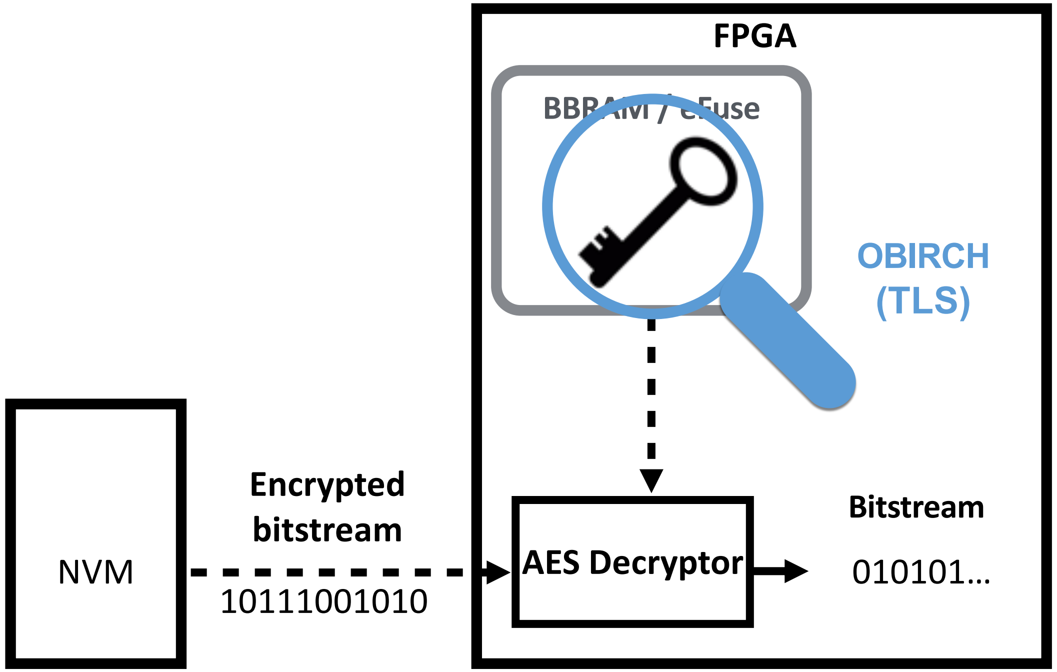
Tajik, S., Lohrke, H., Seifert, J. P., & Boit, C. "**On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs**," In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

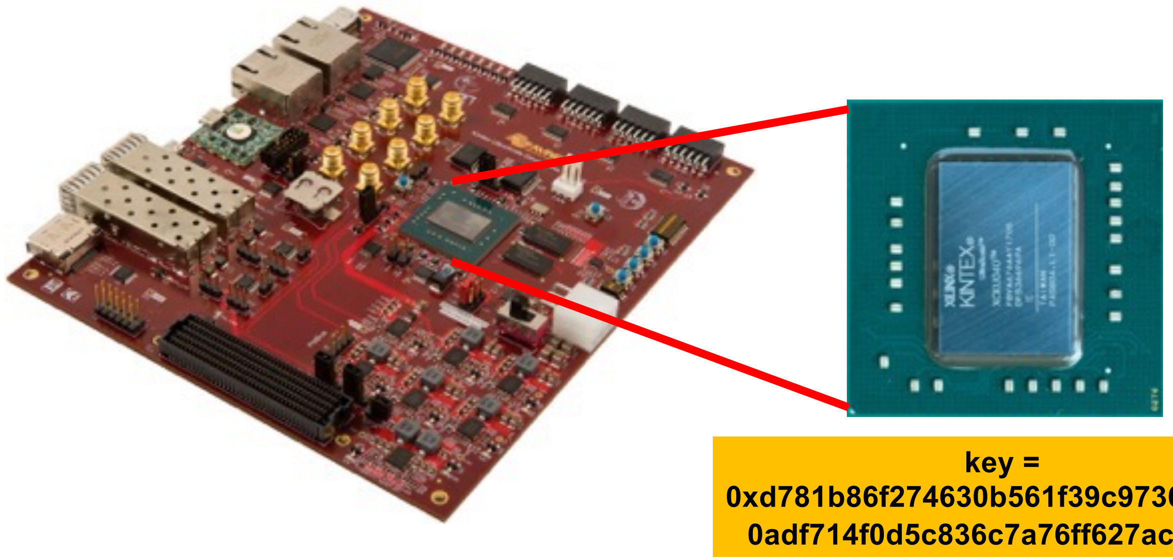
Localizing Decryption Engine


Random Logic
AES Core
Main Core
Clock activity for unencrypted bitstream
Clock activity for unencrypted bitstream



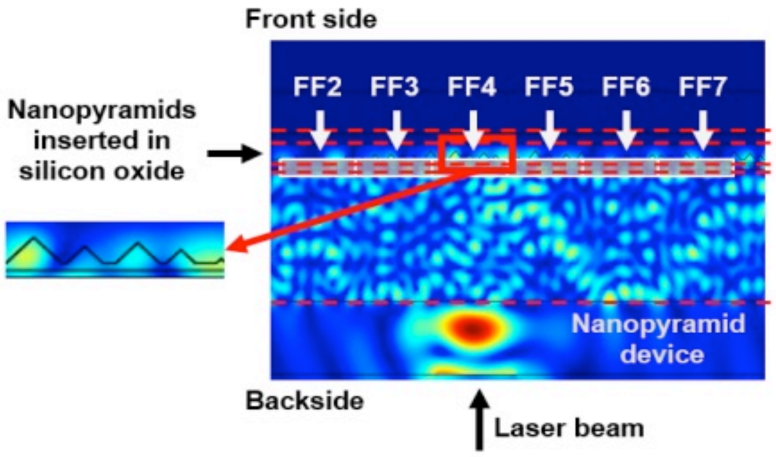
Key Extraction

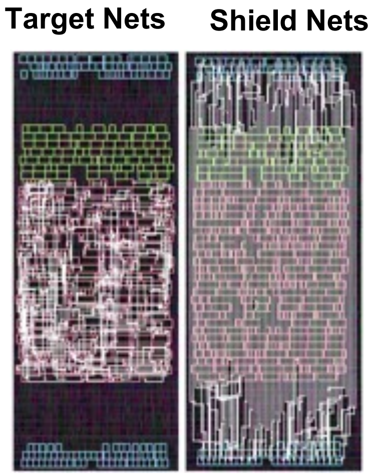




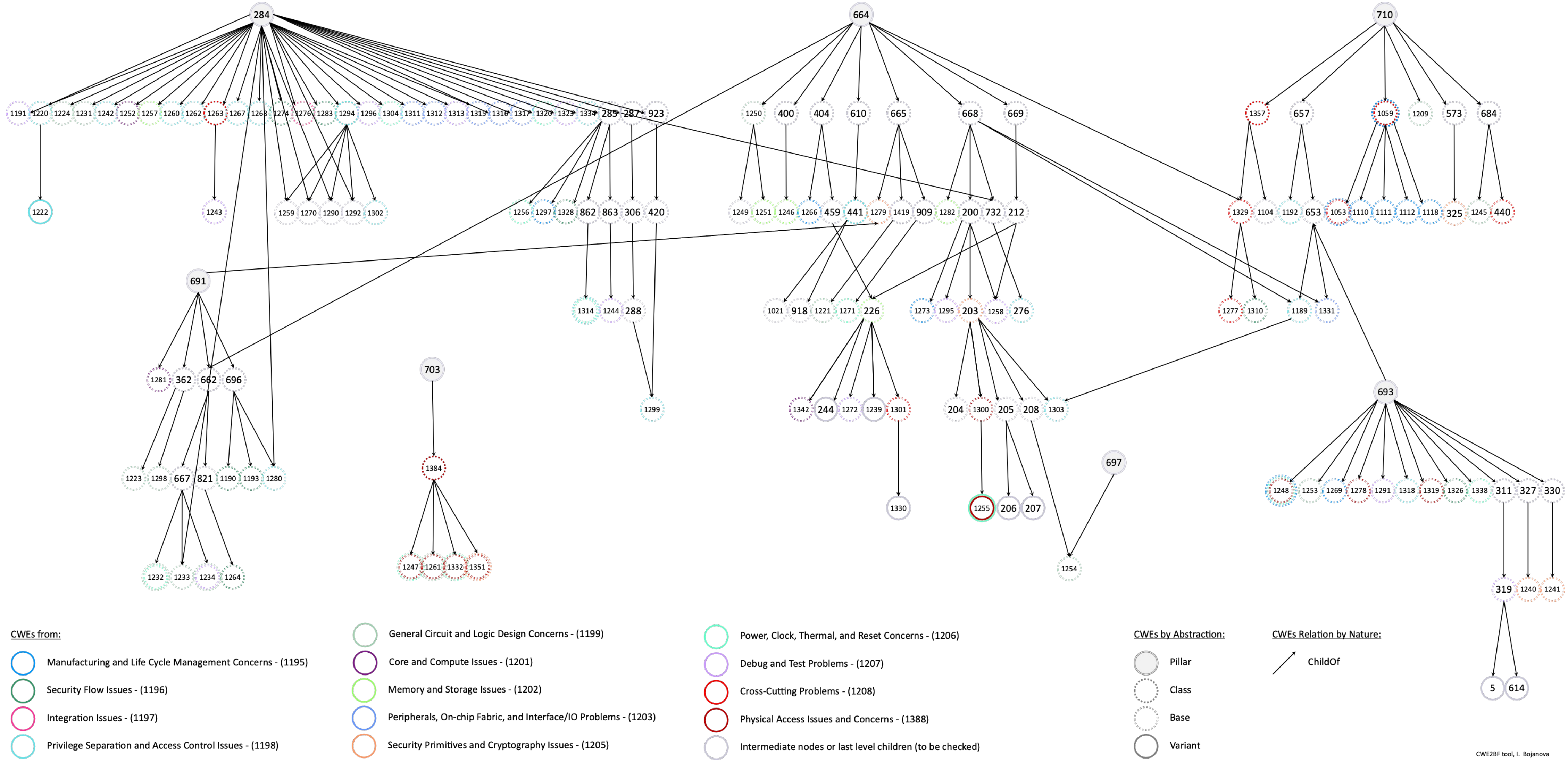
key =
0xd781b86f274630b561f39c9736f512eb
0adf714f0d5c836c7a76ff627aca4923

- **Protection**
  - **Circuit Level Solutions**
  - **Device Level solutions**
  - **Material Level Solutions**

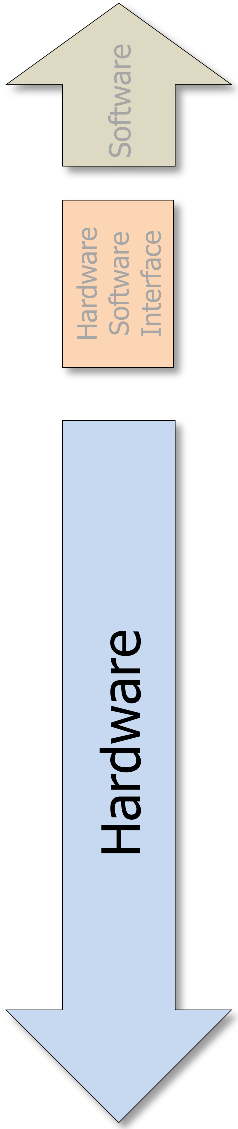




NIST Research: Hardware Weakness Hierarchies Looking at ‘how’ they are exploited



Attack Surface **Reference Model** SoC/ASICs)



Software

Hardware Software Interface

Hardware

- Substantial efforts are on-going in the software community

- Alteration of system behavior based on software-accessible points of illicit entry that exist due to hardware design weaknesses or architectural flaws

- **Side Channel** – extraction of secrets through physical communication channels other than intended (assumption: attackers are able to "listen" to emissions) → Economic Attackers

- **Reverse Engineering** – extraction of algorithms from an illegally obtained design representation (assumption: attackers have access to design files) → Economic Attackers *and* Nation States

- **Supply Chain** – Cloning, counterfeit, recycled or re-marked chips represented as genuine (assumption: attackers can manufacture perfect clones) → Economic Attackers

- **Malicious Hardware** – insertion of secretly triggered hidden disruptive functionality (assumption: attackers successfully inserted malicious function(s) into the design) → Nation States