ISPAB Review – Hardware Security Program

NIST

*Creating Helpful Incentives to Produce Semiconductors [for America]

Agenda

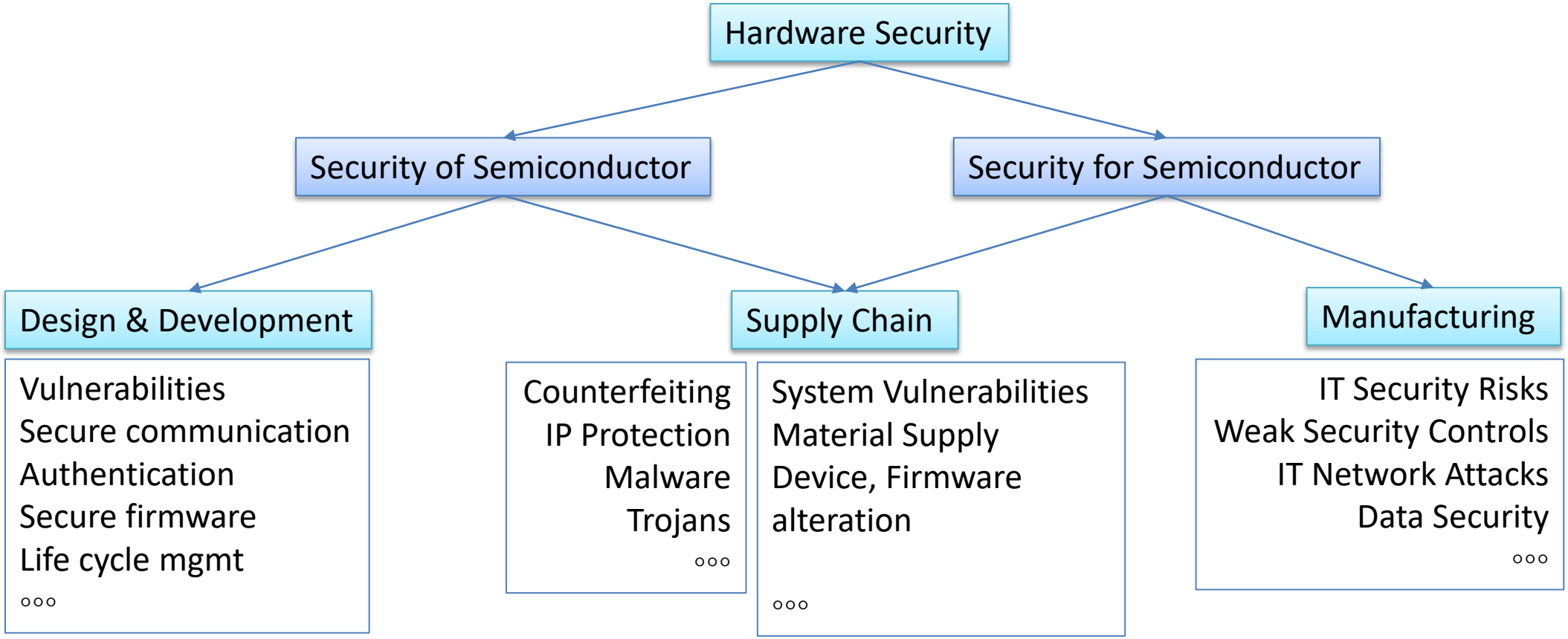
- Overview of Program
- CHIPS Act & NIST
- Challenge & Next Steps

Hardware Cybersecurity Program

Develop Standards, Guidelines, Best Practices, Reference Design Kits, Demos and Support Research in the field of **Semiconductor Design** Security and Trust

Why	• Cybersecurity challenges and Hardware vulnerabilities often go undetected • Semiconductor continues to be pervasive including for critical commercial and military applications - Cybersecurity and Assurance in Semiconductor Design Development and Across Supply Chain
What	• Collaborate with Industry to establish best practices for trust, security risks and vulnerability management across semiconductor development chain industry • Develop Secure Data Sharing practices and standards • Best Practices for IP Protection • Vulnerability detection and management best practices during development and post deployment • Establish trust/provenance across supply chain
How	• Tech Transfer of 'what' in industry: Reference Design kits, Standards bodies, Develop foundational builds with external partners to demonstrate use. • Leverage Applied Sec Division/NCCoE capabilities

Problem Statement & Scope



Example Challenges, not comprehensive

CHIPS at a Glance

Creating **H**elpful **I**ncentives to **P**roduce **S**emiconductors for America (CHIPS Act)

$52 Billion total budget over 5 years

Financial Incentives Programs

$39 billion

Research and Development

$11 billion

Technology Center
Packaging Program
MFG USA Institute(s)
Metrology program

Workforce Development

Not Passed Yet – 7/12/22

US Code: 15 USC 4652: Semiconductor incentives

NIST R&D for CHIPS

- NIST has a central role in the implementation of the CHIPS Act R&D
  - The pending funding vehicles includes significant funding for semiconductor R&D
- Established internal NIST task force across the different laboratories
- Connect research groups with different disciplines across NIST
- Investigate the development of the measurement science the semiconductor industry needs for next-generation manufacturing
- Connect across govt, industry and academia to solicit input around measurement needs across the different semiconductor areas

NIST Workshop on CHIPS

Semiconductor Metrology R&D Workshop Apr 6-7 and Apr 21-22

- Collection of Representatives from Numerous NIST Divisions
- Over 800 participants across Academia, Industry and Govt (40+% Industry)
- Purpose: Determine Prioritized List of Activities that NIST should pursue

One Panel focused on Security and Trust in Semiconductor – Apr 21 and 22

- Panelists from Industry – Matt Areno/Intel
- Academia – Mark Tehranipoor/University of Florida
- Govt/Research – Serge Leef/DARPA (now Microsoft)
- Industry/Research – Bill Tonti/IEEE-Future Direction

Several Grand Challenges Identified including for Security and Trust in Microelectronics

Security and Provenance of Semiconductor

Challenge: Advance the state of metrology needed to enhance the security and provenance of devices and packaging across supply chains and increase trust and assurance.

Strategy: Pursue a comprehensive approach to hardware security protection that includes standards, protocols, formal testing processes, and advanced computational technologies—providing avenues for assurance and provenance of devices across the supply chain.

The Path Forward

Conduct activities to support development of standards, protocols, and testing processes for analysis of security vulnerabilities in microelectronics across their entire their life cycle. Critical areas of pursuit include:

- Methods, reference design kits, and guidelines for security analytics and automation to include pervasive security to address formalized threat models.
- Enhanced vulnerability management across the overall product life cycle from inception to end-of-life, including activities such as
  - Formal testing and processes for independent verification and validation.
  - Tracking of materials and components, detecting, and mitigating trigger mechanisms.
  - Common test structures, test methods, and test and measurement strategies for end-to-end provenance.
- Build & Use of trusted techniques, e.g., Artificial Intelligence and Machine Learning methods across the entire semiconductor value chain
- Documentary standard for hardware security and provenance.

Path Forward Contd ..

Grand Challenge: Standardizing New Materials, Processes, and Equipment for Microelectronics

- Standards for interoperable equipment and software from different vendors that ensure the protection of intellectual property (IP), data integrity, and provenance across the supply chain

Summary

- State of Hardware Security, Challenges and Path Forward identified
- Proposed research and application ideas:

Security Engineering Principles, Physically Unclonable Functions to detect Counterfeits, Secure Hardware Development Framework (~SSDF) for eAsic or similar, Security Design Rule Checkers, etc.	System Assurance and Provenance Across Supply Chain with Root of Trust & Measurement, Side channel attack detection, etc	Cybersecurity Framework for Semiconductor Manufacturing, ~NICE Framework for r Hardware Security W/F Development	Data Security and System Security Standards, IR, Guidelines, Obfuscation, Reference Design Kits, extension of DARPA Security work, e.g., SAHARA, etc.