Semiconductor Research Corporation

PIONEERS IN COLLABORATIVE RESEARCH®

Panel 1: Motivation for Action

Benjamin Jun / Cryptography Research, Moderator

Mark Tehranipoor / UConn CHASE

Serge Leef / Mentor Graphics

Saverio Fazzari / Booz Allen Hamilton

Bruce Newgard / Xilinx

Bob Bell / Cisco

Paul England / Microsoft Research

T3S

Semiconductor Research Corporation

PIONEERS IN COLLABORATIVE RESEARCH®

Mark Tehranipoor

Charles Knapp Associate Professor in Engineering Innovation

Center for Hardware Assurance, Security, and Engineering (CHASE)
Comcast Center of Excellence for Security Innovation (CSI)

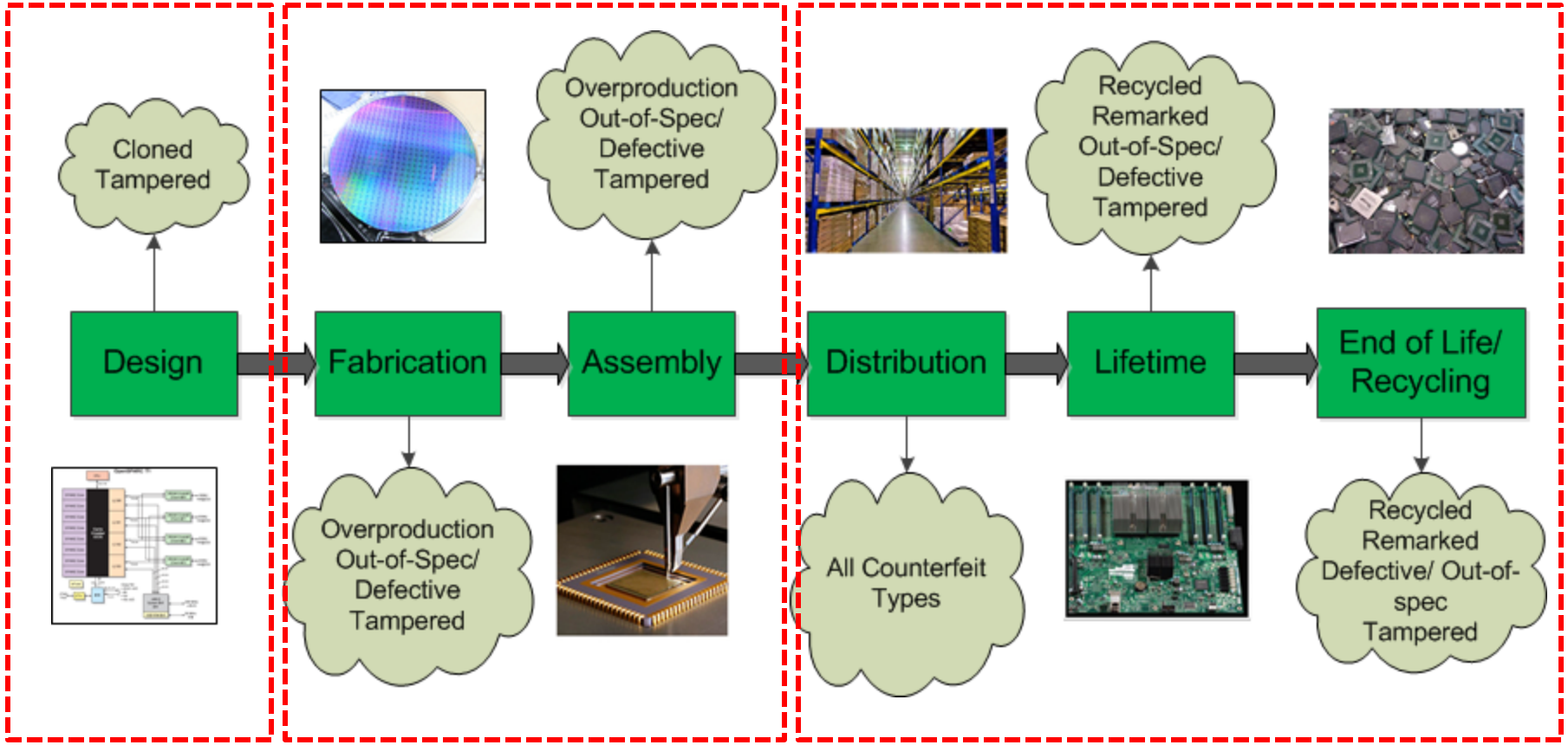
CHASE

UCONN

T3S

www.chase.uconn.edu

Supply Chain Vulnerability



Untrusted IP Vendor & Sys. Integ.

Untrusted Foundry & Assembly

In the Field & Recycling

Maximum Flexibility ← → **Minimum Flexibility**

Grand Challenges

Immediate Needs

- Security at the low levels of abstraction should NOT be an after thought anymore
- Improve supply chain security
  - Untrusted foundry and assembly
    - IP, design flow, and IC
  - More effective chip/device identification and authentication

3-5 Years

- Metrics for security assessment
- Development of robust security primitives
  - Anti-reverse engineering
  - Anti-tampering
  - Anti-counterfeit
  - More …
- Advanced track & trace
- Development of standards

5-10 Years

- Development of innovative silicon authentication platform
  - To reduce area and power
  - Offers solutions such as PUF, TRNG, sensing capability, COA, anti-tampering, cloning, anti-Trojan, etc.

Continuous Attack Analysis and Understanding of Vulnerabilities

Semiconductor Research Corporation

PIONEERS IN COLLABORATIVE RESEARCH®

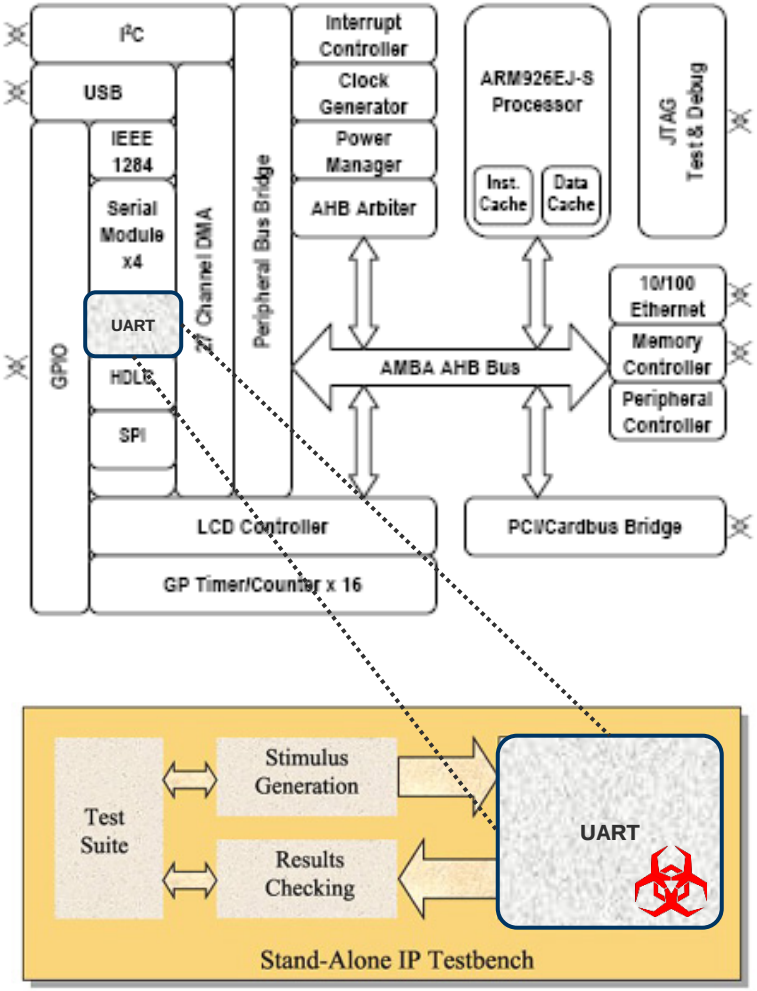
Serge Leef

VP, New Ventures

GM, System Level Engineering Division

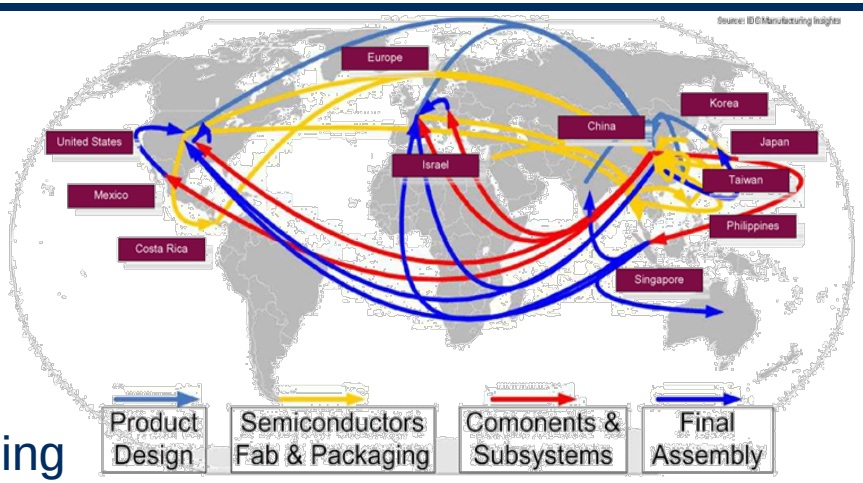
Mentor Graphics Corporation

Threat: IP as a Trojan carrier



- In a typical IP-based design, each block can originate from different sources
- Incoming IP blocks are verified to confirm promised functionality
- Additional verification may be done to confirm proper interaction with other IP blocks operating in the system context
- A key question that does NOT get asked in this process is: “does this block do anything ELSE?”

Risk: “Chain of custody” no longer workable



Mitigation Strategies:

Authentication circuits

- Embedded ID + Crypto engine
- Challenge/response dialog

On-chip odometers to address recycling

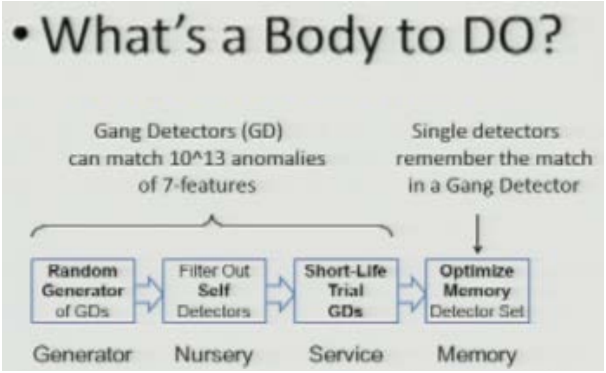
- On chip structures that count some physical events like power cycles, memory accesses or other inexpensively measurable values
- Data in the odometer is encrypted; reset to ‘0’ indicates an attack
- Can be accessed at the authentication time

Activation – chips do not work as manufactured

- Only the IP rights holder would have the keys needed to activate chips
- Different degrees of activation need to be offered to enable the customer to make trade-offs between security and costs
- Pre-existing test methods should be accommodated
- Power-up, event-based or periodic activation offers highest security

Grand Challenges

- Near term: Recognition of the problem
  - Skepticism in the hardware design community
  - Change can be driven by crisis or strong top-down requirements
- Medium term: Industry/Government collaboration
  - Handed down policies are ineffective & quickly obsolete
  - Ambiguous economic incentives for compliance
  - Partnership with technological countermeasure vendors
- Long term: Methods for finding Unknown Unknowns
  - Proactive anomaly detection:
    - Mimicking biological systems
    - Search for zero-day bugs
    - Very large number of varieties
    - Most are first time encounters
    - Use immune system as a model*



*Source: Rick Dove, Paradigm Shift International, COFES 2014
http://cofes.com/ADMIN-STUFF/Video/Video-Player/VideoId/295/MP2-Rick-Dove-Paradigm-Shift-International.aspx

Semiconductor Research Corporation

PIONEERS IN COLLABORATIVE RESEARCH®

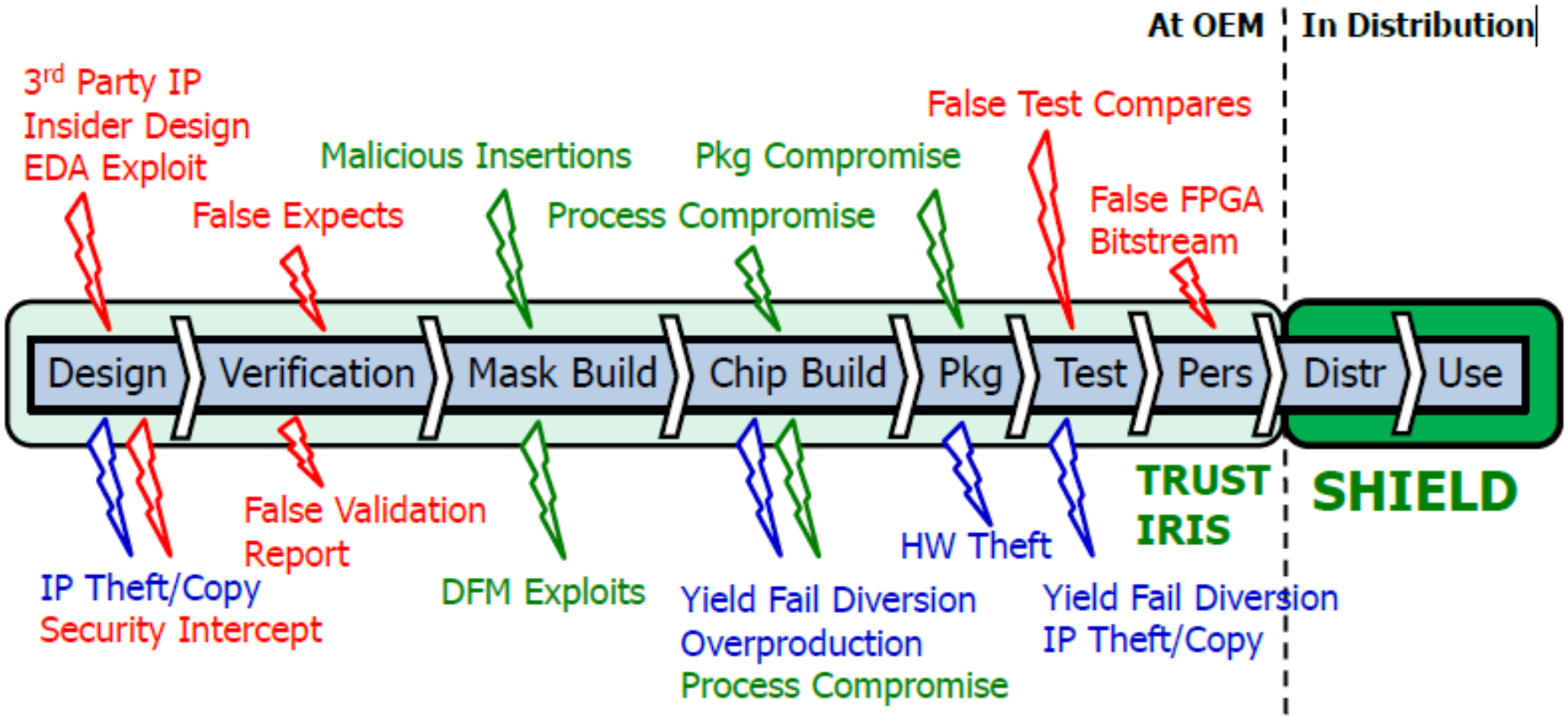
Saverio Fazzari

Booz Allen Hamilton

T3S

TRUST, IRIS Programs Validated Design Preceding Distribution:
- SHIELD Will Take it From There

LEGEND: Design Attack - Hardware Attack - Logistics Attack



DARPA TRUST and IRIS Programs developed techniques for validating the design and process integrity before distribution.

Semiconductor Research Corporation

PIONEERS IN COLLABORATIVE RESEARCH®

Bruce Newgard

Director, Product Planning

Xilinx, Inc.

XILINX

ALL PROGRAMMABLE™

T3S

Today's World

- I rob banks because that's where the money is
  - Attributed to **Willie Sutton**

- Systems are attacked today because the information (IP, User data, etc.) is valuable
  - Economically
  - Militarily

View From the Foundation (H/W)

- Threats (not exhaustive)
  - Side channel attacks such as DPA & EMI
  - Environmental Attacks (e.g. Temp, Voltage)
  - Counterfeit Si (reclaiming, re-marking, up-screening)
  - Focused Ion Beam (FIB)
  - Memory Imprinting
  - IP protection - copying & modification
- System & H/W designers must understand and mitigate all or most of most of the attack vectors

Basic Requirements

- Security MUST be designed in early
  - Difficult & costly to add security after design stage
- For system to be secure, the H/W MUST be trusted and boot securely
  - Solid foundation which to build on
- Trust and authentication must be established BEFORE the system can process data

Si Grand Challenges

- Near term
  - Low to zero penalty to invoke security features
  - Trusted Si & IP
  - Resistance to attack vectors (e.g. DPA)
- Medium term
  - Si, Tools & IP- correct by design, no “extra” or dead code
  - Counterfeit-proof
- Long term
  - Supply Chain – manufactured anywhere in world – trusted and secure by design
  - Life cycle management – cradle to grave tracking and authentication

Semiconductor Research Corporation

PIONEERS IN COLLABORATIVE RESEARCH®

Bob Bell

Senior Product Security Architect, TRIAD

Cisco Systems

CISCO

T3S

View from the Trenches

- Hack and Shack attacks becoming better with low-cost access to better tools
- Lab attacks becoming better through outsourced tools and expertise
- Nation State attacks are confirmed not theoretical any more!
- Customers are not DEMANDING security and integrity in the products
  - At least that is what Product Marketing keeps saying
  - This drives adoption into products

Grand Challenges

- Near term –
  - Overcome reluctance to add security and integrity functions into products
  - Increase accountability of manufacturing partners
- Medium term –
  - Raise the bar to tampering and modifying of equipment by several orders of magnitude
  - Build in stronger IP Protection measures all along the supply chain
- Long term –
  - Develop new and stronger methods to detect hardware and software “Trojans” which are commercially usable

Semiconductor Research Corporation

PIONEERS IN COLLABORATIVE RESEARCH®

Paul England

Software Architect

Microsoft

The View from Above

Secure and Trustworthy Hardware from an OS & Service Perspective

T3S

A Decade of New/Improved Security Tools

The Cloud	Data Centers: Your life in the cloud
Appliances	Phones, Tablets, Game consoles...
App Model	Better App-containers, White-Lists, App-Stores
OS-Lockdown	Kernel-Lockdown, Measured Boot
Hypervisor-Security	Hypervisors for Security Isolation + Invariants
New CPU Modes	ARM-TrustZone, SGX, VT, Security Processors
Secure Boot	TPM-Based Measured Boot, UEFI Secure Boot
TPM	Key Storage, root-of-trust

Grand Challenges

- Near term
  - Use the tools!
  - Executing well
    - Certainly a “grand challenge”
  - Security usability:
    - make it hard for users to make poor choices
- Long term
  - Coexistence of security and openness
  - Supporting both strong identity and anonymity
    - On the Internet nobody knows you’re a dog
  - Secure by construction or proof:
    - hardware, runtimes, languages...