Trustworthy Semiconductor Design and the IP Business

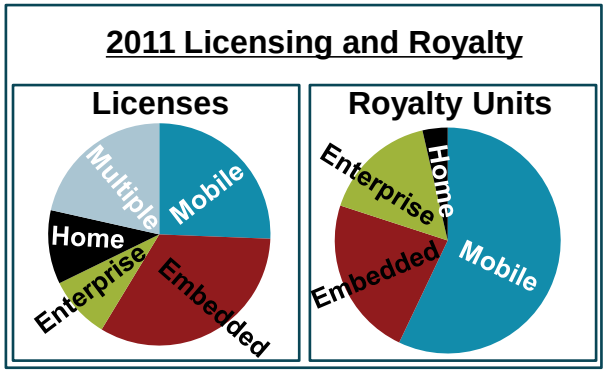
Convergence of Software Assurance Methodologies and Trustworthy Semiconductor Design and Manufacture Workshop, January 2013

Rob Aitken

ARM Fellow, San Jose CA

What Sorts of Things Use ARM?

- Mobile devices plus many others
- (Corporate Marketing makes nice slides)
- Vastly different security needs



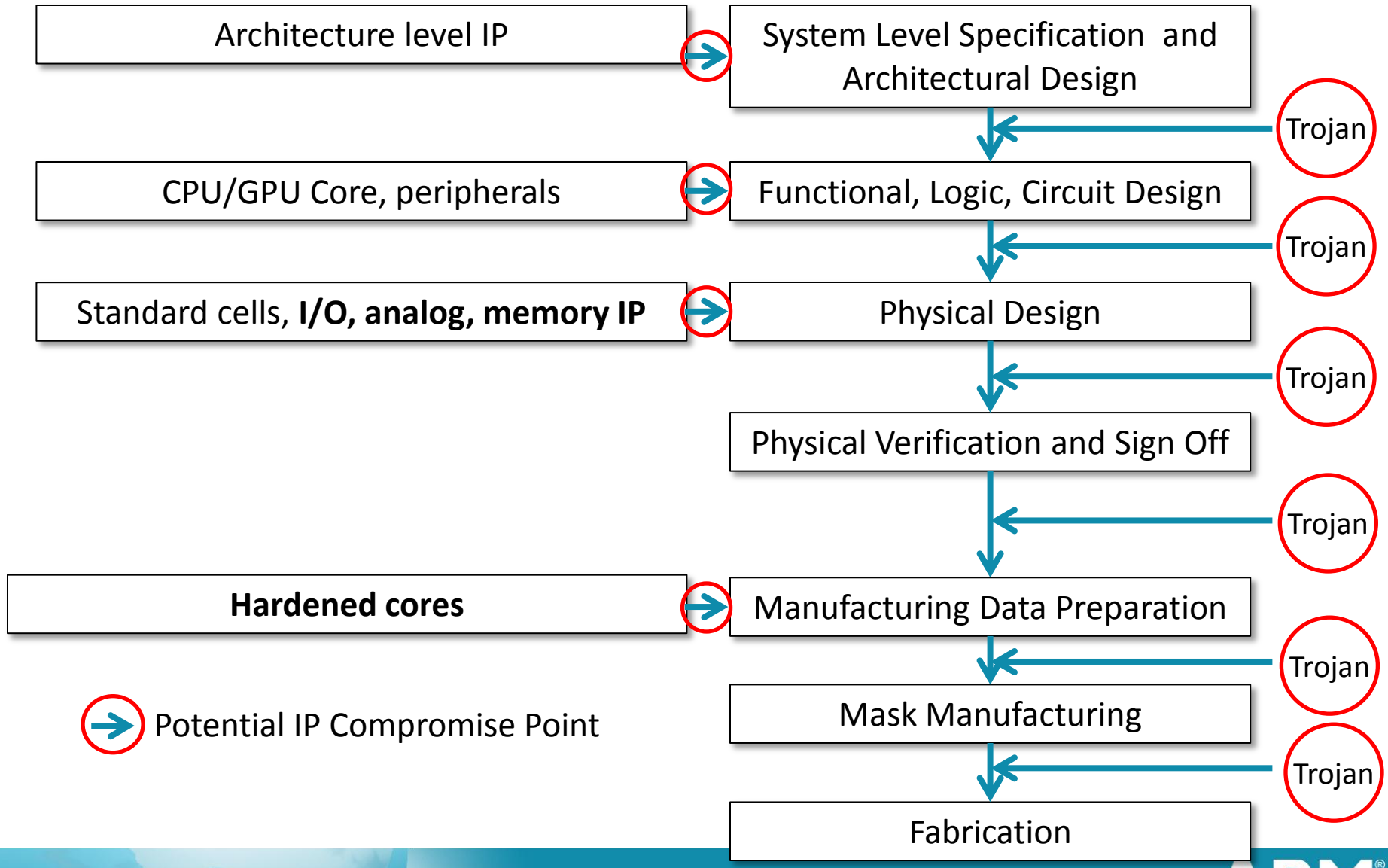
Mobile	15%	4.5bn in 2011
Embedded	70%	1.8bn in 2011
Enterprise	30%	1.3bn in 2011
Home	10%	0.3bn in 2011

Product Categories

- Architecture level IP
  - License to develop a processor compatible with an instruction set
- “Soft IP”
  - CPU/GPU cores, peripherals, interconnect
- “Hard IP”
  - Standard cell libraries, I/O pads
  - SRAM instances, analog IP
  - Hardened CPUs

The Architecture for the Digital World®
ARM®

Design Flow IP Vulnerability Points



The Architecture for the Digital World®
ARM®

Product Categories

- Architecture level IP
  - License to develop a processor compatible with an instruction set
- “Soft IP”
  - CPU/GPU cores, peripherals, interconnect
- “Hard IP”
  - Standard cell libraries, I/O pads
  - SRAM instances, analog IP
  - Hardened CPUs
- “Evil IP Company” model would be difficult to pull off successfully
  - Thousands of licensees, lack of control, too many eyes
- “Selectively Malicious” somewhat more plausible
  - Single corrupt transfer, rogue employee or design contractor
- Similar logic applies to software vendors

The Architecture for the Digital World®
ARM®

OMTP Security Requirements

GLOBALPLATFORM

Reference for Mobile Platform Security and Trusted Execution Environment

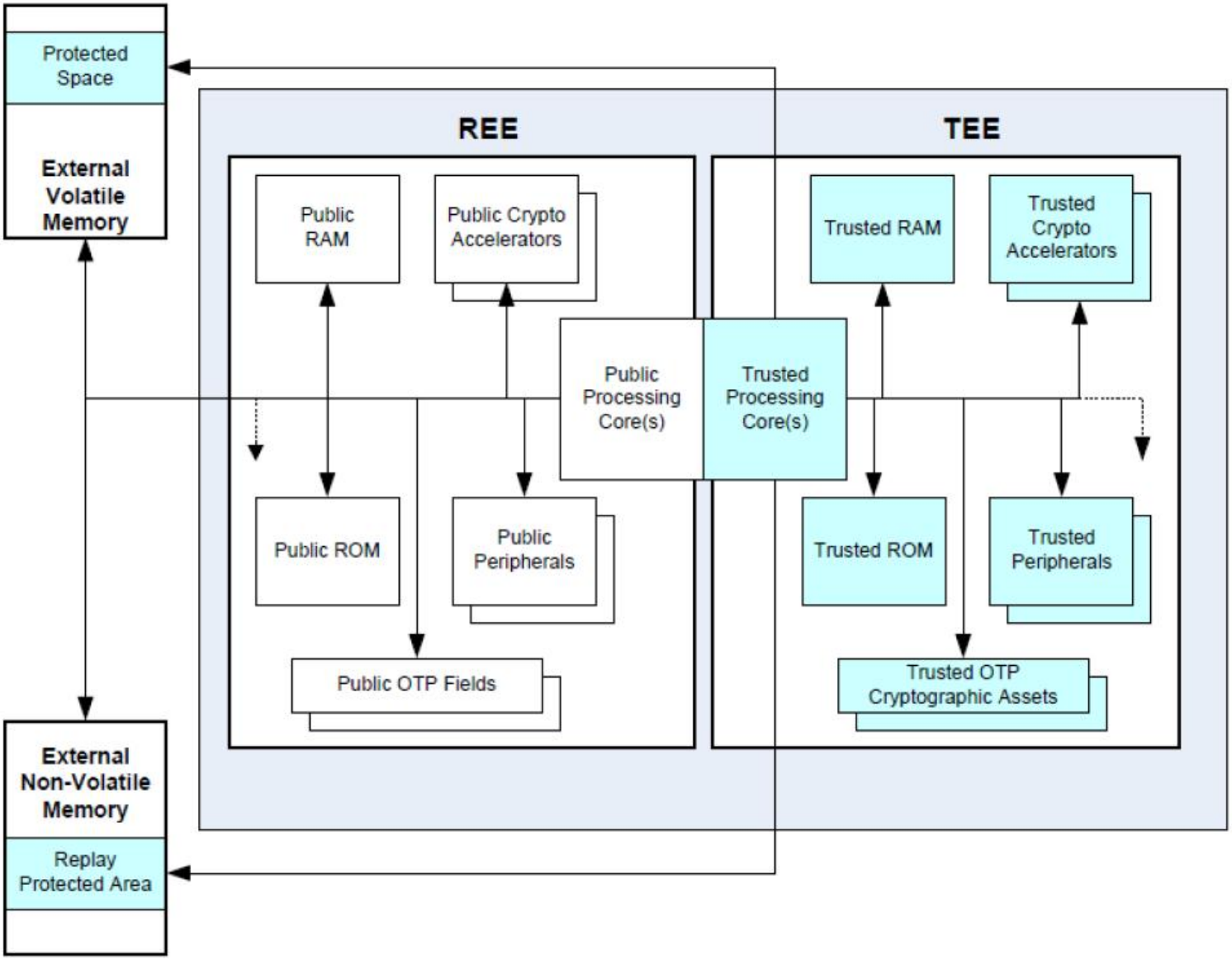
- Trusted Environment TR0 *(V1.2 – May 2009)*
  - Hardware Unique Key
  - Debug Port Protection
  - Secure Boot and Secure Flash Update
  - IMEI & SIM Lock Protection

- Advanced Trusted Environment TR1 *(V1.1 – May 2009)*
  - Isolated environment from main mobile OS
    → Trusted Execution Environment
  - Secure storage
  - Flexible secure boot
  - Secure communication with USIM and key exchanges
  - Runtime Integrity Check
  - Secure User Interface

http://www.gsmworld.com/newsroom/document-library/omtp.htm

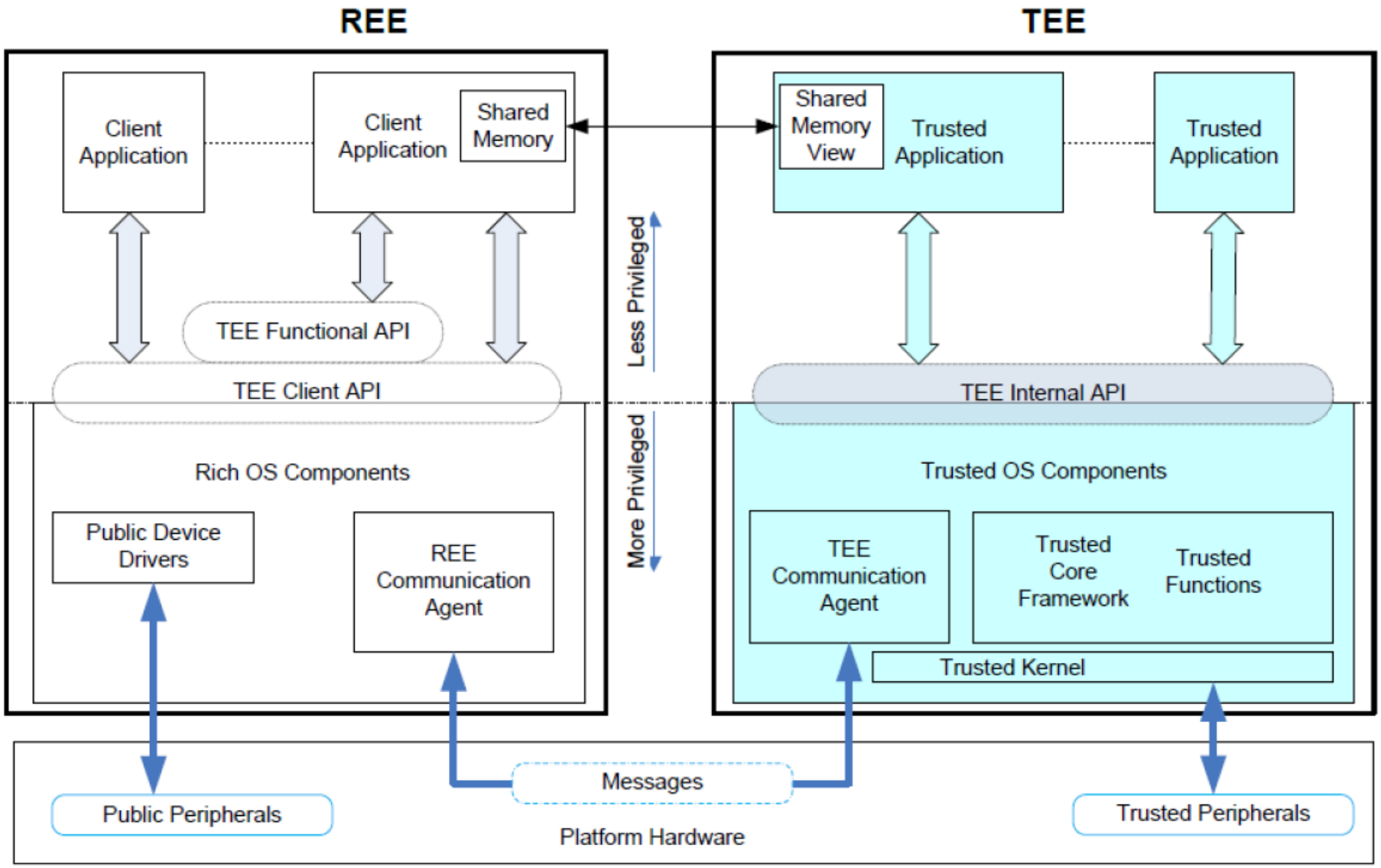
GlobalPlatform TEE HW System Architecture

GLOBALPLATFORM



GlobalPlatform TEE SW System Architecture

GLOBALPLATFORM



Summary

- Multiple levels of security being implemented across hardware and software for e-cash, video, etc.
  - Designed to thwart teenage hackers, “Fred in the Shed”, economically-motivated larger-scale players
  - Mostly not intended to prevent attacker with unlimited resources from causing trouble (decap, FA lab, FIB, etc.)
    - Attempt to minimize subsequent damage from such attacks
- This security is both a problem and an opportunity for hardware Trojan detection
  - Provides infrastructure for trust
    - Education of issues
    - Place to insert efforts
  - May hamper detection methods (e.g. Smartcard side channel security features)

The Architecture for the Digital World® ARM®

Complication: Power Intent

- Power intent conveys semantic content not present in standard design flow
- Examples: voltage domain control, power gating, leakage mitigation modes
- Multiple paths for information to traverse design steps

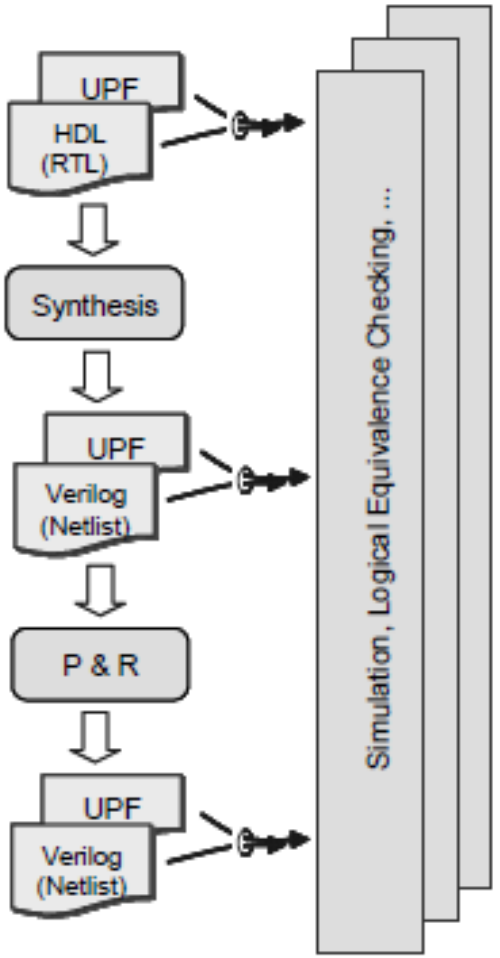
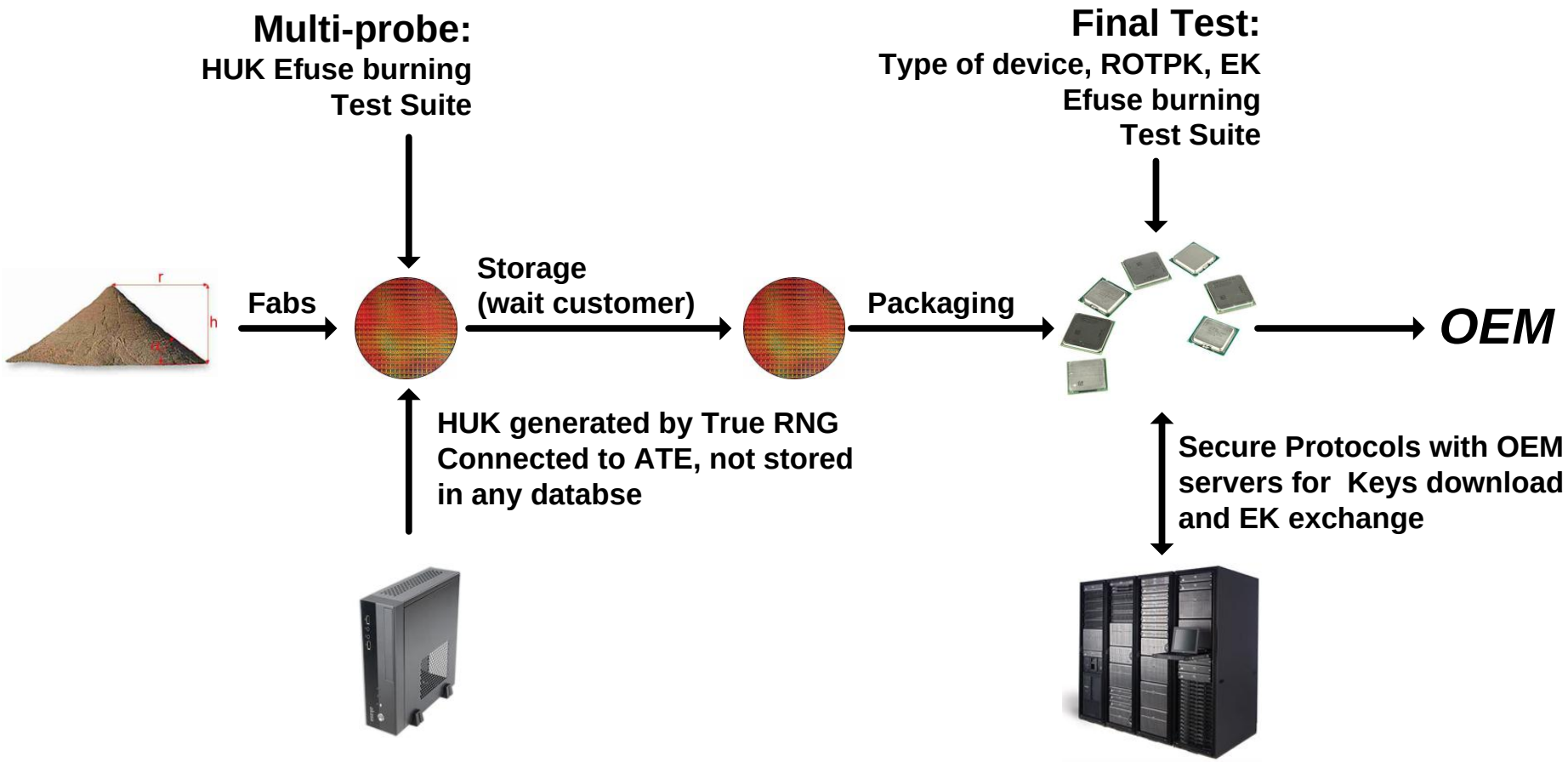


Figure 1—UPF tool flow

The Architecture for the Digital World®
ARM®

Trusted Test Manufacturing & Factories



- Multi-site (possibly multi-country) flow

The Architecture for the Digital World®
ARM®

Opportunity (Test)

- ATPG (Automated-Test-Pattern-Generation)
  - Scan-in and Scan-out to identify failing logic
- BIST (Built-In-Self-Test)
  - Automatic test of SoC memory such as ROM and SRAM.
- At speed tests
  - Functional tests used for speed binning and reproducing specific full speed patterns not detected by structural test
- Many others tests
  - DC Parametric (DC current/voltage test for shorts and opens)
  - IDDQ (measuring the supply current (Idd) in the quiescent state).
- Application Mode
  - Normal functional boot with Rich OS and Trusted OS

The Architecture for the Digital World®
ARM®

What's The Motivation?

- Key theft
  - Single key theft versus widespread
- ID theft
  - Some personal data more valuable than others
- Counterfeit Keys/Products
  - Illicit sales, financial system compromise, jailbreaking, DRM
- Denial of Service
  - Hackery, national security
- On-board Security Compromise
  - Various malicious intent (e.g. sniffing, logging)
- Example attack
  - The device boots in application mode, the TEE is used and consequently the SoC SRAM & L1/L2$ are full of trusted assets (keys)
  - A switch to BIST, ATPG, or at-speed manufacturing mode is performed and the attacker patches the TEE memories with its own code and then switches back to application mode.

The Architecture for the Digital World® ARM®

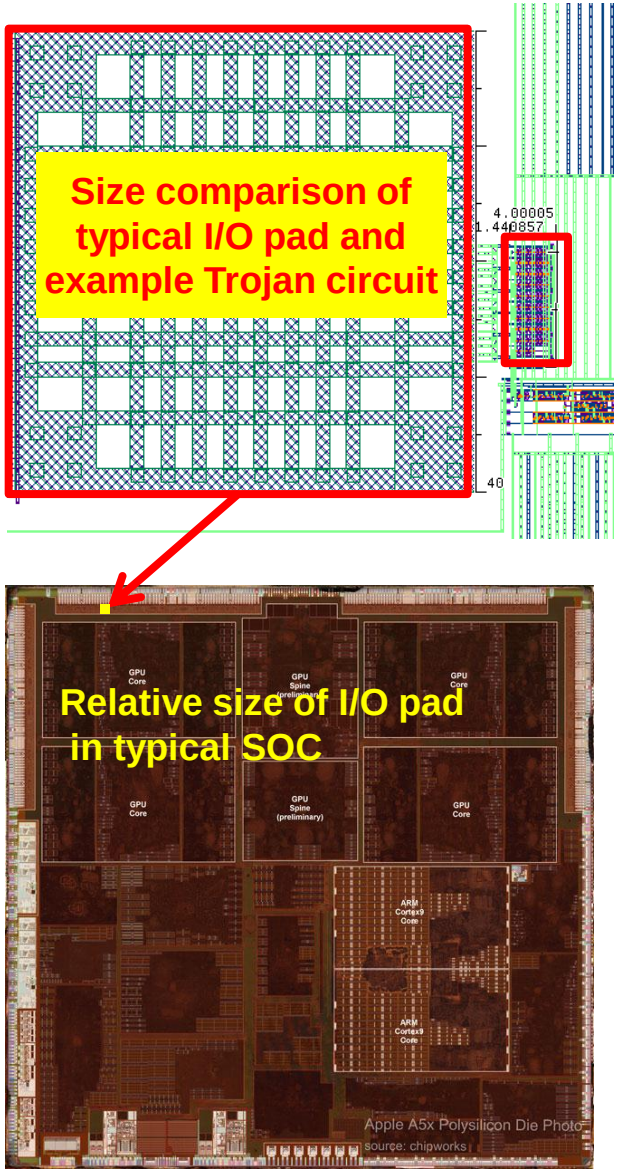
Opportunities for Detection

- Many approaches not viable in a world of 100M+ transistor designs and hardware designed for attack prevention
  - Power signatures, EMI monitoring, etc.
- “Reachable” H/W
  - Find transistors, make sure there is an explanation for them elsewhere in design spec (“super LVS”)
  - Challenges: spare gates (deliberately unreachable), fets2gates, analog circuits, complex functionality
- Memory scrubbing
  - Part of trusted test process
  - Force Trojans to be hardware based or hide their memory
- Disable test/debug circuitry
  - Often part of trusted test process
- Execution-time checking
  - Make use of trusted execution environment

The Architecture for the Digital World® ARM®

Simple Trojan: Denial of Service Circuit

- Counter (~40 bits)
  - Counts to large predetermined value
    - Large enough that it is not hit accidentally during test or burn-in
    - Small enough that it will trigger when needed
  - Shorts power and ground buses when match hit
  - Hide in I/O circuits or power distribution network (logically isolated)
  - <500 transistors (<0.0005%)
    - Area ~45um^2 @ 28nm, leakage <1uA, dynamic current needs to be managed (e.g. tap system clock or not)
- This type of trigger is probably useful for other purposes



The Architecture for the Digital World®
ARM®

Hiding In Plain Sight (Example)

- Few people understand debug circuitry
- Few people understand cache behavior
- Fewer people understand interaction of both, use for attack
- Embed virus code in simple ROM, load into cache
- Disable trust hardware as needed via debug

The Architecture for the Digital World®
ARM®

RAM Erasing?

Cryogenically frozen RAM bypasses all disk encryption methods

By George Ou | February 21, 2008, 11:59pm PST

Summary: *Computer encryption technologies have all relied on one key assumption that RAM (Random Access Memory) is volatile and that all content is lost when power is lost. That key assumption is now being fundamentally challenged with a $7 can of compressed air and it's enough to give every security professional heart burn. We all had [...]*

Computer encryption technologies have all relied on one key assumption that RAM (Random Access Memory) is volatile and that all content is lost when power is lost. That key assumption is now being fundamentally challenged with a $7 can of compressed air and it's enough to give every security professional heart burn.

We all had some theoretical concerns, but surely it would be too difficult to transport hot memory from one computer to another to extract its contents right? That's what we all thought until a group of researchers from Princeton University showed that memory wasn't as volatile as we had all assumed (see Techmeme). As a matter of fact, memory would hold its contents for a duration of seconds or even minutes with the power cut off. If that wasn't long enough, a can of compressed air used upside down will cryogenically freeze memory and keep the data intact for several minutes to an hours. This means the ultrasensitive encryption keys used to protect data can be exposed in the clear.

- Rationale for Test Manufacturing RAM HW eraser requirements

- http://www.zdnet.com/blog/security/cryogenically-frozen-ram-bypasses-all-disk-encryption-methods/900

The Architecture for the Digital World®
ARM®

Who Do You Trust?

- Trust Nobody
  - Expensive
  - Supply change challenges
  - Can never eliminate all vulnerabilities
  - Vulnerable to usual set of spy novel plot lines
- Trust but Verify
  - Network of trusted suppliers (silicon, test, IP, tools, SW, etc.)
  - Work with other interested parties
  - Mechanism for compliance checking
  - Also vulnerable, but typically in ways that make boring books