RAPID AUTHENTICATION THROUGH VERIFICATION, VALIDATION, AND MARKING

Mr. Kerry Bernstein, DARPA/MTO Program Manager

NDIA Trusted Microelectronics Workshop

August 17, 2016

DISTRIBUTION A. Approved for public release: distribution unlimited.
The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need.

<table>
<thead>
<tr>
<th>Protection</th>
<th>Program</th>
<th>Loss of information</th>
<th>Fraudulent products</th>
<th>Loss of access</th>
<th>Malicious insertion</th>
<th>Quality and reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government-proprietary</td>
<td>Other</td>
<td>⬤</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TIC (IARPA)</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VAPR</td>
<td>⬤</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SPADE</td>
<td>⬤</td>
<td></td>
<td>⬤</td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DAHI</td>
<td>⬤</td>
<td></td>
<td>⬤</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHIPS</td>
<td></td>
<td></td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td></td>
<td>CRAFT</td>
<td></td>
<td>⬤</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>eFuses</td>
<td>⬤</td>
<td></td>
<td></td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td>SHIELD</td>
<td></td>
<td>⬤</td>
<td>⬤</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification and Validation</td>
<td>IRIS</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TRUST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>⬤</td>
</tr>
</tbody>
</table>

SHIELD, IRIS, and TRUST can help protect against the introduction of fraudulent products and ensure that genuine microelectronics perform only as expected.
Hardware-specific exploits, mitigations

**LEGEND:**
- **Design Attack**
- **Hardware Attack**
- **Logistics Attack**

- 3rd Party IP
- Insider Design
- EDA Exploit

**TRUST, IRIS**
- Malicious Insertions
- Pkg Compromise
- Process Compromise
- False Test Compares
- False FPGA Bitstream

**SHIELD**
- False Expects
- Process Compromise
- False FPG Bitstream
- False Test Compares
- False FPGA Bitstream

- VHDL
- RTL
- GDSII
- PROCESS
- Pkg
- PNP
- ID

**DISTRIBUTION**
- Approved for public release: distribution unlimited.
Counterfeits vs clones

Counterfeits

*Still the original part from OEM:*
- Recycled used components
- OEM’s fab test failures sold on black market
- Unlicensed fab overproduction

Clones

*A completely different part:*
- Copies fabbed in foreign plant
- New design of reverse-engineered components using stolen IP, potentially with altered function

All images courtesy of NSWC CRANE

DISTRIBUTION A. Approved for public release: distribution unlimited.
Counterfeiter skills for reverse engineering complex components are growing, and tracking Moore’s Law.

* Developed with B. Hamilton, NSWC Crane.
Integrated circuits must function as designed – no more, no less.

The TRUST program addressed these vulnerabilities in four thrusts:

1. Trust in fabrication for ASICs
2. Trust in design for ASICs
3. Trust in FPGAs
4. Trust in third-party intellectual property (IP)
Integrity and Reliability of Integrated circuitS (IRIS)
IC functionality extraction and reliability estimation

Objectives
• 100% functionality derivation given a limited data sheet and an IC, FPGA or 3rd party IP
• MTTF analysis of an IC given limited sample size
• Forensics to identify IC anomalies and determine impact on reliability

Capabilities developed
• Non-destructive imaging for feature resolution
• Algorithms for pattern recognition and netlist extraction
• Data analytics for functional derivation
• Advanced modeling and simulation techniques for reliability analysis

Virtual Laboratory
• Designed, developed and debugged test articles for performer analysis
• Evaluated performer techniques for scientific soundness, and results against program metrics

Performers
BAE Systems
SRI International
USC Information Sciences Institute
Raytheon
Luna (MacAulay Brown)
Orora
R3 Logic
Case Western Reserve Univ.
Georgia Tech
University of Michigan
Boeing
IBM
University of Arkansas

DISTRIBUTION A. Approved for public release: distribution unlimited.
3D reconstruction of DAC – Non-destructive

Video not included here

All images courtesy of SRI International

Enables 3D Visualization and Spatial Analysis

DISTRIBUTION A. Approved for public release: distribution unlimited.
Layer extraction on DAC

Video not included here

All images courtesy of SRI International

HIGH RESOLUTION IN DEPTH ENABLES LAYER SEPARATION AND MEASUREMENT OF
THICKNESS WITHOUT GRINDING
The global nature of today’s supply chains

Global nature of supply chain makes chain-of-custody unworkable

Lifecycle shown for a single Joint Strike Fighter component, which changes hands 15 times before final installation
For all but simplest exploits, DoD has little system component assurance of authenticity

*Assume parts have OEM integrity before leaving first Trusted Zone
SHIELD: DARPA’s supply chain solution

DARPA SHIELD will develop the ability to provide nearly 100% assurance against certain known threat modes quickly, on demand, at any step of the supply chain, at extremely low cost.

SHIELD makes counterfeiting too expensive and too hard to do.

Image courtesy of Hitachi:
http://www.hitachi.com/New/cnews/030902.html

SHIELD Target Spec
- 100µm x 100µm (0.01 mm² Area)
- 100K Devices
- 100 MHz Clock Rate
- 50 µW Total Power
- T ≤ 120°C
- <1¢ per dielet

Hardware Root-of-Trust
Fragile Key Storage

Full Encryption Engine

Unpowered
Passive Sensors

Inductive Powering and Communication

Microscopic
SHIELD dielet
Example SHIELD CONOP

1. Serial ID Upload
   - Database with Dielet Serial ID
   - Fab Name, Fab Date, Part Number

2. Challenge Download
   - Random Challenge Generator
   - Decryption Engine w/Crypto key; decrypt; compare to original challenge

3. Encrypted Sensors
   - Sensor Status
   - Auditor Identity

4. Authentication Out
   - Test Date
   - Key Requests

TCPIP Address (VPN)

Dielet

Serial ID No.

Encryption Engine w/ Crypto Key

Temp Extremes

X-Ray Exposure

Light Exposure

Smartphone

Server

DISTRIBUTION A. Approved for public release: distribution unlimited.
Revisiting the supply chain – now with SHIELD implementation

Component compromises are now visible at any point along the supply chain

* Assume parts have OEM integrity before leaving first Trusted Zone

Image Sources:
1. defense.gov
2. Clovis Pack and Ship
3. pcbisino.org
4. brighthub.com
5. Wikimedia commons
6. texasmicro.com
7. digilent.com
What makes SHIELD “DARPA-worthy?”

At 100µm by 100µm by 10µm thick, the SHIELD dielet is on track to be the smallest integrated circuit ever developed

- Whole new technologies for building the “science of SMALL”
- Remote chip communication and powering using microscopic antennae
- Design of passive sensors that cannot be reset or inadvertently triggered

SHIELD dielet surrogate (SRI International)  
Microscopic Sort and Pick (SRI International)
Example technology - Draper fragility

Goal: design and develop a high-yield, low cost architecture for the fabrication, testing, and packaging of ultra-thin (<10µm) dielets with engineered fragility

A. Dielet (100um x 100um x 10um)
B. Silicon frame
C. Silicon tether (electrical and mechanical support)

Released dielets anchored to a silicon frame

Carrier wafer with etched cavities under individual dielets

Top View (1,500x)
Perspective View (10,000x)

G. Perlin, et al.
Images courtesy of Draper Laboratories

DISTRIBUTION A. Approved for public release: distribution unlimited.
Fab-of-Origin (ClearMark, Chromologic, IC Forensics)

- Fab-of-Origin looks for fab-signatures to identify origin of a component
- Idiosyncrasies associated with fab-specific tooling, recipe, sequence
- Needed to trace DoD, non-DoD clones and counterfeits to originating foundry (Smart Grid, Cyber Systems, Communications, etc...)

**MTO SBIR SB133-03: Fab of Origin**

Once SHIELD determines a chip to be a counterfeited, Fab-of-Origin will provide the insight needed to identify where it was made.
Thinking “outside the box”
Determining Fab-of-Origin

Two parts, marked by the same laser tool

Two parts, marked by different laser tools in the same facility

Images compliments of Clearmark, Inc.
What characterizes the circuit layout of an ASIC?

Medium is (M1) metallization patterns in SEM image tiles

Basis patterns are unknown cell designs from the standard library for the foundry

The layout information is contained in the line drawing of the patterns