RAPID AUTHENTICATION THROUGH VERIFICATION AND VALIDATION

Mr. Kerry Bernstein, DARPA/MTO Program Manager
The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need. SHIELD, IRIS, and TRUST can help protect against the introduction of fraudulent products and ensure that genuine microelectronics perform only as expected.

<table>
<thead>
<tr>
<th>Protection</th>
<th>Program</th>
<th>Microelectronics Security Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foundry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partnerships</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fine Disaggregation</td>
<td><strong>TIC</strong> (DARPA): Disaggregate ASICs into non-functional parts</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td><strong>VAPR</strong>: Shatter lost, misplaced, or end-of-life ASICs on command</td>
<td>•</td>
</tr>
<tr>
<td>Blended Partnerships</td>
<td><strong>SPADE</strong>: Use secure parts to monitor commercial components packaged together into a single ASIC</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DAHI</strong>: Disaggregate ASICs into functional subcomponents</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td><strong>CHIPS</strong>: Establish a library of pre-verified, modular ASIC design IP</td>
<td>•</td>
</tr>
<tr>
<td>Commercial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obscuration and Marking</td>
<td><strong>CRAFT</strong>: Apply modularity to reduce ASIC design effort and allow portability across foundries</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td><strong>eFuses</strong>: Obscure ASIC functionality until after manufacture</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td><strong>SHIELD</strong>: Authenticate ASICs at any point in the supply chain</td>
<td></td>
</tr>
<tr>
<td>Verification and Validation</td>
<td><strong>IRIS</strong>: Derive an ASICs functionality and reliability</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td><strong>TRUST</strong>: Reverse engineer ASICs and compare to design</td>
<td></td>
</tr>
</tbody>
</table>

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

Exemplary high-level clone discoveries collected over past 3 years*

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

ASIC (Application-Specific Integrated Circuit) vulnerabilities

Top level specifications and design data

Foreign Semiconductor Fab

Unknown ASIC

Image: tufts.edu
Image: extremetech.com
Image: directindustry.com

FPGA (Field Programmable Gate Array) vulnerabilities

Black Box
Binary Firmware
10010010110101001
00110100101010101
11001011010100101

Known FPGA

Image: xilinx.com

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

ENAVLES 3D VISUALIZATION AND SPATIAL ANALYSIS

Video not included here

All images courtesy of SRI International

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

All images courtesy of SRI International

HIGH RESOLUTION IN DEPTH ENABLES LAYER SEPARATION AND MEASUREMENT OF THICKNESS WITHOUT GRINDING