Supply Chain Hardware Integrity for Electronics Defense (SHIELD)

Serge Leef
Program Manager, Microsystems Technology Office
Defense Advanced Research Projects Agency

Software and Supply Chain Assurance Winter Forum 2018

18 December 2018
Threats to Integrated Circuit Integrity
Threats to integrated circuit integrity

DARPA mitigation technologies

**TRUST**
- 3rd Party IP
- Insider Design
- EDA Exploit
- False Expects

**IRIS**
- Malicious Insertions
- Process Compromise
- Package Compromise
- False Test Compares

**SHEILD**
- False FPGA bit stream

---

**Design** | **Verify** | **Mask Build** | **Chip Build** | **Package** | **Test** | **Pers.** | **Dist.** | **Use**

**IP Theft/Copy**
- Security Intercept
- False Validation Report

**DFM Exploits**
- Yield Fail Diversion
- Overproduction
- Process Compromise

**HW Theft**
- Yield Fail Diversion

**IP Theft/Copy**
“Defense acquisition revolves around 15-year programs, 5-year plans, 3-year management, 2-year Congresses, 18-month technologies, 1-year budgets, and thousands of pages of regulations.”
Report to SecDef FY12-02
The Global Nature of Today’s Supply Chains makes chain-of-custody unworkable.

Lifecycle for a single Joint Strike Fighter component, which changes hands 15 times before final installation.
US Electronic Waste is a Contributing Factor

- Received in Developing Country
- Removed from boards and sorted
- Shipping from/to U.S.
- Refurbished and remarked
- Resold
- Repackaged

All images courtesy of SMT Corporation
Uncontrolled heating during part removal can cause die cracks or delamination, leading to immediate or latent failures.

Mishandling or sanding of parts can cause latent Electrostatic Discharge (ESD) failures.
Counterfeits vs Clones

A counterfeit part is manufactured by the OEM and presented as new, but the performance and reliability of the part is questionable:
- Used components recycled/remarked
- OEM test failures
- Unlicensed fab overproduction

A cloned part is not manufactured by the OEM but may be designed to mimic the performance of the authentic part:
- Copies manufactured 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 Unlimited Distribution
Counterfeits, Clones, Trojans
Things are Not Always as They Appear!

This part looks pretty good, right????

Blacktopped – After Dynasolve Soak

Re-Plated Leads

Different Lead Frames in Same Lot

Source: Images NSWC Crane

Distribution A, Approved for Unlimited Distribution
Physical and Optical Inspection is Time Consuming, Labor Intensive, Thus Expensive!

Trimmed (wedge) vs. Untrimmed (flat) Leads

One Part has Trimmed Leads (Shorter than Legitimate Part)

Scratched Window from Sanding and Corroded Metal

Source: Images NSWC Crane

Distribution A, Approved for Unlimited Distribution
Poor Quality Integrated Circuits

Low quality manufacturing process

Example of Poor Quality

Good Part

Source: Images NSWC Crane

Distribution A, Approved for Unlimited Distribution
Stealthy Dopant-Level Hardware Trojans\textsuperscript{1}

Abstract. “…..In this paper we propose an extremely stealthy approach for implementing hardware Trojans below the gate level, and we evaluate their impact on the security of the target device. Instead of adding additional circuitry to the target design, we insert our hardware Trojans by changing the dopant polarity of existing transistors. Since the modified circuit appears legitimate on all wiring layers (including all metal and polysilicon), our family of Trojans is resistant to most detection techniques, including fine-grain optical inspection and checking against “golden chips“...........”

\textsuperscript{1}Source: Georg T. Becker\textsuperscript{1}, Francesco Regazzoni\textsuperscript{2}, Christof Paar\textsuperscript{1,3}, and Wayne P. Burleson\textsuperscript{1}
\textsuperscript{1}University of Massachusetts Amherst, USA
\textsuperscript{2}TU Delft, The Netherlands and ALaRI - University of Lugano, Switzerland
\textsuperscript{3}Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum, Germany

Fig. 2. Layout of the Trojan DFFRX1 gate. The gate is only modified in the highlighted area by changing the dopant mask. The resulting Trojan gate has an output of $Q = V_{DD}$ and $QN = GND$. 
SHIELD Overview
A Hardware Root of Trust for Integrated Circuits

Apply RFID chip concept...

Common Access Card
- PIN (known only to card holder)
- ID Certificates

...to integrated circuit integrity

SHIELD Dielet
- Onboard encryption engine with secret key
- Serial ID
SHIELD – The DARPA Supply Chain Solution

Key SHIELD Specifications
- Unique Key Storage
- Full 256-bit AES encryption engine
- Unpowered, passive intrusion sensors
- RF power and communication
- Transfer fragility
- 100µm x 100µm
- 50 µW Total Power
- Operating temp < 120°C
- Cost < $0.01 per dielet

Asymmetric Security
- Non-resettable, “always on” intrusion sensors on dielet
- On-board encryption symmetric key that cannot be “coaxed” from dielet
- ID and Key are unique to the individual host IC (not just the part number)
- Interrogation history (date, time, location) stored on secure server
- Built-in fragility structures kill dielet if removal from host is attempted

SHIELD makes counterfeiting too expensive and too hard to do.
### SHIELD Key Components

<table>
<thead>
<tr>
<th>Dielet</th>
<th>Reader</th>
<th>Remote Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Dielet Chip Image" /></td>
<td><img src="image2.png" alt="Reader Image" /></td>
<td><img src="image3.png" alt="Remote Server Image" /></td>
</tr>
<tr>
<td>Programmed on-reticle after manufacture</td>
<td>Transmits at 5.8GHz to power dielet; 3.6GHz for data transfer</td>
<td>Communicates with reader via Internet connection; performers using Amazon and Microsoft web services</td>
</tr>
</tbody>
</table>
| Installed on or within host IC package  
  - Embedded within package  
  - Custom package  
  - Epoxy to surface | USB connection to smartphone, tablet or computer | Maintains a record for each IC  
  - Manufacture date  
  - Part/package information  
  - Interrogation history | No impact to host IC performance or reliability | Can be configured for high-volume interrogation (transaction time < 1 sec) |
1. Interrogate dielet on host IC
2. Unique ID returned by host IC; reader sends ID to server

FAIL if no response from host IC
3. Server sends unencrypted challenge to reader; reader forwards challenge to host IC

FAIL on discrepancy between server record and user visual ID
(example: user is testing microcontroller, but server reports ID belongs to an FPGA)
4. Host IC sends encrypted response and sensor status; reader forwards to server

PASS if challenge/response match
FAIL if challenge/response do not match
A complete SHIELD authentication transaction, including internet latency, takes only 1-2 seconds.
SHIELD Program Structure and Performers
• Program start: January 2015
• Performers:
  • Northrop Grumman (full SHIELD design)
  • SRI International (full SHIELD design)
  • Draper (sensors, fragility)
  • University of California, Berkeley (dielet power/communication, fragility)
  • University of Illinois/Carnegie Mellon University (dielet power/communication)
• Four year program in three phases
  • Phase 1: Technology Development (1.5 years)
  • Phase 2: Hardware Design (1.5 years)
  • Phase 3: Demonstrate the CONOP (1 year)
A Root-of-Trust Prohibitively Difficult to Exploit With Key Protection, Attack Resistant AES, and Smallest OTP

Advancing a Proven AT Tech Base Assessed to Defeat Advanced Threats

- **Physically Unclonable Function (PUF)** – Random process variation used to create dielet-derived portion of encryption key.

- **Tamper Detection Sensor** – Sensor detects potential counterfeiting by capturing temperature excursions.

- **14nm Gate-Oxide Rupture One-Time Programmable (OTP) Memory** – Small and difficult to exploit. OTP contains 64-bit SN and 256-bit key split.

- **Innovative Encapsulation** – Lamination process facilitates compatibility with existing surface mount infrastructure.

- **Attack Resistant Cryptography** - AES engine and jointly randomized split keys creates a strong Root-of-Trust.

- **Innovative Power Harvesting** - Carefully modeled resonant inductive coil and rectification provide power to dielet.
SHIELD Dielet Block Diagram

100 μm x 100 μm, 10-μm thick ICEPAC dielet

Passive sensor

Mixed-signal sensor circuitry

Sensor interface

Intrusion sensor

Extensible to other sensors

Control logic

64-bit ID

AES encryption engine

Unclonable Sensor Code (USC)

Secure OTP key memory

Secure unpowered key storage

Digital logic

Ultra-miniaturized RF interrogation system

Analog RF section

Power generation (rectifier/voltage regulator)

RF modulator/demodulator

RF appliance

On-chip antenna

Baseband signal

Nonce

50 MHz ring oscillator

Clock

Data Channel

Power Channel

10-μm thick die

Distribution A, Approved for Unlimited Distribution
Draper Fragility Summary

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)

Key Features

- CMOS compatible architecture with high-yield backend processing
- Higher die count (lower cost) compared to dicing processes
- Strategically placed microstructures to aid in fragmentation

G. Perlin, et al.