THE ELECTRONICS RESURGENCE INITIATIVE

SHIELD SUPPLY CHAIN ASSURANCE TECHNOLOGY

KERRY BERNSTEIN, PROGRAM MANAGER, DARPA MTO
MICHAEL KANE, PRINCIPAL INVESTIGATOR, SRI INTERNATIONAL
CHRISTOPHER LANTMAN, SRI INTERNATIONAL
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
THREATS TO INTEGRATED CIRCUIT INTEGRITY

DARPA mitigation technologies

<table>
<thead>
<tr>
<th>TRUST</th>
<th>IRIS</th>
<th>SHIELD</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd Party IP</td>
<td>Malicious Insertions</td>
<td>False Test Compares</td>
</tr>
<tr>
<td>Insider Design</td>
<td>Process Compromise</td>
<td>Package Compromise</td>
</tr>
<tr>
<td>EDA Exploit</td>
<td>False FPGA bit stream</td>
<td></td>
</tr>
</tbody>
</table>

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

IP Theft/Copy | False Validation Report | DFM Exploits | Yield Fail Diversion | Overproduction | Process Compromise | HW Theft | Yield Fail Diversion | IP Theft/Copy

Security Intercept |
"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
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
This work was funded by the Defense Advanced Research Projects Agency (DARPA) Microsystems Technology Office (MTO) under Contract No. HR0011-15-C-0010. The views, opinions and/or findings expressed are those of the authors and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government. Approved for Public Release, Distribution Unlimited.
Electronic systems that are relied upon for national security depend on the performance and reliability of highly sophisticated electronic components. However, counterfeit electronics entering the DoD supply chain place our military personnel and our country at risk.

Under DARPA’s SHIELD Program, SRI International has developed a novel end-to-end solution to secure the electronic component supply chain by using a low-cost identification chip embedded in microelectronic circuit packaging.
The SHIELD ID chip is called a “dielet” because it is only 100 µm square, smaller than a grain of fine sand. It can be authenticated wirelessly via an RF reader communicating securely over the internet with a remote SHIELD Verification Server.

The SHIELD dielet provides a hardware root-of-trust, guaranteeing the authenticity of the host IC by making counterfeiting very difficult and prohibitively expensive.
The dielet has a full Advanced Encryption Standard (AES) encryption engine with a unique 256-bit secret key programmed into nonvolatile memory at wafer probe and also enrolled with the server, enabling secure dielet authentication through a challenge-response protocol. It is fabricated in the TSMC 28 nm HPC CMOS process.
Because it is only 100 µm square and 30 µm thick, a SHIELD dielet is easily embedded in a host IC package.

Dielet being placed into well in QFP package

SHIELD-enabled Xilinx FPGA in Kyocera 228-lead QFP package
The SHIELD reader communicates wirelessly with the dielet. It is controlled by an Android handheld device such as a tablet or smartphone, which communicates over the internet via a secure VPN connection with the secure SHIELD server.

The SHIELD server is hosted on Amazon Web Services (AWS), where the dielet keys are stored securely using the AWS Key Management Service.
A complete SHIELD authentication transaction, including internet latency, takes only 1-2 seconds.
MARKET ANALYSIS FOR ANTI-COUNTERFEITING SOLUTION
THE COST OF COUNTERFEITING IS ESTIMATED TO APPROACH A HALF TRILLION DOLLARS

Sources: Havoscope (http://www.havoscope.com/counterfeit-goods-ranking/). Data used as a reference by the industry and multiple sources such as PwC, EY; NetNames, Counting the cost of counterfeiting, 2015; Frontier Economy - The Economic Impacts Of Counterfeiting And Piracy
US semiconductor manufacturers are losing $7.5Bn in annual revenue to counterfeiting.

Percent of reported incidents:
- Analog IC: 25%
- Microprocessor IC: 13%
- Memory IC: 13%
- Programmable Logic IC: 13%
- Transistor: 8%
- Other: 8%

Sources: Anti-Counterfeiting of Integrated Circuits: RFID Tags as a Countermeasure, Sathya Kanth Vardhanapu, 2012; IHS Part Management, 2012; Counterfeited components, IHS, 2014
BRAND OWNERS ARE CONFRONTED BY FIVE COUNTERFEITER GROUPS

Many prominent terrorist organizations rely on illicit trade for financing up to 20% of terrorist attacks, an example of which is the 2015 Charlie Hebdo attack in Paris.

Sources: Business strategies in the counterfeit market, Journal of business research, 2011; Counterfeiting, piracy and smuggling: Growing threat to national security, EY, 2014
GRAY MARKET ACTIVITIES ARE A CHALLENGE

“Criminals remove microchips from old devices, recycle them and resell them to illegal device manufacturers. It is significant problem in Asia.”

(Senior Director Strategic Development, Qualcomm)
END-TO-END ANTI-COUNTERFEITING SOLUTIONS CAN ALSO GATHER SUPPLY CHAIN INFO

**Spectrum of security services**

**Integrated System**
- Sell anti-counterfeiting tag with unique signatures, readers and encrypted data backbone.

**Maintenance & Support**
- Remotely control reader, pick and place equipment, provide associated services (e.g., maintenance and repair).

**Data Management**
- Inactivate recalled products and clear associated data sets.

**Brand protection**
- Monitor product and data streams along the supply chain.
- Assist originators in prosecution of counterfeiting activities.

Source: Webinar TAKING A FRESH LOOK AT COUNTERFEITING IN PHARMA & MEDICAL DEVICES: FROM ROOT CAUSES TO CURRENT SOLUTIONS, SICPA CLARIANT, 2017; Fighting counterfeit pharmaceuticals, PwC, 2017
SUPPLY MODEL OF SHI ELD

SHI ELD facility

Step ① Dielet Production
Step ③ Dielet installation on product
Step ④ Product with dielet

IC manufacturer

Step ② Customer ships IC

Packaged IC BEFORE Shield

Product protected WITH SHIELD is shipped to designated distributor/OEM
SRI CONVERTS GOVERNMENT INVESTMENT TO SOCIETAL IMPACT

We look forward to partnering with you to bring SHIELD to the electronics industry.
CONTRACTS AND TRUST

https://evollution.com/opinions/personalized-service-key-to-winning-training-contracts/
IDENTIFY AND ADDRESS IMPORTANT FEATURES FOR A CROSS-INDUSTRY OPEN STANDARD FOR DISTRIBUTED LEDGERS

THE HYPERLEDGER PROJECT

- Permissioned system: strong identity management
- Distinct roles of users and validators
- Users deploy new pieces of code (chaincodes) and invoke them through deploy & invoke transactions
- Validators evaluate the effect of a transaction and reach consensus over the new version of the ledger
- Ledger = total order of transactions + hash (global state)
- Pluggable consensus protocol, currently PBFT & Sieve

THE BLOCKCHAIN-PROTECTED SUPPLY CHAIN

Potential Smart Contract Triggers at each stage

- Parts Mfg.
  - Component Data
  - Manufacture Logs
  - Manufacture Certs

- Design
  - Design Specs
  - Design Certifications

- Integrated Assemblies
  - Assembly Details
  - Inspection Results

- Blockchain Network
  - Create Asset
  - Notifications/Queries
  - Update status

- Delivery/Inspection
  - Notifications/Queries
  - Update Installation data
  - Delivery/Transfer Logs
  - Export Compliance QAI

- Operation
  - Operational Usage data

- Installation/Archival
  - Notifications/Queries
  - Update attributes
  - Regulatory Compliance
  - Installation Logs
  - Disposal Logs
  - Counterfeit Detection/Reporting

Image compliments of IBM Research
Chain of Trust in Blockchain/Hardware-Backed Supply Chains

**Interaction/ Reporting Layer**
Visualization to track components and assemblies through various stages and time frames of a supply chain. Roles for various network participants.

**Blockchain Layer**
Immutable and certified recording of events observed on components at various stages of the supply chain in to the Blockchain Ledger.

**Bridge Layer**
Software Bridge on scanners to read data from components/assemblies with SHIELD hardware.

**Hardware Layer**
Authentication, encryption, identity, data recording and reporting when sensed.

End to End multi-party chain-of trust
Protocols based on
- public/private keys
- encryption, signing
- HW identity

Source: IBM Research
HI ERARCHICAL, AUDITABLE SHIELD/BLOCKCHAIN INTEGRITY

- Supply Chain and System
- Board and Subassembly
- Module/Package
- Chip Fabrication
- Mask Build
- IP Watermark

Distribution A, Approved for Unlimited Distribution
SHIELD-BASED MANUFACTURING CHAIN-OF-ASSURANCE

Watermark the base design
- SHIELD-supported Blockchain of on-chip AVP/RTPG ScanRing Outputs and LBIST/ABIST
- IBM Hyperledger / Smart Contracts

Include as IP in the chip
- To maintain chip provenance through the supply chain
- Make use of open space on chip to instantiate dielet IP
- May be used as a watermark throughout the design
- Example shown: discrete placement on unused I/O pad

Attach SHIELD to wafer
- SHIELD dielet is physically affixed to wafer blanks at supplier
- Track wafer authenticity through process gates in-line
- Interrogated at process gate transfer

Install in the wafer’s dicing streets (kerf)
- To maintain design integrity during manufacturing
- Dielet instantiated into kerf GDSII layout and diced out at singulation

Install within the chip reticle
- To maintain integrity of the chip design during manufacturing
- Dielet physically attached to reticle frame or glass and interrogated at transfer points
- Dielet instantiated as a site in the reticle

Install within- or upon-chip packaging
- To provide component supply chain provenance
- Custom package with recess for dielet, OR affixed to surface of chip with epoxy

SHIELD IP can ensure trusted components from an untrusted fab

Distribution A, Approved for Unlimited Distribution