Hardware Security and Assurance: The Power of Reverse Engineering

Domenic Forte
Associate Professor and Steven A. Yatauro Faculty Fellow
Electrical & Computer Engineering Dept. University of Florida
Globalization of IC/PCB Supply Chain

2015 Worldwide Fab Capacity by Region

Source: SEMI.org
Motivation – Hardware Trojan Insertion in ICs

Insertion @ Untrusted Foundry: Exploit space in layout for smallest footprint
- Replace filler cells (decoupling, ECO, etc.)

Trigger: Rare precondition
Payload: Leak information or disable/derange IC
Motivation – State-level Tampering of Electronics

(1) Interdiction

E.g.) NSA’s Tailored Access Operations (TAO) Unit
- Intercepted and tampered with Cisco products
- Installation of secret firmware to monitor communications and siphon data

Source: No Place To Hide, 2014

(2) The Big Hack

E.g.) Supermicro Server Motherboards
- Chinese spies implanted chip at subcontractor facility
- Told the servers to communicate anonymous computers on the internet that were loaded with more complex code
- Preparing the server’s operating system to accept new firmware

Source: Bloomberg Businessweek, 2018
Motivation – Counterfeit Electronics

75 Billion Connected Devices by 2025!

Top Part Types Reported in Counterfeit Instances

Source: IHS, 2016

Reported Counterfeits vs. Global Semiconductor Sales

Source: ERAI, 2018

Pandemic-induced Chip Shortage

Source: https://creativeelectron.com/
Trust but Verify: Reverse Engineering (RE) for HW Assurance

Identification of exploits
Development of attacks
HW/SW Trojans and malware
Intellectual property (IP) theft
Cloning and counterfeiting

Failure analysis
Assurance of integrity
Proof of IP infringement
Assurance of authenticity
Obsolescence mitigation
**MythBusters: The Case for Reverse Engineering (RE)**

### Cons (Myths?) of RE

- **Destructive to samples (?)**
  - X-ray CT is nondestructive for PCBs
  - Non-invasive and semi-invasive attack methods can be used to extract FW, SW, etc.
  - Synchrotron and X-ray ptychography promising for IC RE
- **Expensive and time consuming (?)**
  - Improvements to instrumentation (e.g., Multi-Beam SEMs by Zeiss)
  - Full blown RE not always needed
- **Manual (?)**
  - Rise of commercial and academic RE tools (e.g., Pix2net, ChipJuice, HAL)
  - Automated delayering & imaging solutions
  - Advances in AI and deep learning

### Pros of RE

- The **only** method available to establish *ground truth* for non-invasive techniques
- RE can be used to *recreate or upgrade legacy* electronics
- Decision making is less impacted by *process variations*
  - Detect both *small differences and gross differences* in layout, technology node, etc.
- Expensive and time consuming (?)
- Improvements to instrumentation (e.g., Multi-Beam SEMs by Zeiss)
- Full blown RE not always needed
- Manual (?)
  - Rise of commercial and academic RE tools (e.g., Pix2net, ChipJuice, HAL)
  - Automated delayering & imaging solutions
  - Advances in AI and deep learning
Advances in PCB Reverse Engineering
Destructive PCB RE

- Solder Mask Removal
  - Sandpaper
  - Chemical
  - Laser
  - Fiberglass Brush
  - Abrasive Blasting

- Delayering
  - Sandpaper
  - Dremel Tool
  - CNC Milling

- Imaging & Netlist Extraction

4-layer PCB

J. Grand, WOOT 2014.
S. Kleber, WOOT 2017.
Nondestructive PCB RE via X-ray CT

Asadi et al., IEEE Trans. CPMT 2017
(2) Pre-processing – Automated Layer Alignment

Re-alignment

= Leveled Axis

X-Plane Board Slice

Y-Plane Board Slice

Z-Plane Board Slice

= Board Area Missing Information
Automated Alignment Solution and Results

Iterative realignment through robust linear regression

Before Alignment

X - Plane  Y - Plane

Spartan-6

Z - Plane

X - Plane  Y - Plane

Z - Plane

RASC

After Alignment

X - Plane  Y - Plane

Spartan-6

Z - Plane

X - Plane  Y - Plane

Z - Plane

RASC

= Regression Based Centroid of PCB

Botero et al., GOMACTech, 2020
**Task:** Automatically assign X-ray CT ‘slices’ to PCB layers

- **Vias** are vertical interconnects between adjacent layers
  - Through-hole types are consistent in all layers
  - Blind and buried are consistent in a subset of layers
- **Traces** are horizontal interconnects between nets within a single layer
  - Traces are usually unique to each layer

Automatic PCB Layer Identification Results

RASC Ground Truth

1

2

3

4

5

6

Clustering Results

1

2

3

4

5

6

Cluster Analysis

<table>
<thead>
<tr>
<th>Layer</th>
<th>SIR</th>
<th>SSIM</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.96</td>
<td>0.91</td>
<td>0.987</td>
</tr>
<tr>
<td>2</td>
<td>0.91</td>
<td>0.99</td>
<td>0.999</td>
</tr>
<tr>
<td>3</td>
<td>0.91</td>
<td>0.99</td>
<td>0.998</td>
</tr>
<tr>
<td>4</td>
<td>0.93</td>
<td>0.99</td>
<td>0.997</td>
</tr>
<tr>
<td>5</td>
<td>0.98</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>6</td>
<td>1.00</td>
<td>0.97</td>
<td>0.993</td>
</tr>
</tbody>
</table>

Botero et al. GOMACTech 2020.
Automated Via Detection Methodology

High Level Features of Methodology

- Fully automated
- Only needs a circular template and number of via classes as input (*Optional*: Range of via size per class)
- Applies domain knowledge / design rules to remove false positive vias
- Iteratively improves templates to remove false positive vias

Botero et al., ISTFA 2020.
Automated Via Detection Methodology

Candidate Via Detection

Tiered Hough Circle Detection
- Raw
- Filtered

Intensity Concentration Check

Radial Template Matching

Mean-Shift Clustering

Overlap Removal

Adjacency Check

Concentricity Check

Iterative False Positive Removal

Known Radii

Reduction in false positives by using prior information

Botero et al. ISTFA 2020.
Automated Via Detection Methodology

Candidate Via Detection

- Frequency Domain Filtering
- Tiered Hough Circle Detection
  - Raw
  - Filtered
  - Large
  - Medium
  - Small

Iterative False Positive Removal

- Intensity Concentration Check
- Radial Template Matching
- Mean-Shift Clustering
- Overlap Removal
- Adjacency Check
- Iteration: Update Ideal Template, Update ThW, ThS, Update ThInt

Concentricity Check

Candidate Vias

Pixel intensity in circle? Radial template match?

1. No
2. Yes
3. Yes

Botero et al., ISTFA 2020.
Automated Via Detection Methodology

Candidate Via Detection
- Frequency Domain Filtering
- Tiered Hough Circle Detection
- Radial Template Matching

Iterative False Positive Removal
- Intensity Concentration Check
- Radial Template Matching
- Mean-Shift Clustering
- Overlap Removal
- Adjacency Check

Concentricity Check

Candidate Vias

Pixel intensity in circle?
Radial template match?

<table>
<thead>
<tr>
<th>Iteration</th>
<th>Gradient-based Radial Template</th>
<th>False/True PDFs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>![Template Image]</td>
<td>![PDF Image]</td>
</tr>
<tr>
<td>5</td>
<td>![Template Image]</td>
<td>![PDF Image]</td>
</tr>
</tbody>
</table>
Automated Via Detection Methodology

Candidate Via Detection
- Frequency Domain Filtering
- Tiered Hough Circle Detection
  - Raw
  - Filtered
- Slice-to-Layer Correspondence
- Raw PCB Stack
- Filtered PCB Stack

Iterative False Positive Removal
- Intensity Concentration Check
- Radial Template Matching
- Mean-Shift Clustering
- Overlap Removal
- Adjacency Check

Concentricity Check
- Previous Layer
- Next Layer

Iteration:
- Update Ideal Template
- Update Thw/Ths
- Update ThInt

Merge candidate circles corresponding to same via with Mean-Shift Clustering

Botero et al. ISTFA 2020.
Automated Via Detection Methodology

Remove candidates violating design rules

Use information from adjacent layers

Layer n-1

Layer n

Layer n+1

Botero et al. ISTFA 2020.
Automated Via Detection Methodology

Candidate Via Detection

- Frequency Domain Filtering
- Tiered Hough Circle Detection
  - Raw
  - Filtered
- Candidate Vias
  - Large
  - Medium
  - Small
- Slice-to-Layer Correspondence
- Layer
  - Raw PCB Stack
- Filtered PCB Stack

Iterative False Positive Removal

- Intensity Concentration Check
- Radial Template Matching
- Mean-Shift Clustering
- Overlap Removal
- Adjacency Check
- Concentricity Check

- Iteration: Update Ideal Template
- Update TH, Ths
- Update THInt
- Previous Layer
- Next Layer

Remove circles containing circles

Botero et al. ISTFA 2020.
Automated Via Detection Results

Xilinx Spartan 3 Layer 1 (S-1)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Known IoU</th>
<th>Unknown IoU</th>
<th>Known Dice</th>
<th>Unknown Dice</th>
<th>Known SSIM</th>
<th>Unknown SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-3</td>
<td>0.880</td>
<td>0.850</td>
<td>0.933</td>
<td>0.912</td>
<td>0.972</td>
<td>0.970</td>
</tr>
<tr>
<td>R-5</td>
<td>0.862</td>
<td>0.825</td>
<td>0.921</td>
<td>0.896</td>
<td>0.973</td>
<td>0.967</td>
</tr>
<tr>
<td>S-1</td>
<td>0.736</td>
<td>0.705</td>
<td>0.826</td>
<td>0.799</td>
<td>0.949</td>
<td>0.940</td>
</tr>
</tbody>
</table>
Automated Trace Detection Using Graph Cycle Deconstruction

Pre-Processing

Parallel Blocks
Adaptive Otsu Thresholding

2 Pass
Connected Components
Advances in IC Reverse Engineering
SEM Image Acquisition, Processing, and Analysis

Deprocessing + Imaging

Raw SEM image

Denoising

Segmentation

Vectorization

Annotation + Netlist Extraction

NAND

Buffer

AOI22

Source: FICS Research
IC Reverse Engineering Flows

Conventional Frontside RE Flow

De-package IC

Clean & Prep (planarize)

Remove Next Layer

Image Layer with SEM

Extract IC Netlist

Automated Plasma FIB Backside RE Flow

Backside 5 Axis Milling

Remove Next Layer

Image Layer with SEM

Extract Circuit Function

Principe et al., ISTFA 2017
Automated IC RE Demonstration

Principe et al., ISTFA 2017
AutoMAG

Tune Magnification Based on Feature Density → Decrease Imaging Time

• Persistence projections use run-length of sequences in the binarized image to obtain an approximation of the density information at any point in the image
• Low persistence indicates high information density

<table>
<thead>
<tr>
<th>Name</th>
<th>High Density Region</th>
<th>Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample 1</td>
<td>60 %</td>
<td>38.34 %</td>
</tr>
<tr>
<td>Sample 2</td>
<td>33 %</td>
<td>64.26 %</td>
</tr>
</tbody>
</table>

Wilson et al., M&M 2019
Sources of Error

Imaging Related
- Imaging Noise
  - Beam Interaction
  - Radiation Damage
  - Die Warpage
- Deprocessing Errors
  - Residue
  - Uneven Delayering
- Alignment Errors
  - Stitching
  - Vertical Alignment

Material Specific
- Layout Specific
  - Feature Dimensions
  - Feature Proximity
- Material Interactions
  - Flicker Noise
  - Oxidation
  - Electron Migration
  - Process Variations

Human Factors
- Operator Interactions
  - Incorrect Information

Random
- Modellable
- Random
LASRE: Large area Accelerated Segmentation for RE

Raw SEM Pixel Intensity Histogram

Texture Segmentation by LASRE

Wilson et al., ISTFA 2020
SEM Analysis for Annotation and Netlist Extraction

Deprocessing + Imaging → Raw SEM image → Denoising → Segmentation → Vectorization → Annotation + Netlist Extraction

Source: FICS Research
Standard Cell Recognition \textit{w/out} Prior Information

**Unsupervised Cell Extraction Results**

<table>
<thead>
<tr>
<th>Node Technology</th>
<th>32nm</th>
<th>90nm</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Unique Cells</td>
<td>64</td>
<td>87</td>
</tr>
<tr>
<td>True Match</td>
<td>60 (94%)</td>
<td>27 (31%)</td>
</tr>
<tr>
<td>Partial Match</td>
<td>0 (0%)</td>
<td>33 (38%)</td>
</tr>
<tr>
<td>Failed Match</td>
<td>4 (6%)</td>
<td>27 (31%)</td>
</tr>
</tbody>
</table>

**Correlation of n-grams of cell contact layer**

- **1-gram**
- **2-gram**

**Feature Encoding**

- **Cell boundary rules**
  - **Start-end rule**
  - **Inter-contact distance rule**

**Claim:** Cell X = Cell Y = Cell Z \[ \text{if} \ d_1 = d_2 \neq d_3 \rightarrow \text{Cell X = Cell Y} \neq \text{Cell Z} \]
Advances in FW Reverse Engineering
Side Channel-based Instruction Disassembly

OP Rd, Rr

Power traces

(a) ADD and SUB

(b) R19 and R20

(c) Data 10 and Data 20
Disassembler

- RISC architecture
- Single cycle execution
- 2-stage pipeline
- 32 working registers
Hierarchical Classification Method

1) Identify group of the instruction
2) Recognize the OP code of the instruction in the group
3) Recognize the other parts of the instruction such as the registers or immediate values

ADD R1, R2 : R1 = 20, R2 = 33
Profiling / Training

- For profiling each class, previous and following instructions are randomly selected and the address of registers and operands are also randomly selected.
- PCA is used for dimensionality reduction.
- 2500 power traces are used for profiling (or training).
- Classifiers: SVM, LDA, Naïve Bayes, and QDA.
SR is the ratio of the number of successes to the total test samples (500)

<table>
<thead>
<tr>
<th># var.</th>
<th>QDA</th>
<th>LDA</th>
<th>SVM</th>
<th>Naïve</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>99.6</td>
<td>77.4</td>
<td>99.9</td>
<td>83.4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th># var.</th>
<th>QDA</th>
<th>LDA</th>
<th>SVM</th>
<th>Naïve</th>
</tr>
</thead>
<tbody>
<tr>
<td>61</td>
<td>99.9</td>
<td>74.5</td>
<td>99.7</td>
<td>80.2</td>
</tr>
</tbody>
</table>
Profiling and Classification (Register)

Notation: Rd: destination register and Rr: source register

- For profiling each register, only the target register is fixed and other variables such as OP code, another register are randomly selected.
- Various machine learning algorithm can be exploited
- Classification results (Rd0 ~ Rd31, Rr0 ~ Rr31)

<table>
<thead>
<tr>
<th># Var (45)</th>
<th>SVM</th>
<th>LDA</th>
<th>Naïve</th>
<th>QDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR (Rd)</td>
<td>98.3</td>
<td>89.1</td>
<td>89.8</td>
<td>99.9</td>
</tr>
<tr>
<td>SR (Rr)</td>
<td>97.6</td>
<td>88.3</td>
<td>87.5</td>
<td>99.6</td>
</tr>
</tbody>
</table>
Targets in Literature

- Contents of SRAM and BBRAM [1,2]
- Logical state of registers (logic locking keys, cryptographic keys, bitstreams) [3,4]
- Outputs of logical gates [5]
- Timing-based PUFs [6]

LVP reveals the waveform at an electrical node similar to an oscilloscope.

Registers/logic switching from 0→1 or 0→1 @ 1MHz revealed by LVI.

Pattern from SRAM/registers using TLS revealing the stored value.

Logical state of all gates/registers extracted with LLSI by freezing clock and modulating Vdd @ 2MHz.

[1] Lohrke et. al., CHES 2018;
RE-enabled HW Assurance
Scenario 1: Original (Golden) Design Available

Input
- PCB Under Inspection

Process
- Imaging / Microscopy
  - Pre-processing & Segmentation
- CAD file Generation

Output
- Original CAD file
- CAD file for PCB Under Inspection
Scenario 2: Authentic (COTS) Image Data Available

PCB Under Inspection

Input

Imaging / Microscopy

Process

Defect Diagnosis

Output

Image Comparison

Authentic PCB Images (Blockchain)

Source: Hackaday.com

Source: Cognex.com
Scenario 3: No Prior Information Available

PCB Under Inspection

Input

Imaging / Microscopy

Process

Pre-processing & Segmentation

Non-destructive Disassembly

Defect Diagnosis

CAD file Generation

Reliability & Security Analysis

Bill of Materials, Software, etc.

Output

X - Plane  Y - Plane

Z - Plane

Missing signals

Counterfeit?

CAD file for PCB Under Inspection

Counterfeit?

Trojan?

Report

Input Process Output
Goal: Replace legacy/obsolete PCB with remake or automated upgrade

- Reduce time and cost of developing whole new system from scratch
- Avoid unreliable distributors which often source counterfeits
### System/Component Security Profiling Examples

<table>
<thead>
<tr>
<th></th>
<th>[1]</th>
<th>[2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCB PDN Model</td>
<td>Lumped</td>
<td>Distributed</td>
</tr>
<tr>
<td>Chip PDN Model</td>
<td>Lumped</td>
<td>Distributed</td>
</tr>
<tr>
<td>Transient Domain Simulation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Frequency Domain Simulation</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Security Analysis
- **Information leakage**
- **Fault injection**
- **Vulnerability evaluation**

---

Summary and Future Work
Summary and Future Work

- Foundation of cybersecurity is HW, which is at risk
- Automated reverse engineering is gaining traction
  - Nondestructive @ PCB level
  - Destructive @ IC level
  - Nondestructive @ FW level
- Assessment capabilities enabling new applications
  - Evaluation of COTS PCBs and ICs (e.g., HW Trojan and counterfeit detection)
  - Upgrade or replacement of obsolete electronic systems
- Future work is multidisciplinary and requires effort from multiple communities
  - Deep learning at all levels (RE, defect diagnosis, security analysis)
    - Data requirements: Share benchmarks, generate synthetic benchmarks, etc.
  - Security analysis tools at all levels
Acknowledgements

Collaborators

Ulbert J. Botero (UF)
Ronald Wilson (UF)
David Koblah (UF)
Pallabi Ghosh (UF)
Dan Capecci (UF)
Rabin Acharya (UF)
Nitin Varshney (UF)
Michael DiBattista (Varioscale)
Dr. Ed Principe (Synchrotron Research)
  Dr. Jungmin Park (UF)
Dr. Mark Tehranipoor (UF)
  Dr. Shahin Tajik (WPI)
Dr. Fatemeh Ganji (WPI)
  Dr. Navid Asadi (UF)
Dr. Damon Woodard (UF)

This work is made possible though the grants, gifts, and partnerships with