Automate inclusion of scalable defense mechanisms into chip designs to enable security vs. economics optimization
AISS: Program Structure

AISS Will Democratize Chip Security through Automation

Security Tools
- Obfuscation
- Watermarking
- Attack Simulation
- Threat Analysis

Automation Integration is Key to Driving Adoption

On-chip Security
TA1

Security Policy Enforcement
Monitoring
Provisioning
Authentication

Integration
TA2
- Silicon Platforms
- Generators
- Interconnect
- Optimization

DISTRIBUTION A. Approved for public release: distribution unlimited.
**Moving Target (I20)**

- Substantial efforts are on-going in the software community

**In Progress (SSITH)**

- Alteration of system behavior based on software-accessible points of illicit entry that exist due to hardware design weaknesses or architectural flaws

---

**AISS Focus Areas**

- **Side Channel** – extraction of secrets through physical communication channels other than intended (assumption: attackers are able to “listen” to emissions)

- **Reverse Engineering** – extraction of algorithms from an illegally obtained design representation (assumption: attackers have access to design files)

- **Supply Chain** – Cloning, counterfeit, recycled or re-marked chips represented as genuine (assumption: attackers can manufacture perfect clones)

- **Malicious Hardware** – insertion of secretly triggered hidden disruptive functionality (assumption: attackers successfully inserted malicious function(s) into the design)
Security Strategies by Company type

**Huge merchant semiconductor companies** (*Intel, Broadcom, Qualcomm…*)
- See the critical need and have large expert teams to create custom solutions

**Mid-size semiconductor and system companies** (*NXP, Cisco, Nokia…*)
- Recognize problems but lack expertise and sufficient economic motivation

**Defense contractors** (*Honeywell, NG, Lockheed…*)
- Possess deep, but limited, expertise (craft) unevenly applied to specific chips

**System integrators** (*Ring, Fitbit, August…*)
- No interest due to time-to-market focus and lack of in-house competency
Long Term EDA Dream: **System Synthesis**

System synthesis & optimization

1. $\Sigma (a \ast \text{Performance}, b \ast \text{Size})$
2. $\Sigma (a \ast \text{Performance}, b \ast \text{Size}, c \ast \text{Power})$
3. $\Sigma (a \ast \text{Performance}, b \ast \text{Size}, c \ast \text{Power}, d \ast \text{Security})$
4. $\Sigma (a \ast \text{Performance}, b \ast \text{Size}, c \ast \text{Power}, \{d \ast \text{SideChannel}, e \ast \text{SupplyChain}, f \ast \text{RevEngineering}, g \ast \text{MalHardware}\})$

Key challenges:

- **Quantification of security**
- **Rapid estimation of attack resistance**
- **Multi-dimensional optimization**

(source: Broadcom)
Combinatorial Optimization explores HUGE solution spaces (billions), but requires rapid estimation of “goodness”

**Performance** and **Size** estimators are well understood and incorporated in modern tools

**AISS** will drive discovery of rapid estimation of **power** and **security**

$$f(a, b, c, d) = \sum (a \cdot \text{Performance}, b \cdot \text{Size}, \overbrace{c \cdot \text{Power}, d \cdot \text{Security}}^{\text{estimate, estimate}})$$
AISS: Optimization Cost Functions

\[ f(a,b) = \sum (a*\text{Performance}, b*\text{Size}) \]

Cost Function Examples

<table>
<thead>
<tr>
<th>Application</th>
<th>Perf.</th>
<th>Size</th>
<th>Power</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawn Sprinkler</td>
<td>2</td>
<td>7</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>Engine Control</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Guided Projectile</td>
<td>5</td>
<td>1</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Network Router</td>
<td>9</td>
<td>5</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>7</td>
<td>9</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Smart Watch</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>3</td>
</tr>
</tbody>
</table>

Security Cost Function Expansion

<table>
<thead>
<tr>
<th>Application</th>
<th>Side Channel</th>
<th>Reverse Eng’g</th>
<th>Supply Chain</th>
<th>Malicious Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawn Sprinkler</td>
<td>1</td>
<td>1</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>Engine Control</td>
<td>1</td>
<td>7</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Guided Projectile</td>
<td>3</td>
<td>9</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>Network Router</td>
<td>9</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>8</td>
<td>9</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>Smart Watch</td>
<td>6</td>
<td>8</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: The 80s
Point: Technology for 2-dimensional optimization has been around for ~40 years

DISTRIBUTION A. Approved for public release: distribution unlimited.