CAN YOU TRUST THIRD-PARTY IPs?

Using (third-party) IPs is crucial for cost-effective IC and SoC design

Risks
- IPs could contain security vulnerabilities and undocumented, malicious logic
- Hardware Trojans can be inserted at various stages during the IP design cycle

In security- and safety-critical chips these risks must be managed

Challenges
- IPs are complex - SoC Integrators don’t know the details
- RTL code review is effort-intensive and likely to miss issues
- Limited engineering resources, expertise, tools

AUTOMATED TRUSTWORTHINESS ASSESSMENT

Highlights
- No trusted/independent IP model is required
- No formal verification or IP expertise required
- Automated, repeatable, objective assessment process
- Leverage unique technology and expertise under-the-hood

RESULTS

Test suite
- 90 designs with and without Trojans inserted
- Size range: 100 to 100K FFs

<table>
<thead>
<tr>
<th>Source</th>
<th>Name</th>
<th>Runtime</th>
<th>Issues Reported</th>
<th>Trojans Inserted</th>
<th>Automatic Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrustHub*</td>
<td>AES</td>
<td>13 hours</td>
<td>240</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TrustHub</td>
<td>PCIe</td>
<td>&lt;1 min</td>
<td>72</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TrustHub</td>
<td>RISC-V</td>
<td>&lt;1 min</td>
<td>3</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Gitch</td>
<td>RISC-V</td>
<td>&lt;1 min</td>
<td>3</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>OneSpin</td>
<td>UART</td>
<td>&lt;1 min</td>
<td>10</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Aerospace**</td>
<td>Spartan6</td>
<td>&lt;1 min</td>
<td>3</td>
<td>No/Yes</td>
<td>No</td>
</tr>
<tr>
<td>Aerospace</td>
<td>RISC-V</td>
<td>13 min</td>
<td>46</td>
<td>No/Yes</td>
<td>No</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Leon3</td>
<td>6 hours</td>
<td>423</td>
<td>No/Yes</td>
<td>No***</td>
</tr>
</tbody>
</table>

* TrustHub designs averaged results over multiple articles
** Aerospace designs contained 1 golden, 3 with Trojans
*** Leon3 articles consisted of 1 Trojan design, 1/3 Trojans discovered

EXAMPLE OF DETECTED TROJAN

- Triggers based on deep counters
- Specific sequences of events triggering unusual control action
- FSM with malicious logic monitoring the occurrence of specific data sequence

SIGNOFF ASSESSMENT REPORT

Concise - Actionable - Customizable - Issues linked to IP model

CONCLUSION

IP trustworthiness is a rising concern
- A vulnerability or hardware Trojan can compromise the security of the entire system

Automated trustworthiness assessment
- Provides a low-effort, objective approach to increase confidence that IP is trustworthy
- Does not require additional IP model or detailed IP knowledge
- Algorithms need continuous improvement
- Low noise level (false alarms) is key

Process limitations
- No trustworthiness metric (open industry topic)
- Detects Trojans, but cannot prove absence of all functional Trojans

To learn more contact
john.hallman@onespin.com