Tortuga Logic is a cybersecurity company providing products and services to detect and prevent hardware vulnerabilities. Unlike software and firmware security solutions that do not find underlying hardware flaws or manual penetration testing that only find issues after the device is manufactured, Radix-M provides a system level hardware security verification solution. Only when leveraging commercial emulators is full System on a Chip (SoC) and firmware security validation feasible. By running firmware and software on the SoC, Radix-M simultaneously analyzes the entire system, which greatly increases the detection and prevention of security vulnerabilities that may be lurking in the system’s Root of Trust or processing system.

The inputs to Radix-M include System IP or SoC’s RTL files, a set of security rules based on the threat models defined for the system, along with the block or system level testbench files that verification teams are already developing. Radix-M then creates and adds a hardware Security Model to the design. The Security Model is used to check the validity of the security rules while running in a commercially available emulator, such as Cadence® Palladium®, Mentor® Veloce® or Synopsys® ZeBu®.

**USE CASES**

- Hardware Root of Trust Security Verification
- SoC access control verification
- Secure boot sequence verification
- Red/Black separation
- Timing side channels
- Configuration register read/write protection
- Encryption key leakage
- Verification of clearing secret content
- External Debug disablement/analysis
- 3rd Party/vendor IP and interface security

**BENEFITS**

- Ensures correct configuration for maximum security
- Prevents unauthorized access
- Verifies boot data and keys remain secure
- Checks for isolation of redundant systems
- Detect and prevent Meltdown/Spectre variants of attacks
- Ensures SoC access control is maintained
- Ensure keys remain secure during and after usages
- Ensure secure data is cleared prior to switching to non-secure modes
- Ensures JTAG does not access secure data or keys
- Increases assurance that IP is secure and does not contain hardware trojans

**PROJECT OVERVIEW:**

<table>
<thead>
<tr>
<th>Types of Hardware Vulnerabilities</th>
<th>Actual Hardware Violations</th>
<th>Security Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Root of Trust Security Verification</td>
<td>146</td>
<td>70.3%</td>
</tr>
<tr>
<td>SoC access control verification</td>
<td>70.3%</td>
<td></td>
</tr>
<tr>
<td>Secure boot sequence verification</td>
<td>29.4%</td>
<td></td>
</tr>
<tr>
<td>Red/Black separation</td>
<td>146</td>
<td></td>
</tr>
<tr>
<td>Timing side channels</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Configuration register read/write protection</td>
<td>56.3%</td>
<td></td>
</tr>
<tr>
<td>Encryption key leakage</td>
<td>30.4%</td>
<td></td>
</tr>
<tr>
<td>Verification of clearing secret content</td>
<td>10.4%</td>
<td></td>
</tr>
<tr>
<td>External Debug disablement/analysis</td>
<td>4.8%</td>
<td></td>
</tr>
<tr>
<td>3rd Party/vendor IP and interface security</td>
<td>2%</td>
<td></td>
</tr>
</tbody>
</table>

**STEP 1:** Express Threat Models

- RTL
- SECURITY RULES

**STEP 2:** Generate Security Model

- SECURITY MODEL GENERATION
- SECURITY MODEL (Verilog RTL)

**STEP 3:** Insert Security Model into Emulation Flow

- HARDWARE EMULATION
- TEST BENCH

**STEP 4:** Analyze Results & Identity Violations
If security vulnerabilities are found, analysis information including custom waveforms and leakage path information helps pinpoint the root cause. The Radix Analysis Views displays both signal values and leakage information to identify the source of the vulnerability and the signal values that caused it.

Using Radix-M greatly speeds up existing RTL security review while diminishing the risk of a hardware security vulnerability. Radix-M is compatible with Cadence, Palladium, Z1 Enterprise Emulation Platform. For early access availability on Mentor Veloce or Synopsys ZeBu, please consult your local sales representative.

**ABOUT TORTUGA LOGIC**

Founded in 2014, Tortuga Logic is a cybersecurity company that provides industry-leading services and solutions to address security vulnerabilities overlooked in today's systems. Tortuga Logic’s innovative hardware security verification solutions, Radix, enables verification and security teams to detect and prevent system-wide exploits in FPGAs, ASICs and SoCs that are otherwise undetectable using current methods of security review.

**HARDWARE SECURITY DEVELOPMENT LIFECYCLE**

- Threat Modeling
- Security Specifications
- Block & Subsystem Design
- Security Verification
- SoC Integration
- Chip-Level Security Verification
- Low-Level Software Testing
- SoC Security Verification w/ Software
- Post-Si Security Testing
- Radix-M Emulation
- Radix-S Simulation
- Radix used to specify & verify security objective pre-silicon
- A complete SDL with Radix

**TO LEARN MORE**  www.tortugalogic.com  info@tortugalogic.com