Cycuity

Is Your Hardware Root of Trust Delivering the Security You Expect?

A hardware root of trust (HRoT) creates a strong foundation for **system security**, reducing the likelihood of full system compromise. While a HRoT provides valuable security features, it is important to ensure that they are **secure features**. Vulnerabilities can have a major impact, including:

Unprivileged access to **your customers' proprietary or confidential data**

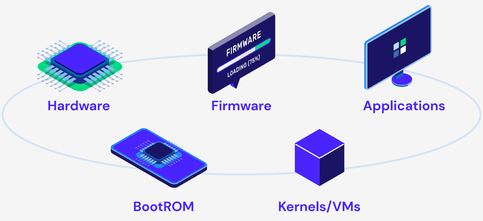
Unauthorized access to device keys, **allowing adversaries to steal**

Side-channel **leakages of critical customer information**

Modifications of authentication keys **for execution of unauthorized software**

Hardware is not developed or used in a vacuum.

Vulnerabilities hide in the design complexity and interactions between different components.



To secure a system effectively:

Each layer of the computer stack must be analyzed individually. The end-to-end system must be examined as a whole

When validating that HRoT is implemented correctly, two other potential risks must be considered:

Integration Mistakes

When adding purchased intellectual property (IP) to an in-house hardware design, it's critical to ensure that its security function remains intact when placed into the SoC context.

Configuration and Usage Mistakes

When programming the security components in software, it's important to create a configuration that ensures security across the entire system.

How can you verify HRoT security confidently?

Is your **implementation** secure?

A purchased or internally reusable HRoT is often highly versatile, but **simple design errors can introduce security vulnerabilities at this core function.**

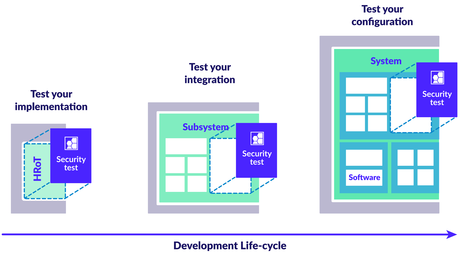
Is your **integration** secure?

Incorporation of the HRoT into a broader **SoC can introduce unintended security vulnerabilities through simple errors or misunderstanding of functionality.**

Is your **configuration** secure?

Even if HRoT is implemented correctly at the hardware level, **errors in any software that configures the HRoT at boot time can introduce vulnerabilities.**

Cycuity provides organizations with a reliable and efficient way to address these concerns without the cost and effort required by traditional techniques — throughout the entire development lifecycle.



Cycuity's Radix technology is more comprehensive than today's common adaptation of functional verification methods and can detect and mitigate hardware vulnerabilities that result from incorrect implementations, integrations, and configurations.

Ensuring hardware security, one chip at a time.