Cycuity

THE NEW RULES OF HARDWARE SECURITY

Now that semiconductors play a central and fast-expanding role in many aspects of everyday life, chip manufacturers face a growing collection of new pressures, including:

- Increasing design complexity
- More demanding security requirements from customers
- New security standards and regulatory requirements
- Increasingly sophisticated threat actors

These challenges are exacerbated by the fact that more non-traditional devices than ever are internet-connected. Connectivity brings many advantages to both product manufacturers and their customers. But it also introduces a substantial new set of security risks with real-world implications.

While formal hardware security practices have existed for decades, the connected era is rewriting the rulebook for how semiconductor companies and product manufacturers need to approach hardware security. The following are a set of new rules that semiconductor manufacturers should embrace to contend with this changing hardware security landscape proactively.

RULE 1: DEVELOP YOUR HARDWARE SECURITY STRATEGY AT THE SUPPLY CHAIN LEVEL.

Nearly all technology-enabled products are built by an ensemble of supply chain partners. While the industry has mastered many of the operational aspects of building products this way, most organizations are less mature when it comes to coordinating hardware security practices across organizational boundaries and phases of the product development lifecycle.

Hardware vulnerability management in the connected era must encompass all third-party and internally developed components. This includes:

- Validating that third-party security intellectual property (IP) is implemented securely.
- Extending the validation approach as security IP is integrated into a system-on-chip.
- Further enhancing the approach as an SoC subsystem is implemented alongside other hardware and software components to create a complete system.

RULE 2: CREATE VERIFIABLE SECURITY REQUIREMENTS EARLY IN THE DESIGN PROCESS.

A sound hardware security strategy starts with clear and comprehensive requirements. But this is more challenging to accomplish than it seems on the surface.

To be effective, security requirements must have the following characteristics:

- Broad coverage of both known and unknown security risks.
- Clear metrics that make it possible to measure validation progress and completeness.

1. Identify all assets that need to be protected.
2. State the security objectives for each of these assets.
3. Identify protection mechanisms that meet these objectives **for each asset**.
4. Define methods of measuring the efficacy of each protection mechanism.

Accomplishing this will likely require new hardware security verification techniques that provide more flexibility and scalability than those used in the past.

RULE 3: MOVE BEYOND FUNCTIONAL VERIFICATION TO IDENTIFY VULNERABILITIES AND UNEXPECTED BEHAVIOR.

Functional verification plays a foundational role in hardware security. Traditional techniques like formal verification and SystemVerilog Assertions (SVA) are effective starting points for verifying expected behavior of security IP, but they still leave a substantial gap in overall hardware vulnerability management.

Verification of expected behavior alone does not ensure that unexpected behavior won't also occur. It also fails to rule out the presence of known or unknown hardware security vulnerabilities. So, while continuing to perform functional verification is important, it's essential to augment these techniques with additional security verification approaches that are expressive and scalable enough to detect unknown or unexpected conditions as well.

One of the most powerful techniques that can be used to close this gap is information flow analysis. By analyzing flow-enabling signals concretely and flow data elements symbolically, information flow analysis can be scaled to detect unknown vulnerabilities and unexpected behavior systematically at every step from foundational security IP to software-enabled SoC.

RULE 4: AUTOMATE THE SECURITY VERIFICATION PROCESS AS MUCH AS POSSIBLE.

Combining verifiable security requirements with more capable and scalable verification techniques like information flow analysis does more than just expand coverage and ensure continuity throughout the product lifecycle. It also enables greater automation.

A more automated and systematic approach to hardware security verification allows for more frequent and consistent security assessments without adding cost, resource demands, or time delays to the product development process. Performing security validation more frequently and at every step from block level to full system significantly reduces the risk of accidental introduction of a security weakness at a later stage of product development.

RULE 5: ENSURE THAT ALL HARDWARE SIGNOFF DECISIONS ARE DATA-DRIVEN.

One of the most difficult aspects of semiconductor development is achieving a formal signoff on a design. Decision-makers are often forced to make signoff decisions based on incomplete information. While this process generally includes a review of hardware security verification steps taken during the design and development process, the individual being asked to sign off often has little visibility into the efficacy of these steps and the resulting security risk.

Once steps are taken to broaden and automate hardware security verification and base these activities on verifiable security requirements, it becomes possible to make the signoff and release of a hardware design a data-driven decision rather than a subjective one. This is desirable for all parties involved. Stakeholders have a clearly defined measurement of success, and decision-makers will have clear criteria for signing off and releasing a design for tape-out with confidence.

RULE 6: PROVIDE SECURITY ASSURANCE TRACEABILITY TO CUSTOMERS.

In addition to simplifying internal signoff processes, adopting a hardware vulnerability management approach that includes verifiable requirements gives semiconductor manufacturers the ability to demonstrate their security assurance measures to their downstream customers.

This has the primary benefit of lowering hardware security risk. But greater traceability also provides other business benefits to both producers and buyers of semiconductor products. Semiconductor manufacturers can highlight verifiable security as a point of differentiation from other competing chips. Meanwhile, companies producing products with integrated semiconductors can simplify their own security and compliance processes through better documentation and greater confidence in their decision to delegate hardware security to their supply chain partners.