Silicon Assurance

Providing assurance for custom microelectronics components

Whitepaper

Analyz™-N: The Armor for RTL and Gate level Designs

INTRODUCTION

Globalization of the microelectronics supply chain has led to significant interest in comprehensive hardware security solutions in recent years. Growing demand for secure edge computing and Artificial Intelligence (AI) hardware has greatly accentuated this interest. Unlike software, network, or information security, hardware security solutions are generally more challenging due to (1) the sheer complexity of silicon chips and (2) vast and rapidly evolving attack surfaces due to the volatile nature of the supply chain. Hence, there is a critical need for innovative technology to automatically (1) identify and analyze diverse hardware vulnerabilities; (2) investigate low-cost protection approaches; (3) quantify the level of threats with metrics; and (4) accurately pinpoint the vulnerable parts of a design. Existing commercial solutions fail to meet all these requirements.

This white paper introduces a modular software platform, Analyz, and one of its tools, Analyz – N, to detect and assess hardware security vulnerabilities and attacks. Analyz – N can detect several classes of vulnerabilities/attacks, including access control violations, asset leakage, and malicious logic or backdoor. The tool suite is semi-automated, and its capabilities have been demonstrated on open source RISC-V chips.

ACCESS CONTROL VIOLATIONS

We examine access control violations on a system-on-chip (SoC) with Hardware Root of Trust (HRoT) and a processor IP. The HRoT is a minimum set of hardware and software intended to offer security as soon as the system is powered on. In most cases, HRoT is embedded in an SoC containing an application processor, on-chip system bus, on-chip memory, USB connectivity, memory controller, and system controller. Any interface connecting the HRoT to the rest of the components of the SoC must have proper access control mechanisms in place to regulate and manage access to the resources and information stored within HRoT. By implementing authentication and authorization mechanisms, HRoT's functionality can be prevented from corruption by malicious inputs from the external components of the SoC. Furthermore, such solutions will ensure sensitive information such as device-specific encryption keys and other critical assets never leaks beyond the HRoT boundary.

Two distinct behaviors can introduce access control vulnerability: incorrect permissions provided to a user or a resource by the administrator or a program, and errors in the mechanism's implementation prohibiting it from effectively upholding the required access control requirements.

For hardware, the access control vulnerabilities are listed in CWE-284: Improper Access Control.

THREAT MODEL

The threats to SoC and IP are many and growing. To identify such threats and develop countermeasures, understanding the usage of the SoC/IP, the associated threat model, and what assets to protect are crucial. This can be challenging as SoCs/IPs are used in many products that address different markets.

A hardware security architect assessing an SoC for threat and vulnerability (particularly with HRoT) should build a threat model based on the following information:

- Operating environment of the system using the SoC
- Assets associated with the SoC
- Type of possible attacks, level of access of a potential attacker, possible attack vectors, resources of an attacker, and impact if the system is compromised

Countermeasures and analysis tools to detect the attack could be designed according to the threat model, and the vulnerability of the implemented protection mechanism can be further assessed.

The threat actor in the access control scenario includes unauthorized users, malicious insiders, and attackers who may attempt to gain unauthorized access to the SoC design and the sensitive data stored within the HRoT. They can leverage the network access ports, physically access the system, or use software-based threats as potential attack vectors.

This process of developing a threat model enables the hardware security architect to develop strategies to reduce the risk of a violation. .

ANALYZ™ - PLATFORM

Security analysis of SoC and processor IP designs requires a good understanding of the threat model. Preventing malicious actors from exploiting SoC and IP vulnerabilities, and introducing post-synthesis components in the design, is critical. Such components can retain the design's intended behavior while augmenting it with undesirable features to hamper functionality or silently exfiltrate data. The ease and detectability of such vulnerabilities and modifications while constantly educating on the rapidly expanding threat landscape are challenges the hardware security architect should overcome.

The Analyz™ platform is a suite of tools designed to alleviate the above challenges. It includes tools, such as Analyz™-N and Analyz™-S, that can algorithmically evaluate pre- and post-synthesis designs for security vulnerabilities and suggest measures to mitigate potential threats. The Analyz™-N discovers security vulnerabilities, zeroes-in on attack vectors, and generates threat mitigation report. The report guides designers to iteratively strengthen the overall security of the chip design. The tool can also be plugged into the security annotation methodology of the IEEE P3164 standard. The Analyz™-S enables the hardware security architect to identify power and electromagnetic side-channels in the post-synthesis design. The tool can also identify leaky paths in the design .

ANALYZ-N™

A bad actor can leverage the hardware design and integration phase to modify the logic and give other SoC components access to the data from HRoT. Analyz-N™ is a software package that discovers security vulnerabilities in SoC of IP designs, which can lead to access control violations. The weaknesses that enable such violations are not always evident at the Register Transfer Level (RTL) or gate level. Furthermore, the test and debug infrastructure at the synthesized logic level can introduce additional vulnerabilities. By working with the RTL or synthesized (gate level) netlist, Analyz-N™ can evaluate the design for weakness and even rework the logic to be functionally identical but more immune to potential attacks.

Analyz-N™ takes as input the RTL or gate level netlist and design library to identify any violations of security properties derived from asset identification and the threat model. The tool uses proprietary algorithms to analyze the design for potential weaknesses and malicious logic at the pre-silicon design and verification stage. This is shown in Figure 1. As such, designers can prevent vulnerabilities before manufacturing and deployment.

ANALYZ-N™ CONTINUED ...

Capabilities:

- Analyz-N™ can detect design flaws and malicious logic/backdoor
- Detect Assets in an IP and SoC
- Generate Security Assertions for an IP and SoC
- Identify Trigger Vectors of Vulnerabilities
- Threat Mitigation Report

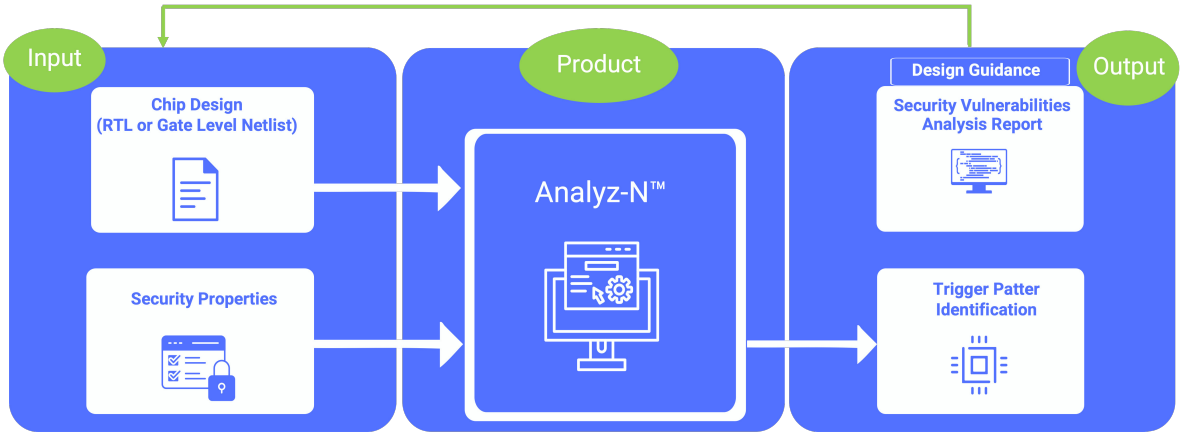

Figure 1: The Workflow of Analyz™-N

Analyz™ - N can be integrated with commercial Simulator or Emulator for fine-grained analysis of security vulnerabilities in SoC modules. Furthermore, our tool can identify isolated regions in the design which could affect performance. The extended workflow is shown in Figure 2.

ANALYZ-N™ IN COMMERCIAL EDA FLOW

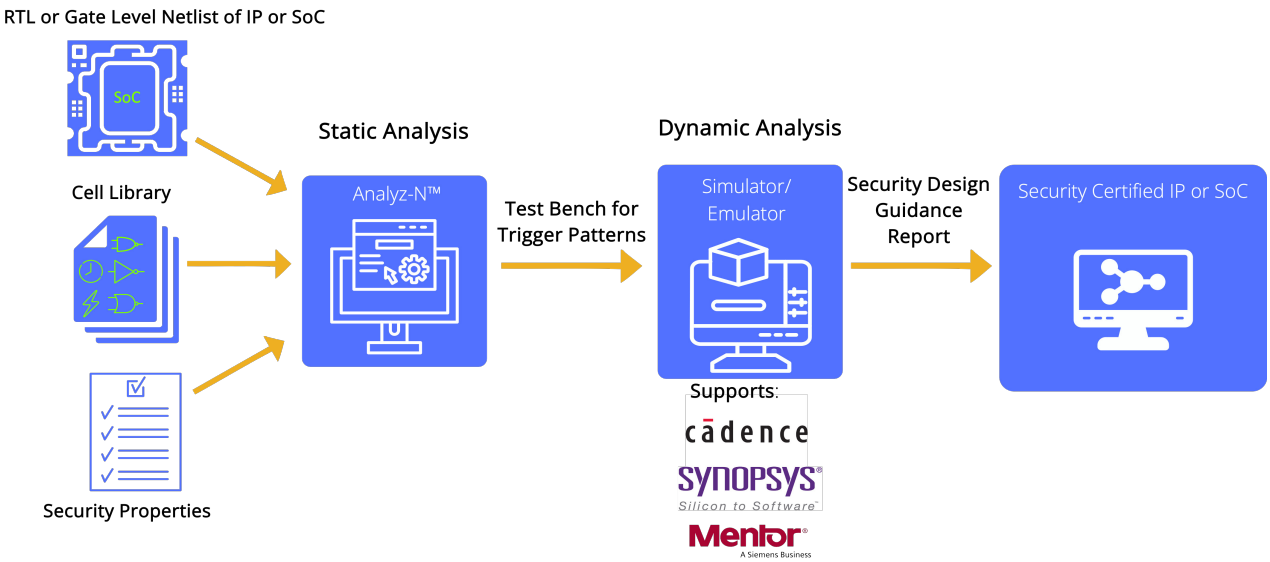

Figure 2: The Workflow of Analyz™ - N with commercial simulators