2024 25th International Symposium on Quality Electronic Design (ISQED) | 979-8-3503-0927-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISQED60706.2024.10528764

Trimming The Fat: A Minimum-Security Architecture for Protecting SoC Designs Against Supply Chain Threats

Kshitij Raj, Aritra Bhattacharyay, Swarup Bhunia, and Sandip Ray
Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, 32611, USA.
Email: kshitijraj@ufl.edu, abhattacharyay@ufl.edu, swarup@ece.ufl.edu, sandip@ece.ufl.edu

***Abstract*—Supply chain security is an interesting facet of modern System-on-chip security. While other attacks (control flow, information flow, side-channel, etc.) may be of interest in specific application domains, supply chain confidentiality attacks are almost *always* possible in virtually every SoC. These attacks include device counterfeiting, overproduction, reverse engineering, illegal recycling, etc. Because supply-chain is a blanket attack space, a security architecture that provides assurance against it is an open research topic. Minimum security threats include protection against counterfeiting, reverse engineering, and illegal recycling across all lifecycles of the device. In this paper, we present SOCRATES, a minimum security architecture that provides security against such attacks. SOCRATES is a viable candidate, especially for low-power and area designs.**

***Index Terms*—Minimum Security, System-on-chip security architecture; Supply-chain**

I. INTRODUCTION

SOCRATES (for SoC Security Architectures) is a security architecture for supply chain for providing security assurance as per the minimum security standards. The idea here is to develop a standardized security architecture with minimal overhead, intended to be deployed in applications with high overhead constraints. System-level behaviors come at zero cost in μC-based architectures and can be implemented via firmware with relative ease. However, when unable to afford a μC, each requirement needs custom hardware to realize these functionalities. SOCRATES takes an orthogonal approach from traditional μC-based security architectures and puts together a lean design built from custom control logic and security countermeasures, dropping the excessive overhead from existing research, yet providing security assurance as per the minimum security standards. SOCRATES incurs an overhead of ∼63,000 gates while maintaining the encryption strength of 256 bits (see Table I).

II. THE SOCRATES ARCHITECTURE

SOCRATES is a low-overhead security architecture that builds on ad-hoc supply chain security countermeasures. The fundamental realization here is that the enforcement of security countermeasures necessitates four essential components: (1) a centralized command and control unit, (2) custom security countermeasures providing the base-level security functionality, (3) a distributed artifact for enforcing said security primitives outside the local boundary, and (4) dedicated interfaces to establish secure on-chip & off-chip communication. Although each serves a dedicated purpose, it is their synchronous coordination that achieves system-level security.

TABLE I
AREA & POWER OVERHEAD OF SOCRATES

ASIC Library	Area (μm2)	Dynamic Power(mW)	Leakage Power(μW)
GSCL45 45nm	80101	61.54	374.69
GF12LP 12nm	9126	16.7	128.1

The architecture platform provided by SOCRATES enables a standardized and streamlined process flow of security integration and implementation, outlined below:

1) Identify the threat model/s pertaining to the use case and develop custom security IPs for each threat (if any).
2) If such security IPs require additional control points or communication, security wrappers need to be augmented to support such requirements. Identify and separate control and data communication in the security enforcement sequences.

Accounting for the minimum security threat model, our strategy is to use a unique chipID, which is derived based on the physical signature of the chip to protect against counterfeiting and overproduction. We make use of the MeLPUF [1] to obtain such signatures using which an unclonable chipID is created. Correspondingly, to protect against reverse engineering attacks, SOCRATES uses the ProtectIP state-space obfuscation [2]. SOCRATES uses the chipID and the lifecycle state of the chip in tandem to track the chip across the device lifecycle to protect against any illegal recycling attempt. While the design obfuscation countermeasure can be enforced using security wrappers, the operation of the MeLPUF requires a dedicated control logic referred to as the PUF Control Module (PCM). The PCM is responsible for initiating transfers of PUF signatures and authenticating the final computed signature.

REFERENCES

[1] C. Vega, P. SLPSK, S. D. Paul, and S. Bhunia, "Melpuf: Memory in logic puf," 2020. [Online]. Available: https://arxiv.org/abs/2012.03162
[2] M. M. Rahman and S. Bhunia, "Practical implementation of robust state-space obfuscation for hardware ip protection," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp. 1–14, 2023.