Tropic Square and TROPIC01: Addressing Security Challenges through Openness

Abstract

The prevailing approach in today's chip design is closed-source. This approach was recently challenged by the broader open-hardware movement, where Tropic Square is positioned as the first supplier of an open-architecture, auditable, secure element chip available on the market - TROPIC01.

In the IC industry, both **trust and security are challenging**. Chips developed under the closed-source paradigm are black boxes. Despite design secrecy, cybercrime can exploit undocumented features and vulnerabilities. Cryptographers, security experts, and academia demand transparency and auditability to **move beyond blind trust**. Opening the design at least to the level that enables auditability leads to **verifiable Security by Design** and **strengthens trust**.

Some of today's standards, such as Common Criteria, imply that securing an open design is more challenging, since publicly available implementation details essentially guide the attacker by providing full disclosure of the attack surface. On the other hand, as reverse-engineering techniques become increasingly feasible and powerful, the closed-source philosophy prevailing in IC design, called **Security by Obscurity**, may **give a false impression of invulnerability**, especially to advanced implementation attacks.

Our view is that **Security by Obscurity is obsolete**, even though it may complement a Security by Design approach to support defense in depth and improve overall security; Security by Obscurity is opposed to trust.

Outline

- Trust, Security, and Auditability
    - Security by Design and Security by Obscurity
- Security Challenges
- The IC Industry Status Quo, The Security Perspective
    - Security by Obscurity and Security by Design
    - Trust Errosion
- Tropic Square Approach
    - Auditability Enabled by Openness
    - TROPIC01
- Future Open IC Design
    - Open Toolchains and PDKs
    - The ORSHIN project