EUROSMART
The Voice of the Digital Security Industry

Certification of Soft IPs and physical products

Context

The number of vulnerable devices on the market has resulted in an increased need for trust. Many new security standards, evaluations and certifications are flourishing, all with different levels of assurance. In this highly competitive market and fast-evolving security threats landscape, it is critical to be able to undertake security assessments in a time and cost-efficient manner. The situation is further complicated by the need for multiple stakeholders to be involved in the design phase of an IoT device, all of whom are involved in the implementation of security functions with layered architecture (application, OS, communication stacks, opensource software, and firmware and hardware).

The composition of security functions across all these IP providers is key to security consistency and efficient final product evaluation. Security assessment based on composition is under deployment to manage security integration with multiple IP providers.

Soft IP

Secure ICs and SoCs are built by integrating Soft IPs with different hardware IPs. Soft Intellectual Property (IP), also called a soft macro, is a macrocell described in a hardware description language such as Verilog or VHDL. To make a hardware product, Soft IPs have to be synthetized to provide a gate-level netlist which is then mapped to the specific process technology. For example, the same cryptoprocessor Soft IP can be synthetized using different standard cell libraries for different technological nodes.

Implementing the correct security protocol is one of the challenges facing hardware designers who have to ensure zero defects at the early stage of the silicon development phase while also maintaining functional security. Circuit development based on strong, formal, tool-supported methods to validate security properties provides superior quality and increased assurance.

A correct security protocol also falls within the scope of Soft IP providers who must demonstrate the quality and robustness of their product through evaluation and certification at the highest assurance levels.

Evaluation and certification

Eurosmart supports and promotes high assurance certification. The Common Criteria is a widely recognized international standard which outlines the Evaluation Assurance Level (EAL) process

describing the depth and rigour of an evaluation. EALs are therefore a measure of assurance quality. The highest EALs provide increased confidence in the security properties claimed.

The 'Security IC Platform Protection Profile' PP-0084 (BSI-CC-PP-0084-2014) is a key standard for security requirements for high-security ICs. PP-0084 refers to a complete Secure IC implementation and includes the assumptions made about the environment and its threats. PP-0084 requires "strict conformance", meaning that it should not be used partially. SOG-IS [(1)]mandates security evaluations based on concrete penetration testing on physical devices, conducted by skilled security experts. Penetration tests must cover the full set of attack classes in the JHAS attack method in order to reach the vulnerability assessment level AVA_VAN.5.

While SOG-IS certifications ensure a clear and reliable evaluation of the security of a physical product, they cannot be used 'as is' for Soft IPs, since only some parts of the evaluation are applicable. Vulnerability assessment may depend on other IPs or development flow and security testing is only feasible on models of the final tangible implementation.

As Soft IPs are customized during the hardware product's development flow, physical characteristics in the hardware end-product depend on the methodology and process used. It is therefore of utmost importance to perform concrete penetration testing on final products (real devices).

Conclusion

Eurosmart welcomes Soft IP evaluation and certification to improve security quality and assurance at the early stage of the development phases of a chip.

For Soft IPs, Eurosmart advocates for SOG-IS certification adaptation to preserve the value of rigorous development methodology and security properties testing.

Furthermore, physical products and Soft IP should be certified on different SOG-IS domains, while developing a methodology that facilitates the composite evaluations required for the highest levels of assurance.

As a vulnerability assessment based on product characteristics is only feasible on the physical product, Eurosmart calls for a clear differentiation of SOG-IS certification of Soft IPs and physical products.

(1) SOG-IS: Senior Official Group Information Systems Security (https://www.sogis.eu/)

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom – IMT, ISEN – Institut Supérieur de l'Électronique et du Numérique Toulon**), and associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several of the European Commission's expert groups: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, such as CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA and TCG.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | email contact@eurosmart.com