SECURE-BY-DESIGN IOT OPERATION WITH SUPPLY CHAIN CONTROL

DOSS Project Overview

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

Agenda

1. **Project introduction and goals**
   a. The consortium
   b. Supply Chain Protection
   c. Software security and identification information

2. **Project details**
   a. Artefacts under tests
   b. Security assurance modules and its workflow
   c. Product and operation security assurance

3. **Standardization activities**
   a. Potential SDOs
   b. ETSI MTS TST NWIs

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

General

Goals, architecture and methodology of the DOSS project

Funded by
the European Union

This project has received funding from the European Union’s Horizon Europe
research and innovation programme under grant agreement No 101120270

The DOSS project consortium

Atos

CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

Fraunhofer
FOKUS

MŰEGYETEM 1782

UNIVERSIDAD
DE MURCIA

RED ALERT LABS
IoT Security

SAFEPAY

IITiS

asvin

tecnalia
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

THALES

EVIDEN

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

RELEVANCE OF SUPPLY CHAIN PROTECTION

- **Poor communication within supply chain; no feedback loop**
  - Supply Trust Chain
  - Device Security Passport (DSP) incl. SBOM, HBOM, MUD
- **Large scale attacks**
  - December 2020 SolarWind, January 2021 MIMECAST, May 2021 Colonial Pipeline
- **Cascading effects**
  - e.g. CVE-2021-44228 (log4j)
- **Huge economic impact**
  - In 2021 the number of supply chain attacks tripled compared to the previous year .
    - Argon, 2021 Software Supply Chain Security Report

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

KEY UNDERTAKINGS

DOSS elaborates a secure-by-design methodology

implements related technology for complex IoT architectures based on

- SUPPLY CHAIN MONITORING
- COMPONENT TESTING
- ARCHITECTURE MODELLING

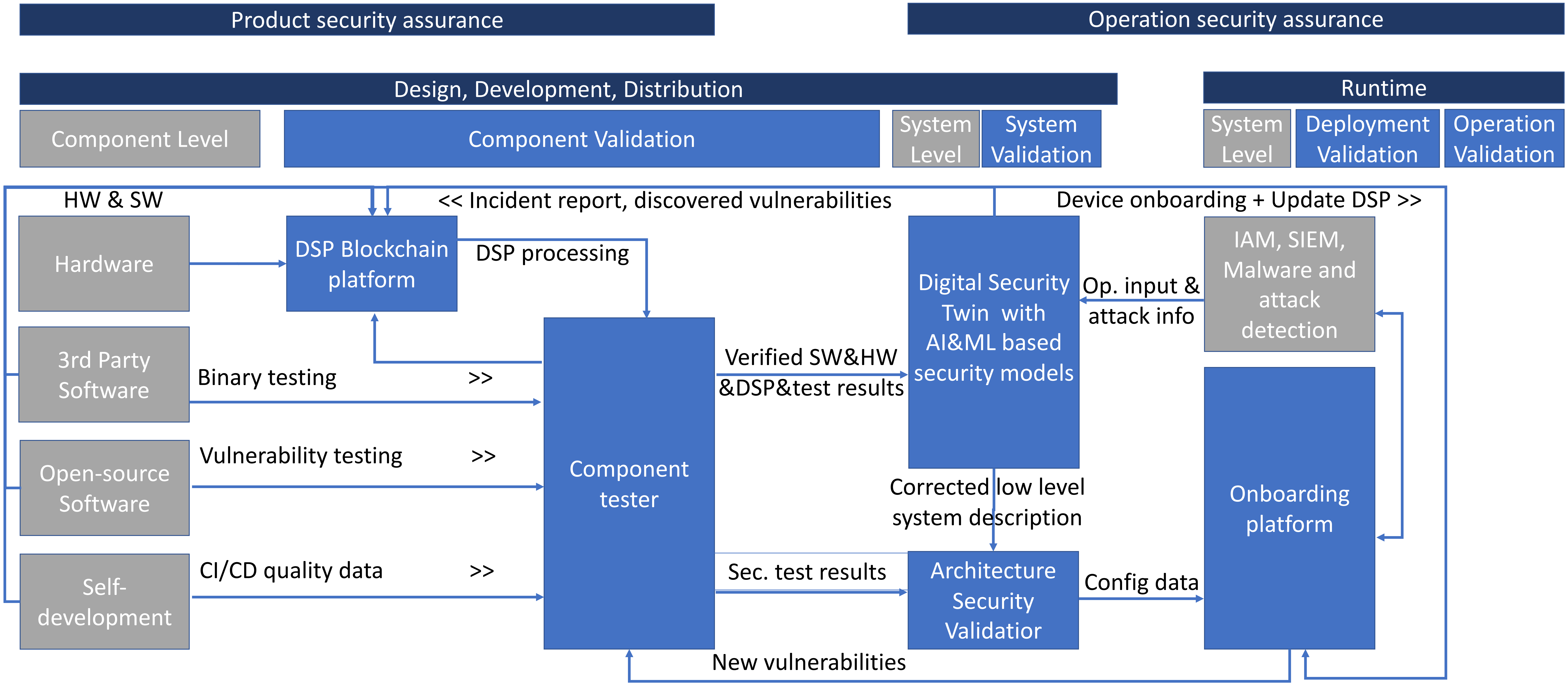
Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

Project details

Security assurance modules and its workflow

Integrated security modell



Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

Define the “Supply Trust Chain”

Collect and store reliable/verified data (e.g. DSP) from software & hardware suppliers including security characteristics.

Update lifecycle status by all authorized actors along the product/software/component supply chain.

All actors of the supply chain will **have real-time, online, actionable access to cybersecurity related information** which may be relevant for their IoT services and architectures.

- Formalize information sharing, data exchange between links of the supply chain – content, format and protocols
- Specify workflows
- Build proof of concept
- Standard recommendation

Funded by
the European Union

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101120270

The “Device Security Passport” (DSP)

A **machine-readable** document containing diverse **security related product information**

- From existing quasi or de facto standards to be included
  - Certificates (if any), Software Bill of Material, Hardware Bill of Material, Manufacturer Usage Description file, VEX, intended security level of usage scenario (EU CSA type labelling) and potentially other relevant information.

- Extension of the content of MUD files, VEX, SBOM and HBOM with **additional security related information**

Funded by
the European Union

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101120270

The Component tester

A **multi-function module for the security testing** of all components of a service architecture

Devices will be screened **based on their DSPs**

Implementing **SAST, DAST and IAST** approach for

- Especially for OSS and self-developed SW
- Establish a DevSecOps Pipeline

3rd party software will be assessed using **binary code-validation techniques**

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

Secure automated onboarding methodology and platform

Technology for the **automated onboarding and update** of even large number of devices

- Definition of the **necessary information** for the DSP (model ID, certificate, MUD file, etc.)
  - required to **identify and configure devices before** providing access to the designated network of the architecture
- Automated processing of DSP
- Use of attestation tokens
- Implementation of a reference architecture for the secure onboarding mechanism

Funded by
the European Union

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101120270

Design and implement the Digital Cybersecurity Twin (DCT)

The system will be able to **simulate the security context of diverse IoT system architectures** on the same hardware infrastructure to identify potential threats and security weaknesses already in their **design phase and prior to any configuration changes**.

- Implementation of a **configurable architecture using infrastructure automation technologies** that enable flexible creation of virtualized environments

- Automated generation of attack scenarios and their **transformation into executable security test cases**

- Use of **ML and AI for generating attack scenarios** and recommending counter measures against such attacks

Funded by
the European Union

This project has received funding from the European Union’s Horizon Europe
research and innovation programme under grant agreement No 101120270

Design and implement the pre-certification Architecture Security Validator

Verification of the design concept of IoT architectures prepared by the DCT against selected security standards and/or compliance requirements.

- **(Semi)automated transformation of standards** into formal and uniform representation of the requirements that an IoT system should comply with
- **Automated compliance checking of IoT architectures** against the selected, transformed standards
- Generation of **composite indicators measuring the compliance level** of IoT architectures – pre-certification

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

Validation of the procedures and technologies

Three pilot cases will be introduced based on existing IoT platforms representing diverse domains: **Automotive, Energy and Smart Home**

- Secure operating architectures will be **established with multiple security tools** and system
- **Service architectures will be connected to the Supply Trust Chain**
- Performance of new modules will be validated, security of the **end-to-end supply chain will be assessed**

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101120270

Standardization activities

Potential SDOs and contribution to MTS WG TST

Funded by
the European Union

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101120270

Contribution to SDOs and standardization interest groups

- **Working closely with the relevant Standard Developing Organisations**
  - National
    - DIN (German Institute for Standardisation)
  - European
    - ETSI
    - ENISA
  - International
    - ISO/IEC
    - IETF
    - Global Platform

- **Making context-relevant recommendations in respect of future standards**

*BO= Business Objective

roject has received funding from the European Union's Horizon Europe
rch and innovation programme under grant agreement No 101120270

Potential drafts for MTS TST NWI

- **Submission of the DOSS results for consideration**
  - Technical Specification (TS)
    - Security validation methodology for supply trust chains (Component Tester)
  - Technical Specification (TS)
    - Specification of a Device Security Passport
  - Technical Specification (TS)
    - Integrated IoT supply trust chain concept
  - Technical Report (TR)
    - Supply Trust Chain Applications and Assurance

*BO= Business Objective

roject has received funding from the European Union’s Horizon Europe
ch and innovation programme under grant agreement No 101120270

THANK YOU!

INFORMATION

https://dossproject.eu/

CONTACT US

info@dossproject.eu

Funded by
the European Union

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101120270