SecOPERA

Secure OPen source softwarE and hardwaRe Adaptable framework

Dr. George Hatzivasilis
Technical University of Crete (TUC)

RISC-V Summit Europe 2024

Project Identity Card

SecOPERA

Secure OPen source softwarE and hardwaRe Adaptable framework

Project Consortium: 13 partners

Project Type:
Research & Innovation Action

Duration: 36 Months

Start Date: 1 January 2023

Total Budget: €4,581,135

SecOPERA Consortium

1. POLYTECHNEIO KRITIS (**TUC**)
2. AEGIS IT RESEARCH GMBH (**AEGIS**)
3. ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS (**ISI**)
4. UNIVERSITY OF CYPRUS (**UCY**)
5. SECURITY LABS CONSULTING LIMITED (**SLC**)
6. ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER (**AUEB**)
7. PIERER INNOVATION GMBH (**PINNO**)
8. THALES SIX GTS FRANCE SAS (**THALES**)
9. COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (**CEA**)
10. IOTAM INTERNET OF THINGS APPLICATIONS AND MULTI LAYER DEVELOPMENT LTD (**ITML**)
11. VOGL SIMON (**VoXel**)
12. GREENCITYZEN (**GREEN**)
13. SPHYNX TECHNOLOGY SOLUTIONS AG (**STS**)

cea list
Green CITYZEN
AEGIS IT RESEARCH
PIERER INNOVATION
VoXel
THALES
ITML
University of Cyprus
Sphynx Technology Solutions
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS
ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
TECHNICAL UNIVERSITY OF CRETE
ΑΘΗΝΑ

13 Partners from 7 Countries: *Greece, Germany, Cyprus, Ireland, Austria, France, Switzerland*

Motivation

Open-source code

Cannot be trusted out of the box and lacks appropriate security guarantees

Open-source cognitive models

Already deployed without security assurance and guarantees against possible sensitive information leakage

Non-verified hardware solutions

Similar to OSS open-source hardware lacks security guarantees and can be prone to vulnerabilities or even contain malware (e.g. Hardware Trojans)

Challenges

1 Third-party components need to be assessed in terms of security

2 Open-source solution security is hard to justify in the current business interconnected market

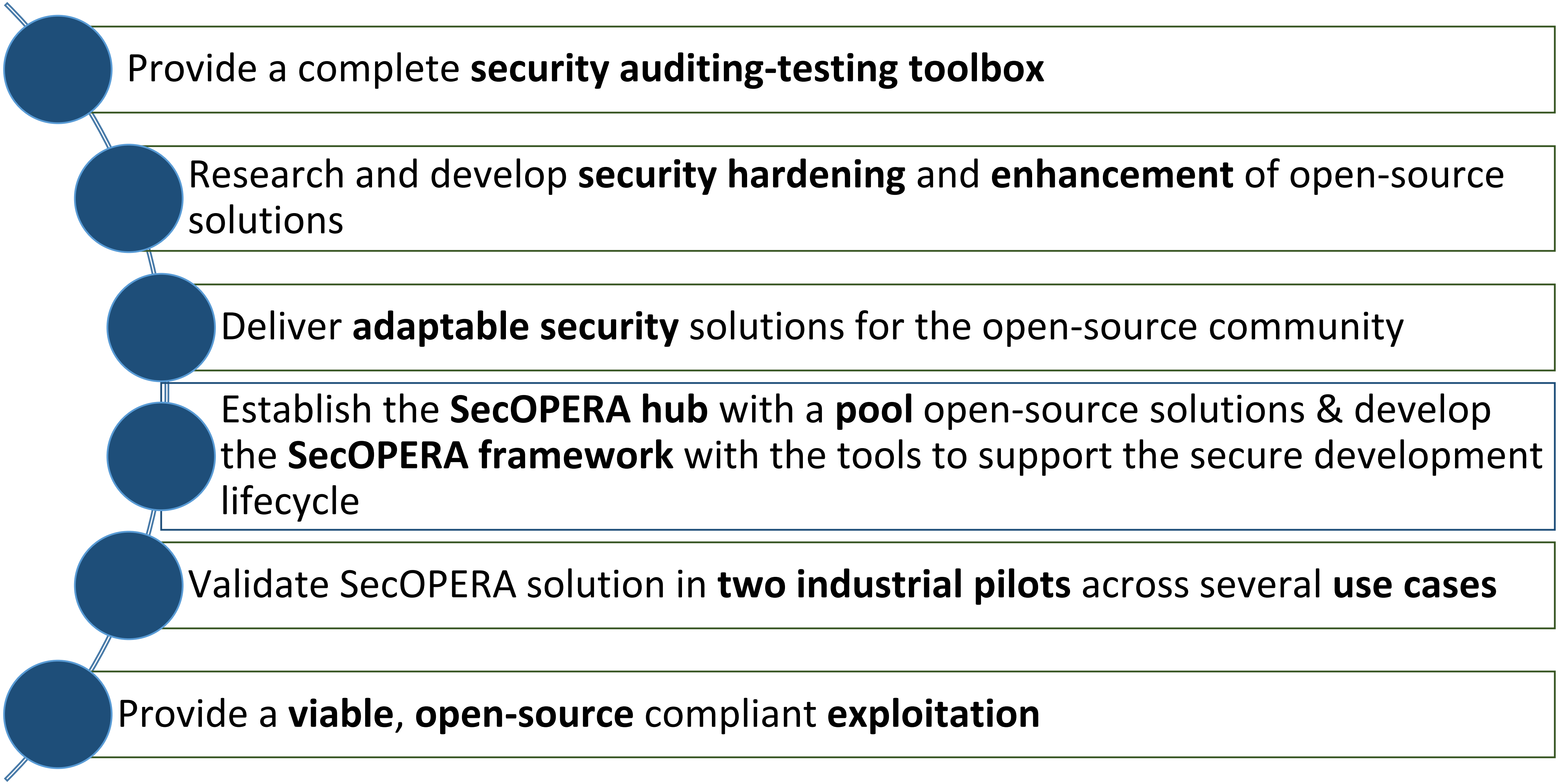
3 Static analysis tools often fail in the vastly diverse open-source landscape

Our mission

SecOPERA will provide a one-stop hub for complex open-source software and open-source hardware (OSS/OSH) solutions delivering to system designers and operators and OSS/OSH developers and testers the means to analyse, assess, secure/harden, and share open-source solutions.

The SecOPERA hub will offer an open-source framework supporting the DevSecOps lifecycle and generate solutions along with appropriate, verifiable security guarantees.

Objectives



- Provide a complete **security auditing-testing toolbox**
- Research and develop **security hardening** and **enhancement** of open-source solutions
- Deliver **adaptable security** solutions for the open-source community
- Establish the **SecOPERA hub** with a **pool** open-source solutions & develop the **SecOPERA framework** with the tools to support the secure development lifecycle
- Validate SecOPERA solution in **two industrial pilots** across several **use cases**
- Provide a **viable**, **open-source** compliant **exploitation**

SecOPERA pillars

Decompose: Decomposes open-source solutions in components and classifies them in the SecOPERA layers (device, application, network, cognitive).

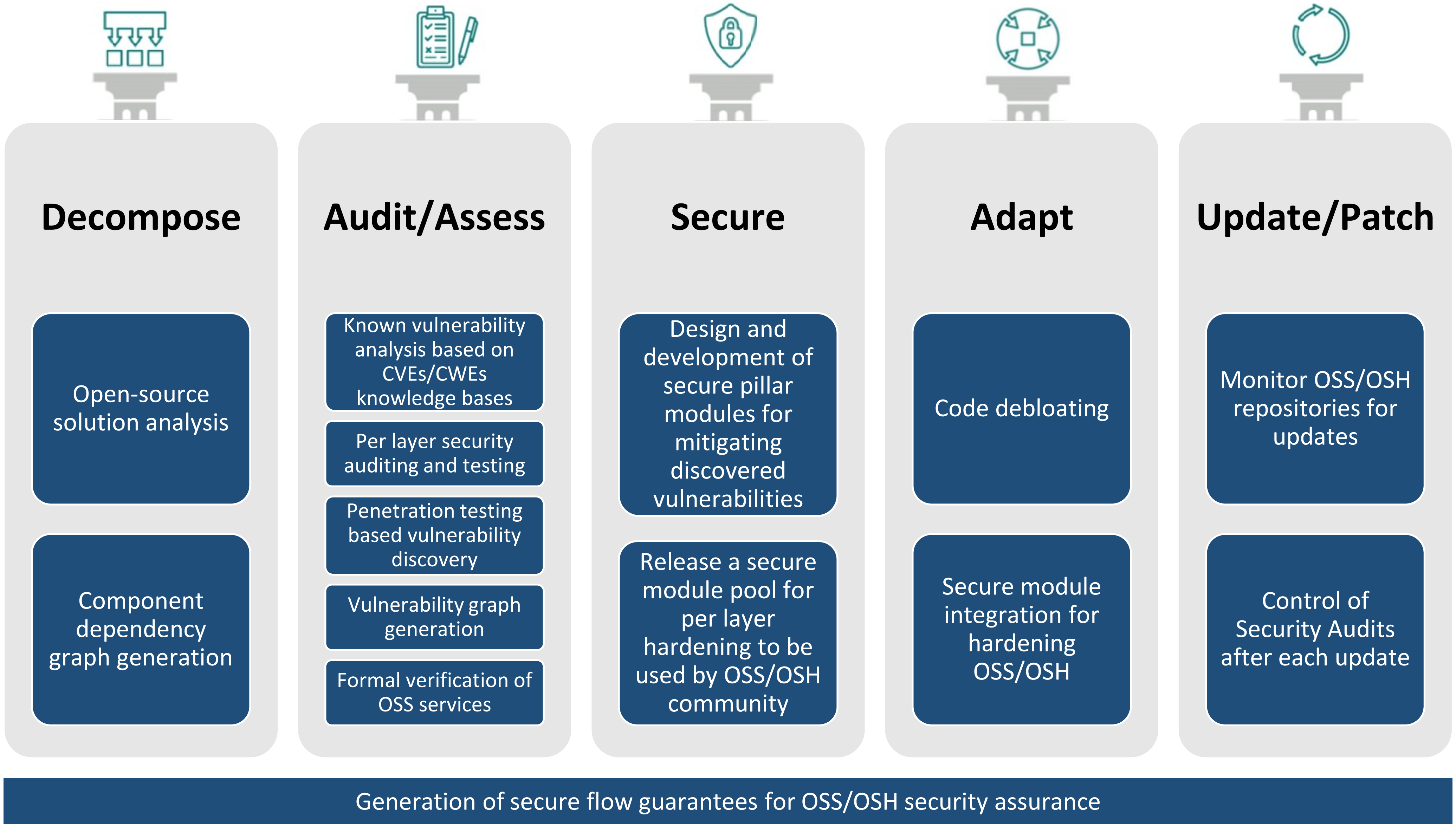
Audit/Assess: Performs vulnerability scan on each component and its dependencies and forms a vulnerability graph.

Secure: Consists of several OSS/OSH security modules which aim to harden each component.

Adapt: Adapts security modules in the OS solution

Update/Patch: Formally verifies the final solution and repeats the audit process after each update

SecOPERA functionalities



Decompose

- Open-source solution analysis
- Component dependency graph generation

Audit/Assess

- Known vulnerability analysis based on CVEs/CWEs knowledge bases
- Per layer security auditing and testing
- Penetration testing based vulnerability discovery
- Vulnerability graph generation
- Formal verification of OSS services

Secure

- Design and development of secure pillar modules for mitigating discovered vulnerabilities
- Release a secure module pool for per layer hardening to be used by OSS/OSH community

Adapt

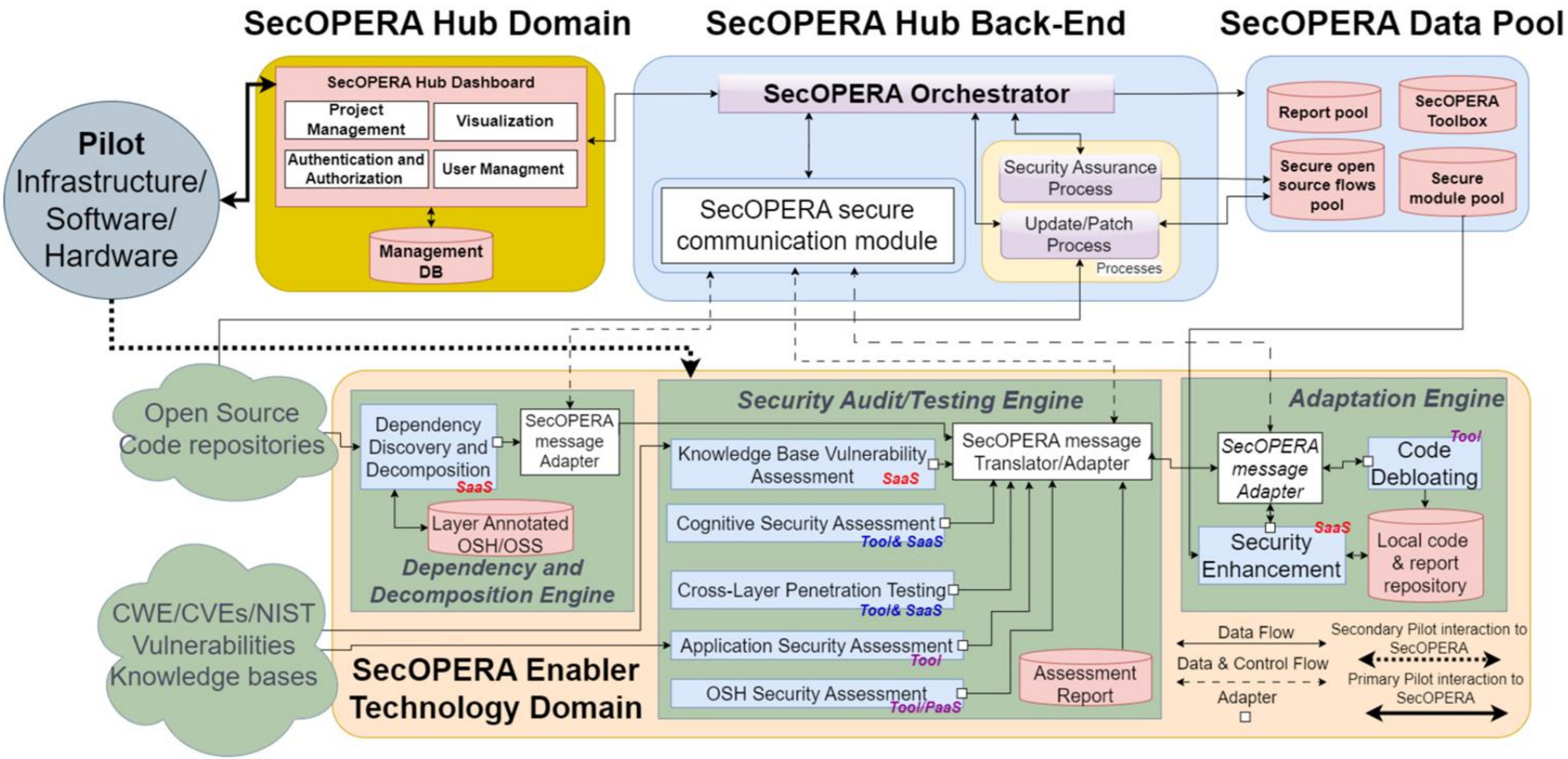
- Code debloating
- Secure module integration for hardening OSS/OSH

Update/Patch

- Monitor OSS/OSH repositories for updates
- Control of Security Audits after each update

Generation of secure flow guarantees for OSS/OSH security assurance

SecOPERA architecture


SecOPERA Hub Domain
SecOPERA Hub Back-End
SecOPERA Data Pool
Pilot Infrastructure/ Software/ Hardware
SecOPERA Hub Dashboard
Project Management
Visualization
Authentication and Authorization
User Managment
Management DB
SecOPERA Orchestrator
SecOPERA secure communication module
Security Assurance Process
Update/Patch Process
Processes
Report pool
SecOPERA Toolbox
Secure open source flows pool
Secure module pool
Open Source Code repositories
CWE/CVEs/NIST Vulnerabilities Knowledge bases
Dependency Discovery and Decomposition
SaaS
SecOPERA message Adapter
Layer Annotated OSH/OSS
Dependency and Decomposition Engine
SecOPERA Enabler Technology Domain
Security Audit/Testing Engine
Knowledge Base Vulnerability Assessment
SaaS
SecOPERA message Translator/Adapter
Cognitive Security Assessment
Tool& SaaS
Cross-Layer Penetration Testing
Tool& SaaS
Application Security Assessment
Tool
OSH Security Assessment
Tool/PaaS
Assessment Report
Adaptation Engine
SecOPERA message Adapter
Code Debloating
Tool
Security Enhancement
SaaS
Local code & report repository
Data Flow
Data & Control Flow
Adapter
□
Secondary Pilot interaction to SecOPERA
Primary Pilot interaction to SecOPERA

Pilot 1
Secure Supply Chain in Automotive Industry

SecOPERA

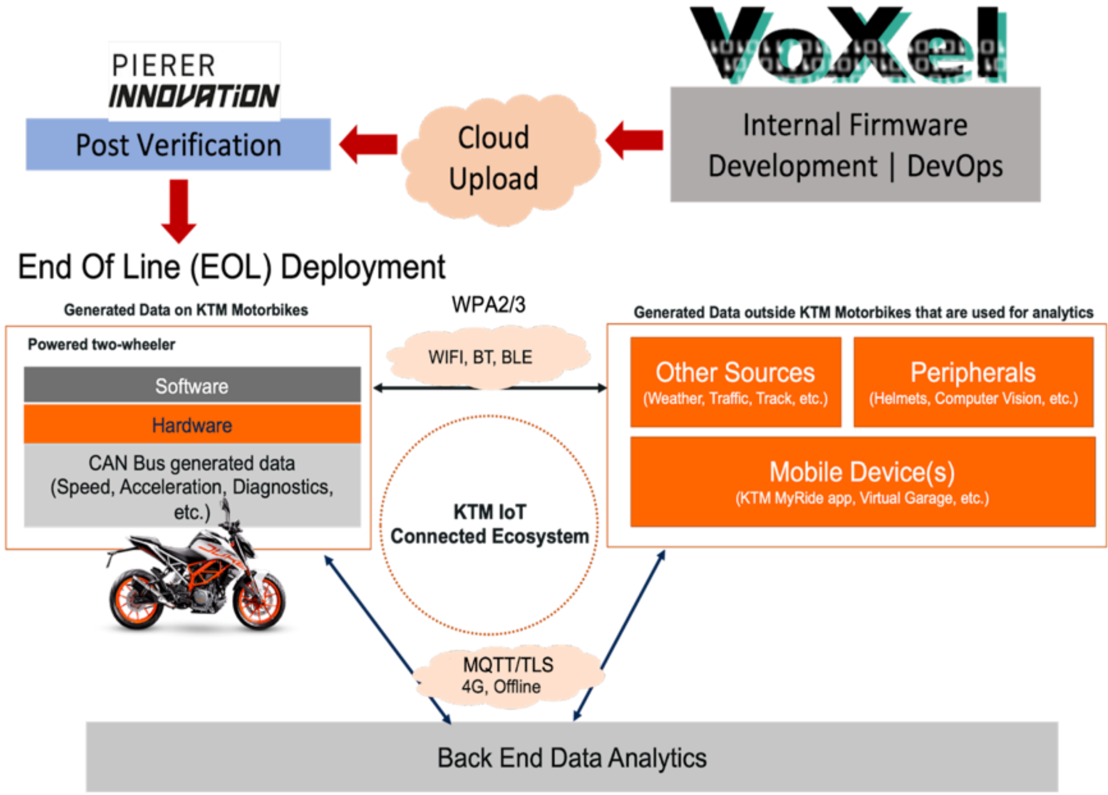
E-bicycle communication unit

Modules:

- Application processor
- RTOS
- Communication processor with LTE
- Various CAN-bus connected sensors

SecOPERA goals:

- Harden each component and the end solution
  - Application debloating
  - Leverage architectural features for security
  - Formally verify the IoT dongle
- Secure communications and data sharing



VoXel

PIERER INNOVATION

Post Verification

Cloud Upload

Internal Firmware Development | DevOps

End Of Line (EOL) Deployment

Generated Data on KTM Motorbikes

WPA2/3

Generated Data outside KTM Motorbikes that are used for analytics

Powered two-wheeler

Software

Hardware

CAN Bus generated data (Speed, Acceleration, Diagnostics, etc.)

WIFI, BT, BLE

Other Sources (Weather, Traffic, Track, etc.)

Peripherals (Helmets, Computer Vision, etc.)

Mobile Device(s) (KTM MyRide app, Virtual Garage, etc.)

KTM IoT Connected Ecosystem

MQTT/TLS 4G, Offline

Back End Data Analytics

Pilot 2
Water Management IoT Critical Infrastructure

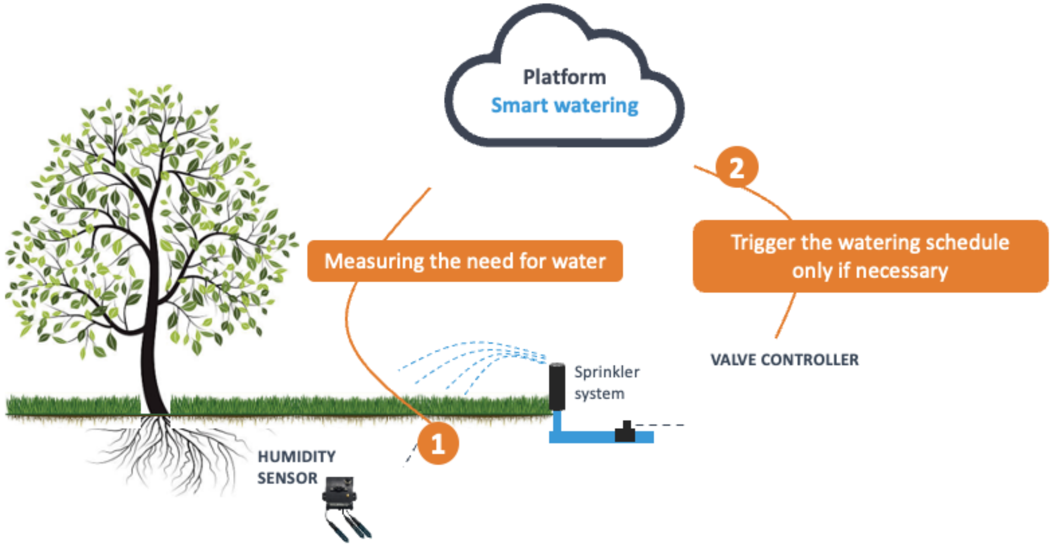
IoT solutions for water infrastructure

Ecosystem:

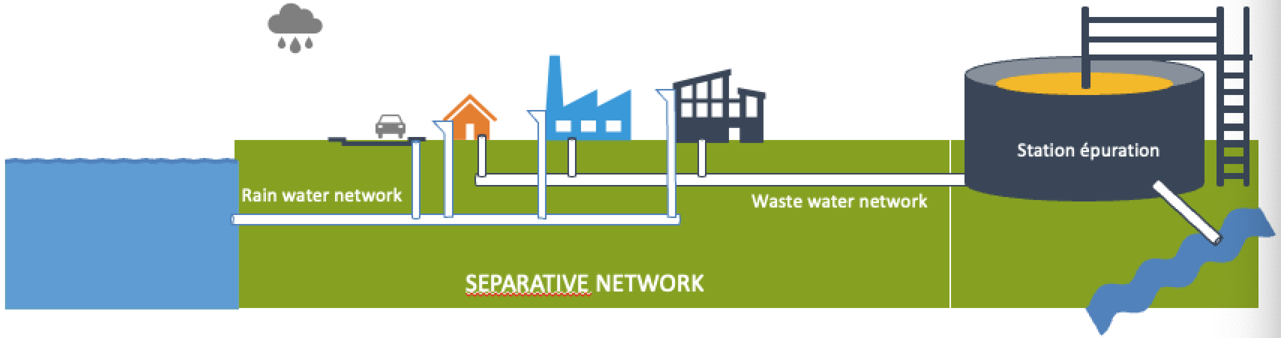
- IoT solutions for sewer, drinking irrigation
- Open-source
- Applied in smart cities

SecOPERA goals:

- Guarantee secure authentication of ecosystem administrators
  - E.g. Gardeners to start irrigation
- Secure OTA firmware updates
- Secure communication between infrastructure server and IoT devices
- Security hardened IoT components
- Deploy in real-world scenarios



Platform
Smart watering
2
Measuring the need for water
Trigger the watering schedule only if necessary
Sprinkler system
VALVE CONTROLLER
1
HUMIDITY SENSOR



Objectives related to RISC-V

- Offer Adaptable security solutions for the open-source community (SW and HW) at cognitive, network, application and **device** layers that is securely updated/patched
    - Provide more than 2 contributions to the RISC-V community regarding security.

- Assess the OSH components (e.g. RISC-V) for implementation attacks i.e. side channel attacks and fault injection attacks enhancing TVLA techniques

- SecOPERA ecosystem open-source pools will include security related RISC-V specification implementations

SecOPERA RISC-V modules

- Dynamic hardware extended containers
  - RISC-V soft SoC with dynamic reconfigurable regions
  - Debian with docker support
  - Implementation of Trusted Execution Primitives to protect dockers

- IP Core Side Channel Assessment Platform
  - Typical targets of side channel attacks are cryptography IP cores
  - Based on the Sakura X board
  - Assessment for common SCAs
    - Simple, Differential, Correlation Power Analysis on symmetric and asymmetric crypto IP cores
    - ML/DL profiling based attacks focused on Asymmetric cryptography
    - SCAs on multitenant FPGA through the exploitation of the FPGA power distribution network

- Shadow Stack and Landing Pads CVA6
  - Protects applications from Code Reuse Attacks
  - Protected Shadow Stack to store copies of return addresses
    - Compared against the regular stack before function returns in order to detect corruption
  - (Labelled) Landing Pads
    - Mark valid targets of indirect branches

Participation in RISC-V foundation

- Members of the security horizontal committee
- Participating in the Runtime Integrity Special Interest Group
- Contributing to Memory Tagging Task Group
- Chairing the Shadow Stack and Landing Pads Task Group
- Implementing the proof-of-concept SSLP extension in CVA6 processor

Collaboration opportunities

- As proposed in the previous CROSSCON
    - Consider the inclusion of CROSSCON project modules in SecOPERA pool
- Asses open-source hardware with SecOPERA assessment tools
- SecOPERA services are in a work in progress status (M18 - M30)
    - SecOPERA Security/Vulnerability Assessment and Assurance
    - Cross-layered Decomposition
    - SecOPERA Adaptation and Hardening
    - SecOPERA repositories (pools)
    - Secure Module integration

Thank you!

Learn more

https://secopera.eu/ info@secopera.eu

Follow us

company/SecOPERA @SecoperaP

SecOPERA Project zenodo /communities/secopera

This project has received funding from the European Union's Horizon Europe Research and Innovation program under grant agreement No 101070599.