SHARCS: Secure Hardware-Software Architectures for Robust Computing Systems

Sotiris Ioannidis

FORTH

Project Details

- Start date: 2015-01-01
- Duration: 36 months
- Budget: 3,105,762
- Coordinator: FORTH

- Academia
  - FORTH
  - Vrije Universiteit
  - Chalmers
  - TU Braunschweig
- Industry
  - Neurasmus BV
  - OnApp Limited
  - IBM Ltd
  - Elektrobit GMBH

Overview

- Design, build and demonstrate secure-by-design system architectures that achieve end-to-end security

- Analyze and extend each H/W and S/W layer

- Technologies developed directly utilizable by applications and services that require end-to-end security

Motivation

- Systems are as secure as their weakest link
    - Must think in terms of end-to-end security
- Security is typically applied in layers
    - Tighten up one layer and attackers move to another
- Ultimately security mechanisms must be pushed down to the H/W
    - Immutability; Clean and simple API; Secure foundation; Efficiency
- H/W on-chip resources are no longer a problem
    - Billions of transistors on-chip; Exploit parallelism and H/W
- Pushing security to the H/W
    - Benefit: performance, energy/power-efficiency; Challenge: flexibility
- Global adoption of embedded systems
    - No widely deployed security software

Objectives

1. Extend existing H/W and S/W platforms towards developing secure-by-design enabling technologies

2. Leverage H/W technology features present in today's processors and embedded devices to facilitate S/W-layer security

3. Build methods and tools for providing maximum possible security-by-design guarantees for legacy systems

4. Evaluate acceptance, effectiveness and platform independence of SHARCS technologies and processes

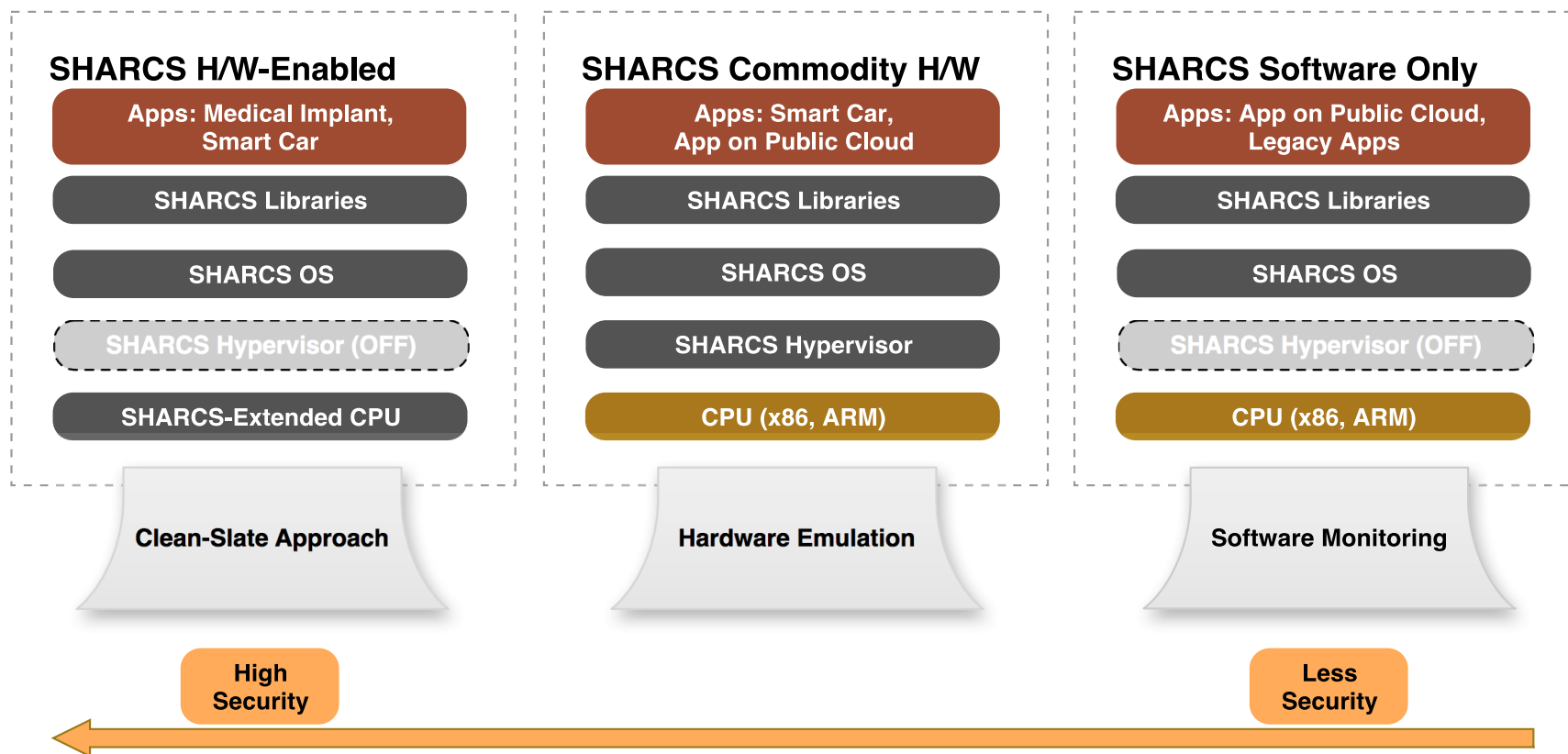5. Create high impact in the security and trustworthiness of ICT systems
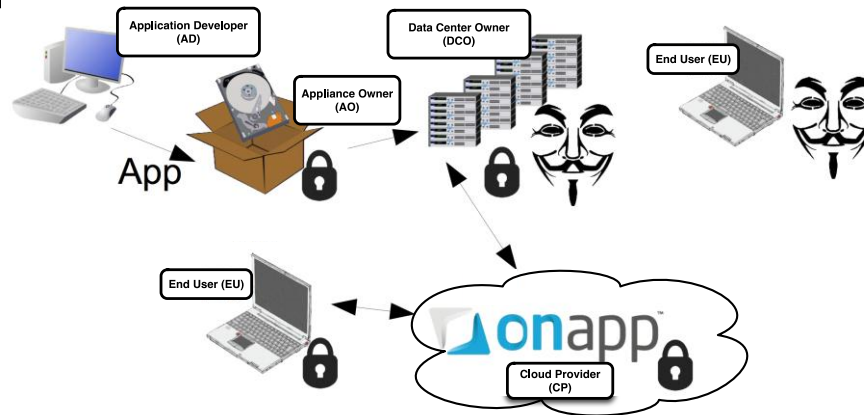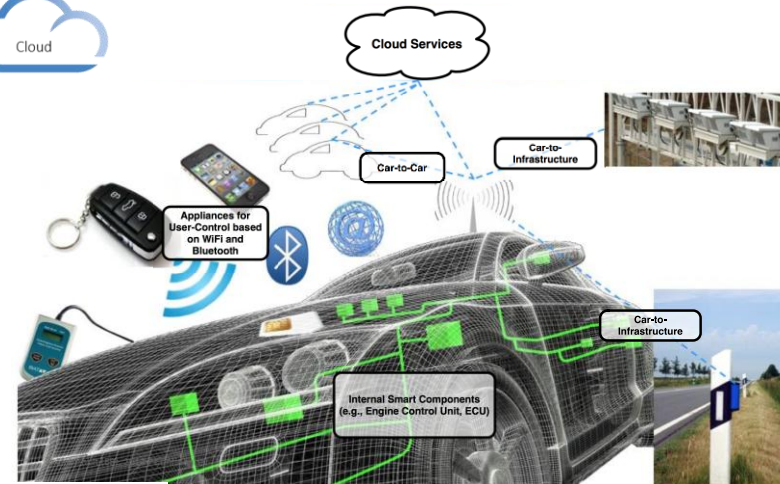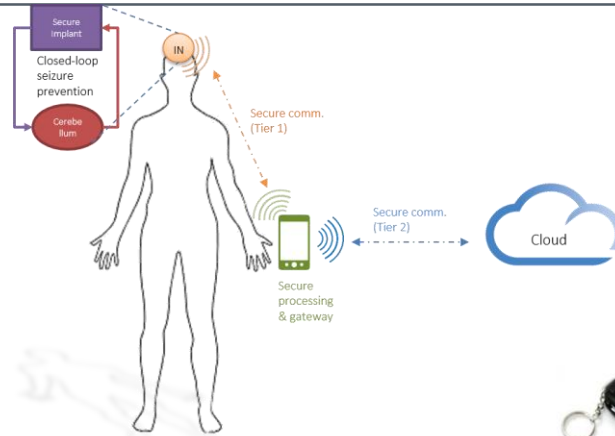
Candidate Hardware Extensions

- Instruction Set Randomization

- Control Flow Integrity

- Information Flow Tracking

- Secure H/W Memory

- Fine-grained Memory Protection
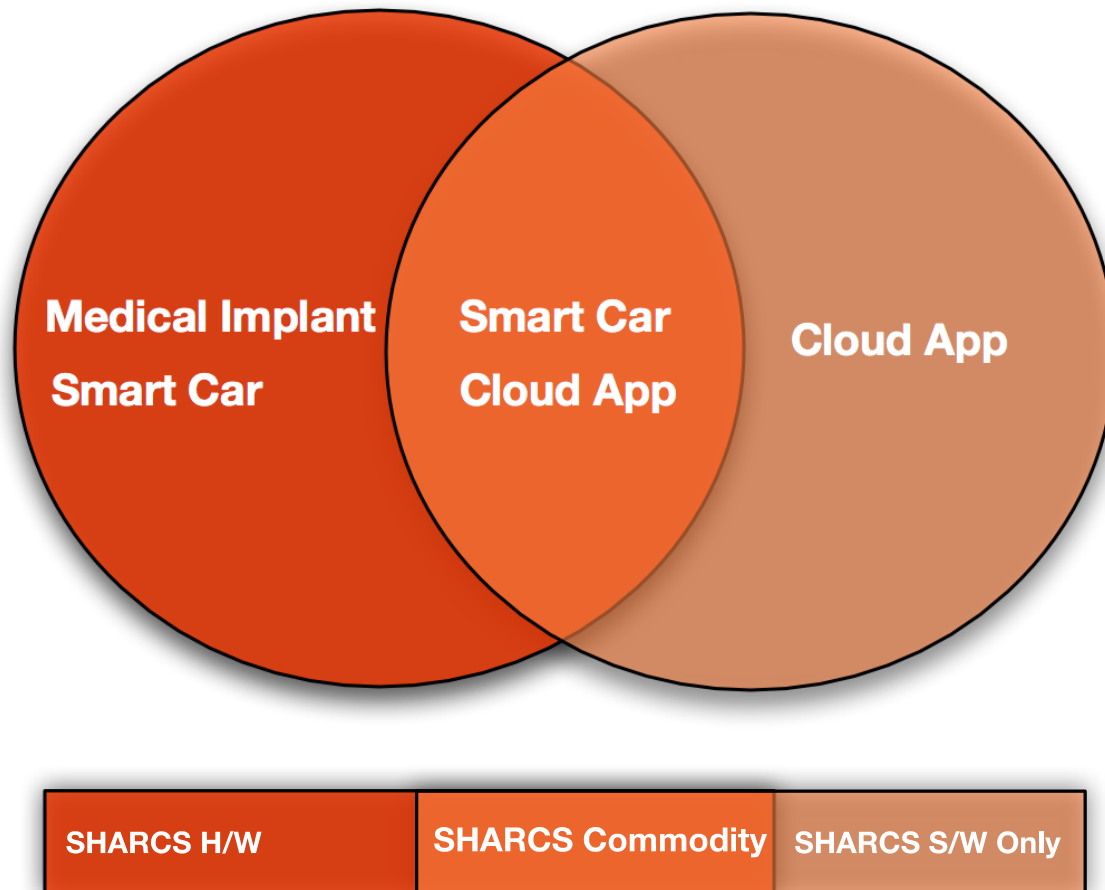
- Dynamic Type Safety

SHARCS Framework

SHARCS H/W-Enabled

Apps: Medical Implant, Smart Car
SHARCS Libraries
SHARCS OS
SHARCS Hypervisor (OFF)
SHARCS-Extended CPU

Clean-Slate Approach

SHARCS Commodity H/W

Apps: Smart Car, App on Public Cloud
SHARCS Libraries
SHARCS OS
SHARCS Hypervisor
CPU (x86, ARM)

Hardware Emulation

SHARCS Software Only

Apps: App on Public Cloud, Legacy Apps
SHARCS Libraries
SHARCS OS
SHARCS Hypervisor (OFF)
CPU (x86, ARM)

Software Monitoring

High Security

Less Security

Applications

- Medical

- Automotive

- Cloud

SHARCS Applications

Venn diagram with two overlapping circles:

Left circle: **Medical Implant** / **Smart Car**

Overlap: **Smart Car** / **Cloud App**

Right circle: **Cloud App**

Legend bar: **SHARCS H/W** | **SHARCS Commodity** | **SHARCS S/W Only**

SHARCS Methodology
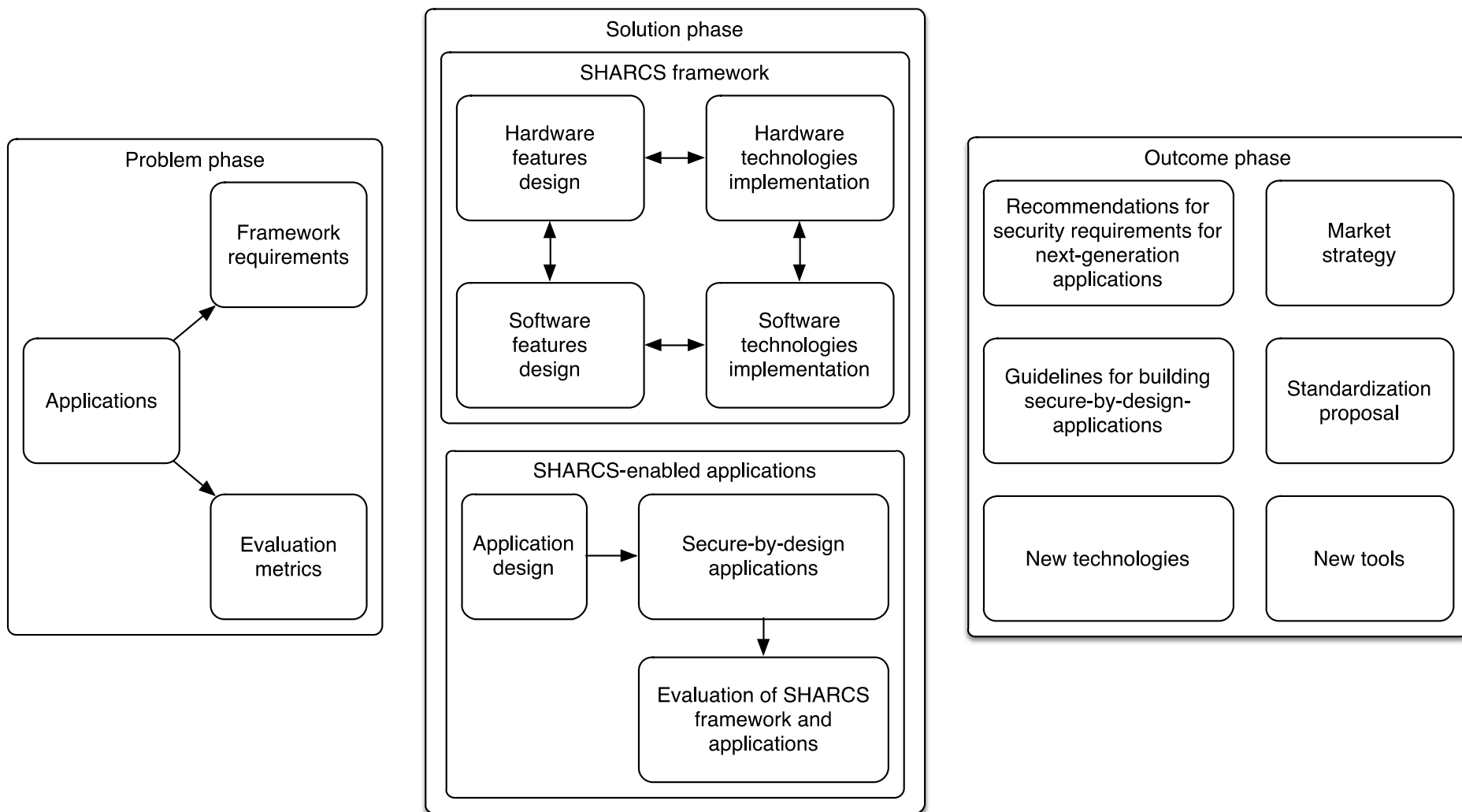
More Information

- Visit us on the web: sharcs-project.eu

- Follow us on Twitter: @sharcs_project

- Like us on Facebook: facebook.com/sharcsproject

- Email us at: sotiris@ics.forth.gr

SHARCS: Secure Hardware-Software Architectures for Robust Computing Systems

Sotiris Ioannidis

FORTH