Trusted execution architectures on light-weight embedded devices

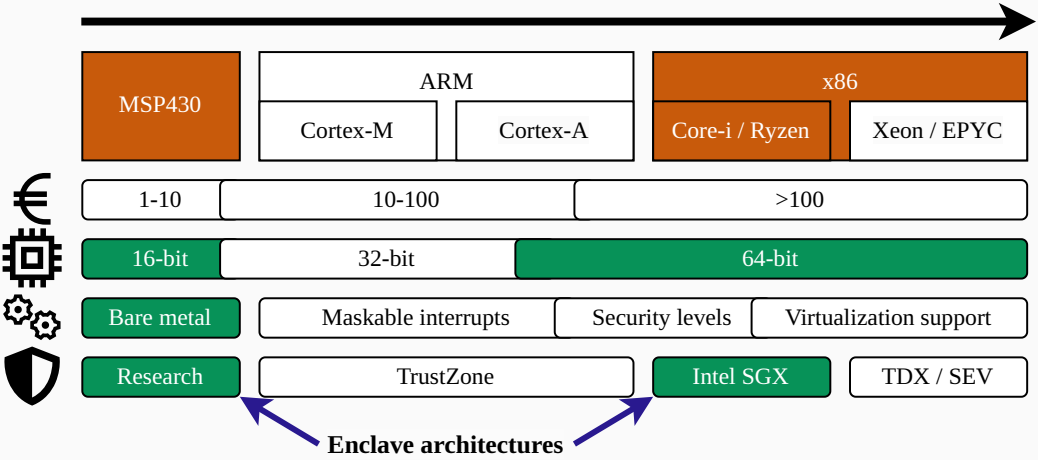
Fritz Alder

June 15, 2023

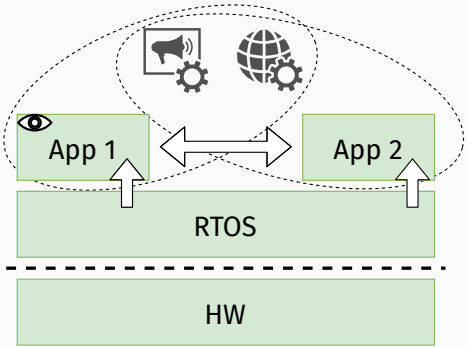
Workshop on Security, Privacy & Verifiable Computing for contemporary distributed systems

DistriNet KU LEUVEN

Processor archictectures recap



Embedded devices have a large TCB

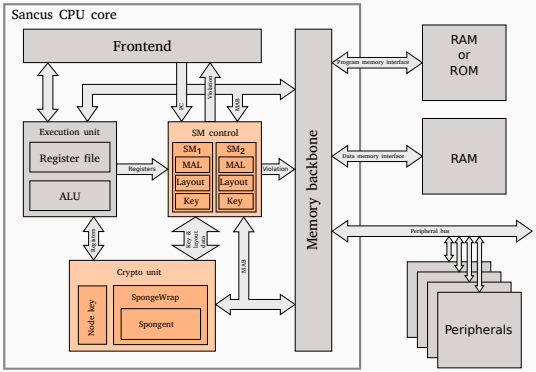


TCB for confidentiality/integrity in open system

Sancus: A Low-Cost Security Architecture for IoT devices

Extends openMSP430 with strong security primitives

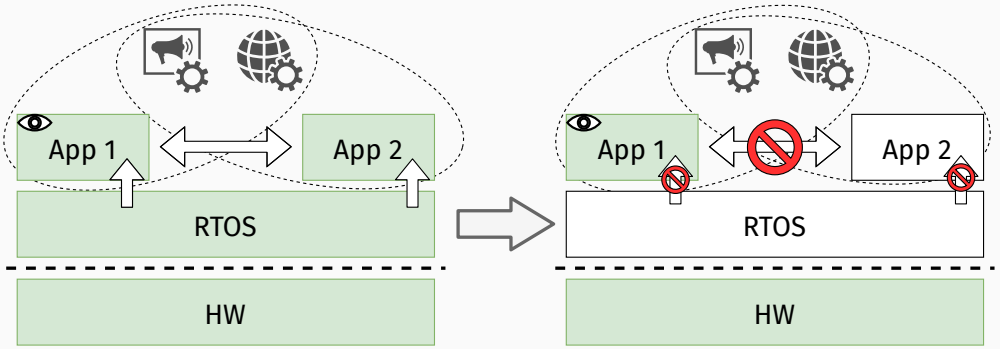
- Software Component Isolation
- Cryptography & Attestation
- Secure I/O through isolation of MMIO ranges
- Efficient, Modular, ≤ 2 kLUTs
- Cryptographic key hierarchy for software attestation
- Isolated components are typically very small (< 1kLOC)



Noorman et al. Sancus 2.0: A Low-Cost Security Architecture for IoT devices. TOPS, 2017

Sancus is open source: `https://distrinet.cs.kuleuven.be/software/sancus/`

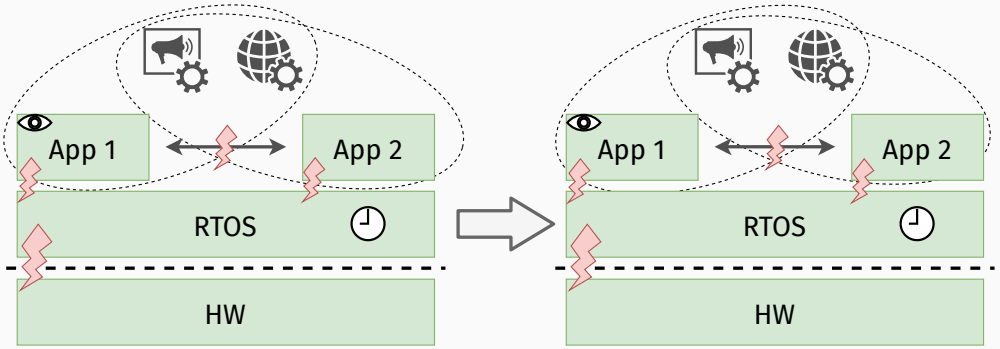
Trusted execution: Good for confidentiality and integrity



TCB for confidentiality/integrity in open system

Good spatial isolation with TEEs

Trusted execution: Not good for availability

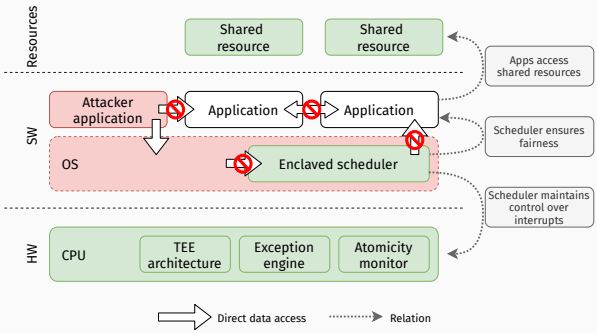


TCB for availability
in open system

No temporal isolation
with current TEEs

Aion: Strong Availability Guarantees for Enclaves

Sancus as a Starting Point



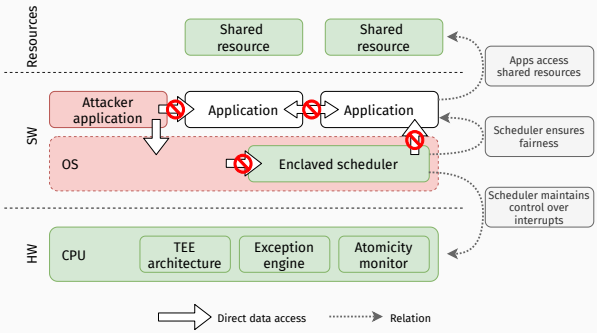
Alder et al., Aion: Enabling Open Systems through Strong Availability Guarantees for Enclaves. CCS, 2021

Aion: Strong Availability Guarantees for Enclaves

Sancus as a Starting Point

Trusted Software

- Protected Scheduler controls interrupts and scheduling decisions



Alder et al., Aion: Enabling Open Systems through Strong Availability Guarantees for Enclaves. CCS, 2021

Aion: Strong Availability Guarantees for Enclaves

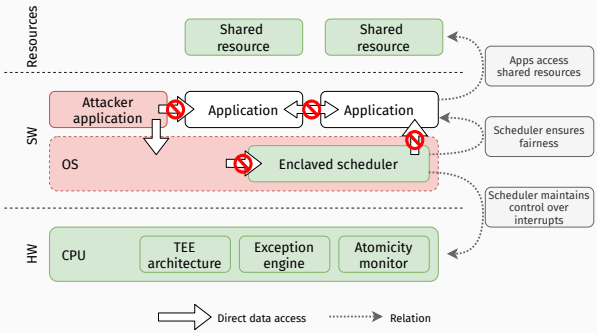
Sancus as a Starting Point

Trusted Software

- Protected Scheduler controls interrupts and scheduling decisions

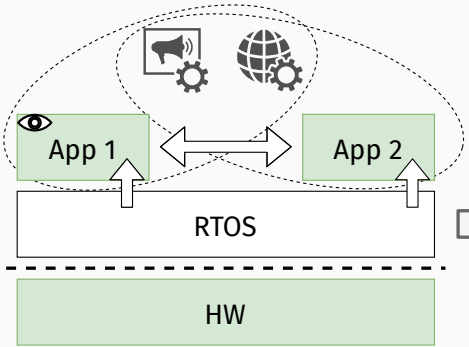
Hardware Extensions

- Exception Engine facilitates interruption of (protected) threads
- Atomicity Monitor provides control over interrupts to scheduler, guarantees bounded critical sections

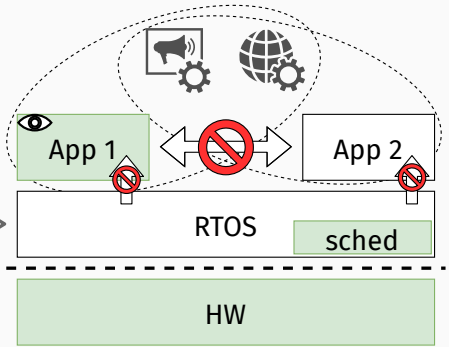


Alder et al., Aion: Enabling Open Systems through Strong Availability Guarantees for Enclaves. CCS, 2021

Result: Good spatial and temporal isolation

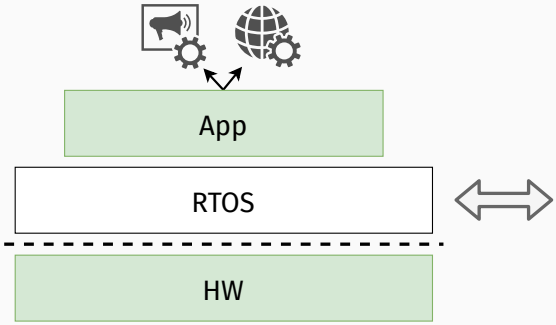


Aion system



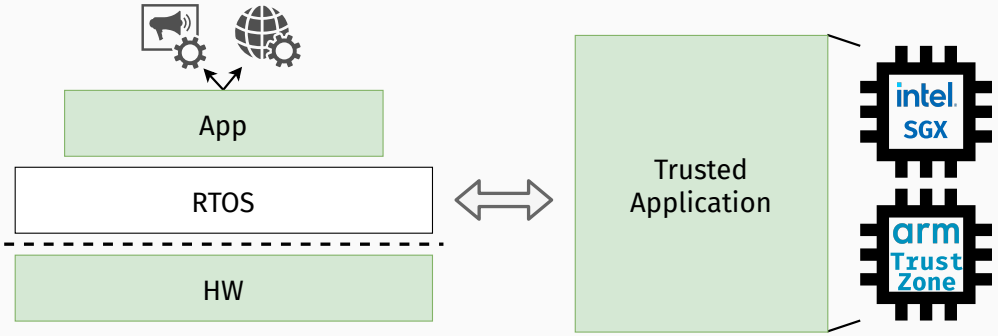
Good spatial **and temporal** isolation with Aion

To be useful, we need heterogeneity



Aion system

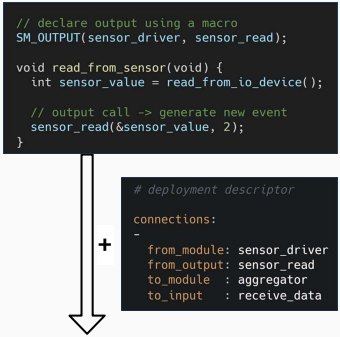
To be useful, we need heterogeneity



Authentic Execution of Event-Driven Applications

Open source framework to connect heterogeneous TEEs

- Mutual attestation
- Encrypted communication
- Minimal code to connect nodes

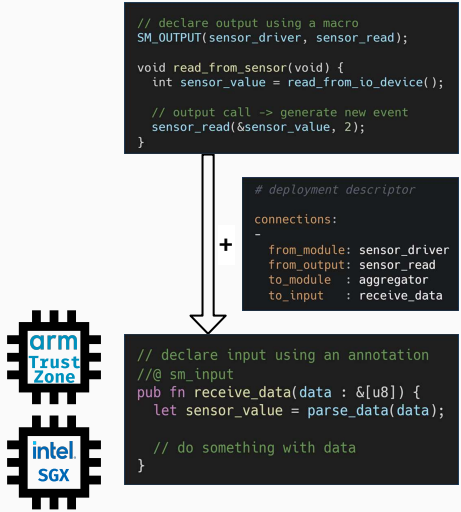


Scopelliti et al., End-to-End Security for Distributed Event-Driven Enclave Applications on Heterogeneous TEEs, TOPS 2023

Authentic Execution of Event-Driven Applications

Open source framework to connect heterogeneous TEEs

- Mutual attestation
- Encrypted communication
- Minimal code to connect nodes
- Supports Sancus, Intel SGX, ARM TrustZone (OP-TEE)
- Output is only generated if relevant input has been received



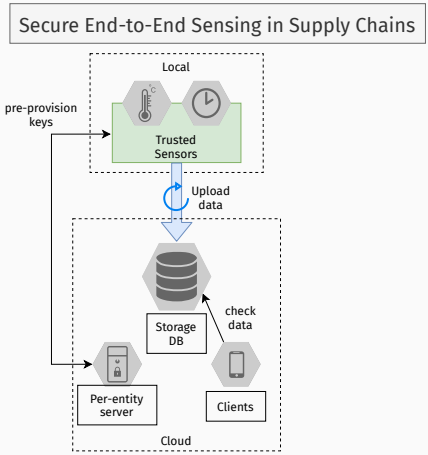
Scopelliti et al., End-to-End Security for Distributed Event-Driven Enclave Applications on Heterogeneous TEEs, TOPS 2023

Example use case: Modern Supply Chains

Trust between supply chain stakeholders is often non-existent:

- Faulty shipments may be hidden
- Accountability is low

Trusted sensors can help . . .



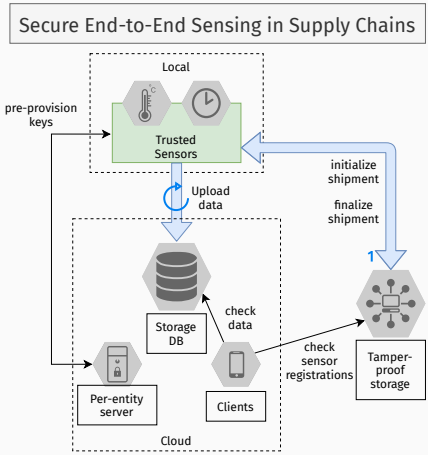
Pennekamp et al., Secure End-to-End Sensing in Supply Chains, CPS-Sec 2020

Example use case: Modern Supply Chains

Trust between supply chain stakeholders is often non-existent:

- Faulty shipments may be hidden
- Accountability is low

Trusted sensors can help . . .
but require additional elements like a tamperproof storage.



Pennekamp et al., Secure End-to-End Sensing in Supply Chains, CPS-Sec 2020