TrustGW : protecting IoT gateways against software and communication threats

Guillaume Hiet

guillaume.hiet@centralesupelec.fr

CentraleSupélec, IRISA, CIDRE Inria Project-Team

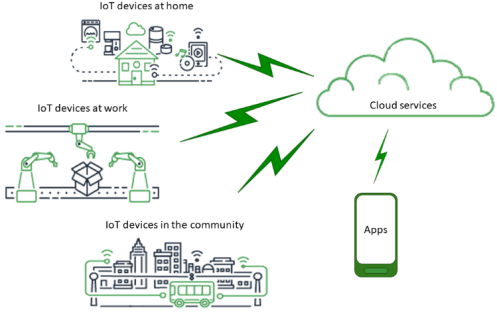
11 May 2023

Context of the TrustGW project

Cyber-security is a major concern

- Sophisticated attacks target many vulnerable systems
- Strongly connected to underground economy and military/intelligence activities

A new type of target: embedded communication systems (e.g., IoT)



- Increasingly widespread in critical infrastructures
- They handle sensitive data
- They increase the global attack surface of information systems

Context of the TrustGW project

Cyber-security is a major concern

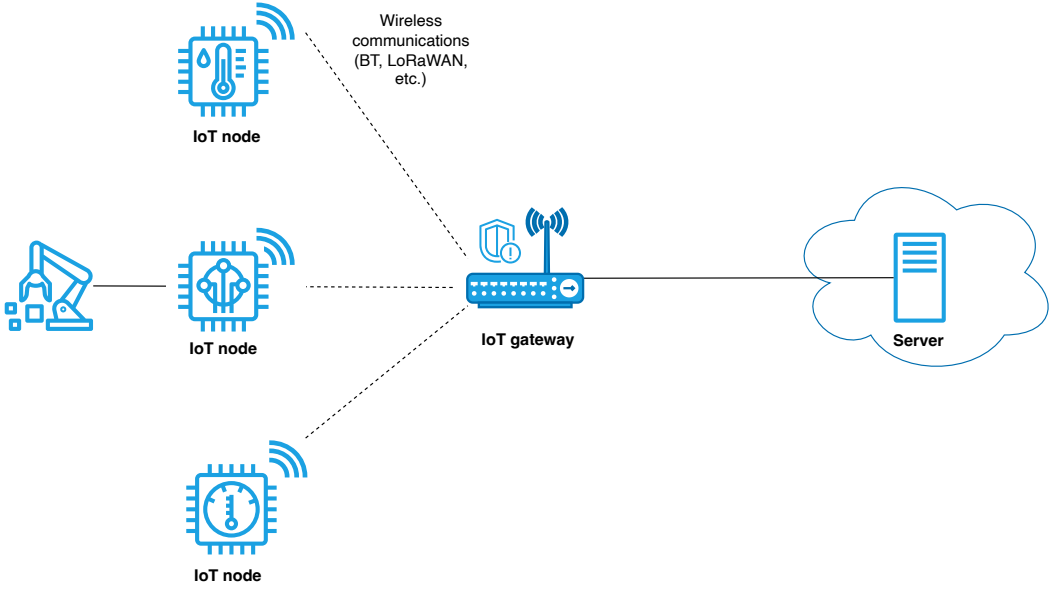
- Sophisticated attacks target many vulnerable systems
- Strongly connected to underground economy and military/intelligence activities

A new type of target: embedded communication systems (e.g., IoT)

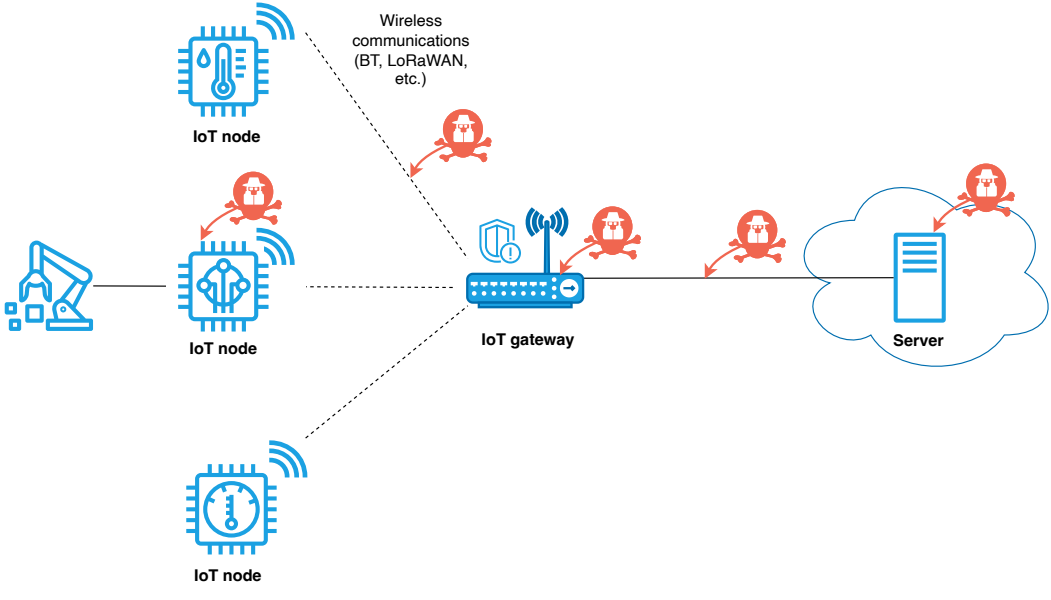
We must guarantee the best level of security for such systems

- Increasingly widespread in critical infrastructures
- They handle sensitive data
- They increase the global attack surface of information systems

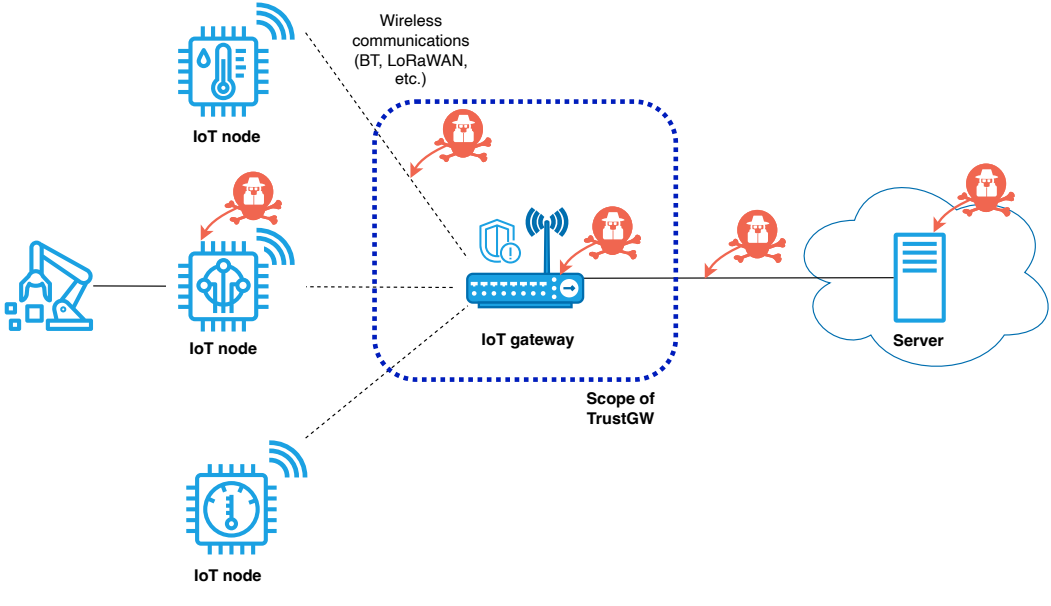
Threats against IoT architecture



Threats against IoT architecture



Threats against IoT architecture



TrustGW research project

Goal

Developing a dynamically reconfigurable and trusted heterogeneous software-hardware IoT gateway architecture

General information

- Started in January 2022. Duration: 44 months
- Funding (ANR): 3 Ph.D. students + travels

Partners

- IRISA - CIDRE group (CentraleSupelec/Inria, Rennes)
- IETR - SYSCOM group (INSA, Rennes)
- Lab-STICC - ARCAD group (Univ. of South Brittany, Lorient, and Brest)

Assumptions and scientific challenges

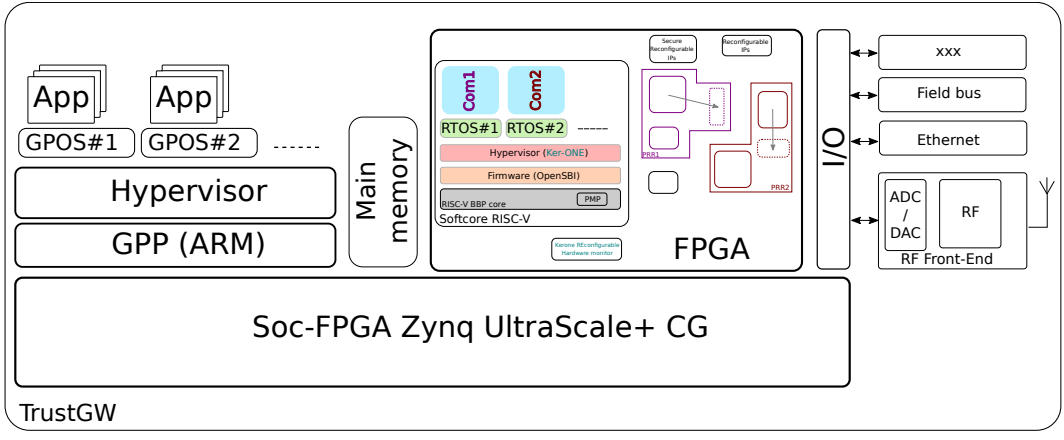
Assumptions

- The gateway is connected to IoT devices using different wireless technologies (BT, LoRaWAN)
- Different tenants share the gateway
- The gateway relies on a heterogeneous architecture (different CPU + hardware accelerators on FPGA)

Challenges

- Designing a trusted heterogeneous hardware/software architecture with dynamic reconfiguration capabilities to **protect wireless communications**
- Developing a trusted hypervisor to **share all hardware resources** (including FPGA) and **isolate** the different applications
- **Protecting** edge-computing **hybrids applications** from software attacks

General architecture



Threat model

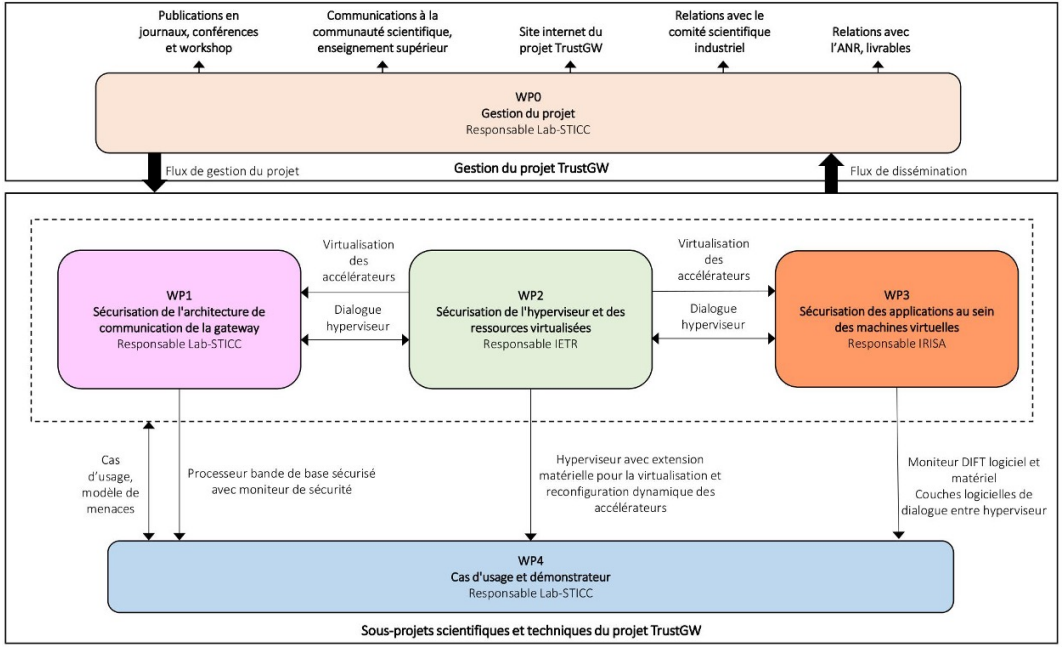
Software attacks

- Malicious contents send through the (wireless) network interfaces
- Exploit a vulnerability in the software executed on the BBP or the GPP
- Target the edge-computing applications or the radio communications
- Software side-channels (e.g., microarchitectural attacks) are not considered in the scope of this project

Hardware attacks

- E.g., fault injections, side-channels
- Not considered in the scope of TrustGW

General organisation of the project



Use-cases and edge-computing applications

Device monitoring

- Monitoring events from smart sensors to detect malfunctions (e.g., predictive maintenance)
- FPGA-accelerated runtime verification of specifications written in TeSSLa[1]

Machine Learning application

- Using ML to classify event traces
- Deploying the inferred model on FPGA to accelerate the classification

Cryptographic application

- Providing cryptographic primitives (signature, encryption) to protect application data
- Offloading part of the computation on FPGA

[1] `https://www.tessla.io/`

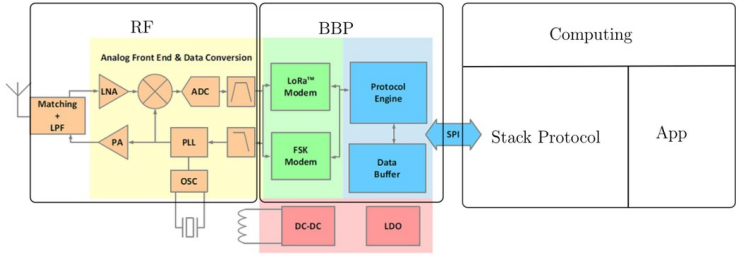
WP1 - Securing the gateway's communication architecture

T1.1 - Designing a secure baseband processor (BBP)

- Add dedicated instructions to a RISC-V processor for Software Defined Radio implementations
- Rely on PMP and virtualization extensions to isolate different wireless technologies

T1.2 - Monitoring wireless communication to detect intrusions

- NIDS executed on the BBP to detect attacks targeting the wireless protocols



WP2 - Secure hypervisor for FPGA accelerators virtualization

T2.1 - Hypervisor-based isolation of hardware ressources

- Modification of Xvisor[2] to virtualize FPGA resources
- Isolation of FPGA accelerators using an IOMMU-inspired mechanism
- Development of specific isolated VMs to manage the system

T2.2 - Handling partial reconfiguration

- Designing a specific service, executed in an isolated VM, to handle partial reconfiguration and secure deployment of FPGA accelerators
- Designing communication mechanisms between accelerators and a secure sharing mechanism of FPGA accelerators

[2] https://xhypervisor.org/

WP3 - Securing edge-computing applications

T3.1 - Hardware-assisted Dynamic Information Flow Tracking for software

- Porting our previous work to monitor applications using a dedicated co-processor (implemented on FPGA)
- Rely on DIFT to detect violations of confidentiality and integrity within edge-computing applications

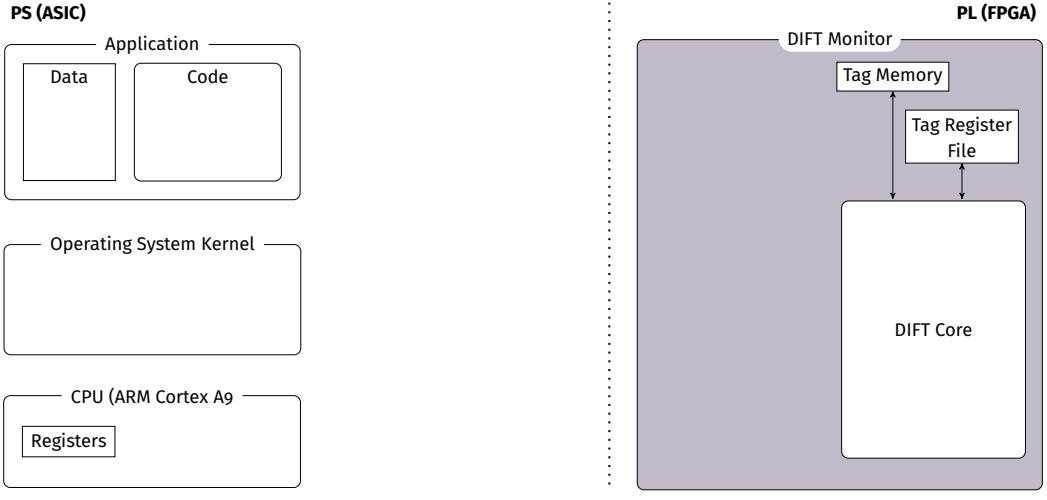
T3.2 - DIFT for hybrid applications

- Modify the previous approach to monitor hybrid applications, i.e., applications that offload part of their computations on FPGA

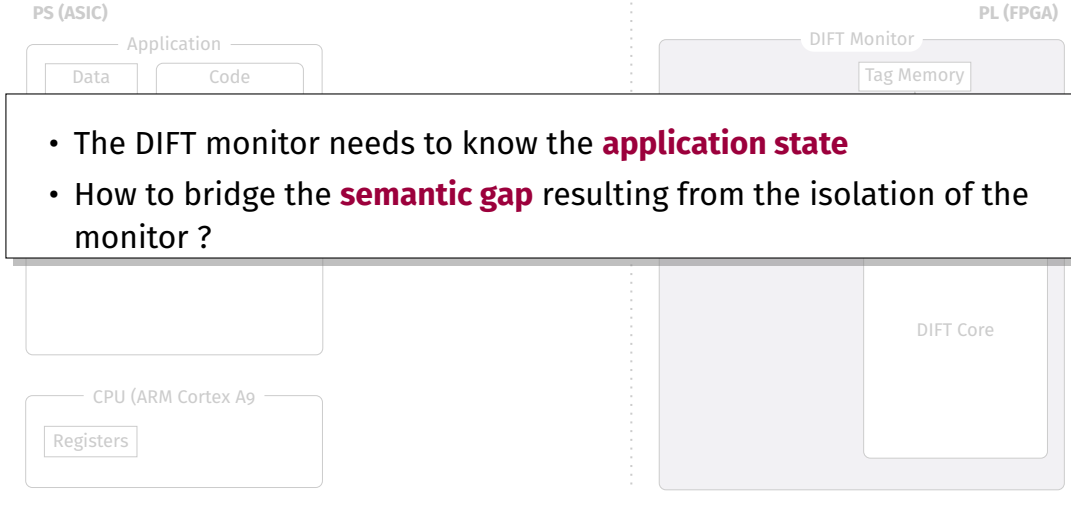
T3.3 - Monitoring the OS

- Implement an isolated monitor within the hypervisor to detect intrusion targeting the guest OSes
- Bridge the semantic gap using a dedicated introspection language

Hardware-assisted DIFT

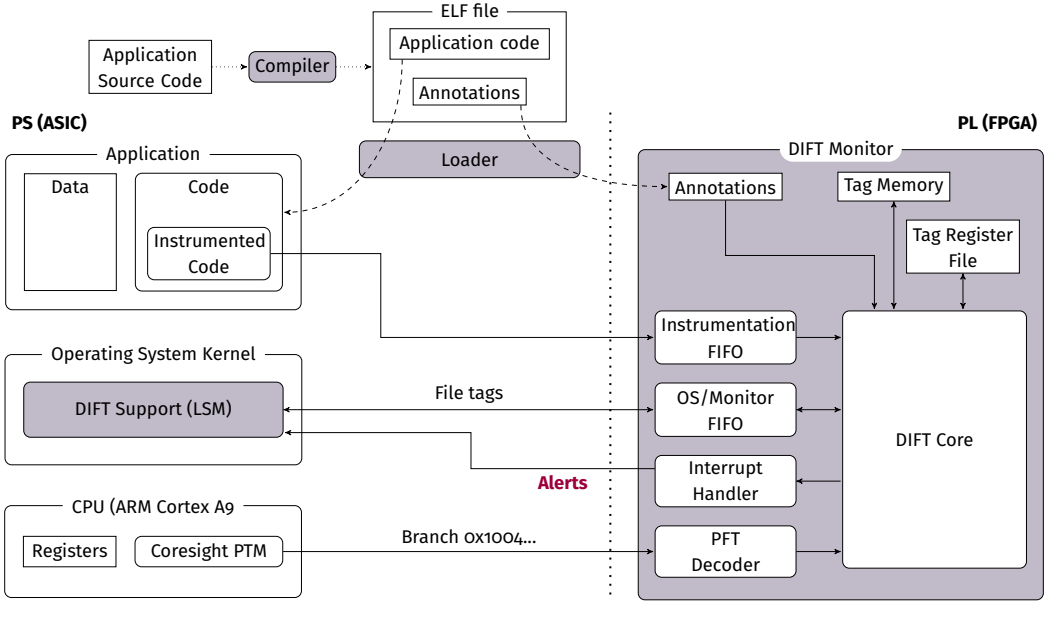


Hardware-assisted DIFT

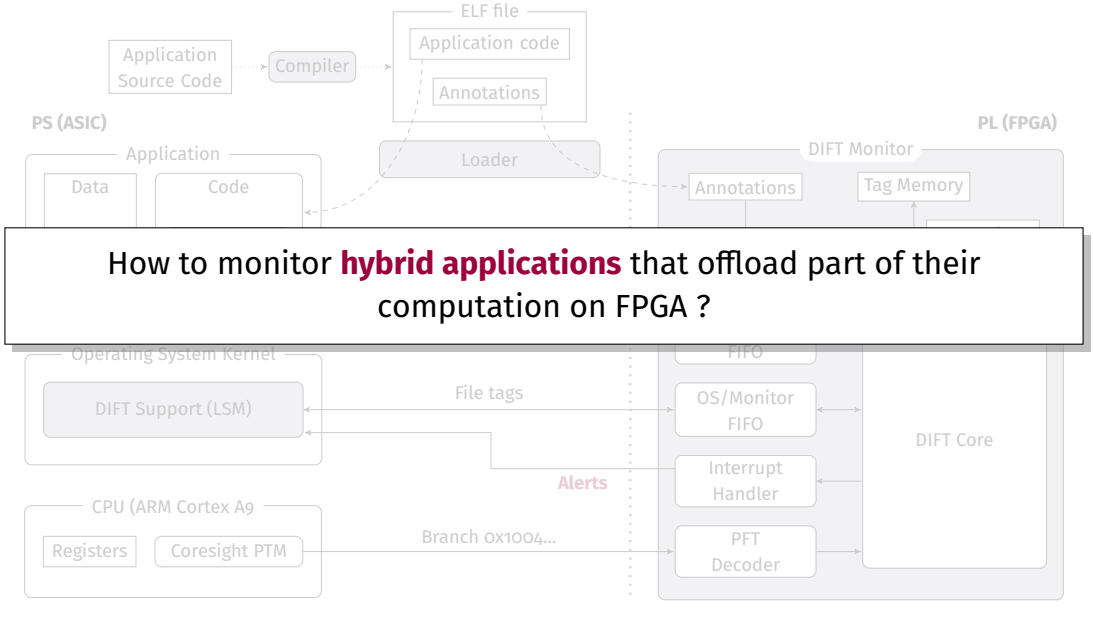


- The DIFT monitor needs to know the **application state**
- How to bridge the **semantic gap** resulting from the isolation of the monitor ?

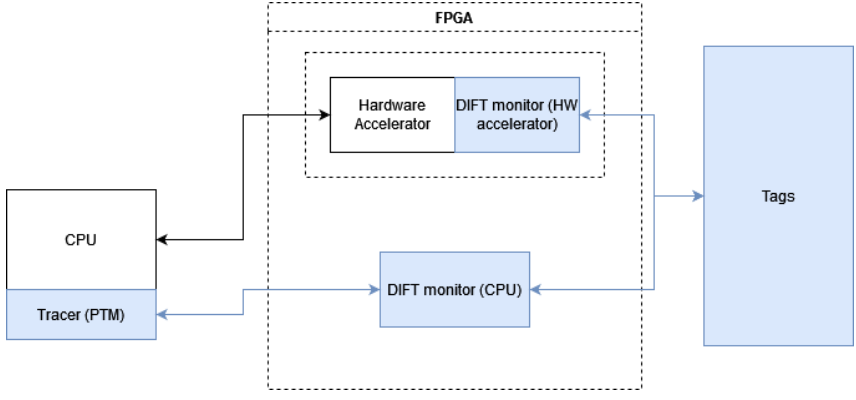
Hardware-assisted DIFT



Hardware-assisted DIFT

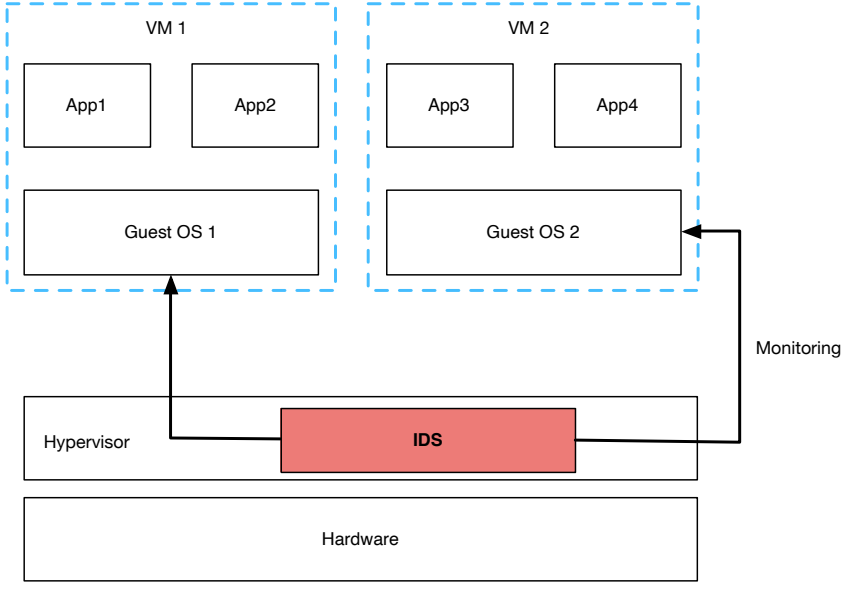


Monitoring Hybrid Applications : Ideal Design

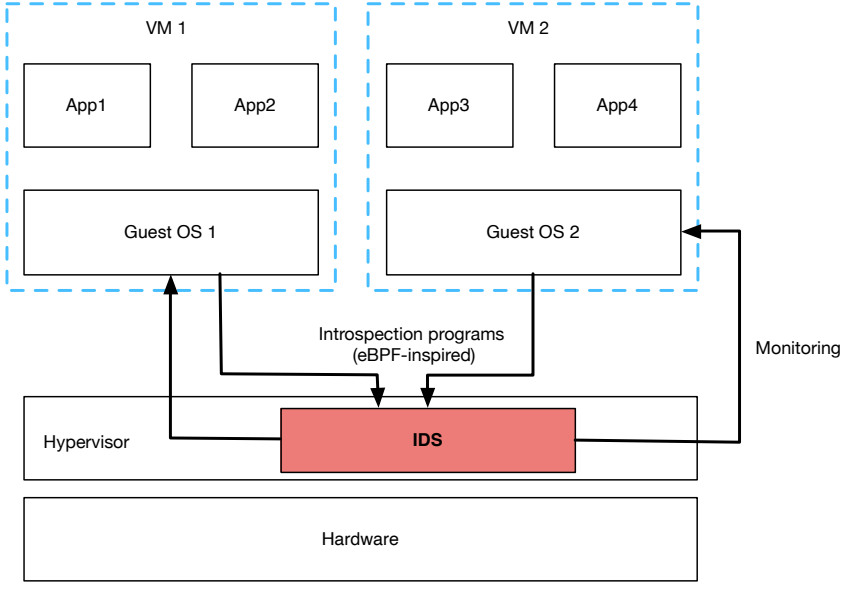


- Preliminary work realized by Romain Ninot and Oumar Niang (master students)
- We are recruiting (master-level internship, possibly Ph.D. position)

Hypervisor-level IDS (Ph.D. of Lionnel Hemmerlé)



Hypervisor-level IDS (Ph.D. of Lionnel Hemmerlé)



Questions?

https:\trustgw.projects.labsticc.fr