HardBlare, a hardware/software co-design approach for Information Flow Control

Guillaume Hiet and partners

November 18, 2019

HardBlare project

General information

- Started in October 2015. Duration: 3 years (some works are still ongoing)
- Funding: 2 PhD students and 1 PostDoc

Partners

- CentraleSupélec, IETR (SCEE) @ Rennes
  - Pascal Cotret (Ass. Prof.) now at ENSTA Bretagne
  - Muhammad Abdul Wahab (PhD student) now R&D engineer at Ultraflux
- CentraleSupélec/Inria, IRISA (CIDRE) @ Rennes
  - Guillaume Hiet (Ass. Prof.)
  - Mounir Nasr Allah (PhD student)
- UBS, Lab-STICC @ Lorient
  - Guy Gogniat (Full Prof.), Vianney Lapôtre (Ass. Prof.)
  - Arnab Kumar Biswas (Postdoc) now research Fellow at NUS

Context

Cyber-security is a major concern

- Many vulnerable systems are targeted by sophisticated attacks

A new type of target: **embedded systems**

- IoT, Industrial Control Systems, Cyber-Physical Systems, etc.
- We target **Systems using rich OS** (Linux, Android, etc.) and powerful **application processors** (e.g. ARM Cortex A family)
  - Smartphones/tablets, smart watches, set-top boxes, business printers, military devices (Android Tactical Assault Kit), etc.

How to secure embedded systems?

- Preventive approaches (avoiding vulnerabilities) are insufficient
- It is also important to **monitor** systems to **detect intrusions at runtime**

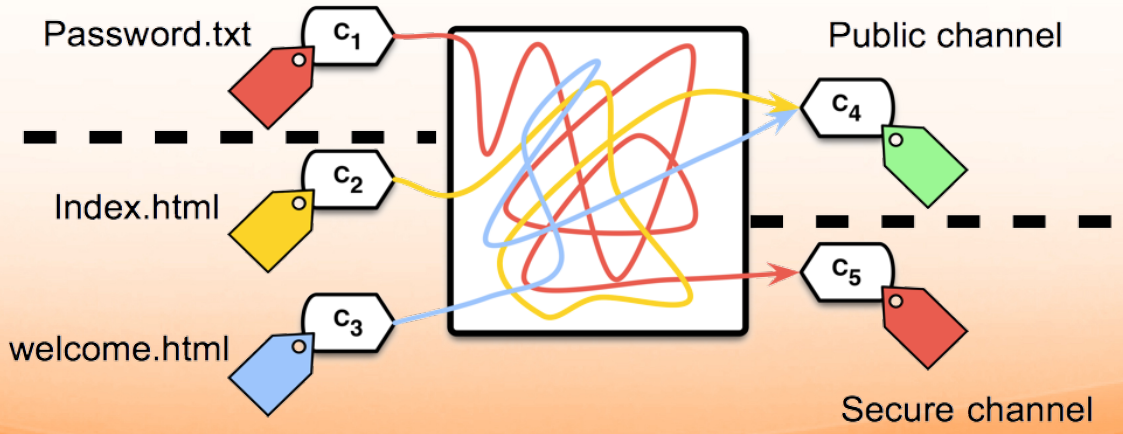
Dynamic Information Flow Tracking

Motivation

A generic approach to detect attacks against confidentiality and integrity at different levels

DIFT principle

- We attach **labels** called tags to **containers** and specify an information flow **policy**, i.e. relations between tags
- At runtime, we **propagate** tags to reflect information flows that occur and **detect** any **policy violation**



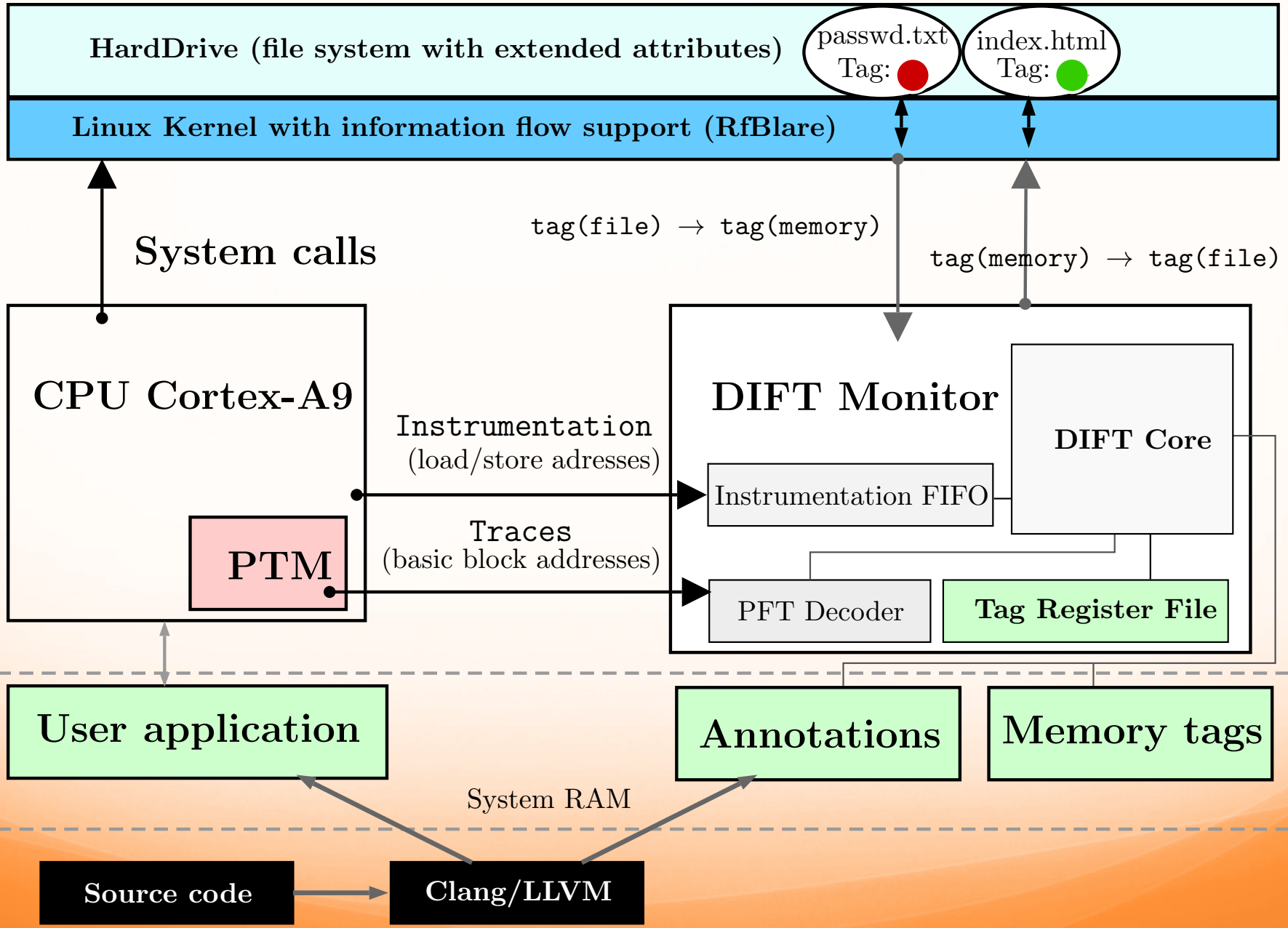
Originality of our approach

- **Combines hardware/software for fine-grained DIFT with OS-level tagging** to associate labels to registers, memory and files
  - Helps the end-user to specify the security policy
  - Saves the security contexts between reboots
- Implements tag propagation in an **external co-processor** to isolate the monitor with **no modification of the main CPU**
- Solves the semantic-gap issue by an original combination of approaches:
  - pre-computing of **annotations** during the compilation of applications
  - sending of branching information using **hardware trace mechanisms**
  - sending of addresses of read/write accesses using **instrumentation** of the application code
- Implementation and evaluation of the approach on a Xilinx ZYNQ SoC (ARM Cortex A9 + FPGA) executing a dedicated Yocto Linux distribution

Threat model

- We target software attacks that directly modify the values of containers (files, registers, memory)
- We do no handle physical attacks (e.g. fault injection using laser or physical side-channel attacks)
- We only monitor applications
  - OS kernel is part of our TCB
  - We could reduce the TCB to the kernel code that manages file tags and communicates with the co-processor

General Overview

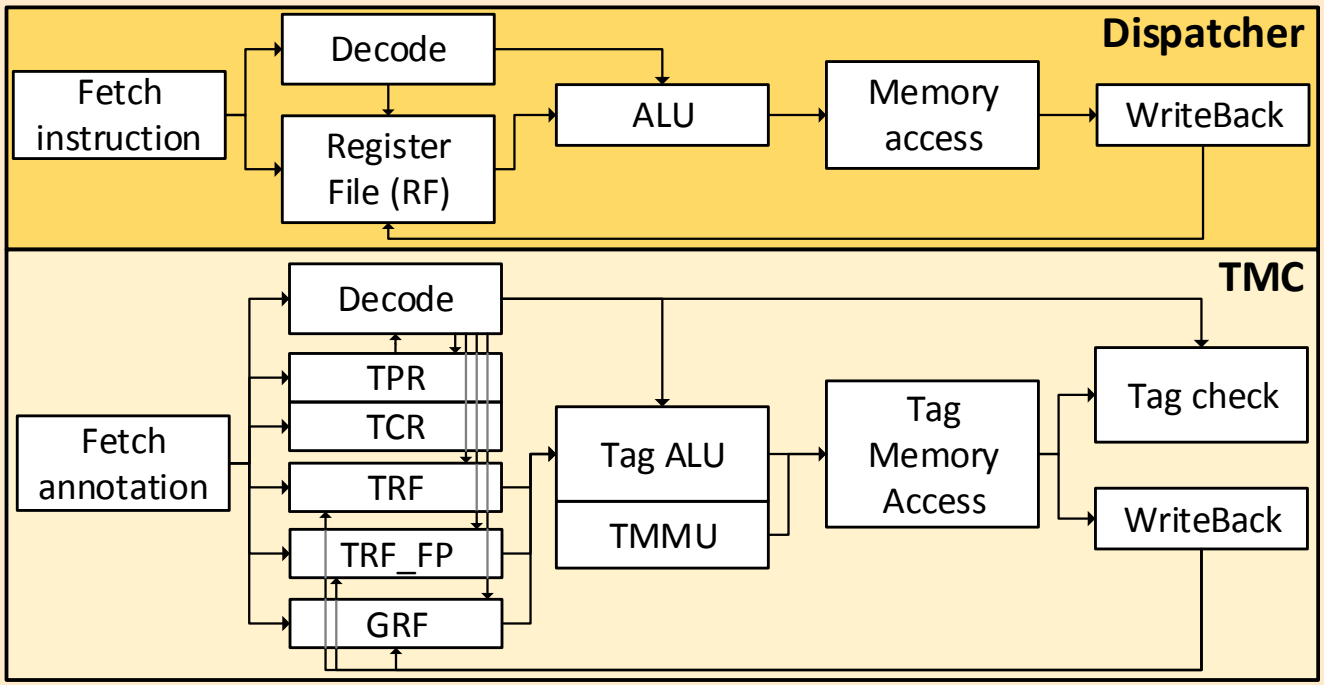


Key contributions

Software

- Modification of the Linux kernel and loader
- Patch of the official Linux kernel PTM driver (now included in the official vanilla Linux kernel distribution)
- LLVM backend pass

Hardware : dedicated multi-core DIFT co-processor in VHDL



Results

	Without OS support			With OS support	
Approaches	**Kannan et al.**	**Deng et al.**	**Heo et al.**	**Heo et al. adapted**	**HardBlare**
Area overhead	6.4%	14.8%	14.47%	N/A	**0.95%**
Power overhead	N/A	**6.3%**	24%	N/A	16.2%
Max frequency	N/A	**256 MHz**	N/A	N/A	250 MHz
Communication time overhead	N/A	N/A	60%	1280%	**335%**
Hardcore portability	No	No	**Yes**	**Yes**	**Yes**
Main CPU	Softcore	Softcore	Softcore	**Hardcore**	**Hardcore**
Library instrumentation	N/A	N/A	partial	**Yes**	**Yes**
FP support	No	No	No	No	**Yes**
Multi-threaded support	No	No	No	No	**Yes**

Publications

- **International conferences with proceedings (3 + 1 short paper)**
  - Abdul Wahab et al.: *A small and adaptive coprocessor for information flow tracking in ARM SoCs*, ReConFig2018
  - Abdul Wahab et al.: *A novel lightweight hardware-assisted static instrumentation approach for ARM SoC using debug components*, AsianHOST2018
  - Abdul Wahab et al.: *ARMHEx: A hardware extension for DIFT on ARM-based SoCs*, FPL2017
  - Abdul Wahab et al.: *Towards a hardware-assisted information flow tracking ecosystem for ARM processors (short paper)*, FPL2016
- **International technical conferences (3)**
  - HITBSecConf 2017, 34th Chaos Communication Congress 2017, Toulouse Hacking Convention 2018
- **National conferences and workshops (4)**
  - France/Japan Cybersecurity workshop 2016, CryptArchi2016, 11ème Colloque National du GDR SoC/SiP, RESSI2017
- **Posters (2)**
  - CHES 2015, séminaire doctorants SIF 2016

External collaborations

PhD Internship

- 6 months internship of Mounir at ARM Cambridge with Alastair Reid (07/2017 to 01/2018)
  - Model checking of the formal specification of ARM Cortex M processors to verify IFC properties
- 3 months internship of Muhammad at ALaRI Lugano with Alberto Ferrante (01/2018 to 03/2018)
  - Explore how trace mechanisms and FPGA of the ZYNQ SoC can be used to accelerate malware detection

Presentation to industrial partners

- ARM research (Cambridge, UK), HP Labs (Bristol, UK), Secure-IC (Rennes, France), IBM OpenPower team (Rochester, USA)

Future collaborations

- Submission to an AURORA project proposal with Norvegian researchers from HVL, who are interested by our approach.

Perspectives

- Reduction of the TCB, implementing isolation of kernel parts using TrustZone
- Reduction of instrumentation overhead (by optimizing the static analysis)
- Implementation of multicore and multi-thread DIFT (by using multiple TMCs)
- Porting of the approach to other platforms (e.g. Intel PT)
- Taking benefit of dynamic partial reconfiguration of FPGA to increase co-processor flexibility

ComInLabs

HardBlare, a hardware/software co-design approach for Information Flow Control

Guillaume Hiet and partners

November 18, 2019

CentraleSupélec

ENSTA BRETAGNE

Inria

Université Bretagne Sud
ubs

IETR
INSTITUT D'ÉLECTRONIQUE ET DE TÉLÉCOMMUNICATIONS DE RENNES

UMR IRISA

Lab-STICC