HardBlare: a Hardware-Assisted Approach for Dynamic Information Flow Tracking
Mounir Nasr Allah, Guillaume Hiet, Muhammad Abdul Wahab, Pascal Cotret, Guy Gogniat, Vianney Lapotre

To cite this version:
HardBlare: a Hardware-Assisted Approach for Dynamic Information Flow Tracking

Mounir Nasr Allah \(^a\), Guillaume Hiet \(^a\), Muhammad Abdul Wahab \(^b\), Pascal Cotret \(^b\), Guy Gogniat \(^\gamma\), Vianney Lapôtre \(^\gamma\)

\(^a\) CIDRE / IRISA / INRIA, CentraleSupélec, Cesson-Sévigné - FRANCE
\(^b\) SCEE / IETR, CentraleSupélec, Cesson-Sévigné - FRANCE
\(^\gamma\) Lab-STICC, University of South Brittany, Lorient - FRANCE

Introduction

HardBlare proposes a software/hardware codesign methodology to ensure that security properties are preserved all along the execution of the system but also during files storage. The general context is to address Dynamic Information Flow Tracking (DIFT) that generally consists in attaching marks (also known as tags) to denote the type of information that are saved or generated within the system.

Let’s suppose that “print” function is public and the tag of a variable \(x\) is underlined variable \(\hat{x}\).

### Example code

```
\(p = 3;\) 
\(s = 42;\) 
\(x = p + s;\) 
```

```java
if (\(x\) != public) 
    raise interruption
```

### Tag propagation

<table>
<thead>
<tr>
<th>p</th>
<th>Tag initialization</th>
<th>Tag propagation</th>
<th>Tag check</th>
</tr>
</thead>
<tbody>
<tr>
<td>= p ← public</td>
<td>= s</td>
<td>= s + s</td>
<td>if ((x) != public) raise interruption</td>
</tr>
</tbody>
</table>

State of the art

#### Advantages

- Flexible security policies
- Multiple attacks detected
- Low overhead (<10%)
- Invasive modifications
- Few security policies
- Fixed security policies
- Security policies not modified
- Communication between CPU and DIFT Coprocessor
- Low overhead (<10%)
- Binary code not modified

#### Disadvantages

- Overhead
- (from 300% to 3700%)
- Invasive modifications
- Wasting resources
- Energy consumption (x 2)
- Coprocessor

Static Analysis

- During the compilation phase, a static analysis is done on the LLVM intermediate representation produced from the source code, and propagated to the ARM backend for the machine code generation.
- The result of static analysis gives a list of dependencies between information containers (e.g. registers, memory spaces...) for every basic blocks which are stored on a dedicated section in a ELF File.
- During run-time, the Program Trace Macrocell (PTM) generates a trace containing the address for each committed instruction modifying the PC value.
- Annotations related to the basic block identified by its address, given by the trace, are processed by the coprocessor to propagate tags.

### ARM Cortex-A9 Trace mode: Coresight components

**Definitions**
- Tag dependencies block contains annotations loaded when the program is launched.
- Memory tags block contains tags related to information containers.
- Tag register file contains tags related to CPU registers.

**DIFT step-by-step**
- ARM CoreSight Components export trace (for both CPUs) towards PL in PFT (Program Flow Trace) protocol.
- PFT Decoder decodes trace in usable format
- Using decoded trace, DIFT Coprocessor reads tags dependencies block.
- DIFT Coprocessor looks for the tags either in memory or tag register file.
- DIFT Coprocessor computes tags depending on propagation rules.
- DIFT Coprocessor updates corresponding tags.
- DIFT Coprocessor checks for security policy violation and raise an interruption

Main Contributions at a Glance

- Hardware-assisted DIFT system with limited time overheads.
- Approach based on a non-modified CPU with a standard Linux and generic binaries.
- Could be implemented by industrial partners in medium-term.
- Hardened with hardware security mechanisms: trusted coprocessor storage and bus protection in terms of confidentiality/integrity.
- Contributions on software-related issues as well (static/dynamic IFC analysis, i.e. hybrid analysis).
- Perspectives on runtime reconfiguration and multicores/manycore systems.

Some References


