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:

HAL Id: hal-01311032
https://hal-centralesupelec.archives-ouvertes.fr/hal-01311032
Submitted on 23 Jun 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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.

Example code

```plaintext
p = 3;
q = 42;
x = p + s;
print(x);
```

Table:

<table>
<thead>
<tr>
<th>Example code</th>
<th>Tag initialization</th>
<th>Tag propagation</th>
<th>Tag check</th>
</tr>
</thead>
<tbody>
<tr>
<td>p = 3;</td>
<td>p ← public</td>
<td></td>
<td></td>
</tr>
<tr>
<td>q = 42;</td>
<td>s ← secret</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x = p + s;</td>
<td>x ← p + s;</td>
<td>if (x != public)</td>
<td>raise interruption</td>
</tr>
</tbody>
</table>

Introduction

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.

State of the art

<table>
<thead>
<tr>
<th>Hybrid</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIFT Coprocessor</td>
<td>Flexible security policies</td>
<td>Overhead (from 300% to 3700%)</td>
</tr>
<tr>
<td>In-core DIFT</td>
<td>Low overhead (&lt;10%)</td>
<td>Invasive modifications</td>
</tr>
<tr>
<td>Dedicated CPU for DIFT</td>
<td>Low overhead (&lt;10%)</td>
<td>Wasteing resources</td>
</tr>
<tr>
<td>Low overhead (&lt;10%)</td>
<td>Communication between CPU and DIFT</td>
<td></td>
</tr>
</tbody>
</table>

Static Analysis

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 (Program Flow Trace) protocol.
  - PFT Decoder decodes trace in usable format.
  - Using decoded trace, DIFT Coprocessor reads tag dependencies block.
  - DIFT Coprocessor checks for security policy violation and raise an interruption.

Some References

[6] Mounir Nasr Allah α, Guillaume Hiet α, Muhammad Abdul Wahab β, Pascal Cotret β, Guy Gogniat γ, Vianney Lapōtre γ

Advanced by

- 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/multicore systems.