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: a Hardware-Assisted Approach for Dynamic Information Flow Tracking

Mounir Nasr Allah α, Guillaume Hiet α, Muhammad Abdul Wahab β, Pascal Cotret β, Guy Gogniat γ, Vianney Lapôtre γ

α CIDRE / IRISA / INRIA, CentraleSupélec, Cesson-Sévigné - FRANCE
β SCEE / IETR, CentraleSupélec, Cesson-Sévigné - FRANCE
γ Lab-STICC, University of South Brittany, Lorient - FRANCE

Tag initialization

s

p

Tag propagation
←
if (x ←
←

p = 3;

x = p + s;
n = 42;

←
= public

x ←
←

⇒

print(x);

{

\[ x = \text{open}("password.txt"); \]
\[ y = \text{open}("host.txt"); \]

if (user = root) {
    read x, buffer;
    also {
        read p, buffer;
    }
    write buffer, socket;
}

State of the art

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
<td><strong>Hardware</strong></td>
</tr>
<tr>
<td>Flexible security policies</td>
<td>Low overhead (&lt;10%)</td>
</tr>
<tr>
<td>Multiple attacks detected</td>
<td>Fixed Security policies</td>
</tr>
<tr>
<td><strong>In-core DIFT</strong></td>
<td>Low overhead (&lt;10%)</td>
</tr>
<tr>
<td>Few security policies</td>
<td>Invasive modifications</td>
</tr>
<tr>
<td><strong>Dedicated CPU for DIFT</strong></td>
<td>Low overhead (&lt;10%)</td>
</tr>
<tr>
<td>Few modifications to CPU</td>
<td>Wasting resources</td>
</tr>
<tr>
<td><strong>Dedicated DIFT Coprocessor</strong></td>
<td>Low overhead (&lt;10%)</td>
</tr>
<tr>
<td>Flexible security policies</td>
<td>Communication between CPU and DIFT</td>
</tr>
<tr>
<td>CPU not modified</td>
<td>Coprocessor</td>
</tr>
</tbody>
</table>

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 block 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.

Introduction

HardBlare proposes a software/hardware co-design 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 underline variable x.

Example code

<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>n = 42;</td>
<td>s ← secret</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x = p + s;</td>
<td>x ← p + 5 = 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>print(x);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>