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

Dedicated CPU for DIFT

- Low overhead (<10%) 
- Few security policies 
- Few modifications to CPU 
- Energy consumption (<2)

Dedicated DIFT Coprocessor

- Low overhead (<10%) 
- CPU not modified 
- Communication between CPU and DIFT 
- Coprocessor

Advantages | Disadvantages
--- | ---
Flexible security policies | Overhead (from 300% to 3700%)
Multiple attacks detected | Invasive modifications
Low overhead (<10%) | Fixed security policies
Few security policies | Invasive modifications
Low overhead (<10%) | Wasting resources
Few modifications to CPU | Energy consumption (<x 2)
Low overhead (<10%) | Coprocessor
Flexible security policies | Communication

State of the art

Hybrid

- Hardware-Assisted DIFT system with limited time overheads.
- Flexible security policies
- Low overhead (<10%)
- Few invasive modifications
- In-core DIFT
- Dedicated CPU for DIFT
- Communication between CPU and DIFT
- Coprocessor