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 as tags) to denote the type of information that are saved or generated within the system. 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.

\[ x = s \]

\[ p = 3; \]
\[ s = 42; \]
\[ p + s = s; \]
\[ x = p + s; \]
\[ x = p + s; \]
\[ print(x); \]

\[ if (x != public) \]
\[ raise interruption \]

### Example code

<table>
<thead>
<tr>
<th>Tag initialization</th>
<th>Tag propagation</th>
<th>Tag check</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p = 3 )</td>
<td>( p \leftarrow \text{public} )</td>
<td></td>
</tr>
<tr>
<td>( s = 42 )</td>
<td>( s \leftarrow \text{secret} )</td>
<td></td>
</tr>
<tr>
<td>( x = p + s )</td>
<td>( x \leftarrow p + s = s )</td>
<td>if ( (x != \text{public}) ) raise interruption</td>
</tr>
</tbody>
</table>