Runtime Code Polymorphism as a Protection against Physical Attacks
Damien Couroussé, Bruno Robisson, Thierno Barry, P Jaillon, O Potin

To cite this version:

HAL Id: emse-01232662
https://hal-emse.ccsd.cnrs.fr/emse-01232662
Submitted on 23 Nov 2015

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.
Core Idea: Runtime Code Polymorphism

Definition
Regularly changing the behaviour of a (secured) component, at runtime, while maintaining unchanged its functional properties

What for?
- Protection against reverse engineering of SW
  - the secured code is not available before runtime
  - the secured code regularly changes its form (code generation interval $\omega \geq 1$)
- Protection against physical attacks
  - polymorphism changes the spatial and temporal properties of the secured code: side channel & fault attacks
  - combine with usual SW protections against focused attacks

How?
- deGoal: runtime code generation for embedded systems
  - fast code generation
  - tiny memory footprint: proof of concept on TI’s MSP430 (512 bytes of RAM)

Compilettes & deGoal in a Nutshell

Polyorphic Code Generation

deGoal runtime capabilities
Performed in this order:
- register selection
- instruction selection
- instruction scheduling

Adaptation to achieve runtime code polymorphism:
- Portability to very small processors and secure elements
  - Limited memory consumption
  - Fast runtime code generation
  - Ability to combine with hardware countermeasures
  - Introduce alea during runtime code generation [1,2,3]
- Polymorphism:
  - random mapping to physical registers [1]
  - use of semantic equivalences [2]
  - instruction scheduling [3]
  - insertion of dummy operations [3]

The deGoal framework builds compilettes
A compilette is:
- an ad hoc code generator that targets one kernel
- aimed to be invoked at runtime

Example: polymorphic AES

Polymorphic implementation of the SubBytes function:
```c
void gen_subBytes( cdg_insn_t* code, uint8_t* state_addr)
{ #
  Begin code Prelude
  Type uint32 state, sbox, i, x, y
  #
  state, #(@state_addr)
  sbox, #(@sbox_addr)
  i, #(0)
  loop:
    lb x, #(@state+i) // x := state[i]
    lb y, #(@sbox+x) // y := sbox[x]
    sb @(@state+i), y // state[i] := y
    add i, i, #1)
    beq loop, i, #16)
  rtn
}
End
#
```

Execution times (in cycles), over 1000 runs:

<table>
<thead>
<tr>
<th>Reference</th>
<th>min</th>
<th>max</th>
<th>average</th>
</tr>
</thead>
<tbody>
<tr>
<td>code generator</td>
<td>6385</td>
<td>6385</td>
<td>6385</td>
</tr>
<tr>
<td>polymorphic instance</td>
<td>7185</td>
<td>9745</td>
<td>8303</td>
</tr>
</tbody>
</table>

Impact of the code generation interval $\omega$:

$$k \cdot \text{overhead vs. reference implementation} = \% \cdot \text{percentage contribution of runtime code generation to the performance overhead}$$

References