Compilation for the Composition of Software Protections for Embedded Systems
Thierno Barry, Damien Couroussé, Bruno Robisson

To cite this version:

Thierno Barry, Damien Couroussé, Bruno Robisson. Compilation for the Composition of Software Protections for Embedded Systems. 5ème édition de la rencontre Crypto’Puce, May 2015, Île de Porquerolles, France. cea-01273410

HAL Id: cea-01273410
https://hal-cea.archives-ouvertes.fr/cea-01273410
Submitted on 13 Feb 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.
Compilation for the composition of software protections for embedded systems

Thierno Barry

Damien Couroussé

Bruno Robisson

1CEA – LIST / DACLE
2CEA / DPACA

Firstname.LASTNAME@cea.fr

Crypto’Puce 2015

Porquerolles Tuesday, May 5, 2015
- Automatic control (centralized and distributed)
- Middleware and communication
- Compilation and code generation
- Methods and tools: design flow for HW/SW integration
- Hardware security
Nowadays, embedded systems have increasingly become critical part of our daily life

One of the major threats against these systems are physical attacks

There are two main categories

1. Side channel attacks
   Observing physical quantities of the device during operation

2. Fault attacks
   Injecting a fault in order to disrupt the normal functioning of the device
Objective

- Proposing a tool for composing several software protections against physical attacks

- Through a compilation toolchain

- Our work involves two disciplines:
  1. Physical security
  2. Compilation

also called: Compilation for security
- Existing countermeasures against physical attacks
  - Concluding remarks

- Our approach

- A safari inside a compiler
  - why compilation + security is not obvious?

- Why operating inside a compiler?

- First results

- Outlook
**EXISTING COUNTERMEASURES**

---

### Side Channel Attacks

- Work because there is a correlation between the operations being processed and some observable physical quantities.

- The objective of countermeasures is: Operations → Physical quantities

- Two concepts:

  1. **Masking**

     Concealing each intermediate value \( v \) by a random value \( m \) such as: \( v_m = v \oplus m \)

     - \( v_m = v \oplus m \) → Boolean
     - \( v_m = v + m \) → Modular addition
     - \( v_m = v \times m \) → Modular multiplication

  2. **Hiding**

     - Software
       - Insertion of dummy instructions
       - Instructions shuffling

     - Hardware
       - Randomize the power consumption
       - Equalize the power consumption
Fault Attacks

- Based on fault models where an attacker can:
  - Skip an instruction
  - Replace an instruction with another one
  - Corrupt data being transferred from/to memory

- Proposed countermeasures are:
  - Instructions redundancy
  - Control flow hardening
  - CRC / Parity Check / ...
Concluding

We notice two approaches for applying countermeasures

1. At the source code level

Problems:

- None of security properties applied to the source code are guaranteed after the compilation

- Except if all the compiler code optimizers are disabled as suggested in [Eldib et al. 2014]

- Leads to very high execution overheads: $\Rightarrow + 400\%$ in [Lalande et al. 2014]
EXISTING COUNTERMEASURES

Concluding

2 At Assembly level

Problems:
- Lack of visibility program context ➔ Overheads ++
- Often ad-hoc [Barenghi et al., 2010]

Assembly approach
A countermeasure is designed to protect against one single attack

[Regazzoni et al. 2008] and [Luo et al. 2014] have shown that a code protected against Fault attacks may increase the power leakage and then become more vulnerable to power analysis attacks

How to take into account several threats inside a countermeasure?
Our Approach

Source code

Compilation + security

Secure binary code

Composition of several protections

Binary code protected against several attacks
Existing countermeasures against physical attacks
  - Concluding remarks

Our approach

A safari inside a compiler
  - why compilation + security is not obvious?

Why operating inside a compiler?

First results

Outlook
What is a compiler?

- The source code passes through several transformations and representation before the Machine code.
- Each one is suitable for some kind of tasks of the compiler.
- Modern compilers are structured in 3 phases:
  - Front end
  - Middle end
  - Back end
Front end

If \((x > 0)\) {
    return a+b;
}

Source code

Reads the source code and splits it into a list of tokens e.g.:

\[
\text{if} \ (x > 0) \ {\text{\{}} \\
\text{Return} \ a + b; \ {\text{\}}}
\]

Take the list of tokens, built the AST \(\Rightarrow\) check the validity of the syntax

Simplified LLVM-IR

\[
\ldots \\
\text{\%cmp = icmp sgt i32 \%x, 0} \\
\text{br i1 \%cmp, label \%if.then, \ldots}
\]

\%
if.then:
\%add = add nsw i32 \%a, \%b
\text{store i32 \%add, i32* \%retval}
\text{br label \%return}
\]

\ldots
Middle end

- Takes as input the Intermediate representation
- The IR is supposed to be language and target independent

A countermeasure applied at the middle end remain valid for all languages and targets supported by the compiler
**Middle end**

- The majority of code optimizer are applied at *middle end*
- Among them we have:
  - Global Value Numbering (GVN)
  - Dead Code Elimination (DCE)
  - Dead Store Elimination (DSE)

```c
int x = 0;
int y = f(x);
for(int i=1; i<= 100; i++)
  if(i > 0)
    x = x + 1;
else
  x = x - 1;
y = f(x)
```

```c
int x = 0;
int y = f(x);
for(int i=1; i<= 100; i++)
  x = x + 1;
y = f(x)
```

```c
int x = 0;
int y = f(x);
for(int i=1; i<= 100; i++)
  x = x + 1;
y = f(x)
```

```c
int y = f(100);
```

```c
int y = f(0);
int x = 100;
y = f(x)
```
Middle end

- Loop Invariant Code Motion (LICM)
- LOOP-UNROLLING / LOOP UNSWITCH

```c
bool flag;
for(int i=7; i*i< 1000; i++){
    flag = verdict(1);
    if(flag == true)
        foo();
    else
        bar();
}
```

```c
bool flag = verdict(1);
if(flag == true)
    for(int i=0; i<25; i++)
        foo();
else
    for(int i=0; i<25; i++)
        bar();
```

```
bool flag = verdict(1);
for(int i=0; i<25; i++){
    if(flag == true)
        foo();
    else
        bar();
}
```

31*31 = 961
32*32 = 1024
⇒ i = [7-32] ⇒ [0-25]
Back end

Takes the IR as input

- Instructions selections
  - Convert the IR to a representation close to the target architecture

- Register allocation
  - Find the best way to assign physical registers to variables in order to reduce register pressure and avoid memory spills

- Instruction scheduling
  - Rearrange instructions to obtain the best execution order in order to avoid stalls inside the pipeline

- Machine code emission
  - Emit executable code that is target-specific
## Compilation vs. Security

<table>
<thead>
<tr>
<th><strong>Goal</strong></th>
<th><strong>Compilation</strong></th>
<th><strong>Security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How?</strong></td>
<td>Generation of executable code for a target architecture</td>
<td>Safety</td>
</tr>
<tr>
<td></td>
<td>Making the execution as fast as possible</td>
<td>Resistance against attacks</td>
</tr>
<tr>
<td></td>
<td>Removing any instruction redundancy</td>
<td>Adding instruction redundancy</td>
</tr>
<tr>
<td></td>
<td>Dead code/store elimination</td>
<td>Insertion of dummy instructions</td>
</tr>
<tr>
<td></td>
<td>Smart scheduling</td>
<td>Random scheduling <em>(shuffling)</em></td>
</tr>
<tr>
<td></td>
<td>Simplifying and combining operation</td>
<td>Masking intermediate values</td>
</tr>
</tbody>
</table>
WHY OPERATING INSIDE A COMPILER?

1. We have a complete view on the program being compiled
   - Possibility to reduce the cost of the security

2. We have control over code optimizers
   - We can decide where and when to apply security
   - We can ensure that the security won’t be removed by the compiler
   - We can take advantage of code optimization

3. We can scale the security level relative to optimization level
Instruction duplication (ID) inside the compiler

1. With a very optimal overhead thanks to our hacked register allocator

**Why?**

With an **Assembly** approach, when comes to duplicate an instruction like: \( \text{add} \ R0, R0, R1 \)

Just doing

\[
\begin{align*}
\text{add} & \ R0, R0, R1 \\
\text{add} & \ R0, R0, R1
\end{align*}
\]

is invalid because \( R0 \) is both source and destination

An extra available register is needed to save \( R0 \):

\[
\begin{align*}
\text{mov} & \ R2, R0 \\
\text{add} & \ R0, R2, R1
\end{align*}
\]

How to find an extra available register?

1. you are designing an ad-hoc countermeasure and you know how many registers are available [Barenghi et al., 2010]

2. you parse your assembly code (not easy)

3. Save an restore

\[
\begin{align*}
\text{push} & \ R2 \\
\text{mov} & \ R2, R0 \\
\text{mov} & \ R2, R0 \\
\text{add} & \ R0, R2, R1 \\
\text{add} & \ R0, R2, R1 \\
\text{pop} & \ R2
\end{align*}
\]
Instruction duplication (ID) inside the compiler

1. With a very optimal overhead thanks to our hacked register allocator (RA)

We modified our RA in such a way that the destination register is always different to source registers:

\[
\text{opcode} \ Rdst, Rsrc1, Rsrc2 \quad (Rdst \neq Rsrc1) \text{ and } (Rdst \neq Rsrc2)
\]

**That’s why**

Instead of generating: \( \text{add} \ R0, R0, R1 \)

We automatically generate: \( \text{add} \ R0, R1, R2 \)

and duplicating such an instruction is straightforward with a reduced overhead compared to:

\[
\begin{align*}
\text{mov} & \quad R2, R0 \\
\text{mov} & \quad R2, R0 \\
\text{add} & \quad R0, R2, R1 \\
\text{add} & \quad R0, R2, R1
\end{align*}
\]

\(X \ 4\)

and

\[
\begin{align*}
\text{mov} & \quad R2, R0 \\
\text{mov} & \quad R2, R0 \\
\text{add} & \quad R0, R2, R1 \\
\text{add} & \quad R0, R2, R1 \\
\text{push} & \quad R2 \\
\text{mov} & \quad R2, R0 \\
\text{mov} & \quad R2, R0 \\
\text{add} & \quad R0, R2, R1 \\
\text{add} & \quad R0, R2, R1 \\
\text{pop} & \quad R2
\end{align*}
\]

\(X \ 6\)
**Instruction duplication (ID) inside the compiler**

1. With a very optimal overhead thanks to our hacked register allocator (RA)

2. Our duplication process is done before the instruction scheduling
   - The compiler will rearrange the instructions in order to find the best execution order
   - As a consequence:
     - duplicated instructions may not necessary be glued
     - improve the execution speed

\[
\begin{align*}
\text{add} & \quad \text{R0, R1, R2} \\
\text{store} & \quad \text{R9, r5} \\
\text{add} & \quad \text{R0, R1, R2} \\
\text{store} & \quad \text{R9, r5} \\
\text{add} & \quad \text{R0, R1, R2}
\end{align*}
\]
Our objective is not to produce new unknown countermeasure.

**But**

Finding a way to combine them in a single tool, without marginalizing the execution performance.

- The next step is to implement power analysis countermeasures in our compiler.
- And then implementing a unified countermeasure model.
- Proving the validity of the model.
Thank you for your attention

http://thiernobarry.fr