SALÃO DE INICIACAO CIENTIFICA XXX SIC

15 A 19 OUTUBRO CAMPUS DO VALE

UFRGS PROPESQ

Ferramenta Configurável de Proteção de Processadores Contra Falhas Transientes por Técnicas Baseadas em Software

Emanuel Novakoski, José Rodrigo de Azambuja
[etnovakoski, jrfazambuja] @inf.ufrgs.br

1. Introdução

Circuitos integrados fabricados com componentes nanométricos, operando em alta frequência, são sensíveis a falhas causadas pela colisão de partículas energéticas. Em processadores, essas falhas são percebidas como erros nos dados ou no fluxo de execução do programa.

Existem várias formas de proteger os processadores de falhas, divididas em técnicas baseadas em software e técnicas baseadas em hardware. Técnicas baseadas em hardware exigem a modificação do circuito, enquanto as baseadas em software alteram apenas o código do programa, sendo possível sua aplicação em processadores comerciais.

2. A Ferramenta: CFT

CFT [1] é uma ferramenta configurável projetada para modificar o código assembly de uma aplicação. Por operar nesse nível, a ferramenta não precisa lidar com as complexidades do código de máquina e pode ser portada para outras arquiteturas, já que é independente dos compiladores e montadores. A figura 1 mostra as etapas de execução da ferramenta.

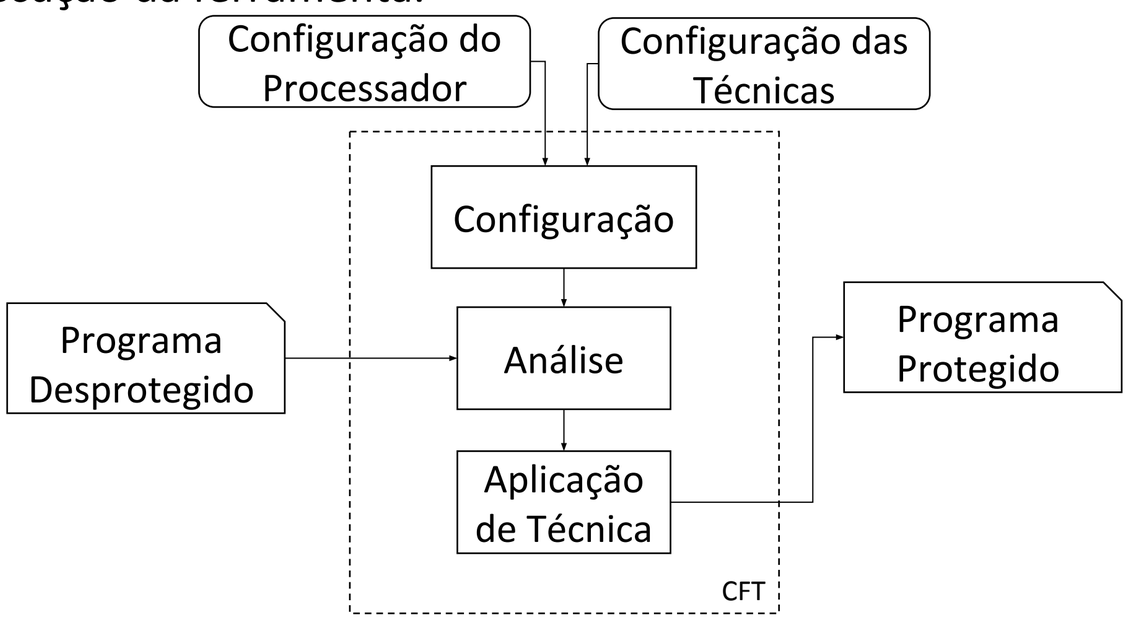

Figura 1. Etapas de execução da CFT.

3. A Nova Arquitetura: RISC-V

A arquitetura RISC-V [2] apresenta algumas diferenças para as arquiteturas já implementadas na CFT, dessa forma foram necessárias algumas modificações na ferramenta.

Para suportar a nova arquitetura, que possui diferenças nas instruções e nos registradores quanto ao tipo de dado: inteiro, ponto flutuante em precisão simples ou ponto flutuante em precisão dupla. A alteração na ferramenta foi feita por mudanças nos arquivos de configurações que descrevem os registradores e as instruções.

3. Resultados

A tabela 1 mostra os resultados de um teste de injeção feito por software [3] em um processador BOOM [4] Single-Issue com algumas das técnicas implementadas pela CFT.

Técnica	Num. de falhas injetadas	Taxa de corrupção de dados	Melhora da sensitividade
Nenhuma	690.083	7,62%	-
Var3Cm	525.102	2,76%	63,78%
Var3Cmb	774.689	2,50%	67,19%
Var3MCm	549.995	2,51%	67,06%
Var3MCmb	549.996	1,75%	77,03%
SIG	519.741	5,26%	30,97%

Tabela 1. Resultados da injeção de falhas em um processador BOOM.

4. Conclusão

A adaptação da ferramenta para a nova arquitetura mostrou resultados positivos em todas as execuções, obtendo uma melhora média na sensitividade a falhas de 61,21%.

Analisando os resultados, notamos uma diferença entre a sensitividade das técnicas de proteção de dados e de proteção de fluxo de controle, sendo os melhores resultados obtidos em proteção de dados.

Referências

1. E. Chielle, R. S. Barth, Â. C. Lapolli and F. L. Kastensmidt, "Configurable tool to protect processors against SEE by software-based detection techniques," *2012 13th Latin American Test Workshop (LATW)*, Quito, Ecuador, 2012, pp. 1-6.
2. RISC-V: The Free and Open RISC Instruction Set Architecture - URL: https://riscv.org/
3. R. B. Tonetto, G. L. Nazar and A. C. S. Beck, "Precise evaluation of the fault sensitivity of OoO superscalar processors," *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, 2018, pp. 613-616
4. RV64G RISC-V superscalar Berkeley Out-of-Order Machine - URL: https://github.com/ucb-bar/riscv-boom

UFRGS UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico

INF INSTITUTO DE INFORMÁTICA UFRGS