Análise das injeções

Introdução

Para a elaboração desse trabalho, foram injetadas entre 3000 e 5000 falhas através do CAROL-FI em 5 aplicações diferentes. Todos os testes foram executados em processadores da família Intel Core, portanto assume-se que se trata da mesma arquitetura, apesar das pequenas diferenças que possam existir entre os diferentes modelos utilizados.

As aplicações foram: - Algoritmo de Cooley-Tukey em C++ - Algoritmo de Cooley-Tukey em C - Algoritmo de Cooley-Tukey em Python - Cálculo da transformada através da biblioteca FFTW utilizando 1 thread - Cálculo da transformada através da biblioteca FFTW utilizando 2 threads

Vulnerabilidade

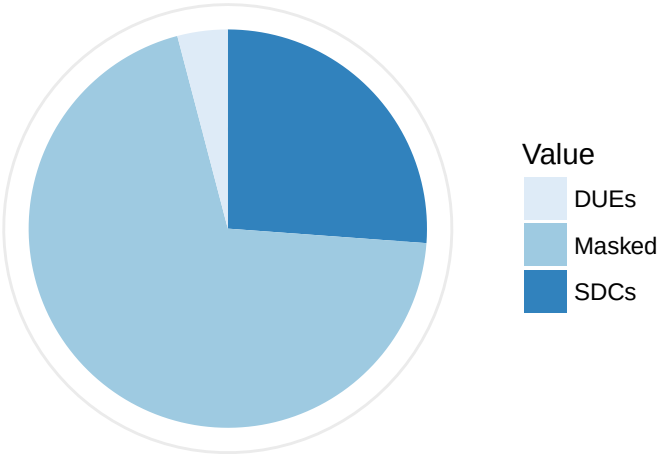
O resultado geral das injeções é mostrado na tabela abaixo.

Implementation	Injections	SDCs	DUEs	PVF	AVF.SDCs	AVF.DUEs
Cooley-Tukey C	NA	NA	NA	NA		
Cooley-Tukey CPP	3723	974	152	NA	0,2616169756	0,0408272898
FFTW CPP	4907	1239	32	NA	0,2524964337	0,0065212961
FFTW 2T CPP	3723	803	333	NA	0,2156862745	0,0894439968
Cooley-Tukey Python	457	437	20	NA	0,9562363239	0,0437636761

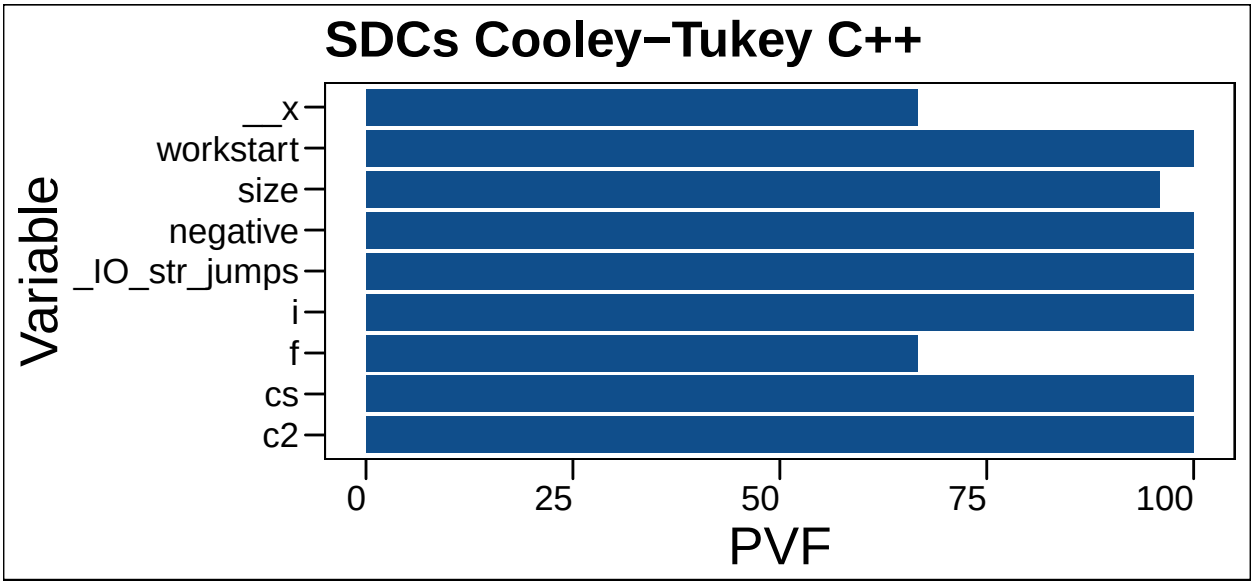
A implementação que se mostrou mais vulnerável foi a em Python que, devido aos resultados obtidos, teve muito menos injeções e foi descartada posteriormente. Além disso, as implementações que fazem uso de uma biblioteca para o cálculo da transformada se mostraram mais resilientes, possivelmente graças à verificações feitas internamente, com exceção da implementação com 2 threads que apresentou uma taxa maior de DUEs. Nas sessões seguintes faremos análises específicas para cada versão.

Análise Cooley-Tukey C++

Na implementação do algoritmo Cooley-Tukey em C++, foram injetados 3723 falhas. No gráfico a seguir, é possível ver a distribuição dos resultados das injeções.

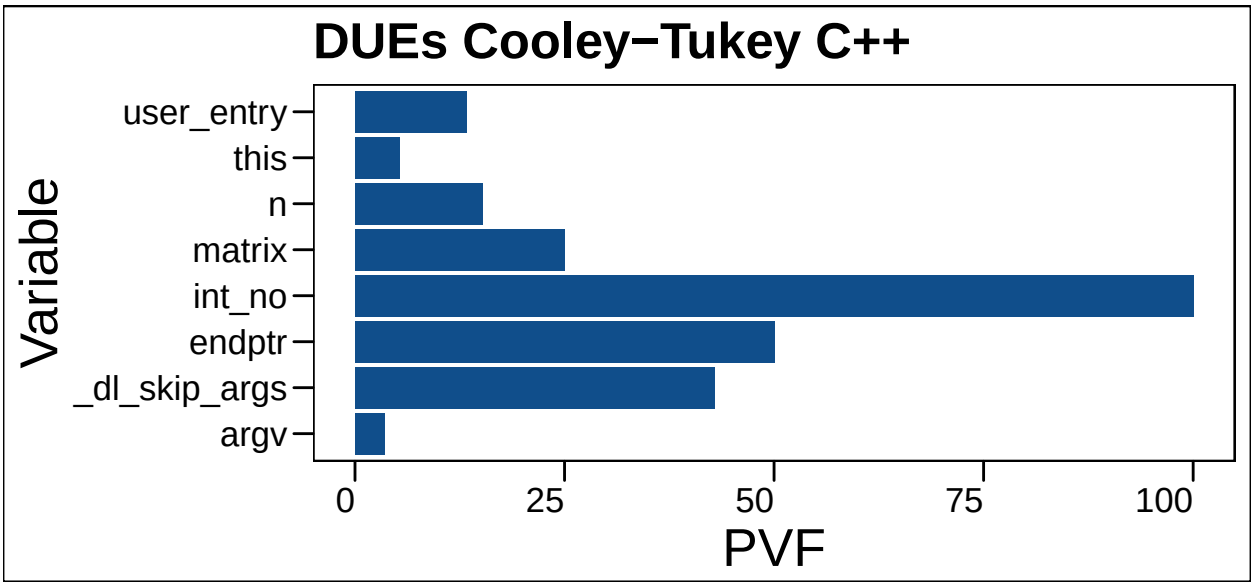


De acordo com os dados obtidos, cerca de 25% das falhas resultaram em SDCs, enquanto os DUEs representam menos de 5%. Felizmente, a grande maioria das injeções não resultou em alterações na saída.



Verificando as 10 variáveis mais vulneráveis, percebe-se que apenas duas entre elas fazem parte da aplicação em si, sendo as outras vindas das bibliotecas utilizadas. Com isso, concluimos que, para que a aplicação seja protegida da melhor maneira possível, é preferível que não sejam utilizadas bibliotecas (ou sejam utilizadas o mínimo possível). No caso deste trabalho, o foco ficará nas variáveis que podem ser protegidas, ou seja, as criadas pelos alunos.

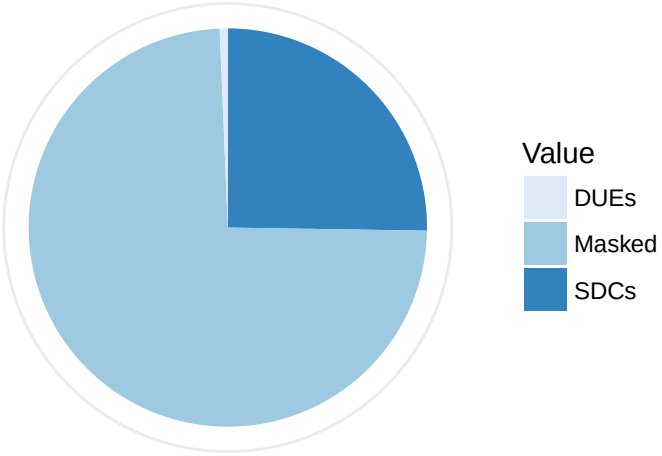
Nesta análise, temos as váriaveis *i* e *size* como mais vulneráveis em questão de SDCs. Como tratam-se de variáveis de controle, uma simples duplicação (ou triplicação) não deve resultar em um *overhead* significativo e, portanto, provavelmente será uma boa solução na etapa seguinte do trabalho.



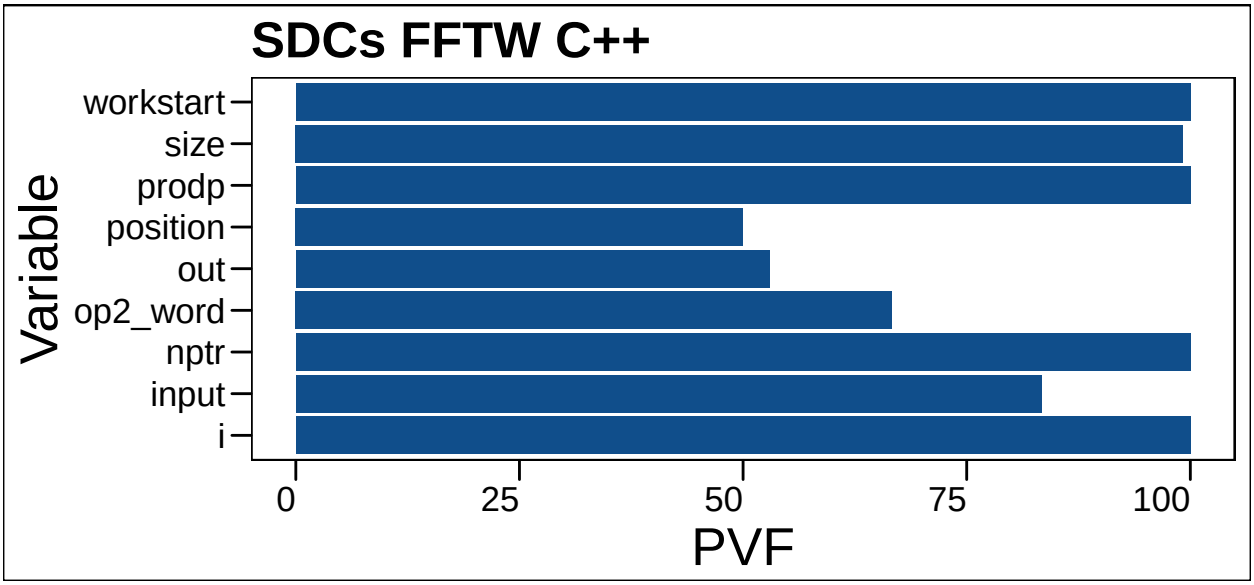
O mesmo se repete se tratando de DUEs; as variáveis que mais os causam são as externas. No entanto, também temos a variável *n* que, assim como as abordadas anteriormente, é uma variável de controle facilmente duplicável, e a variável *matrix*, responsável pela estrutura da aplicação. Para proteger esta, serão necessárias técnicas mais sofisticadas que uma simples duplicação, possivelmente explorando as redundâncias inerentes à transformada.

Análise FFTW C++

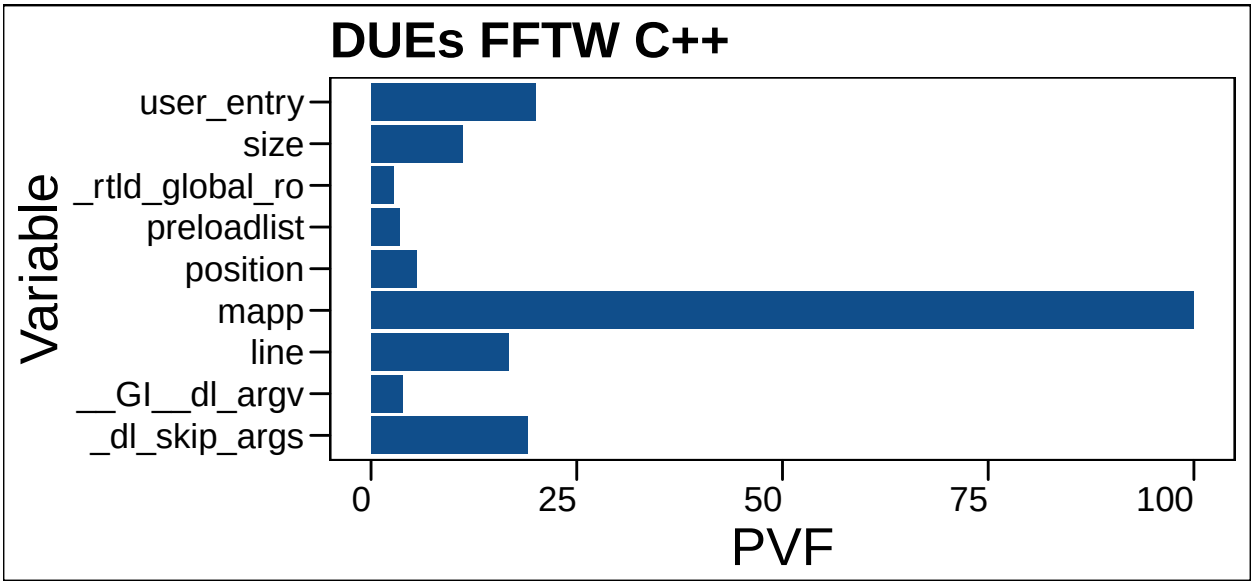
Em seguida, foram realizados testes utilizando uma biblioteca que calcula a transformada de Fourier.



Nessa implementação, novamente temos cerca de 25% de SDCs, mas os DUEs, em compensação, são ainda menos frequentes. Isso se deve provavelmente às medidas de asserção tomadas internamente na biblioteca, que foram capazes de impedir que o sistema entrasse em um estado irrecuperável.



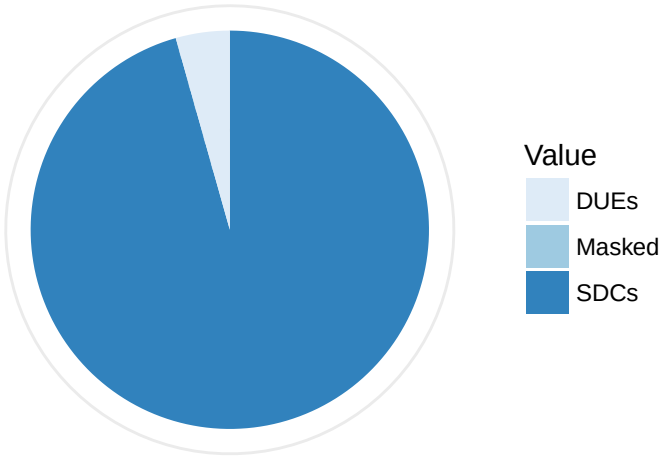
Assim como na implementação anterior, muitos dos SDCs são causados por variáveis fora do nosso controle. Porém, diferentemente da anterior, encontramos a matriz original (na variável *in*) e o arquivo de saída (na variável *output*) entre as variáveis mais vulneráveis. Provavelmente as verificações que a biblioteca implementa são capazes de barrar parte dos erros, conforme mencionado anteriormente; portanto, com maior resiliência entre as variáveis da biblioteca, valores que são menos sensíveis passam a aparecer devido à sua falta de proteção.



Já no caso de DUEs, as únicas variáveis implementadas pelos alunos que apresentaram algum risco foram variáveis de controle. No entanto, o ponto fraco claramente é a variável *mapp*, utilizada apenas pela biblioteca e, portanto, fora do alcance de nossa proteção.

Análise Cooley-Tukey Python

O grupo optou por incluir uma linguagem interpretada para verificar o impacto dessa escolha na vulnerabilidade da aplicação. Para isso, foi feita uma implementação do algoritmo de Cooley Tukey em Python.

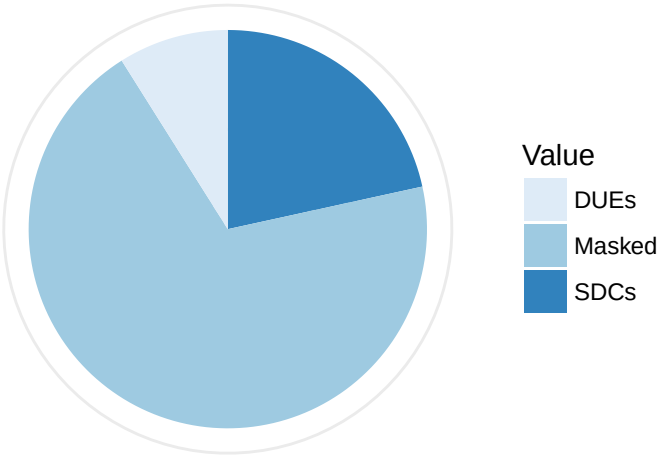


Nessa versão da aplicação, em cerca de 500 injeções não houve nenhum mascaramento. Ao verificar as variáveis que foram afetadas, percebeu-se que todas elas eram pertencentes ao interpretador Python. Com isso, surgem duas possibilidades: ou o grupo não soube utilizar o injetor, de forma que ele não foi capaz de injetar as falhas na aplicação corretamente, ou linguagens interpretadas simplesmente são extremamente vulneráveis a falhas devido à necessidade de um interpretador. Como o grupo conversou com o desenvolvedor responsável pelo CAROL-FI para elaborar os testes, pressupõe-se que trata-se realmente da vulnerabilidade de aplicações que exigem um interpretador executando suas instruções.

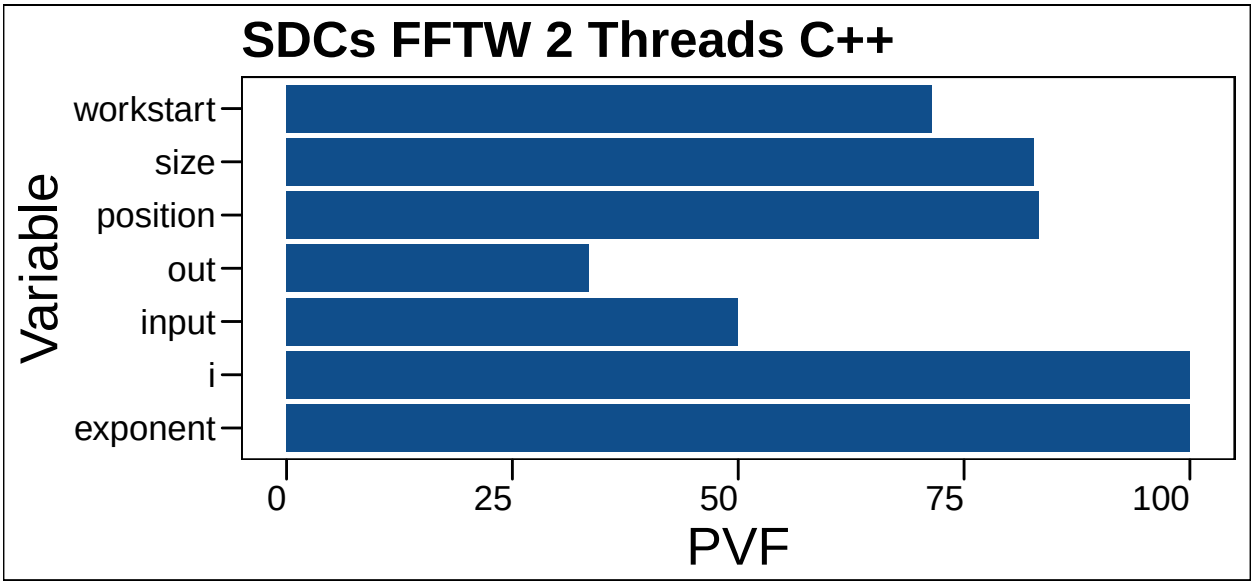
Dadas essas conclusões, não foram injetadas mais falhas nessa implementação.

Análise FFTW C++ 2 Threads

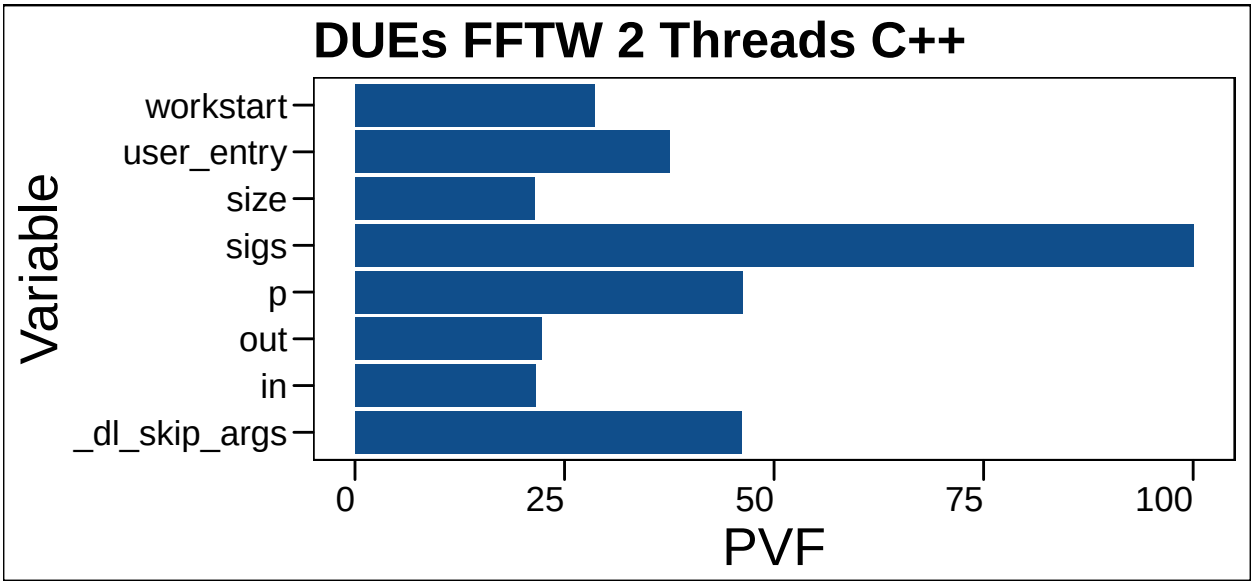
Após perceber que a análise em Python não seria capaz de fornecer os resultados apropriados, decidiu-se utilizar umas das funcionalidades da biblioteca FFTW, que permite que a transformada seja calculada em mais de uma thread.



Utilizando 2 threads, o percentual de DUEs foi o maior encontrado enquanto o de SDCs diminuiu. Isso sugere que, nessa implementação, o efeito das injeções é "mais nocivo" à execução, possivelmente devido às variáveis de controle utilizadas para utilização e sincronização das threads.



Apesar dos resultados anteriores, as variáveis mais vulneráveis nessa implementação não são muito diferentes das analisadas com uma única thread quando se trata de SDCs.



No entanto, se tratando de DUEs, surge uma nova variável extremamente vulnerável, possivelmente vinculada ao controle das diferentes threads, conforme suposto anteriormente. Além disso, surge a variável p, responsável por definir o método da transformada a ser aplicado, o que também sugere que as configurações para controle das threads estão relacionadas ao aumento dos DUEs nessa implementação.

Conclusão

Após analisados os dados, conclui-se que uma duplicação (ou triplicação) das variáveis de controle apresentará um impacto considerável nas implementações do algoritmo Cooley-Tukey.

Já nas implementações que utilizam a biblioteca FFTW, a maior preocupação é com a estrutura do problema em si. Para proteger esses trechos, o grupo planeja utilizar algumas redundâncias presentes na transformada de Fourier, que permitem, no mínimo, detectar quando o resultado não é correto. Essas técnicas também serão aproveitadas nas implementações de Cooley-Tukey, apesar desse não ser o maior causador de erros nesses casos.