Projeto de Formatura – 2021

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

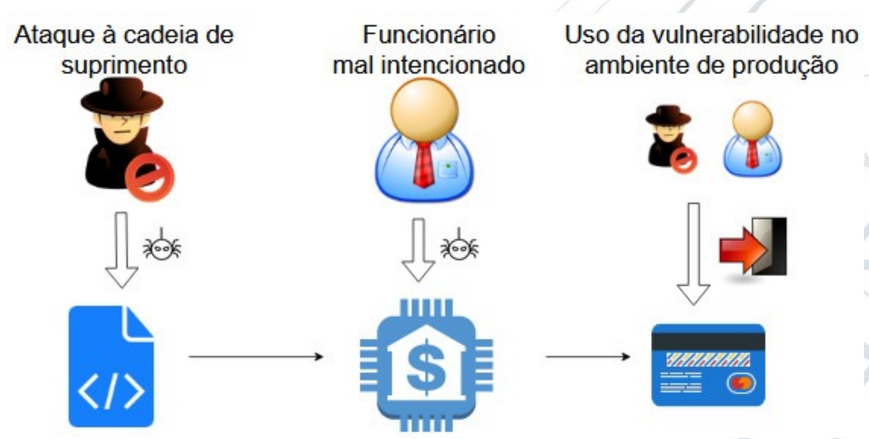
Engenharia de Computação

Tema:

Detecção de Ameaças Silenciosas em Software

Contexto e Motivação

A demanda por segurança cibernética em ambientes corporativos cresceu durante a pandemia da COVID-19 devido ao fato dos ataques cibernéticos contra empresas terem aumentado ao menos 300% no período. Apenas no Brasil, foram mais de 5 milhões ataques do tipo no período. Atualmente, com o uso difundido de bases de código aberto, atacantes buscam formas de inserir *"backdoors"* nessas bases, de forma a ter a possibilidade de corromper sistemas que utilizam dessas bases e também de escalar seus ataques. Esse tipo de ameaça não se restringe apenas às grandes cadeias de suprimento de software, mas também à própria equipe de desenvolvedores da corporação, que podem utilizar de seus acessos privilegiados para inserir *backdoors* no sistema e explorar tais trechos de código malicioso futuramente.



Objetivo

O projeto tem como objetivo a concepção de uma ferramenta e técnicas que possibilitem a detecção da presença de código malicioso inserido de forma sorrateira em aplicações de software. O objetivo ainda é garantir que os administradores dos sistemas recebam avisos sobre a existência de tais trechos de código malicioso, de forma a saberem caso alguma exploração ocorra.

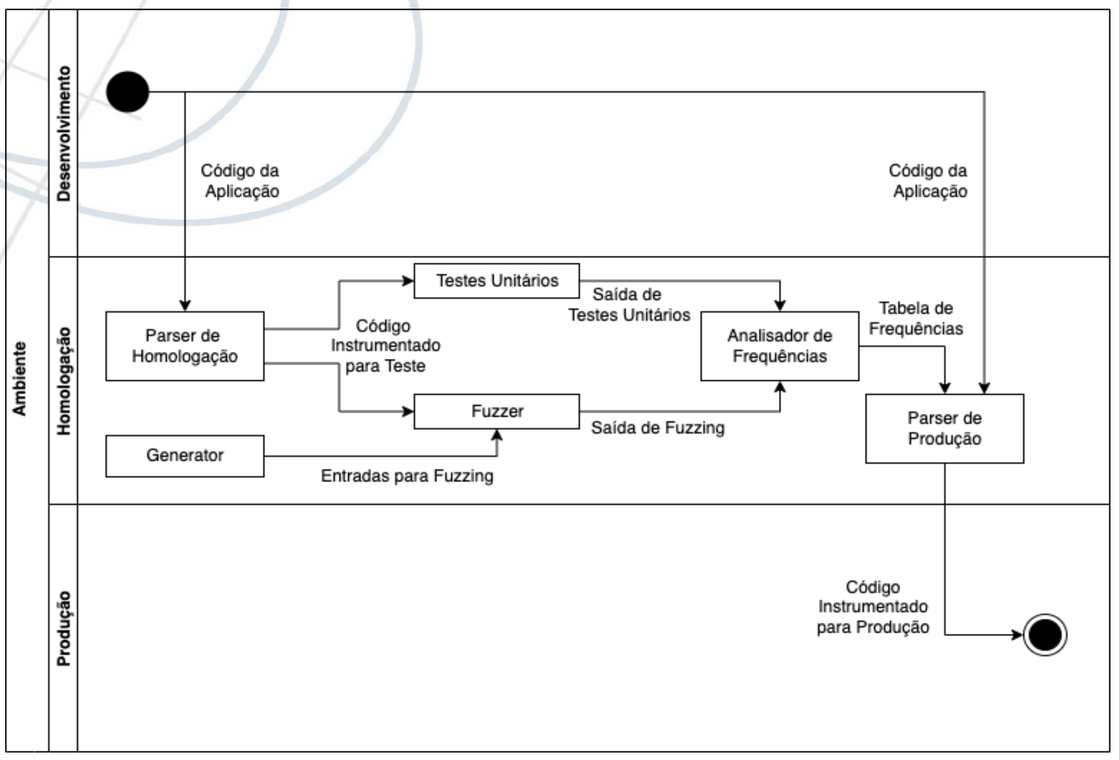
Método

O método encontrado para alcançar tal objetivo foi baseado na instrumentação do código em diferentes fases do processo de desenvolvimento e implementação de software.

Uma instrumentação consiste no processo de adicionar trechos de códigos que gerem *logs* de sistema ao serem executados. A instrumentação é possível por meio do processo de *parsing*, a transformação de trechos de códigos em estruturas de dados que possibilitem sua navegação e inserção de novas instruções no código.

Arquitetura

O projeto se insere nos ambientes de Homologação e Produção. Inicialmente, o trecho de código a ser testado passa por um *Parser* que instrumenta todos os condicionais e, a partir disso, são realizados testes unitários e *Fuzzing* na aplicação para se entender quais trechos de código são executados mais frequentemente e quais não são. Os trechos que forem menos executados nos testes são considerados suspeitos, por isso, de modo a não prejudicar o desempenho, apenas estes são instrumentados no código a ser colocado em produção. Se executado, o trecho suspeito gera um *log*.



Resultados

Os testes para averiguar o funcionamento da ferramenta foram realizados em uma plataforma de *Internet Banking* na qual foram inseridos *backdoors* criados a partir de condicionais, como *backdoors de* senha mestra. Ao se executar tais *backdoors*, a ferramenta foi capaz de identificar que um trecho de código suspeito foi executado. O resultado foi de acordo com o esperado.

Integrantes:
- Eduardo Fernandes Correia Neto
- Felipe Augusto Schaedler Damin
- Victor Min Sub Kim

Professor Orientador: - Prof. Dr. Marcos Antonio Simplicio Junior