Projeto de Formatura – 2021 – Press Release
PCS - Departamento de Engenharia de Computação e Sistemas Digitais
Engenharia de Computação

Tema: Detecção de Ameaças Silenciosas em Software

Estudantes da Escola Politécnica da Universidade de São Paulo desenvolvem ferramenta capaz de detectar inserção de trechos de códigos maliciosos em software.

São Paulo, 8 de dezembro de 2021

Nos dias 05 e 06 de janeiro, os alunos Eduardo Fernandes Correia Neto, Felipe Augusto Schaedler Damin e Victor Min Sub Kim, do curso de Engenharia de Computação da Escola Politécnica da USP, apresentarão seu projeto de formatura, desenvolvido sob orientação do Prof. Dr. Marcos Antonio Simplicio Junior.

Atualmente, a preocupação com a segurança cibernética em sistemas corporativos vem crescendo cada vez mais. Durante a pandemia do COVID-19, ataques cibernéticos contra empresas cresceram ao menos 300%. Apenas no Brasil, foram mais de 5 milhões de ataques, de acordo com a Kaspersky. 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.

Seja em grandes corporações, seja em grandes projetos colaborativos de desenvolvimento de software livre, alterações realizadas no software não necessariamente são devidamente revisadas, o que abre espaço para que funcionários, terceiros ou colaboradores do projeto insiram *backdoors*, trechos de códigos maliciosos que permitem que seu criador tenha acessos que não deveria ter. Um funcionário de um banco pode, por exemplo, inserir um *backdoor* que permita que ele acesse uma conta e transfira valores para sua própria conta. Ou ainda, um atacante pode adicionar a uma biblioteca de software livre trechos de código que realmente façam o proposto, mas que também insiram *backdoors* que permitam acesso remoto aos sistemas que utilizam a biblioteca. É nesse contexto que se mostra a necessidade de criar ferramentas que previnam que situações como essas ocorram.

Pensando nisso, os três alunos junto com seu orientador, Prof. Dr. Marcos Antonio Simplicio Junior e em parceria com o Laboratório de Arquitetura e Redes de Computadores da Escola Politécnica da USP (LARC-USP), decidiram criar uma ferramenta que fosse capaz de verificar a ocorrência de inserções de *backdoors* em sistemas corporativos. A principal finalidade desta é garantir que, durante a fase de homologação de novos códigos no sistema em questão, a ferramenta identifique uma potencial ameaça e, ao executar o trecho supostamente malicioso em ambiente de produção, envie um aviso ao administrador do sistema, de forma a se alertar sobre a ameaça e documentar com exatidão a localização no código em que essa ameaça foi inserida.

Com a ferramenta, os alunos acreditam que as empresas poderão tornar seus sistemas mais seguros contra aqueles que mais teriam facilidade em atacá-los, os próprios funcionários, ou até contra as aparentemente inofensivas bibliotecas de software livre. Além disso, a mitigação do risco de ataques cibernéticos originados internamente permitirá ainda que as organizações concentrem seus esforços na mitigação de ameaças externas, tornando seus sistemas cada vez mais seguros.

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

Professor(a) Orientador(a): Prof. Dr. Marcos Antonio Simplicio Junior