Plan Overview

A Data Management Plan created using DMP Tool

Title: Detecção de Hardware Trojans usando Aprendizado de Máquina

Creator: Victor Hayashi

Affiliation: Universidade de São Paulo (www5.usp.br)

Template: Template USP - Mínimo

Project abstract:

Hardware trojans podem levar a uma degradação acelerada ou comportamentos inesperados em dispositivos utilizados em aplicações críticas como autenticação de usuário para transações financeiras e votação eletrônica. Os dispositivos de hardware de código fechado limitam a capacidade de verificações de segurança, e as soluções do estado da arte para detecção de hardware trojans possuem problemas de escalabilidade. O objetivo da pesquisa é propor métodos de detecção de hardware adequados para designs complexos de hardware aberto, abrangendo trojans de hardware de diferentes fases de inserção.

Start date: 09-01-2022

End date: 12-31-2025

Last modified: 07-08-2024

Copyright information:

The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customize it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan's text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal

---

Detecção de Hardware Trojans usando Aprendizado de Máquina - Descrição dos Dados e Metadados produzidos pelo projeto

Descrição dos dados e metadados produzidos

Que dados serão coletados ou criados?

Dados de exemplos de hardware trojans em dispositivos de hardware de RISC-V e Web3 (Crypto Wallet e Proof-of-Work Miner) na linguagem de descrição de hardware Verilog.

Como os dados serão coletados ou criados

Um total de 10 modelos corretos foram obtidos no GitHub (https://github.com/Saazh/Trojan-D2/tree/main/TrojanD2/Trojan_D2/RISC-V/ALL_FILES_IN_ONE_FOLDER, https://github.com/progranism/Open -Fonte-FPGA-Bitcoin-Miner/tree/master/src, https://github.com/jmaldon1/Crypto_wallet/tree/master/firmware).
Há uso de IA generativa (e.g., ChatGPT) para criação dos exemplos de hardware trojans baseados nos exemplos corretos obtidos nos repositórios GitHub.