Projeto de Formatura – 2023

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema: **Avaliação de Desempenho de Um Sistema Computacional com O Padrão SPDM**

Motivação

O número de dispositivos embarcados no mundo está em crescimento, 14,4 bilhões conectados em 2022 e com **previsão de 16,7 bilhões ao final de 2023**, assim como a necessidade de investimento na segurança desses aparelhos, em 2023 **7,4 bilhões de dólares é o investimento estimado**.

Segundo uma pesquisa realizada pelo time de segurança da Microsoft em 2021, **83% das empresas que participaram** sofreram ao menos um ataque a nível de firmware entre 2019 e 2020. Em outro relatório da Microsoft, há a informação de que **57% dos dispositivos embarcados estão vulneráveis** a mais de 10 vulnerabilidades CVE que são públicas há mais de 10 anos.

Objetivo

O padrão SPDM não possui uma implementação sólida e amplamente testada até o momento deste trabalho, portanto, por meio do código aberto de referência da organização DMTF – **LibSPDM** –, objetiva-se verificar que a sobrecarga oferecida, desde o boot até a totalidade do funcionamento, no sistema computacional é similar aos métodos alternativos com o mesmo nível de segurança.

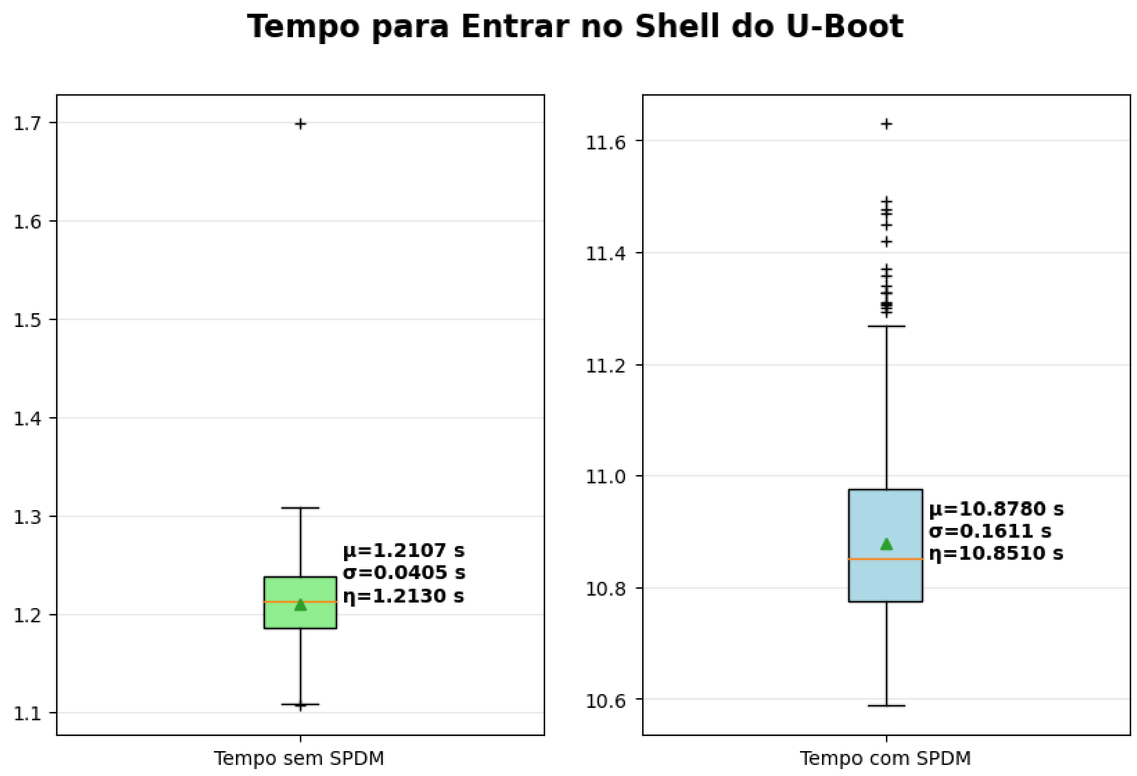
Resultados

Este projeto de formatura implementou a verificação para um HD virtual que deseja iniciar o Linux, mas o padrão SPDM pode ser aplicado para outros drivers presentes no firmware e oferecer os mesmos serviços: confiabilidade, integridade e autenticidade.

A aplicação desse padrão a nível de firmware pode levar a empecilhos, pois, apesar da segurança em hardware embarcado estar sendo confrontada por ataques, as vulnerabilidades não são corrigidas por um longo período devido a fatores como acesso ao dispositivo, economia energética e negligência do usuário. **A sobrecarga apresentada implica em maior gasto energético e, também, tempo de desenvolvimento**, fatores que podem influenciar entidades fornecedoras a serem resistentes à adoção do padrão SPDM.

Os **testes** realizados foram **em ambiente emulado**, o que implica em interações entre dispositivos trafegando em camadas de abstração e, por conseguinte, degradando o desempenho. Para melhor avaliar a sobrecarga imposta, um protótipo físico é necessário, além de incluir o padrão SPDM em outro driver distinto de um virtual.

Um dos objetivos iniciais era a comparação da implementação do padrão SPDM com outras tecnologias de mitigação de vulnerabilidades no firmware, entretanto, devido ao processo de desenvolvimento ter sido lento, **não foi possível comparar com outras técnicas de proteção**. Por conta do tempo empregado na busca de um firmware e na inclusão do padrão nos softwares necessários, também não houve janela para estudar o uso de outras tecnologias e criar uma métrica eficaz para realizar comparações.



Integrante: Otávio Felipe de Freitas
Professor(a) Orientador: Prof. Dr. Marcos Antônio Simplicio Junior
Co-orientador : Prof. Dr. Bruno de Carvalho Albertini