Projeto de Formatura – 2023 – Press Release
PCS - Departamento de Engenharia de Computação e Sistemas Digitais
Engenharia de Computação

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

Estudante da Poli-USP aplica um padrão de segurança a nível de firmware em arquitetura RISC-V 64 bits.

São Paulo, 05 de dezembro de 2022

Segurança em nível de firmware torna-se ainda mais relevante ao considerar o número de dispositivos de internet das coisas, segundo uma matéria da IoT Analytics, em um documento de maio de 2023, haviam 14,4 bilhões de aparelhos conectados em 2022, com previsão de 16,7 bilhões ao final de 2023. Seguindo o crescimento de IoT, ocorre fomento no investimento de segurança nesses aparelhos. Em 2023, estima-se o investimento de 7,4 bilhões de dólares e projeta-se para 2028, 9,8 bilhões de dólares uma matéria da Yahoo Finance.

Em um relatório confeccionado pelo time de segurança da Microsoft em 2021, foi realizado uma pesquisa online com 1000 indivíduos envolvidos em decisões de segurança em países como EUA, Reino Unido, Alemanha, China e Japão. Nesse documento publicado, 83% das empresas responderam que sofreram ao menos um ataque em nível de firmware entre 2019 e 2020, entretanto relata-se que apenas 29% do orçamento de segurança é alocado para a proteção de software.

A organização *Distributed Management Task Force*, DMTF, tem a iniciativa de um padrão de segurança chamada *Security Protocol and Data Model*, SPDM, para habilitar autenticação e troca de chaves com o intuito de oferecer uma infraestrutura de segurança Esse padrão de segurança ainda não é amplamente adotado, pois as vantagens e desvantagens ainda são avaliadas. O projeto realizado pelo aluno visa promover a utilização do SPDM e analisar a sobrecarga imposta em um sistema computacional. O trabalho foi realizado em ambiente emulado, utilizando o software QEMU, o firmware U-Boot e a arquitetura RISC-V 64 bits.

Os resultados encontrados para um dispositivo com padrão SPDM, implementado em seu firmware e no driver do dispositivo de blocos virtual, apresentam uma média de tempo 9 vezes superior a um dispositivo sem o padrão SPDM. As trocas de mensagens utilizando o canal seguro de comunicação também demonstram um aumento no tempo de boot. Entretanto, a queda do desempenho era esperada, pois funcionalidades que exigem maior processamento são adicionadas nos dispositivos.

Mesmo que o tempo aumente, os serviços de segurança fornecidos pelo padrão SPDM, confidencialidade, autenticidade e integridade, estão presentes no modelo emulado. Há intenções futuras de testar as modificações em um dispositivo físico para adquirir métricas fidedignas, além de comparar a solução com outros métodos de segurança a nível de firmware.

Integrante: Otávio Felipe de Freitas

Professor Orientador: Prof. Dr. Marcos Antonio Simplicio Junior
Co-orientador: Prof. Dr Bruno de Carvalho Albertini