



Estudantes da Poli-USP desenvolvem protótipo de dispositivo de segurança que utiliza duas tecnologias de estado-da-arte pela primeira vez

São Paulo, 04 de dezembro de 2022

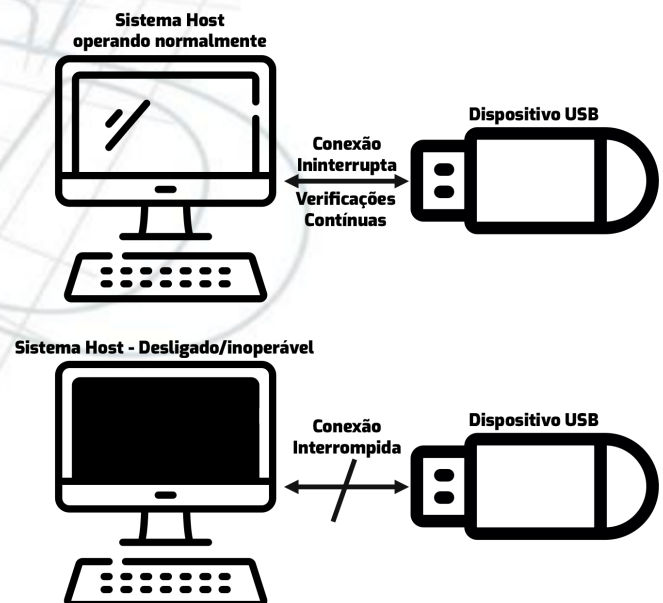
Nos dias 20 e 21 de dezembro, os alunos Leonardo Rodrigues Murad Cassiano, Lucas de Menezes Cavalcante e Marcio Suguiyama de Abreu, do curso de Engenharia de Computação da Escola Politécnica da USP, apresentarão seu projeto de formatura, baseado na criação de um dispositivo USB de segurança que implementa o protocolo Security Protocol and Data Model (SPDM) aliado à tecnologia de Time-based One Time Password (TOTP).

Sistemas computacionais modernos devem prevenir ataques à supply-chain como um todo, incluindo a manipulação de componentes através da modificação do firmware. Nesse cenário, surge o protocolo SPDM, que especifica um formato de troca de mensagens para autenticação de hardware e firmware.

Em conjunto com este protocolo, foi utilizada a tecnologia TOTP, que adiciona uma camada temporal à segurança do sistema, possibilitando verificações periódicas entre dois dispositivos, o que dificulta a execução de ataques como de spoofing. Adicionalmente, a encriptação proporcionada pelo SPDM impede também a execução de ataques do tipo Man-In-The-Middle.

Com isso, foi desenvolvido um sistema composto principalmente por dois elementos: o driver USB e o dispositivo emulado pelo QEMU. Estes trabalham em conjunto, de tal forma que qualquer inconsistência no firmware do sistema *host* ou falha na comunicação SPDM inativa o sistema como um todo, garantindo, assim, a segurança do sistema a nível de firmware.

Por fim, foi desenvolvido também um protótipo físico, que utilizou a placa Intel® Galileo como plataforma para a criação de um dispositivo USB que substituiria o dispositivo emulado pelo QEMU, cumprindo seus mesmos requisitos de funcionamento.



Integrantes: Leonardo Rodrigues Murad Cassiano
Lucas de Menezes Cavalcante
Marcio Suguiyama de Abreu

Orientador: Prof. Dr. Renan Cerqueira Afonso Alves
Co-Orientadores: Prof. Dr. Marcos Antonio Simplicio Junior
Prof. Dr. Bruno de Carvalho Albertini