Projeto de Formatura – 2022

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema: Segurança de sistemas a nível de firmware: aplicação com Time-based One-Time Password aliado ao Security Protocol and Data Model

Motivação

- Prevenção de ataques à *supply chain*
- Protocolo SPDM (Security Protocol and Data Model): especificação que identifica inconsistências no firmware e no hardware e encripta comunicação, protegendo o sistema
- Utilizado em conjunto com o TOTP (Time-based One-Time Password)

Objetivos

- O projeto tem como objetivo a criação de uma aplicação real integrando SPDM e TOTP, gerando uma solução de segurança mais robusta a nível de Firmware.
- A utilização do TOTP adiciona uma camada temporal à segurança do sistema, dificultando a execução de ataques como de spoofing.
- A encriptação proporcionada pelo SPDM impede a execução de ataques do tipo Man-In-The-Middle, que poderiam ser realizados por meio da interceptação de códigos TOTP.

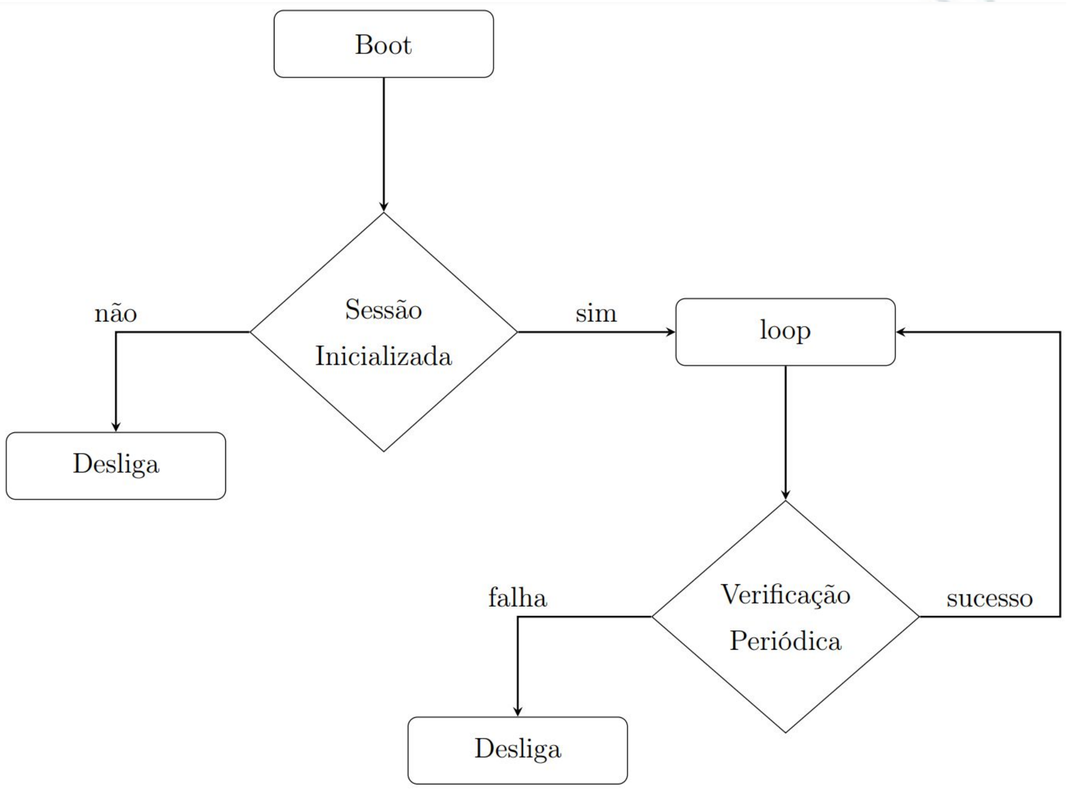
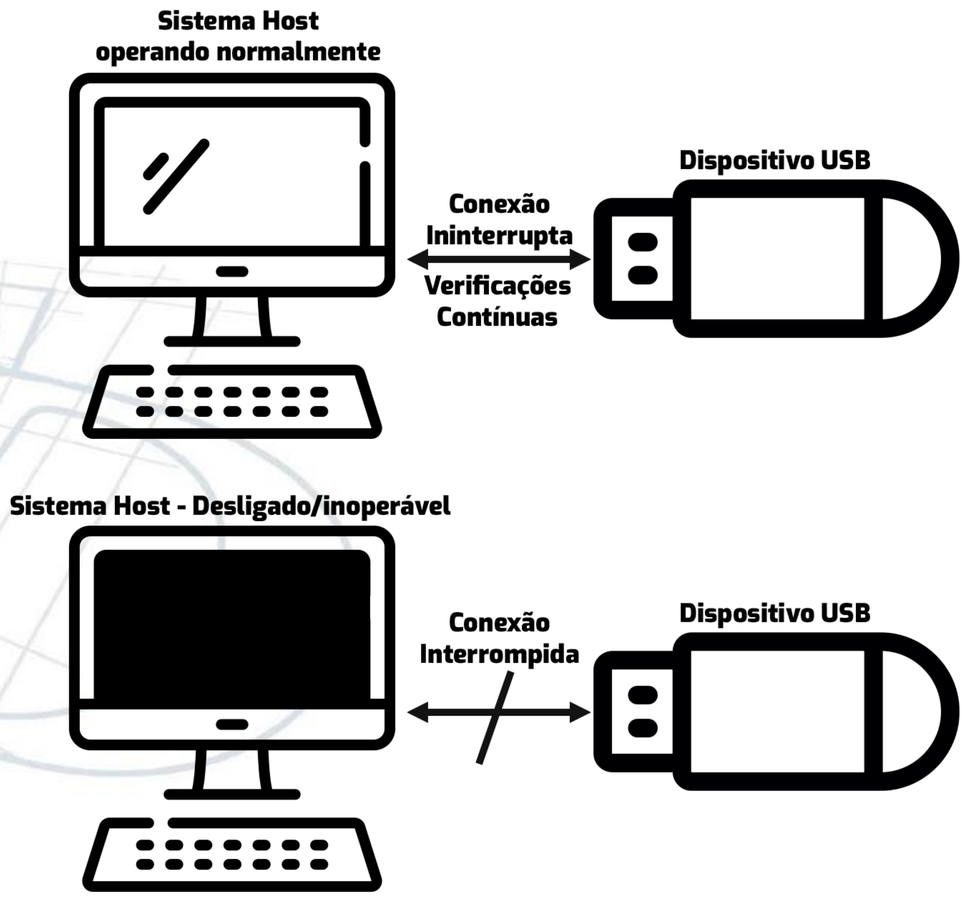


Diagrama de fluxo do sistema.
Fonte: do autor.

Arquitetura

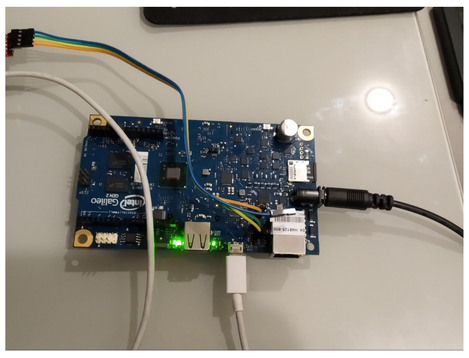
O sistema desenvolvido é composto por dois elementos: o driver USB e o dispositivo emulado por QEMU, software de emulação de sistemas. Os dois elementos trabalham em conjunto, de tal forma que qualquer inconsistência no firmware do sistema host ou falha na comunicação SPDM inativa o sistema como um todo, garantindo, assim, a segurança do sistema a nível de firmware, como indicado pela figura abaixo.



Esquematização do funcionamento do sistema.
Fonte: do autor.

Resultados

- Desenvolvimento de driver para Linux e dispositivo USB emulado que implementam a arquitetura proposta.
- Criação de dispositivo físico que cumpre a função do dispositivo emulado em um ambiente físico.
- Agilização da verificação periódica em 99%
- Uso de apenas 0,7% do processamento da máquina



Montagem da placa Intel Galileo para testes do dispositivo físico. O dispositivo conta com conexão serial e conexão USB com o sistema host.
Fonte: do autor.

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