Ataques rubber ducky e mitigações

Chapter de computação visual

Caio Volpato

04 de janeiro de 2022

Resumo

Hoje vamos falar dos ataques rubber duck e possíveis mitigações.

Em resumo: Esses ataques são dispositivos USB que se comportam como um teclado, que digitam rapidamente, para instalar algum programa malicioso.

Agenda

1. Demo
2. Alguns devices de rubber ducky
3. Mitigações possíveis
4. Uma aplicação
5. Bonus: usando uma yubikey como rubber ducky.

Demo

Nessa demo vamos ver como:

1. gerar um apk malicioso.
2. programar um arduino para atuar como teclado
3. plugar o arduino no celular e instalar o apk
4. ter acesso ao celular remotamente

Link da demo: github.com/caioau/badUSB-Targeting-Android

Quão grave é o ataque?

Com o apk instalado o atacante terá um shell que consegue:

- Acessar contatos, arquivos e fotos
- Acessar localização
- Abrir a câmera e microfone

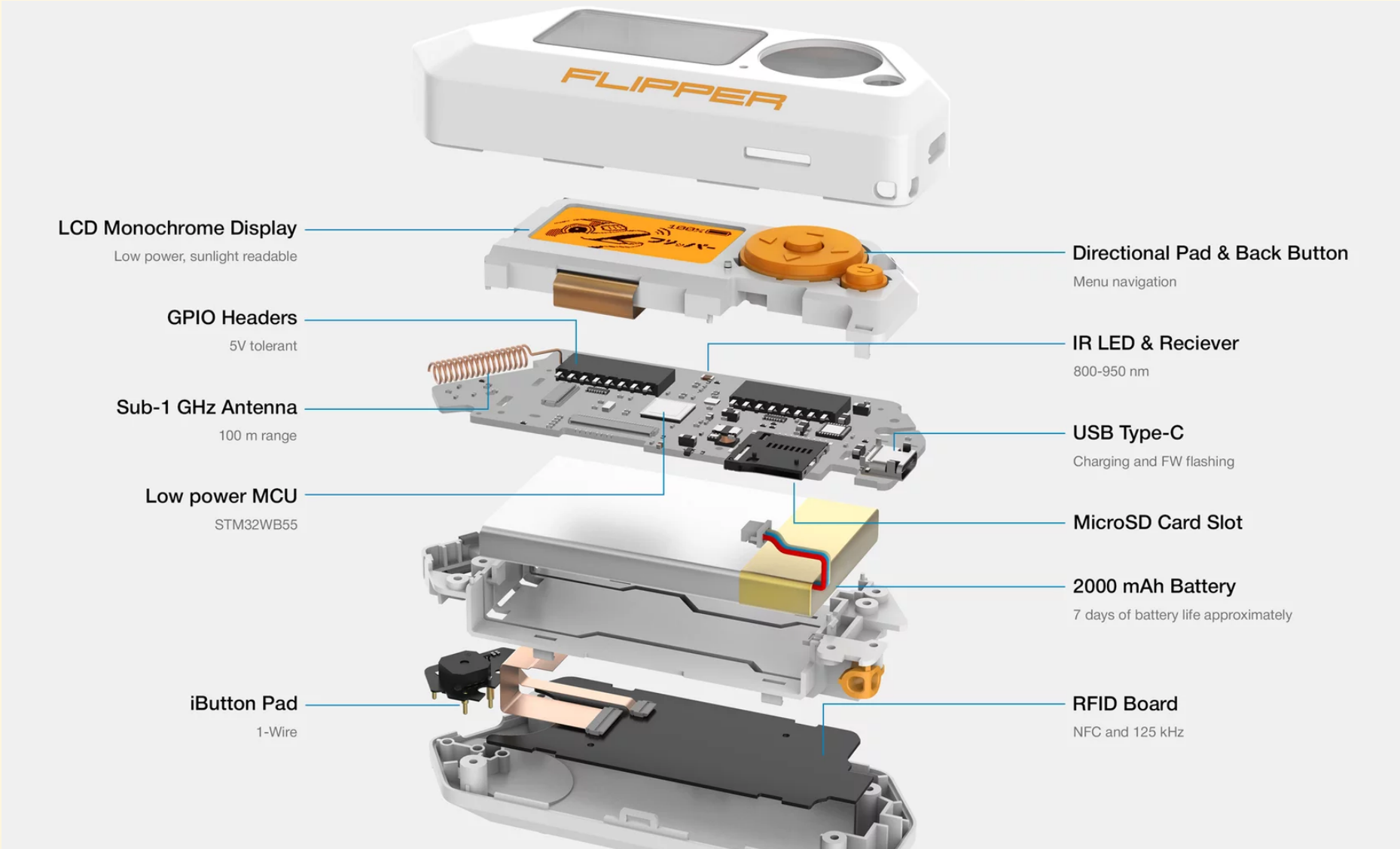
Quão grave é o ataque ? Limitações

Felizmente, tem com algumas limitações:

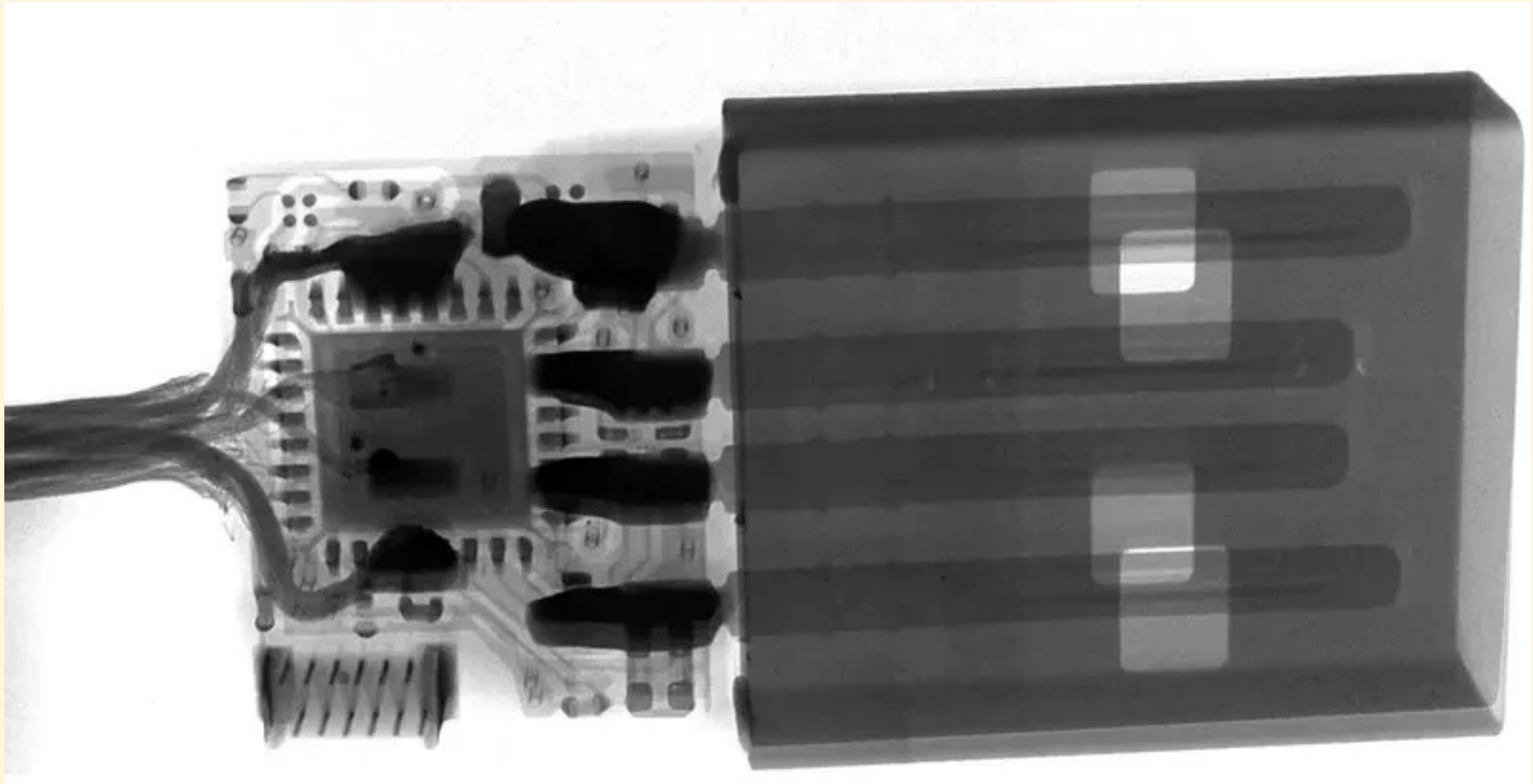
- A sessão não é persistente, depois do reboot o app deixa de rodar.
- O app por mais que não seja listado no launcher ele aparece na lista de apps
- Os atalhos são muito específicos para cada versão de android e marca, dificultando um ataque genérico.
  - Exemplo: (Jan/2017) Trump's Still Using His Old Android Phone. That's Very, Very Risky

Alguns devices: rubber Ducky original da hak5

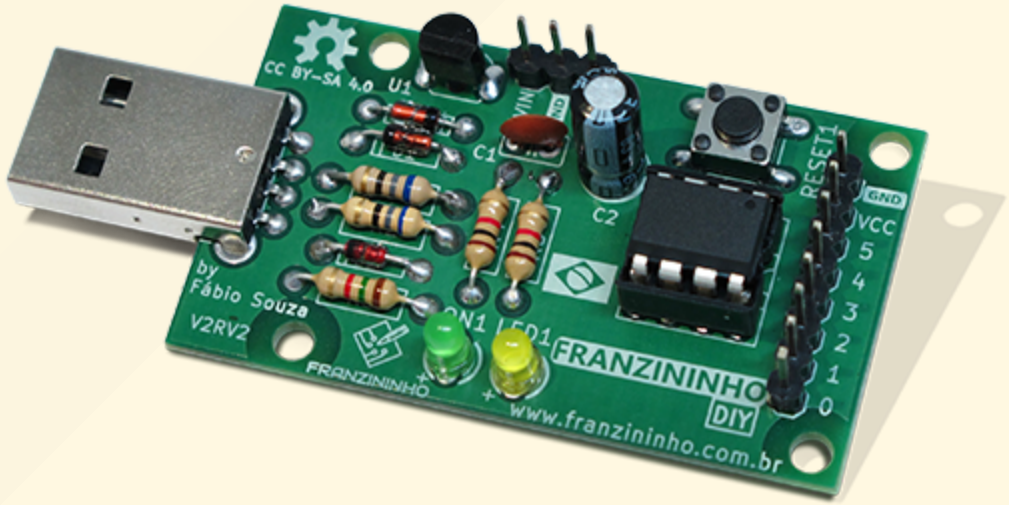
Alguns devices: flipper zero



alguns devices: omg cable (o.mg.lol)



Alguns devices: arduino (franzininho.com.br)

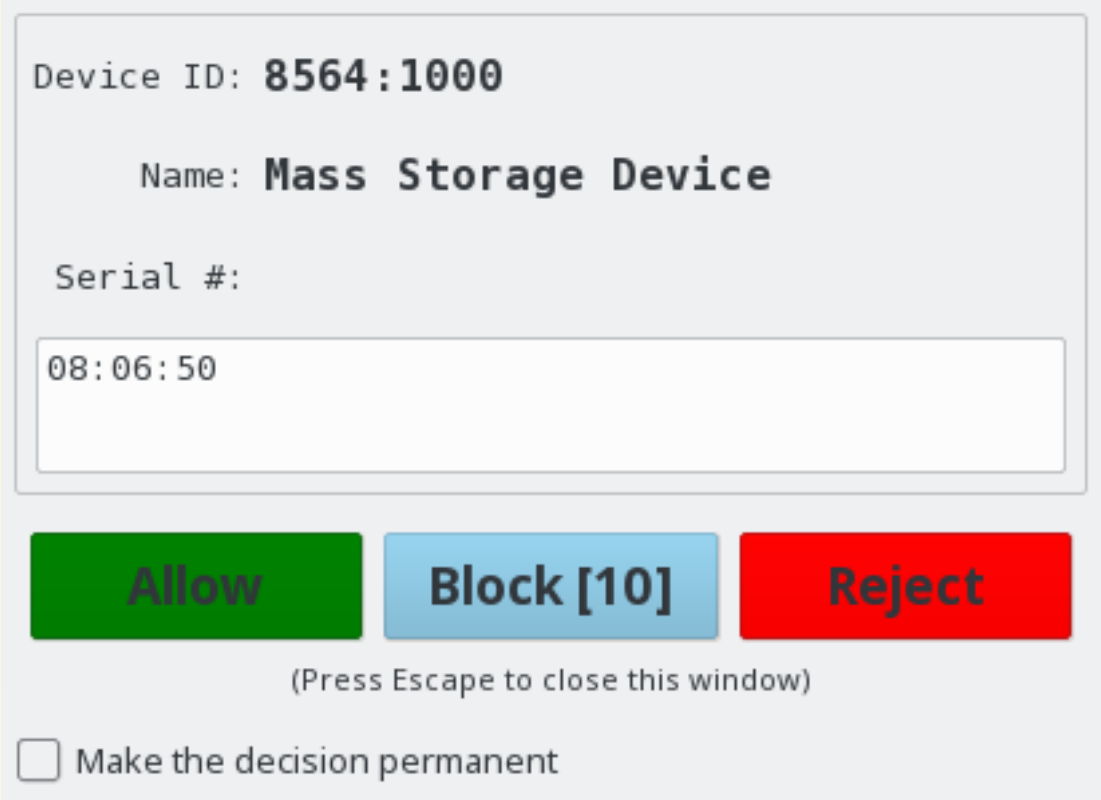


Mitigações: usb data blocker

Desvantagem: Sem os pinos de dados, nao funciona o fast charging.

Mitigações: usbguard

Usbguard é um daemon para Linux que gerencia quais devices USB são autorizados, baseado em listas e regras.

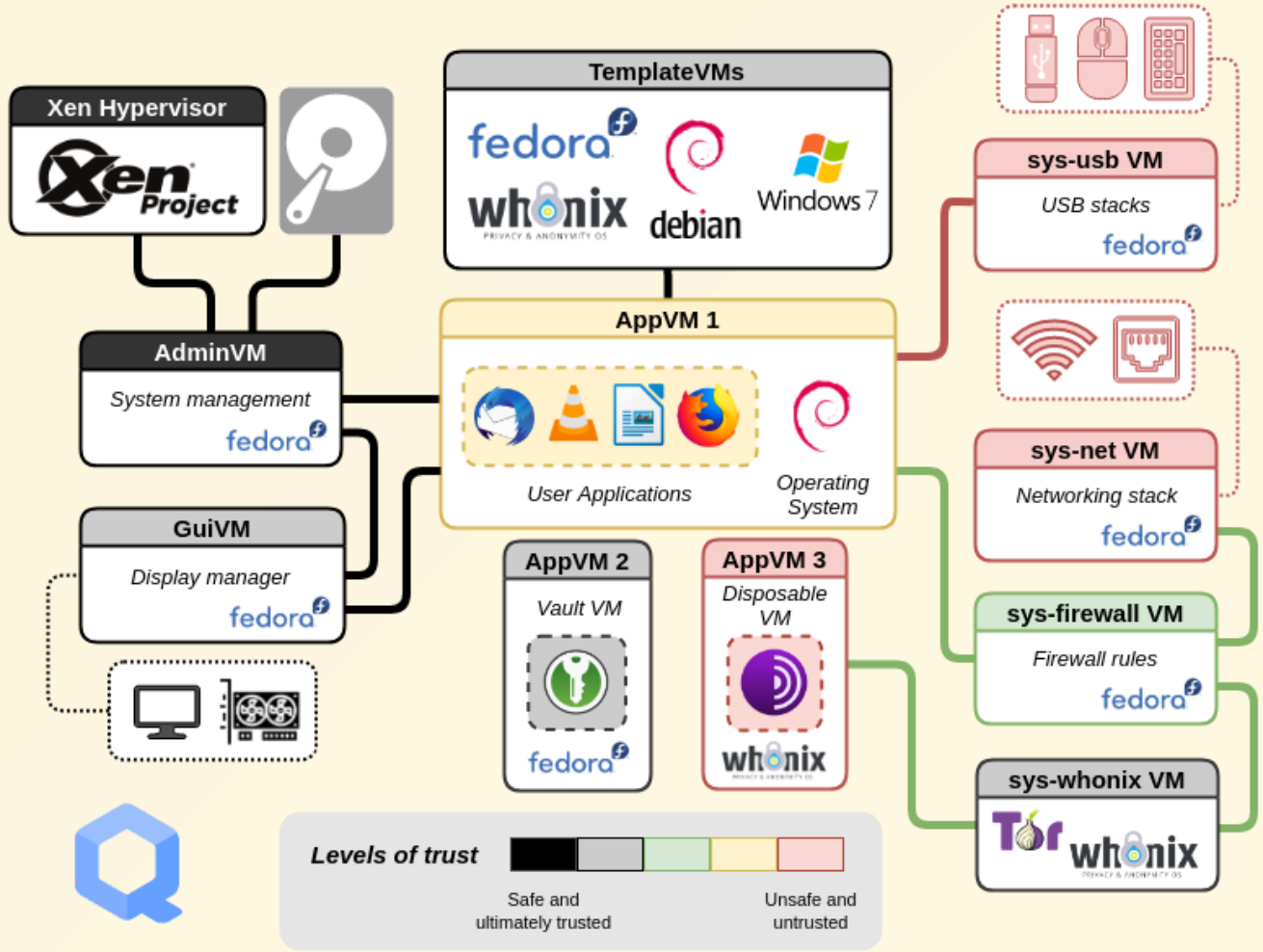


Mitigações: QubesOS

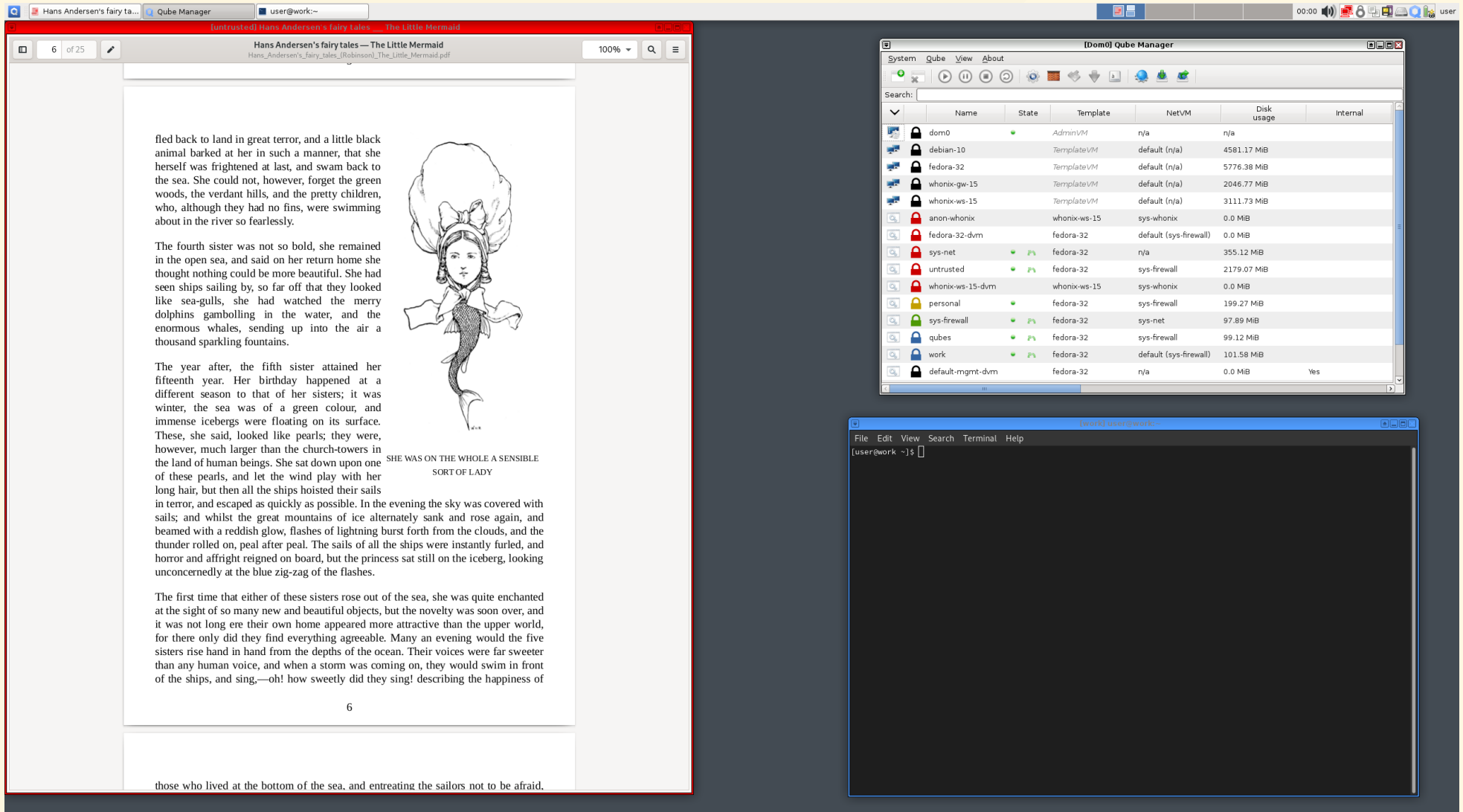
QuebesOS é um sistema operacional baseado em Linux que compartimentaliza os usos do computador em diversas maquinas virtuais.

Website: qubes-os.org

Arquitetura do QubesOS



Screenshot qubesOS



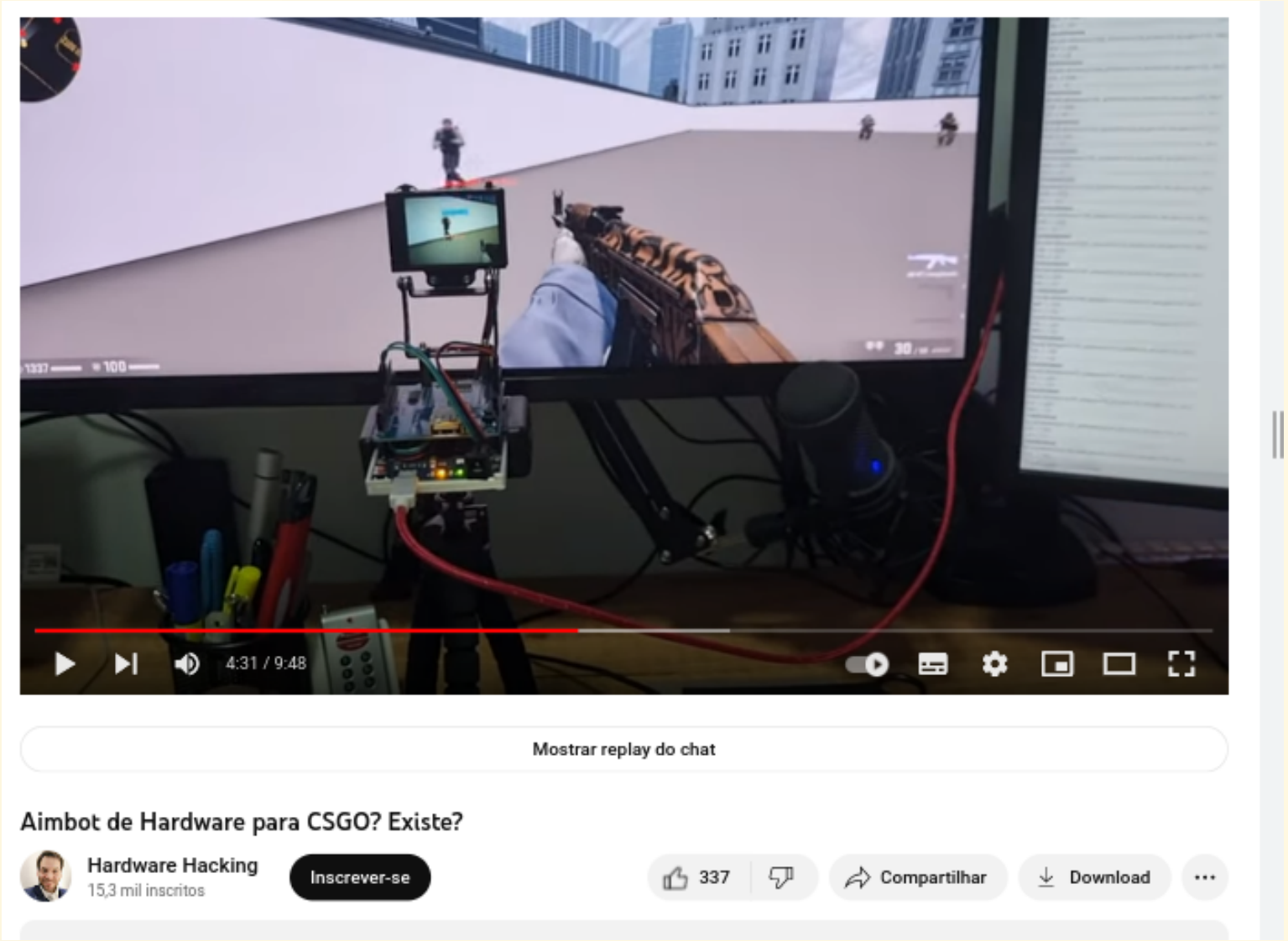
Aplicação: Uso como cheat em games

Alguns sistemas anti cheat para rodar em modo privilegiado, em ring 0, a nivel de kernel, o que fez alguns cheats irem para o hardware, para não serem detectados.

- macros do teclado
- compesador de recuo
- aimbot

A closer look at Valorant's always-on anti-cheat system

HARDWARE para TRAPACEAR EM JOGOS: Os cheats quase indetectáveis (Ft. Julio Della Flora)



[Aimbot de Hardware para CSGO? Existe? (Julio Della Flora)]

Bonus: Usando a yubikey como rubber Ducky

O que é a yubikey?

Yubikey é a marca mais conhecida de chaves físicas de segurança, provendo um mecanismo adicional de segurança em 2 fatores.

Bonus: Usando a yubikey como rubber Ducky

Dentre os protocolos suportados a yubikey tem o Yubico OTP, que são inputados via teclado.

A yubikey não é um device estranho a ser plugado em uma porta USB, levantando menos suspeitas.

O blogpost: How to Weaponize the Yubikey descreve como configurar a yubikey para esse uso.