USB-Ports härten

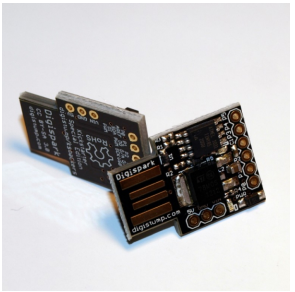
Wie schütze ich meine USB-Ports unter Linux?

Warum will ich meine USB-Ports schützen?

- Jeder mit physischem Zugriff auf einen Rechner kann Dateien kopieren
- Du willst verhindern, dass deine Urlaubsfotos ins Internet gestellt werden...
- Unternehmen wollen verhindern, dass Daten auf ungeschützte USB-Sticks kopiert werden
- USB-Geräte mit modifizierter Firmware können einen Rechner mit Schadprogrammen infizieren

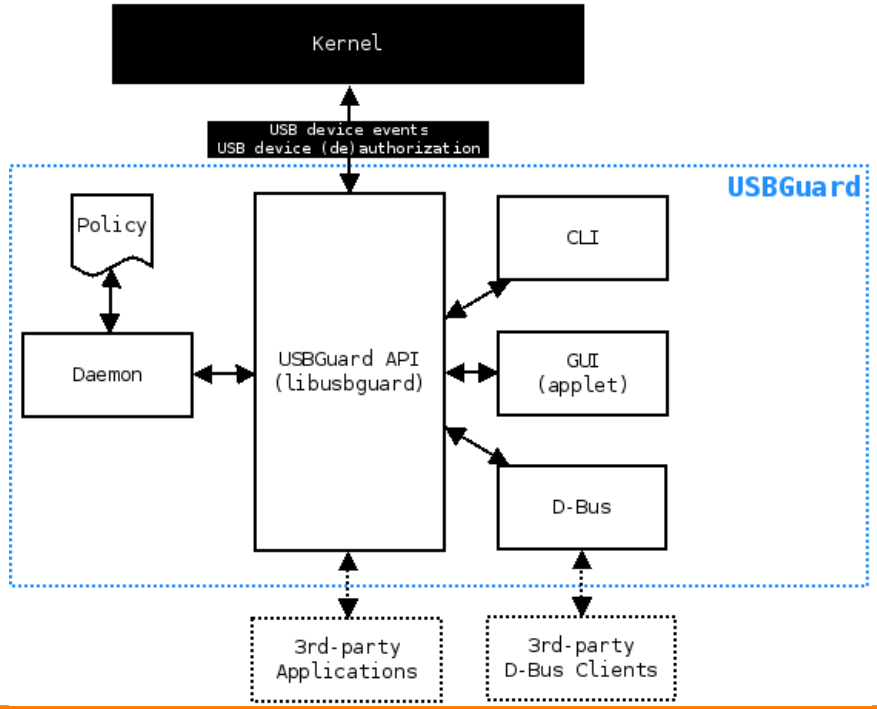
BadUSB

- USB-Sticks die als Tastatur Befehle ausführen:
  - Kommerziell und einfach: https://hakshop.com/products/usb-rubber-ducky-deluxe
  - Oder Marke Eigenbau: https://github.com/digistump/DigistumpArduino/



USBGuard

- Homepage: https://dkopecek.github.io/usbguard/



π

USBGuard: Installation

- Für Fedora gibt es die aktuellen Versionen über ein Repository

```
$ sudo yum install yum-plugin-copr
$ sudo yum copr enable mildew/usbguard
$ sudo yum install usbguard usbguard-applet-qt
```

USBGuard: Konfiguration

- /etc/usbguard/usbguard-daemon.conf:

```
RuleFile=/etc/usbguard/rules.conf
ImplicitPolicyTarget=block
PresentDevicePolicy=apply-policy
PresentControllerPolicy=apply-policy
IPCAllowedUsers=root
IPCAllowedGroups=wheel
DeviceRulesWithPort=false
AuditFilePath=/var/log/usbguard/usbguard-audit.log
IPCAccessControlFiles=/etc/usbguard/IPCAccessControl.d/
```

USBGuard: Konfiguration (2)

- Dem eigenen Benutzer die USB-Guard-Steuerung ermöglichen:

```
$ sudo usbguard add-user joe \
    --devices ALL \
    --exceptions ALL
```

- Regeln für die initiale Richtlinie erzeugen:

```
$ sudo usbguard generate-policy > /tmp/rules.conf
```

- Regeln (nach Prüfung!!!) installieren:

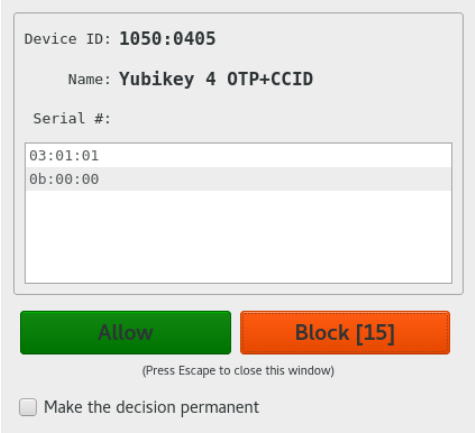
```
$ sudo install -m 0600 -o root -g root /tmp/rules.conf /etc/usbguard/rules.conf
```

- Automatischen Start einrichten und den Dienst starten:

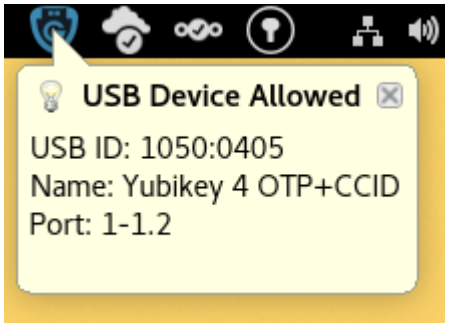
```
$ sudo systemctl enable usbguard
$ sudo systemctl start usbguard
```


USBGuard: Benutzung

- Auswahldialog beim Einstecken eines unbekannten Geräts



- Benachrichtigung bei bekannten Geräten



π

Vielen Dank für die Aufmerksamkeit

www.chaos-consulting.de

Grundlagen USB

Regelwerk