USBGuard

DevConf.cz 2019
The USBGuard software framework helps to protect your computer against rogue USB devices (a.k.a. BadUSB) by implementing basic whitelisting and blacklisting capabilities based on device attributes.
Agenda

● attack access vectors
● basic design
● service configuration
● command line interface
● rules (policy)
● graphical user interface
attack access vectors
basic design
first install necessary packages

### Fedora based distros

# dnf install usbguard usbguard-applet-qt

### Debian/Ubuntu based distros

# apt install usbguard usbguard-applet-qt
service configuration
# grep -v -e ^# -e ^\s*$ /etc/usbguard/usbguard-daemon.conf

RuleFile=/etc/usbguard/rules.conf
ImplicitPolicyTarget=block
PresentDevicePolicy=apply-policy
PresentControllerPolicy=keep
InsertedDevicePolicy=apply-policy
RestoreControllerDeviceState=false
DeviceManagerBackend=uevent
IPCAAllowedUsers=root
IPCAAllowedGroups=wheel
IPCAccessControlFiles=/etc/usbguard/IPCAccessControl.d/
DeviceRulesWithPort=false
AuditBackend=FileAudit
AuditFilePath=/var/log/usbguard/usbguard-audit.log
command line interface
to get information see

# usbguard [command] --help
# man usbguard
# man usbguard-rules.conf
# man usbguard-daemon
# man usbguard-daemon.conf
```
# usbguard generate-policy
allow id 1d6b:0002 serial "0000:00:14.0" name "xHCI Host Controller" hash "jEP/6WzviqdJ5VSeTUY8PatCNBKeaREEvO20qdp1ND/o=" parent-hash "G1ehGQdrL3dJ9HvW9w2HdC//pk87pKzFE1WY25bq8k4=" with-interface 09:00:00
allow id 1d6b:0003 serial "0000:00:14.0" name "xHCI Host Controller" hash "3Wo3XWDgen1hD5xM3PSN13P98kLp1RUTgQ5HSxtf8k=" parent-hash "G1ehGQdrL3dJ9HvW9w2HdC//pk87pKzFE1WY25bq8k4=" with-interface 09:00:00
...```
# usbguard generate-policy -X
allow id 1d6b:0002 serial "0000:00:14.0" name "xHCI Host Controller" with-interface 09:00:00
allow id 1d6b:0003 serial "0000:00:14.0" name "xHCI Host Controller" with-interface 09:00:00
...

# usbguard generate-policy -H

allow hash "jEP/6WzviqdJ5VSeTUY8PatCNBKeaREvo20qdp1ND/o=" parent-hash "G1ehGQdr13dJ9HvW9w2HdC//pk87pKzFE1WY25bq8k4="
allow hash "3Wo3XWDgen1hD5xM3PSNl3P98kLp1RUTgGQ5HSxtf8k=" parent-hash "G1ehGQdr13dJ9HvW9w2HdC//pk87pKzFE1WY25bq8k4="

...
# usbguard generate-policy > rules.conf
# install -m 0600 -o root -g root rules.conf
/etc/usbguard/rules.conf
# systemctl restart usbguard
usbguard watch

# usbguard watch
# usbguard list-devices
# usbguard allow-device <id>
# usbguard block-device <id>
# usbguard reject-device <id>
rules handling

# usbguard list-rules

# usbguard append-rule <rule>

# usbguard remove-rule <id>
rules (policy)
allow \
id 0bda:0316 \
serial "20120501030900000" \
name "USB3.0-CRW" \
with-interface 08:06:50

allow \
hash "WG1MSC3YZsmCs1TNGpjTTjT21UvhNfU4gEVvD3gIuV4=" \
parent-hash "3Wo3XWDgen1hD5xM3PSN13P98kLp1RUTgGQ5HSxtf8k="
attribute forms
single-valued
<attribute> <value>

multi-valued
<attribute> [operator] {<value> [<value>] ..}

allow with-interface equals { 08:*:* }
reject with-interface all-of { 08:*:* 03:00:* }
reject with-interface all-of { 08:*:* 03:01:* }

to get more details, see man usbguard-rules.conf
conditional rules
<rule> if <condition>

allow with-interface one-of { 03:00:01 03:01:01 } if \ 
!allowed-matches(with-interface one-of { 03:00:01 03:01:01 })

allow if localtime(09:00-18:00)
block

to get more details, see man usbguard-rules.conf
graphical user interface
- package usbguard-applet-qt provides GUI front-end
- instantly notifies of device insertion
- make simple changes to policy rules
Device ID: **192f:0416**

Name: **USB Optical Mouse**

Serial #: 03:01:02

- **Allow**
- **Block [59]**

(Press Escape to close this window)

☐ Make the decision permanent

**USB Device Blocked**

USB ID: 192f:0416
Name: USB Optical Mouse
Port: 1-2

**USB Device Inserted**

USB ID: 192f:0416
Name: USB Optical Mouse
Port: 1-2
QUESTIONS?

USBGuard home page  https://usbguard.github.io