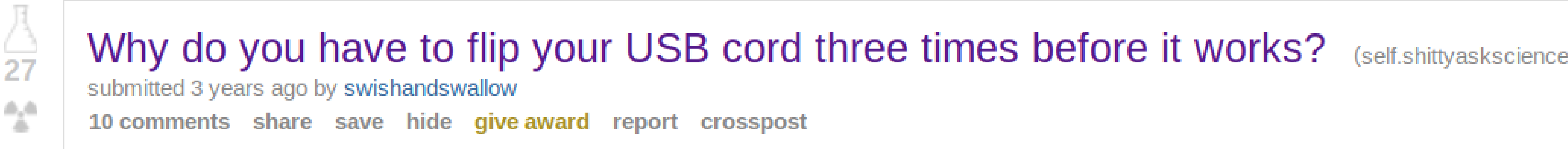
Usable USB Protection

Ludovico de Nittis

Tobias Mueller

Background

USB was meant to be cheap



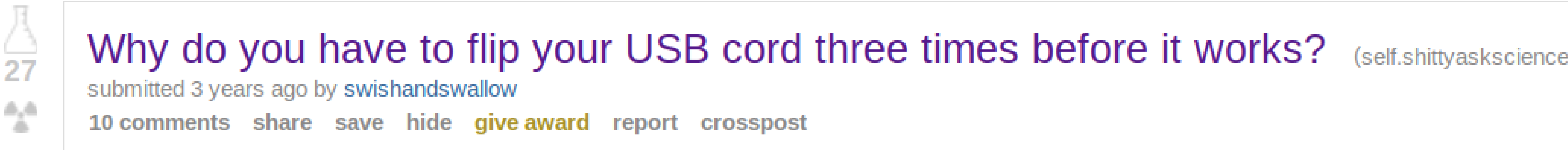
27

Why do you have to flip your USB cord three times before it works? (self.shittyaskscience

submitted 3 years ago by swishandswallow

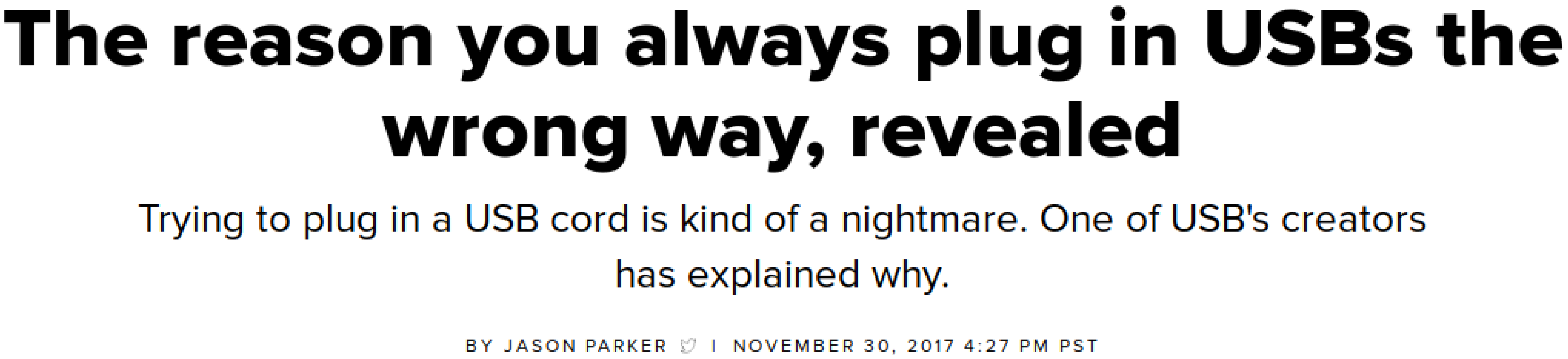
10 comments share save hide give award report crosspost

USB was meant to be cheap



Why do you have to flip your USB cord three times before it works? (self.shittyaskscience

submitted 3 years ago by swishandswallow

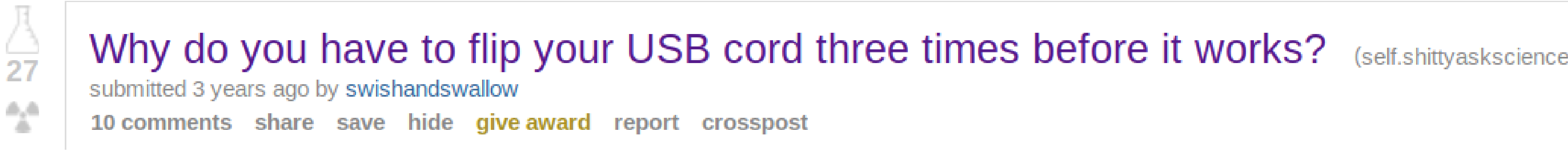


The reason you always plug in USBs the wrong way, revealed

Trying to plug in a USB cord is kind of a nightmare. One of USB's creators has explained why.

BY JASON PARKER | NOVEMBER 30, 2017 4:27 PM PST

USB was meant to be cheap

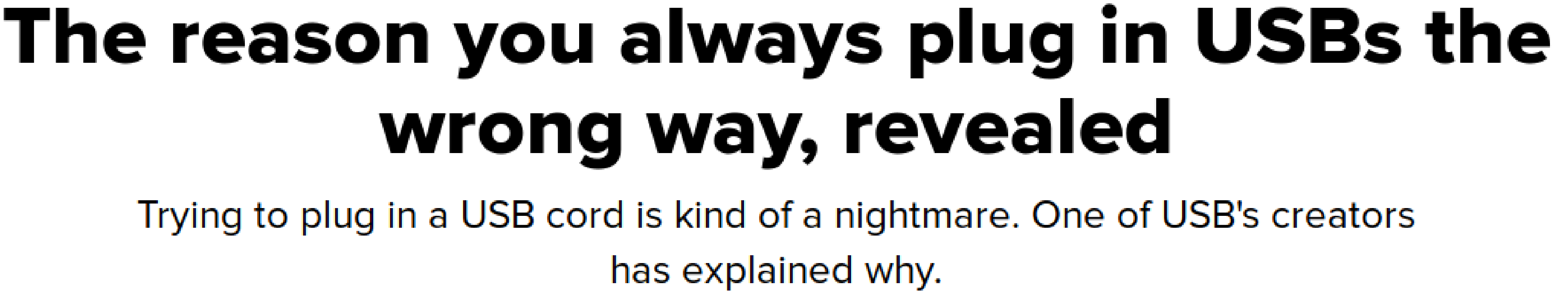


27

Why do you have to flip your USB cord three times before it works? (self.shittyaskscience

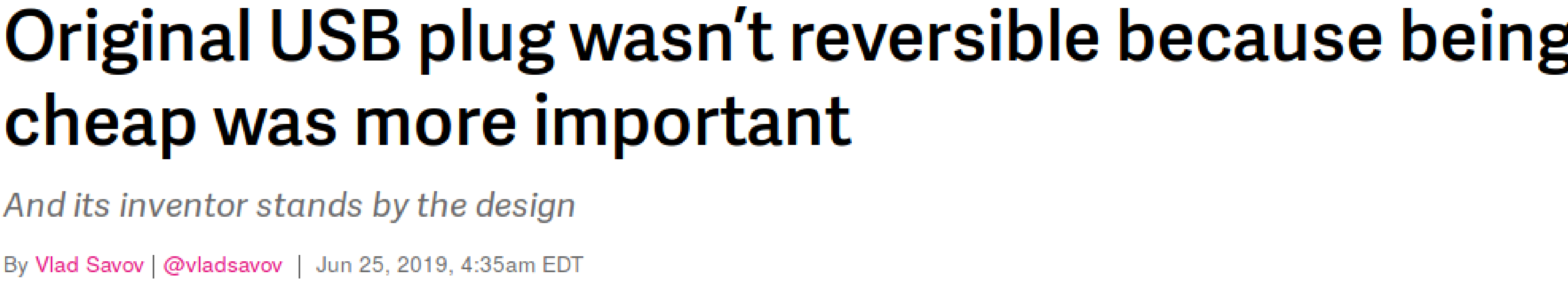
submitted 3 years ago by swishandswallow

10 comments share save hide give award report crosspost



The reason you always plug in USBs the wrong way, revealed

Trying to plug in a USB cord is kind of a nightmare. One of USB's creators has explained why.



Original USB plug wasn't reversible because being cheap was more important

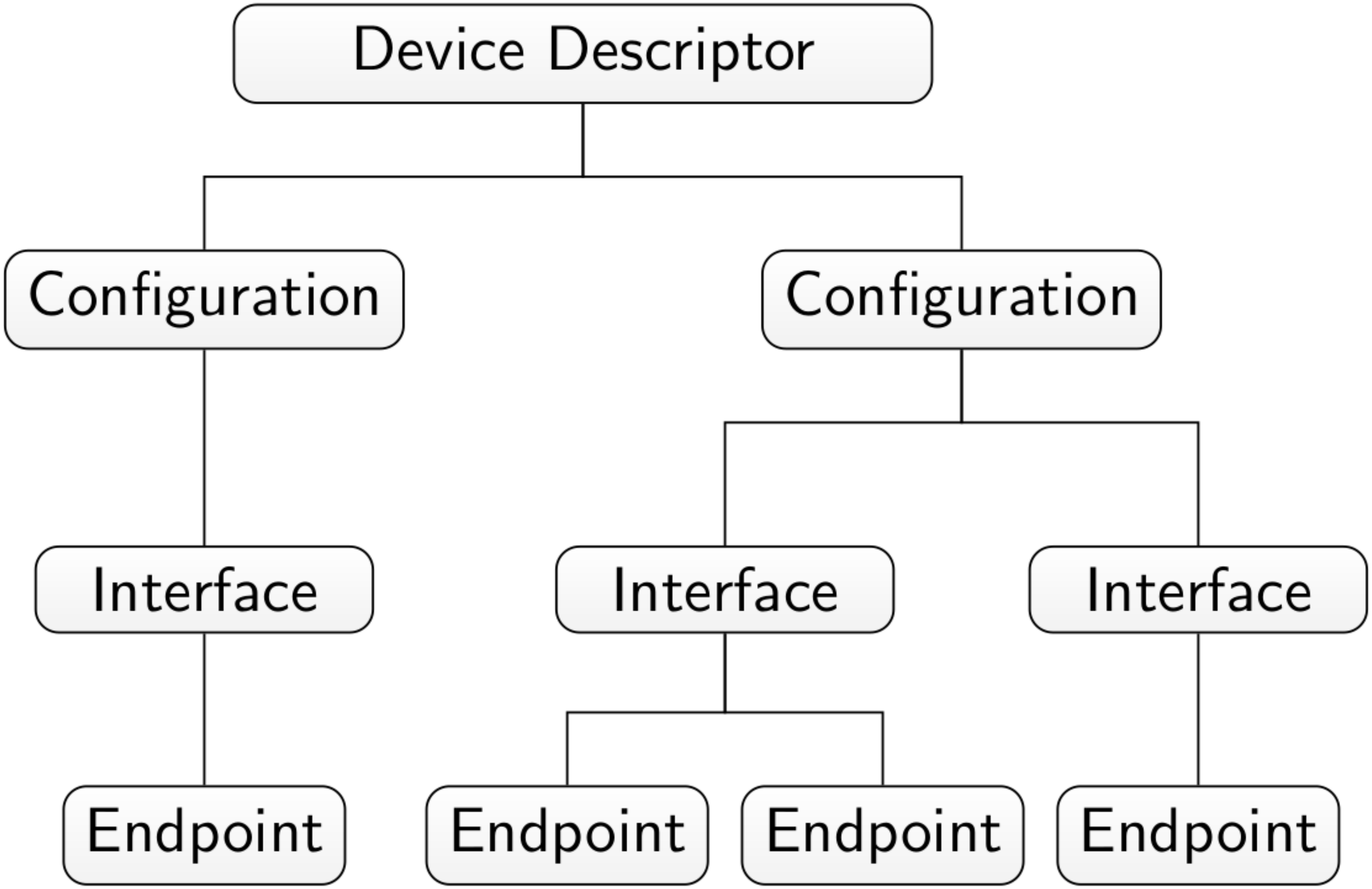
And its inventor stands by the design

By Vlad Savov | @vladsavov | Jun 25, 2019, 4:35am EDT

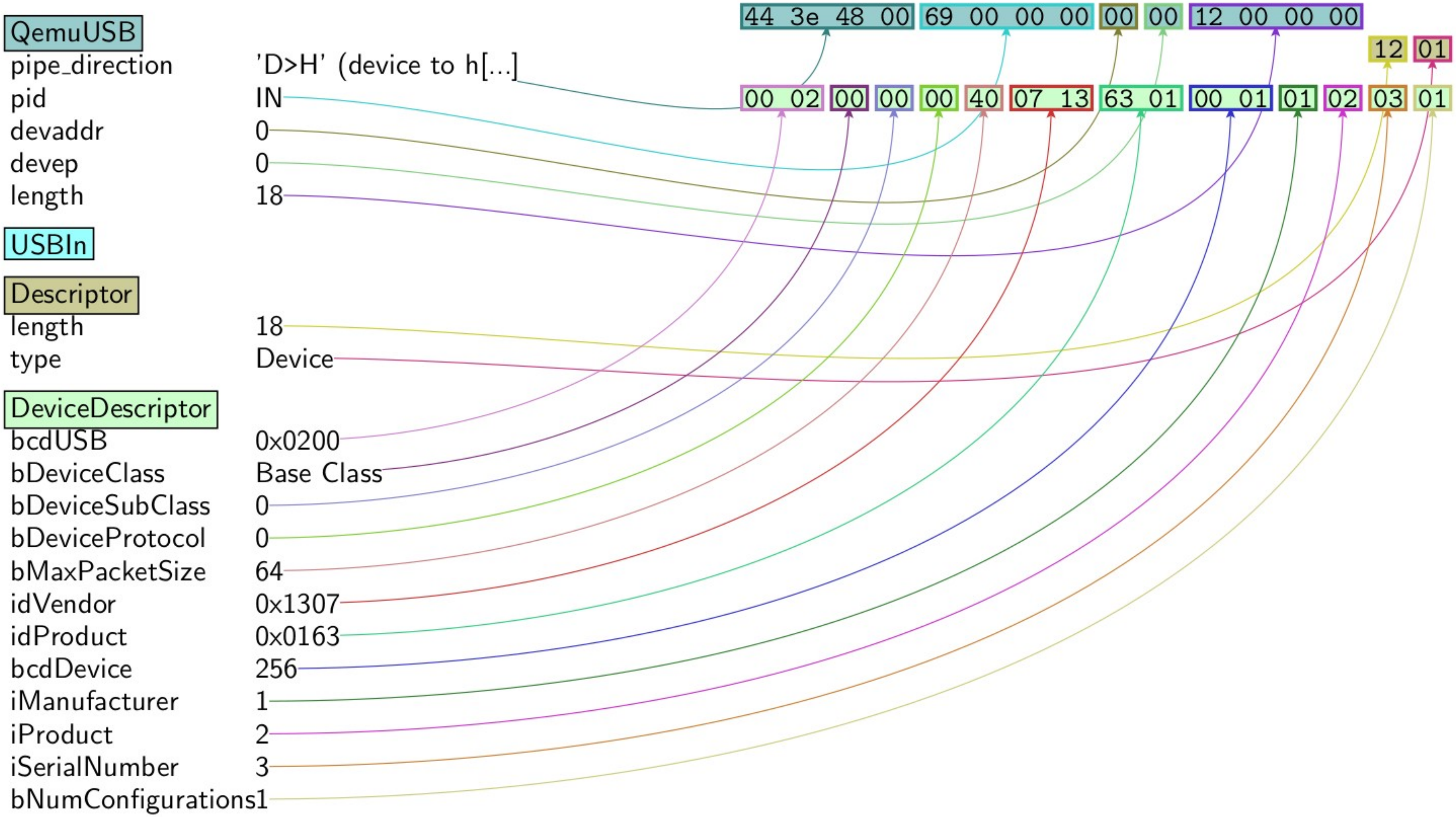
STOW AND LATCH HANDSET FOR TAXI, TAKEOFF AND LANDING
FASTEN SEAT BELT WHILE SEATED

Sie können hier 1 Stimme abgeben
Christlich Demokratische Union
SPD
CDU

USB Device claim their identity and capabilities



USB Descriptor



44 3e 48 00 69 00 00 00 00 00 12 00 00 00

12 01

00 02 00 00 00 40 07 13 63 01 00 01 01 02 03 01

QemuUSB

pipe_direction	'D>H' (device to h[...]
pid	IN
devaddr	0
devep	0
length	18

USBIn

Descriptor

length	18
type	Device

DeviceDescriptor

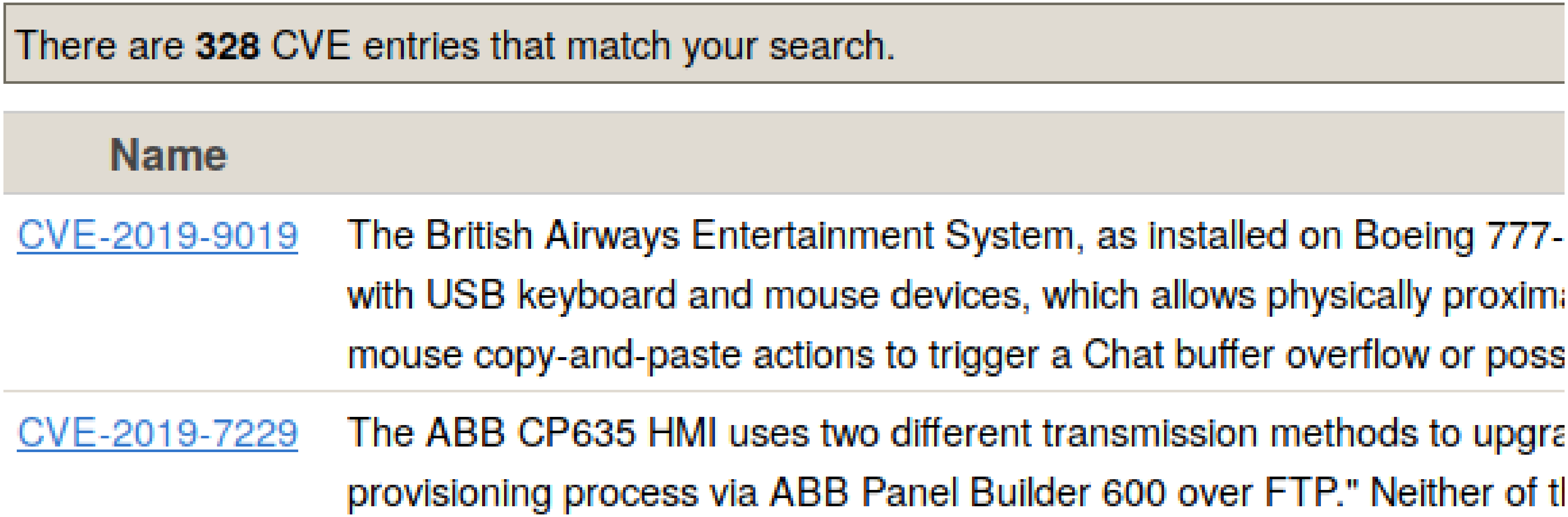
bcdUSB	0x0200
bDeviceClass	Base Class
bDeviceSubClass	0
bDeviceProtocol	0
bMaxPacketSize	64
idVendor	0x1307
idProduct	0x0163
bcdDevice	256
iManufacturer	1
iProduct	2
iSerialNumber	3
bNumConfigurations	1

Problems

Session locked with a password?

USB Attack Surface (Kernel space drivers)

Attack surface of USB



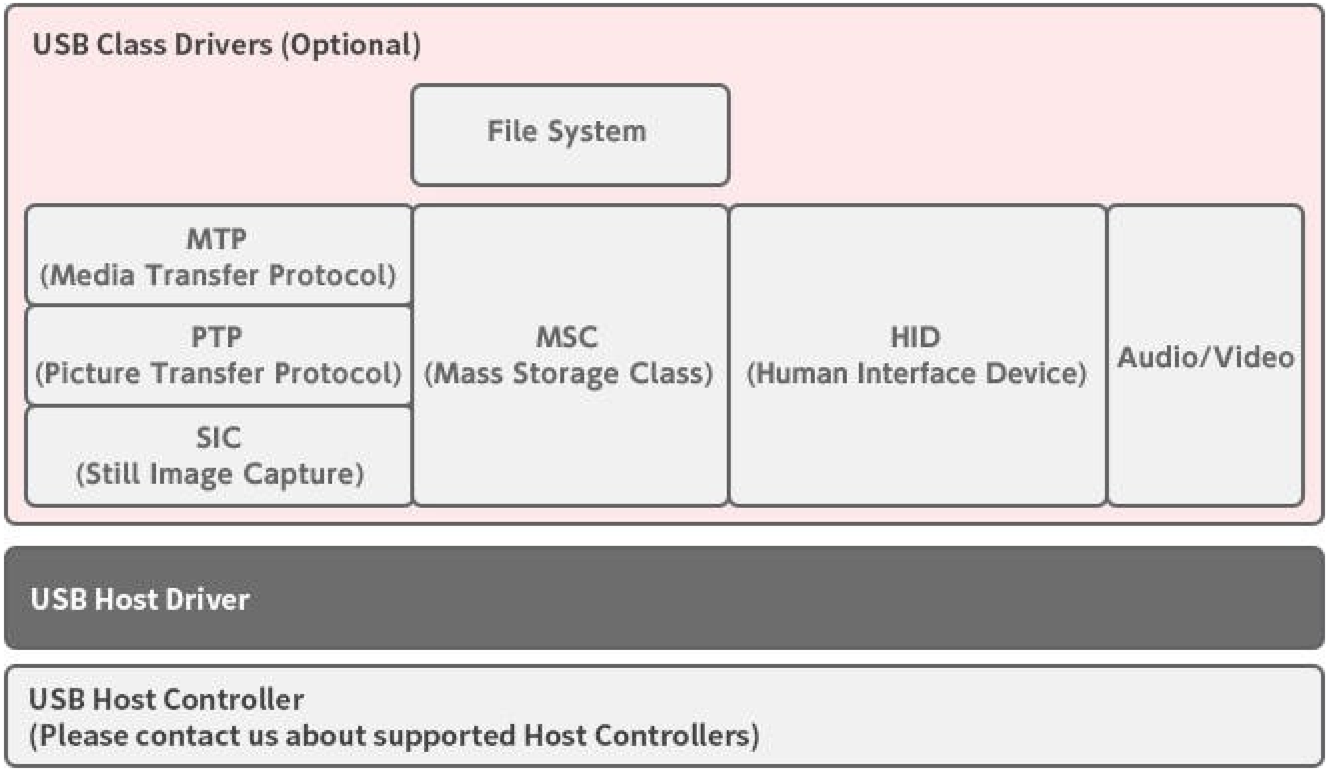
There are **328** CVE entries that match your search.

Name	
CVE-2019-9019	The British Airways Entertainment System, as installed on Boeing 777- with USB keyboard and mouse devices, which allows physically proxim mouse copy-and-paste actions to trigger a Chat buffer overflow or poss
CVE-2019-7229	The ABB CP635 HMI uses two different transmission methods to upgra provisioning process via ABB Panel Builder 600 over FTP." Neither of tl

USB without borders

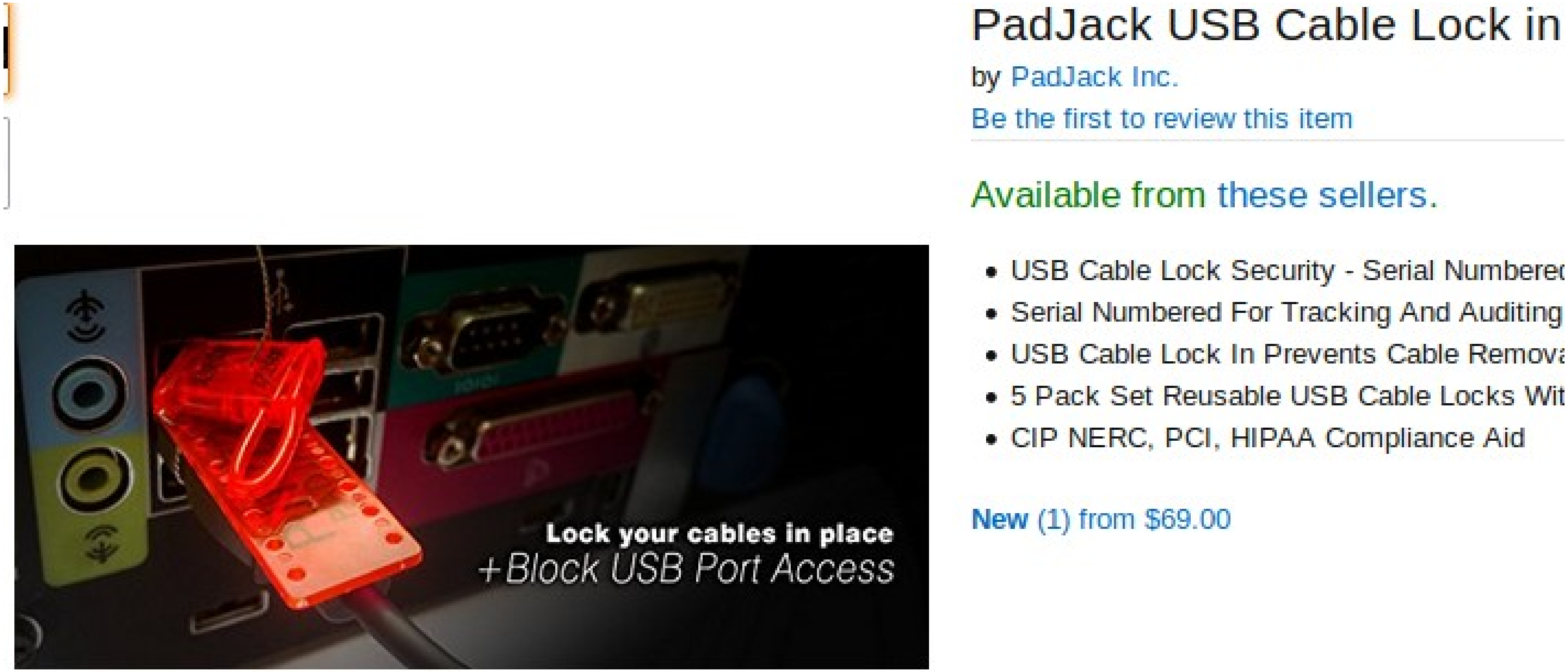
USB REQUEST OVER IP NETWORK

People expect USB to work



Other Solutions

Lock your USB Ports (hardware)



PadJack USB Cable Lock in

by PadJack Inc.

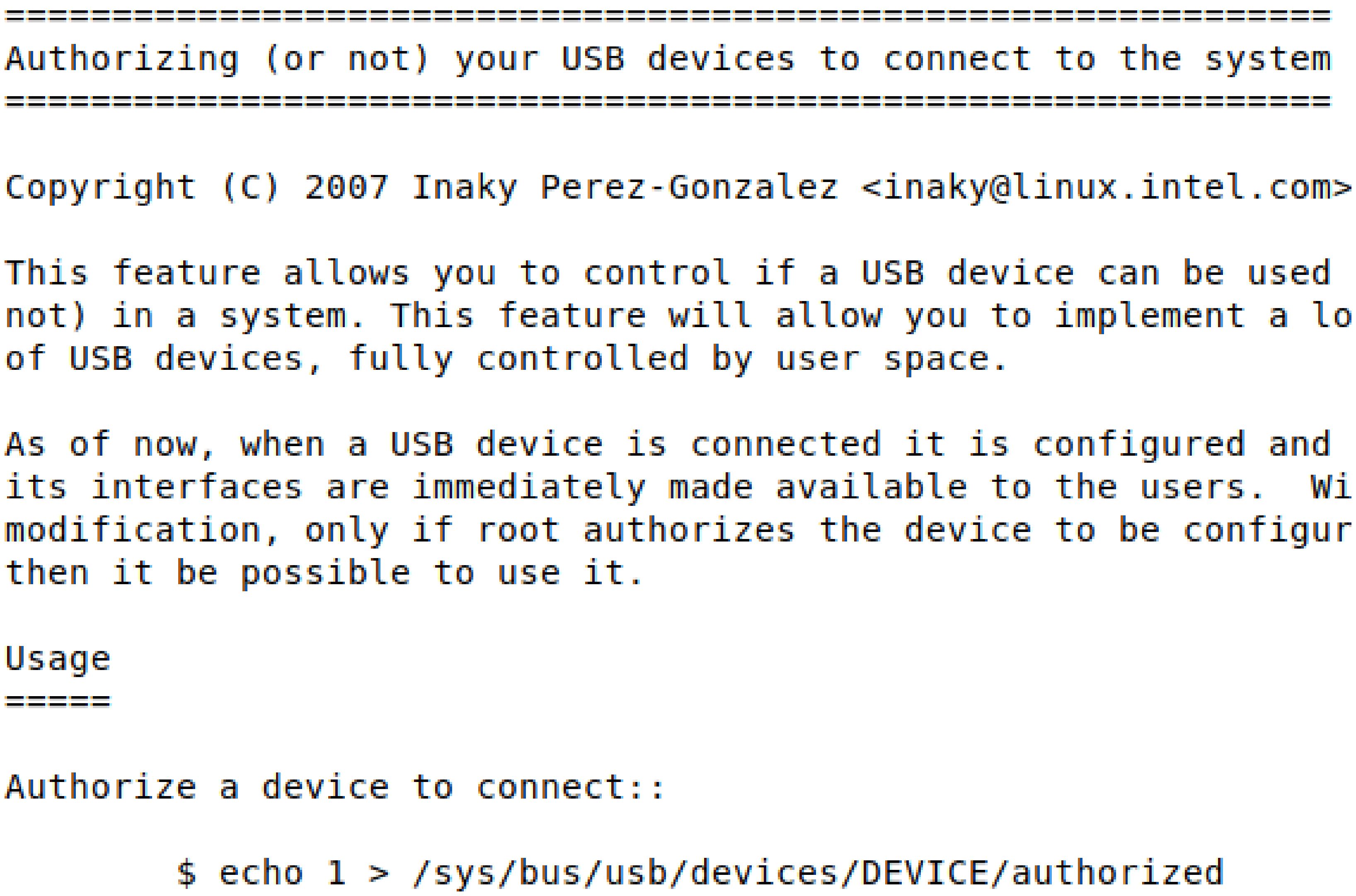
Be the first to review this item

Available from these sellers.

- USB Cable Lock Security - Serial Numbere
- Serial Numbered For Tracking And Auditing
- USB Cable Lock In Prevents Cable Remov
- 5 Pack Set Reusable USB Cable Locks Wit
- CIP NERC, PCI, HIPAA Compliance Aid

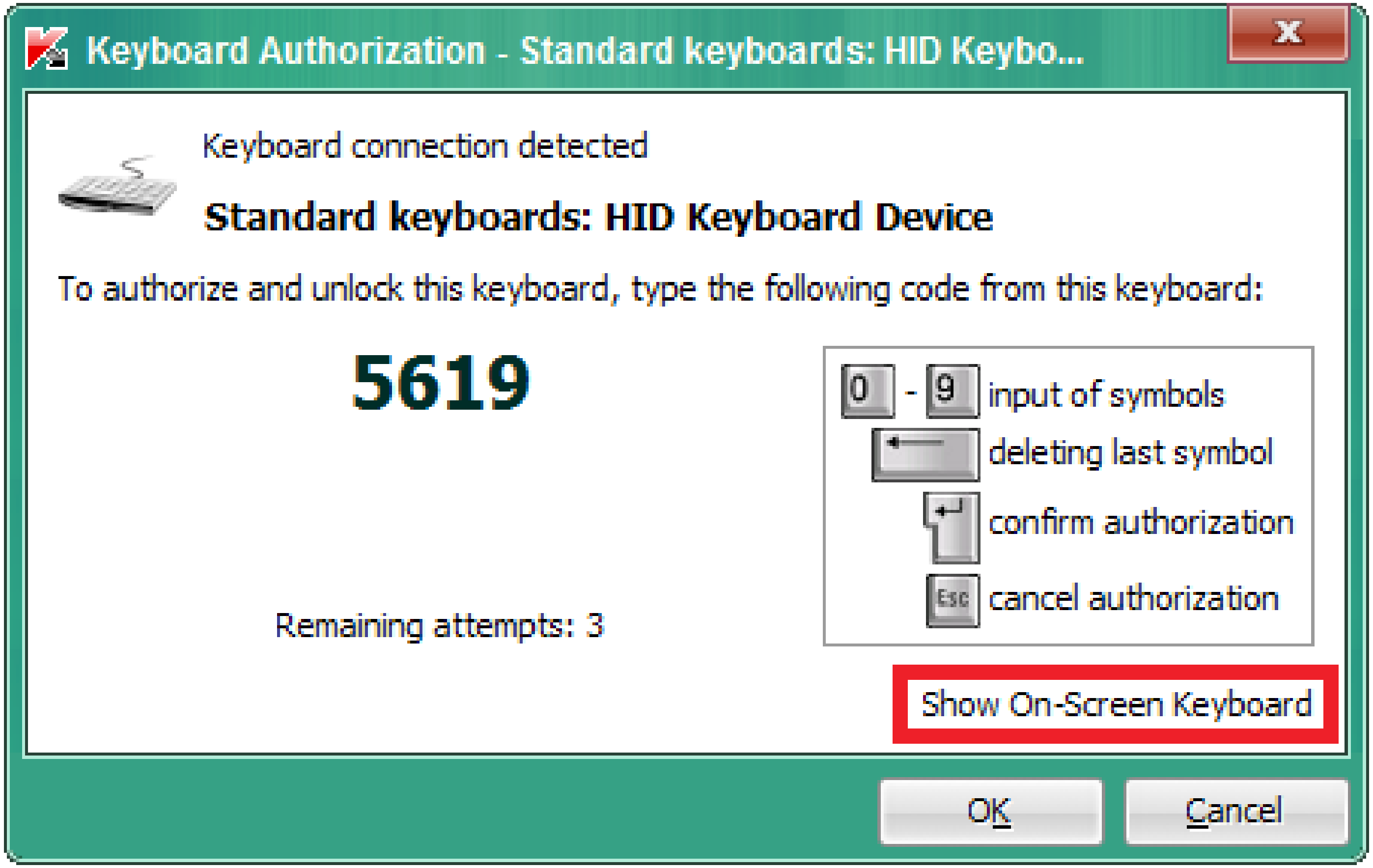
New (1) from $69.00

Lock your USB Ports (software)



```
==============================================================
Authorizing (or not) your USB devices to connect to the system
==============================================================

Copyright (C) 2007 Inaky Perez-Gonzalez <inaky@linux.intel.com>

This feature allows you to control if a USB device can be used
not) in a system. This feature will allow you to implement a lo
of USB devices, fully controlled by user space.

As of now, when a USB device is connected it is configured and
its interfaces are immediately made available to the users.  Wi
modification, only if root authorizes the device to be configur
then it be possible to use it.

Usage
=====

Authorize a device to connect::

        $ echo 1 > /sys/bus/usb/devices/DEVICE/authorized
```

Windows - Kaspersky



Keyboard Authorization - Standard keyboards: HID Keybo...

Keyboard connection detected

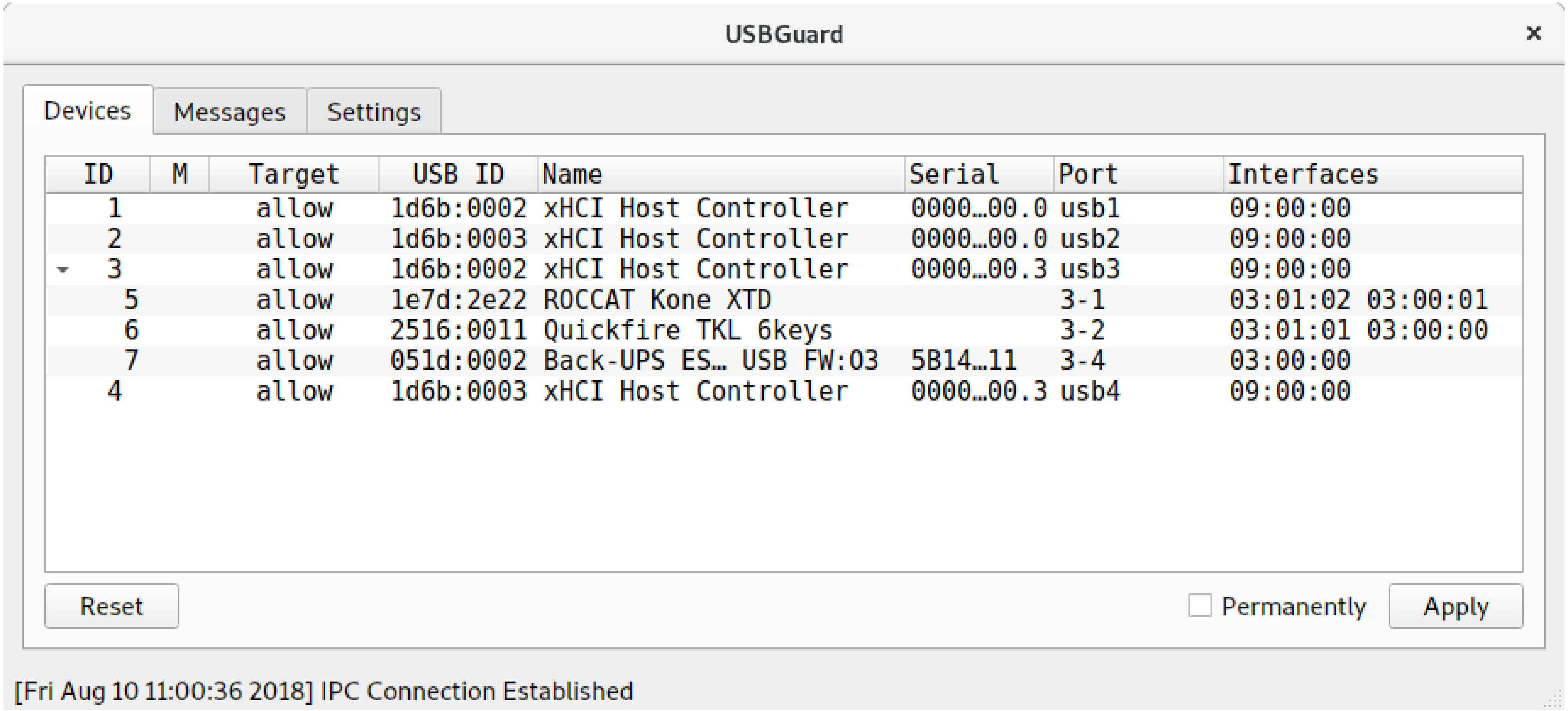
Standard keyboards: HID Keyboard Device

To authorize and unlock this keyboard, type the following code from this keyboard:

5619

Remaining attempts: 3

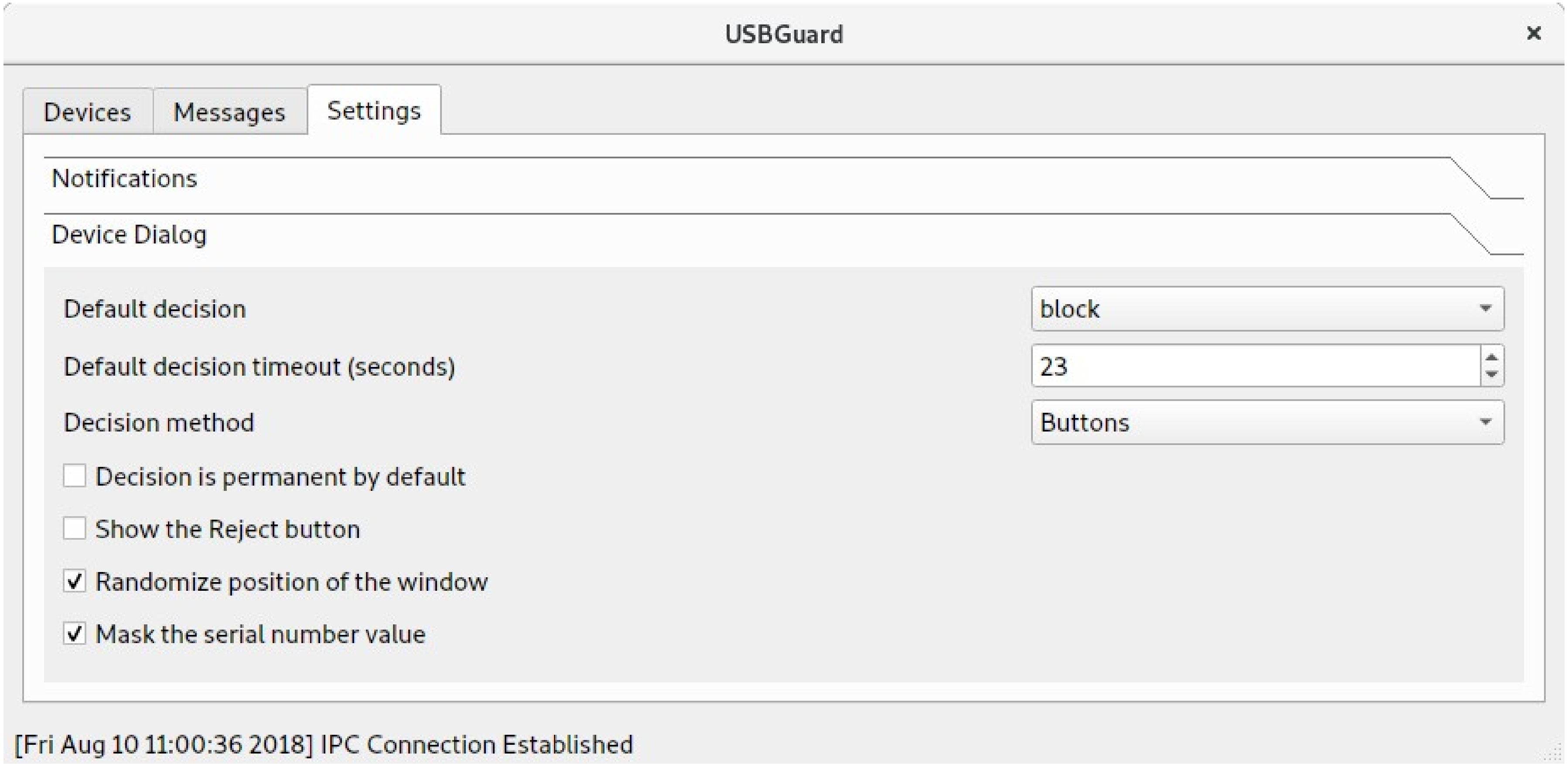
USBGuard - ~~Official Qt applet~~



ID	M	Target	USB ID	Name	Serial	Port	Interfaces
1		allow	1d6b:0002	xHCI Host Controller	0000…00.0	usb1	09:00:00
2		allow	1d6b:0003	xHCI Host Controller	0000…00.0	usb2	09:00:00
▾ 3		allow	1d6b:0002	xHCI Host Controller	0000…00.3	usb3	09:00:00
5		allow	1e7d:2e22	ROCCAT Kone XTD		3-1	03:01:02 03:00:01
6		allow	2516:0011	Quickfire TKL 6keys		3-2	03:01:01 03:00:00
7		allow	051d:0002	Back-UPS ES… USB FW:03	5B14…11	3-4	03:00:00
4		allow	1d6b:0003	xHCI Host Controller	0000…00.3	usb4	09:00:00

[Fri Aug 10 11:00:36 2018] IPC Connection Established

USBGuard - Official Qt applet



Default decision: block

Default decision timeout (seconds): 23

Decision method: Buttons

□ Decision is permanent by default

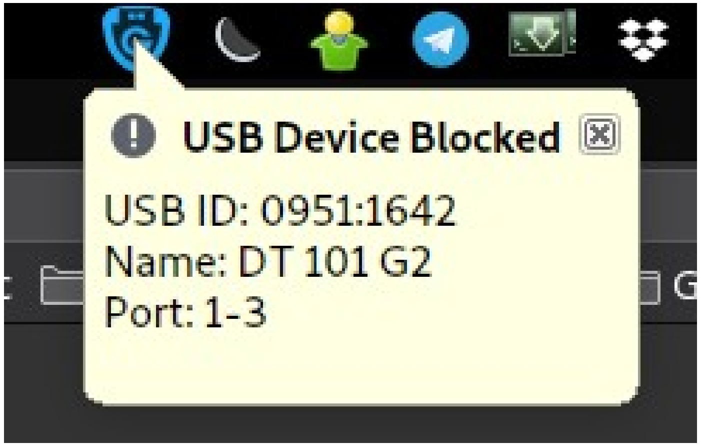
□ Show the Reject button

☑ Randomize position of the window

☑ Mask the serial number value

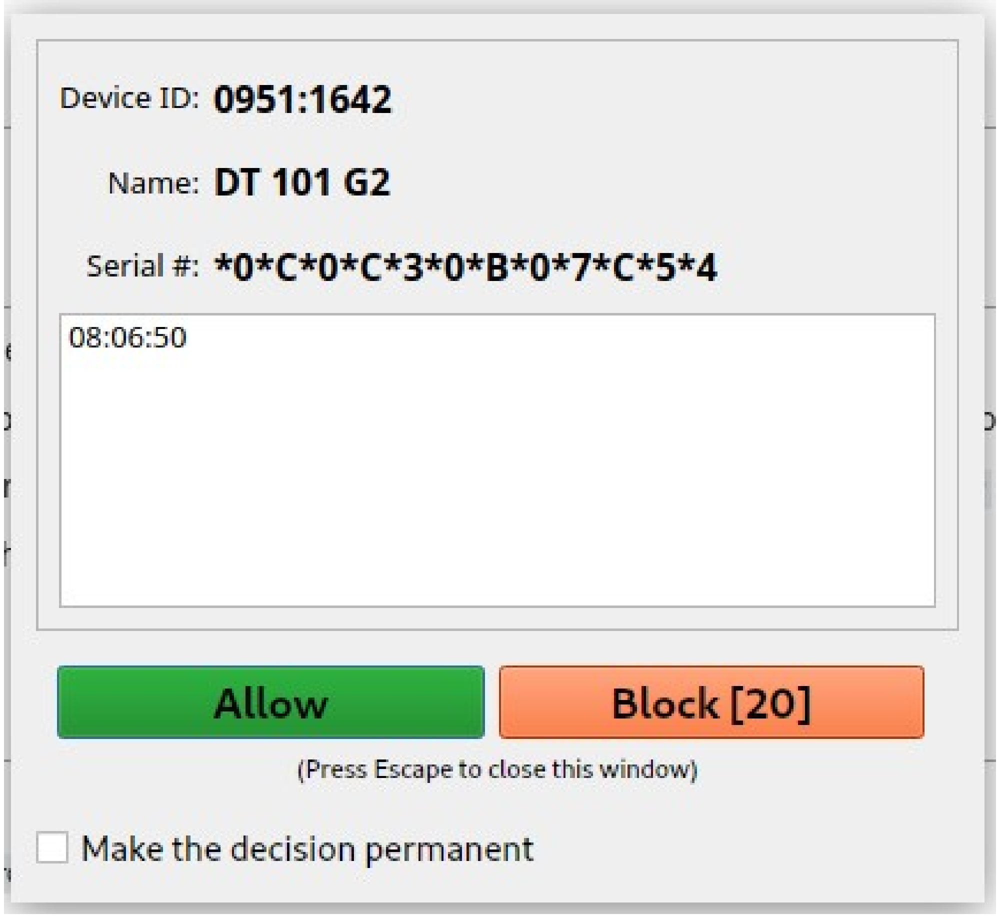
[Fri Aug 10 11:00:36 2018] IPC Connection Established

USBGuard - Official Qt applet



USB Device Blocked

USB ID: 0951:1642
Name: DT 101 G2
Port: 1-3



Device ID: 0951:1642

Name: DT 101 G2

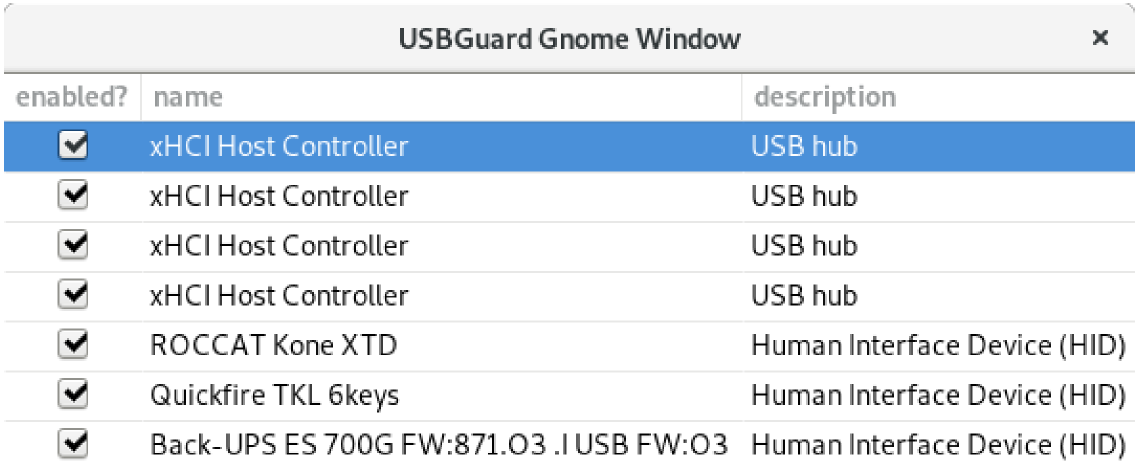
Serial #: *0*C*0*C*3*0*B*0*7*C*5*4

```
08:06:50
```

(Press Escape to close this window)

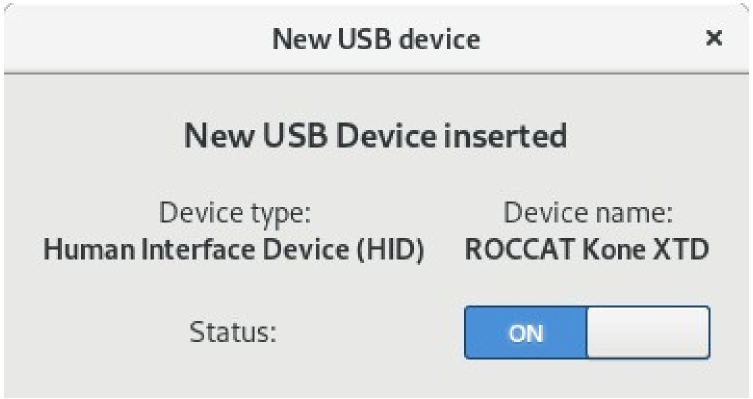
☐ Make the decision permanent

USBGuard GNOME



USBGuard Gnome Window

enabled?	name	description
☑	xHCI Host Controller	USB hub
☑	xHCI Host Controller	USB hub
☑	xHCI Host Controller	USB hub
☑	xHCI Host Controller	USB hub
☑	ROCCAT Kone XTD	Human Interface Device (HID)
☑	Quickfire TKL 6keys	Human Interface Device (HID)
☑	Back-UPS ES 700G FW:871.O3 .I USB FW:O3	Human Interface Device (HID)



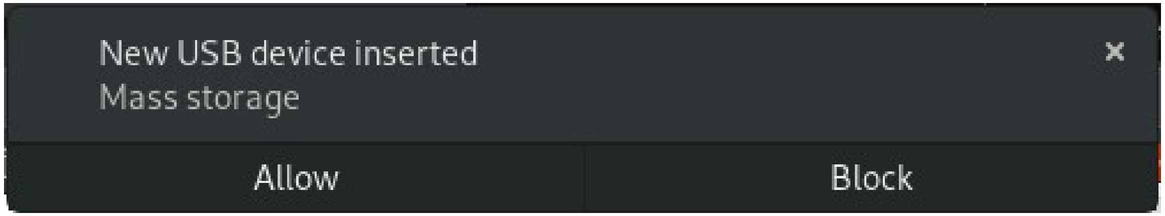
New USB device

New USB Device inserted

Device type: Human Interface Device (HID)

Device name: ROCCAT Kone XTD

Status: ON

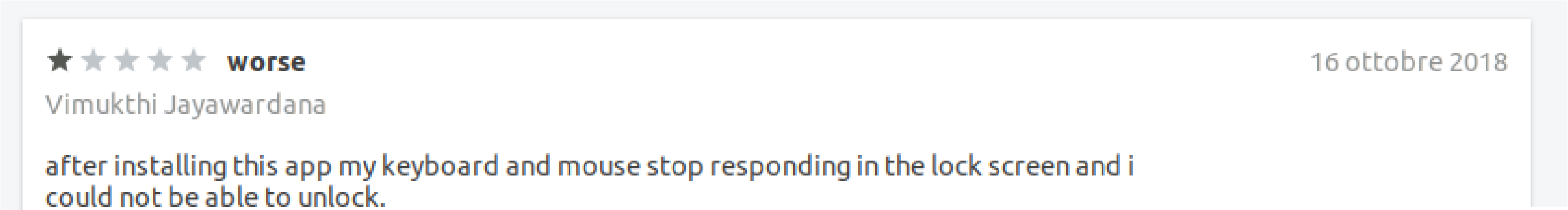


New USB device inserted
Mass storage

USBGuard

If there are already working USB protection, why start this project at all?

apt install usbguard



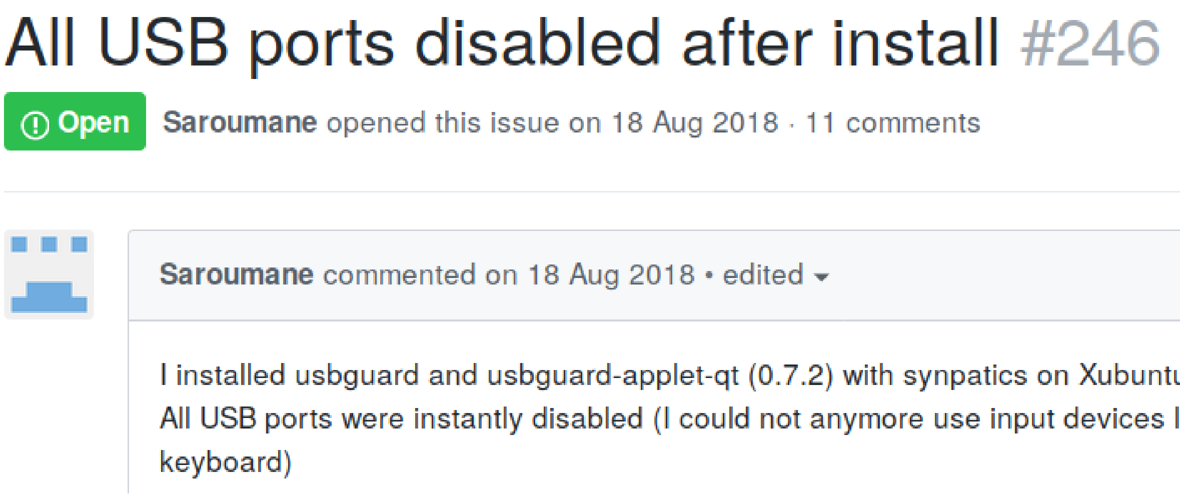
★☆☆☆☆ **worse**

Vimukthi Jayawardana

16 ottobre 2018

after installing this app my keyboard and mouse stop responding in the lock screen and i could not be able to unlock.

Was this review useful to you? Yes | No

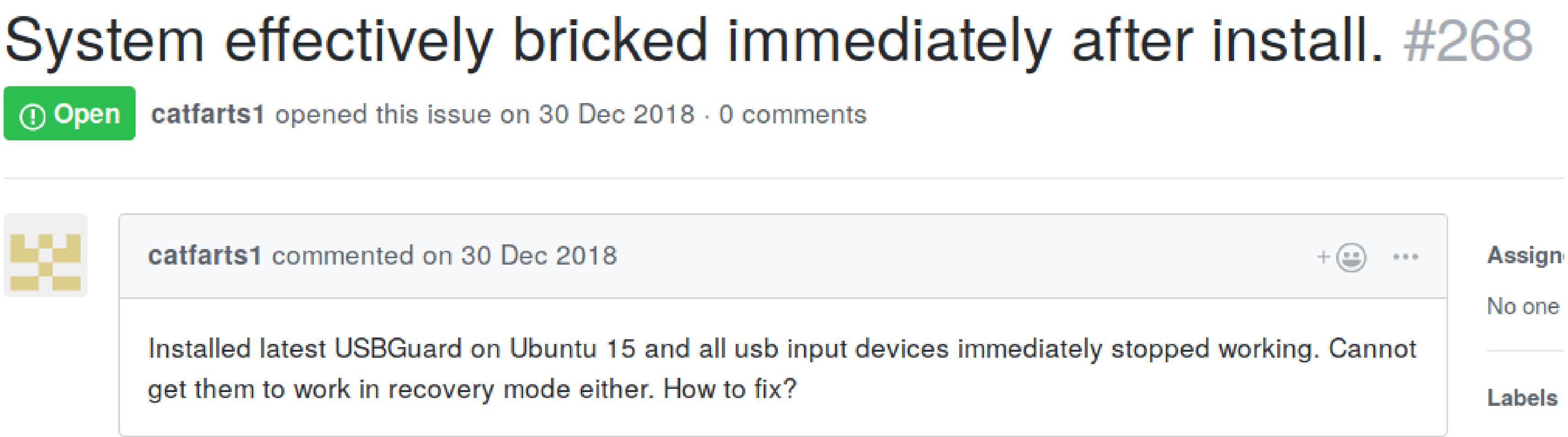


All USB ports disabled after install #246

ⓘ Open **Saroumane** opened this issue on 18 Aug 2018 · 11 comments

Saroumane commented on 18 Aug 2018 • edited ▾

I installed usbguard and usbguard-applet-qt (0.7.2) with synpatics on Xubuntu
All USB ports were instantly disabled (I could not anymore use input devices l
keyboard)



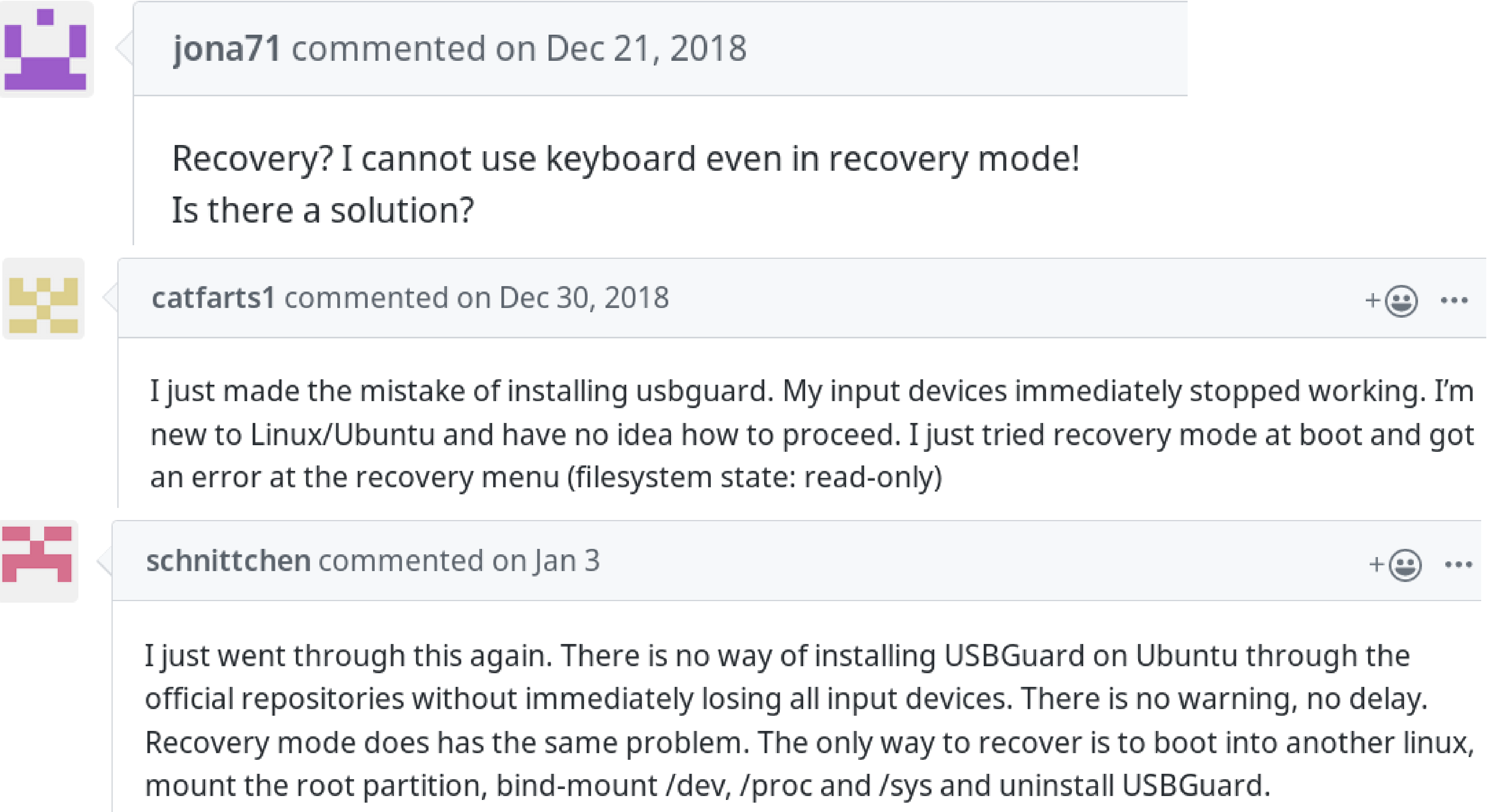
System effectively bricked immediately after install. #268

ⓘ Open **catfarts1** opened this issue on 30 Dec 2018 · 0 comments

catfarts1 commented on 30 Dec 2018

Installed latest USBGuard on Ubuntu 15 and all usb input devices immediately stopped working. Cannot get them to work in recovery mode either. How to fix?

apt install usbguard



jona71 commented on Dec 21, 2018

Recovery? I cannot use keyboard even in recovery mode!
Is there a solution?

catfarts1 commented on Dec 30, 2018

I just made the mistake of installing usbguard. My input devices immediately stopped working. I'm new to Linux/Ubuntu and have no idea how to proceed. I just tried recovery mode at boot and got an error at the recovery menu (filesystem state: read-only)

schnittchen commented on Jan 3

I just went through this again. There is no way of installing USBGuard on Ubuntu through the official repositories without immediately losing all input devices. There is no warning, no delay. Recovery mode does has the same problem. The only way to recover is to boot into another linux, mount the root partition, bind-mount /dev, /proc and /sys and uninstall USBGuard.

"Security at the expense of usability, comes at the expense of security."

-- AviD's Rule of Usability

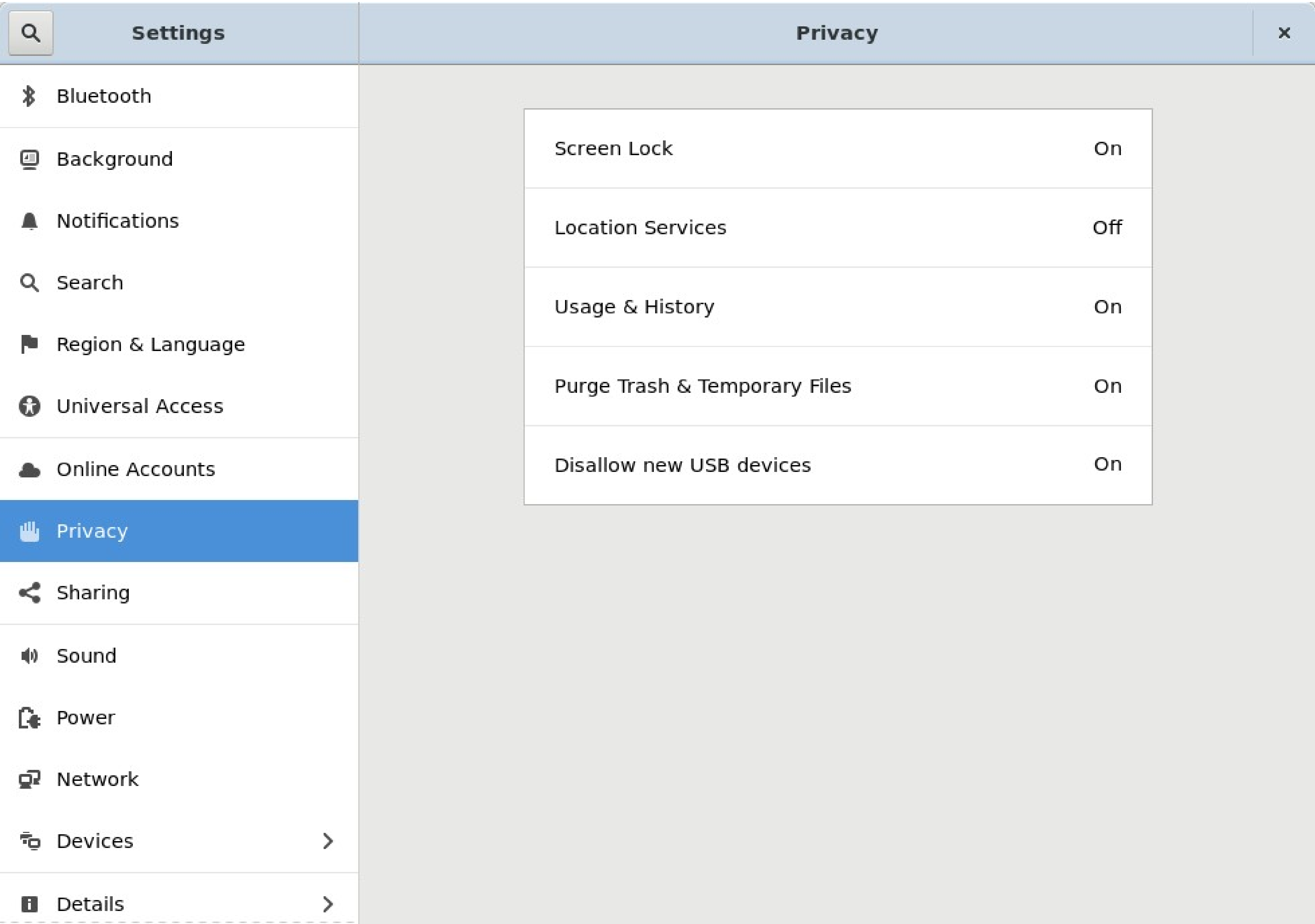
Our Solution

GNOME’s USB protection

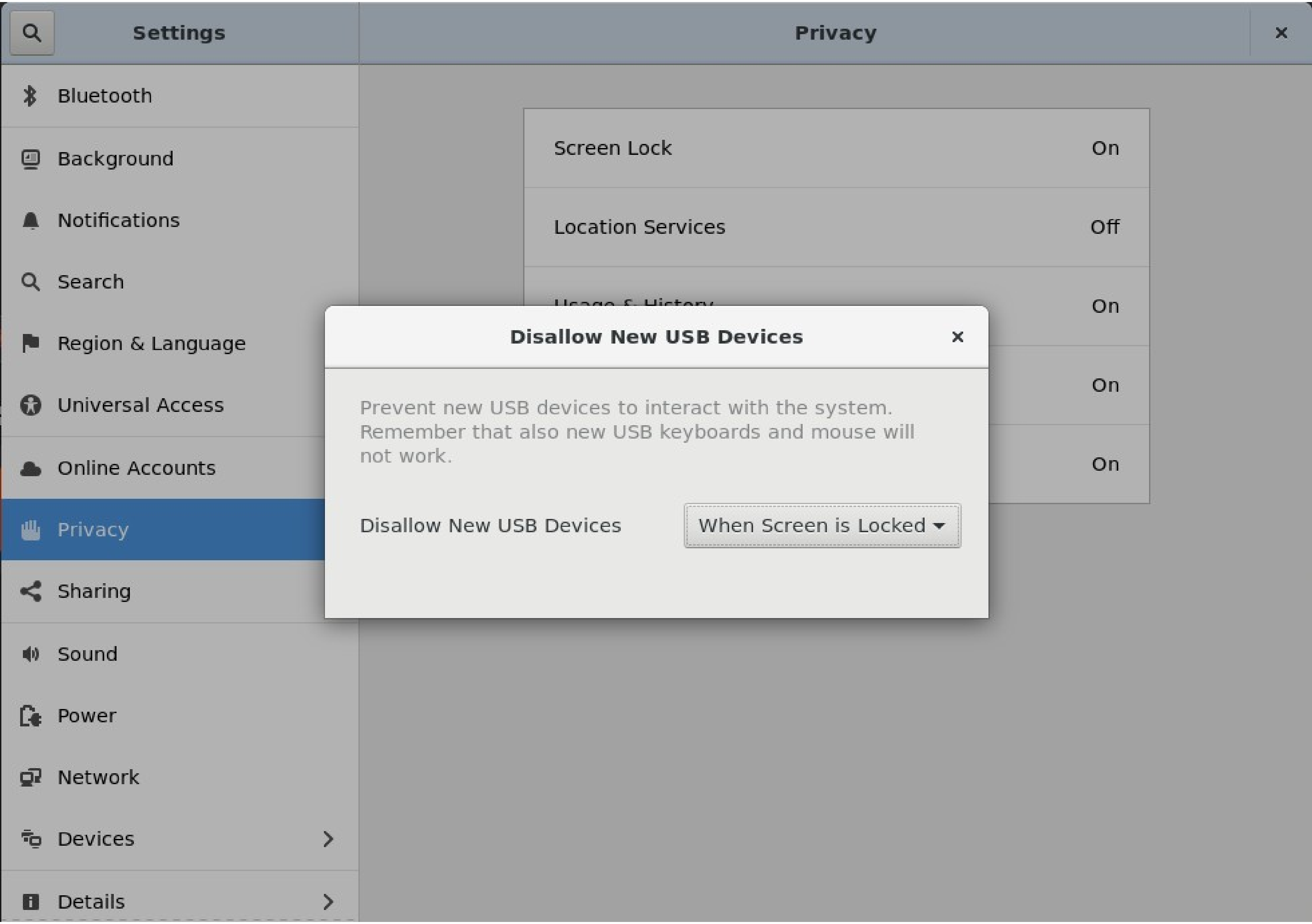
- Based on USB Guard
- Do not break existing behaviour
- Reduce attack surface as much as possible without the user noticing
- Tighten security later

Iterative Design

1. On / Off
2. Lockscreen
3. Keyboards
4. Unlocked Protection



Screen Lock	On
Location Services	Off
Usage & History	On
Purge Trash & Temporary Files	On
Disallow new USB devices	On



Screen Lock On

Location Services Off

Usage & History On

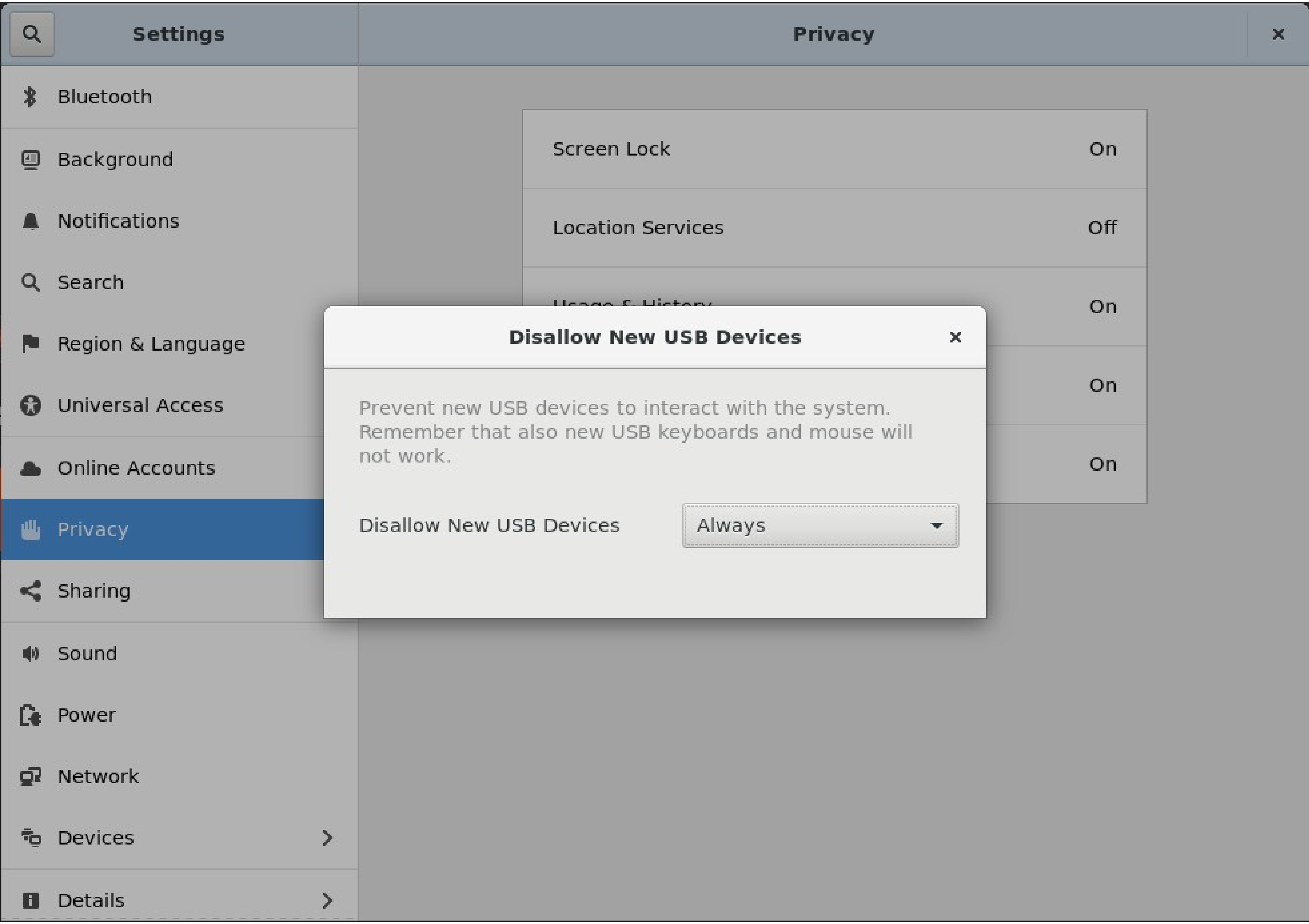
On

On

Disallow New USB Devices

Prevent new USB devices to interact with the system. Remember that also new USB keyboards and mouse will not work.

Disallow New USB Devices: When Screen is Locked

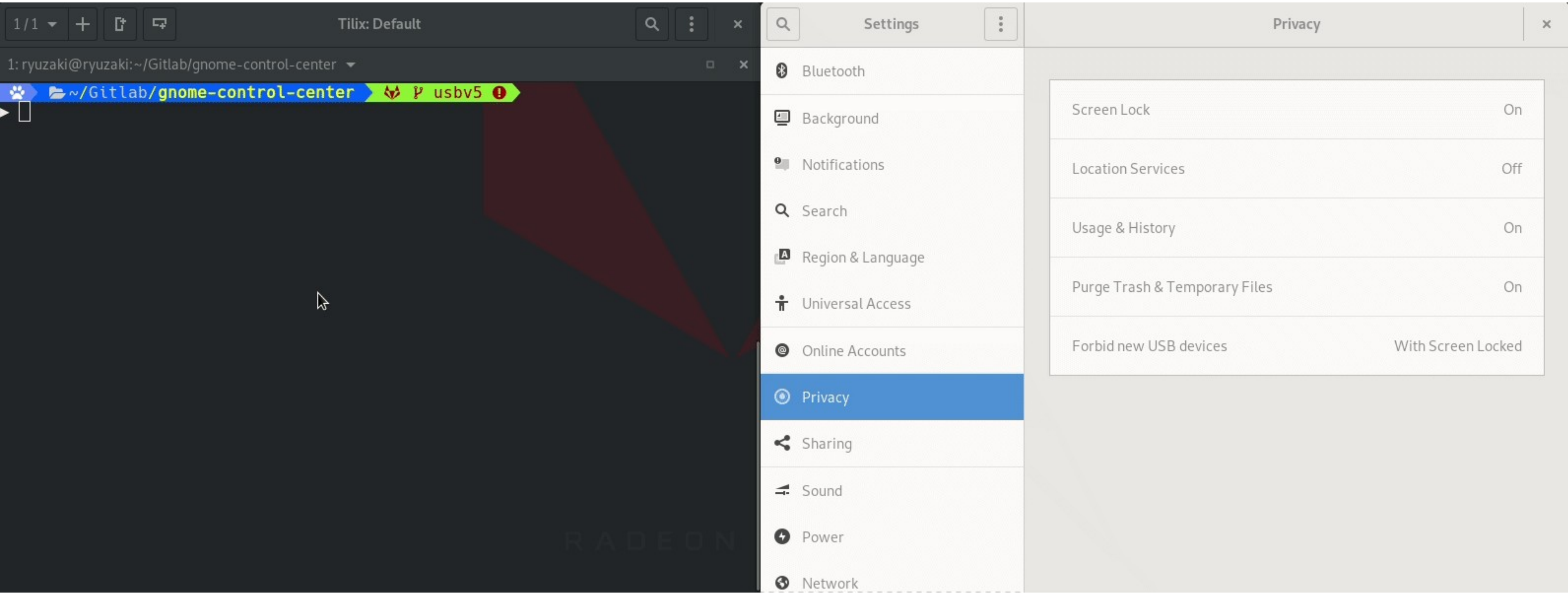


Disallow New USB Devices

Prevent new USB devices to interact with the system. Remember that also new USB keyboards and mouse will not work.

Disallow New USB Devices: Always

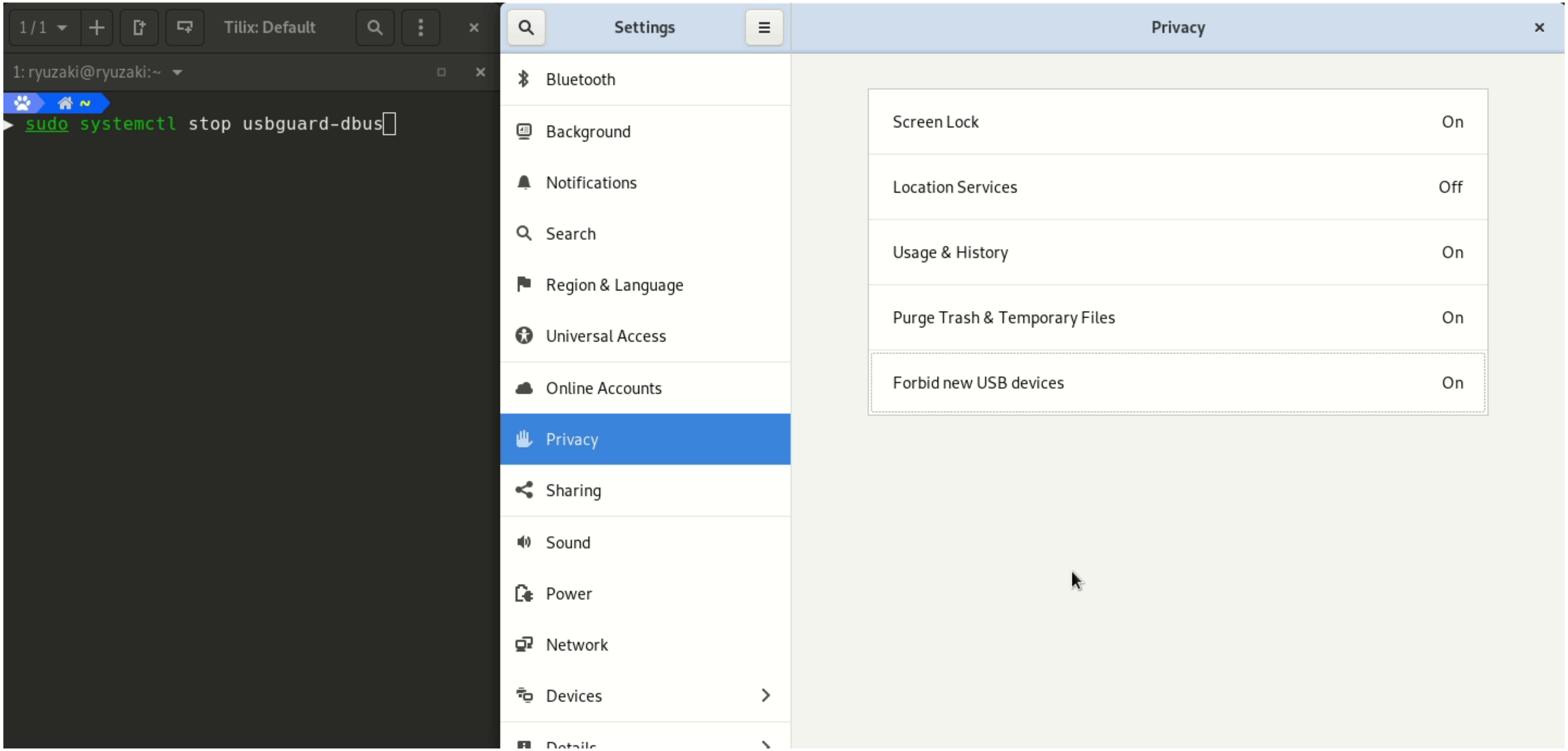
USB Protection - One of the first iterations



```
1: ryuzaki@ryuzaki:~/Gitlab/gnome-control-center
~/Gitlab/gnome-control-center  usbv5
>
```

Screen Lock	On
Location Services	Off
Usage & History	On
Purge Trash & Temporary Files	On
Forbid new USB devices	With Screen Locked

USB Protection - New single switch



```
sudo systemctl stop usbguard-dbus
```

Screen Lock On

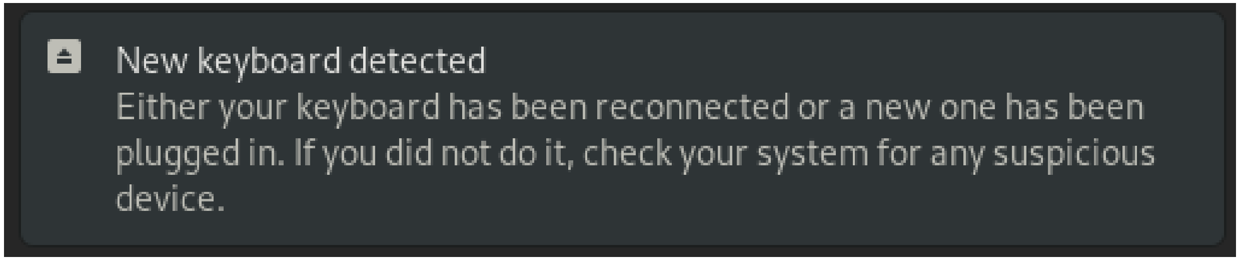
Location Services Off

Usage & History On

Purge Trash & Temporary Files On

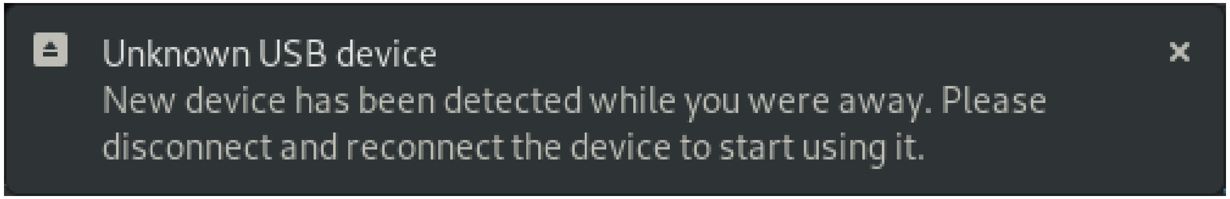
Forbid new USB devices On

USB Protection - Notification system



New keyboard detected

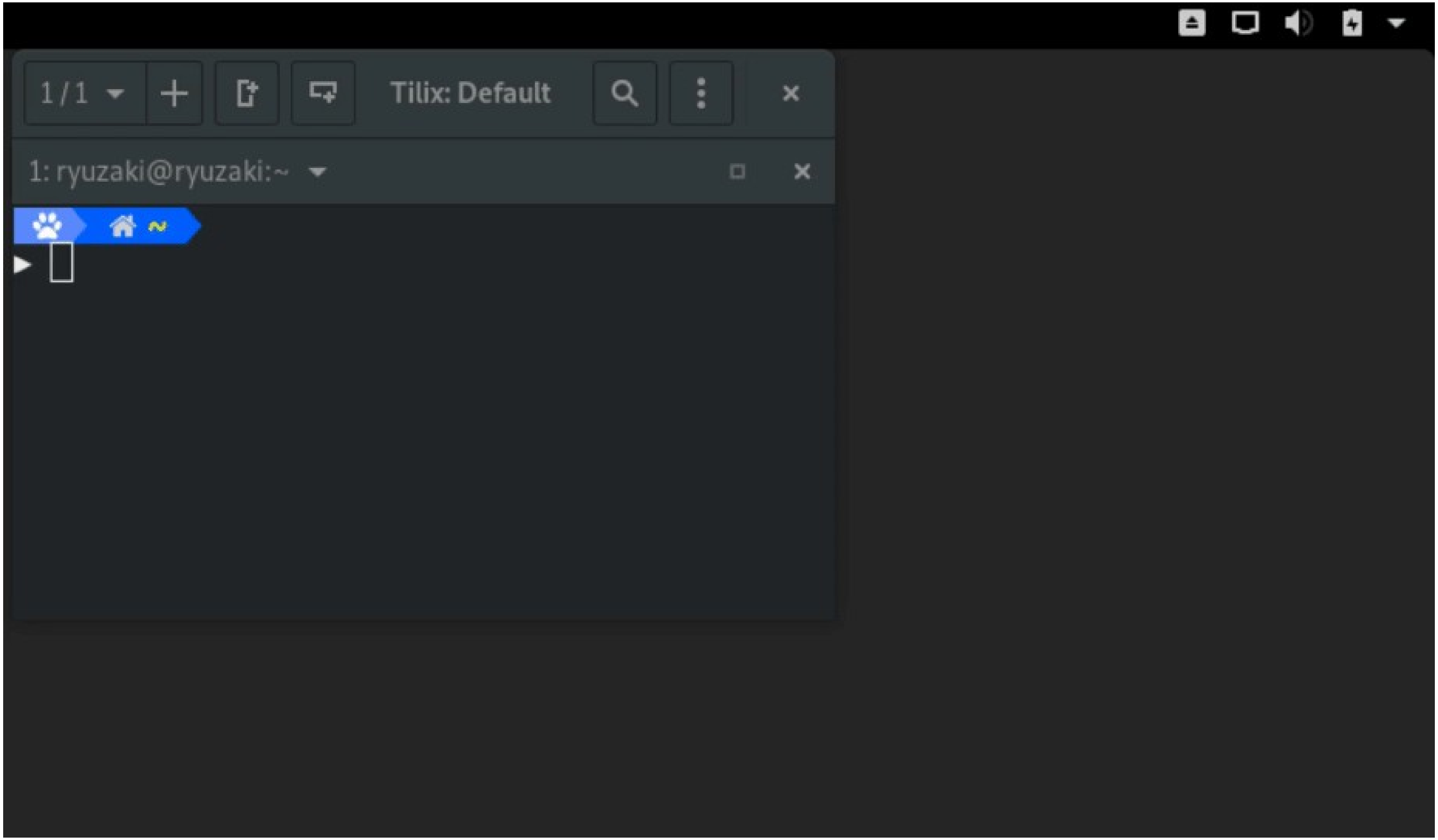
Either your keyboard has been reconnected or a new one has been plugged in. If you did not do it, check your system for any suspicious device.



Unknown USB device

New device has been detected while you were away. Please disconnect and reconnect the device to start using it.

GNOME Shell integration

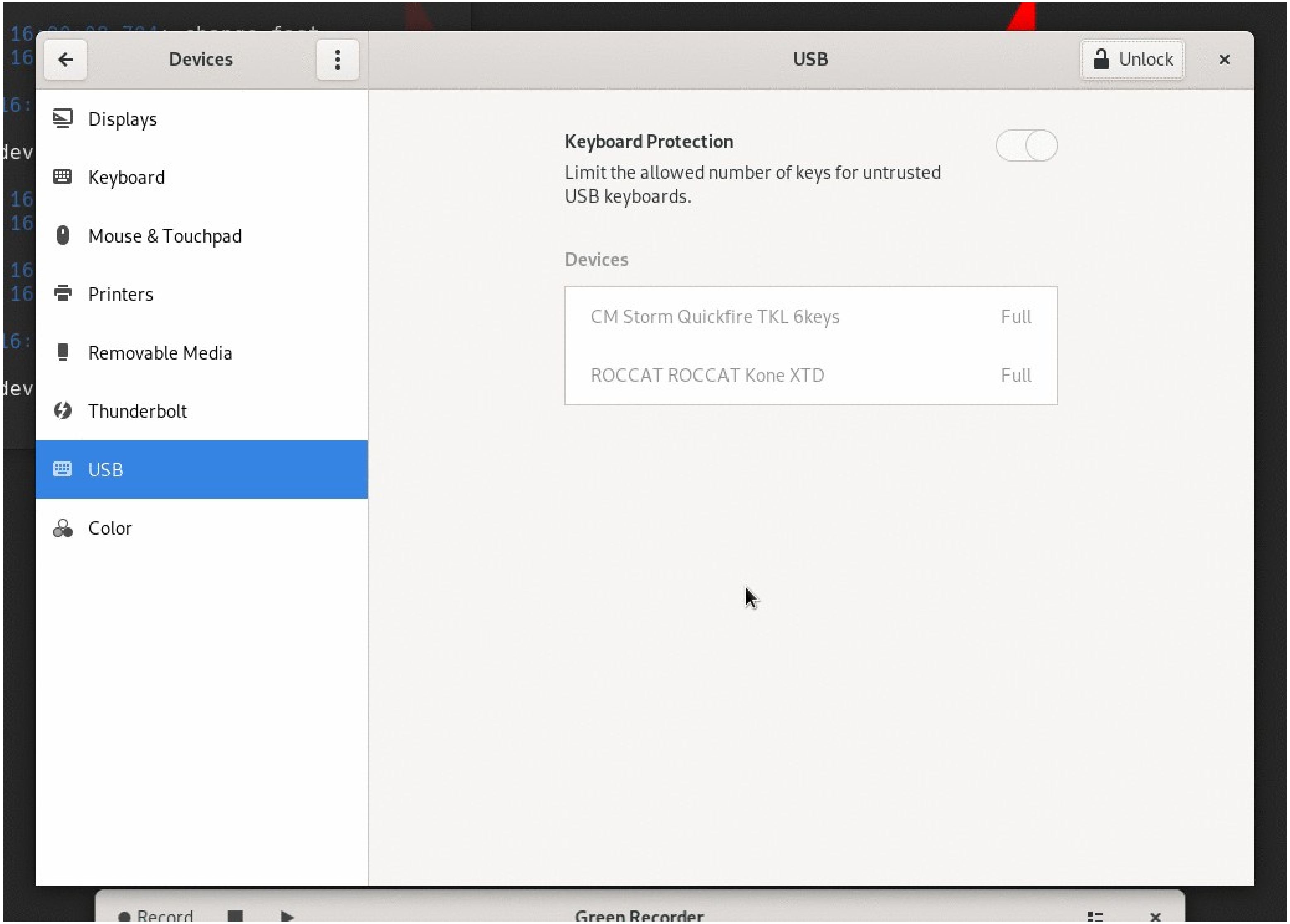


Cool, but this doesn’t protect us from the very same attack you showed at the beginning of this talk, does it?

USB protection when the session is unlocked

- Easy to block/allow everything
- Hard to selectively block malicious (or potentially malicious) devices without interfering with users workflow.

USB Keyboards Protection



Keyboard Protection

Limit the allowed number of keys for untrusted USB keyboards.

Devices

CM Storm Quickfire TKL 6keys	Full
ROCCAT ROCCAT Kone XTD	Full

Call for Action

Test the Patches!

Stage 1:

GNOME Settings Daemon !75
https://gitlab.gnome.org/GNOME/gnome-settings-daemon/merge_requests/75

Stage 2:

GNOME Shell !369
https://gitlab.gnome.org/GNOME/gnome-shell/merge_requests/369

Thank you

GNOME™

COLLABORA

Thank you!