Usable USB Protection

Ludovico de Nittis

Tobias Mueller
Background
USB was meant to be cheap

Why do you have to flip your USB cord three times before it works?

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?
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.

BY JASON PARKER  NOVEMBER 30, 2017 4:27 PM PST
USB was meant to be cheap

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
USB Device claim their identity and capabilities

![Device Descriptor Diagram]

- **Device Descriptor**
  - **Configuration**
    - **Interface**
      - **Endpoint**
    - **Configuration**
      - **Interface**
      - **Endpoint**
      - **Endpoint**
      - **Endpoint**
Problems
Session locked with a password?
USB Attack Surface (Kernel space drivers)
There are 328 CVE entries that match your search.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2019-9019</td>
<td>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</td>
</tr>
<tr>
<td>CVE-2019-7229</td>
<td>The ABB CP635 HMI uses two different transmission methods to upgra provisioning process via ABB Panel Builder 600 over FTP.&quot; Neither of t</td>
</tr>
</tbody>
</table>
USB without borders
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 Numbered
- Serial Numbered For Tracking And Auditing
- USB Cable Lock In Prevents Cable Removal
- 5 Pack Set Reusable USB Cable Locks With
- 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 (or not) in a system. This feature will allow you to implement a lot 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. With modification, only if root authorizes the device to be configurable 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 Keyboard Device

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

Show On-Screen Keyboard
### USBGuard - Official Qt Applet

The USBGuard application is shown with a table of devices and settings. The table includes columns for ID, M (mode), Target, USB ID, Name, Serial, Port, and Interfaces. The table displays various USB devices, such as xHCI Host Controllers and other USB devices with specific serial numbers and port assignments.

**Table Example**

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

**Application Details**

- **Reset** button
- **Permanently** checkbox
- **Apply** button

**Log Entries**

- [Fri Aug 10 11:00:36 2018] IPC Connection Established
USBGuard - Official Qt applet
USBGuard GNOME
USBGuard

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

Vimukthi Jayawardana

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

Saroumane opened this issue on 18 Aug 2018 • 11 comments

I installed usbguard and usbguard-applet-qt (0.7.2) with synpatics on Xubuntu 17.10. All USB ports were instantly disabled (I could not anymore use input devices like keyboard)

System effectively bricked immediately after install.  #268

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
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
USB Protection - New single switch
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

<table>
<thead>
<tr>
<th>Devices</th>
<th>Keyboard Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit the allowed number of keys for untrusted USB keyboards.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Devices</th>
<th>Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM Storm Quickfire TKL 6keys</td>
<td></td>
</tr>
<tr>
<td>ROCCAT ROCCAT Kone XTD</td>
<td></td>
</tr>
</tbody>
</table>
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
Thank you!