USB attacks explained

Krzysztof Opasiak

SAMSUNG

Samsung R&D Institute Poland

LVEE

Linux Vacation / Eastern Europe

Agenda

What is USB about?

Plug and Play

USB host attacks

USB traffic analysis + modification

USB device attacks

Summary

Q & A

What is USB about?

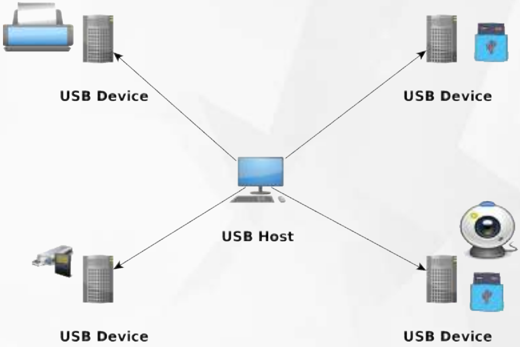
LVEE

Linux Vacation / Eastern Europe

What is USB about?

It is about providing services!

- **Storage**
- **Printing**
- **Ethernet**
- **Camera**
- **Any other**



What USB device is?

- **Piece of hardware for USB communication**
- **USB protocol implementation**
- **Some useful protocol implementation**
- **Piece of hardware/software for providing desired functionality**

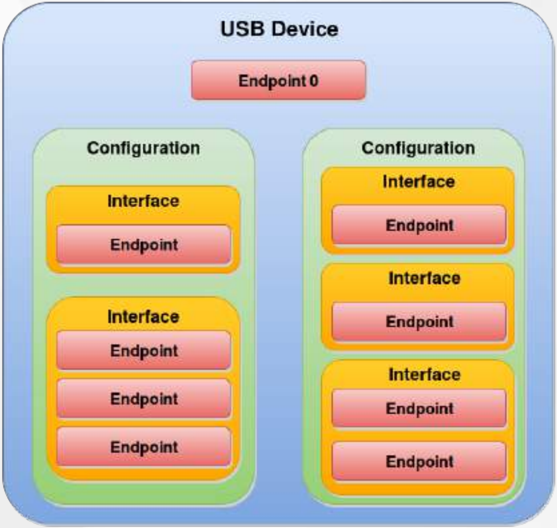
Endpoints…

- Device may have up to 31 endpoints (incl. ep0)
- Each of them gets a unique Endpoint address
- Endpoint 0 may transfer data in both directions
- All other endpoints may transfer data only in one direction:

IN	Data transfer from device to host
OUT	Data transfer from host to device

- Control, Bulk, Interrupt, Isochronous

USB device

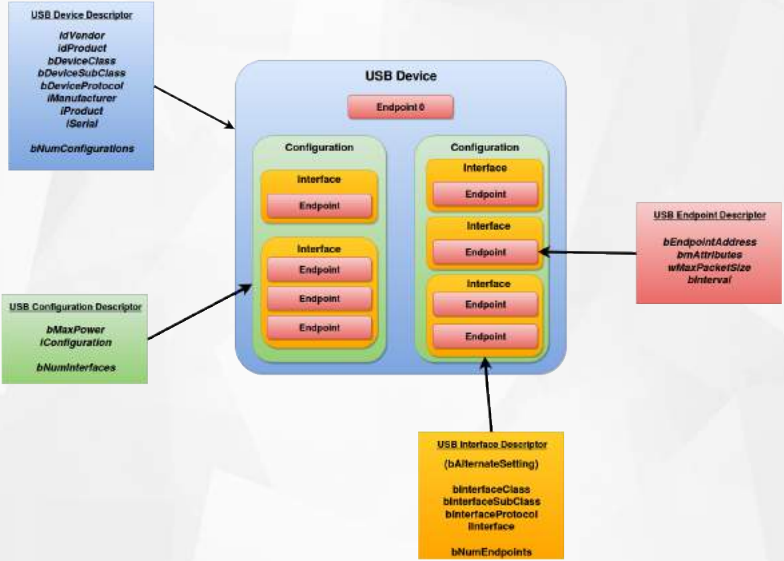

USB Device
Endpoint 0
Configuration
Interface
Endpoint
Interface
Endpoint
Endpoint
Endpoint
Configuration
Interface
Endpoint
Interface
Endpoint
Interface
Endpoint
Endpoint

Plug and Play

Step by step

- **Plug in device**
- **Detect Connection**
- **Set address**
- **Get device info**
- **Choose configuration**
- **Choose drivers for interfaces**
- **Use it ;)**

USB descriptors



USB Device Descriptor

idVendor
idProduct
bDeviceClass
bDeviceSubClass
bDeviceProtocol
iManufacturer
iProduct
iSerial

bNumConfigurations

USB Device

Endpoint 0

Configuration

Interface

Endpoint

Interface

Endpoint

Endpoint

Endpoint

Configuration

Interface

Endpoint

Interface

Endpoint

Interface

Endpoint

Endpoint

USB Endpoint Descriptor

bEndpointAddress
bmAttributes
wMaxPacketSize
bInterval

USB Configuration Descriptor

bMaxPower
iConfiguration

bNumInterfaces

USB Interface Descriptor

(bAlternateSetting)

bInterfaceClass
bInterfaceSubClass
bInterfaceProtocol
iInterface

bNumEndpoints

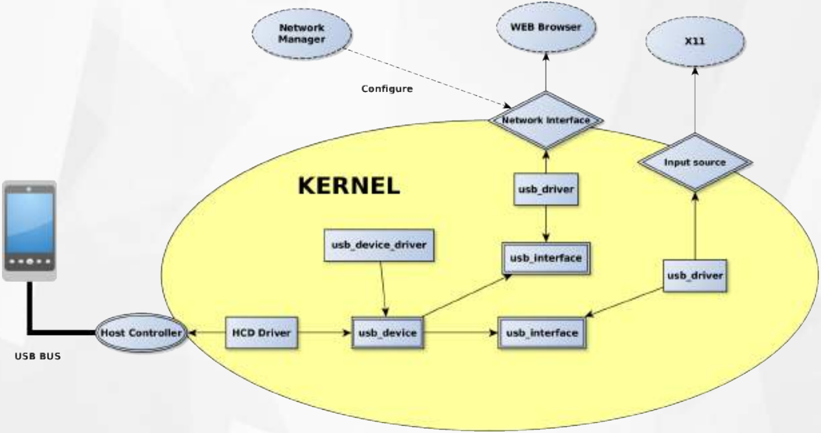
What USB driver really is?

- **Piece of kernel code**
- **Usually provides something to userspace (network interface, tty, etc.)**
- **Implementation of some communication protocol**

How to choose a suitable driver?

- *struct usb_driver*
- **When device needs special handling:**
    - Using VID, PID and interface id
    - Driver probe()s for each interface in device that match VID and PID
- **When driver implements some well defined, standardized protocol**
    - Using bInterfaceClass, bInterfaceSubClass etc.
    - Driver probe() for each interface which has suitable identity
    - No matter what is the VID and PID
    - Driver will not match if interface hasn't suitable class

Big picture


Network Manager
WEB Browser
X11
Configure
Network interface
Input source
KERNEL
usb_driver
usb_device_driver
usb_interface
usb_driver
Host Controller
HCD Driver
usb_device
usb_interface
USB BUS

What's next?

- **We have the driver which provides something to userspace**
- **So what's next?**

What's next?

- **We have the driver which provides something to userspace**
- **So what's next?**
- **It depends on interface type:**
  - Network devices - Network manager should handle new interface setup
  - Pendrives, disks etc - automount service should mount new block device
  - Mouse, keyboard - X11 will start listening for input events
  - And many many other things are going to be handled **AUTOMATICALLY**
  - without any user action…

USB host attacks

AutoRun…[7]

- ***autorun.inf*** **file**
- **May be used to automatically run program when medium is inserted**
- **Now considered as a subset of AutoPlay**
- **GNOME also has AutoPlay-like capabilities**
- **Since Windows 7 disabled for USB device**

```
[autorun]
open=malware.exe
icon=my_icon.ico
label=Awesome Program
```

Stuxnet[8, 7]

- **Simens PLC controllers**
- **USB pendrives**
- **LNK Vulnerability (CVE-2010-2568)**
- **Vulnerability in icon rendering software**
- **Requires user action (list folder)**

USB protocol impl. attacks[1]

- **USB protocol layer**
- **May target USB core or particular driver**
- **Vulnerabilities in:**
  - descriptors parsing
  - particular protocol implementation
- **Popular some time ago**
- **Example: PSGroove**
- **Now quite hard to achieve (at least on recent Linux kernels)**
- **Thank you Johan Hovold!**

USB fuzzers

- **HW:**
  - facedancer[3]

- **Software:**
  - umap[9]

My beautiful tablet

BadUSB attack scenario[5]

- **User connects hacked device**
- **Device looks like pendrive, tablet…**
- **But sends descriptor taken from some keyboard**
- **And implements HID protocol**
- **Kernel creates new input source**
- **and X11 just starts using it**

USB traffic analysis + modification

LVEE

Linux Vacation / Eastern Europe

Keyboard MITM[4, 10]

- **Simple MITM device which logs key strokes**
- **Usually can be found in some public spaces (libraries, schools, etc.)**
- **It's nothing new, it existed also in PS/2 times**

Bad USB 2.0[6]

- **Both USB device and USB MITM for HID**
- **Hidden communication channel using set report**
- **Allows not only to execute the code but also get the result**
- **Doesn't generate network traffic**

USB device attacks

LVEE

Linux Vacation / Eastern Europe

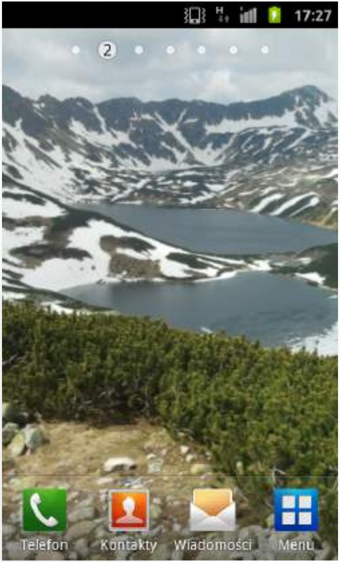
Charging stations from Poland

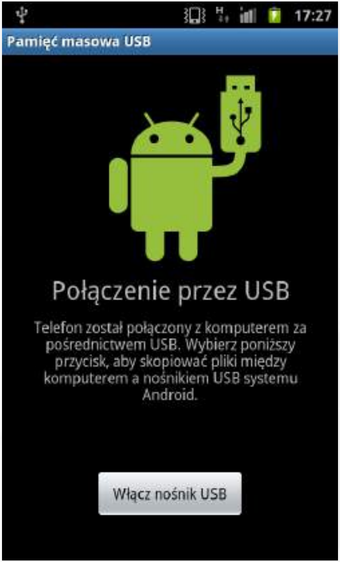
Source : dziennikwschodni.pl

Data stealing

- **USB is universal connector used for charging**
- **but it's still fully functional USB!**
- **So it may be used to transfer files to PC**
- **and you never know what is inside your charger!**

Difference on smartphone screen (v2.3.6)





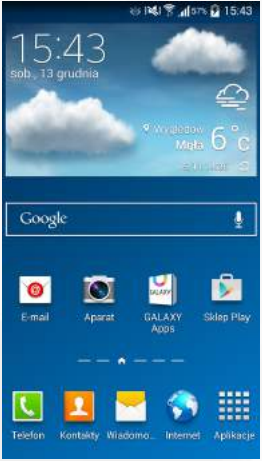
Pamięć masowa USB

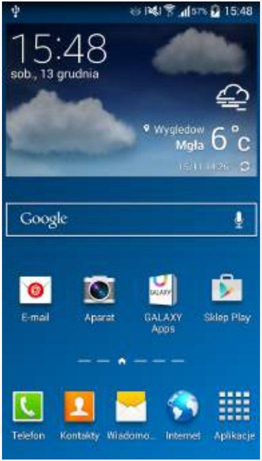
Połączenie przez USB

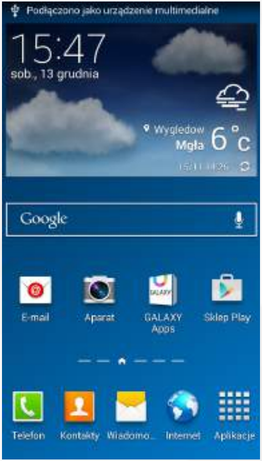
Telefon został połączony z komputerem za pośrednictwem USB. Wybierz poniższy przycisk, aby skopiować pliki między komputerem a nośnikiem USB systemu Android.

Włącz nośnik USB

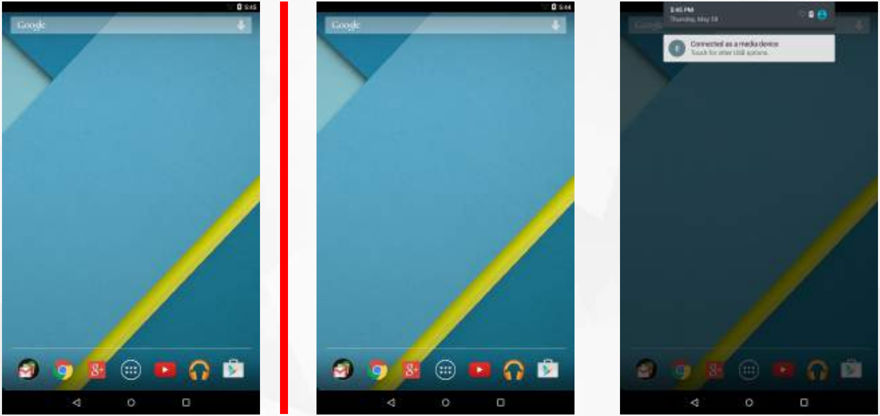
Difference on smartphone screen (v4.4.2)






Podłączono jako urządzenie multimedialne

Difference on smartphone screen (v5.1)



Connected as a media device
Touch for other USB options

ADB resource exhaustion[2]

- **Android access for developers**
- **Comes disabled by default**
- **"Enable and forget"**
- **Root access to old android phone**
- **Bug in ADB -- no setuid() return code check**

Summary

- **USB is everywhere**
- **Host automatically serves all connected devices**
- **The device introduce itself using USB descriptors**
- **There is no relation between physical outfit and descriptors**
- **USB attacks are real and they are evolving**
- **Always check return codes!**

Q & A

LVEE

Linux Vacation / Eastern Europe

Thank you!

Krzysztof Opasiak

Samsung R&D Institute Poland

+48 605 125 174
k.opasiak@samsung.com

References I

[1] Darrin Barral and David Dewey. ``"Plug and Root," the USB Key to the Kingdom". In: *Black Hat*. Las Vegas, NV, USA, 2005. URL: https://www.blackhat.com/presentations/bh-usa-05/BH_US_05-Barrall-Dewey.pdf.

[2] *CVE-2017-5554*. Jan. 2017. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5554.

[3] *FaceDancer21 (USB Emulator/USB Fuzzer)*. URL: https://int3.cc/products/facedancer21.

References II

[4] *Hardware keyloggers discovered at public libraries*. URL: https://nakedsecurity.sophos.com/2011/02/14/hardware-keyloggers-discovered-public-libraries/.

[5] Sascha Krissler Karsten Nohl and Jakob Lell. ``BadUSB -- On accessories that turn evil". In: *Black Hat*. Las Vegas, NV, USA, 2014. URL: https://srlabs.de/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf.

[6] David Kierznowski. *BadUSB 2.0: USB man in the middle attacks*. Tech. rep. Royal Holloway University of London, Apr. 2016.

References III

[7] John Larimer. ``Beyond Autorun: Exploiting vulnerabilities with removable storage". In: *Black Hat 2011*. Las Vegas, NV, USA, 2011.

[8] Liam O Murchu Nicolas Falliere and Eric Chien. *W32.Stuxnet Dossier*. Feb. 2011. URL: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[9] *umap: The USB host security assessment tool*. URL: https://github.com/nccgroup/umap.

References IV

[10] *US school expels pupils for using hardware keyloggers to change grades*. Feb. 2004. URL: http://www.techworld.com/news/security/us-school-expels-pupils-for-using-hardware-keyloggers-change-grades-3500558/.