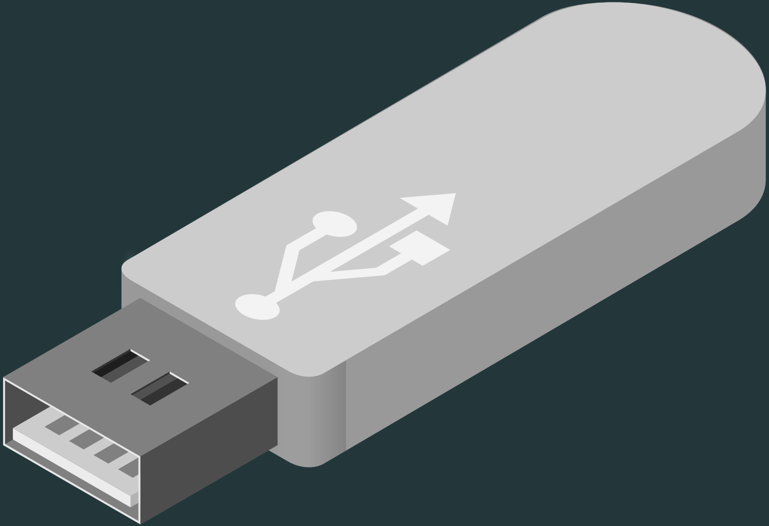
USB Devices Phoning Home

Roland Schilling & Frieder Steinmetz

February 09, 2016

Security in Distributed Applications
Hamburg University of Technology

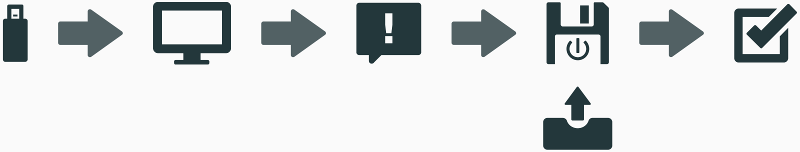


Considering Properties of “Storage” Devices

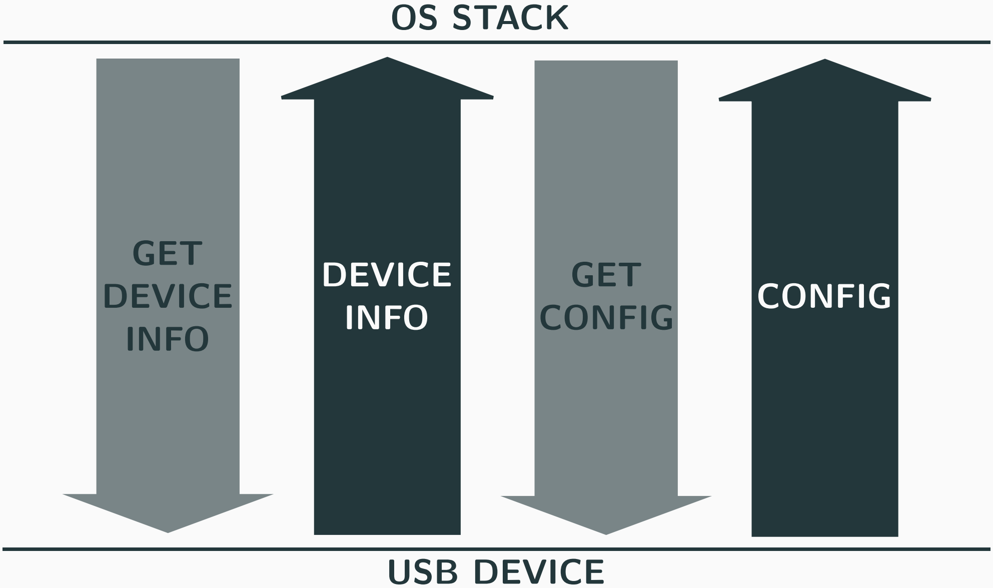
- USB sticks have widely replaced floppy disks and CDs
- We use USB storage devices in the same way
  - → CDs and floppy disks are “stupid” storage-only devices
- USB has replaced dedicated protocol solutions like PS/2 and LPT

A User’s View

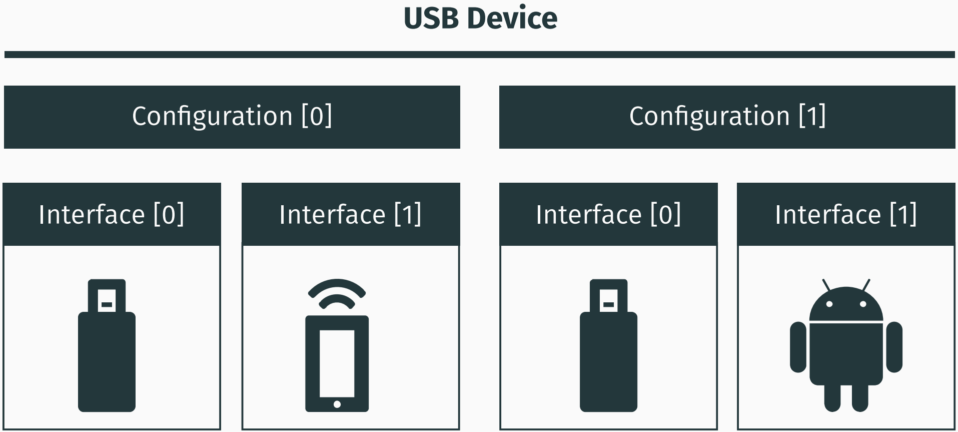
What really happens when you connect a thumbdrive?



The USB Enumeration Process



USB Architecture



USB Device

Configuration [0]

Configuration [1]

Interface [0]

Interface [1]

Interface [0]

Interface [1]

Looking Beyond Programming Errors

Exploiting Software Bugs via USB

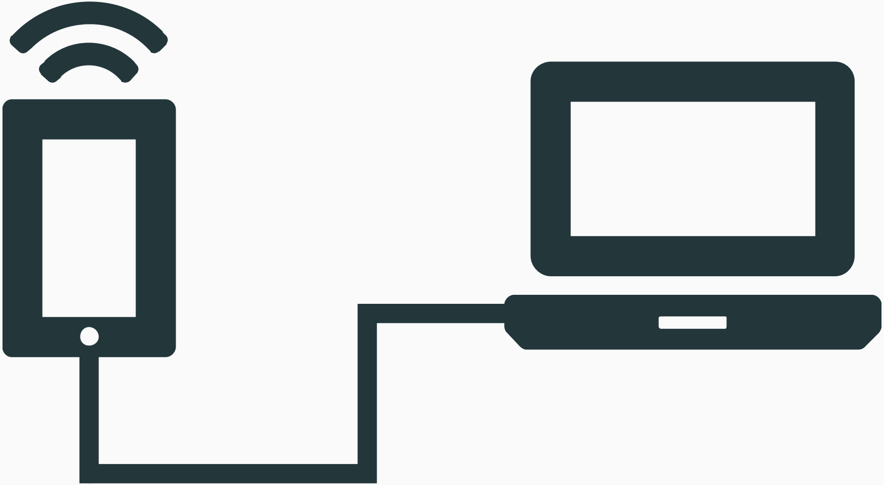
- Buffer Overflows
- Format String Flaws
- Integer Overflows
- Null Pointer Dereference
- Logic Bugs
- Denial of Service

→ *Is feasible and has been done. What else is possible?*

Motivational Question

Can we ever know what kind of device we are handling, prior to inserting it?

Example: Smartphone Tethering



Smartphone Tethering – Implications

What happens?

- Ethernet-over-USB
- Host is configured via DHCP
- Device is new default gateway and DNS

The implications

- Can change the hosts network configuration
- Device sees all the traffic

Take-away:

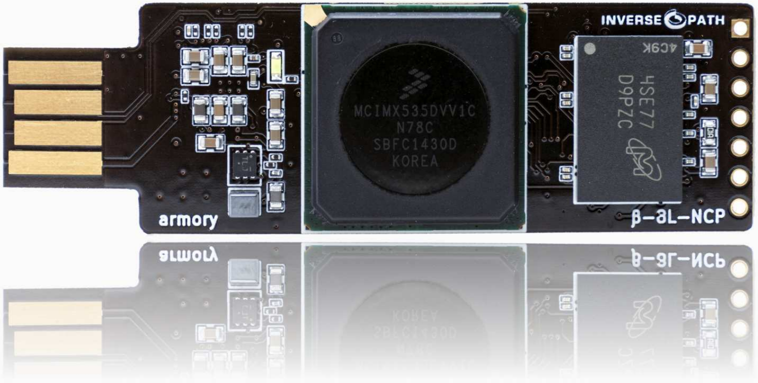
Advertising as a certain type of device equips the device with unexpected privileges!

Moving On

What would prevent a USB thumbdrive from doing the same?

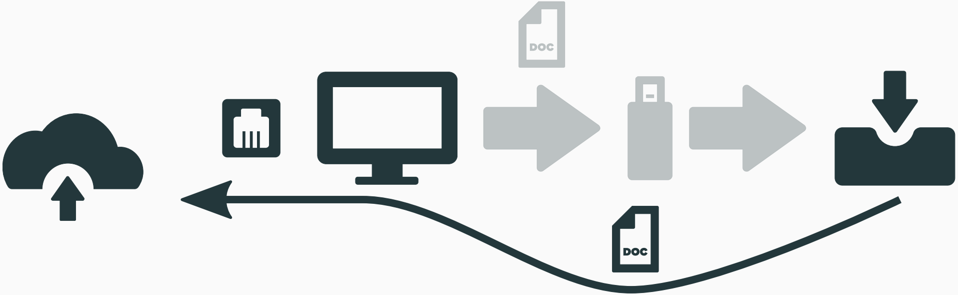
Nothing - and we found just the right device to demonstrate that!

USB Armory

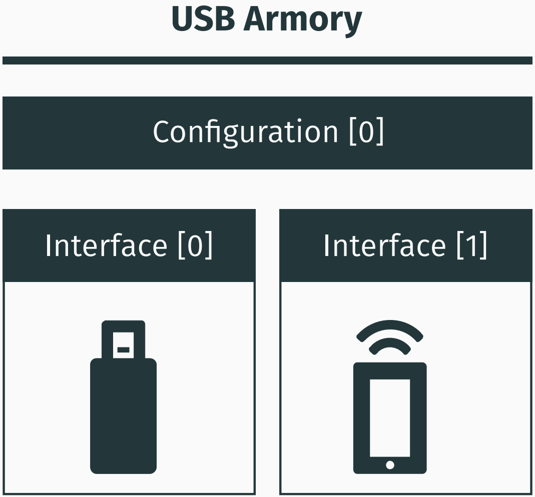


- ARM Cortex-A8 800 Mhz, 512 MB DDR3 RAM
- Runs Linux from microSD card

Setup



USB Armory Configuration



USB Armory

Configuration [0]

Interface [0]

Interface [1]

Setup

USB Armory Setup:

- DHCP server
- Web server
- DNS server

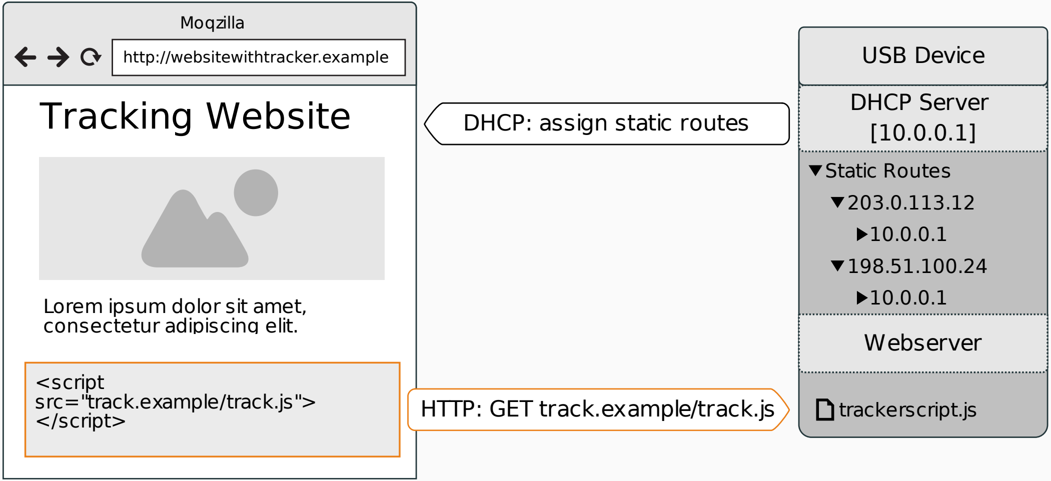
Used for:

→ Propagating routes

→ Serving custom JavaScript

→ Rerouting domain names

Setup



Moqzilla

http://websitewithtracker.example

Tracking Website

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

```
<script
src="track.example/track.js">
</script>
```

DHCP: assign static routes

HTTP: GET track.example/track.js

USB Device

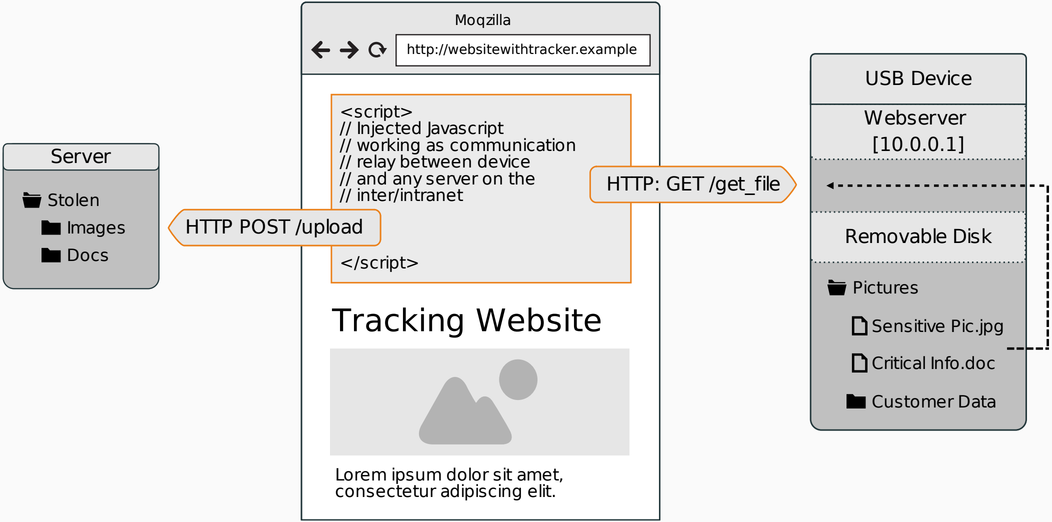
DHCP Server [10.0.0.1]

- ▼ Static Routes
  - ▼ 203.0.113.12
    - ▶ 10.0.0.1
  - ▼ 198.51.100.24
    - ▶ 10.0.0.1

Webserver

trackerscript.js

Setup



Server

Stolen

Images

Docs

HTTP POST /upload

Moqzilla

http://websitewithtracker.example

```
<script>
// Injected Javascript
// working as communication
// relay between device
// and any server on the
// inter/intranet

</script>
```

HTTP: GET /get_file

Tracking Website

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

USB Device

Webserver
[10.0.0.1]

Removable Disk

Pictures

Sensitive Pic.jpg

Critical Info.doc

Customer Data

Related: BadUSB

- Showed that firmware of retail USB devices is reprogrammable
- This PoC could theoretically be implemented as flashable firmware

Summary

- Our handling of modern complex USB devices is based on old paradigms
- There is no way to tell the function of a USB device from its looks
- Devices do not need expensive hardware to be used in abusive ways

Roland Schilling

✉ schilling@tuhh.de

@NerdingByDoing

github.com/corrupt

Frieder Steinmetz

✉ frieder.steinmetz@tuhh.de

@twillnix

github.com/willnix

Security in Distributed Applications

Hamburg University of Technology

Am Schwarzenberg-Campus 3
21073 Hamburg

www.sva.tuhh.de

Project Repository:

github.com/willnix/usbpoc

TUHH
Technische Universität Hamburg-Harburg

Resources

- *Metropolis* theme by Matthias Vogelgesang: `https://github.com/matze/mtheme`
- *Foundation* Icons by ZURB Studion: `http://zurb.com/playground/foundation-icon-fonts-3`
- *Ethernet* icon made by Freepik from www.flaticon.com is licensed under Creative Commons BY 3.0 CC BY 3.0
- Picture of *USB Armory* curtesy of Andrea Barisani of Inverse Path: `https://inversepath.com/images/usbarmory_coin.jpg`