OTG from a hacker's perspective

What happens when the gta04 came?

Overview

- OTG overview
- Issues with Vbus
- How to influence things
- A-side as Host
- B-side as Host

OTG overview

- Two types of devices
  - A devices
    - Provides power, Host on start
  - B devices
    - Gets power from the A side, peripheral on start
- Methods of switching host/peripheral dynamically

Issues with Vbus

- Vbus monitoring plays a deeper role
  - State resets
    - After switching roles, back to normal role
  - Session intialisation
    - Pulses on vbus line
- Problems with unusual Vbus behavior
  -

How to influence things

- Whole state system set in stone by hardware
- Little documentation available about MUSB hardware
- But we can talk to Phy via I2C, MUSB does not know about it and can be cheated

A device

- ID pin is grounded
- Is in host role without software intervention, Vbus is output
- Hacking possibilities:
  - Tell usb phy to switch off vbus using i2c and provide vbus externally (can be a bit dangerous)
  - If MUSB notices there is no vbus out → short circuit detected → usb reenumeration

B-Device

- ID pin is floating
- Is in device mode without software intervention, vbus is input
- “A”-side can say:”you can be host”
  - Roles are changed then
- Official way to have a host with vbus input
- Host mode cannot be simply enabled by setting a bit somewhere, you have to move through a state system
- Role reset on vbus disconnect

B device state changes