

# BadUSB

Michael Koch

[pib.michael.koch@htw-saarland.de](mailto:pib.michael.koch@htw-saarland.de)

Urs Oberdorf

[urs.oberdorf@autistici.org](mailto:urs.oberdorf@autistici.org)

Stephan Wendt

[stephanwendt@freenet.de](mailto:stephanwendt@freenet.de)

Fakultät für Ingenieurwissenschaften  
Hochschule für Technik und Wirtschaft des Saarlandes

06.07.2015

# BadUSB

## Einleitung

- ▶ Entwurf in den 90ern
- ▶ bietet hohe Anschluss-Flexibilität bei Peripheriegeräten
- ▶ Bus-System
- ▶ Host-Controller kontrolliert Kommunikation

# BadUSB

## Anschluss eines Geräts

- ▶ Reset
- ▶ Device Descriptor
- ▶ Interface Descriptor

# BadUSB

## Live Demonstration

- ▶ Live Demonstration

### Testumgebung

- ▶ Notebook mit Windows 7
- ▶ HP Proliant DL380 G5, 2x Xeon Quadcore, 16GB RAM

Drei Images (base, hello, ftp)

- ▶ Timeline
- ▶ MD5 Hashes der Dateien
- ▶ Differenzen
- ▶ Windows Logfiles
- ▶ `setupapi.dev.log`

# BadUSB

Fazit

Fazit

- ▶ Abwehrmöglichkeiten



# BadUSB

Ende

Vielen Dank für Ihre Aufmerksamkeit