BadUSB

Michael Koch [*] Urs Oberdorf [†] Stephan Wendt [‡]

06.07.2015

[*] pib.michael.koch@htw-saarland.de
[†] urs.oberdorf@autistici.org
[‡] stephanwendt@freenet.de

1 USB - Eine kurze Einführung

In der Mitte der neunziger Jahre entwickelte ein Firmenkonsortium den *Universal Serial Bus*. Er sollte einen Standard für den Anschluss von Peripheriegeräten bieten und wurde ein Erfolg. Heute finden sich an nahezu jedem Peripheriegerät eine USB Schnittstelle.

Wie im Namen enthalten, handelt es sich um ein Bus System, welches einen Mechanismus benötigt, die Kommunikation zu steuern. Im Fall des USB-Standards ist dies der auf der Hauptplatine verbaute Host-Controller der angeschlossenen Geräten u.a. das Senden von Daten erlaubt. Das bedeutet, dass ein per USB angeschlossenes Gerät nur dann Daten senden kann wenn es von dem Host-Controller abgefragt wird.

Sobald an einen USB-Port ein Gerät angeschlossen wird, sendet der Host-Controller ein USB-Reset Signal an das betreffende Gerät. Dieses wird dadurch aufgefordert sich neu zu konfigurieren und seinen *Device Descriptor* zu senden. Dieser Deskriptor enthält Informationen über die Klasse des Geräts, also als welches Gerät es sich selbst anmelden möchte sowie welcher Treiber dafür geladen werden soll. Für diesen Deskriptor sowie alle weitere Kommunikation zwischen Host-Controller und Peripheriegerät ist eine Art Minibetriebssystem auf dem Anschlussgerät vorhanden, die sogenannte *Firmware*. Wenn diese manipuliert wurde kann sich das Gerät, z.B. ein USB-Stick, auch als Tastatur identifizieren und über den vom Host-Controller geladenen, generischen Treiber beginnen Eingabesignale zu senden wie eine normale Tastatur. Die Spezifikation ist außerdem so ausgelegt, dass sich Geräte auch mit einem *Interface Deskriptor* anmelden können und somit zwei Geräte gleichzeitig sein können. Gewünscht ist dieser Fall bei z.B. Webcams welche sich als Audio aber auch Video Gerät anmelden. Dies ist nur ein Beispiel was mit einer Firmwaremanipulation möglich ist. Alles was per USB angeschlossen werden kann, kann mit einer Firmwaremanipulation von einem anderen USB-Gerät imitiert werden.