ingenieur
wissenschaften
htw saar

Hochschule für
Technik und Wirtschaft
des Saarlandes
University of
Applied Sciences

# BadUSB

Michael Koch * Urs Oberdorf † Stephan Wendt ‡

01.07.2015

## 1 Introduction

### 1.1 Angriffsmöglichkeiten

- Tastatur-Eingaben (bzw. allgemein HID-Devices)
- "Boot-Sektor-Virus"
- gefälschter Netzwerkadapter mit DHCP-Server
- FTP-Server
- alles verfälschen, was auf dem Stick gespeichert werden soll - Abwehr: Stick komplett mit Truecrypt/LUKS verschlüsseln

### 1.2 Abwehrmöglichkeit

- nur USB-Massenspeicher zulassen: darf dann aber nicht beim Reboot drin stecken, bzw. Booten von USB-Sticks unterbinden und BIOS-Passwort setzen, damit der USB-Stick nicht mit Tastatureingaben das BIOS umkonfigurieren kann. Problem ist aber, irgendeine Tastatur muss zugelassen werden, zum Zeitpunkt an dem das BIOS den Rechner an das OS übergibt, welche sollte das sein? Vielleicht nach dem BIOS keine Tastatureingaben zulassen, bis eine Passworteingabe verlangt wird (entweder vom Bootloader oder vom Betriebssystem) und die Tastatur, die dann das richtige Passwort eingibt, ist die erlaubte Tastatur) Wie würde man es mit der Maus machen? Tastatur nur an bestimmtem Port zulassen?
- Sollte man Bestätigungsdialoge beim Anschließen von neuer USB-Hardware einblenden, so dürfen diese nur von Menschen bedienbar sein (CAPTCHA).
- Stick direkt beim Anstecken mit sauberer Firmware überschreiben? - Klappt wahrscheinlich nicht, weil das Betriebssystem das auf der USB-Stick-CPU läuft, wahrscheinlich sich dazwischen schalten kann
- The firmware of a USB device can typically only be read back with the help of that firmware (if at all): A malicious firmware can spoof a legitimate one. D.h. es würde nichts bringen, die Firmware auszulesen, um sie zu überprüfen. Ist es irgendwie feststellbar, dass es doch mal ein USB-Stick war, bevor die manipulierte Firmware aktiv wird?
- Abfragen, ob die Chip-Familie einen Hardware-Firmwareschreibschutz hat.
- FreeBSD adds an option to switch off USB enumeration.

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

- Vielleicht alle erlaubten USB-Geräte so umflashen, dass sie sich eindeutig identifizieren?
- Offene Hardware und Firmware, und USB-Geräte, die man zuverlässig mit der eigenen signierten Firmware flashen kann
- Wie kann man verhindern, dass die eigenen USB-Geräte (Sticks, etc.), die man an fremde Rechner anschließt, infiziert werden?
- Nur Flashspeicher verwenden, der komplett vom Betriebssystem gesteuert wird.

## 1.3 Projektrichtung

- neuartige Attacke im USB-Stick
- Entwickeln und Testen von Schutzmaßnahmen
- Versuchen, ein fest in den Laptop eingebautes Gerät zu flashen
- Versuchen, mit forensischen Methoden einen Angriff per USB-Gerät festzustellen

http://www.crypto-fuer-alle.de/wishlist/hardware-usb-filter/ http://theinvisiblethings.blogspot.de/2011/06/usb-security-challenges.html https://github.com/adamcaudill/Psychson