17 November 2014 Study · Digital Identity · Transparency

Threats Posed by Malicious USB Devices

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/malicious-usb-devices/

Recently, manipulated USB devices have appeared that can not be detected as a threat to current protection measures. This short study summarizes known methods that enable the manipulation of USB devices in order to attack a computer. After a brief introduction to the USB standard, known attack vectors have been subsumed. Particular attention has been paid to the manipulation of the firmware of USB flash drives („BadUSB" attack). Practical case studies have been used to highlight the problem and to illustrate the possible consequences of an attack. Finally, the use of possible protective mechanisms has been discussed.

The key findings are as follows:

- Physically prepared devices are only suitable for targeted attacks and mostly implementing only a specific functionality (eg. a „Hardware keylogger").
- Attacks on USB devices work independently of a vulnerability in an operating system. They rather exploit shortcomings of the USB standard or weaknesses in faulty drivers.
- Manipulated USB devices mimic the functionality of other device classes but, depending on the given hardware equipment, may be unable to fulfil all requested operations. For example, a USB flash drive hardly provides the capabilities of a smartcard reader.
- The „BadUSB" attack is only applicable to devices for which the manufacturer of the microcontroller provides the ability to replace the firmware via USB.
- In general, the firmware of USB devices is not equipped with a digital signature that could be used to verify the integrity and authorship of a file.

- The „BadUSB“ attack has been presented so far only for USB flash drives using microcontrollers from Phison. The methodology used can be systematically applied to other USB devices, but does not necessarily lead to a successful attack.
- The feasibility of technical protection mechanisms is limited; attack vectors should also be considered on the basis of organizational measures.