Peer Review of ”Classification of USB based attacks”

Nico Petzendorfer

June 20, 2023

1 Summary

The paper highlights vulnerabilities stemming from the design of the USB specification. It classifies these vulnerabilities to allow readers to understand the main attacks without needing to know every single variation. Additionally, an overview of the USB protocol is given to allow for a better understanding of the reasons for the possible attacks. Differences in the USB versions are highlighted and a brief history about the development of the USB specification is given.

2 Strength

The paper presents attacks on the USB protocol that might not be immediately obvious. These are not only classified, but it is also shown how they arise from crucial design flaws in the USB protocol. Additionally, a high level overview of the USB protocol is given. This allows even non-technical readers to understand the paper without having to resort to external resources.

3 Weakness

- It is said that the USB devices do not need “intelligence”, as this is put on the host. However, as the USB protocol is not straightforward and the devices generally still need to do some processing (e.g. converting the sensor readings of a mouse to movements), this can not really be said.
- When the paper gives examples on how some mechanisms work in operating systems, only Microsoft Windows is used as an example. It might be interesting to also include other operating systems (e.g. Linux, macOS) to show how it is implemented there.
- It is stated that USB type A connectors have four pins. This is only true up until USB 2.0. As USB 3.0 added two additional differential data pairs, a USB 3.0 type A connector has nine pins.
- When it is stated that `D+` transmits the inverse of `D-`, the technical term “differential pair” could be used.
- In section IV-A, it is stated that solutions will be proposed, and the added overhead is negligible. However, the solutions and influence of overhead are not apparent from the text.
- It is often stated that the vulnerabilities stem from the design of the USB specification. It might be interesting to explain why it was specified this way (performance, easy implementation, ...).
- The paper says that capturing all data is not trivial. Such a device could, however, simply capture the raw USB transmissions and decode them in software, which seems rather easy.
- It is stated that the possibility of Man-in-the-Middle and Man-on-the-Side attacks on the physical layer comes from missing encryption. It is not clear how encryption could save against Man-in-the-Middle attacks, as a USB device could not verify whether it has exchanged keys with the host system or with an attacker, and pre-shared keys with the operating systems could be extracted.
- The author states that denial of service attacks through high voltage arise from missing voltage regulators. This is not true: USB hosts have voltage regulators to ensure a stable 5 V supply. To prevent these attacks, a sufficient overvoltage protection circuit is needed.
- It is said that a USB device could execute malicious code on a locked PC by using a screensaver. It does not become clear how such a USB device could introduce a malicious screensaver onto a locked pc or how a non-malicious screensaver could be exploited.
- The paper states that the USB device acts as a DHCP server. It seems more probable that the device acts as a network adapter with a connected DHCP server.

- It is stated that by changing the DNS server, all network traffic can be intercepted. It is not clear how this is useful when using HTTPS or TLS.
- The paper states that the functionality of the fuzzing attack will be described in a proof of concept. However, the following proof of concept explicitly states that fuzzing techniques could not have discovered the vulnerability.
- While it is true that a USB cable could be used as an antenna to transmit RF signals, the extent and feasibility of this attack does not get clear.
- The classification might become more clear if the results are presented in a table, so that the different classes can easily be compared and the most important facts can be seen.

4 Comments

Comments on the paper can be seen in the provided annotations. Most notable were the spelling mistakes and the broken citations.

It shall be noted that these suggestions (especially the ones regarding style) can be personal preference and the presented possibilities should therefore not be taken as the final decision.