Dear Prof. Michael Schwarz

Thanks again for serving as our shepherd for our WOOT 21 paper. We have addressed the issues raised by you and other reviewers. Here is a summary of our revision.

\* Provide more details what happens when you attach an external monitor to the tested devices.

\* Describe any notifications on the tested devices (e.g., keyboard-present indicator, blue notification bar, pop up, ...) or explicitly mention that are none.

\* Describe how BadUSB-C ensures that the external monitor is mirrored. Does this require user interaction? Does it already require injecting keystrokes/mouse movements?

- We have added a part named *Attack Initialization* in Section V, which describes what notification will be raised when attaching our BadUSB-C to the tested devices. Apart from that, we also added a part describing how BadUSB-C responded to these notifications. For example, on Windows 10, BadUSB-C can inject “Win+P”and a click on the “Duplicate”option to dismiss the pop-up. The same steps are used to ensure screen is mirrored on Windows 10.

\* Discuss the requirements/limitations more honestly.

- We have added more details in Limitation Part, which further talks about our limitation, including issues related to mirroring screen, notifications of devices and screen lock.

\* Provide details (exact versions) of tested devices.

- In Section V, we have added the detailed versions of devices and OS build versions.

\* Better compare your attack to Juice Filming Attacks.

- In the end of Section III, we compare our work to Juice Filming Attacks. The main advantage of our work is that we combine BadUSB to take control of victim’s devices. Apart from that, we also utilize the latest USB-C standard, while JFA uses an old protocol named MHL.

\* Is there any realistic threat model for laptops? Most people probably don't charge their laptop with a borrowed power bank.

- We found that in some railway stations and airports there are charging stations providing Type C charging cables instead of AC sockets. This is a realistic threat model. We have added a part in Section V-E describing this scenario.

\* How exactly does the GoodUSB bypass work? Isn't the idea that GoodUSB only allows injecting keystrokes after the user confirms that the device is trusted? How can BadUSB-C inject the keystrokes/mouse movements, shouldn't they be blocked?

- We are terribly sorry about the GoodUSB bypass part. When we were conducting survey for our paper, we came across the GoodUSB. As GoodUSB is proposed in 2015 and its implementation is based on Linux Kernel 3.x, we failed to compile such old version of kernel on our tested devices. Thus, we decided to implement a home-brewed version of GoodUSB. But we misunderstood some points in their paper and did not implement all security features. We thought GoodUSB will allow limited function before authorization to ensure that first USB device is usable on a brand-new device. And thus we mistakenly believe that our BadUSB-C is able to complete such authorization process and bypass GoodUSB. After we received reviews for our paper, we further looked into the details of GoodUSB and found that we cannot bypass GoodUSB. We have revised all content related to this issue. Apologize again for our mistake.

\* Substantiate or remove claims as mentioned in the reviews, e.g., "The designers of the USB protocol did not care much about security issues as they wanted to make an easy-to-use protocol."

- We have substantiated these claims.

\* Which vendors did you disclose the attack to? What are their responses?

- We disclosed to Huawei and Apple, Huawei responded on 7th March and holds an online meeting with us on 10th March to discuss about mitigation. Apple has not responded yet.

\* Discuss countermeasures mentioned in the reviews (e.g., USBeSafe, USB Condom, ...)

- We have added these in Section III and discussed some of them in countermeasure.

\* Provide more details on the user study as requested in review D.

- We have elaborated the process of user study and added details of protection of sensitive data. After each experiment, the participant first goes through all data and desensitized it, e.g., change sensitive characters into \*. After the desensitized process, the original copy is deleted by the participant. Then we started to process the desensitized data, ensuring the whole process is ethical.

\* Use some grammar checker (e.g., Grammarly) or maybe ask a native speaker to proof-read your paper.

- We have asked a native speaker to proofread our paper and use Grammarly to check our paper.