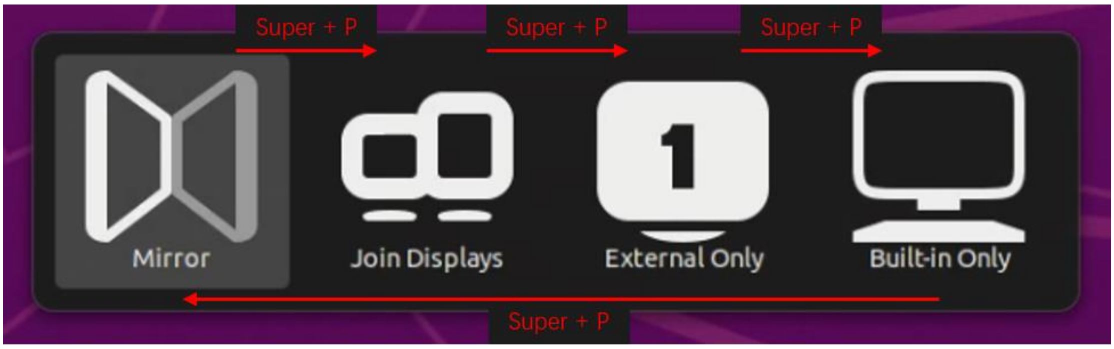
Dear Prof. Michael Schwarz

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: do they automatically mirror the screen? do they extend the screen? do they switch to Desktop mode (e.g. https://youtu.be/SW-nHwq5P0Y?t=59)?

** We added more details about Desktop Mode in both Experiment and Attack Initialization and how to ensure BadUSB-C is mirroring the primary screen, which still relies on HID injection but as BadUSB-C can obtain the video (the desktop) in Desktop Mode, hence it can be performed with mouse clicks. We did not figure out a way to inject keystrokes to achieve that as HUAWEI Desktop Mode does not provide shortcuts like Windows/Ubuntu/MacOS.

* 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 further looked into hotkeys related to the mode switch of external monitors. And we found that on both Ubuntu/Windows 10, "Win(Super)+P" can be used to switch modes for the external monitor. But it depends on the default settings of the user. Different default settings require different times of "Win(Super)+P" to set the external screen into mirror mode like the following picture describes. BadUSB-C may have to try multiple times to get it right.



As for MacOS, as described in its official manual, BadUSB-C can inject "Command+F1" to set itself into mirroring the primary screen. All content listed above are added to the Attack Initialization Part

* Better compare your attack to Juice Filming Attacks [17]. What is the difference? What are the advantages/disadvantages of your attack?
** MHL may not be an outdated standard, but it does lack support on mobile phones today. According to an official list provided by the MHL Tech, the latest smart phones listed was released in 2015 while an unofficial list of DisplayPort over USB Type-C presents much more devices supporting DisplayPort over Type-C. As for the permanent notification/mitigations of JFA, we were unable to test JFA on our tested devices as it requires MicroUSB connector which is hard to find on today's mobile phones and there are no mobile phones listed on the official list actually support MHL over USB Type-C. But to our best knowledge, after JFA is published, HUAWEI deployed mitigation that requires user authentication before outputting the video

stream.
We also provided a scenario where victim leave their phone charging in absence of a screen lock. In this case, JFA cannot do anything as it does not have control over the victim's device while BadUSB-C can directly perform malicious actions and obtain victim's privacy actively.

* Currently, there is no case study in the paper that demonstrates the unique properties of BadUSB-C. The attacks on the smartphones only use the video capturing and are thus not different to JFA. The attacks on the laptop do not seem to use the screen. The executed scripts are already known from BadUSB and do not require any mouse movements or UI interactions. The only example is the full-control mode on the iPad, but this example is not automated and requires an attacker to perform the attack.
** We added a further explanation about BadUSB-C in Experiment. We performed experiments of three modes on three different devices to better cover all types of devices. Attacks on smartphones and laptops can also uses screens to obtain victim's privacy more efficiently. We also revised the case study hence it does not only rely on video capturing but full controlling as well.

* Substantiate or remove claims as mentioned in the reviews
** We have substantiated the mentioned claims.

* Result of the discussion with HUAWEI
** We are currently facilitating HUAWEI with the mitigation plan, who are weighing between different defense approaches to better protect users. After the mitigation being deployed, HUAWEI will also apply for a CVE ID for this vulnerability.

* The changes to the description of the user study are problematic.
** We have rewritten the entire user study and gathered the information removed by ourselves. Also, we use both Full Control Mode and Video Capture Mode in the new case study, which further differentialize our work from JFA.
* Use some grammar checker (e.g., Grammarly) or maybe ask a native speaker to proof-read your paper.
** We have fixed those grammar error.

* The paper now sometimes mentions USB 3.1, sometimes USB 3.2, and sometimes USB 3.x. Please clarify which standard is used for BadUSB-C and what the differences are.
** We have unified our choice of word to USB 3.x. USB 3.1 and USB 3.2 now are only mentioned in Background. As for the protocol used by BadUSB-C, all devices used a Type-C connector and support DisplayPort over Type-C alternative mode are vulnerable to BadUSB-C. We used USB 3.x for simplicity and more detailed information is discussed in Background.