THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

May 2023

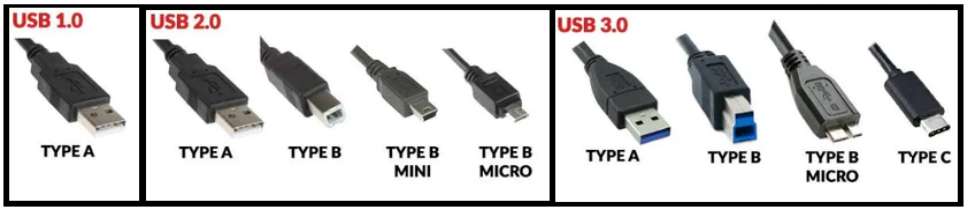
Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats.

I received a request to discuss the physical cyber threat called “juice jacking” that has been emerging in the media (tweets from the FBI, FCC, Forbes, and other sites). This trend is not new by any means, as it has been around for more than 10 years, but the technology surrounding it has been upgraded since its introduction. Although the initial request centered around the innocent-looking kiosk charging stations found in airports, since summer travel season is coming up, I believe it is important to address the technology completely so I will be including a bit more than just this topic.

What is Juice Jacking?

Malls, airports, hotels, coffee shops and other public places may have a courtesy kiosk where folks can charge their battery powered devices when they are running low on power. These kiosks can consist of simple USB powered plugs, plugs with cables and/or actual computer systems behind them meant to be used as a hub to provide power for a variety of USB connectors.



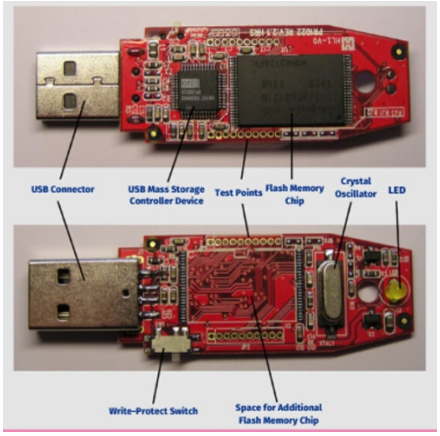
...

Occasionally, especially when not maintained, malicious charging stations are rigged with hardware or software that can:

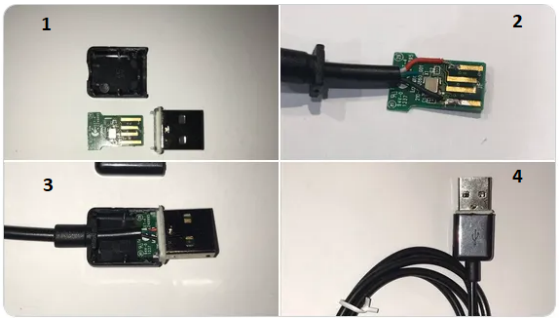
- Infect your device with malware or spyware
- Extract sensitive data without the user's knowledge
- Lock you out of your device
- Purposely send a high voltage charge to damage your device

How does it work?

Disclaimer: We do not endorse the use of technology for malicious purposes, and I encourage you to seek professional advice before making any decisions or taking any action with such devices. It is crucial that you use the information below ethically and responsibly. We cannot be held liable for any actions taken based on the information provided.



At a fundamental level, Operating Systems generally trust physical devices when they are connected, unless specific security measures are in place to prevent that trust. For example, security controls like the widely-used BSD application, CrowdStrike, play a vital role in safeguarding against potential threats related to USB devices and their inherent vulnerabilities. While CrowdStrike provides robust protection against data connectivity risks, it is important to note that it cannot address the security concerns associated with USB cable connectors themselves.



With the miniaturization of device chips, which now resemble the size of cable connectors, their increased capacity and capabilities have introduced new challenges. A USB cable head essentially becomes a small battery or computer that can be reprogrammed to be recognized as a different type of peripheral, such as a keyboard or a mouse, which a trusting device will treat as such and allow the use of its features.

These tiny computers, now disguised as indistinguishable-from-the-original-manufacturer-equipment (OEM) cables, can have their own Wi-Fi, can be controlled by a nearby system, have their own web services, can have a SIM card tracked via GPS, and can even have a self-destruct mechanism to prevent tracing. It is very much a James Bond spy gadget come to life. These USB cables range in price from $5 to well over $200 depending on the features. The low cost, when compared to the gains of identity theft and an increased prevalence of these devices, significantly raises the risk of becoming a victim of these tools.

What are the methods for detecting malicious connectors?

Besides having x-ray vision, you can use peripherals designed to identify suspicious activity on a connector prior to its insertion. However, these peripherals tend to be costly and may not be compatible with the specific connector type one has (there are lots of them). Another approach involves using an

infrared thermal camera to detect a potentially malicious connector. Connectors with additional features tend to generate more energy compared to regular cables, resulting in higher temperatures when touched. Nevertheless, distinguishing between an original equipment manufacturer (OEM) cable and a malicious one can be challenging in practical terms. It is worth noting that even the manufacturers of these malicious cables may struggle to differentiate them from genuine OEM cables.

Here are several tips to avoid Juice Jacking:

- Carry your own chargers and USB cables with you when traveling. Do not use any cables or adapters that are provided by strangers or left behind by others.
- Use AC power outlets instead of USB ports on charging stations whenever possible. This way, you can avoid any potential risks of data transfer or malware infection.
- Carry a charging-only cable that can prevent data from being sent or received.
- Carry an external battery pack or a power bank that can charge your device without connecting it to a USB port. This can also extend your battery life and save you from looking for a power source.
- If you plug your device into a USB port and a prompt appears asking you to select “share data” or “trust this computer” or “charge only,” always select “charge only.” This can prevent any unwanted data exchange or pairing between your device and the USB port.

If you have any topics that you would like us to write about in our newsletter, please feel free to drop us a line and let us know by e-mailing security@bsd.uchicago.edu