USB-Ultimately Sinister Power Block

Benjamin Draffin, Shivani Singhal, Shekhar Sharma, Rishikesh Yardi
Carnegie Mellon University

Abstract

Mobile phones share many similar characteristics with traditional computers. With rich connectivity options and powerful processors, smartphones and mobile devices are able to integrate and communicate with many types of devices. This, however, leads to some unfortunate security considerations. Devices need lots of power and must be recharged frequently, often outside of one's home. Public smartphone charging stations are an effective and convenient solution for the battery life concerns, but can these charging stations be trusted?

This research identifies ways in which public or malicious charging stations can be used to exploit the smartphones of unsuspecting users. The work considers what kinds of sensitive information can be be extracted from devices, how applications can be surreptitiously pushed to the devices, and how it is possible to physically harm mobile devices through manipulation of charging protocols and electrical attacks. This work also discusses ways to defend against some of these attacks by locking the phone or using external protection equipment.

The primary function for evaluating each of the attack options is the ratio between impact and detectability. Highly impactful attacks are of value to adversaries, but if they trigger strange lights, sounds or warnings, they will quickly raise alarms with users. Detectability can be influenced by the way a charging station is built or placed within a room. It is common, for example, to find public charging stations with lockable storage containers. These protect the phone from theft, but can effectively hide symptoms of an attack. Overall, this work analyzes the convenience to danger tradeoff that must be made when using untrusted chargers.

References:

[1] https://www.blackhat.com/us-14/briefings.html#badusb-on-accessories-that-turn-evil
[2] https://www.youtube.com/watch?v=nuruzFqMgIw
[3]https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
[4]http://www.androidpolice.com/2013/02/12/new-android-4-2-2-feature-usb-debug-whitelist-prevents-adb-savvy-thieves-from-stealing-your-data-in-some-situations/
[5] (https://github.com/kosborn/p2p-adb/)
[6]http://www.wallofsheep.com/pages/juice
[7]http://krebsonsecurity.com/2016/08/road-warriors-beware-of-video-jacking/
[8]http://www.slideshare.net/RobertRowley/juice-jacking-101-23642005
[9]http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6067669
[10]https://samy.pl/poisontap/
[11] https://usbkill.com/
[12]Park Joon Young, Jo Hyo Jin, Samuel Woo and Dong Hoon Lee, Ubiquitous and Future Networks (ICUFN) 2016 Eighth International Conference on, pp. 882-887, 2016, ISSN 2165-8536.
[13]http://www.pcworld.com/article/2460540/most-usb-thumb-drives-can-be-reprogrammed-to-silently-infect-computers.html

RSAConference Security Scholar

USB-Ultimately Sinister Power Block

Benjamin Draffin, Shivani Singhal, Shekhar Sharma, Rishikesh Yardi
Carnegie Mellon University

Problem Statement and Goals

The circuit above is a common USB system on a phone. Observe the lack of regulator on the Data pins (D+ and D-)

- Public charging stations are commonplace, but they are not always what they seem. They can steal data, send messages, spoof network connections, grab sensitive data through screen captures, and permanently damage your charging circuitry!
- There have been a number of other research groups tackling this danger, including "Juice Jacking" by the Wall of Sheep, "MacTans" by Billy Lau et al, and "USB Device Spoofing" by Security Research Labs as well as USB electrical attacks by *USBKill.com*.

Approach

- Many phones support voice control, and some allow usage while the phone is locked. Recorded commands can be played back by the charging station, extracting data or performing actions. Audio input and output can be silenced by the charger posing as a USB audio device.
- Phones can support many USB connected devices using the USB On the Go protocol (OTG). Mice, keyboards, audio cards, and monitors can be emulated in software. The charging can pretend to be a keyboard and run an automated script to enable developer mode and gain trusted ADB privileges, after which a malicious app can be pushed.
- Malicious WiFi equipment can be hidden within the charging box. The demo victim device scanned for an "Expedia-Corp" WiFi network and the Pineapple automatically created a network by that name. The user requested a CMU.edu site over HTTP and the charging station replied with an attacker controlled page.
- ADB is the debugging interface for Android devices. Old versions of Android allow any computer to connect (making attacks trivial), though newer versions request confirmation. Once ADB is enabled (e.g. using USB OTG attack above), many attacks are possible without any visual indication to the user.
- Smartphone voltage regulators only handle low voltages (charging range 3-9 v) and can be damaged by high voltages. Also it is possible to destroy a phone by applying large voltages (~110v) to the data lines.

Defenses

- Don't Use Public Charging Stations
- Lock Phone Before Plugging in
- Disable Siri / Ok Google while locked
- Disable Auto-connecting to WiFi Networks
- Watch the screen of the phone while the device is charging

Conclusion

Public USB chargers are not to be trusted. Avoid using them whenever possible, and try to carry portable chargers or battery packs when you travel. If public charging is necessary, ensure the device is backed up, locked, and password protected to defend against the OTG attacks and minimize losses from electrical attacks.