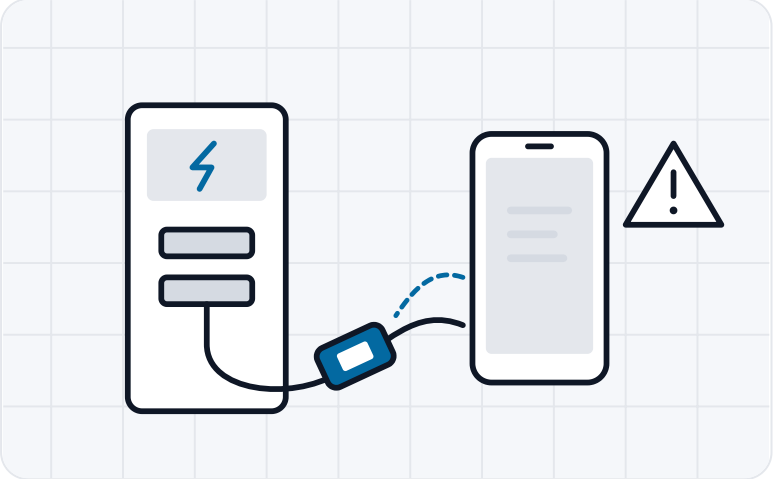
A-SIT Technology

E-Government Innovation Center

25 January 2024 Overview · Mobile Security · 22 min read

State of the Art Juice Jacking Attacks and Countermeasures for Mobile Devices

Florian Draschbacher



Authors	Florian Draschbacher
Version	2024-01-17
Source	https://technology2.a-sit.at/en/publications/state-of-the-art-juice-jacking-attacks-and-countermeasures-for-mobile-devices/
Note	Machine translation.

Key findings

- Since iOS 7 and Android 4.2, users must confirm USB data connections; nevertheless, modified forms of juice jacking remain possible.
- The attacks exploit USB OTG functions (input, video, audio) or the power-line side channel, i.e. fluctuations in charging current.
- The power-line side channel needs no data connection, so USB data blockers do not help; the attacks mostly work only under controlled conditions.
- USB data blockers are only recommended to a limited extent, for example because they are useless when the attack is built into the cable.

- The most effective measure is an operating system confirmation for USB host mode too; public charging stations should only be used in an emergency.

Juice Jacking describes a family of attacks on mobile device that utilise a manipulated charging cable for extracting data or installing malware. Users are particularly susceptible to these attacks in places where they use public charging infrastructure instead of their own equipment, such as at charging stations at airports. Although the general attack mechanism has been known for several years, new methods keep being found that allow circumventing countermeasures.

As part of this project, we provide an overview of different options for Juice Jacking. In addition to a literature research regarding existing approaches, we present considerations for exploiting technological changes in charging interfaces to bypass existing countermeasures.

1. Introduction

In contrast to traditional computer systems, the physical dimensions of mobile devices such as smartphones or tablets are decisive selling points. To still provide wired interconnectivity with accessories and computers while keeping the device dimensions small, mobile devices have a single port that can be used for both power supply and data transfer.

The versatility of this port was recognised as a weakness soon after the first smartphones were introduced. For the user, the function of a device plugged into the smartphone can often only be read from its outward appearance. If a connected device does not behave as its appearance suggests, however, the average end user has no way of recognising this deception.

The best-known form of attack based on such a deception is the juice jacking attack. In it, data is extracted from the mobile phone via a manipulated charging port or a manipulated charging cable. While there is no difference from a normal charging process for the end user, the attacker gains access to, for example, the photos, passwords, documents and much more stored on the phone. In some cases, even the installation of apps on the device is possible, so that the attacker still has access to user data after the physical connection has been disconnected.

The original form of this attack was publicly discussed about 10 years ago and quickly led to countermeasures that were integrated into the mobile operating systems Android and iOS. Nevertheless, various modified forms of the attack are still possible.

Although no malicious juice jacking attacks on end users have been documented so far, public authorities regularly warn of the danger posed by potentially manipulated, freely accessible phone charging infrastructure at airports or shopping centres. In 2023, for example, the US security agency FBI [1] and the US communications authority FCC [2] once again warned travellers in particular to avoid public charging infrastructure as far as possible. Shortly afterwards, a discussion about the sense of these warnings flared up on various IT news websites [1], [2]. Critics accused the authorities of failing to acknowledge that the danger had long since been averted by changes in the operating systems.

This report examines the situation regarding juice jacking in detail. To do so, we explain the basics of the connectors involved and summarise various current attacks from scientific sources. In addition, we discuss the effectiveness of existing countermeasures against juice jacking and provide an outlook on new developments.

2. Background

This section explains the technologies that are necessary for understanding the later discussion.

2.1. USB

USB, the Universal Serial Bus, is an interface with which peripheral devices can be connected to a computer. The standard is the first successful attempt to unify the many proprietary connectors that until then had been used by different manufacturers for a wide variety of input and output devices. Since its introduction in the mid-1990s, USB has become established in the consumer sector for almost every type of peripheral device. There are USB mice and keyboards, hard drives, DVD drives and other storage media that use the port, as do printers, cameras, and many more. The wide adoption of the USB standard and corresponding sockets led, after only a few years, to many devices using USB ports for their power supply even when they are not input or output devices at all. There are now bicycle lights or fans, for example, that can be charged or operated via the USB port.

In USB, all communication takes place between a USB host and a USB device. The USB host is the device that has control over the connection and can essentially request functionality or data from the USB device. Data flows in the opposite direction only if this was initiated by the USB host. The communication can therefore be described as directed.

Conceptually, when using USB, data is only ever transferred between one USB host and one USB device (that is, not between several USB hosts or several USB devices). It is possible, however, to operate several USB devices on one USB host. This bus topology is realised by means of USB hubs, which can forward communication packets from the host to several different devices. USB can therefore be said to have a tree-shaped bus architecture.

When a USB device is plugged into a host, the host starts the communication by querying the device for its descriptors. These are data structures that provide information about the properties of the USB device. They transmit, for example, the manufacturer and product name of the device, as well as the functionality provided by the device in the form of interface descriptors. Using these descriptors, the host can determine the type of the connected device and load a corresponding device driver.

2.2. USB Connectors and Versions

Since the first release of the USB standard in the mid-1990s [3], several revisions have been published. Essentially, the revisions differed from their respective predecessors in the possibility of higher data transfer rates. While extensive backward compatibility with older USB standards exists, new functionality requiring hardware changes was also introduced.

In the first two versions, 1.0 and 1.1 [4], the USB standard provides only connectors with 4 connections. Of these, 2 connections (pins) are used for the power supply of the USB device (5V and ground), and a differential pair of lines is dedicated to data transfer.

Various USB sockets and plugs were specified that define the role of the respective connector in the USB connection. A distinction is made between the following connectors:

- USB-A: This is the common USB connector, as known from USB sticks, for example. The USB host is always the device that has the USB-A socket.
- USB-B: For USB devices that have no permanently attached cable (or no permanently attached USB-A plug), a USB-B socket is used. Devices that have a USB-B socket (according to USB 1.0 or 1.1) always operate in the role of a USB device (that is, they are never hosts).

An essential change in version 2.0 of the USB standard [5] with regard to juice jacking attacks was the introduction of USB On-The-Go [6]. This is the ability to use a USB-capable device both as a device and as a host. This was implemented by equipping the newly introduced miniaturised variants of the USB-A and USB-B connections (Mini USB and Micro USB) with an additional pin. Different assignments of this pin signal the role of the connected device in the USB connection. After the physical connection has been established, OTG-capable devices check the status of this so-called ID or sense pin in order to switch their USB stack into the appropriate mode. The decision as to which communication partner assumes the role of host or device is thus still fixed in hardware. Various cables are available in which the wiring of the ID pin on the Micro-USB-B connector allows either the connection of USB peripherals (such as mice, keyboards, etc.) to a USB OTG socket, or a connection of the OTG-capable device to a computer.

Before the introduction of USB Type-C, Micro-USB connectors (often also OTG-capable) were widely used on smartphones and tablets, in particular those running Android.

Version 3.0 of the USB standard [7] introduced additional pins in the USB-A connector as well as new backward-compatible Micro and Mini connectors. The additional pins allow faster transfer speeds through two parallel data pairs.

2.3. Lightning

In contrast to devices running the Android operating system, Apple did not equip its devices with a Micro-USB interface, but has always relied on proprietary connectors in the past. Early iPhones and iPads had a 30-pin connector that contained dedicated connections for all available types of accessories. Some of the pins carried, for example, analogue audio signals or USB signals for connecting USB sticks.

To further optimise the dimensions of the devices and the user experience, Apple replaced the 30-pin connector in 2012 with the still proprietary but more modern Lightning connector. It has a row of 8 pins on each side. The connected mobile device can detect which type of cable has been connected in which orientation, and assigns signals to the 16 pins accordingly. To implement this procedure, the iPhone or iPad communicates with a chip built into the cable. The counterpart in the iPhone then enables the required signals by means of multiplexing.

2.4. USB Type-C

For about five years, the USB Type-C standard [8] has been increasingly establishing itself among mobile devices. It is a new USB connector that has some advantages over Micro-USB (Type B):

- Reversible The plug can be inserted into the socket in either orientation.

- Higher data rates Thanks to the higher number of pins, data rates of several Gbit/s can be achieved.
- Higher charging current The connector was designed for at least 15 watts of power.

It must be noted at this point that the USB Type-C connector can be used largely independently of the USB specification that governs data transfer. Specifically, this means that devices with USB Type-C sometimes only support USB 2.0 speeds for data transfer. For the latest USB 4.0 standard, however, the use of the Type-C connector is mandatory. This abolishes the distinction between host and device at the connector level, which was still partly present up to USB 3.0.

While early adopters of Type-C simply used it as a physical connector for a USB 2.0 port, nowadays almost every mobile device also supports Power Delivery [9]. This is an additional communication protocol with which two devices connected via USB Type-C can negotiate details of their data and power exchange. This communication takes place over a separate pair of pins in the USB Type-C connector. In addition to some standardised messages, Power Delivery also allows device manufacturers to extend the protocol with proprietary messages.

3. Juice Jacking

In the literature, juice jacking attacks are only ever documented by research projects whose aim was to warn the public of the technical possibility of such attacks. No reports are available of attacks actually carried out outside research environments, which nevertheless does not mean that none have taken place.

The conceptual siblings of juice jacking attacks can be found in BadUSB attacks on classical computer systems. These use devices that visually give the impression of a mass storage device in USB stick format, but actually operate at the technical level like USB input devices (such as a mouse or keyboard). The attack envisages that unsuspecting users find one of these devices and, out of curiosity about the content stored on the seemingly harmless USB stick, plug it into their computer. There, the simulated input device can then be used, for example, to generate a sequence of input events that installs malware on the computer, for instance. Attacks of this kind have been used by hacker groups in the past to gain access to the internal computer networks of large companies, for example [3] [4].

Juice jacking itself was first demonstrated in 2011 at the computer security conference Defcon [10]. The original implementation was a seemingly harmless charging station for mobile devices. In fact, however, connected devices were not only supplied with power. Instead, computers integrated into the charging station established a data connection to the mobile device, via which data could then be copied from the device. This exploited the fact that Android and iPhone devices at the time trusted every connected computer by default. The operating system assumed that the connection to the computer had been deliberately initiated by the user, and therefore established a data connection without further consultation with the user.

In 2013, Lau et al. again presented an attack at the computer security conference Black Hat, called Mactans [11], which used access to the device port during charging to install apps on an iPhone via the debugging interface.

After the vulnerability had been extensively demonstrated in public, Google and Apple responded with changes to their mobile operating systems. Since iOS 7 and Android 4.2, USB data connections between a computer (as host) and the mobile device (as device) must be confirmed by the user via a dialogue before access to files or the debugging interface is granted.

4. Current Juice Jacking Variants

As part of this research project, it was investigated in what form juice jacking is still possible today. To this end, publications were analysed that use the physical connection during charging either to extract data from the mobile device or to manipulate its state.

The literature yields the following categories of attacks:

4.1. Exploiting the USB OTG Function

Since version 3.1 (tablets) and 4.0 (smartphones), the Android operating system supports USB OTG, that is, the operation of USB input and output devices such as mice, keyboards and mass storage devices on the USB port. Most current Android devices still support the connection of such devices, but USB OTG is no longer used for this; USB Type-C is. For ease of use, no confirmation from the user is required to operate these accessories. With Power Delivery, it is easily possible here to supply the Android device with power while simultaneously putting it into USB host mode. For devices with a Micro-USB connector, a special wiring of the ID pin is required for this, which is not compatible with all device models.

Current versions of iOS and iPadOS also support the connection of USB peripherals. For devices that still use the Lightning connector (iPhones up to model 14), a proprietary adapter is required that contains the corresponding Apple chip in order to get the iPhone to enable USB host mode on the Lightning connector. For newer devices (iPhone from model 15), a standard USB-C cable can be used. Charging in USB host mode is possible with both connectors. It is also worth mentioning that current iOS versions only trust connected USB peripherals if they are plugged in while the mobile device is unlocked.

The various attacks differ essentially in the USB peripheral that they use to siphon off data.

Input-based attacks (BadUSB) Similar to the attack against classical computer systems mentioned above, here the malicious charging station injects input events by simulating a keyboard or mouse. Meanwhile, commercial products such as the Hak5 O.M.G. cable [5] are even available that hide all the hardware necessary for the attack in the charging cable. This bypasses simple countermeasures such as USB data blockers, which cut the data lines at the USB socket of the charger.

Attacks of this category, however, have the decisive disadvantage that they do not directly allow the extraction of data (since they merely simulate input devices). Only through automated interaction with the user interface of the mobile device can data be shared over a separate channel (such as the internet). This interaction, however, most likely does not remain hidden from the user.

Video-based attacks (Video Jacking / Juice Filming) Here, an HDMI adapter is embedded or simulated in the malicious charger, which otherwise serves to transmit the screen content of the mobile device to a television or projector. With this attack, sensitive information visible on the display can be extracted from the device. This can be login information or emails, for example.

The attack was first presented in a scientific context in 2015 by Meng et al. [12]. In a later publication, they extended the approach with a system for automatic character recognition [13], with which textual data could be extracted automatically from the user interface.

Attacks of this category suffer from some limitations:

- They require hardware support. While Apple devices have long supported video output via the 30-pin or Lightning connector using a proprietary adapter and protocol, this was possible on only a few Android devices with Micro-USB, for which different adapters (such as MHL) were needed depending on the manufacturer. With DisplayPort AltMode, the USB-C connector does offer a uniform standard for wired video transmission, but even this is reliably supported only by Apple devices with USB Type-C. On Android devices, support depends on the respective device manufacturer. Samsung, for example, only builds in the necessary hardware in the expensive flagship models, while Google does not support USB-C DP AltMode at all on its flagship Pixel series.
- The entry of the device PIN is not transmitted to the external display (with a current OS). The attack therefore cannot be used to bypass the device lock.
- The screen sharing is communicated by the operating system. Depending on the device, the user is informed in the status bar of the operating system that an external monitor is connected. They therefore have an opportunity to detect and prevent the attack.
- The attacker has no control over the device They can only extract data that is visible in the user interface of the device. In addition, the data must first be separated from the visual user interface.

Audio-based attacks Many mobile devices support audio input and output via their multifunction port. Since the introduction of system-wide voice assistants in mobile operating systems, this functionality can also be abused for an attack. This attack was first described in 2022 by Wang et al. [14]. The researchers manipulated a charging cable so that the attacker can generate audio input (attach a virtual microphone) and intercept the audio output. By interacting with the voice assistant, the complete input-output loop can thus be controlled.

The approach nevertheless has some disadvantages:

- The voice assistant must be activated.
- Limited data access. Only those text-based contents that the voice assistant makes accessible can be extracted. In addition, any data output must first be converted back into data that can be meaningfully processed by the computer by means of speech-to-text.

4.2. Exploiting the Power Line Side Channel

Every electronic device needs power to operate. One property that has been exploited in recent times for a whole series of security research papers is the fact that the power consumption of some components built into computer systems depends on the data or instructions currently being processed. This property is particularly relevant for juice jacking attacks as well. During charging, mobile devices not only feed their battery with the power from the charger, but also cover their operating consumption from it. A connected charger can therefore draw conclusions from the charging current about the operations currently being

executed on the mobile device. Via electromagnetic effects, sensor values on the mobile device can also be manipulated through deliberate control of the power supply. None of these attacks requires a data connection to the mobile device. Common countermeasures such as USB data blockers are therefore not effective against them. It must be noted, however, that most of these attacks only work under controlled conditions. The mathematical models used are, for example, optimised for specific mobile devices, and then only work for exactly those.

Extraction of data Yang et al. presented an approach in 2016 that uses fluctuations in the charging consumption of a mobile device to draw conclusions about the websites being visited at the same time in the browser on the device [15]. The researchers were able to show that even factors such as the current charge level of the battery or different network connections hardly affect its detection. In 2016, Genkin et al. used this attack vector to read cryptographic keys from the mobile device via the charging connection [16].

In 2021, Cronin et al. succeeded in detecting the position of changes in the screen content from the power consumption during charging [17]. This is possible with a sufficiently high measurement resolution, because modern screens build up their display pixel by pixel sequentially and have an increased power demand for each changing pixel. Using this approach, the researchers were even able to read unlock PINs as they were entered on a number of test devices, since the visual feedback on a key press reveals the position of the pressed key.

Transmission of data The power line side channel can also be used in the opposite direction for data exchange. Spolaor et al. propose an Android app that deliberately loads the CPU of the device in such a way that data can be transmitted, by means of variations in power consumption, to the charging infrastructure, which is likewise provided by the attacker [18].

5. Possible Countermeasures

Different countermeasures are available for the various types of attacks described above.

For a long time, USB data blockers were recommended against attacks that exploit the USB data connection (such as USB OTG). These can be plugged between the USB socket of the charging station and the charging cable and interrupt the data lines at this point. Due to more recent developments, however, these solutions can only be recommended to a limited extent:

- They are useless if the attack is built into the cable.
- Some manufacturers use proprietary solutions with which the charger communicates the permitted charging current to the mobile device. Some of them use the data lines for this. If these are cut, the device can only charge slowly.
- iPhones and iPads with a Lightning connector only start the charging process after they have obtained information about the cable used. This happens via the so-called IDBUS pin. The same pin is also used to implement JTAG (hardware debugging). Every functioning charger thus inevitably has the ability to perform hardware debugging.
- Mobile devices with a USB-C connector only charge at full speed if communication with the charger via Power Delivery is possible. For this, the CC lines in the connector are used, which on some devices can also be used to overwrite the firmware of the USB Type-C controller.

In addition, these measures presuppose that the user is aware of the potential for an attack. Mass effectiveness cannot therefore be achieved.

The most effective and far-reaching option against misuse of the data connection in the charging port is therefore to be seen in a mechanism in the operating system that also asks for explicit confirmation from the user for the connection of peripherals (USB host mode). An equivalent protection mechanism against attacks that exploit the USB device mode has proven its worth in the past.

Due to the specificity of current power line side channel attacks, they do not pose a realistic danger for average end users. Since the exploited effects are in part produced by the hardware as a result of its design, no countermeasures are available to end users.

As a simple countermeasure, end users are advised to use public charging infrastructure only in an emergency and to exercise caution. If an unexpected message appears on the device after the charger is connected, the connection should be disconnected immediately.

6. Future Research

Due to the widespread use of mobile devices and the sensitivity of the data often processed on them, juice jacking attacks will also remain an active field of research. Particularly in combination with USB-C, whose support the EU recently forced all device manufacturers to provide, exciting research questions arise. For example, there is as yet no research on hybrid juice jacking attacks, or on the prevalence and vulnerability of firmware updates via USB Power Delivery.

Proprietary solutions in particular have proven in the past to be a source of exciting research questions. Examples relevant to juice jacking were the investigation of proprietary AT interfaces that can be addressed via USB by Tian et al. [19] or the investigation of vendor-defined messages for USB Power Delivery by Alendal et al. [20].

7. Summary

In this report, we examined juice jacking attacks on mobile devices. After explaining necessary information on the USB standard and the connectors involved, we provided an overview of the emergence of early juice jacking attacks. Finally, we discussed various approaches for current attacks and corresponding countermeasures.

Although the potential for attacks still exists at the technical level, current attacks are either only capable of data extraction to a very limited extent or have to be adapted to a specific target device.

References

[1] D. Goodin, „Ars Technica: Those scary warnings of juice jacking in airports and hotels? They’re mostly nonsense,“ 05 2023. [Online]. Available: https://arstechnica.com/informationtechnology/2023/05/fearmongering-over-public-charging-stations-needs-to-stop-heres-why/. [Zugriff am 01 2024].

[2] B. Krebs, „Krebs on Security: Why is ‘Juice Jacking‘ Suddenly Back in the News?,“ 04 2023. [Online]. Available: https://krebsonsecurity.com/2023/04/why-is-juice-jacking-suddenly-back-in-thenews/. [Zugriff am 01 2024].

[3] Compaq, Digital Equipment Corporation, IBM PC Company, Intel, Microsoft, NEC, Northern Telecom, „Universal Serial Bus Specification,“ 01 1996. [Online]. Available: https://web.archive.org/web/20180130144424/https://fl.hw.cz/docs/usb/usb10doc.pdf. [Zugriff am 01 2024].

[4] Compaq, Digital Equipment Corporation, IBM PC Company, Intel, Microsoft, NEC, Northern Telecom, „Universal Serial Bus Specification Revision 1.1,“ 09 1998. [Online]. Available: https://fabiensanglard.net/usbcheat/usb1.1.pdf. [Zugriff am 01 2024].

[5] Compaq, Hewlett-Packard, Intel, Lucent, Microsoft, NEC, Philips, „Universal Serial Bus Specification Revision 2.0,“ 04 2000. [Online]. Available: http://sdpha2.ucsd.edu/Lab_Equip_Manuals/usb_20.pdf. [Zugriff am 01 2024].

[6] USB Implementers Forum, Inc, „On-The-Go Supplement to USB 2.0 Specification,“ 12 2001. [Online]. Available: https://www.rockbox.org/wiki/pub/Main/DataSheets/OTG1_0a.pdf. [Zugriff am 01 2024].

[7] Hewlett-Packard Company, Intel Corporation, Microsoft Corporation, NEC Corporation, ST-NXP Wireless, Texas Instruments, „Universal Serial Bus 3.0 Specification,“ 11 2008. [Online]. Available: http://www.softelectro.ru/usb30.pdf. [Zugriff am 01 2024].

[8] USB 3.0 Promoter Group, „Universal Serial Bus Type-C Cable and Connector Specification,“ 08 2014. [Online]. Available: https://www.usb.org/sites/default/files/USB%20Type-C%20Spec%20R2.0%20-%20August%202019.pdf. [Zugriff am 01 2024].

[9] USB 3.0 Promoter Group, „Universal Serial Bus Power Delivery Specification,“ 07 2012. [Online]. Available: https://www.usb.org/document-library/usb-power-delivery. [Zugriff am 01 2024].

[10] B. Krebs, „Krebs on Security: Beware of Juice-Jacking,“ 08 2011. [Online]. Available: https://krebsonsecurity.com/2011/08/beware-of-juice-jacking/. [Zugriff am 01 2024].

[11] Y. J. C. S. T. W. P. H. C. P. R. Billy Lau, „Mactans: Injecting Malware into iOS devices via malicious chargers,“ in BlackHat, 2013.

[12] W. H. L. S. M. S. K. Weizhi Meng, „Charging Me and I Know Your Secrets!: Towards Juice Filming Attacks on Smartphones,“ in CPSS ‘15: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 2015.

[13] W. H. L. S. M. S. K. Weizhi Meng, „JuiceCaster: Towards automatic juice filming attacks on smartphones,“ Journal of Network and Computer Applications, Bd. 68, 2016.

[14] H. G. Q. Y. Yuanda Wang, „GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line,“ in Network and Distributed Systems Security (NDSS) Symposium, 2022.

[15] P. G. G. Z. A. F. K. S. B. Qing Yang, „On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-Channel,“ IEEE Transactions on Information Forensics and Security, Bd. 12, Nr. 5, 2017.

[16] L. P. I. P. E. T. Y. Y. Daniel Genkin, „ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels,“ in CCS ‘16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[17] X. G. C. Y. Patrick Cronin, „Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakag,“ in Proceedings of the 30th USENIX Security Symposium, 2021.

[18] L. A. V. M. M. C. Riccardo Spolaor, „No Free Charge Theorem: A Covert Channel via USB Charging Cable on Mobile Devices,“ Lecture Notes in Computer Science, 2017.

[19] G. H. J. C. V. F. C. R. P. T. H. V. L. H. A. R. M. G. K. B. Dave Tian, „ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem,“ in Proceedings of the 27th USENIX Security Symposium, 2018.

[20] S. A. G. O. D. Gunnar Alendal, „Exploiting Vendor-Defined Messages in the USB Power Delivery Protocol,“ in IFIP International Conference on Digital Forensics, 2019.

---

1. https://twitter.com/FBIDenver/status/1643947117650538498 ↩
2. https://twitter.com/FCC/status/1645849934728511494 ↩
3. https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and- teddy-bears-via-usps/ ↩
4. https://www.zdnet.com/article/fbi-cybercriminals-are-mailing-out-usb-drives-that-will-install- ransomware/. ↩
5. https://shop.hak5.org/products/omg-cable ↩