The Threat of Juice Jacking

N Veerasamy

Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa

nveerasamy@csir.co.za

Abstract: Cyber attacks can affect the confidentiality, integrity and availability of data/ systems. Some attacks aim to steal data whereas others try cause destruction. One such vulnerability stems from the malicious use of USB chargers. When travelling and our smartphone battery level is very low, users may find a nearby charging station. However, users need to think twice before simply plugging in their device. What seems like an innocent charge could turn into a golden opportunity for attackers. Malware could actually be introduced into smartphones and other devices through the USB charger. Juice jacking is emerging as a potential risk as cyber criminals aim to infect users and potentially steal their passwords and infiltrate bank accounts. Users could even get locked out of their devices. This paper takes a closer look at this developing threat. These public charging stations are now being fraudulently used by attackers to gain access to sensitive information. Scammers are now using USB chargers as a method to steal data or install malware. However, users may be unaware of the potential risk. In this research, the malicious use of USB charging stations found in spots popular with travellers are revealed. In addition, protective measures are described in order to help users from falling victim to this latest cyber threat. Attackers try to take advantage of the situation in that most users trust their mobile devices more than their desktop devices. In addition to data theft, malicious attackers could also cause destruction of our mobile devices. When fast charging, malware could be installed onto a mobile device overwriting its firmware and arming it as a weapon. The firmware could be overwritten and the phone overloaded. The charger is thus compromised and used to overload a device. These various attack vectors are discussed in the paper to show the danger of juice jacking.

Keywords: juice jacking, USB, charge station

Introduction

The popularity of smartphones has grown tremendously over the past decade. The number of smartphone users worldwide today surpasses three billion and is forecast to further grow by several hundred million in the next few years- see Figure 1 (O' Dea S, 2020) . With its increased use comes the dependency to keep the devices charged. USB charging stations offers a convenient form of keeping these devices powered on.

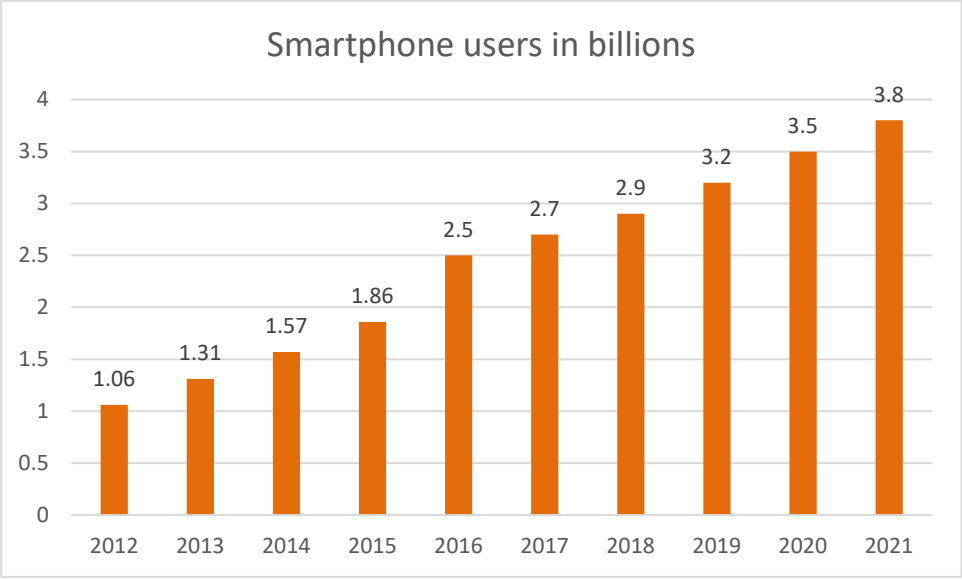

Figure 1: Smartphone users in billions (Statista .com 2020)

Many users may experience feeling of panic when their smart phone battery is about to die while on the go. The discovery of a USB charging station in public locations like airports, hotels, libraries, public transportation and malls provides some relief. However, the public needs to exercise caution before simply plugging in for a power boost.

A new form of security exploitation in the form of “Juice Jacking” has emerged. Public USB charging stations can now be used to infect malware onto smartphones and other devices. Public charging stations now pose a risk and users are advised not to use them without some form of security measures. In an extreme case, there is the potential that a free phone charge could even result in a bank account being drained due to the infection of malware that steals passwords. “A free charge could end up draining your bank account," Deputy District Attorney Luke Sisak warns, adding the malware has the ability to lock devices and share passwords with hackers (Edmond 2019). Adversaries will continue to target our smartphones with attacks like malware, malicious apps, accessibility abuse, ransomware and ad fraud. When a user’s device is infected, there lies the potential for data to be read and exported, including passwords. There also lies the possibility that the device is infected with ransomware and the user is locked out of their device, making them unusable.

The concept of juice jacking was first coined by Brian Krebs in 2011 with a proof of concept at DEFCON. A free charging station was set up but when users plugged into their devices, the following warning message appeared on the kiosk (Krebs, 2011):

“You should not trust public kiosks with your smart phone. Information can be retrieved or downloaded without your consent. Luckily for you, this station has taken the ethical route and your data is safe. Enjoy the free charge!”.

Other proof of concepts have been created over the years. Mactans was presented at the Blackhat 2013 security conference and showed a malicious USB wall charger with malware for iOs devices (Cimpanu 2019).

Then in 2016, KeySweeper a stealthy Arduino-based device was demonstrated. It was camouflaged as an operational USB wall charger but actually was able to passively sniff, decrypt, log and report back (over GSM) keystrokes of any Microsoft wireless keyboard in the vicinity (Cimpanu 2019).

Moreover in 2016, another malicious USB wall charger proof of concept was developed. This one was capable of recording and mirroring the screen of the device plugged in for the charge and lead to the concept of “video jacking” (Cimpanu 2019).

Juice jacking is a type of cyberattack in which a charging port that is also used for data connection is hijacked for malicious purposes. The cyber attacker hijacks the power supply (hence juice jacking) and utilises it for offensive actions. This is done by installing malware on the victim’s device and/or stealing data. The malicious programs that are installed can track the device or mirror the screen to capture passwords and PIN codes while the device is charging. This leads to juice jacking also being termed juice filming or “juice filming charging attacks” (Crane 2020). Cybercriminals wait for victims to use a USB charging connection in order to launch an attack.

Hackers are aware that users may not willingly plug an unfamiliar storage device into their machine, but they think of charging cables and power banks as batteries, not IT devices (Kumar 2020).Juice jacking is comparable to card skimming scams in that an attackers sets up a malicious device over a real charging station.

USB cables can be branded to look like any other cable. This creates the impression that the cables are safe and users do not suspect that the cables are malicious. In some cases, malicious cables can even be given away as promotional gifts (Ortiz 2019).

In a survey carried out by SpreadPrivacy.com in 2020 of 1029 American adults, 54.6% of respondents were not aware of the risk of public charging stations.

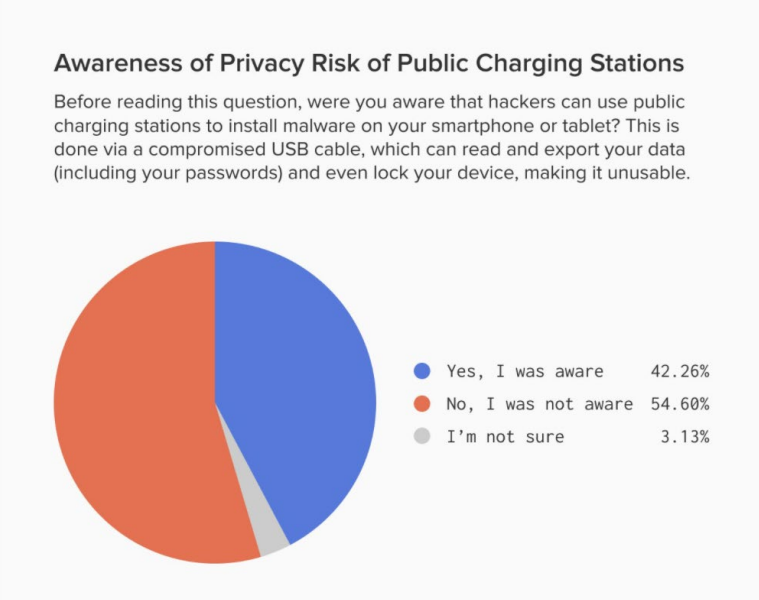

Figure 2: Survey of awareness of risk of public charging stations (Spreadprivacy.com 2020)

Juice Jacking Explained

When a smart phone is plugged into the USB port of a computer or laptop, there is an option to transfer files across the two systems. A USB port is not only a power socket but also the ability to transfer data. A standard USB connector has five pins. One pin is used to charge the receiving end. Two of the others can by default used for data transfers. Table 1 shows a summary of USB connections.

Table 1: USB connection table (Sunrom in Arntz 2019)

Pin	Name	Cable Colour	Description
1	V Bus	Red	+5V
2	D-	White	Data-
3	D+	Green	Data+
4	ID	N/A	Permits distinction of a host connection from device connection: - Host: connected to the signal round - Device: not connected
5	GND	Black	Signal ground

Unless, changes have been made in the settings, the data transfer mode is disabled by default, except on devices running older versions of Android. When a user connects to a USB port for a charge, they could be opening up a pathway through which data can be moved across.

Generally, a juice filming charging attack should have the following characteristics (Meng et al. 2019): 1) easy to implement yet efficient; 2) ease of use- i.e. user-friendly; 3) does not need the attacker/user to install additional application or component on the target device; 4) no additional permission requested from the device; 5) cannot be detected by existing anti-malware software; 6) scalable and effective on a broad range of devices (Eg, Android, iOS, Windows); and automatic extraction of textual information from captured videos.

Juice jacking attacks can fall into two main categories:

- Data theft: Once the device is plugged into the compromised/fake charging station using data- transmitting USB cables, data is stolen like passwords and pins. Data theft can be automated. Malware could be planted onto the device and an additional payload dropped that steals information from connected devices. Crawlers exist that search a phone for personally identifiable information (PII), account credentials, banking related or credit card data seamlessly. Malicious apps can also clone all of the phones data onto another phone with the use of a Windows or Mac computer as an interface. An attacker can thus gain access to a wealth of information that can be used to impersonate another user. Mobile devices contain an abundance of PII that can also be sold on the dark web for profit or used as part of social engineering scams.
- Malicious installation: Users make use of compromised mobile device accessories like charging cables (e.g., an O.MG cable which has a hidden microchip inside the USB-C cable). Such a device appears like an ordinary lightning charging cable but it has been transformed into phone charger that can infect your device. Microcontrollers and electronic parts have become so small that attackers can hide mini-computers and malware inside the USB cable itself such as the O.MG cable (Cimpanu 2019). Attackers can make use of these exploited cables to infect the device with malicious payloads. Malware has the potential to monitor and track users' activities over a period of time. For example, malware can capture information like GPS location, purchases, social media engagements, photos, call logs and other processes. The range of malware that attackers could install includes adware, crypto-miners, ransomware, spyware and Trojans. Crypto-mining makes use of a mobile phone's CPU/GPU to mine for cryptocurrency and drain its battery. Ransomware prevents access to a phone by encrypting the device and demanding a ransom payment. Spyware results in continuous monitoring and tracking of the victim and Trojans hide in the background and can release other infections as well. Some signs that can indicate a possible infection include a slow phone, quickly drained battery, random icons on the screen, advertisement popups, notifications and a strange large phone bill. In some cases, the malware may leave no trace at all which makes it difficult to detect that the phone is infected.

An even more extreme form of juice jacking is the physical destruction of the device through digital methods. This vulnerability resides in mass-market fast chargers that are being used worldwide. When a device is connected to a fast charger with a USB cable, a negotiation occurs between the two, thereby establishing the most powerful charge that a device can handle. The management of the negotiation of this charge is handled by the firmware on the device and firmware on the charger. There is an underlying assumption that both will co-operate with each other. However, if the charger is compromised, this negotiation can be overridden and more power can be pushed down the cable than the device is able to handle safely. This will effectively destroy the device and even potentially cause a fire. A fast charger is fundamentally a smart device and thus it can be tampered with. The attack vector consists of loading malware onto the smartphone. When the device is connected to the charger, the firmware is overwritten which makes it a weapon for whatever is plugged in next. The curveball is that the malware may be targeted at the device itself. Malware can initially be pushed onto a phone. The first time the phone is connected to the vulnerable fast charger, the phone overwrites the firmware. The next time the phone is connected to the same charger, the phone will be overloaded with power. This type of attack is termed "BadPower" and products with Badpower issues can be attacked with special hardware and target smart devices like mobile phones, tablets and laptops that support the fast charging protocol.

In research carried out by Tencet, 35 fast chargers were tested. Of those, they found "at least 18 had BadPower problems and involved eight brands." Of those 18 charging devices, 11 were vulnerable to a simple attack through a device that also supports the fast charging protocol, such as a mobile phone (Duffman 2020). The advice offered is not to plug 5V devices with fast chargers with USB to USB- C cable. Users need to exercise care when connecting smart devices with a smart cable as it is capable of doing more than just a simple charge. These findings are indicative of the perils of the rapidly expanding IoT space. Various devices can be purchased and plugged in. Technology continues to grow with a myriad of devices and there countless little computers in the forms of phones and tablets. Data can be stolen and devices compromised. In addition, relatively innocent acts like charging a device can result in total destruction.

Protection again Juice Jacking

A few steps can be taken to keep mobile phones and devices charges while on the go. The following measures can be implemented to protect against this type of threat:

- Training: Cyber awareness training to educate employees about the dangers of USB charging stations should be carried out. Users need to be educated about why they should not plug their data transmitting USB cables into public USB ports as they could potentially be exploited.
- Avoid the use of free, promotional USB charging station to prevent becoming infected

- Do not make use of plugs that are left plugged into public USB charging stations. This is comparable to the scenario whereby a lost USB is picked up from the ground. There is no way of knowing that the USB device is secure and does not contain malware and so too random technology can be tampered with and should not be implicitly be trusted.
- Only make use of USB devices from trusted reputable supplies
- If connecting , also ensure that the "Decline" option is selected when asked whether to trust the connected device
- Make use of power banks as a backup power supply. Although power banks have limited charging capabilities, they can still offer some power to hold off until a location can be found with an AC wall charger. Certain types and brands of power banks can hold enough power for several recharges. Rather invest in a high capacity power bank that can even charge multiple devices. This will help eliminate the need to look for suitable power outlets constantly.
- Make use of a USB Condom or Power-only USB cables in public. USB condoms are a devices that can serve as a buffer between the data charging cable and the public USB port. It acts as a data blocker and prevents data from being transmitted between the cable and the USB port. It limits access to the power source only and does not connect the data transfer pins. They can be attacked to the charging cable as an "always on" protection. The use of a USB data blocker or "juice- jack defender" can help prevent data exchange when the device is plugged into another device with a USB cable.
- Make use of AC adapters or power-only USB cables that can be charged through the standard AC power outlets. Carry the correct adapters for various power outlets along your route (or a universal type adapter).
- Some phones have USB preference settings. However, this is not a fully secure option. Despite setting the "no data transfer setting" data transfers have still taken place.
- Try to fully charge devices before going out.
- Non-USB options like external batteries and wireless charging can also be used.
- Switch off the device, when using a charger that is not yours. This may allow the device to be charged without any transmission of data.

Conclusion

Attackers are keen to find new and creative ways to infiltrate devices. Users need to remain current on the latest threats and trends. When a phone or laptop is running out of battery power, user may be keen to plug into a charging station at public locations like airports, hotels or the mall. What appears like a seemingly ordinary smartphone charge can result in a user's phone being infiltrated and infected. Through juice jacking, hackers have found an innovative way to compromise smart technology and potentially steal data or infect devices. This paper tries to create awareness on a potential exploit that can see users infecting themselves with malware or exposing their sensitive data on smart phone, tablets and other devices. The aim of this paper is to help users prevent falling victim to this type of attack and help protect themselves by describing the manner in which this attack is carried out and how to protect against this threat.

Cyber attacks are typically associated with threats like phishing, ransomware or malware. However, attackers are also keen to infiltrate devices via the USB port on smart phones. This digital form of ambushing compromises the data on a smart phone and can become a serious issue. The question arises whether this is a real threat and whether users should be concerned. From a business point of view if an attacker is able to gain backdoor into the company's data and systems, this can potentially lead to the infection of scams, malware or data theft. Ransomware or crypto miners could be planted onto a user's device. Potentially, business critical information could also be stolen. Juice jacking could potentially escalate in the future as attackers try to grow their arsenal of attacks. While it may not be as common as phishing or ransomware it is important that people are made aware of this type of threat. This paper tries show the practicality of this type of attack as attackers aim to become more ingenuous. The issue could escalate in the future as hackers try to expand their attack field.

References

Arntz, P. (2019) Explained: juice jacking, Malwarebytes labs. [Online]. Available at: https://blog.malwarebytes.com/explained/2019/11/explained-juice-jacking/, (Accessed 18 December 2020).

Cimpanu, C. (2019). Officials warn about the dangers of using public USB charging stations. [Online], Available at: https://www.zdnet.com/article/officials-warn-about-the-dangers-of-using-public-usb-charging-stations/, (Accessed 18 December 2020)

Crane, C. (2020) Juice Jacking: How Hackers steal your info when you charge devices. [Online]. Available at: https://securityboulevard.com/2020/02/juice-jacking-how-hackers-can-steal-your-info-when-you-charge-devices/, (Accessed 18 December 2020)

Doffman, Z. (2020) Hackers Can Now Trick USB Chargers To Destroy Your Devices—This Is How It Works Forbes. [Online]. Available at: https://www.forbes.com/sites/zakdoffman/2020/07/20/hackers-can-now-trick-usb-chargers-to-destroy-your-devicesthis-is-how-it-works/?sh=383c0f95bf27, (Accessed 18 December 2020)

Edmond, C. (2019) Hackers can use public USB chargers to steal personal data. Here's what you need to know about 'juice jacking'. [Online]. Available at: https://www.weforum.org/agenda/2019/11/phone-cell-mobile-charging-usb-security-malware-criminal-juice-jacking-cyber-security/, (Accessed 18 December 2020)

Krebs, B. (2011) Beware of Juice Jacking. [Online]. Available at: https://krebsonsecurity.com/2011/08/beware-of-juice-jacking/, (Accessed 18 December 2020)

Kumar, Y. (2020) Juice Jacking - The USB Charger Scam. [Online]. Available at SSRN: https://ssrn.com/abstract=3580209 or http://dx.doi.org/10.2139/ssrn.3580209 , (Accessed 5 January 2021).

Meng, W. Jiang, L. Choo, K,K.R. Wang, Y. and Jiang, C. (2019) "Towards detection of juice filming charging attacks via supervised CPU usage analysis on smartphones", Computers & Electrical Engineering, Vol 78,pp 230-241.

O'Dea, S. (2020) Number of smartphone users worldwide from 2016 to 2021 (in billions), [Online]. Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/, (Accessed 18 December 2020).

Ortiz, A. (2019) Stop! Don't Charge Your Phone This Way. [Online] Available at : https://www.nytimes.com/2019/11/18/technology/personaltech/usb-warning-juice-jacking.html, (Accessed 5 January 2021)

Spreadprivacy.com (2020) The risky business of charging your phone in public, Available at : https://spreadprivacy.com/privacy-risks-usb-charging/, (Accessed 6 April 2021).