European Journal of Information Technologies and Computer Science
www.ej-compute.org

The Cyber Crime of Juice Jacking in Developing Economies: Susceptibilities, Consequences and Control Measures

John Adinya Odey, Bamidele Ola and Iwinosa Agbonlahor

ABSTRACT

It is convenient and the norm to have both data and power cables (battery charge) integrated as a single Universal Serial Bus (USB) cable for today's mobile devices. While the data component of the cables serves as the channels for data communication, the power channel charges the mobile devices through an adapter connected to an Alternating Current (A/C) socket or directly to a USB port. This convenient and seemingly harmless design could also serve as a medium through which malicious hacks are carried out on the connected mobile devices as studies and recent experimentations has shown. This hacking variant called Juice Jacking now serve as a potential avenue for mobile device exploitation, especially in developing economies where poor power grid infrastructures has allowed for indiscretions in charging devices from any available. This paper formulates a simple architecture for Juice Jacking cyber-crime, review prove-of-concept experimentation for Juice Jacking from available literatures, identifies significant threats and levels of impact of this cyber-crime on the community. It also highlights strategies that could mitigate juice jacking in developing economies.

Keywords: Juice Jacking, cyber-crime in developing economies, USB cybercrimes, Susceptibilities and Control Measure of Juice Jacking.

Published Online: November 03, 2021

ISSN: 2736-5492

DOI :10.24018/ejcompute.2021.1.5.33

J. A. Odey
Department of Computer Science, University of Calabar, Calabar, Nigeria
(e-mail: johnodey@unical.edu.ng)
B. Ola*
Department of Computer Science, University of the Cumberlands, USA
(e-mail: bola43559@ucumberlands.edu)
I. Agbonlahor
Department of Computer Science, University of Calabar, Calabar, Nigeria
(e-mail: iwinosaagbonlahor@unical.edu.ng)

****Corresponding Author***

I. Introduction

Developing countries, especially those in Sub Saharan Africa, conveniently lag behind in the development and utilization of electric power infrastructures. However, current report from the International Telecommunication Union (ITU), [1] indicates that "developing countries now account for the majority of Internet users, with 2.5 billion users compared to one billion in developed countries". The increasing use of information technology systems by individuals, small and medium enterprises (SMEs), corporations in developing countries has the potential to bring substantial benefits but in the same vein, exposes it users to cybercrime.

Cybercrime is any activity that targets a computer or networked devices with malicious intentions. Recently, cyber-crime has been on the rise in developing countries due to inadequacy of security tools and strategies on information technology (IT) infrastructures resulting in varied vulnerabilities. These vulnerabilities create risks for economies that rely on the integrity of these IT infrastructures.

Juice jacking is a cyber-security threat that's brimming with potentials for cyber-criminals; it is a type of cyber-crime that involves unwary users connecting to a compromised USB power charging ports in a bid to charge their mobile devices (mobile phones, note pads, game consoles etc.), without the knowledge that the devices compromised. Juice jacking is a topical cyber-crime carried out typically over the USB; it involves using a USB cable to connect a mobile device through the charging port of a modified USB charging stations, and thus granting illegal access to the contents of mobile devices or allowing the transfer of unhealthy malwares to these devices. This likelihood is made possible because majority of today's USB power charging cables have both capacities to charge mobile devices as well as to allow data communication when connected to USB port [2]. As a norm, users of mobile devices find it comfortable to quickly connect their device to any available USB socket to recharge their batteries when their battery is getting low or drained as shown in Figure 1. This regular practice which was in the past harmless and habitual must now be carried out with great caution as studies and prove-of-concept (PoC) experimentations have confirmed that hackers can now perform malicious attacks on mobile devices through the USB cable as there are plugged to charge.

Juice jacking has raised brows and scares in every place its awareness has reached. This is because of the ease of susceptibility and risks of it happening to anyone is enormously high and the consequences outrageous. This reality poses a great risk to everyone, but even to residents of developing economies, who suffer poor electricity supply,

European Journal of Information Technologies and Computer Science
www.ej-compute.org

very poor cyber security administration, and other numerous peculiar challenges that increases vulnerabilities to this hazard.

Fig. 1. An automobile bus charging port.

A. Architecture of Juice Jacking

Juice jacking is a topical cyber-attack carried out typically over USB; it involves infiltrating and/or ex-filtrating a mobile device via a USB cable connected to a compromised charging source.

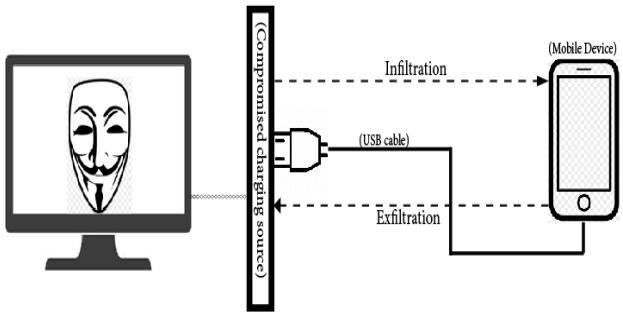

Fig. 2. A simple architecture of Juice Jacking attack.

TABLE I: USB CONNECTION TABLES [18]

Pin	Name	Cable Color	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 signal ground • device: not connected
5	GND	Black	Signal ground

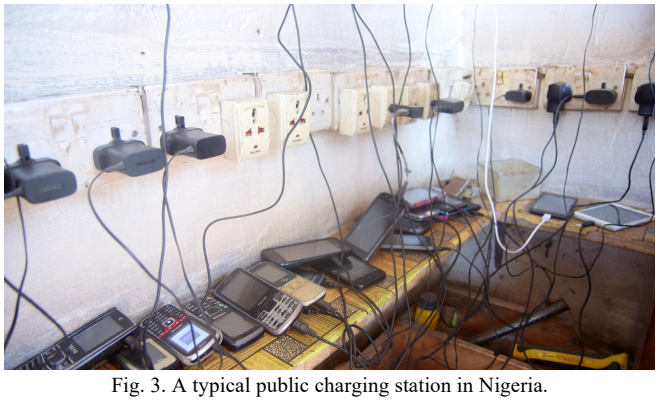

Fig. 3. A typical public charging station in Nigeria.

When charging your cell through the USB port of your mobile devices, you will get a prompt to transfer files back (Exfiltration) and forth (Infiltration) between the two devices. That is because the USB port is not only a power socket but could serve as a medium to transfer files. A regular USB connector has five pins, where only one is needed to charge the receiving end. Two of the others are used by default for data transfers.

B. The Problem

Developing economies who are quickly embracing the numerous opportunities available in cyberspace have begun utilization of the provisions of the internet in almost every of their industries and public institutions. Some of these institutions significantly utilizes IT infrastructures as a core entity for the running of their organizational structure. However, according to [3] most developing countries lack a healthy and secure cyber space, which poses great risk to any player within this domain. Another notable challenge in developing countries is the absence of reliable electricity supply from the power grid infrastructures. This challenge compels residents to utilize any readily available power outlets to charge their mobile devices. This practice could expose their devices to the exploitation of juice jacking.

Also, the dearth of research and academic publication on juice Jacking has made public awareness of this cybercrime nonexistent. There is a general lack of public awareness about the existence and behavior of juice jacking even in most developed country; a poll taken in the United State of America (USA) among 1,029 American adults surveyed, 54.6% (±3.1) of all respondents weren't aware of this risk [19].

II. LITERATURE REVIEW

Juice jacking threat was first brought to public conversation in 2011 at DefCon, when researchers from Aires Security experimentally staged a public charging kiosk advertising a free charging outlet, but when users plug in their devices, the screen switched to a warning post educating that malware could be transferred through public charging stations [6], [12], [13]. Since then, a number of researchers have come up with proves that malware could be transferred via USB cables.

In 2012 Kyle Osborn, a security researcher described an attack he called Phone to Phone Android Debug Bridge (P2P-ADB). The attack allowed one Android phone to attack another Android phone stealing authentication keys allowing unauthorized access to their mailing accounts and unlocking their phone, through a USB cable, it made use of USB OTG (on-the-go) features [12], [13].

The year following at the Black Hat Conference (2013), Georgia Institute of Technology researchers introduced 'Mactans', an experimentation that presented an electronic device that could fit into a USB wall charger or AC adaptor to deliver iOS malware in seconds, and the attacked device will launch a Trojan virus when the user opens their Facebook app. This hack was affected on an Apple iPhone [10], [12], [13].

In 2014 firmware of USB microcontrollers made by 'Phison' a Taiwanese company was reprogrammed by some researchers, upon which this reprogrammed firmware could be corrupted with malware, impersonate a keyboard to allow an attacker perform keystrokes on a victim's machine, and also can inject malware into files as they are copied from a

USB device to a computer, turning the computer port into a vector, able to infect other USB devices afterward connected to the computer [14].

With the use of an Arduino-based USB AC adaptor, Samy Kamkar, a security researcher in 2015 could decrypt and record all keystrokes from any Microsoft wireless keyboard within range, this device He called KeySweeper [10]. Aries security researchers in 2016 demonstrated again at DefCon the ability of smartphone to mirror that displays onto another monitor, this also is transmitted through a HDMI-USB charging cable. This practice could visualize and record the contents of the mobile device, and displaying it to another screen [13], [15].

During the RSA conference in 2016, Symantec researchers proved that if an iOS device is granted access to a system to exchange data, this access also applies to the iTunes API which is accessible over wifi. This connection could allow access to an iOS device even after the user has unplugged the device from the USB source, this they dubbed as Trust-jacking [13], [20].

Florida Institute for Cyber Research, in 2018, during the 27th USENIX symposium on security presented a PoC that showed multiple vulnerabilities on a target phone when they exploited some old modem commands when accessed over USB. The exploitation proved that an attacker could unlock a USB connected target phone and take full control of the phone [15]. This threat was quickly addressed by responsible vendors. In 2019 a researcher by name MG developed a USB-Type C cable which hides a chip that could be remotely activated; this could act as a USB-HID (Human Interface Device), mouse or keyboard on any system when connected. The USB he called O.MG cable [15].

III. Methodology

During the course of carrying out this research, searches for literatures were performed on several academic libraries and search engines, using these keywords: juice jacking, cyber-crime in developing countries, cyber-crime, USB cyber-crime, hacking. A number of articles were reviewed, and 20 articles were selected and referenced in producing this paper, as was relevant to the purpose of the study. Knowledge drawn from these literatures formulated this research paper. An architectural framework for juice jacking was developed. A composite behaviour of juice jacking was designed, the present means through which it is practiced, and the several proven exploitations possible by the attack. In addition, the risk it poses on developing nations was discussed and technical advice to mitigate juice jacking was proposed.

IV. Editorial Policy

About 85% of referenced articles directly talked about juice jacking, the history, experimentation, its risks, and control measures, the others talked on cyber-security in developing economies and hacking. Research and proof -of-concepts experiments have been carried out over the years that validate the possibility that hacks can be conducted on mobile devices via a USB port connection. Also, these experimentations have proven that this USB exploitation can be in the form of exfiltration (allowing the transfer of data from the mobile devices) and/or infiltration (allowing the transfer of data to the devices).

A review of the prove-of-concept experimentations has shown that hacking through juice jacking can enable an attacker to unlock connected phones [17], steal personally identifiable information (PII), launch Trojan virus, record and keystrokes of a keyboard, mirror device display, and even establish remote access points during and even after disconnection from the USB plug.

An alarming 50% of the referenced articles decry that the awareness of this threat to the public is grossly inadequate, in comparison to the threat that it poses. Some other authors [4]-[6] argue against the need to panic, seeing juice jacking has not been implemented in the wild, stressing that all evidence of its existence have only been prove of concepts (PoC) experimented by ethical hackers. This argument is in conflict with the claims that there are known cases in the east coast [4], and Snowden's report which submitted that Juice Jacking was used by NSA to install malware on a mobile device firmware in a bid to track information of persons of interest [7].

It was discovered in the course of this research that very little academic publications has been carried out on juice jacking, however a number of bloggers and content writers have taken it upon themselves to sensitize on the history and nature of juice jacking, drawing knowledge from the various experimentations and prove-of-concept.

V. Susceptibility of Mobile Devices to Juice Jacking

Juice jacking attack is actually surreptitious in nature, meaning a device could have been compromised without the owner ever knowing that they had fallen victims [8]. Identified red flags if confirmed present in mobile devices, that should necessitate device integrity checks and initiation of recovery procedures were necessary. These red flags include:

1. A rise in periodic data usage: Some malwares utilize user's internet service, thereby propelling abrupt increase in the data usage without any significant change of data usage pattern by the user.
2. Rapid Battery Discharge: There are viruses that suck battery charge. If a cell charge seems to be abruptly quickly drained, this is a possible red flag that your device may have been compromised.
3. Identity theft Alert: When a victim is under attack, their personally identifiable information (PII) could be obtained and used to impersonate the victim for financial gains, blackmail, or access to secured data.
4. Existence of unsolicited apps: Trojan malware infecting a device will automatically download unsolicited malicious apps which should also attract concerns [5].

Observing any such behaviors should draw any user attention to the suspicion that their devices may have been compromised and should initiate rescue alternatives. The attack can really be invasive and may require the formatting of the mobile device completely and reinstallation of the factory settings to regain device integrity [9].

A. Factors That Could Abate Juice Jacking in Developing Countries

As summarized in [3], the following factors affect the implementation and susceptibilities of efficient cyber security strategies in developing countries, these factors are grouped into two (2), internal and external environmental factors as depicted in Fig. 4. These factors negatively affect the setting up of reliable cyber security infrastructures in developing countries and this makes the cyber-space of these nations vulnerable to exploitation to cyber-crimes including Juice Jacking. Fig 4 summarizes the list of these factors.

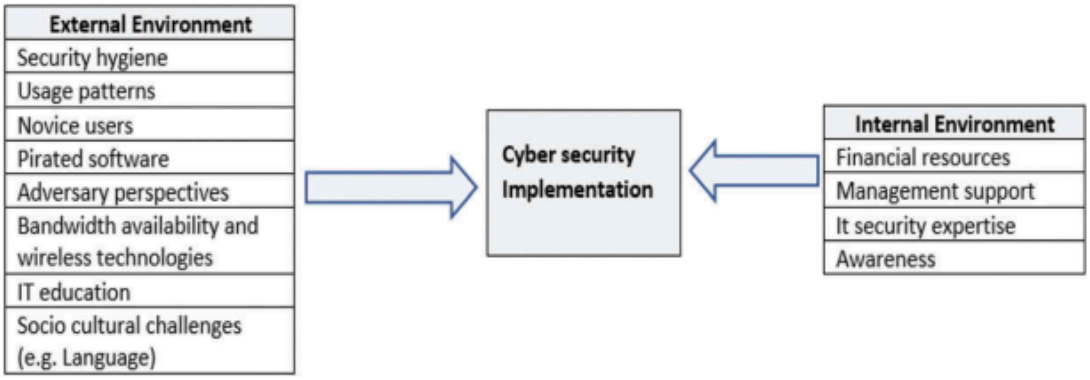

Fig. 4. Factors influencing the implementation of cyber-security in developing countries [3].

Also developing economies are susceptible to Juice Jacking among several cybercrime due to the following reasons:

1. Unreliable power supply to recharge cells which subjects residents to seek alternative means to power their devices.
2. The ease at which it can be executed on unaware device owners.
3. It is also very cheap to setup, the hardware to facilitate juice jacking can be designed for as less as $10.
4. Humans have a high tendency to plug into ubiquitous USB ports in airports, commercial shops, theme parks, hotel rooms, without consideration.
5. The devoted dependency on mobile devices which utilizes the charge of the cell.
6. Absence of sustainable frameworks to checkmate fraudulent attacks also presents this cyberspace as a luxuriant playground for this form of attack.
7. The lack of proper awareness on Juice jacking.

VI. Consequences

The impact juice jacking could have on individuals, industries and society are enormous and are as varied as any security compromise could, from illegal access to data and IT infrastructure to planting of unhealthy bugs in compromised systems. It could take the form of Malware installation, Emotet, Denial of Service (DoS), Man-in-the-middle, Phishing, device-mirroring, Password attacks, backdoor attack, etc.

As stated by [10] Juice jacking poses a particularly high risk to businesses. The current annual ecommerce spending in Nigeria is estimated at $12 billion and is projected to reach $75 billion in revenues per annum by 2025 in Africa [11]. This makes businesses the most titillating targets of these infiltrators [12]. For example, should an employee who accesses a company mail/server with their smartphone, connects their device to a manipulated USB power station, perpetrators may get hold of corporate proprietary information such as login credentials and corporate secrets. This attack could lead to network-wide malware blitzes, industrial spying, spear-phishing attacks, and business email compromise (BEC) scams. Hackers may even be able to gain a foothold to the enterprise IT infrastructure and perpetrate effective swindles, poison the network with malicious programs such as ransomware, crypto mining and could also sell illegally obtained business-critical information to competition. These scenarios can depreciate investments and capital development within the cyberspace. Although the cyber space holds great prospects, yet its vulnerability could scare risk sensitive institutions from plugging into this pool of opportunities.

VII. Control Measures to Mitigate Juice Jacking

The follow general and technical measures are advised here to mitigate the crime of Juice Jacking in developing economies:

1. Public Awareness: It is said awareness remains the primary key to tackling and combating insecurity of any kind. However, very little is known about this threat by the public even in developed countries [19]. This is even worse in developing economies with little cyber security mitigation infrastructures and dysfunctional electricity grid systems. Corporations and SME's should include juice jacking to their security awareness trainings, educate team members and the public of the risk of exposure to Juice Jacking by using public ports and/or cables, just as the Los Angeles' district attorney [4] and antivirus giant Kaspersky [7] is doing to sensitize travelers of the risk involved in using a public USB charging points.
2. Portable Power Pack: In cases where users may be on transit or cannot access private AC ports to plug their

chargers to direct power, they are advised to make use of a personal portable power pack, popularly known as power bank. These handy devices could keep your device running for a considerate amount of time [20].

3. Use USB charge-only adapter: A USB charge-only adapter, also called USB condom is a small device that was released in 2012, it serves as a protective shield between the charging source and the charging cable. It works by stopping data flow through the USB cable but allowing just the charging service of a USB cable functional.
4. Use charging-only cables rather than data cables: Some USB cables allows for only charging connections, with allowing for data transfer. It only engages the connector's pin (or pins) required for charging and disengages the ones intended for data transfer – as simple as that [9].
5. Use the AC socket where possible: You can also maintain the traditional use of AC power socket with your own adapter and USB cable in charging your device [20], as they do not allow for data transfer [2].
6. Decline data transfer requests: Updates on most mobile devices operating systems (OS) now signify a consent prompt that appears whenever a charging session commences, seeking permission to allow or decline data transfer, declining such prompt while connected to untrusted sources can provide a safeguard to this attack. [10].
7. Switch Off the mobile device: Switching off your device before plugging it into the charging port, will only let the power supply flow and will avoid any data transfer. Windows Phone users may fall disadvantaged here, because whenever the phone is connected to a charging source it automatically switches on [9].

VIII. Conclusion

Without carefulness we can boldly say Juice Jacking is a very heavy sensitive cyber-threat brimming with dangerous possibilities. Although it is not yet very prevalent in use today, it is however presently applicable, and therefore its occurrence should be consciously prevented, as it could create serious problems for users of mobile devices. In Summary, it is advised that users avoid using the public charging stations but if they must, as may be the case in an emergency, it should be used with considerations of the afore-mentioned precautionary control measures.

References

[1] R. Hill, "Dealing with Cyber Security Threats: International Cooperation, ITU and WCIT, 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 2015, NATO CCD COE Publications, 2015.

[2] K. Sharma, *Juice Jacking - How it Happens & Safety Measures | REVE Antivirus*, REVE Antivirus, 2018. [Online]. Available: https://www.reveantivirus.com/blog/en/juice-jacking. [Accessed: 03- Jul- 2021].

[3] S. Kabanda, M. Tanner and C. Kent, "Exploring SME cybersecurity practices in developing countries," *Journal of Organizational Computing and Electronic Commerce* 28:3, 269-282, 2018.

[4] Z. Whittaker, *LA warns of 'juice-jacking' malware, but admits it has no cases,* Techcrunch.com, 2019. [Online]. Available: https://techcrunch.com/2019/11/15/los-angeles-juice-jacking-usb/. [Accessed: 04- May- 2021].

[5] M. Charboneau, *How to Avoid 'Juice Jacking' and Keep Your Data Safe While Traveling*, Men's Journal, 2020. [Online]. Available: https://www.mensjournal.com/travel/juice-jacking-usb-port-malware-privacy-data-protection/. [Accessed: 04- May- 2021].

[6] C. Crane, *Juice Jacking: How Hackers Can Steal Your Info When You Charge Devices – Hashed Out by The SSL Store™,* Hashed Out by The SSL Store™, 2020. [Online]. Available: https://www.thesslstore.com/blog/juice-jacking-usb-how-hackers-can-steal-your-info-when-you-charge-devices/. [Accessed: 04- Jun- 2021].

[7] "Juice Jacking History - Juice-Jacking Foundation", *Juice-Jacking Foundation*, 2021. [Online]. Available: https://juicejacking.org/juice-jacking-history/#_ftn19. [Accessed: 04- May- 2021].

[8] "Technical Juice Jacking – Juice-Jacking Foundation", *Juice-Jacking Foundation*, 2021. [Online]. Available: https://juicejacking.org/technical-juice-jacking/. [Accessed: 04- May- 2021].

[9] S. Peswani, *What is Juice Jacking and how to prevent it & protect your smartphone*, The Windows Club, 2018. [Online]. Available: https://www.thewindowsclub.com/juice-jacking-prevent-protect-device. [Accessed: 02- Jul- 2021].

[10] D. Balaban, *The Ins And Outs Of Juice Jacking Attacks | Information Security Buzz*, Information Security Buzz, 2020. [Online]. Available: https://informationsecuritybuzz.com/articles/the-ins-and-outs-of-juice-jacking-attacks/. [Accessed: 04- May- 2021].

[11] "Nigeria – eCommerce", International Trade Administration | Trade.gov, 2020. [Online]. Available: https://www.trade.gov /knowledge-product/nigeria-ecommerce. [Accessed: 02- Jul- 2021].

[12] M. Elgan, *Is Juice Jacking a Legitimate Threat or Nothing to Worry About?,* Security Intelligence, 2020. [Online]. Available: https://securityintelligence.com/articles/is-juice-jacking-a-legitimate-threat-or-nothing-to-worry-about/. [Accessed: 04- Jun- 2021].

[13] "Juice jacking – Wikipedia", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Juice_jacking. [Accessed: 04- Jun- 2021].

[14] A. Greenberg, *The Unpatchable Malware That Infects USBs Is Now on the Loose,* 2014. [Online]. Available: https://www.wired.com /2014/10/ code-published-for-unfixable-usb-attack/. [Accessed: 04- Jul- 2021].

[15] R. Lei, *A Short History of Juice Jacking*, Secjuice, 2019. [Online]. Available: https://www.secjuice.com/history-of-juice-jacking/. [Accessed: 02- May- 2021].

[16] L. Fitzgibbons, *What is juice jacking? - Definition from WhatIs.com*, SearchSecurity, 2020. [Online]. Available: https://searchsecurity. techtarget.com/definition/juice-jacking. [Accessed: 04- Jun- 2021].

[17] M. Potuck, *How to prevent juice jacking on iPhone and what is it? - 9to5Mac*, 9to5Mac, 2020. [Online]. Available: https://9to5mac. com/2020 /03/12/prevent-juice-jacking-iphone/. [Accessed: 04- Jun- 2021].

[18] P. Arntz, *Explained: juice jacking – Malwarebytes Labs,* Mal warebytes Labs, 2020. [Online]. Available: https://blog.malw arebytes. com/explained/2019/11/explained-juice-jacking/. [Accessed: 04- Jun- 2021].

[19] "The Hidden Privacy Risk of USB Charging Stations", *Spread Privacy*, 2020. [Online]. Available: https://spreadprivacy .com/privacy-risks-usb-charging/. [Accessed: 04- Apr- 2021].

[20] N. Goud, *Beware of Juice Jacking Cyber Attack – Cybersecurity Insiders*, Cybersecurity Insiders, 2020. [Online]. Available: https://www.cybersecurity-insiders.com/beware-of-juice-jacking-cyber-attack/. [Accessed: 04- Apr- 2021].