Threats of Juice Jacking: Security Issues and Control Measures

Pratin R[1]
[1]UG Student, AI&DS
Panimalar Engineering College,
Chennai, India.

Prawin Raj V M[2]
[2]UG Student, AI&DS
Panimalar Engineering College,
Chennai, India.

Vigneshwaran S[3]
[3]UG Student, AI&DS
Panimalar Engineering College,
Chennai, India.

ABSTRACT:

To create a secure system, it is crucial to develop security software that can safeguard the system against external attacks and protect the internal data from unauthorized access. Juice Jacking is a cyber-attack method which is done by hackers in order to gain unauthorized access to a system via USB connections and steal sensitive user data. USB is a commonly used standard for connecting peripherals in 5G computer systems and also for charging devices. However, the use of USB for transferring data between devices can pose significant security threats, and maintaining data privacy on the bus line is crucial to ensure data integrity. This work aims to analyse the attack by using 10 malware attacks which affects the device, and various ML and deep learning models were employed to predict and prevent these attacks. The experimental results showed that the deep learning model was effective in identifying and predicting the Juice Jacking attack. Additionally, the paper discusses several techniques that can prevent or mitigate Juice Jacking attacks, ensuring the security of the system and the privacy of the user's data.

Keywords: cyber-attack, malicious code, USB code, security, hacker, keystroke dynamics, authentication

I. INTRODUCTION:

Juice Jacking is a cyber-attack which targets mobile phones, tablets, and computers that support the Universal Serial Bus (USB). It typically uses a device's charging port and when someone plugs a specific device into the system using this connection, the hackers steal all of their personal data or may download malware onto the device [1]. As a result, it is important to recognize and stop these cyber-attacks. Public USB power charging stations are increasingly available to business travellers where they travel or stay. This attack is more suitable for Android OS and iOS, and the smartphone's display can be made visible through a regular Micro-USB coupled with the MHL standard or the iPhone's Lightning port [2]. However, a kiosk or other public charging points, may be prone to infected charger points might lead to security threats. When the device is connected with a computer, it can access some of the files like documents, images, e-mails and many more. In general, a USB connector can be used for both data and power transfer [5]. Ten years ago, researchers in the field of security discovered a way to take advantage of USB connections, which were commonly believed to be only for power transfer, in order to conceal and convey confidential information, as mobile phones became more widespread [3].

II. Types of juice jacking:

There are several types of juice jacking attacks that attackers can use to exploit vulnerabilities in public USB charging stations and steal sensitive data from mobile devices. Some of the most common types of juice jacking attacks include:

Malware injection: This type of juice jacking attack involves injecting malware onto a public charging station. When a user connects their device to the station, the malware is automatically downloaded onto their device and can be used to steal information or install additional malware [4].

Data Theft: In this type of attack, attackers use a compromised charging station to steal data from connected devices. This can include sensitive information such as login credentials, credit card information, and personal files [5].

Keylogger attacks: Keylogger attacks involve installing a keylogger on a public charging station that records every keystroke entered on a connected device. This can be used to capture login credentials, passwords, and other sensitive information.

Ransomware attacks: In a ransomware attack, attackers install ransomware onto a public charging station that encrypts the data on connected devices. The attackers then demand payment in exchange for the decryption key, which can be used to unlock the encrypted data.

Remote access attacks: This type of juice jacking attack involves installing a remote access tool (RAT) onto a public charging station that allows attackers to remotely access connected devices. This can be used to steal sensitive data, track a user's location, or control the device remotely.

Fake Charging Station Attacks: In this type of attack, attackers set up a fake charging station that looks like a legitimate one. When users connect their device to the fake station, the attackers can steal sensitive data or install malware onto the device.

By understanding the different types of juice jacking attacks, users and organizations can take steps to protect themselves and prevent data theft and malware infections.

III. Attributes of Juice Jacking Attacks/Malware

• The user will be unaware of the attack as it trespasses the security system.

• The hacker does not require installing any additional remote-control software.

Multi-platform: This cyber-attack can be done in IPhone or android devices.

IV. Working of Juice Jacking attack:

Juice Jacking works via pairing, although the USB cable can transmit both power and data. A USB cable contains four pathways consisting of two power and two twisted signal conductors. In a typical USB connection, there are five pins available, one of which is responsible for charging the receiving end, while two others are utilized for data transfer by default[10][11].

Juice jacking occurs when a USB port is used to transfer data and power, providing a pathway for an attacker to access user data. The attacker can exploit the twisted-pair D+ and D- conductors to transfer data and the VBus and Gnd connectors to supply power which is shown in Figure 1. The device providing power, typically a charger, is the only one that can detect the network, leaving the appliance owner unaware of the threat. In some cases, victims unknowingly download malware disguised as harmless media files, putting their data at risk which is done by the Juice Jacking Filming charger which is shown in Figure 2 and 3 respectively [12]. Recently, a security researcher named Mike Grover developed a malicious USB-lightning cable that resembles a regular cable but contains a hidden Wi-Fi chip. This cable can trigger a de-authentication process and hack into the victim's device.

Table 1 provides the information about the USB color cables with their description.

Table 1. USB Colour Cables with their Descriptions.

Pins	Name	Cable Color	Description
1.	VBUS	Red	+5v
2.	D–	Blue	Input–
3.	D+	Green	Input+
4.	ID	N/A	Host connected to the signal
5.	GND	Yellow	Ground or not connected.

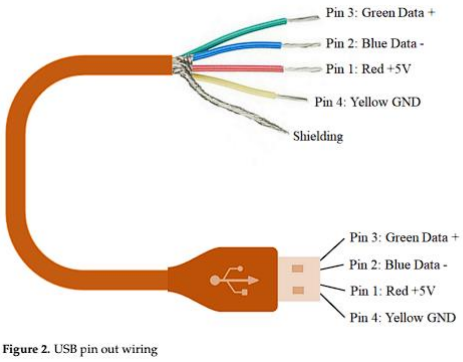

Figure 2. USB pin out wiring

Fig 1: USB pin out wiring

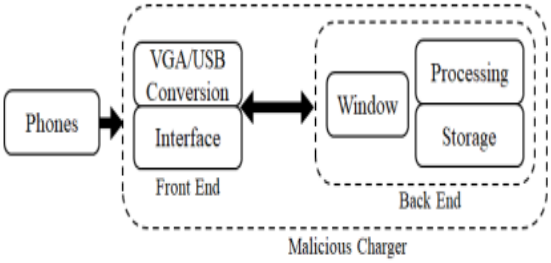

Fig 2: Basic Setup of Malicious Charger

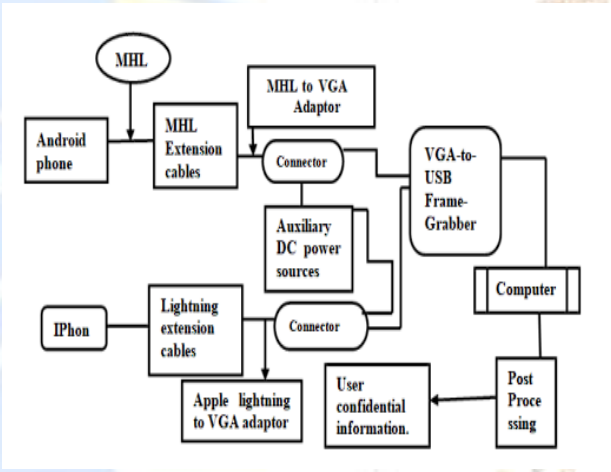

Fig 3: Setup of infected charger using VGA2USB.

V. Analysis made based on Performance:

The unlock pattern in Android's OS and iPhone's iOS has been identified as a potential means of capturing user account and password inputs, which can be recorded using the source code illustrated in Algorithm 1. To address this issue, the proposed system generates alerts for users whenever new devices are connected to the system [1].

Algorithm 1: Pseudocode for recording the data patterns.

```
Data: Device
Result: Obtained data patterns
initialization;
#! /bin/bash ;
while the device is connected with charger do
    mkdir –p output ;
    mkdir –p images ;
    now =(date +% s) #filename ;
    /dev./video0 output/ now.mkv #record for 15 sec ;
    mkdir –p images/now #make new directory for this videos frames ;
    sleep ;
end
```

Table 2 provides the information about the number and percentage of ten malwares and their behaviours for smart devices that are depicted in Figure 4 [1].

Table 2. Status of number and percentage of malware.

Number of Malware	Behaviour/Type of Malware	Percentage (%) of Malware
1	Viruses, Worms, Spyware and other malicious code	66
2	Spam	61
3	Phishing attacks	36
4	Network hacking	24
5	Thefts of mobile devices	21
6	DoS, DDoS attacks	19
7	Thefts of larger hardware	17
8	Corporate espionage	13
9	Targeted attacks	9
10	None	7

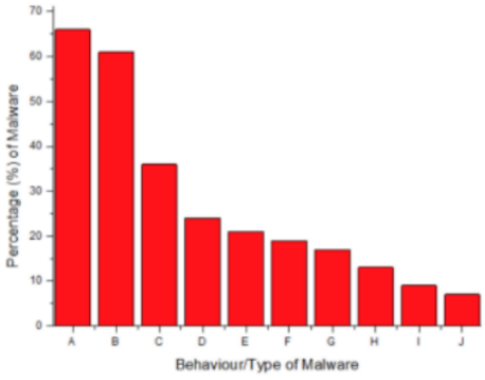

Fig 4: Malwares and its behaviour in smartphones

A group of 1250 participants conducted the overall analysis. Initially, we gathered different features and designated the Malware type as the target class. To create the juice jacking classification model, we employed various ML and deep learning models. 70% of the dataset is allotted for training the models and the 10% and 20% were used for validation and testing of models respectively.

VI. Comparative Analysis:

This work utilized several ML and deep learning models in order to build a classification model, including models like J48, SVM, k-NN classifier, ANN, Random Forest, ANFIS, and CNN [1]. At first, implemented features were converted to numeric features using one-hot encoded vectors. Then, the Z-score method was implemented to normalize the data. For the CNN-based deep learning model, a connected layer of size 35 was used, followed by batch normalization, ReLU activation, another fully connected layer, and softmax and classification layers. The RMSprop algorithm was used to optimize the cost function with a mini-batch size of 32. The proposed deep learning model achieved an accuracy of 76.7% with an error rate of 23.3%, which could be useful in identifying and preventing potential security threats in charging stations.

Table 3 compares the performance of the proposed model to other machine learning models for all ten malwares, and demonstrates that the proposed deep learning model outperformed the competition by an average improvement of 2.1789%, 1.9578%, 2.3458%, 2.0696%, and 2.1926%, respectively [1].

Table 3. Comparative analysis of the proposed system.

Model	Accuracy	F-Score	Precision	Recall	Hit Rate
J48	68.2481	77.9055	70.0374	76.4227	69.7421
SVM	72.4264	79.1583	73.7827	78.8732	72.6881
KNN	70.2702	78.7406	71.9723	77.3199	71.0369
ANN	72.4264	78.1583	73.7827	78.8732	72.6881
RF	72.2433	79.0957	74.8031	79.0391	72.4252
ANFIS	73.0784	78.5149	70.5454	80.9132	73.0316
Deep learning	**76.0784**	**78.1333**	**70.2898**	**82.7683**	**75.3015**

VII. Security Improvements:

There are several methods to improve the security system of a device. Some of them are mentioned below.

Use a Data Blocker: A data blocker is a small device that plugs into the USB port of a charging station and prevents the transfer of data while still allowing your device to charge. This is an inexpensive way to protect your personal information from hackers.

Confidentiality of USB Traffic: Upon further examination, it is evident that a substantial amount of data is being transmitted via the USB network channel. By executing a "sniffing" attack, the addresses of the packets can be accessed, thereby compromising the security. A conceptual attack can be done on a test system by using the USB bus to simulate a keyboard input, which can expose the user's keystrokes. Since data is transmitted in plain text, it is crucial to employ encryption to intercept it. In order to enhance the security of the USB line, it is necessary to establish a private channel between the user display screen and the USB device. Various methods are evaluated to determine the most effective approach for safeguarding communication [13].

The integrity of USB Traffic: Ensuring the integrity of data is a crucial issue in USB technology that needs to be addressed. There is a risk of devices mistakenly identifying themselves as separate devices, which can be exploited by attackers using spoofing techniques [14]. For instance, a maliciously programmed printer can pose as a keyboard on a computer, sending unauthorized commands that can widen the scope of potential attacks. This type of attack can go undetected until the device is used, and any USB device can be used in such an attack [15].

Authentication of USB: To prevent tampering and exploitation of the bus, a verification and certification process is necessary. To confirm that a device is genuine, a key signature is required. The use of digital signatures can also protect USB data. Cryptography methods for data protection can be implemented, ensuring that every device has a unique signature that the host can authenticate and validate.

Security features of device: Despite the presence of multiple security features, they are often underutilized by the users. For instance, when we connect the device to a USB port, it prompts us to authorize data transfer, and we can decline to stop the transmission of our data. Here is a simple pseudocode for enabling it.

Pseudocode :

BEGIN

IDENTIFY assets TO BE PROTECTED

ASSESS potential THREATS and VULNERABILITIES to those assets

DETERMINE security CONTROLS needed TO ADDRESS those threats and vulnerabilities

IMPLEMENT security CONTROLS including access control, encryption, authentication, and authorization mechanisms

MONITOR and EVALUATE the effectiveness of the security controls regularly

IF new THREATS or VULNERABILITIES arise THEN

UPDATE and MODIFY the security controls as necessary

END IF

END

VII. Conclusion:

Juice Jacking is a significant cyber threat that requires caution to avoid the potentially dangerous consequences. While it is not currently widespread, it remains a real and present danger to mobile device users. It is recommended that users refrain from using public charging stations, but in the event of an emergency, precautions should be taken to minimize the risk. Overall, everyone should be aware of the potential dangers and to take appropriate measures to prevent Juice Jacking [16].

References:

1. Debabrata Singh, Anil Kumar Biswal, Debabrata Samanta, Dilbag Singh, Heung-No Lee. "Juice Jacking: Security Issues and Improvements in USB Technology" , Sustainability, 2022
2. Waters, D.W. USB Port Controller with Automatic Transmit Retries and Receive Acknowledgements. U.S. Patent 9824045B2, 21 November 2017.
3. Chu, W. Application of data encryption technology in computer network security. J. Phys. 2019, Tran, M.Q.; Elsisi, M.; Mahmoud, K.; Liu, M.K.; Lehtonen, M.; Darwish, M.M. Experimental setup for online fault diagnosis of induction machines via promising IoT and machine learning: Towards industry 4.0 empowerment. IEEE Access 2021.
4. Kuamr Nanda, P.; Prasad Das, S.; Ranjan Panda, S. and Singh, D. Impact of Structural Aspect, Metal Gate and Channel Material on UTB-SOI-MOSFET. Int. J. Innov. Technol. Explor. Eng. 2019.
5. Jeong, H.; Choi, Y.; Jeon, W.; Yang, F.; Lee, Y.; Kim, S.; Won, D. Vulnerability analysis of secure USB flash drives. In Proceedings of the 2007 IEEE International Workshop on Memory Technology, Design and Testing, Taipei, Taiwan, 3–5 December 2007.
6. Tran, M.Q.; Liu, M.K.; Elsisi, M. Effective multi-sensor data fusion for chatter detection in milling process. ISA Trans. 2021.
7. Kaur, M.; Singh, D.; Kumar, V.; Gupta, B.; Abd El-Latif, A.A. Secure and Energy efficient based E-health Care Framework for Green Internet of Things. IEEE Trans. Green Commun. Netw. 2021.
8. Sanjaa, B.; Chuluun, E. Malware Detection Using Linear SVM, 2013.
9. Sanwal, S.; Singh, K. Juice Jacking—A type of Cyber Attack. Cybernomics 2020.
10. Mishra, N.; Swagatika, S.; Singh, D. An Intelligent Framework for Analysing Terrorism Actions Using Cloud. In New Paradigm in Decision Science and Management; Advances in Intelligent Systems and Computing; Patnaik, S., Ip, A.W.H., Tavana, M., Jain, V.,Eds.; Springer: Singapore, 2020.
11. Singh, D.; Pati, B.; Panigrahi, C.R.; Swagatika, S. Security Issues in IoT and their Countermeasures in Smart City Applications. In Advanced Computing and Intelligent Engineering; Advances in Intelligent Systems and Computing; Pati, B., Panigrahi, C.R., Buyya, R., Li, K.C., Eds.; Springer: Singapore, 2020.
12. Kaur, J.; Singh, D.; Kaur, M. A novel framework for drug synergy prediction using differential evolution based multinomial random forest. Int. J. Adv. Comput. Sci. Appl. 2019.
13. Luqman, M.; Faridi, A.R. An Overview of Security Issues in Fog Computing. In Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 13–15 March 2019.

14. Khorsand, Z.; Hamzeh, A. A novel compression-based approach for malware detection using PE header. In Proceedings of the 5th Conference on Information and Knowledge Technology, Shiraz, Iran, 28–30 May 2013.

15. Kuamr Nanda, P.; Prasad Das, S.; Ranjan Panda, S. and Singh, D. Impact of Structural Aspect, Metal Gate and Channel Material on UTB-SOI-MOSFET. Int. J. Innov. Technol. Explor. Eng. 2019.

16. The Cyber Crime of Juice Jacking in Developing Economies: Susceptibilities, Consequences and Control Measures by John Adinya Odey, Bamidele Ola and Iwinosa Agbonlahor.