IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Juice Filming Attack

Puneeth S P[1], Varshitha H[2], Yogashree P M[3]

Assistant Professor, Department of Information Science and Engineering, BIET, Davanagere, India[1]

B.E Student, Department of Information Science and Engineering, BIET, Davanagere, India[2,3]

Abstract: Smartphones have become a part of our daily lives. Thus, they have become a big target for attacks such as malware. While smartphone malware is very popular in their search community, charging attack are often ignored by the literature. As public charging stations are common, the charging attacks will become a big concern and be used to compromise user's privacy. Vulnerability of smartphone charging and introduce juice filming attacks that can steal sensitive information by recording screen activities during charging. The display of smartphones can be leaked through a standard micro USB connector using the Mobile High-Definition Link (MHL) standard or the iPhones' lightning connector, making our attack feasible in both Android OS and iOS. Furthermore, the implementation of prototype called Juice Caster, which can automate the whole adversary procedure including video-capturing user's inputs, dividing videos into images extracting texts from images with OCR (Optical Character Recognition) technology.

Keywords: Mobile security and vulnerabilities, Android and iOS security, Video recording, charging attacks.

I. INTRODUCTION

Smartphones running the Android Operating System (OS) from Google and the iPhones by Apple are widely adopted by millions of people to communicate with others, surf the Internet and purchase online. According to the records from the International Data Corporation (IDC), the shipments of smartphones have passed 1.3 billion in 2014, where Android OS and iOS account for a total of 95% of the mobile market in the second quarter of 2014. This shows that more and more users are likely to store their personal information and data on the phones.

In this case, smartphones have become an attractive target for hackers and malware. A lot of malware has been developed to steal users' private information such as passwords. For example, they explored a vulnerability of 3G smartphones and proposed a video-based spyware, called Stealthy Video Capturer (SVC). They later implemented this spyware and conducted experiments on real world 3G smartphones.

In this case, we describe a vulnerability of smartphone charging and introduce juice filming attacks that can steal sensitive information by recording screen activities during charging. We show that the display of smartphones can be leaked through a standard micro-USB connector using the Mobile High Definition Link (MHL) standard or the iPhones' lightning connector, making our attack feasible in both Android OS and iOS. Furthermore, we implement a prototype called Juice Caster, which can automate the whole adversary procedure including video-capturing users' inputs, dividing videos into images and extracting texts from images with OCR (Optical Character Recognition) technology. In the evaluation, experimental results from various studies demonstrate that our attack is effective in practice. Our efforts aim to stimulate more awareness in this area.

Software-based threats (e.g., malware) often require some permissions to install software on phones. In addition, they are only available on a specific platform – either Android OS or iOS. In contrast, hardware- based threats such as charging attacks are often ignored. In this work, we aim to automate the process of video analysis and implement a prototype of JuiceCaster, which is able to launch our attack automatically, including video-capturing users' inputs, dividing videos into images and extracting texts from images using OCR.

II. LITERATURE REVIEWS

In 2016, Weizhi Meng proposed a work on juice filming attacks in which he described how the attack works by the usage of the protocol called juice caster and OCR technology. This experimental result demonstrate that our attack is effective in practice. The prototype of Juice Caster, which can automate the whole adversary procedure including automatically video-capturing user's inputs, dividing videos into images & extracting texts from images using OCR technology.

In 2015, Weizhi Meng, Wang Hao Lee, S. R. Murali and S. P. T. Krishnan proposed a novel charging attack, called juice filming attack, which can automatically record user inputs when they are interacting with their phones during the charging process. This attack is very effective in real scenarios as it does not need to install any apps and ask for any permissions, which also distinguish our work from others. They further conduct several studies regarding user's behaviours during

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

charging and user awareness on charging attack. It is found that user's lack of awareness on this attack and our attack can record all user's inputs. Through manually analysing the recorded videos, and can extract users sensitive information such as email accounts and social networking accounts, even the relevant passwords. We later discuss some implementation challenges and present several strategies to defend against this attack.

In 2017, Wang Hao Lee, Zhe Liu, Chunhua Su, Yan Li made a survey and the collaborating organizations for assisting the real deployment and evaluation. An International Conference on Information Security and Cryptography based on the Impact of Juice Filming attack in practical environment.

In 2018**,** Lijun Jiang, Yu Wang, Jin Li, Jun Zhang, Yang Xiang worked on JFC Guard Detecting juice filming charging attack via processor usage analysis on smartphones. Motivated by the potential damage of JFC attack in this work they investigate the impact of JFC attack on processor usage including both CPU and GPU usage. If is founded that JFC attack would cause a noticeable usage increase when connecting the phone to the JFC charger. JFC Guard is a mechanism to detect JFC attack based on processor usage analysis for smartphone users.

III. PRPOSED SYSTEM

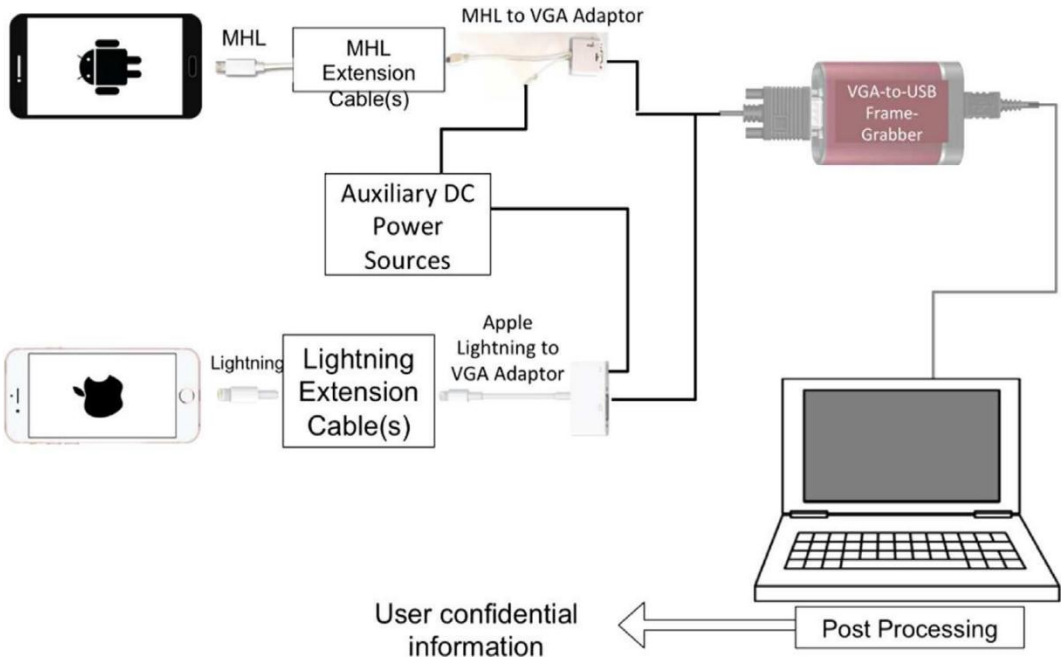

Fig. 1 Architecture of JFC

It is possible to plug Android or iPhones to a projector, where the projector can mirror the phone's display. For Android phones this is usually done through the micro-USB port. The micro-USB (available on most Android devices as of time of writing) can sometimes involve connectors with MHL (Mobile High-definition Link) connectivity. Therefore, rather than charging the victim's device with a standard micro-USB-B port, it is charged by an 11pin micro-USB supporting MHL output (an 11-pin micro-USB is visually very similar to the standard 5-pin connector). On the other end of the USB cable, video signals have to be decoded into a digital format. In the Audio/Visual industry, there are means to record screen activities to a video as demonstrated by screen casts during lectures or demonstrations done on a computer. The device that converts Analog video signals from VGA to digital format in a compact package. This VGA-to-USB frame grabber is connected to a recording device forming a malicious charger, and this device can automatically record users' inputs and screen information when the phone is connecting to the charger.

For iPhones, the lightning-to-VGA connector along with a lightning extension is used. The high-level architecture of the juice filming attacks is depicted in figure. One major issue of our previous work is that the video processing is conducted manually, which would become inefficient when the number of collected videos is significantly increased. Variations of implementation: This kind of attacks can be implemented in two main forms: Implementation as a charging station: A PC is used as the backend for capturing and processing videos. Due to the size, a public charging station is more viable. This is the current form of the attack that is used in the experiment's implementation as a portable power bank: By deploying the frame-grabbing hardware and its driver on an IoT device with wireless internet.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

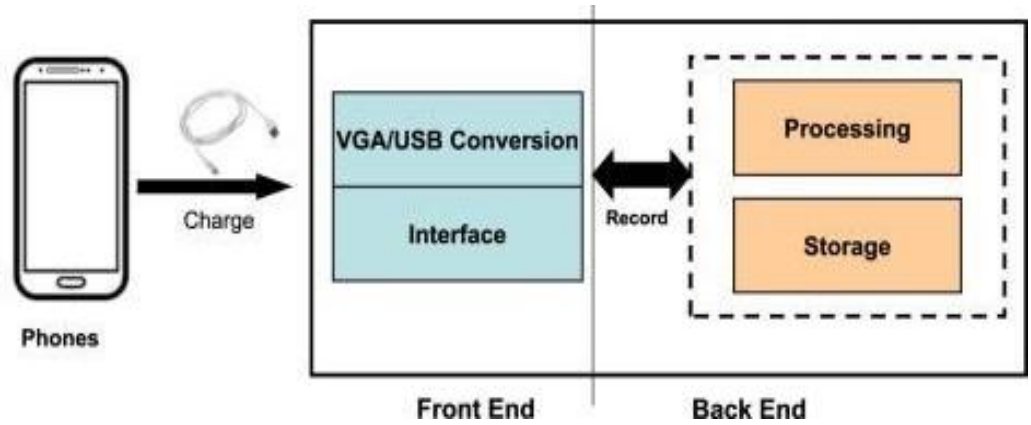

Fig. 2 Device connection detection

IV. IMPLEMENTATION

The prototype called Juice Caster, which comprises a Linux system and VGA2USB converter with the Video4Linux API. In the prototype, the OCR technology to automate the process of video analysis. Thus, there are two phases of Juice Caster: device checking and OCR of collected videos. Juice Filming Attacks which can steal private information by screen-casting the display of victims as they use phone while charging in public ports. As shown in Fig 2.1, the key to this capability to record videos of screen activities is to find a VGA/USB interface. Hardware interface called VGA2USB which allows to display phone screens through USB and High-Definition Multimedia Interface (HDMI). Based on implementation, the prototype called Juice Caster is automated. Thus, there are two phases of Juice Caster: device checking and OCR technology. There are two phases of Juice Caster: device checking and OCR technology.
Phase 1: Device Checking

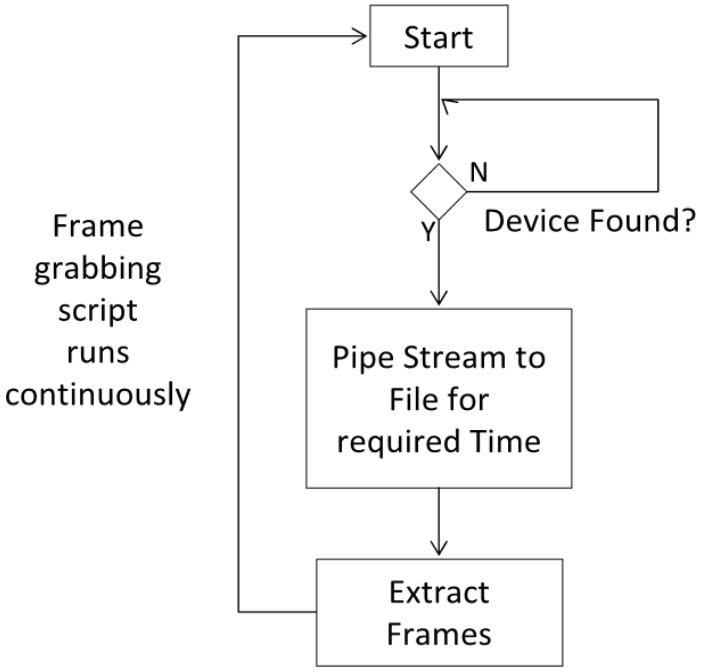

Fig. 3 Workflow of checking for device

Phase 1 - Device Checking: This phase allows Juice Caster to decide when to start the recording process. The Epiphany frame grabber enables a VGA device to send input through the USB of a computer. On Linux, Epiphany devices expose the Video4Linux (V4L) API, so that whenever a device is connected to the Linux machine, the V4L API can provide a real time stream of the display of the device. Then configure to read the V4L stream and write it into a file. A script will periodically check for the presence of a new V4L capable USB connected device. If such a device is found, the stream is piped into a file. After 15 seconds of device detection, the script automatically pauses to evaluate whether the device is still connected. If connected, it continues streaming the screen contents into a file. Otherwise, it goes back into waiting

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

mode – periodically polling for the presence of new V4L devices. From this 15-second video clip, frames are extracted and stored into a new directory.

Phase2 - Optical Character Recognition (OCR): This phase involves the OCR component, which can help automatically extract texts from the collected videos. Since OCR may take a while, it is not done synchronously with the above phase. While the script in Phase 1 is running, the OCR code can be launched simultaneously to process the videos that have been generated, and check for new frames.

More specifically, we build our OCR engine based on the project, which is able to extract text from the images. However from practical usage, it is found that direct processing of the image did not yield accurate results. The Android homescreen wallpaper, for example, can show such a wide variety of colors that the text is simply not recognizable by the OCR engine.

To mitigate this issue, there is an approach of converting the images to grayscale before running it through the OCR engine, which yield significantly better OCR output. For converting the images to grayscale, we use the imagemagick command line tools. The final output is stored in text files and the workflow of this phase is described and the code of automatic OCR can be seen.

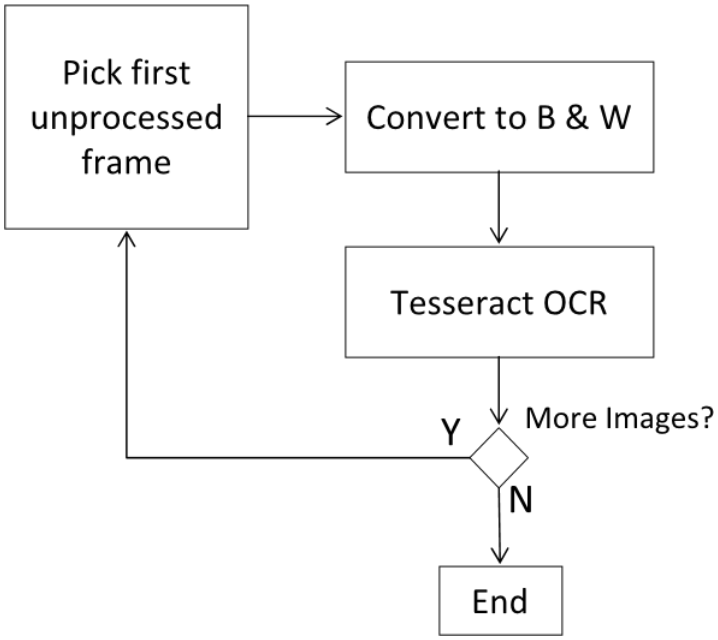

Fig. 4 Workflow of OCR Technology

V. CONCLUSION

Juice filming attack which can automatically record user inputs when they are interacting with their phones during the charging process. This attack is very effective in real scenarios as it does not need to install any apps and ask for any permission which also distinguishes our work from others. The further conduction oft several studies regarding user's behaviour during charging and user awareness on charging attack. It is found that user's lack of awareness on this attack and our attack can record all user's inputs. Through manually analysing the recorded videos, we can extract user's sensitive information such as email accounts and social networking accounts, even the relevant passwords. We later discuss some implementation challenges and present several strategies to defend against this attack.

REFERENCES

[1]. Weizhi Meng, Wang Hao Lee, S. R. Murali and S. P. T. Krishnan "Charging me and I know your secrets!: Towards Juice Filming Attacks on Smartphones"a conference paper and a journal researchGate paper .Aug 2015.
[2]. Weizhi Meng "Juice Caster:Towards Automatic Juice Filming Attacks on Smartphone. An article Jour of network & comp application. Apr 2016.
[3]. Wang Hao Lee, Zhe Liu, Chunhua Su, Yan Li "Evaluating the Impact of Juice Filming Charging Attack in Practical Environments" in 2017.
[4]. Lijun Jiang, Yu Wang, Jin Li, Jun Zhang, Yang Xiang "JFC Guard: Detecting juice filming charging attack via processor usage analysis on smartphone" in 2018.