Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016
A. Mathur and A. Roychoudhury (Eds.)

doi:10.3233/978-1-61499-617-0-99

A Framework for Large-Scale Collection of Information from Smartphone Users based on Juice Filming Attacks

Weizhi MENG [a,1], Wang Hao LEE [a] and S. P. T. KRISHNAN [a]
[a] *Infocomm Security Department, Institute for Infocom Research, Singapore*

Abstract. Cyber security refers to protecting computers, networks, programs and data from unauthorized access, change or destruction. With the wide adoption of smartphones, a lot of sensitive information can be cleaned from users' interaction with their smartphones and tablets. In our previous effort, we have developed a type of charging attacks called *juice filming attacks*, which can sniff smartphone users' information when they are interacting with their phones during charging. With the increasing number of public charging stations, we notice that this type of charging attacks may become a big threat to compromise users' privacy. In this work, we propose a framework of collecting smartphone information in large-scale based on juice filming attacks. Then, we show that such charging attacks work well not only on Android phones, but also on the newly released iPhones. Our work points out that the proposed framework is feasible to threaten users' privacy in practice.

Keywords. Cyber Security, Smartphone Security, Charging Attacks,

1. Introduction

Cyber security research aims to protect networks, computers, programs and data from attack, damage or unauthorized access. It includes applications security, information security, network security and so on. With the increasing adoption of smartphones, more recent research has focused on mobile security and the data stored in these phones has become a major target for hackers.

As an example, Xu *et al.* [13] investigated video-based vulnerabilities in 3G Smartphones and designed a video-based spyware, called Stealthy Video Capturer (SVC), which allows hackers to automatically activate the built-in camera on 3G Smartphones. They then implemented the spyware and conducted experiments on real world 3G smartphones. The results showed that SVC spyware can capture private video information with unremarkable power consumption, CPU and memory footprint. There are also several surveys about smartphone malware such as [1,2,10].

However, we find that few studies in the literature give attention to charging attacks that could steal information through charging facilities. In our previous research [9], we

[1] Corresponding Author: Infocomm Security Department, Institute for Infocom Research, Singapore; E-mail: mengw@i2r.a-star.edu.sg.

developed a new type of charging attacks called *juice filming attacks* on smartphones, which can automatically video-capture screen information of smartphone users during charging process. Based on the captured video, it is feasible to extract huge amounts of sensitive information such as PIN code, emails accounts and various passwords. Moreover, our attack is scalable on both Android OS and iOS, distinguishing this type of attacks from malware attacks.

Motivation. With the increasing demands, public charging stations are becoming popular and widely available in our daily lives. For example, Singapore Power (SP) promised to provide 200 free mobile charging stations for SG50 [12]. As it said, these stations will be launched progressively in busy locations including hospitals, tertiary institutions, libraries and supermarkets, and will become available for one to two years. More specifically, each station will be equipped with 10 individual slots, which contain multiple charging connectors such as mini and micro USBs which will fit most mobile phones and tablets. These charging facilitates can greatly benefit smartphone users, but also open a hole for hackers. This work aims to emphasize that more attention should be given to charging attacks.

Contributions. In this work, we focus on proposing a proof-of-concept framework to show how to collect a large-scale smartphone users' information based on *juice filming attacks*, aiming to explain the potential impact of such attacks on smartphone users in practice. The contributions of our work can be described as below:

- Firstly, we propose a framework to launch *juice filming attacks* in larger-scale, which can greatly threaten smartphone users' privacy in public places. In particular, we take Singapore MRT stations as an example and illustrate how to widely collect users' information with cloud computing. We point out that our framework is feasible to deploy in practice and would be even more severe when utilized by large agents or organizations.
- To illustrate the attack capability, we further verify *juice filming attacks* on recently released Android and iOS devices. It is found that our attack works well in these newly developed platforms. To mitigate it, we also discuss some countermeasures. Our effort demonstrates that charging attacks may become a major threat for cyber security and attempts to stimulate more attention to this area.

The remaining parts are organized as follows. Section 2 briefly introduce the principles of *juice filming attacks*. We describe our framework and show how to implement it through an example in Section 3. In Section 4, we validate the effect of *juice filming attacks* on newly released mobile operating systems and phones. Then, we discuss some countermeasures in Section 5. Finally, we conclude this work in Section 6.

2. Background of Juice Filming Attacks

In [9], juice filming attack was developed, which can refer users' private information through automatically video-capture smartphone screens when users are interacting with their phones during charging. It does not need to install any additional apps or ask for any permissions. Overall, it can provide six features as below:

- It is easy to implement but quite efficient.
- It is a kind of passive attack, which receives less user awareness.

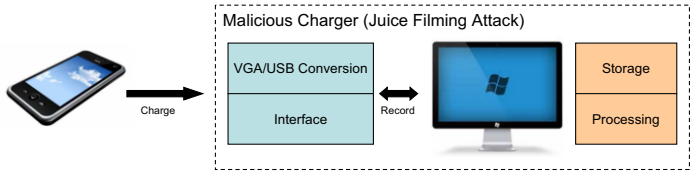

Figure 1. The high-level architecture of juice filming attacks.

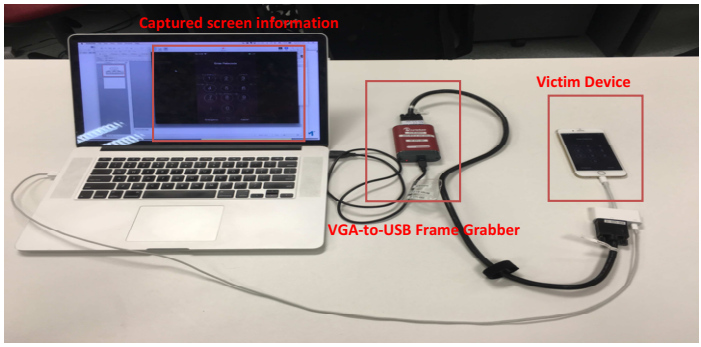

Figure 2. The real setup for juice filming attacks using VGA2USB.

- It does not need to install any additional apps or components on phones.
- It does not need to request any permissions.
- It will not be detected or notified by any current anti-malware software.
- It can be scalable and effective in both Android OS and iOS.

Threat model. The basic assumption is that most smartphone users would not treat public chargers as highly sensitive or dangerous. This assumption is reasonable since it is easy to see lots of smartphone users charge their phones in public places such as airports, subways and so on.

Basic idea. We observe that presently, no permissions will be asked when plugging iPhones or Android phones to a projector, while the projector can display the phone screen. In addition, there are no compelling notifications on the screen when the device is being plugged, or the indicators are very small and last only few seconds. Based on these, *juice filming attacks* can automatically video-record users' inputs during charging by using a VGA/USB interface. This attack reveals that the display can be leaked through a standard micro USB connector through the Mobile High-Definition Link (MHL) standard. For iPhones, the lighting connector is used.

The high-level architecture of such attacks is depicted in Figure 1. When users charge their phones to juice filming charger facilities, their phone screens can be video-captured by the malicious charger. These sensitive videos can be stored and processed in the cloud to conserve compute and network resources.

Real setup. To implement juice filming attack, choosing an appropriate VGA/USB interface is critical as there are many alternatives online. In the previous study [9], we employ a hardware interface called *VGA2USB* from Epiphan system Inc.[2] The *VGA2USB* is

[2] `http://www.epiphan.com/products/vga2usb/`.

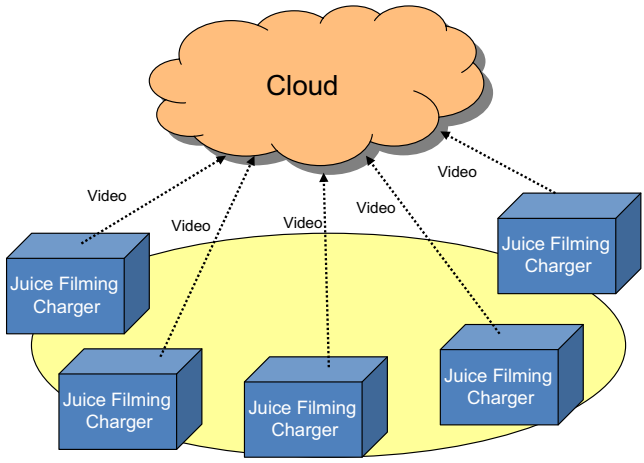

Figure 3. A framework to conduct a large-scale juice filming attack using cloud.

particularly a full-featured VGA/RGB frame grabber, which can send a digitized video signal from VGA to USB.

The real setup is shown in Figure 2. It can be seen that the connected iPhone's screen activity can be shown in the computer end. In this case, it is easy to imagine that all user interaction on the device screen would be captured by our attack. It is worth noting that the computer and other cables can be crampted into a portable charger, making the attack mobile and even more transparent.

3. Our Proposed Framework

In [9], we have shown the feasibility and effectiveness of *juice filming attacks* in a local charging station. In this section, we aim to illustrate that this type of attacks may become a big threat for cyber security through connecting to a cloud environment.

In Figure 3, we present a framework to show how to conduct *juice filming attacks* in large-scale. It is seen that the impact of such attacks can be magnified when deploying malicious chargers to various public locations such as MRT stations, airports and so on. The malicious chargers can upload recorded videos to a cloud environment and extract sensitive information. It is worth noting that this framework is very effective if utilized by a large organizations as large amount of video information can be collected through various charging points. We point out that this attack can be a big threat to users' privacy with the increasing adoption of public charger stations. We summarize some features of this framework as follows.

- *Automatic recording.* Our attack is able to automatically check whether phones are charging to the station and decide when to start video-recording periodically. The script of checking and video-capturing phone screens is shown in Figure 4.
- *Sustainable capturing.* Different from conducting *juice filming attacks* in local stations, our framework make such attack sustainable in capturing videos. For example, it is feasible to delete all videos after uploading them to a cloud, which can save much space.

```
#!/bin/bash
while [ 1 ]
do
        now="$(date +%s)"
        ./ffmpeg -probesize 32 -framerate 25 -analyzeduration 1 -f v4l2 -t 00:00:05 -i
/dev/video0 output/$now.mkv
        sleep 1
done
```

Figure 4. Source code for automatically checking and video-capturing phone screens in period time.

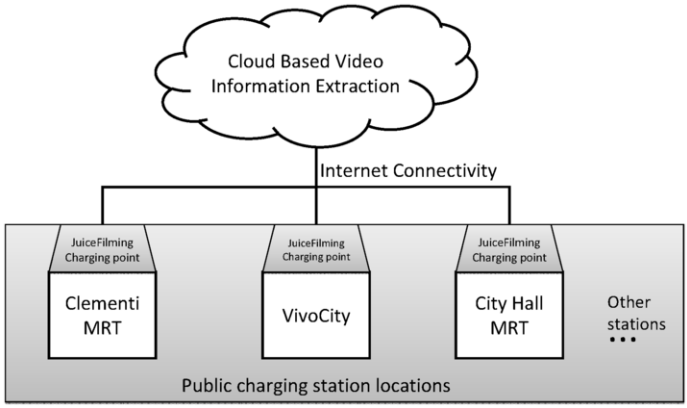

Figure 5. A realization of our framework in Singapore MRT stations.

- *Large impact.* The framework employs a distributed deployment, which can collect information in large-scale. The recorded videos can be processed in one cloud or multiple clouds. Due to very large crowd in public places, our framework can make a large impact on compromising users' privacy.

Based on the above proposed framework, we take Singapore MRT as a hypothetical example to show how to conduct a large-scale *juice filming attack*. As shown in Figure 5, we deploy the juice filming charging stations to various MRT stations such as Clementi, City Hall, etc. All these malicious chargers are connected to a cloud (i.e., uploading recorded videos) through Wi-Fi. In the cloud, all videos can be processed to extract sensitive information including PIN, Android unlock patterns, account names, email content, chat history and so on. According to the surveys conducted in [9], most users (over 95%) have no idea about charging attacks so that they would pay no attention to charging station security. Due to less user awareness, our framework can be feasible in practice and make a large impact.

4. Verification on Newly Released Platforms

In this section, we validate the effect of *juice filming attacks* on various mobile platforms like Samsung Android phones, iPhone 6s and iPad, and recent operating system versions like Android OS 5.0.1 and iOS 9. Several mobile platforms are shown in Figure 6 including iPhone 6s, Samsung Note 4 and iPad.

Figure 6. Several mobile facilities used in our evaluation including iPhone 6s, Samsung Note 4 and iPad.

4.1. iOS Validation

Apple launched the new iPhone 6s and 6s Plus at the time of writing this paper. This motivates us to validate our attack on this newly released platform. The iPhone 6s we obtained is also updated to the latest version of iOS 9. Several screenshots are shown in Figure 7 and present that our attack works well on the iPhone 6s.

- Figure 7 (a) shows the screenshots for Facebook apps. It is easily seen that contact names and relevant information can be captured. After processing the recorded videos, it is feasible to infer private information of users and his or her friends.
- Figure 7 (b) shows that our attack can record the whole process of users' passcode input, so that we can know the actual passcode of that user. Similarly, our attack is able to record various passwords since the video would record all typing actions on the software keyboard.

4.2. Android Validation

For the Android platform, we employ Samsung Note 4 in this evaluation with Android version 5.0.1. Two screenshots are shown in Figure 7.

- Figure 7 (c) shows the screenshots for message apps. It is visible that all messages shown on the screens can be captured on video. After processing these videos, it is feasible to extract private dialogue and sensitive information such as credit card numbers.
- Figure 7 (d) shows that our attack can record Android unlock patterns. Similarly, all input passwords during charging process can be recorded by our attack.

It is found that the newly released Android phones and iPhones did not pay much attention to such type of charging attacks, which still opens a hole for conducting juice filming attacks in large-scale.

5. Countermeasures

As described in [9], the root cause of our attack is that Android OS and iOS allow screen mirroring *without explicit permission at the discretion of the user*. In this case, we point

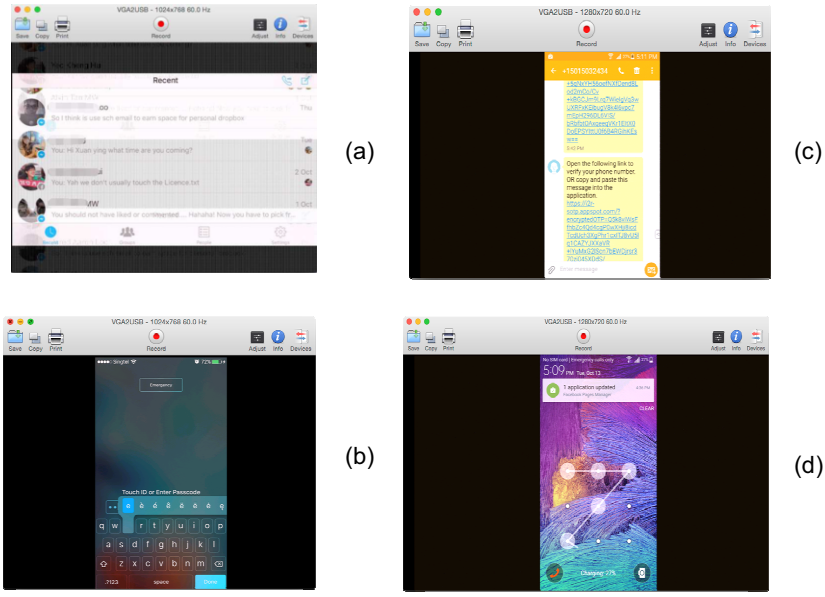

Figure 7. Examples of screenshots on iPhone 6s: (a) Facebook and (b) Passcode, and Samsung Note 4: (c) Message app and (d) Android unlock patterns.

out that more attention should be given to such attacks, which may cause a huge threat for cyber security. Also, it is very critical to protect users' privacy by taking proper countermeasures to defend against such attacks. We discuss several mitigation strategies as follows.

- *Making notifications.* When connecting iPhones to a computer, iOS should prompt a notification asking whether to trust the computer or not. Similarly, to defend against our attack, the smartphone should also warn and make notifications before output of the display. This strategy can increase user awareness and let users consider their actions carefully.
- *Securing the charger interface.* As described in [9], one potential solution to defend against such charging attacks is to use a safe charger such as USB Condom [11]. This USB can prevent accidental data exchange when the device is plugged into another device with a USB cable, by cutting off the data pins in the USB cable and allowing only the power pins to connect through.
- *Employing biometrics.* It is feasible to defend such attacks by combining other techniques like biometrics. For example, behavioral biometrics can be added to the process of inputting PIN code and unlock patterns (i.e., building a fingerprint-based unlocking mechanism), then our attack cannot easily capture these secrets. Several behavioral-based authentication can be referred to [3,5,6,8].
- *Educating users.* Until patches are issued by vendors, such charging attacks are hard to control by filtration mechanisms [7], thus, user education should be a necessary countermeasure to raise users' attention on this threat. It is also a widely used method for securing systems related to human factors such as spam detection [4] & phishing.

6. Conclusion

Charging attacks are often ignored by the literature. In this paper, we proposed a framework to largely collect smartphone users' information by means of juice filming attacks. This type of attacks can extract users' private information through automatically video-capture smartphone screens when users are interacting with their phones during charging. Based on such attacks, we show the feasibility of our framework in practice, which would greatly threaten users' privacy in collaboration with cloud environments, and validate its effectiveness on recently released iPhones and Android phones. Our work aims to stimulate related research in this area and raise user awareness of such attacks.

References

[1] P. Faruki, A. Bharmal, V. Laxmi, and V. Ganmoor: Android Security: A Survey of Issues, Malware Penetration, and Defenses, *IEEE Communications Surveys and Tutorials* 17(2), pp. 998-1022, 2014.

[2] A.P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner: A survey of mobile malware in the wild, *Proceedings of the ACM Workshop on Security and privacy in smartphones and mobile devices (SPSM)*, pp. 3-14, ACM, New York, NY, USA, 2011.

[3] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song: Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication, *IEEE Transactions on Information Forensics and Security* 8(1), 136-148, 2013.

[4] W. Li and W. Meng: An Empirical Study on Email Classification Using Supervised Machine Learning in Real Environments, *Proceddings of the 2015 IEEE International Conference on Communications (ICC)*, IEEE, pp. 7438-7443, 2015.

[5] Y. Meng, D.S. Wong, R. Schlegel, and L.F. Kwok: Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones, *Proceedings of the 8th China International Conference on Information Security and Cryptology (INSCRYPT)*, pp. 331-350, 2012.

[6] Y. Meng, W. Li, and L.F. Kwok: Enhancing Click-Draw based Graphical Passwords Using Multi-Touch on Mobile Phones, *Proceedings of the 28th IFIP TC 11 International Information Security and Privacy Conference (IFIP SEC)*, Springer, pp. 55-68, 2013.

[7] W. Meng, W. Li, and L.F. Kwok: EFM: Enhancing the Performance of Signature-based Network Intrusion Detection Systems Using Enhanced Filter Mechanism, *Computers & Security* 43, pp. 189-204, Elsevier, 2014.

[8] W. Meng, D.S. Wong, S. Furnell, and J. Zhou: Surveying the Development of Biometric User Authentication on Mobile Phones, *IEEE Communications Surveys & Tutorials*, 2015.

[9] W. Meng, W.H. Lee, S.R. Murali, and S.P.T. Krishnan: Charging Me and I Know Your Secrets! Towards Juice Filming Attacks on Smartphones, *Proceedings of the ACM Workshop on Cyber-Physical System Security (CPSS)*, pp. 89-98, ACM, New York, NY, USA, 2015.

[10] S. Peng, S. Yu, and A. Yang: Smartphone malware and its propagation modeling: A survey, *IEEE Communications Surveys and Tutorials* 16(2), pp. 925-941, 2014.

[11] The Original USB Condom. `http://int3.cc/products/usbcondoms.`

[12] Singapore Power to provide 200 free mobile phone charging stations for SG50. (July 27, 2015) `http://www.straitstimes.com/singapore/singapore-power-to-provide-200-free-mobile-phone-charging-stations-for-sg50`

[13] N. Xu, F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng: Stealthy Video Capturer: a new video-based spyware in 3g smartphones, *Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec)*, pp. 69-78, ACM New York, NY, USA, 2009.