Evaluating the Impact of Juice Filming Charging Attack in Practical Environments

Weizhi Meng[1], Wang Hao Lee[2], Zhe Liu[3], Chunhua Su[4] and Yan Li[5]

[1] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark
[2] Infocomm Security Department, Institute for Infocomm Research, Singapore
[3] APSIA, Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg
[4] Division of Computer Science, University of Aizu, Japan
[5] Advanced Digital Sciences Center, Singapore

Abstract. Nowadays, smartphones are widely adopted in people's daily lives. With the increasing capability, phone charging has become a basic requirement and a large number of public charging facilitates are under construction for this purpose. However, public charging stations may open a hole for cyber-criminals to launch various attacks, especially charging attacks, to steal phone user's private information. Juice filming charging (JFC) attack is one such threat, which can refer users' sensitive information from both Android OS and iOS devices, through automatically monitoring and recording phone screen during the whole charging period. Due to the potential damage of JFC attacks, there is a need to investigate its influence in practical scenarios. Motivated by this, in this work, we firstly conduct a large user survey with over 2500 participants about their awareness and attitude towards charging attacks. We then for the first time investigate the impact of JFC attack under three practical scenarios. Our work aims to complement the state-of-the-art and stimulate more research in this area.

Key words: Smartphone Privacy, Android and iOS, Video Recording, Charging Station, Juice Filming Charging Attack, Practical Evaluation

1 Introduction

Mobile devices are widely adopted by millions of people, in which the number of smartphone users is forecast to grow from 1.5 billion in 2014 to around 2.5 billion in 2019. International Data Corporation (IDS) reported that phone shipments grew 5.3% from 344.7 million in the second quarter of 2016, and vendors shipped a total of 362.9 million smartphones worldwide in the third quarter of 2016 [6]. Current smartphones are able to provide various tasks, so that more and more users are likely to store their personal and private data on the phones. Due to the increasing capability, people are often using smartphones in their daily lives (e.g., playing gaming app, video-chatting with friends), which may greatly increase the demand of recharging their mobile devices. To meet this requirement, more and more public charging stations are under construction.

For instance, Singapore Power (SP) promised to deploy up to 200 free mobile charging stations for SG50 [24]. These stations will be launched progressively in various busy locations including hospitals, tertiary institutions, libraries and supermarkets, and will become available in one to two years. In particular, each station will be equipped with 10 individual slots, which contain multiple charging connectors such as mini and micro USBs that can fit most mobile phones and tablets. These charging facilitates can greatly benefit smartphone users; however, they may also expose a big threat on smartphone privacy and security, since we are not sure that these charging facilities are not maliciously controlled by cyber-criminals (e.g., charging station developers and managers, Government agencies). For example, Lau *et al.* [8] in 2013 presented *Mactans*, a malicious charger that can launch malware injection attacks using BeagleBoard after users connect their phones to the charger. Spolaor *et al.* [23] proposed *PowerSnitch*, a malicious application that can refer users' data by analyzing power consumption over a USB charging cable during the charging period. As a result, there is a significant need to pay more attention to the defence of charging threats.

Mactans and *PowerSnitch* can work on either iOS or Android devices, while a scalable charging attack was developed by Meng *et al.*, called juice filming charging (JFC) attack, which can be effective on boh Android and iOS platforms [16]. This attack can steal users' sensitive information through automatically monitoring and recording phone screen (including users' input) during the period of phone charging, as long as people keep charging and interacting with their phones. Moreover, such attack can be launched automatically by integrating OCR technology [16]. As JFC attack does not install any piece on phone's side or require any permission from users, it may have a large impact on users' privacy and increase the difficulty of detection. Previous studies have verified that current anti-virus software are unable to detect JFC attacks [15, 16].

Contributions. In literature, several simulated scenarios had been investigated regarding charging threat, but there is no real evaluation under practical environments. Due to the potential damage of charging attacks, in this work, we focus on JFC attack and conduct an empirical study to investigate its influence in three practical environments for the first time. In particular, we conduct a large survey to study users' attitude towards charging attacks and investigate the influence of JFC attack based on practical setup. The contributions of our work can be summarized as below.

- We conduct a large survey with over 2500 participants to explore users' attitude and awareness towards charging attacks. There are two ways to distribute the questions: online form and paper form. The collected results describe a security concern that most phone users are not aware of charging threat.
- We then introduce how to launch JFC attack with a cloud and investigate its practical impact on users' privacy in three practical locations. To our knowledge, this is the first work that evaluates the influence of JFC attack in real

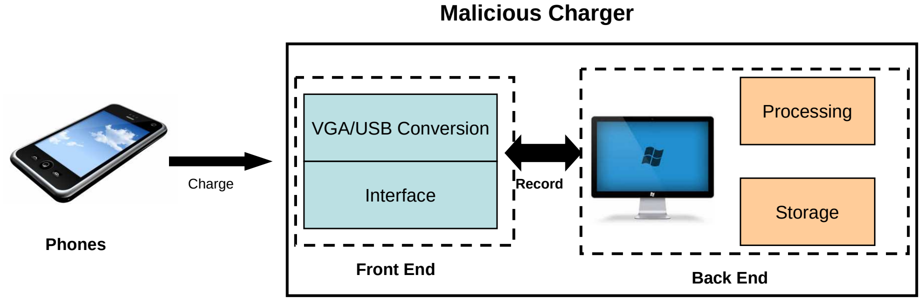


Fig. 1. The high-level architecture of juice filming charging attack.

scenarios. We are particularly interesting in the number and the total size of collected videos, which determine how much information can be extracted.

The remaining parts are organized as follows. Section 2 introduces the background of JFC attack. Section 3 describes our survey and analyzes the obtained results. In Section 4, we describe how to setup JFC attack in real scenarios and investigate its practical influence. We discuss related studies in Section 5 and conclude this work in Section 6.

2 Background

JFC attack is able to steal users' private information through automatically video-capturing phone screens when users are playing their phones (or phone screen awake) during the whole charging period [15]. This attack does not need to install any additional parts or ask for any permissions on phone's and user's side. By integrating with OCR technology, JFC attack can provide seven features: 1) can be easy to implement but quite efficient; 2) with less user awareness; 3) does not need to install any additional apps or components on phones; 4) does not need to ask for any permissions; 5) be hard to be detected by current anti-malware software; 6) can be scalable and effective on both Android OS and iOS devices; and 7) can automatically handle collected videos and extract information.

Threat model There are two basic assumptions: 1) phone charging is a basic and common demand for smartphone users, and 2) most smartphone users would not treat public chargers as highly sensitive or dangerous. It is not hard to observe that many smartphone users charge their phones in public places such as airports, subways, shops and so on. Generally, charging attacks can be divided into either *public* or *private*. In particular, a public charging attack works mainly based on a public charger like charging interfaces provided by airports, while a private charging attack often utilizes a private charger from friends or other familiar persons.

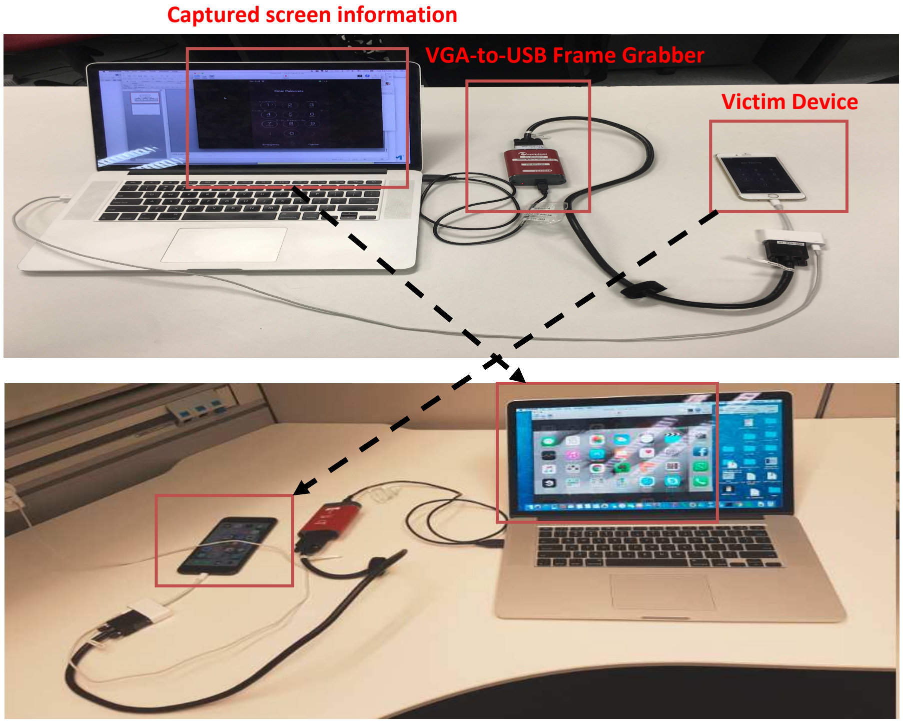


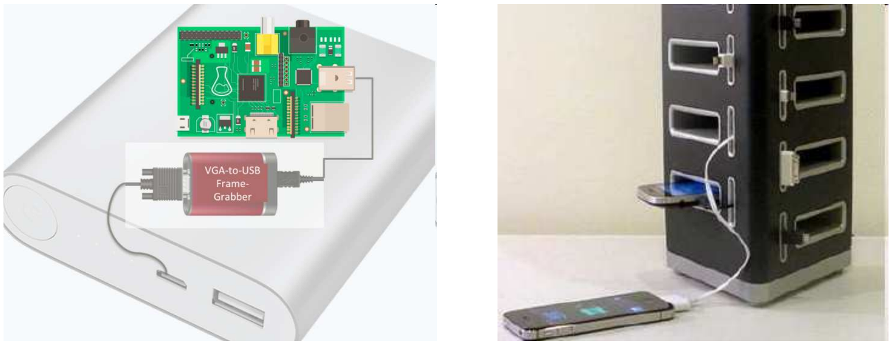
Fig. 2. Real setup for juice filming charging attack using VGA2USB.

Basic idea The design of JFC attack is based on the observation that no permission would be asked when plugging iPhones or Android phones to a projector, but the projector can automatically display the phone screen. In addition, there are no compelling notification on the screen when the device is being plugged, or the indicators are very small and last only few seconds. Taking advantage of these, JFC attack can automatically video-record users' inputs by using a VGA/USB interface. This attack reveals that the phone display can be leaked through a standard micro USB connector that uses the Mobile High-Definition Link (MHL) standard. For iPhones, the lighting connector is used.

The high-level setup of JFC attack is depicted in Figure 1. When users connect their phones to JFC charger facilities, the phone screens can be video-captured into video files in the back-end. These collected sensitive videos can be stored and processed to extract private information.

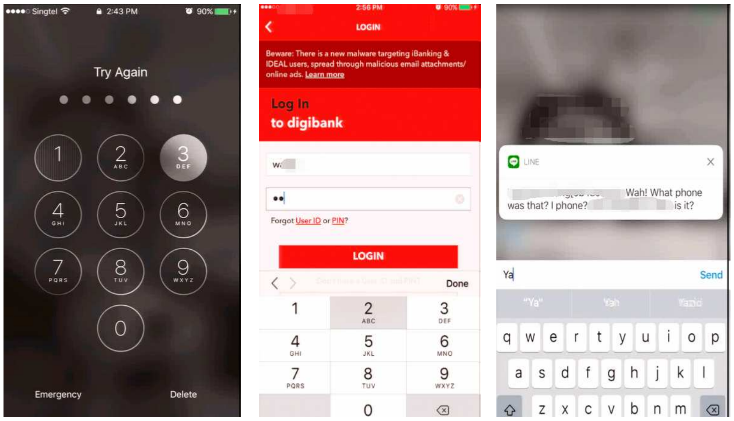
Real setup To implement JFC attack, choosing an appropriate VGA/USB interface is critical as there are many alternatives online. The previous studies like [15, 16] employed a hardware interface called *VGA2USB* from Epiphan, which is particularly a full-featured VGA/RGB frame grabber, and is responsible for sending a digitized video signal from VGA to USB.[1]

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



(a) (b)

Fig. 3. (a) The construction of JFC-based power bank and (b) A charger box.



Beware: There is a new malware targeting iBanking & IDEAL users, spread through malicious email attachments/ online ads. Learn more

Log In
to digibank

w[redacted]

••

[redacted] was that? I phone? [redacted] Wah! What phone is it?

Ya

(a) (b) (c)

Fig. 4. Collected private information by JFC attack. (a) PIN Input, (b) Bank Login, and (c) Line Chat.

The real setup is shown in Figure 2: the connected iPhone screen could be captured in the computer end. It is easy to imagine that all phone screen information would be captured by JFC attack including users' inputs such as typed passwords, PIN code, email address, used application types and so on. It is worth noting that the hardware interface and other cables can be replaced by smaller devices or hidden by a power bank, which only provides an external charging cable as shown in Figure 3: Figure 3 (a) shows how to construct a JFC-based power bank (e.g., [16]) and Figure 3 (b) describes a charger box that can be used to launch JFC attack.[2]

[2] http://www.coolthings.com/life-spot-smartphone-charging-station/

Collected private information. In Figure 4, we present several images of collected phone screen via JFC attack. In particular, Figure 4 (a) shows the captured screen for inputting a 6-digit PIN on an iPhone, Figure 4 (b) presents the captured screen of bank login, and Figure 4 (c) shows the captured screen of Line chat. These examples indicate that various information can be extracted by analyzing the recorded videos, and that JFC attack may become a big threat for smartphone privacy and security.

3 User Awareness

User awareness is a critical factor that affects the impact of a security threat such as malware spread, spam and charging threat. In this section, we conduct a large survey including over 2500 participants, with the purpose of investigating users' awareness and attitude towards malware, charging attacks and public charger usage. The survey results aim to complement existing studies like [15, 16].

Table 1. Information of participants in the study.

Occupation	Male	Female
Students	773	801
Engineers	108	115
Professors/Teachers	52	68
Researchers	101	130
Business People	102	91
Senior People	119	110

Participants. We have two ways to distribute our questions through either online form or paper form. A total of 2570 participants attended our study and gave their feedback including students, engineers, professors, researchers, teachers, business people and senior people. All participants are volunteers and have no security background (i.e., without attending any security related courses before). They are aged from 18 to 65 and the detailed information of participants is summarized in Table 1. It is worth noting that up to 64.2% of them are currently using Android phones and 1783 participants were distributed by an online form.

Survey results. The main survey questions and users' feedback are summarized in Table 2. It is noticeable that 1253 (48.8%) of the participants had installed one kind of anti-virus software on their smartphones. Encouragingly, there are 1082 (42.1%) participants can specify the name of at least one smartphone malware. Similar to the previous study [16], these two questions present that common smartphone users have paid more attention to defend against malware (i.e., nearly half of them had installed a security mechanism such as anti-virus to protect their phones from malicious applications).

Table 2. User feedback in the survey about malware, charging threat and charger usage.

Questions	# of Yes	# of No
Have you installed any anti-virus software on your smartphones?	1253	1317
Can you specify any kind of smartphone malware?	1082	1488
Do you have the need to charge your phone in public places like airport?	1768	802
Are you willing to use a public charging station (e.g., in airport, shops)?	1455	1115
Do you have the potential to interact with your phone during charging like chatting with friends?	1678	892
Do you know any charging attack (i.e., attacks through a USB charging cable)?	582	1988

For the questions regarding smartphone charging, it is found that 1768 (68.8%) of the participants had the need to recharge their phones in public places. With the increase of phone usage, this number seems to continue increasing. Due to the demand of charging, 1455 (56.6%) of the participants adopt the use of a public charging station in several places (e.g., in shops, airports). During the charging period, up to 1678 (65.2%) participants reported that they were likely to interact with the phone. For example, they may check their emails and chat with their friends or family members. Unfortunately, 1988 (77.3%) of them were not aware of charging attacks.

Overall, the survey results demonstrate that users would pay less attention to smartphone charging threat as compared to malicious applications (malware); thus, charging attacks have a large potential to cause more victims than malicious applications due to the lack of user awareness in practice. These observations are in line with the observations in former studies [15, 16].

4 Practical Impact

According to the above survey results, JFC attack has the potential to collect users' private information in large. In this section, different from the former research [15, 16], our motivation is to investigate the impact of JFC attack in practical environments. We have two particular interests:

- The number of videos that could be collected from JFC attacks each day.
- The total size of recorded video that could be extracted for private information each day.

Deployment. To launch JFC attack in practical scenarios, we seek approval and collaborated with three organizations: a company (with over 200 personnel), a university and a business hall. In particular, we deployed five JFC chargers for each environment, where the chargers can keep uploading the recorded videos to a cloud in the back-end, as shown in Figure 5. After uploading the videos

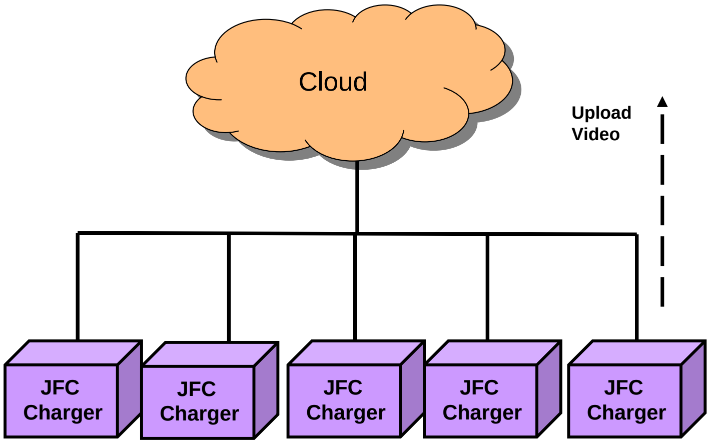


Fig. 5. The high-level deployment for JFC chargers.

Table 3. Extracted information in practical environments.

User Information	**User Information**
Android unlock pattern / PIN for iPhones	Gmail Account and content
Other Email Account and content (e.g., Sina, 163)	Social Networking Account (e.g., Facebook, Twitter, Wechat, QQ)
Bank Account and Bank Message	Visited Website Content
Social Networking Chat History (e.g., Facebook, Twitter, Wechat, QQ)	Installed Mobile Applications
Email Passwords (web-login)	Phone Number List
Smartphone Settings	Personal Photos

successfully, the chargers can delete the corresponding videos locally in order to save space for new videos. The back-end was capable of 250G hardware space, where one minute-video may need 30M space. The video processing with OCR technology can be referred to [16]. The deployed location for each environment is described as below.

- *Company environment.* Five chargers were deployed in one main dining room, where most personnel would spend their time having breakfast, lunch and even dinner.
- *University environment.* Five chargers were deployed at the ground floor of two teaching buildings, so that students can use when they have a rest.
- *Business hall environment.* Five chargers were deployed around the hall, so that visitors can use when queuing up (i.e., waiting for the number).

Data Collection and Results. To protect users' privacy, we seek users' approval and all data will be deleted after processing. At least one IT administrator helped monitor the whole process and make sure all steps are correct.

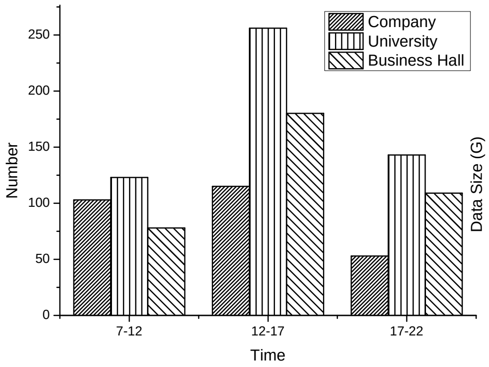


Fig. 6. The average number of collected videos for five days.

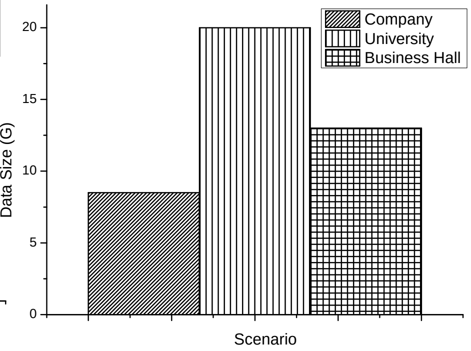


Fig. 7. The average size of collected videos for each day.

We performed JFC attack in each environment for five days (i.e., from Monday to Friday). The average number of recorded videos is shown in Figure 6. The opening hours for both the company and the business hall are from 8am to 8pm, so that we mainly recorded the information from 7am to 10pm by considering the university environment. The figure shows that JFC chargers can collect more than 250, 500 and 350 videos each day for company environment, university environment and business hall environment, respectively. More specifically, it is found that JFC chargers could collect the highest number of videos during the time period of 12-17. This is because most of their phones were out of power due to the usage in the morning, and there is a high possibility of charging their phones during this period.

Intuitively, each video has a different length and size, in which a longer video may provide more private information about a smartphone user. As a result, one of our interests is to explore the total size of collected videos. Figure 7 depicts the average total size of collected videos for each environment. It is noticeable that JFC chargers could collect 8.5G, 20G and 13G data each day for company environment, university environment and business hall environment, respectively. From these collected videos, we can extract a large amount of private information about users, as shown in Table 3, such as Android unlock pattern, PIN for iPhones, Email account and content, social networking chat history, visited website, personal photos and so on. On the whole, our results validate that JFC attack can make a large impact on smartphone users' privacy. There is a need to increase users' awareness towards such attack.

5 Related Work

In literature, physical side channel is believed to be an effective method to infer users' private information and data. Such attacks are often based on oily residues left on the touchscreen. Aviv *et al.* [1] had explored the feasibility of smudge attacks on touch screens. They considered different lighting angles and light sources and the results indicated that the pattern could be partially identifiable in 92% and fully in 68% of the tested lighting and camera settings. Zhang *et al.* [27] proposed a fingerprint attack against tapped passwords via a keypad instead of graphical passwords. Their experiments on various platforms including iPad, iPhone and Android phone demonstrated that the attack can reveal more than 50% of the passwords in most cases. Raguram *et al.* [21] presented that automated reconstruction of text typed on a mobile device's virtual keyboard is possible via compromising reflections such as those of the phone in the user's sunglasses. Their results showed that their approach could reconstruct fluent translations of the recorded data.

Charging attacks are often ignored by phone users. To our knowledge, Lau *et al.* [8] designed *Mactans*, an early malicious charger that used BeagleBoard to conduct malware injection on iOS smartphones. However, a major drawback is that their attack requires users to unlock the phone screen and install developer licenses in advance. Spolaor *et al.* [23] described *PowerSnitch*, a malicious application that can refer personal data on smartphones by analyzing power consumption over a USB charging cable. The scalability is a major limitations for this charging attack. Juice filming charging (JFC) attack [15, 16] is a scalable charging attack, which works on both Android and iOS devices, and can record screen information during the whole charing period, without the need to request any permission or action to unlock phone screen. In this work, we conduct an empirical study to investigate the impact of JFC attack in practical environments. Some other related work can be referred to [17, 18, 19].

6 Conclusion

As compared to mobile malicious applications, charging threats are often ignored by the literature. In this paper, we focus on juice filming charging (JFC) attack, which has the capability of referring users' private data from both Android OS and iOS devices, through automatically monitoring and recording phone screen during the charging period. The rationale is that screen information can be leaked through a standard micro USB connector that employs the Mobile High-Definition Link (MHL) standard.

Due to the potential damage of charging threat, we focus on JFC attack and perform an empirical study for the first time to investigate the impact of JFC attacks in practical environments. In particular, we conduct a user survey with over 2500 participants about their awareness and attitude towards charging attacks, and then investigate the impact of JFC chargers in three practical scenarios like company environment, university environment and business hall. The results validate that JFC attack would have a large impact on smartphone users' privacy. Our work aims to stimulate more research in this area and raise user awareness of such threat.

Acknowledgment

We would like to thank all participants for their efforts in the survey and the collaborated organizations for assisting the real deployment and evaluation.

References

1. A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J.M. Smith, “Smudge attacks on smartphone touch screens,” *Proceedings of the 4th USENIX conference on Offensive technologies (WOOT)*, pp. 1-7, Berkeley, CA, USA: USENIX Association, 2010.
2. D. Dagon, T. Martin, and T. Starner, “Mobile Phones as Computing Devices: The Viruses are Coming!” *IEEE Pervasive Computing* 3(4), pp. 11-15, 2004.
3. A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, “Touch Me Once and I Know Its You!: Implicit Authentication based on Touch Screen Patterns,” *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems (CHI)*, pp. 987-996, ACM, New York, 2012.
4. T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunary, Y. Jiang, and N. Nguyen, “Continuous mobile authentication using touchscreen gestures,” *Proceedings the 2012 IEEE Conference on Technologies for Homeland Security (HST)*, pp. 451-456, IEEE, USA, 2012.
5. 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.
6. IDC, Smartphone Momentum Still Evident with Shipments Expected to Reach 1.2 Billion in 2014 and Growing 23.1% Over 2013. `http://www.idc.com/getdoc.jsp?containerId=prUS24857114.`
7. Juice Jacking Vulnerability for iOS: `https://www.infotransec.com/news/juice-jacking-vulnerability-ios.`
8. B. Lau, Y. Jang, and C. Song, “Mactans: Injecting malware into iOS devices via malicious chargers,” Blackhat USA, 2013.
9. L. Li, X. Zhao, and G. Xue, “Unobservable Re-authentication for Smartphones,” *Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS)*, pp. 1-16, 2013.
10. 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.
11. 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.
12. 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.
13. 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.

14. W. Meng, D.S. Wong, S. Furnell, and J. Zhou, “Surveying the Development of Biometric User Authentication on Mobile Phones,” *IEEE Communications Surveys & Tutorials*, pp. 1-10, 2015.
15. 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 Cyber-Physical System Security Workshop (CPSS)*, in conjunction with AsiaCCS’15, ACM, 2015.
16. W. Meng, W.H. Lee, S.R. Murali, and S.P.T. Krishnan, “JuiceCaster: Towards Automatic Juice Filming Attacks on Smartphones,” *Journal of Network and Computer Applications* 68, pp. 201-212, 2016.
17. Meng, W., Lee, W.H., Krishnan, S.P.T.: A Framework for Large-Scale Collection of Information from Smartphone Users based on Juice Filming Attacks. In: Proceedings of the Singapore Cyber Security R&D Conference (SG-CRC), pp. 99-106 (January 2016)
18. Meng, W., Fei, F., Li, W., Au, M.H.: Harvesting Smartphone Privacy through Enhanced Juice Filming Charging Attacks. In: Proceedings of the 20th Information Security Conference (ISC), 2017.
19. Meng, W., Jiang, L., Wang, Y., Li, J., Zhang, J, Xiang, Y: JFCGuard: Detecting juice filming charging attack via processor usage analysis on smartphones. Computers & Security, In Press, 2018.
20. M. Ossmann and K. Osborn, “Multiplexed Wired Attack Surfaces”. Black Hat USA, 2013. Available at: `https://media.blackhat.com/us-13/US-13-Ossmann-Multiplexed-Wired-Attack-Surfaces-WP.pdf.`
21. R. Raguram, A.M. White, D. Goswami, F. Monrose, and J.-M. Frahm, “iSpy: automatic reconstruction of typed input from compromising reflections,” *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS)*, pp. 527-536, ACM New York, USA, 2011.
22. N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed, “Multitouch Gesture-Based Authentication,” *IEEE Transactions on Information Forensics and Security* 9(4), pp. 568-582, 2014.
23. Spolaor, R., Abudahi, L., Moonsamy, V.,Conti, M., Poovendran, R.: No Free Charge Theorem: A Covert Channel viaUSB Charging Cable on Mobile Devices. In: Proceedings of the 15th International Conference on Applied Cryptography and Network Security (ACNS), pp. 84-102 (2017)
24. Singapore Power to provide 200 free mobile phone charging stations for SG50, 2015. [Online Available:] `http://www.straitstimes.com/singapore/singapore-power-to-provide-200-free-mobile-phone-charging-stations-for-sg50`
25. The Original USB Condom. `http://int3.cc/products/usbcondoms.`
26. 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.
27. Y. Zhang, P. Xia, J. Luo, Z. Ling, B. Liu, and X. Fu, “Fingerprint attack against touch-enabled devices,” *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, pp. 57-68, New York, NY, USA: ACM, 2012.