Your OTP Is Also Not Secure: Security Issues Of Mobile Apps in the E-Commerce

Anand Kr Shukla, Harmanjeet Singh

Abstract: ***Now a days most of the persons doing their banking transactions, bill payments online through mobile app or web. Almost all the financial*** **institutions are providing** ***second layer of authentication*** **by providing one time password while online transactions. But one the other hand in almost every mobile applications have the features to read your contacts, your locations, your messages not only read but they have the features to write the massages, write the contacts in your contacts list. Are these features really helps us? Are they really for our time saving? In this research article we will see the dark side of these features of our mobile applications.**

Keywords : Mobile Apps, Security, Online Transactions.

I. INTRODUCTION

This is an International reputed journal that published research articles globally. All accepted papers should be formatted as per Journal Template. Be sure that Each author profile (min 100 word) along with photo should be included in the final paper/camera ready submission. It is be sure that contents of the paper are fine and satisfactory. Author (s) can make rectification in the final paper but after the final submission to the journal, rectification is not possible. In the formatted paper, volume no/ issue no will be in the right top corner of the paper. In the case of failure, the papers will be declined from the database of journal and publishing house. It is noted that: 1. Each author profile along with photo (min 100 word) has been included in the final paper. 2. Final paper is prepared as per journal the template. 3. Contents of the paper are fine and satisfactory. Author (s) can make rectification in the final paper but after the final submission to the journal, rectification is not possible.

II. MOBILE APPLICATIONS

Mobile Apps (Mobile Application) are basically application software which is used to perform task and services on the mobile devices like smartphones and tablets. If a user wants to perform any task like online shopping, online banking, online chatting, online movies, videos, games, tracking etc. through the mobile device then he/she needs specific mobile app for that. In compare to the application software installed on PCs, mobile apps are usually light weighted (small) *software's;* sometimes they need online support and backup for performing a huge task [6].

III. SECUTITY ISSUES AND RISK

Mobile application security is one of the primary concerns, as the data residing within the app can be at danger if proper securities controls are not applied during the application design. Also, due to the mass usage of apps in today's world, mobile application vulnerabilities have greatly increased [07].Hackers nowadays are targeting mobile applications to gain access to consumer personal information and details to maliciously use it. Hence, developers need to be extra cautious while they build an app for both IOS and Android platforms Application Binary-Level Attacks [08].Unlike web apps, mobile apps are also able to be exposed to binary-level attacks, as this application must be made public. The attacker is capable of downloading the app and compromising the source code. Ways of doing so are: Reverse-engineering, can extracting sensitive information, by Inserting malicious code and redistributing your app, that may be a mobile device-level attacks, malicious apps that can steal data may also there, they can installed your app on Rooted / Jail-broken devices [09], they can also modify app data etc.

IV. VULNERABILITIES OF ANDROID

Most of the peoples are using Android phones in India for their work, and they are getting more dependent upon it. In such scenario mobile security is a matter of concern. In the year 2014-15 the Android vulnerabilities was very high, user were on huge risk, lot of frauds have been reported, Up to June 2017, 40% of the total Android vulnerabilities have been reported. After analysis of vulnerabilities occurrence from 2017 to 2018 on their supporting systems that have been observed that is occurred mostly into the business applications through mobile phones [10]. An analysis said that Google Android (Mostly used Mobile OS) was one of the most vulnerable products along with the e-Business applications. Following figures No. 02 & 03 respectively are showing this.

Revised Manuscript Received on October 05, 2019
***** Correspondence Author
Dr Anand Kumar Shukla*, University Institute of Computer Applications, Chandigarh University, Mohali,
Harmanjeet Singh, University Institute of Computer Applications, Chandigarh University, Mohali,

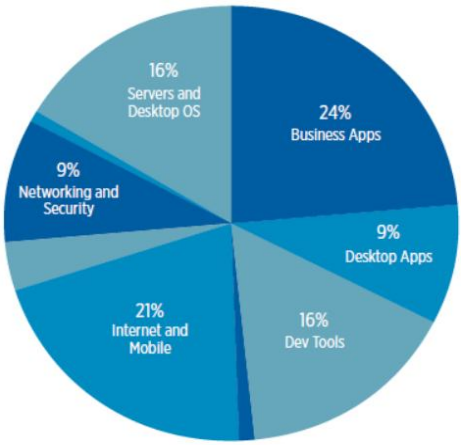

Fig No. 02; 2017 Vulnerabilities by category

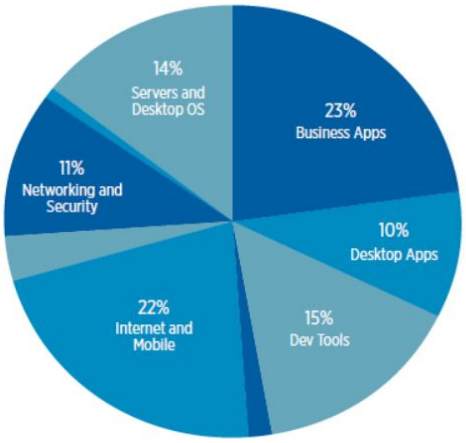

Fig No. 03, 2018 Vulnerabilities by category

V. GOOGLE PHA FOR ANDROID SECURITY.

From preventing the vulnerabilities, Google also lunched some assessment methodologies like Cyber Process Hazards Analysis PHA) that conforms to ISA 62443-3-2 [11]. If we talk about t 2017-18, Google has installed PHA for almost every categ following.

a) Backdoor
b) Trojan
c) Hostile downloader
d) Click froud
e) SMS froud
f) Rooting
g) Privilege escalation
h) Troll froud
i) Phishing
j) Spware as can be seen in the

There Installation rate can be seen in figure No. 04 and 05 respectively.

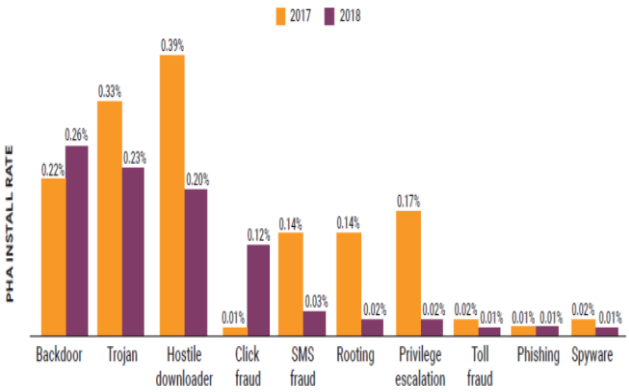

Figure No.04, Percentage of PHA installs by category of Google Play, 2017 Vs 2018 [12]

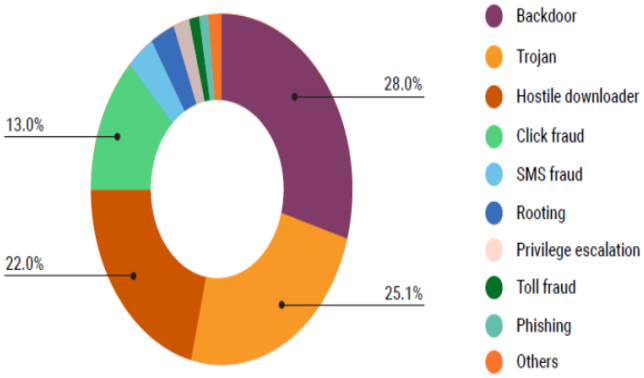

Figure No. 05, Distribution of PHA categories outside of Google Play, 2017 Vs 2018 [11]

While such apps do exist, it is hard to scale up and make money that way. These apps may consist some attractive features like music and gaming, but some features like SDK have observed with some background frauds, without coming into the lime lite of developers. Downloads rate of PHA in 2018-19 has increased by .03% from 2017, because of security levels. Android 9 have 0.19% of PHA in comparison to Android 8 that have 0.18% that can be seen in the following figure No. 06 and 07 respectively.

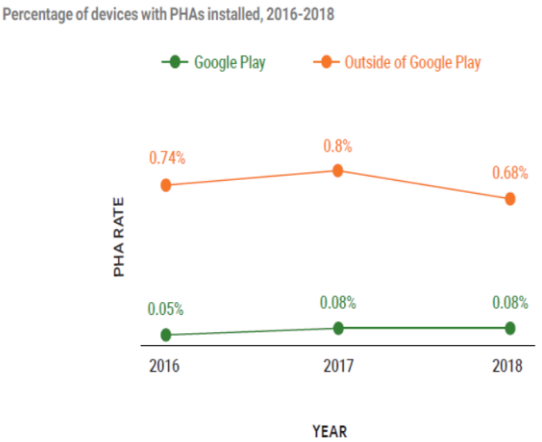

Figure No 06

As result Google Play Protect prevented 1.6 billion PHA installation attempts from outside of Google Play in 2018. In the year 2016 the prevented rate was 41% and due to the PHA installations it has decreased up to 27 % means till 2018 73% devices were much secured, that can also be seen in the figure No. 07 [13].

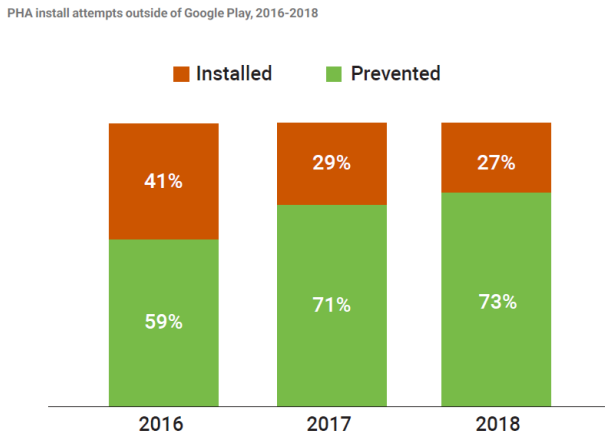

Figure No 07.

This is the reason that the fraud level is decreased from last one or two years but not at satisfying levels, still there are lot of work pending. Apart from that security level will may very much increase if user will aware about the risk related activities, applications, process etc.

VI. PREVENTION FROM FRAUD THROUGH AWARNESS:

There are numbers of fraud applications are still there that can still important and personal information specially related to the bank accounts. Yes off-course this is the matter of worry but that can also preventable by just awareness of the users. First see, areas on which users have to give their concern [14].

App Installations: Users have to be very careful while installations on any mobile applications or app, because now a days mobile applications wants some writes like

a. It can access your locations
b. It may want to access your phone directory and can make changes in it
c. It may also want the permission for making and answering the phone calls
d. It may also want to send and read the SMS

All the permission can be granted by clicking on ALLOW button that appears at the time of app installations as shown in figure No 07 and 08 [14]. Sometimes users may in hurry in apps installation so they used to ignore the permission messages and they just used to click on **ALLOW** button that could be very dangerous some times.

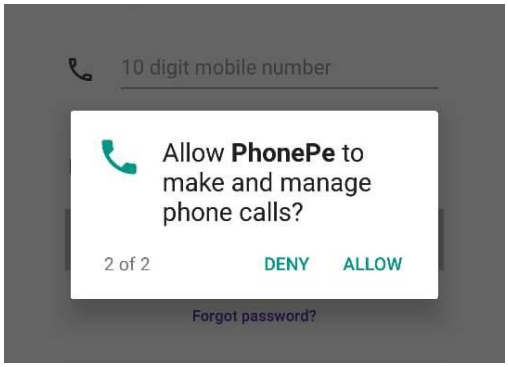

Figure No 08, Apps demanding the permission for making and managing yoour phone calls.

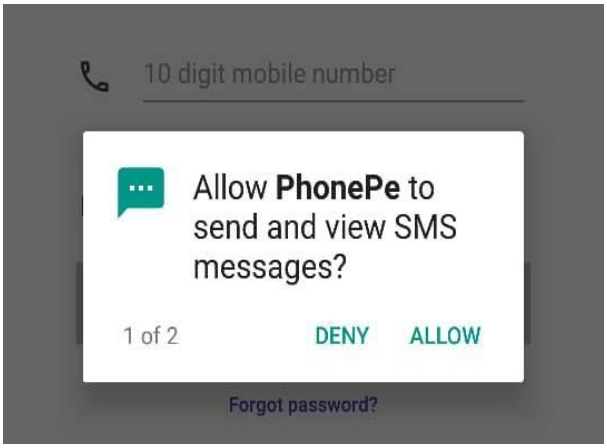

Figure No 09, Apps demanding the permission for writing, reading and sending SMS.

VII. YOUR OTP IS ALSO ON RISK:

Most of the user used to give the above mention permissions while installing these types of mobile apps, if we talk about the message reading and writing permissions; it could steal the information and your privacy by reading your mobile messages and can send these information to somewhere else.

Especially at the time of mobile banking user think that their transactions are safe because of One Time Password (OTP), but they are not aware that their OTP is also not safe, because they already have given the permission to read and write their messages and OTP comes in the message as shown in the above figure No. 09 and 10 respectively, so it can be read by the third party (through mobile app) and can be sent to someone else. That third party can misuse user's secure information, and can also hack their bank accounts and can cause huge damage to you.

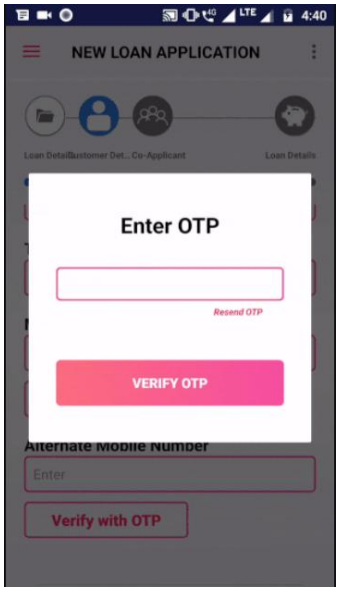

Figure No 010, App is waiting for OTP

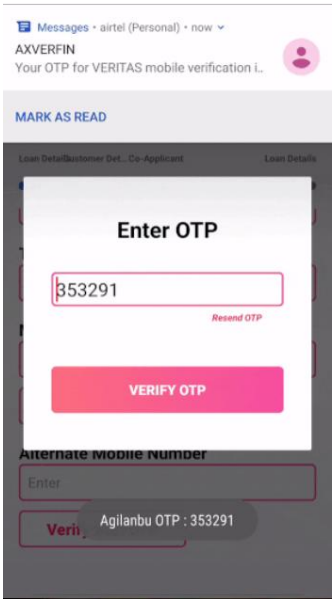

Figure No.11, App reading your OTP, automatically

VIII. CONCLUSION:

As per the study and analysis, author has come to this conclusion there are several vulnerabilities have been found in the Android Applications but Google is trying to recover from it and they are getting success also, and lot of efforts are still needed not only from the developers side but also from the user side. User have to be very careful while installing any type of mobile apps and specially while giving it permissions for accessing and managing your phone directory, phone calls and mobile messages. These efforts will be very helpful and handy to control the online frauds.

REFERENCES

1. L. Polla, M., F. Martinelli, and D. Sgandurra, (2013), "A Survey on Security for Mobile Devices," IEEE Commun. Surveys & Tutorials, Vol.15, issue.1, 446-447, pp.83-92.
2. G. Gorbil, O. H. Abdelrahman, M. Pavloski and E. Gelenbe, "Modeling and analysis of RRCbased signaling storms in 3G networks", IEEE Transactions on Emerging Topics in Computing, Special Issue on Emerging Topics in Cybersecurity, 113 – 127, 4 (1), March 2016.
3. Kaspersky Lab Threat Review for 2016, Retrieved September 5, 2017,http://usa.kaspersky.com/about-us/press-center/pressreleases /2016/Kaspersky_Lab_Threat_Review_for_2016_servers_for_sale_global_botnets_and_a_strong_focus_on_mobile
4. R. Dhayal, & M. Poongodj, (2014), "Detecting Software Vulnerabilities in Android Using Static Analysis", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT). Doi: 10.1109/ICACCCT.2014.7019227
5. W. Melicher, D. Kurilova,Sean M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin, L. Faith Cranor, Michelle L. Mazurek, (2016) , Usability and Security of Text Passwords on Mobile Devices, CHI"16, May 07-12, 2016, San Jose, CA, USA, ACM 978-1-4503-3362-7/16/05, pp.1-13.
6. S. Bojjagani, & V.N. Sastry, (2015) , STAMBA: Security Testing for Android Mobile Banking Apps, Advances in Intelligent Systems and Computing, Springer, Vol. 425, pp.671-683.
7. L. Nosrati, and A. Bidgoli, (2015) Security assessment of mobile-banking, Int. Conf. on Computing and Communication (IEMCON), IEEE. Doi: 10.1109/IEMCON.2015.7344489
8. M. Yesilyurt, & Y. Yalman, (2016), Security Threats on Mobile Devices and their Effects: Estimations for the Future, International Journal of Security and Its Applications, Vol.10, No.2, pp.13-26. Doi: 10.14257/ijsia.2016.10.2.02
9. A. Houmansadr, S. A. Zonouz, and R. Berthier, "A cloud-based intrusion detection and response system for mobile phones," in 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), 2019, pp. 31–32.
10. https://www.welivesecurity.com/2018/08/29/semi-annual-balance-mobile-security/ 2019/
11. C. Miller, "Mobile attacks and defense," IEEE Security and Privacy, vol.9, no. 4, IEEE, 2011, pp. 68-70. Doi: 10.1109/MSP.2011.85
12. Z. Xu and S. Zhu, "Abusing notification services on smartphones for phishing and spamming," in Proceedings of the 6th USENIX conference on Offensive Technologies. USENIX Association, 2018, pp. 1–1.
13. G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in MIPRO, 2011 Proceedings of the 34th International Convention. IEEE, 2016, pp. 1468–1473.
14. M. Roland, J. Langer, and J. Scharinger, "Relay attacks on secure element-enabled mobile devices," in Information Security and Privacy Research. Springer Berlin Heidelberg, 2017, pp. 1–12.

AUTHORS PROFILE

Dr Anand Kr Shukla, working as an Associate Professor, in the University Institute of Computing, **Chandigarh University, Chandigarh**, India. He is having 12+ years of experience. He is also the solo author of five books and more than 30 national and International publications. He is Java & .Net expert and motivational speaker also.

Mr Harmanjeet Singh, working as an Assistant Professor, in the University Institute of Computing **Chandigarh University, Chandigarh**, India. He has published more than 05 National and International publications. He is having 8+ years of experience. He is also the academic coordinator of BCA.