Survey on Smartphone Securities

Pragy Vaishnav¹, Manju Kaushik² and Linesh Raja³

¹Research Scholar, AIIT, Amity University, Rajasthan, India
²Associate Professor, AIIT, Amity University, Rajasthan, India
³Assistant Professor, Department of Computer Application, Manipal University Jaipur, Rajasthan, India

E-mail: pragya.vaishnav23@gmail.com

Abstract. Recently Mobile data security has become a serious subject for everyone, who save their private and confidential data on mobile and perform financial transactions on the daily basis through their mobile. Mobile users are aware that their mobile data is no more secure after stealing their smartphone. 84% person wants advance mechanism for smartphone security so even after login the application, monitoring user can be possible throughout the session. Author conducted a survey on mobile security for 105 participants. This survey responses gave a clear out motive to do research on advance authentication method which is keystroke dynamics on smartphone.

1. Introduction

Since last decades all the mobile applications especially related to online financial transactions have been developed to make easier process for users. There are great innovations in mobile commerce that have facilitated users to do online transactions through their smartphone. There are purchasing, banking, and investing applications where online payments services are available [1]. Therefore, users are always concern with the security of their confidential data. Because of sensitivity of confidential data, users accept it that their personal data can be stolen or hacked.

There are various security threats which can steal smartphone data such as unauthorised mobile apps are the main reason of unintentional data leakage like, mobile apps ask for permission to access mobile’s contacts, photos and other apps and users grant them broad permissions, but do not always check security aspects. Free wifi are often unsecured and people always wants free hotspot and free wifi network which is not secure. Using malware and threats hackers can gain full access of mobile without user knowledge. There are so many threats which can get root access of mobile and use users mobile as it is their mobile and can do anything with bank and financial based applications, read all personal messages and confidential records and can communicate with contacts of mobile. Thus, smartphone has made our life well off and provide comfort life, but it has become dangerous for us and give us insecure life as well. So, it is required to provide security to the smartphone.

Therefore, advance mechanism for continuous authentication using keystroke dynamics and touch dynamics must require. It will secure all the applications of smartphone and all the data.

Keystroke dynamics is a behavioural biometric authentication method it identifies user identity through their typing behaviour on the smartphone. We can check user behaviour throughout the session even
after login the application. This method will improve security of smartphone and give confidence to mobile users to keep their data and perform financial transactions carefree.

2. Related Work

Most of the mobile applications save data in simple text format, and 87% mobile apps use weak cryptographic algorithms [2]. Stealing data from smartphone devices inspire the user to install mobile applications which is malware affected [3]. Without user’s knowledge Malware or malicious software install on user’s smartphone [4]. Malware spread all over to use of the internet or insecure applications. Malware sends SMS to the contacts of mobile or unwanted numbers, and it steal and send sensitive information to imposters and therefore imposters can gain full access of the smartphone device using malware [5]. Mobile Worm [6] behaves as a typical computer worm, it can regenerate itself and spread to everywhere on mobile devices. Without user knowledge mobile Worms can be spread by messages or using different communication sources. Trojan: malicious codes add into executable files and as user run these files then Trojan will be activated. Trojan can get access sensitive information, disable some functions of smartphone devices and can provide full access rights to the imposters to install any kind of malware [7]. Spyware: The important goal of Spyware [8] is to steal user’s personal and sensitive information and to spread that information without user’s knowledge. Ghost Push: This malware can achieve root access in the smartphone devices and then installs malicious applications, convert it to system application and loss root access permissions. Thus, users need to do factory reset to their smartphones to remove these infections. These malwares can achieve user’s personal information [9].

3. Methodology

3.1. Preparation

In preparation to gather data, author first designed 15 sample questions. Questions were based on smartphone, data security on mobile, authentication and password and pin patterns such as are they satisfied with the password and pin authentication method or they think password and can be steal by imposter and they can do anything in their mobile, are they think their smartphone data are not secured because password and pin pattern can be guess or steal by finger oil and shoulder surfing after stealing their smartphone, Are they think another advance authentication must be required apart from password authentication, are they agree that without user knowledge, authentication process should be continue even after login the application so unauthorised access can be stop, Are they think that without user knowledge identifying the user identity even after login the application will secure mobile data and application and are they accept that typing pattern and touch pattern of users are unique? Neither one can copy it nor match it or steal it.

3.2. Data Collection

For this survey author received data from 105 participants. All were from different age groups and different professions. 58 participants were male and 47 were female. 61 participants are in private job, 3 were from business profession, 15 participants were unemployed, and 26 participants comes into another professional category. Data file are downloaded in excel and csv file.

3.3. Feature Extraction

Collected data are categorized in different age group, Age group was from 16 – 70, and in different professions. This survey helped to understand how people are aware of smartphone security, and what they want to improve security on smartphone. Around 85% smartphone users are aware about mobile security and they want advance mechanism for mobile application authentication.

4. Result
1. According to survey 54 participants accepted that their personal and confidential data are not secured on smartphone and 40 participants were not sure about this, but 9 participants did not accept it, presenting through columns of figure 1.

![Figure 1. Respondent Input](image)

2. 82 participants know about authentication that it provides security to their smartphone but 21 participants who were very young or older than 50 they don’t think so.
3. 72 participants keep their private and confidential data on smartphone. Which is a large number.
4. 41 participants were agreed that typing pattern and touch pattern of users are unique. Neither one can copy it nor match it or steal but 33 participants were not sure about it and 30 did not agree with this.
5. 79 participants agreed that password and pin of their smartphone can be steal by imposter and they can do anything in their mobile applications but 27 do not think so.

Figure 2 presenting how mobile data are no more secure because password and pin pattern can be guess or steal by finger oil and shoulder surfing after stealing your smartphone, 88 participants agreed with this strong point.
5. Proposed Work

Author is proposing keystroke dynamics method for continuous authentication on smartphone it will identify the identity of the user through their typing behavior and touch pattern on the smartphone. Keystroke dynamics biometric authentication is more secure rather than other authentication method. This survey gave an opportunity to choose this method because according to survey 84 participants admitted that security options on smartphone should be improve and 87 participants agreed that advance authentication method is required apart from password authentication method on smartphone. Hence 44 participants accepted that typing pattern and touch pattern is more secure than password and pin pattern and another 44 participants think that it may be possible. 65 participants were agreed, and 6 participants strongly agreed that without user knowledge identifying the user identity even after login the application will secure mobile data and application. Therefore, it made to author more confident that research on keystroke dynamics will revolution on smartphone security in mobile world.

Reason behind to choose keystroke dynamics method.

- Pie Figure 3 presenting 38 participants strongly agreed and 50 participants agreed that without user knowledge, authentication process should be continuing even after login the application so unauthorised access can be stop.
- In addition to 42 participants knows about keystroke dynamics and touch dynamics they all are from IT profession.

Hence it gave me motive to choose continuous authentication using keystroke dynamics and touch dynamics.
6. Conclusion

Due to growing technology in mobile world insecurity is also increased. Hence password and pin authentication are no more secure lately. What normal public think about on it, author conducted a survey to get to know what people think about mobile and its security. Author collected 105 responses and knew that people are not satisfied with password and pin authentication they want an advance mechanism which monitor to the user after the login.

7. Future Work

In future we will work on continuous authentication and check typing and touch pattern of the mobile user through different feature sets such as dwell time, flight time, typing speed, finger pressure, finger size. Hence after stealing mobile we will be able to find out the unauthorised access on mobile applications.

8. References

[1] Ruggiero, P. and Foote, J., 2011. Cyber threats to mobile phones. United States Computer Emergency Readiness Team, 6.

[2] Chatzikon Stantinou, A., Ntantogian, C., Karopoulos, G. and Xenakis, C., 2016, May. Evaluation of cryptography usage in android applications. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS) (pp. 83-90).

[3] Nagarjun, P.M.D. and Ahamad, S.S., 2018. Review of Mobile Security Problems and Defensive Methods. International Journal of Applied Engineering Research, 13(12), pp.10256-10259.

[4] Malware. (2017, July 6). In Wikipedia, The Free Encyclopedia. Available at: https://en.wikipedia.org/w/index.php?title=Malware&oldid=789247319.

[5] Mercaldo, F., Visaggio, C.A., Canfora, G. and Cimitile, A., 2016, May. Mobile malware detection in the real world. In 2016 IEEE/ACM 38th International Conference on Software Engineering Companion (ICSE-C) (pp. 744-746). IEEE.

[6] IEEE. Tiwari, S. and Tiwari, V., 2016, September. Bluetooth Worm Propagation in Mobile Networks. In 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE) (pp. 235-239). IEEE.

[7] Otrok, H., Mizouni, R. and Bentahar, J., 2014, November. Mobile phishing attack for Android platform. In 2014 10th International Conference on Innovations in Information Technology (IIT) (pp. 18-23). IEEE.

[8] Spyware. (2017, July 2). In Wikipedia, The Free Encyclopedia. Available at: https://en.wikipedia.org/w/index.php?title=Spyware&oldid=788660061

[9] New “Ghost Push” Variants Sport Guard Code; Malware Creator Published Over 600 Bad Android Apps (2015, September). Trend labs Security Intelligence Blog. Available at: http://blog.trendmicro.com/trendlabs-securityintelligence/new-ghost-push-variants-sport-guardcode-malware-creator-published-over-600-badandroid-apps/