International Journal of
Computer & Software Engineering
Review Article Open Access

Protecting Smartphones Based on Usage Patterns

Weifeng Chen
Department of Mathematics, Computer Science and Information Systems, California University of Pennsylvania, California, PA 15419, USA

Abstract

Due to the rapid developments of cloud technologies, mobile devices, especially smartphones, have become much more powerful, bringing people great convenience. People can do many things on their smartphones: checking email, updating Facebook/Snapchat/Instagram, or shopping via different apps. With all these applications, people tend to access their smartphones frequently and instantly, i.e., they want to use the phone right away. On the other hand, more and more sensitive information is now stored or accessible on smartphones such as Visa Signature or Paypal apps. Smartphones need to be protected more than ever before.

How to protect smartphones while still provide convenience becomes a challenging problem. In this paper, we describe an approach aiming to solve this problem. The approach provides an authentication framework to protect smartphones. This authentication framework requires stronger authentication to accesses that are classified as suspicious, whereas still offers quick access for those authentic.

Publication History:

Received: November 19, 2016
Accepted: April 16, 2017
Published: April 18, 2017

Keywords:

Authentication, Usage patterns

Introduction

Since iPhone came out in 2007, cell phones have become more intelligent. Today's smartphones are so powerful that people can do many things, in addition to traditional voice calls. Different apps have been developed for smartphones. Social network apps such as Facebook, Snapchat and Instagram, make people use the phones more frequently. Financial apps make people life convenience, including Google wallet, PayPal apps, and various bank apps [1]. People could also use their smartphones to access cloud storage. Protecting sensitive information onmobile phones becomes more and more important.Quite a few breach accidents have been reported due to compromise of smartphones. How to protect smartphones becomes more important than ever. *Authentication* is a basic way of protection.

Authentication is a process "to establish the authorship or origin of conclusively or unquestionably, chiefly by the techniques of scholarship" [2]. It is a critical component of information security. For example, passcode (Figure 1) is one basic kind of authentication. Only the person knowing the code can unlock the phone. People go through different authentication processes daily. The combination of a username and a password is a common one. For example, a person needs a username and the correct password to access his/her emails, cloud storage or bank account. If a person wants to withdraw money from an ATM machine, he/she also needs to go through an authentication process, by inserting a valid ATM card and typing the correct PIN. You may also remember in some movies, people need to scan their retina in order to get into a highly classified area. In all these examples, authentication is completed by different factors, including knowledge factors ("things only the user knows", such as the phone passcode, the usernames and passwords), possession factors ("things only the user has", such as ATM cards), and inherence factors ("things only the user is", such as retina or other biometrics). An authentication that involves more than one factor is referred to as *multi-factor* authentication [3]. Normally, the more factors are included, the more secure the authentication is. But on the hard hand, more authentication factors will take a longer time to go through. Obviously, there is a trade off between security and convenience.

It is important to protect today's smartphones using multi-factor authentication. However, existing multi-factor authentication schemes

Figure 1: Simple passcode.

[4,5,6] could not be directly used on smartphonesdue to the following two reasons. First, people may need to frequently unlock the phone to check emails or use social network apps. Second, people want to unlock the phone immediately to either take a quick picture or make a phone call. In other words, authentication on smartphones should be convenient.

In this paper, we describe an authentication framework that aims to protect smartphones while still provide conveniences. The main idea of this framework works as follows. If we assume that users have patterns using their smartphone, we can extract the patternssuch as access time, access location, or access interval. After the patterns are extracted, a new access is classified as authentic if it follows the patterns; otherwise, it is classified as suspicious. For authentic access

***Corresponding Author:** Dr. Weifeng Chen, Department of Mathematics, Computer Science and Information Systems, California University of Pennsylvania, California, PA 15419, USA; E-mail: chen@calu.edu

Citation: Chen W (2017) Protecting Smartphones Based on Usage Patterns. Int J Comput Softw Eng 2: 113. doi: https://doi.org/10.15344/2456-4451/2017/113

requests, the framework applies simple authentication (e.g., a simple slide on the screen) so that users can quickly use their phones. For suspicious requests, stronger authentication (e.g., multiple factors including passcodes and some biometric authentication) will be used to protect the phones. If a user passes a strong authentication, access requests will be granted, i.e., the user will be able to use the phone. This may happen in two scenarios. First, the owner of a phone has emergency and needs to use the phone. This access request does not exhibit the pattern and will be classified as a suspicious request. However, the owner will be able to pass the strong authentication. In a second scenario, the owner may lend the phone to his/her friends or kids. Access requests from a friend or kid will be classified as suspicious requests. With the permit of the owner, the friend or kid may be able to pass the stronger authentication an still be able to use the phone.

Section 2 describes a survey on mobile users thatsupports the assumption of usage patterns on smartphones. The survey questions are presented and the survey results are analyzed. Section 3 describes the authentication framework. Section 4 concludes the paper.

Survey on Daily Usage of Mobile Phones

In 2015, an anonymous online survey was conducted in the university where the author is working. The purpose of the survey was to find out whether patterns exist on users' daily usage on their mobile phones. Figure 2 shows part of the survey questions.

A total of 478 responses to the survey were collected. Table 1 summarizes the demography data of the survey. From the table, one can see major participants are college students.

Gender	Male (116) Female (362)
Age	10-20 (240), 20-30 (203) 30-40 (17) 40-50 (13) Other (5)
Phone OS	Android (160) iOS(292) Others: (26)
Provider	Verizon (257) AT&T (94) T-Mobile (19) Sprint (63) U.S. Cellular (3) Others (42)

Table 1: Demography data of the Survey on daily usage of mobile phones.

Usage patterns on social apps

Social apps are popular. Among the total 478 respondents, 440 indicated that they use social apps on their mobile phones. Figure 3 shows the number of respondents who use a corresponding social app. Facebook is the most popular one. Note that a respondent may use more than one social apps on his/her mobile phone.

Among the total 440respondents who indicated that they use social apps on their mobile phones, 376 (a 85.45%) indicated that their usage of social apps exhibits some patterns and 64 (a 14.54%) respondents indicated no pattern. Figure 4 illustrates different time patterns when survey respondents use social apps daily on their mobile phones, most of them at night before going to bed.

Usage patterns on alarms

As a built-in feature, alarms on mobile phones have been used frequently. Among the total 478 respondents, 434 indicated that they use social apps on their mobile phones. 363 out of 434 (a 83.64%) of the respondents indicated that their usages of alarms exhibit some patterns. Figure 5 demonstrates different time patterns when survey respondents use alarms on their mobile phones.

Gender: Male Female
Age: 10-20, 20-30, 30-40, 40-50, Other
Your mobile phone's OS: Android iOS Others: _____
Your mobile phone carrier: Verizon AT&T T-Mobile Sprint
U.S. Cellular Others: _____

Q1-1: Do you use any **social apps** on your mobile phones, such as Facebook, Instagram, Whatsapp, Wechat? Yes No

If you answer "No", please go to Q2-1

Q1-2: Which social apps you use mostly? _____

Q1-3: Do you think your usage of social apps exhibits some patterns? Yes No

If you answer "No", please go to Q2-1

Q1-4: Please tell us when you use your social apps (can choose more than one that applies)

- Right after wake up
- During noon break
- Evening around supper
- At night before going to bed
- Others (please specify _____)

Q2-1: Do you play **games** on your mobile phones? Yes No

If you answer "No", please go to Q3-1

Q2-2: Which games you play mostly? _____

Q2-3: Do you think your usage of play games exhibits some patterns? Yes No

If you answer "No", please go to Q3-1

Q2-4: Please tell us when you play games: (can choose more than one that applies)

- Right after wake up
- During noon break
- Evening around supper
- At night before going to bed
- Others (please specify _____)

Figure 2: Survey on daily usage of mobile phones

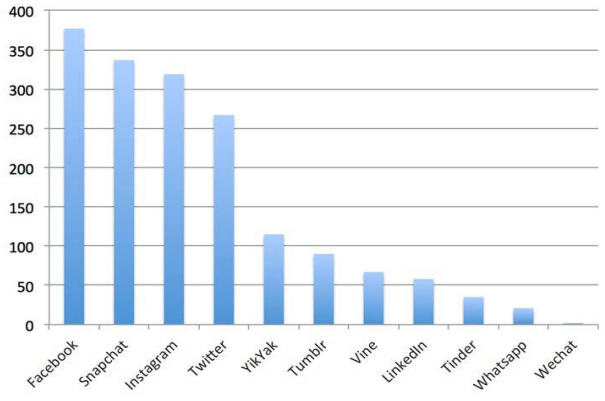

Figure 3: # of survey respondents using different social apps on mobile phones.

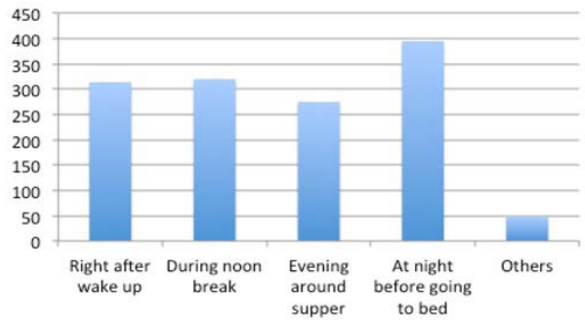

Figure 4. # of survey respondents using social apps on different time patterns

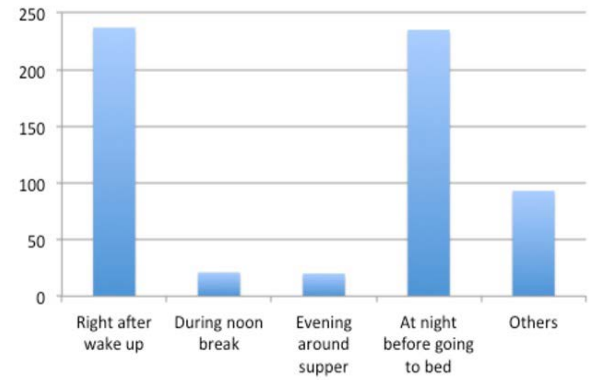

Figure 5: # of survey respondents using alarms on different time patterns

Usage patterns on listening music on mobile phones

A total of 408 respondents indicated that they listen to music on mobile phones, out of which, 265 (a 64.95%) answered that their listening to music exhibit some pattern. As shown in Figure 6, respondents listen to music throughout a day.

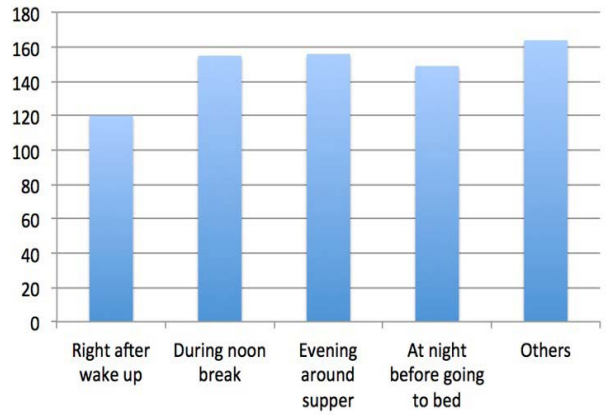

Figure 6: # of survey respondents listening to music on different time patterns

Usage patterns of using web browsers on mobile phones

With data plan becoming common, people now use web browser daily on mobile phones. A total of 435 out of 478 (a 91%) indicated that they used web browsers on mobile phones. Only 204 out of 435 (a 46.90%) responded that their usage of web browser exhibit some pattern, which is demonstrated in Figure 7.

Usage patterns of using calendar on mobile phones

Similar to alarms, calendarsare also a built in function for all smartphones. In this survey, 316 respondents had used calendars, out of which, only 127 (a 40.18%) thought that their usage of calendars exhibits some patterns.

Usage patterns of using camera on mobile phones

Cameras have become critical for smartphones. 462 respondents in the survey had used cameras on their phones, out of which, only 159 (a 34.41%) thought that their camera usage exhibits some patterns.

Usage patterns of playing games on mobile phones

People now can play games on mobile phones. However, due to the limited hardware resource, games played on phones may not be as attractive as those played on PC computers. In this survey, only 234 (a 48.95%) respondents played games on their mobile phones.

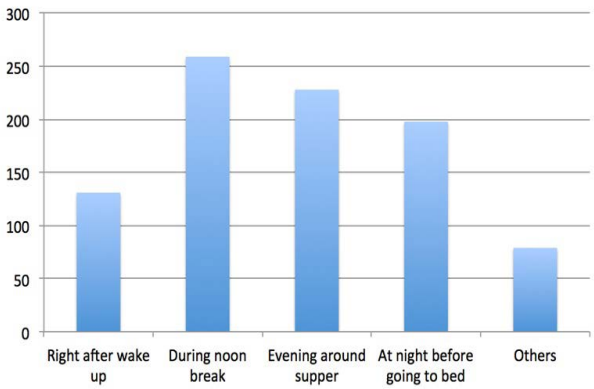

Figure 7: # of survey respondents using web browsers on different time patterns.

Summary of the survey

Conducting this survey is important to this research. The results of the survey verify the assumption that phone usages exhibit some patterns. As we described above, although some usages may not have patterns such as the games, cameras and calendars, other usages exhibit patterns, including social apps (85.45%), alarms (83.64%) and music (64.95%).

It should be noted that the patterns collected in the survey only indicate that usage of smart phones exhibits some patterns. It is true that these patterns reveal that people actually have many similarities when they use their mobile phones. For example, many people browse websites with mobile phones during noon break. Thus only these usage patterns themselves are not able to differentiate users. However, these usage patterns, together with other patterns (e.g., access time, access location, or access interval) that are not collected in the survey, can be used to generate signatures that are unique enough to differentiate users and consequently distinguish suspicious requests from authentic requests.

Protection Framework

Figure 8 presents the workflow of the proposed framework. Each component of the framework is described in details.

Training and signature generation

Before the authentication scheme is enforced, a training process is required. During this process, users' usage patterns are collected. In addition to the time patterns demonstrated in the survey described in Section 2, other information that can be integrated into patterns includes access locations, access interval and phone positions. During the training process, every time when a user is using his/her phone, different kinds of information are collected. In each phone usage, no matter how long the user uses the phone, information such as the access time, access locations, and access intervals, can be collected. If a user uses the phone long enough, then information such as the usage patterns presented in the previous section will be collected.

Today's phones are equipped with GPS, which can collect the location info. Access interval is the time between two consecutive accesses. Different sensors have been integrated in today's smartphones, such as accelerometers, orientation sensors and magnetic field sensors. These sensors are able to provide info on phones' positions.

With these different kinds of information available, a user's usage signature could be created after standard information extraction techniques such as factor analysis [7], standardization, projection & dimension reduction and least square regressions. Typical clustering algorithms such as DB-SCAN [8] and GDILC [9] will be applied to generate a usage pattern. A usage pattern is vector with four elements <Time, Locations, Interval and Positions>, denoted as <*T, L, I, P*>. Four coefficients wt, wl, wiandwpare associated with these four elements such that $w_t+w_l+w_i+w_p=1$. By adjusting these four coefficients, different weights can be assigned to different elements in a usage pattern.

During the training process, theframework will assume that all of the accesses are authentic. Whenever the authentic user is using the phone, signals are collected, standardized, projected and clustered to the pattern vector. Four coefficients w_t, w_l, w_i and w_p are adjusted using learning algorithms. When the coefficients become stable, the training process is completed and the framework can begin to enforce authentication on access requests, a topic described next.

Enforcing

As shown in Figure 8, once the usage pattern is created, it can be used to protect phones by enforcing stronger authentication for suspicious accesses.

Suspicious accesses are those accesses that do not match the usage pattern created during the training process. Determining whether a current access matches the established usage pattern is a process of model matching. For example, Local outlier factor (LOF)[10] is a data mining technique that is proposed for outlier detection [11, 12], which can be used to determine whether a collected data is an outlier.

Stronger authentication can be implemented using different approaches, such as a longer password rather than just a simple slide on the screen or just a 4-digit passcode. Multiple factor authentication [3] could be also an idea solution. In addition to passcodes/passwords, we can add biometric authentication such as voice [13] or fingerprints [14]. Biometric authentication has become available in mobile phones [15].

If the access request is identified as an authentic access, the framework will just apply a simple authentication so that the authentic user can access the phone quickly. Examples of simple authentication include a simple pattern lock or just a 4-digit passcode.

Feedback

It is possible that the model matching process makes mistakes, e.g., false positive, by classifying an authentic access as a suspicious access. After successfully passing the stronger authentication, this authentic user can provide this false positive feedback to the framework, which can adjust the usage pattern. The feedback mechanism also helps when people suddenly change their usage patterns, e.g., when people travel, they use their phones differently from when they work. In this case, a user can similarly provide this false alarm feedback to the framework.

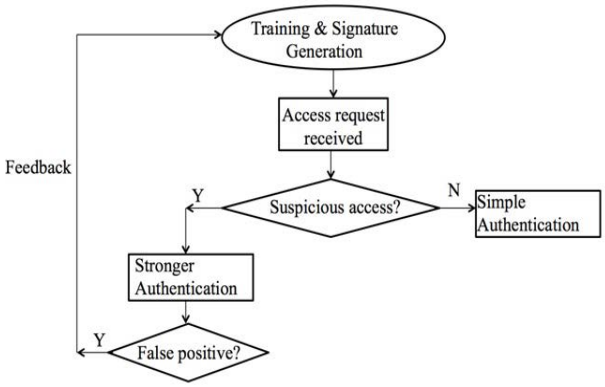

Figure 8: Data flow of the protection framework based on usage signatures.

Limitation

The idea of the proposed framework is to use a built usage signature to distinguish suspicious requests from authentic requests. Thus the limitation of the framework exists. It cannot prevent a bad person from logging in the phone in the first place before pattern signatures are built, which is a common challenge to all authentication problems, i.e., how to authenticate a person at the beginning. Normally, at the beginning, authentication cannot be done just based on the information of the person to be authenticated. Other information, such as a signature from a trusted third-party, is necessary.

Conclusion

In this paper, we presented a survey on mobile usage patterns with detailed analysis. Different kinds of phone usage were surveyed. Analysis results supported the hypothesis that mobile phone usages exhibit some pattern. Based on the results, a framework to protect mobile phones based on usage patterns is discussed.

Competing Interests

The authors declare that they have no competing interests.

References

1. Android Apps on Google Play.
2. Authentication definition on Dictionary.com.
3. Multi-factor authentication, Wikipedia entry.
4. Jin ATB, Ling DNC, Gohb A (2004) Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition 37: 2245 - 2255.
5. Lumini A, Nanni L (2007) An improved BioHashing for human authentication. Pattern Recognition, 40: 1057-1065.
6. Connie T, Teoh A, Goh M, Ngo D (2004) PalmHashing: a novel approach for dual-factor authentication. Pattern Analysis and Applications7: 255- 268.
7. Factor Analysis (2016) Wikipedia entry.
8. Ester M, Kriegel HP, Sander J, Xu X (1996) A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise, Proceedings of the 2nd International Conference on Knowledge Discovery and Data Mining (KDD'96), Portland, Oregon, USA, August 1996, pp. 226-231.
9. Zhao Y, Song J (2001) GDILC: a grid-based density-isoline clustering algorithm, Proceedings of the 2001 International Conferences on Info-tech and Info-net (ICII'01), Beijing, China, October 2001, pp. 140 -145.

10. Breunig MM, Kriegel HP, Ng RT, Sander J (2000) LOF: identifying density-based local outliers, Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data (SIGMOD'00), Dallas, Texas, USA, June 2000, pp. 93 - 104.

11. Ma Y, Shi H, Ma H, Wang H (2013) Dynamic process monitoring using adaptive local outlier factor. Chemometrics and Intelligent Laboratory Systems 127: 89-101.

12. Liu J, Deng H (2013) Outlier detection on uncertain data based on local information. Knowledge-Based Systems 51: 60-71.

13. Campbell J (1996) Speaker Recognition, In Jain A, Bolle R and Pankati S (Eds.) Biometrics: Personal Identification in Networked Society, Springer, pp. 165-189.

14. Subban R, Mankame D (2013) A Study of Biometric Approach Using Fingerprint Recognition. Lecture Notes on Software Engineering 1: 209-214.

15. Curran K (2016) Biometric Authentication: Making mobile devices and apps safer.