Volume 2, Issue 1, January 2017 ISSN (online): 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

Authentication of Smartphone Users Using Behavioral Biometrics And OPass Technique

Miss.Kalyani Kate
Dept. of Computer Engg.
SVIT college of engineering,Nashik
MH,INDIA

Miss.Shital Ahire
Dept.of Computer Engg.
SVIT college of engineering,Nashik
MH,INDIA

Miss.Jyoti Hake
Dept.of Computer Engg.
SVIT college of engineering,Nashik
MH,INDIA

Miss.Harsha Shelke
Dept. of Computer Engg.
SVIT college of engineering,Nashik
MH,INDIA

Abstract: ***Smartphones and tablets have become ubiquitous in our daily lives. Smartphones, in particular, have become more than personal assistants. These devices have provided new avenues for consumers to play, work and socialize whenever and wherever they want. Password-based user authentication can resist brute force and dictionary attacks if users select strong passwords to provide sufficient entropy. However, password-based user authentication has a major problem that humans are not experts in memorizing text strings. oPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through oPass, users only need to remember a long-term password for login on all websites. However, mobile devices are also susceptible to various problems. One of the greatest concerns is the possibility of breach in security and privacy if the device is seized by an outside party. It is possible that threats can come from friends as well as strangers. Due to the size of smart devices, they can be easily lost and may expose details of users' private lives. In addition, this might enable pervasive observation or imitation of one's movements and activities, such as sending messages to contacts, accessing private communication, shopping with a credit card, and relaying information about where one has been. This paper highlights the potential risks that occur when smartphones are stolen or seized, discusses the concept of continuous authentication, and analyzes current approaches and mechanisms of behavioral biometrics with respect to methodology, associated datasets and evaluation approaches.***

Keywords: Smartphone, User Behavior, Biometrics, Progressive Authentication, Implicit Authentication.

I. INTRODUCTION

OVER the last few years, the world has witnessed the beginning of a revolution taking shape in the field of technology. One of the greatest innovations in technology is the Smartphone device. Smartphone devices are characterized by expedient features, such as sophisticated operating systems that can allow users to browse the Internet; to listen, watch, and record video streams; and to navigate, using GPS. These devices also have large internal storage that enables users to store gigabytes of valuable information, such as personal photos, contact details, call histories and private messages. To mitigate the issue, we propose a context-aware ad recommendation framework that takes into account the relatively static personal interests as well as the dynamic news feed from friends to drive growth in the ad click-through rate. We treat the news feed as a dynamic context that provides additional clue in the spatial, temporal and social dimensions for ad recommendation. For example, when a friend posts in Facebook the dining photos in a restaurant, relevant promotion coupons can be recommended. When a friend shows the status in hospital, displaying gift delivery ads is a good choice. Such motivation was also supported by a very recent work from Twitter in which the contents in the tweet stream were taken into account to enhance the click-through prediction rate of advertising.

1) We propose a new context-aware ad recommendation framework on social networks by considering both long-term user interests and highly dynamic contents in the news feed.
2) We present an online retrieval strategy that obtains k most relevant ads when a read operation is triggered.
3) We devise a safe region technique to avoid repetitive retrieval when the context varies little.
4) We propose a hybrid model to seamlessly combine the merits of the two retrieval strategies.

5) We conduct extensive experiments on real social networks with billions of edges and real ad datasets with millions of tuples. The experimental results show that our hybrid method significantly outperforms the other two retrieval strategies up to 30x speedups.

A. Motivation

In this paper, we plan to comprehensively review the state of- the-art in smartphone authentication focusing on seven types of behavioral biometrics, which are handwaving, gait, touchscreen, keystroke, voice, signature and general profiling. We summarize existing studies which propose significant solutions for smartphone authentication by discussing the following points:

- The amount of the data the authors use,
- The types of classifiers the authors choose, and
- The results the authors obtain.

II. LITERATURE SURVEY

Rapid progress in mobile technology has led to a significant shift in large numbers of consumers using smartphone devices instead of personal computers. Market research finds that the number of smartphones sold has surpassed the number of laptops sold worldwide [1]. The tremendous increase in the number of consumers who are buying smartphones has pushed these devices to the top of the market, and they now lead all other electronic devices in terms of sales. According to the International Data Corporation (IDC), the total number of shipments in the second quarter of 2015 reached 337.2 million smartphones worldwide, an increase of 11.6% compared to the same quarter in 2014 [2]. The second quarter in 2015 has the second highest quarterly total on record. The number of smartphones is shipped predicted to rise to 1,928.4 million in 2019 [3]. As much as these devices have gained in popularity and enhanced users' productivity and consumption of entertainment, the security of these devices continues to be a major concern for manufacturers and users alike. This paper focuses on current methods for user authentication on smartphone devices. Over the past few decades, text password has been adopted as the primary mean of user authentication for websites. People select their username and text passwords when registering accounts on a website. In order to log into the website successfully, users must recall the selected passwords. Generally, password-based user authentication can resist brute force and dictionary attacks if users select strong password to provide sufficient entropy. However, password based user authentication has a major problem that humans are not experts in memorizing text strings. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe. Another crucial problem is that users tend to reuse passwords across various websites. Password reuse causes users to lose sensitive information stored in different websites if a hacker compromises one of their passwords. This attack is referred to as the password reuse attack. The above problems are caused by the negative influence of human factors. Up to now, researchers have investigated a variety of technology to reduce the negative influence of human factors in the user authentication procedure Since humans are more adept in remembering graphical passwords than text passwords many graphical password schemes were designed to address human's password recall problem. Using password management tools is an alternative. These tools automatically generate strong passwords for each website, which addresses password reuse and password recall problems. The advantage is that users only have to remember a master password to access the management tool. Despite the assistance of these two technologies graphical password and password management tool the user authentication system still suffers from some considerable drawbacks. Although graphical password is great idea it's not implemented very well. Password management tools work well; however, general users doubt its security and thus feel uncomfortable about using it. Furthermore, they have trouble using these tools due to the lack of security knowledge. Phishing is the most common and efficient password stealing attack. Some researches focus on three-factor authentication rather than password-based authentication to provide more reliable user authentication. Three-factor authentication depends on what you know (e.g., password), what you have (e.g., token), and who you are (e.g., biometric).

- **RELATED WORK**

A. Authentication:

Methods that work to enhance security and privacy need to pay particular attention to authentication. This section introduces concepts that are necessary to discuss methods of information security, in particular authentication. A. Authentication Authentication is the process used to validate the true user of a system. Authentication, in the context of security, takes into account three primary strategies [22].

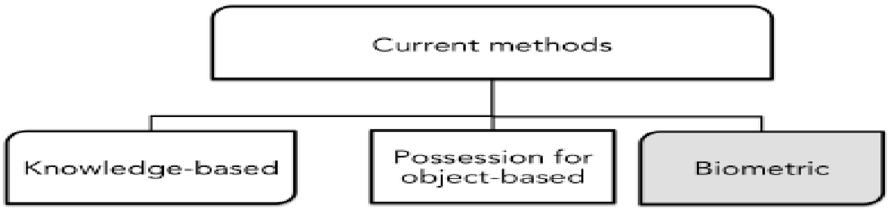


Figure 1: Authentication Strategies for Interaction between Users and Smart devices

1) Knowledge-based, which uses something unique to an individual: This type of entity could be a password, answer to a security question, or an ID number that a user must know.
2) Possession for object-based, which uses something one possesses in a physical sense: The prevalent examples of this type are a security token, an ID card or another trusted device.

3) Biometric, which denotes a physical or behavioral characteristic: This can be represented by one or more physical or behavioral attributes. Common examples are fingerprints and keystroke dynamic models of the owner of the device.

Figure. 1 illustrates these strategies that aim to improve authentication between users and smartphones.
Authentication can be active or passive. Active Authentication requires dealing with a device and inputtingone or more pieces of valid information or answers to questions. Because most individuals use many applications or services, this kind of authentication can become tedious and frustrating; if required by individual applications. As a result, many individuals prefer to use their applications with fewer security impediments each time they decide to access their devices [23]. Current smartphones are based on entry-point authentication, which can be either a Personal Index Number (PIN) or a secret pattern. To use PIN, a user is usually required to pick 4 digits for validation. The user has to input this code correctly otherwise, he/she cannot pass the entry-point to his/her device. Another current method is the use of a secret gesture. A secret gesture is defined by moving a finger over the screen to create a certain pattern. This pattern can be used as authentication to allow the user to enter the device. Continuous authentication, also known implicit, passive or progressive authentication, aims to offer another way to prevent unauthorized accesses of smartphones [24]. This method works passively in the background of the device to make a decision. It is divided into two phases. First, the user accesses his/her device as usual, but the system records appropriate features as the user goes about his/her business. In the case of touchscreen analysis, the recorded features may include finger movement, speed, X and Y coordinates of fingers and the pressure applied at sampled time points. After observing the user behavior for a period of time, the system learns characteristics of behavior data by performing statistical analysis or using machine learning. Second, at a later time after the user logs in to his/her device by using for example, a PIN, the system continuously compares current user behavior with the learned user model or computed statistical profile to make an authentication decision [20]. Any proposed approach based on continuous authentication should include three features: It should be continuous, should not intrude on normal user behavior and should be light-weight. In other words, the system should allow a legitimate user to use the device without interrupting him/her, e.g., by asking for authentication information such as a PIN each time he/she wants to access the device. In addition, the authentication approach should use low computational resources [20].

B. Biometric

A biometric characterizes unique physical or behavioral features of an individual. A biometric scheme aims to detect and correctly identify the user [22]. The US National Science and Technology Council's Subcommittee (NSTC) on Biometrics defines two categories of biometrics: behavioral and physiological [23]. Physiological security detects the physical make-up of a person and uses resources such as retina or iris scans, fingerprints and face recognition. Behavioral biometrics are based on a user's behavior and includes analysis of information like the shape and flow of one's handwriting, timing of keystrokes, unique patterns inherent in one's gait, speech and usage of styluses, and other features of one's general behavior [24]. The use of biometrics, generally, is divided into two groups based on the type of application: identification and authentication [24]. Fig. 3 outlines the two types of biometrics and examples of each type. Once we combine more than one primary type of authentication, we may be able to develop stronger security systems [22].

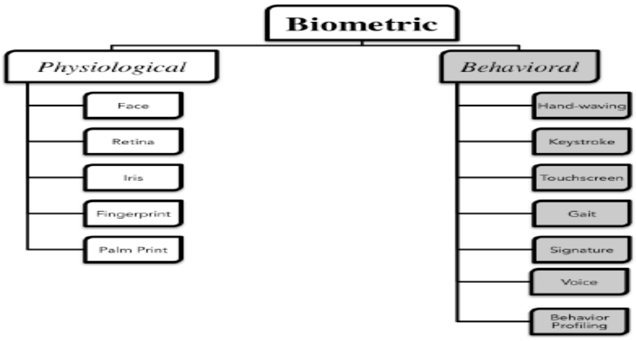


Figure 2: Approaches to Authenticate Users

C. Behavior Biometric

In this paper, we focus on comprehensively summarizing the state-of-the-art in improving a smartphone's security based on continuous authentication using behavioral biometrics. Behavioral biometrics, as defined in III-B, use behavioral traits of a subject like how one touches screen, walks, talks, signs a signature, and types to identify a subject. Each subject is expected to differ from all others when analyzed using one or more of these features. In the following sections, we discuss in depth four types: keystroke, touchscreen behavior, gait and handwaving, and also introduce other types such as voice, signature and profiling. A powerful argument for behavioral biometrics is that it can assist in continuous and passive authentication without requiring additional hardware. As a result, behavioral authentication is likely to be cheaper than using physiological biometrics. In the following sections, we will discuss several examples of behavioral biometrics. These are based on touchscreen behavior, gait, keystroke, handwaving, voice, profiling and signature.

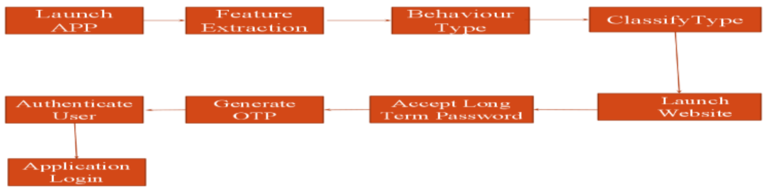
D. Evaluation Metrics

Various metrics have been used for evaluating each of the proposed mobile authentication systems. For example, to assess the performance of a biometric system, we need to understand two error rates, False Acceptance Rate (FAR) and False Rejection Rate (FRR). Table II contains several metrics that have been used to assess implemented approaches. As an example, FAR is defined as the percentage of impersonators who were incorrectly identified by security systems as genuine users. The purpose of evaluating an authentication system should include the following objectives: providing a trade-off between strong protection and appropriateness of the authentication process, achieving reasonable accuracy in estimating the level of user authenticity, and providing for acceptable execution time and power consumption, i.e., reducing authentication overhead on smartphone devices.

E. Smartphone Sensors

Most modern smartphones have built-in sensors which can measure motion and environmental and positional environment the devices are subject to. They provide several facilities such as providing accurate and precise raw data, observing the position in three dimensions, and measuring any possible changes in the surrounding environment sufficiently close to the device . The raw measurements may be aggregated by programs or applications to recognize aspect of how people walk, drive, sit up or talk. Many studies in different fields in physiological and behavioral biometrics are based on different sensors to record and extract user's features like the orientation of the device, the pressure on the touchscreen, the pattern of holding the device and the speed of movement. In general, smartphones these days include Android, Apple and Windows platforms and come with three types of sensors, which are Position sensors, Motion sensors and Environmental sensors . Position sensors are employed to find the physical position of a device. This group includes several sensors including orientation sensors and magnetometers. The magnetometer is used to measure the strength and the direction of earth's magnetic fields, which are expressed in tesla. It can be used as a compass, which can be used to find directions in a map. Accelerometers, gyroscopes and magnetometers consistently return three-dimensional values, which are X or -X, Y or –Y and Z or -Z . Motion sensors measure acceleration and rotational forces along three axes. Examples of such sensors are accelerometers, gravity sensors, gyroscopes and rotational vector sensors . An accelerometer can measure any movement of the phone including fall of the owner when holding the phone or free fall of the phone. A gyroscope detects the current orientation of the device and any possible spin or rotational change. Accelerometers and gyroscopes always return three dimensional values [13]. The orientation of the smartphone can be computed from the angular velocity detected by the gyroscope, which is expressed on 3 axes S(t) = S−!x + S−!y + S−!z (1) where S(t) denotes the angular velocity, and S−!x, S−!y, and S−!z refer to the vectors of angular velocity around X, Y, and Z axes . Environmental sensors measure parameters of the environment. Tools in this category of sensors include barometers, photometers and thermometers Besides these sensors, smartphones also include other sensors such as microphones, cameras, touchscreens, Global Positioning Systems (GPS), and compasses.

III. PROPOSED SYSTEM



A. *Feature Extraction:*

First, the user accesses his/her device as usual, but the system records appropriate features as the user goes about his/her business. In the case of touchscreen analysis, the recorded features may include finger movement, speed, X and Y coordinates of fingers and the pressure applied at sampled time points. After observing the user behavior for a period of time, the
system learns characteristics of behavior data by performing statistical analysis or using machine learning.

B. *Behavior Type Recognition:*

Based on the features system will check weather which is the behavior type and will take input to system accordingly.

C. *Classify:*

Naïve bayes Classification for the behavior type classification is been done based on the features .

D. Long Term Password:

1. User enters the username, userid and server no to the server.
2. Then based on the mobile which the user is using the TSP traces the phone number of user and long term password is sent to him via mobile.
3. Based on the long term password and the server number one time password will be generated.
4. The one-time password generated is unique for every session.

E. Authenticate User:

The user uses her cell phone to produce a one-time password, e.g., and deliver
necessary information encrypted with to server via an SMS message. Based on pre shared secret credential, server can verify and authenticate user.

CONCLUSION AND FUTURE WORK

The growing number of users of smart device is resulting in an increasing amount of private information being stored inside each such devices. Numerous problems in security and privacy are constantly being raised. To resolve these issues, researchers have implemented many methods including continuous authentication approaches based on user behavior. This paper has discussed and compared a number of existing solutions from several perspectives. New methods must focus on multiple characteristics and secure against a variety of attacks, while making the security system easy to use and adapted to each owner. In addition to the methods discussed above, a promising approach may be to measure user behavior in terms of application usage. Each smartphone contains applications which can be used for various purposes. Therefore, making Continuous authentication based on application usage can be one way to enhance security and privacy. OPass has been implemented for secure passwords. The design principle of opass is to eliminate the negative influence of human factors as much as possible. Through opass, each user only needs to remember a long-term password which has been used to protect her cellphone.

REFERENCES

1. Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks, IEEE Transactions of Information Forensics and Security, Vol 7 No 2, April 2012, pp. 651-663
2. *J. Thorpe and P. van Oorschot, "Towards secure design choices for implementinggraphical passwords," presented at the 20th. Annu. Computer Security Application Conf., 2004.*
3. P. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Information Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.
4. S. Gawand E. W. Felten, "Password management strategies for online accounts," in SOUPS '06: Proc. 2nd Symp. Usable Privacy . Security, New York, 2006, pp. 44–55, ACM.
5. D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM.
6. B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.
7. S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords,"Proc. 16th ACM Conf. Computer Communications Security, New York, 2009, pp. 500– 511, ACM.
8. Adrian perrig, Diana song, "Hash visualization: A new technique to improve real world security, computer science department, Carnegie mellon university, 2010.
9. N. Duta, "A survey of biometric technology based on hand shape," Pattern Recognition, vol. 42, no. 11, pp. 2797–2806, 2009.
10. R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," International Journal of Biometrics, vol. 1, no. 1, pp. 81–113, 2008.
11. X. Zhang and Y. Gao, "Face recognition across pose: A review," Pattern Recognition, vol. 42, no. 11, pp. 2876–2896, 2009.
12. A. K. Jain, "Biometric recognition: overview and recent advances," in Progress in Pattern Recognition, Image Analysis and Applications. Springer, 2007, pp. 13–19.
13. M. Rogowski, K. Saeed, M. Rybnik, M. Tabedzki, and M. Adamski, "User authentication for mobile devices," in Computer Information Systems and Industrial Management. Springer, 2013, pp. 47–58.
14. W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: A survey," Communications Surveys & Tutorials, IEEE, vol. 15, no. 1, pp. 402–427, 2013.
15. S. A. Hoseini-Tabatabaei, A. Gluhak, and R. Tafazolli, "A survey on smartphone-based systems for opportunistic user context recognition," ACM Computing Surveys (CSUR), vol. 45, no. 3, p. 27, 2013.
16. Lookout, "Lost and Found: The Challenges of Finding Your Lost or Stolen Phone," "https://blog.lookout.com/blog/2011/07/12/ lost-and-found-the-challenges-of-finding-your-lost-or-stolen-phone/", 2011, [Online; accessed 05-DECEMBER-2015].
17. "Smart phone thefts rose to 3.1 million in 2013," "http://www.consumerreports.org/cro/news/2014/04/ smart-phone-thefts-rose-to-3-1-million-last-year/index.htm", 2013, [Online; accessed 05-DECEMBER-2015].
18. F. Breitinger and C. Nickel, "User survey on phone security and usage." in BIOSIG, 2010, pp. 139–144.
19. X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Computer security applications conference, 21st annual. IEEE, 2005, pp. 10–pp.
20. L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones," in Proceedings of the 20th Network and Distributed System Security Symposium, NDSS, vol. 13, 2013, pp. 1–16.
21. A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," Proc. 4th USENIX Conf. Offensive technologies (WOOT ´ 10), vol. 10, pp. 1–7, 2010.
22. W. E. Burr, D. F. Dodson, and W. T. Polk, Electronic Authentication Guideline, 2004. "Committee on technology, committee on homeland and national security, subcommittee on biometrics," Vascular Pattern Recognition, pp. 1–33, 2006.
23. S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," Journal of Pattern Recognition Research, vol. 7, no. 1, pp. 116–139, 2012.