Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

An Android Application for Authentication by Learning User Biometric Behavior

A Saipriya[1], Aduri Manasa[2], Chaithra C[3], S M Amurtha[4]

Abstract

Smartphones and tablets have turned out to be universal in our day by day lives. Smartphones, specifically, have turned out to be more than individual collaborators. These gadgets have given new roads to purchasers to play, work and mingle at whatever point and wherever they need. Smartphones are little in size; so, they are anything but difficult to deal with and to stow and convey in clients' pockets or satchels. Be that as it may, Smartphones are likewise powerless to different issues. One of the best concerns is the likelihood of rupture in security and protection if the gadget is seized by an outside gathering. It is conceivable that dangers can originate from companions and additionally outsiders. Because of the measure of brilliant gadgets, they can be effortlessly lost and may uncover points of interest of clients' private lives. What's more, this may empower inescapable perception or impersonation of one's developments and exercises, for example, sending messages to contacts, getting to private correspondence, shopping with a charge card, and handing-off data about where one has been. This paper highlights the potential dangers that happen when Smartphones are stolen or seized, examines the idea of persistent validation, and breaks down current methodologies and systems of behavioral biometrics concerning strategy, related datasets and assessment approaches.

Key Terms—Authentication, Continuous Authentication, Smartphone, User Behavior, Biometrics, Progressive Authentication, Implicit Authentication

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. 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].

Problem

Smartphones provide substantial personal benefits for users every day. Many people have come to rely on smartphones for many common, personal and work-related communication tasks. Most users tend to store their passwords and private information on smartphones to efficiently perform these operations in a hassle-free manner. Attackers are likely to access Online Social Networks (OSNs), financial application and other applications on stolen devices. According to 1 [17], the total number of lost or stolen devices in the USA increased from 1.6 million in 2012 to 3.1 million in 2013. Breitinger and Nickel's survey [18] of 548 subjects shows that only 13% of owners tends to

© 2017, This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

use PIN or visual codes, which means that information contained in the smartphones of at least 87% of the owners is in danger once these devices are lost or stolen. 74% of the participants justify this by saying that they want quick access to their devices or that they do not think about security. As a result, protecting the security and privacy of smartphone users against unauthorized access is very important and has become a crucial area of research.

SOLUTION CHARACTERISTICS

Unfortunately, most widely-used authentication techniques for mobile devices are vulnerable, including PINs and patterns as shown in Fig.1. Indeed, these authentication methods fail to detect and identify an intruder once he or she has passed the point of entry. These methods are also deficient in dealing with various non-conventional attacks such as smudge attack, which picks up oils from users' skin to detect patterns or PINs, or a make conventional one such as the shoulder surfing attack, which uses direct observation techniques like glancing over the shoulder of a user to gain information. So, what is the most viable solution to these security problems? An obvious solution is to perform entry point authentication as usual, but go beyond it by performing authentication constantly as a user uses the device. Currently, there are two ways to perform continuous authentication: using physiological and behavioral biometrics. Physiological biometric authentication relies on user's static physical attributes such as fingerprints, facial features or retina images, whereas behavioral biometric authentication adapts to identify features of user's behavior that do not vary over a period of time during daily activities such as typing motions, photo manipulations and hand motions.

Figure 1: Example of Smart phone authentication Entry

BACKGROUND CONCEPTS

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

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. 2 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 inputting one 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.

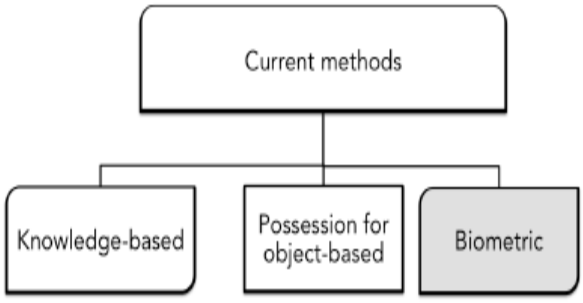

Figure 2: Authentication strategies between user and smartphone

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, touch screen behavior, gait and hand waving, 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.

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 aspects 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 .

APPROACHES TO AUTHENTICATION

This section discusses current research on reinforcing interactions between users and smart devices so that authentication becomes seamless. Studies show that the security and privacy of smartphones and smart devices can be implemented better by using implicit or continuous authentication. Continuous or implicit authentication can potentially offer a stronger line of defense and implement passive security with nonintrusive measures. Such approaches analyze interactions of users with devices and build approximate models of situations when legal users are the ones using the devices. A continuous authentication strategy can strike a balance between passive authentication and entry-point authentication based on the examination of successful logins. In certain situations, a security method may even be able to substitute active authentication with continuous authentication. This section discusses several studies that aim to enhance security based on continuous authentication. These studies use different methods like environment authentication, typing and touchscreen-based authentication, authentication based on user activities and authentication based on gait. Fig. 3 outlines these approaches.

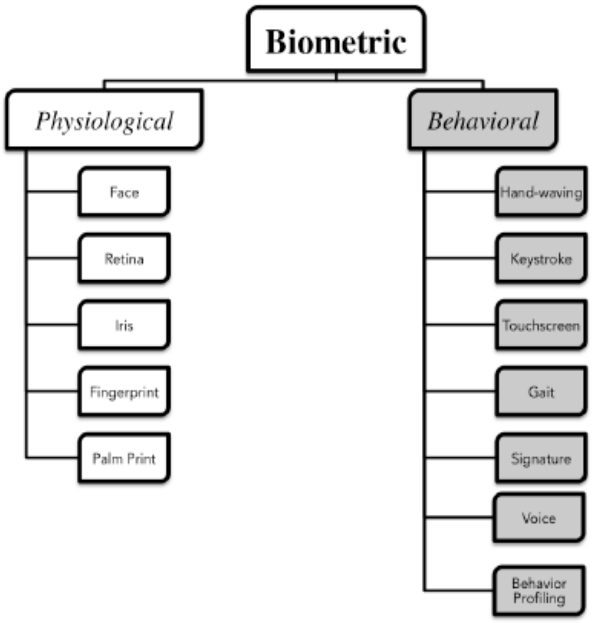

Figure 3: Different approaches used as biometric behavior authentication

Handwaving Based Authentication

Identifying users based on wave gesture has gained attention recently. Hand-waving behavior is the waving pattern of a person. In other words, it can be used to distinguish users because different individual, while interacting with the phone or not, the movement of hand holding the phone is difficult for different people wave differently. For example, many people use their hands to wave in a gentle way while others wave drastically when an individual waves while holding a smartphone. Several features can be used to distinguish among users. These include speed, frequency, waving range and the wrist twisting.

Keystroke Based Authentication

Validating the nature of typing motion is one of the oldest methods to validate users. This technique analyzes keystrokes to determine authorized and unauthorized users. Typing motion or keystrokes can

be used to detect and identify the user based on his/her manner of typing. Typing motion is divided into static and dynamic typing. In static typing, participants are asked to type a short and pre-defined text to compare motion information, while in dynamic typing, the subject is not required to type a specific string. He/she is free to type any text

Gait Based Authentication

A new approach to validating users is gait biometric. Gait biometric aims to identify and verify users' walking styles such as how a person moves at normal or fast pace.The first two approaches that use machine vision and floor sensors are not applicable in the case of smartphones. Therefore, we concentrate on the Wearable Sensor based (WS) approach. Wearable Sensors are devices worn on the bodies of subjects in order to gather information. Information can be collected using a motion recording system, which allows subjects to wear devices at any location on the human body, such as waist, belt, trouser pockets and hand. Sensors like accelerometer, speed sensors gyroscope and force sensors may also be used. Gait features can be extracted using cyclic and non-cyclic methods . A cyclic approach works in two steps. First, cycles in gait are identified in terms of time series. Features of these cycles are computed to extract characteristic templates for classification. This approach is easier to implement than a non-cyclic approach, which requires computing features without prior identification of cycles. A non-cyclic method chooses time intervals during walking to capture locations of sensors

CONCLUSION

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. For example, applications can be categorized into social applications such as Twitter, Facebook and Google+; media applications such as those related to photos, camera and video; chatting applications such as WhatsApp, Snapchat and BBM; and transaction applications such as bank and credit card applications. Quantifying how, when and for how much duration these applications are accessed by specific users may help an implicit authentication system learn manners of fine-grained use and differentiate between authorized and non-authorized persons. Building a corpus for different patterns of app usage with a large number subjects over a number of days will be an excellent way to contribute to the field.

References

[1] I. IGartner, "Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013," "http://www.gartner.com/newsroom/id/2408515/", 2013, [Online; accessed 05-DECEMBER-2015].

[2] M. FRAMINGHAM, "Worldwide Smartphone Market Posts 11.6in Q2 2015, the Second Highest Shipment Total for a Single Quarter, According to IDC," "http://www.idc.com/getdoc.jsp?containerId= prUS25804315/", 23 Jul 2015, [Online; accessed 05-DECEMBER-2015].

[3] ——, "Global Smartphone Growth Expected to Slow to 11.3% in 2015as Market Penetration Increases in Top Markets, According to IDC," "http://www.idc.com/getdoc.jsp?containerId=prUS25641615/", 26 May 2015, [Online; accessed 05-DECEMBER-2015].

[4] J. Ashbourn, Biometrics in the New World: The Cloud, Mobile Technology and Pervasive Identity. Springer Science & Business Media,2014.

[5] L. Long, "Biometrics: The future of mobile phones," Proc. Interactive Multimedia Conference, pp. 1–5, 2014.

[6] A. Goode, "Bring your own finger–how mobile is bringing biometrics to consumers," Biometric Technology Today, vol. 2014, no. 5, pp. 5–9, 2014.

[7] W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," IEEE Communications Surveys, 2015.

[8] H. Crawford, "Keystroke dynamics: Characteristics and opportunities," in Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on. IEEE, 2010, pp. 205–212.

[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.