A Fine-Grained Analysis of User Activity on Mobile Applications: The Sensitivity Level Perception

Saud Alotaibi[1], Steven Furnell[1, 2] and Nathan Clarke[1, 2]
[1]*Centre for Security, Communications and Network Research*
Plymouth University
Plymouth, UK
[2]*Security Research Institute*
Edith Cowan University
Perth, Western Australia

Abstract

Mobile devices contain different levels of data and applications such as photos, text messages, emails and mobile banking applications. Each process within each application has a different level of sensitivity; thus, protection needs to be considered in this context after initial access to the mobile device. The main aim of this research is to investigate when to authenticate the mobile user by focusing on the sensitivity level of each intra-process (within the application) and understanding whether a certain user action in a process may require protection. To accomplish this, the 10 most popular mobile categories were analysed to gain a comprehensive understanding of how to categorise the applications in terms of their sensitivity level. Building upon this analysis, the results show that 78% of 125 user actions are considered sensitive processes. This paper also demonstrates that existing authentication systems lack adequate security solutions to unauthorised access to the mobile device. Consequently, this indicates the need for a robust and usable access control approach to establish a transparent and a continuous authentication system.

1. Introduction

The use of mobile devices in our daily lives has grown steadily. These mobile devices contain sensitive data such as text messages, photos, communication logs, contact lists, personal information and stored passwords. They are also used to perform activities such as sending emails or transferring money via mobile Internet banking, which is considered a sensitive process. In 2015, mobile applications will fail in security tests by 75%. By 2017, the main breaches will be in mobile devices and tablets. In particular, mobile application misconfigurations will be the most common mobile security breaches, accounting for approximately 75% of all breaches [1]. Thus, authentication is vital in securing the sensitive data. This is because after the point-of-entry authentication stage at the beginning of a session, using modalities such as a PIN or password, the user of the device can perform almost all tasks without having to periodically re-authenticate to revalidate the user's identity [2]. This signifies an urgent need to verify the identity of the current user of a mobile device. It must be possible to authenticate legitimate users and detect impostors in a continuous and transparent manner, maintained beyond the point of entry, without the explicit involvement of the user [2].

By regularly checking user behaviour to continuously monitor the protection of the mobile device, data on user behaviour are gathered in the background without requiring any dedicated activity by the user [3]. Additionally, security and usability can be increased through transparent authentication, since the mobile device has a great source of data in terms of user behaviour [2]. In this context, a transparent authentication system can be described as implicit, passive, non-intrusive, unobtrusive, unobservable, active and silent.

This paper begins by presenting transparent authentication systems for mobile devices using unimodal and multimodal approaches. It then discusses the problem and provides a comprehensive analysis of user actions on mobile applications. Finally, the paper offers a conclusion and suggests future work in this area.

2. Transparent authentication systems for mobile devices

Transparent authentication systems for mobile devices may be classified into physiological biometrics such as fingerprint scanning or face recognition and behavioural biometrics such as keystrokes or touch. Physiological biometrics are considered useful for one-off authentication [4, 5] because they require considerable computing power and high-quality images, which are not easy to obtain [5]. For instance, iris recognition needs the user to face the camera, takes more time for authentication and requires high-cost additional hardware [5]. Moreover, iris recognition faces challenges such as detection, segmentation, coding and matching [4]. On the other hand, fingerprint recognition suffers in the presence of poor conditions such as cuts and dirt [4]. As a result, fingerprint and iris scanning are

considered intrusive [3]. In addition, although facial recognition suffers from some problems, such as difficulty of authentication in the dark and changes over time, it could be used in a transparent authentication system to collect a sample without effort from the user [3].

In contrast, behavioural biometrics refer to something the user does, such as typing, gait, application usage, voice or signature, which are considered less sensitive to darkness or noise [3]. Consequently, behavioural biometrics is presented as a suitable method and is more commonly used for transparent and continuous authentication and to provide usability [4]. In the literature, various behaviour-based authentications have been presented to verify the rightful owner of a device, such as keystroke patterns, touchscreen input behaviour, physical location patterns, application usage, call and text patterns, voice patterns and micro-movement patterns [6]. These authentications enable a mobile phone to gather a user's behavioural data without requiring deliberate actions from the user and without requiring additional devices.

Transparent authentication systems for mobile devices have been classified into the following [7]:

- Keystroke-based authentication
- Gait-based authentication
- Touch-based authentication
- Device sensor–based authentication
- Behavioural profiling–based authentication

2.1. Unimodal transparent authentication

Keystroke dynamics or typing rhythm have been used to authenticate the original user in a transparent fashion as the user types characters on a keyboard; this is done by using features such as key hold time, latency, horizontal digraph or vertical digraph. Considerable research has been undertaken on this approach. For instance, Clarke et al. [8] used a neural network classifier to study the feasibility of using keystroke dynamics to verify users' identity on mobile phones. In a follow-up study, Clarke and Furnell [9] asked 30 participants to type telephone numbers and text messages to validate themselves as mobile users, focusing on their typing characteristics, particularly key hold time and the number of times the backspace key was pressed. In addition, Karatzouni and Clarke [10] suggested applying a thumb-based keyboard approach on a mobile phone to authenticate 50 participants. Nevertheless, it is difficult for a keystroke dynamic system to achieve authentication consistently if the user performs the typing in an unusual manner. This system could also be rendered obsolete by touchscreen mobile phones [5].

Gait-based biometric authentication methods validate the user of the phone in a transparent and continuous manner based on the user's gait while walking. Three types of gait recognition systems have been identified: machine vision–based technique, floor sensor–based technique and wearable sensor–based technique [11]. The machine vision–based technique uses cameras from various distances to gather the user's gait data. The floor sensor–based technique collects gait data from several sensors placed on floor mats, measuring things such as pressure and force. Wearable sensor–based techniques take advantage of sensors built into mobile phones, such as accelerometers, gyroscopes and force sensors.

A variety of studies have been conducted on touch-based authentication. For instance, Zheng et al. [12] used a combination of acceleration, pressure, size and time, which can be collected from sensors in touchscreen mobile phones. They claimed that this approach is a non-intrusive authentication method. A similar research project by Li et al. [13] examined user authentication on a mobile phone by continuously observing finger movements on the touchscreen without requiring any deliberate action from the user. However, it employed a two-class classifier, which is considered an unrealistic method, since it requires input data from non-owner users in the training phase [12].

Several studies have investigated the leveraging of multiple sensors on smartphones, combining touch, accelerometer and gyroscope sensor data. Wang et al. [14] claimed that sensor fingerprints could be a feasible solution for user verification. They introduced two new unlocking gestures for sensor-based user authentication based on the sensor fingerprint. Further studies in a similar context, relying only on multiple sensors, have also been conducted. Lin et al. [15] argued that multiple sensor inputs could improve accuracy compared with a single sensor. They presented a non-intrusive authentication approach based on data from an orientation sensor, i.e. gyroscope sensor, by taking the pitch, roll and heading based on how the user holds the phone. Zhu et al. [16] proposed SenSec, an implicit authentication framework, which captures passive sensory data from a mobile device, namely an accelerometer, orientation, compass and gyroscope, which determine where the user is and what he or she is doing.

Studies have proposed application usage aiming at providing transparent authentication. Hayashi et al. [17] argued that device-centric continuous authentication cannot discriminate between data from different applications. They argued that this method cannot make any assumptions in terms of the importance of the application currently being used. More specifically, the lack of a device-centric approach, unaware of the task that the user is performing within an application, can lead to not delivering authentication control at the task level [6]. This will lead to higher authentication overhead.

Hayashi et al. [17] argued for the inefficiency of the all-or-nothing access model and suggested that a mobile user should be authenticated only when a sensitive application is opened, since most applications do not require explicit authentication. In the context of the sensitive application concept, the authors created paper prototypes, i.e. a theoretical method, of two alternative access mechanisms: group accounts (access to some of the functionality that is normally available only when the phone is unlocked) and an activity lock (share a specific set of applications with others users).

In the same context, the work of Riva et al. [18] is based on when (as opposed to how) the user should authenticate and for which application. The authentication decision depends on the confidence level and the level of sensitivity for each application, which are stated by the user to protect sensitive applications from unauthorised use. Similarly, Li et al. [19] introduced a behaviour profiling approach to identify mobile device misuse by focusing on the mobile user's application usage, namely general application usage, voice calls and text messaging. The authors presented a novel behaviour profiling framework that can collect user behaviour to evaluate the system security status of the device in a continuous manner before accessing sensitive services. They investigated the sensitivity of the application, which is mapped with high-risk levels to make the framework more secure and transparent when the user requires access to high-value applications. They concluded that this approach seems to distinguish mobile users through their application usage, particularly by focusing on the names of applications and location of usage, which are considered valuable features.

2.2. Multimodal transparent authentication

Previous studies have investigated the feasibility of combining biometric modalities to authenticate the mobile user [7]. Clarke and Furnell [9] offered a mobile-based system, the intelligent authentication management system, by grouping a secret knowledge-based method and available biometrics modalities. In a follow-up study, Clarke et al. [20] proposed a framework called non-intrusive continuous authentication (NICA) to provide secure, transparent and continuous authentication. The framework uses keystroke dynamics, facial recognition and voice patterns to identify an alert level while the user interacts with the mobile device. NICA is based on 'authentication confidence', which is mapped to each service to allow the user to access a service if confidence levels are higher than the alert level. The authors took into account the hypothesis that different services require different levels of security and protection by understanding the risks associated with specific user actions and services.

Crawford et al. [2] introduced a transparent authentication framework that uses a combination of behavioural biometrics, namely keystroke dynamics and voice recognition, based on the device confidence level. Each task on the device is assigned a particular device confidence level as the minimum threshold for access to the task, either explicitly by the owner or by default. As a result, private or sensitive information can be accessed only at the highest device confidence levels. On the other hand, if the device confidence level is less than the required task confidence level, the user must try to raise the device confidence to be authorised. Therefore, this step will lead the user to use a second authentication action in an explicit manner, such as a password or physiological biometric.

Similarly, Saevanee et al. [21] examined a combination of three diverse biometric methods: keystroke dynamics, behavioural profiling and linguistic profiling. They presented a text-based authentication framework using those modalities and introduced a security level by allowing the user to set security levels for access to different applications. They claimed that this approach would reduce the number of intrusive authentication requests for high security applications by 91%. Likewise, Fridman et al. [22] proposed parallel binary decision-level fusion architecture for active authentication. This fusion is used for classifiers based on four biometric modalities: text analysis, application usage patterns, web browsing behaviour and the physical location of the device by computing GPS (outdoors) or Wi-Fi (indoors).

From a different perspective, some frameworks aim to facilitate the user's shifts from one device to another without asking the user to authenticate. Hocking et al. [23] introduced the Authentication Aura concept, which is based on the enabling of cooperative and distribution authentication between devices owned by a single user. The results of their study demonstrated that this concept could reduce the number of intrusive authentication requests by up to 74%. Building upon the Authentication Aura concept, Abdulwahid et al. [24] suggested a conceptual authentication model hosted in the cloud, called federated authentication. The main principle of this model is taking advantage of cloud computing features such as scalability, universality and adaptability to reduce the need for logging on to and authenticating on each device in a transparent and continuous manner. However, some issues such as privacy, trust and response time need to be considered to make this model more secure and feasible.

3. Discussion

In light of the foregoing exploration, studies have found that behavioural biometrics can operate in

transparent and continuous authentication by constructing a user behavioural profile while the user is using the device, without requiring deliberate actions from the legitimate user. Furthermore, the majority of recent research in this domain has focused on finding appropriate behaviour-based classifiers, such as keystroke, gait, touch or sensors, for a transparent authentication approach. However, these device-centric behavioural authentication approaches apply a specific classifier to verify user identity without taking into account the nature of the applications currently being used. For instance, gait authentication is not suitable for authenticating a mobile user when the text message application is being used, whereas keystroke analysis is suitable to this type of application.

Considering all the above, there is a lack of research on behavioural profiling, particularly on application usage for transparent authentication systems on mobile devices. Moreover, only a few studies have investigated when to authenticate the mobile user. The present study will provide a preliminary analysis of the taxonomy of application-based behaviour by focusing on the sensitivity level of each user action on the application and understanding whether a certain intra-process (within the application) may require protection. For instance, it is unnecessary to authenticate users when they are reading the news or checking the weather forecast through a browser application. By studying user behaviour and interaction with each application, a great deal of information could be collected on user behaviour. This behavioural information might contribute towards monitoring the user's identity by choosing a suitable classifier based on the application type and level of protection.

Therefore, this approach can result in the reduction of unnecessary authentication overheads by focusing on the sensitivity of the user action within the application. For example, an energy consumption challenge can be addressed by turning off sensors based on these factors if there is no need to authenticate the user. Hence, a smarter biometric approach that is able to categorise data from different applications and know what interactions the user is performing within the application will reduce the authentication overhead.

4. Methodology

Each application contains data, and some data require a higher level of protection. To determine whether an application is sensitive, it is useful to identify the confidentiality of data within each application. This classification will be based on how to estimate the risk level for each process. Furthermore, the level of sensitivity is likely to change during the process [25]. The application data can be classified into two types based on their level of confidentiality: public data and sensitive data. This classification of data might help determine which security controls are suitable for protection. The types of application data are shown in Figure 1.

For public data, there is no need to require login because there is no risk to and impact on the owner's data. Examples are reading the news, forecasting the weather and opening maps. No controls are required to protect the confidentiality of public data when a non-owner tries to access public information. On the other hand, the loss, misuse and modification of, or unauthorised access to, sensitive information can adversely affect an individual, cause financial loss and leak personal information such as credit card numbers, bank accounts and health information. Thus, the highest level of security controls should be applied to sensitive data to deny unauthorised access to the content of the application.

Data sensitivity is determined by the types and uses of data within a system [26]. The type and use of the data will have different effects on the protection requirements. The data type is the most significant factor in determining the confidentiality requirement [26].

Table 1 shows the 10 most popular mobile categories and the most popular application for each category in Google Play [27].

Table 1. The 10 most popular mobile categories

No.	Category	Application name
1	Social	Facebook
2	Entertainment	YouTube
3	Communication	Gmail
4	Productivity	Google Drive
5	Shopping	Amazon
6	News	BBC News
7	Travel	Google Maps
8	Lifestyle	Gumtree
9	Photography	Google Photos
10	Finance	HSBC Mobile Banking

For the classification of sensitive data, the impact on the user is divided into the following types:

- Availability: If the action destroys or deletes user information.
- Integrity: If the action changes, modifies or updates user information or causes financial loss
- Privacy: If the action affects the user's safety or privacy or causes embarrassment

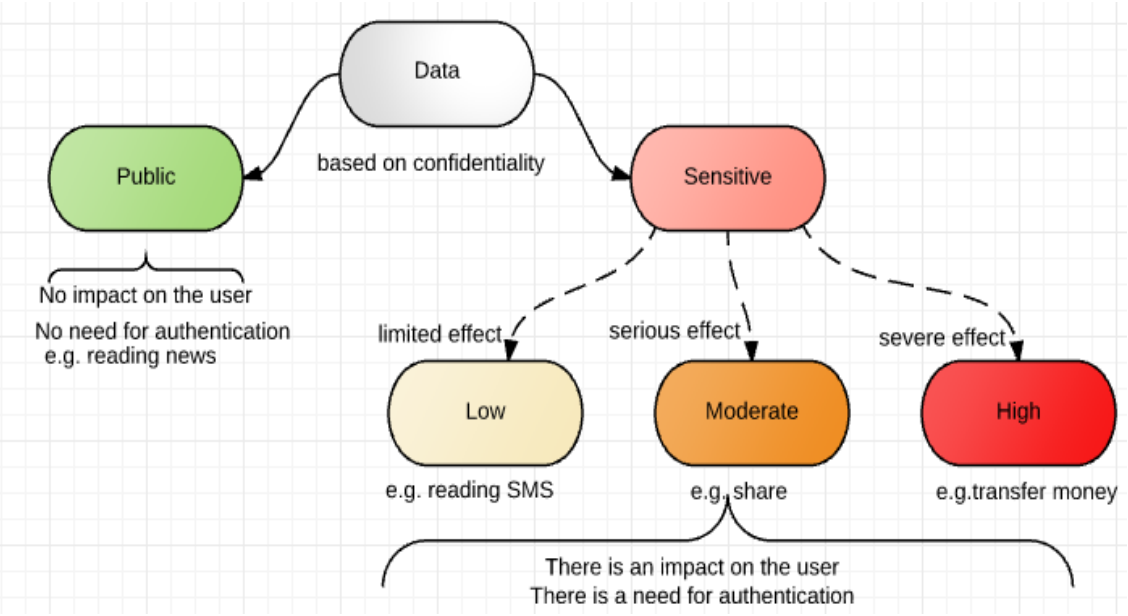

Figure 1. Classification of mobile app data

The sensitivity level is classified into three types [28]:

- Low: If the non-owner's mobile phone action could be expected to have a limited adverse effect on the original user, e.g. rreading SMS.
- Moderate: If the non-owner's mobile phone action could be expected to have a serious adverse effect on the original user, e.g. changing settings
- High: If the non-owner's mobile phone action could be expected to have a severe adverse effect on the original user, e.g. writing, posting on a Facebook wall.

Table 2 presents a more detailed analysis that considers the most regular user actions on these applications. For instance, adding photos on Facebook might be considered a sensitive process that affects the user's privacy, whereas reading the news on BBC News does not have an effect on the user. Nevertheless, there are different levels of application sensitivity. Paying bills and reading products/services are considered as having the same level of risk in the HSBC Mobile Banking application. There is clearly a different level of risk within the application; thus, there is a need for a continuous authentication system to maintain user legitimacy.

After the analysis of user actions (processes) on each application, a total of 125 actions were identified. These actions could be classified based on the data type (public or sensitive). The results show that 78% of the actions involve sensitive data and 22% involve public data. Therefore, the majority of actions involving sensitive data (72%) affect user privacy. As a result, more than 77% of user actions need to verify the user's identity after the point-of-entry authentication.

Figure 2 shows that Gmail, Google Drive and Google Photos are considered sensitive applications because they include sensitive personal user data, whereas BBC News is not considered a sensitive application because it does not contain user data. The majority of user actions on Facebook (85%) and HSBC Mobile Banking (69%) are considered sensitive processes. Google Maps is a moderate application because 58% of its data are sensitive and 42% are public. On the other hand, Amazon, YouTube and Gumtree are sensitive applications because 81%, 73% and 77%, respectively, of their data are sensitive. Figure 2 indicates that 97 of 125 user actions on 10 different mobile application categories involve sensitive data. These findings suggest the need to move the access control system from on the application to within the application based on the sensitivity level and the risk for each user action.

Table 2. Mobile application analysis

App	No.	User action	Data type	Impact on user
Facebook	**1**	Open Facebook	Public data➔ no impact on the user➔ no need to authenticate	
	2	Search on Facebook	Public data➔ no impact on the user➔ no need to authenticate	
	3	Read news feed	Public data➔no impact on the user➔ no need to authenticate	
	4	Read user profile	Sensitive	Privacy
	5	Post on a wall	Sensitive	Privacy
	6	Add photo/link	Sensitive	Privacy
	7	Tag friends/check in	Sensitive	Privacy
	8	Like	Sensitive	Privacy
	9	Comment	Sensitive	Privacy
	10	Share	Sensitive	Privacy
	11	Read notifications	Sensitive	Privacy
	12	Send message	Sensitive	Privacy
	13	Open message	Sensitive	Privacy
	14	Delete message	Sensitive	Availability
	15	Join group	Sensitive	Privacy
	16	Voice call/video call	Sensitive	Privacy
	17	Change settings	Sensitive	Integrity
	18	Update information	Sensitive	Integrity
	19	Add friend	Sensitive	Privacy
	20	Remove friend	Sensitive	Availability
YouTube	**1**	Open YouTube	Public data➔ no impact on the user➔ no need to authenticate	
	2	Search on YouTube	Public data➔ no impact on the user➔ no need to authenticate	
	3	Watch on YouTube	Public data➔ no impact on the user➔ no need to authenticate	
	4	Upload	Sensitive	Privacy
	5	Share	Sensitive	Privacy
	6	Like/dislike	Sensitive	Privacy
	7	Add a public comment	Sensitive	Privacy
	8	Search history	Sensitive	Privacy
	9	Watch later	Sensitive	Privacy
	10	Subscribe	Sensitive	Privacy
	11	Unsubscribe	Sensitive	Integrity
	12	Read subscriptions	Sensitive	Privacy
	13	Read created playlists	Sensitive	Privacy
	14	Create a new playlist	Sensitive	Privacy
	15	Browse channels	Public data➔ no impact on the user➔ no need to authenticate	
Gmail	**1**	Open Gmail	Sensitive	Privacy
	2	Search on Gmail	Sensitive	Privacy
	3	Send an email	Sensitive	Privacy
	4	Read a new email	Sensitive	Privacy
	5	Read an old email	Sensitive	Privacy
	6	Reply to/forward	Sensitive	Privacy
	7	Delete an email	Sensitive	Availability
	8	Chat on Gmail	Sensitive	Privacy
	9	Make a call	Sensitive	Privacy
	10	Change settings	Sensitive	Integrity
	11	Read user's contact	Sensitive	Privacy
	12	Read sent mail	Sensitive	Privacy
	13	Read important email	Sensitive	Privacy
	14	Read user's note	Sensitive	Privacy
Google Drive	**1**	Open Google Drive	Sensitive	Privacy
	2	Search on drive	Sensitive	Privacy
	3	Read file	Sensitive	Privacy
	4	Share file	Sensitive	Privacy
	5	Delete file	Sensitive	Availability
	6	Upload file	Sensitive	Privacy
	7	Download drive	Sensitive	Privacy
	8	Show recent file	Sensitive	Privacy
	9	Upgrade storage	Sensitive	Integrity
	10	Change settings	Sensitive	Integrity

Amazon	**1**	Open Amazon	Public data➔ no impact on the user➔ no need to authenticate	
	2	Search on Amazon	Public data➔ no impact on the user➔ no need to authenticate	
	3	Read user's order history	Sensitive	Privacy
	4	Read user's account	Sensitive	Privacy
	5	Change user's account	Sensitive	Integrity
	6	Manage payment	Sensitive	Integrity
	7	Write a review	Sensitive	Privacy
	8	Add to basket	Sensitive	Integrity
	9	Proceed to checkout	Sensitive	Integrity
	10	Delete from basket	Sensitive	Availability
	11	Edit basket	Sensitive	Privacy
	12	Share	Sensitive	Privacy
	13	Show browsing history	Sensitive	Privacy
	14	Create wish list	Public data➔ no impact on the user➔ no need to authenticate	
	15	Sell on Amazon	Sensitive	Integrity
	16	Read wish list	Sensitive	Privacy
BBC News	**1**	Open BBC News	Public data➔ no impact on the user➔ no need to authenticate	
	2	Read news	Public data➔ no impact on the user➔ no need to authenticate	
	3	Search on BBC News	Public data➔ no impact on the user➔ no need to authenticate	
	4	Forecast the weather	Public data➔ no impact on the user➔ no need to authenticate	
	5	Watch BBC News	Public data➔ no impact on the user➔ no need to authenticate	
	6	Listen to BBC Radio 5	Public data➔ no impact on the user➔ no need to authenticate	
	7	Share	Public data➔ no impact on the user➔ no need to authenticate	
Google Maps	**1**	Open Google Maps	Public data➔ no impact on the user➔ no need to authenticate	
	2	Search on Google Maps	Public data➔ no impact on the user➔ no need to authenticate	
	3	Read user's timeline	Sensitive	Privacy
	4	Add photo	Sensitive	Privacy
	5	Write a review	Sensitive	Privacy
	6	Share link	Sensitive	Privacy
	7	Read user's history	Sensitive	Privacy
	8	Search nearby places	Public data➔ no impact on the user➔ no need to authenticate	
	9	Delete location history	Sensitive	Availability
	10	Download all data	Sensitive	Privacy
	11	Get directions	Public data➔ no impact on the user➔ no need to authenticate	
	12	Show traffic	Public data➔ no impact on the user➔ no need to authenticate	
Gumtree	**1**	Open Gumtree	Public data➔ no impact on the user➔ no need to authenticate	
	2	Search on Gumtree	Public data➔ no impact on the user➔ no need to authenticate	
	3	Post an ad	Sensitive	Privacy
	4	Add a photo	Sensitive	Privacy
	5	Read user's ads	Sensitive	Privacy
	6	Read favourites	Sensitive	Privacy
	7	Send SMS/email	Sensitive	Privacy
	8	Delete ad	Sensitive	Availability
	9	Change settings	Sensitive	Integrity
Google Photos	**1**	Open Google Photos	Sensitive	Privacy
	2	Search on Google Photos	Sensitive	Privacy
	3	Create a new album	Sensitive	Privacy
	4	Share	Sensitive	Privacy
	5	Delete an account	Sensitive	Availability
	6	Back up and sync	Sensitive	Privacy
	7	Delete device copy	Sensitive	Availability
	8	Add to album	Sensitive	Privacy
	9	Change setting	Sensitive	Integrity
HSBC Mobile Banking	**1**	Open HSBC	Sensitive	Privacy
	2	Read transactions	Sensitive	Privacy
	3	Read balances	Sensitive	Privacy
	4	Pay bill	Sensitive	Integrity
	5	Make transfer	Sensitive	Integrity
	6	Paym service	Sensitive	Integrity
	7	Read secure messages	Sensitive	Privacy
	8	Read account details	Sensitive	Privacy
	9	Change settings	Sensitive	Integrity

	10	Read products/services	Public data➔ no impact on the user➔ no need to authenticate
	11	Find HSBC branch	Public data➔ no impact on the user➔ no need to authenticate
	12	Read offers	Public data➔ no impact on the user➔ no need to authenticate
	13	Contact us/help	Public data➔ no impact on the user➔ no need to authenticate

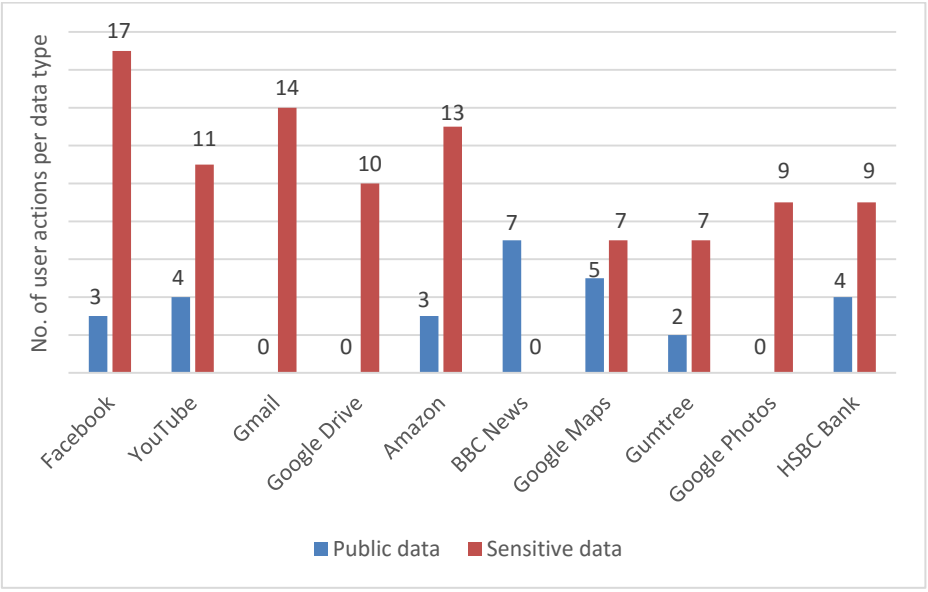

Figure 2. Number of actions involving public and sensitive data for each mobile application

5. Conclusion

In this paper, we argued that there is a severe lack of protection for user's data stored in mobile phones, particularly to prevent further access to sensitive data due to there is no authentication process after accessing the mobile device at the beginning. The results of this analysis study show that 78% of user data are considered sensitive data. This in turn means that there is an ever increasing need for introducing the level of authentication beyond the point-of–entry approach. Consequently, intra-process security should be addressed, and fine-grained authentication control should be provided against unauthorised use based on the sensitivity level of each process within the application. More specifically, this work underscores the need for a usable scheme for accessing mobile phones by considering the risk level for each sensitive process and suggesting the appropriate levels of authentication for each service. Bearing in mind, the solution should take into account the balancing between security and user convenience in order to be more effective.

6. References

[1] Gartner (2013) '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 (13 December 2015).

[2] Crawford, H., Renaud, K., and Storer, T. (2013) 'A Framework for Continuous, Transparent Mobile Device Authentication', Elsevier Computers & Security 39 (2), pp. 127-136.

[3] Clarke, N. (2011) Transparent User Authentication: Biometrics, RFID and Behavioural Profiling, 1st ed., Springer Science & Business Media.

[4] De Marsico, M., Galdi, C., Nappi, M., and Riccio, D. (2014) 'FIRME: Face and Iris Recognition for Mobile Engagement', Image and Vision Computing 32 (12), pp. 1161-1172.

[5] Meng, W., Wong, D. S., Furnell, S., and Zhou, J. (2015) 'Surveying the Development of Biometric User Authentication on Mobile Phones', IEEE Communications Surveys & Tutorials. vol.17, pp. 1268 – 1293

[6] Khan, H. and Hengartner, U. (2014) 'Towards Application-Centric Implicit Authentication on Smartphones', In Proceedings of the 15th Workshop on Mobile Computing Systems and Applications (p. 10). ACM.

[7] Alotaibi, S., Furnell, S., and Clarke, N. (in press) 'Transparent Authentication Systems for Mobile Device Security: A Review', in Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), pp.406-413.

[8] Clarke, N., Furnell, S., Lines, B., and Reynolds, P. (2003) 'Keystroke Dynamics on a Mobile Handset: A Feasibility Study', Information Management and Computer Security 11 (4), pp. 161-166.

[9] Clarke, N. and Furnell, S. (2007) 'Authenticating Mobile Phone Users Using Keystroke Analysis', International Journal of Information Security 6 (1), pp. 1-14.

[10] Karatzouni, S. and Clarke, N. (2007) 'Keystroke Analysis for Thumb-Based Keyboards on Mobile Devices', in Proceedings of the IFIP International Information Security Conference. In New approaches for security, privacy and trust in complex environments. Springer US. , pp. 253-263.

[11] Muaaz, M. and Mayrhofer, R. (2013) 'An Analysis of Different Approaches to Gait Recognition Using Cell Phone Based Accelerometers', in Proceedings of the International Conference on Advances in Mobile Computing and Multimedia, ACM, p. 293.

[12] Zheng, N., Bai, K., Huang, H., and Wang, H. (2014) 'You Are How You Touch: User Verification on Smartphones via Tapping Behaviors', in the 22nd International Conference on Network Protocols (ICNP), IEEE, pp.221-232.

[13] Li, L., Zhao, X., and Xue, G. (2013) 'Unobservable Re-Authentication for Smartphones',In 20th Network and Distributed System Security Symposium (NDSS),volume 13.

[14] Wang, H., Lymberopoulos, D., and Liu, J. (2015) 'Sensor-Based User Authentication', in Wireless Sensor Networks, Springer International Publishing, pp.168-185.

[15] Lin, C., Liang, D., Chang, C., and Yang, C. (2012) 'A New Non-Intrusive Authentication Method Based on the Orientation Sensor for Smartphone Users', in Proceedings of the IEEE Sixth International Conference on Software Security and Reliability, pp.245-252.

[16] Zhu, J., Wu, P., Wang, X., and Zhang, J. (2013) Sensec: Mobile Security through Passive Sensing', in Proceedings of the 13th International Conference on Computing, Networking and Communications,IEEE,pp. 1128-1133.

[17] Hayashi, E., Riva, O., Strauss, K., Brush, A. J., and Schechter, S. (2012) 'Goldilocks and the Two Mobile Devices: Going beyond All-Or-Nothing Access to a Device's Applications', In Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM,p.2.

[18] Riva, O., Qin, C., Strauss, K., and Lymberopoulos, D. (2012) 'Progressive Authentication: Deciding When to Authenticate on Mobile Phones', in Proceedings of the 21st USENIX Conference on Security Symposium, USENIX Association, Berkeley, CA,pp.301-316.

[19] Li, F., Clarke, N., Papadaki, M., and Dowland, P. (2014) 'Active Authentication for Mobile Devices Utilising Behaviour Profiling', International Journal of Information Security 13 (3), pp. 229-244.

[20] Clarke, N., Karatzouni, S., and Furnell, S. (2009) 'Flexible and Transparent User Authentication for Mobile Devices', IFIP Advances in Information and Communication Technology 297, pp. 1-12.

[21] Saevanee, H., Clarke, N., Furnell, S., and Biscione, V. (2014) 'Text-Based Active Authentication for Mobile Devices', in ICT Systems Security and Privacy Protection, Springer, Berlin Heidelberg, pp. 99-112.

[22] Fridman, L., Weber, S., Greenstadt, R., and Kam, M. (2015) 'Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location', in arXiv Preprint Archive, pp. 1-10.

[23] Hocking, C., Furnell, S., Clarke, N., and Reynolds, P. (2011) 'Authentication Aura - A Distributed Approach to User Authentication', Journal of Information Assurance and Security 6(2), 149-156.

[24] Al Abdulwahid, A., Clarke, N., Furnell, S., and Stengel, I. (2013) 'A Conceptual Model for Federated Authentication in the Cloud', in Proceedings of the 11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, pp.1–11.

[25] Clarke, N., Karatzouni, S., and Furnell, S. (2010) 'Towards a Flexible, Multi-Level Security Framework for Mobile Devices', in Proceedings of the 10th Security Conference, Las Vegas, USA, 4-6 May 2011.

[26] Furnell, S., Gaunt, P., Pangalos, G., Sanders, P., and Warren, M. (1994) 'A Generic Methodology for Health Care Data Security', Medical Informatics 19 (3), pp. 229-445.

[27] Nielsen (2014) 'Smartphones: So Many Apps, So Much Time';
http://www.nielsen.com/us/en/insights/news/2014/smartphones-so-many-apps--so-much-time.html (9 November 2015).

[28] Zevin, S. (2009) Standards for Security Categorization of Federal Information and Information Systems, DIANE Publishing.

