A Systematic Literature Review of Behavioural Profiling for Smartphone Security: Challenges and Open Problems

Saud Alotaibi[1], Abdulrahman Alruban[1,2]

[1]*Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK*
[2]*Computer Sciences and Information Technology College, Majmaah University, Al Majma'ah, Saudi Arabia*

Abstract

Smartphones contain different types of data and applications, such as images, text messages, emails, and mobile banking applications, and may also hold personal and health information. Current authentication approaches do not re-authenticate in order to re-validate the user's identity after the user has initially accessed the mobile phone. Consequently, there is a security benefit if authentication could be applied continuously and transparently (i.e., without obstructing the user's activities) to authenticate legitimate users and be maintained beyond the point of entry. Behavioural profiling is an example of behavioural biometric authentication. The main aim of this research study is to conduct a systematic review of the current research literature regarding behavioural profiling for smartphone security. The paper demonstrates that there is a lack of investigation into behavioural profiling for mobile devices. The study also examines possible challenges in behavioural profiling authentication and points to some of the open problems which need to be tackled.

1. Introduction

User authentication is a vital concept in achieving a high level of security in an IT system to protect it from unauthorised actions. User authentication has been defined as "the process of verifying the validity of a claimed user" [1]. In order to grant access to a certain system, user authentication is the first phase of a control process that decides whether this access is allowed. Traditionally, authentication mechanisms could be implemented by utilising one or more of the three following approaches [2]:

1. Something you know, such as a password, PIN, or answer to a cognitive challenge question. This is known as secret-knowledge-based authentication.

2. Something you have, such as a smart/ATM card, RFID (radio-frequency identification) chip, or a key fob or hardware/software OTP (one-time password) token. This is known as token-based authentication.

3. Something you are, which involves biometrics, including physiological, such as fingerprint, iris and retina scans and facial recognition, and behavioural characteristics (referred to as something you do) - for instance, typing, voice, and device use patterns.

Although physiological biometrics can be more difficult to mimic or forge compared with secrete knowledge or tokens, it is computationally more difficult to process [7] and can require more hardware than other methods, whereas behavioural biometrics often does not. Therefore, combining multiple authentication methods, a process known as 'multi-factor authentication', tends to provide a better authentication mechanism and thereby enhance system security, but can complicate the process of authentication. It is commonly acknowledged that behavioural biometrics authentication is a reliable solution to authenticating users using convenient and trusted methods [8, 9]. As secret knowledge is easy to guess and share, this type of verification can be combined with token-based authentication to increase the security provided. This is known as 'two-factor authentication'.

The use of mobile devices in our daily lives has grown steadily. Our mobile devices contain sensitive data, such as text messages, images, 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 are considered sensitive processes. In this context, some active applications are considered sensitive and confidential, and the risks are high in the event of sensitive data loss as a result of privacy breaches [3, 4]. Thus,

authentication is vital in securing sensitive data because, after the point-of-entry authentication stage at the beginning of a session that uses a PIN or password, the user of the device can perform almost any task [5]. As a consequence, there is no single level of risk associated with a given application; the risk level should, instead, change during use [6].

Most behavioural biometrics authentication systems are capable of providing a wide range of transparent authentication approaches to achieve a high level of balance between usability and security [10]. A transparent and continuous authentication mechanism, behavioural biometrics provides a basis for convenient and secure re-authentication of the user and gathers user data in the background, without requiring any dedicated activity [5], by regularly and periodically checking user behaviour for continuous monitoring of the protection of the smartphone [10,11] as shown in Figure 1. In this context, behavioural biometrics is often presented as a suitable authentication method and is, indeed, commonly used for transparent and continuous authentication while ensuring usability [5, 8]. In addition, security and usability can be increased by using transparent authentication, due to mobile devices having a large source of data in terms of user behaviour [10, 12]. In this context, transparent authentication systems (TAS) can be described as implicit, passive, non-intrusive, unobtrusive, unobservable, active, and silent.

The remainder of this paper is organized as follows. Section 2 presents the current state of knowledge on systems and mobile authentication mechanisms. A detailed explanation of the research methodology for this systematic literature review is given in section 3 and section 4 presents the results and discussion. Section 5 discusses existing research solutions in detail and highlights open issues. Finally, section 6 highlights the conclusions of this paper.

2. Biometric systems

Biometrics is defined by the International Biometrics Group [13] as "The automated use of physiological or behavioural characteristics to determine or verify identity". Biometric systems are used for two purposes [14]:

1. ***Verification*:** in which the system matches the captured biometric characteristics of the claimed person with the stored template of that person held in the database. The verification process checks whether the newly acquired sample matches the original sample template by performing a one-to-one comparison. The system then either rejects or accepts the submitted claim of identity. The verification process will answer the following question: does this identity belong to you?

2. ***Identification*:** in this mode, the system detects the user by capturing a sample from the user and matching it against all the biometric reference templates stored in the database of registered users. In the identification process, the user has no need to claim an identity and the system performs a one-to-many comparison. Ultimately, this system is looking to find an identity, rather than verify a claimed identity. The identification process will answer the following question: whose identity is this?

Jain et al. [15] recommended that biometric characteristics should meet the following criteria in order to be utilized for an authentication system:

•***Universality*:** Every user should have the characteristic being used as a biometric. For example, the user needs to have fingers for the fingerprint technique to be used as a biometric identifier.

•***Uniqueness*:** The selected characteristics of the biometric should be sufficiently different in order to discriminate between them.

•***Permanence*:** the biometric characteristic should not change over time; for instance, the fingerprint of a person tends not to change, whereas the way a person types tends to. As a result, "the more frequent changing of a biometric, the more the need to update the biometrics template and therefore the higher the cost of maintenance" [10].

•***Collectability*:** The biometric samples should be easy to capture, such as a face image by using a normal camera or capturing voice samples during a phone call. In contrast, the user has to position the eye to a special infrared camera for a much longer time to obtain an iris image, a method that is considered intrusive.

•***Performance*:** The proposed system should meet the requirements of accuracy, speed of matching, robustness and scalability of technologies.

•***Acceptability*:** This refers to the degree to which users prefer and will accept the use of biometrics as an authentication scheme in their lives, such as a fingerprint scan when compared with an iris scan.

•***Circumvention*:** This means that the system should be adequately robust and stand up against various techniques, such as sample forgery. For instance, an iris scan is almost impossible to imitate. Moreover, although a fingerprint scan can be fooled using an artificial finger, it is difficult to trick a facial thermograph-based authentication system with a replicated face, as the system has the ability to detect whether the face is alive.

Biometric authentication systems can be divided into two types: physiological and behavioural. Physiological biometric methods use the characteristics of a human body part to distinguish an individual based upon specific physical

characteristics, such as face, fingerprint, or iris. These physical features are more likely to stay constant over time and in different conditions. Furthermore, physiological biometrics naturally contain high levels of discriminative information and hence high levels of recognition performance. In comparison, behavioural biometrics refers to something the user does, such as typing, gait, application usage, voice, or signature [16]. Human behaviour is likely to change over time for several reasons, such as aging, fitness, mood, and weather conditions; this might, therefore, result in lower performance rates than physiological biometrics. However, this effect can be minimized if the reference template is regularly updated. To collect behavioural-based data, there is no need for special hardware and it can thus be cost effective. As a result, behavioural-based techniques are less unique but more flexible and convenient [10]. Behavioural-based approaches also perform better in verification mode than they do in identification mode. Behavioural biometrics rely on a user's distinctive behaviour, such as typing, gait, touch screen interaction patterns, device use patterns and voice. In this context, there is no need to use a device to collect user data.

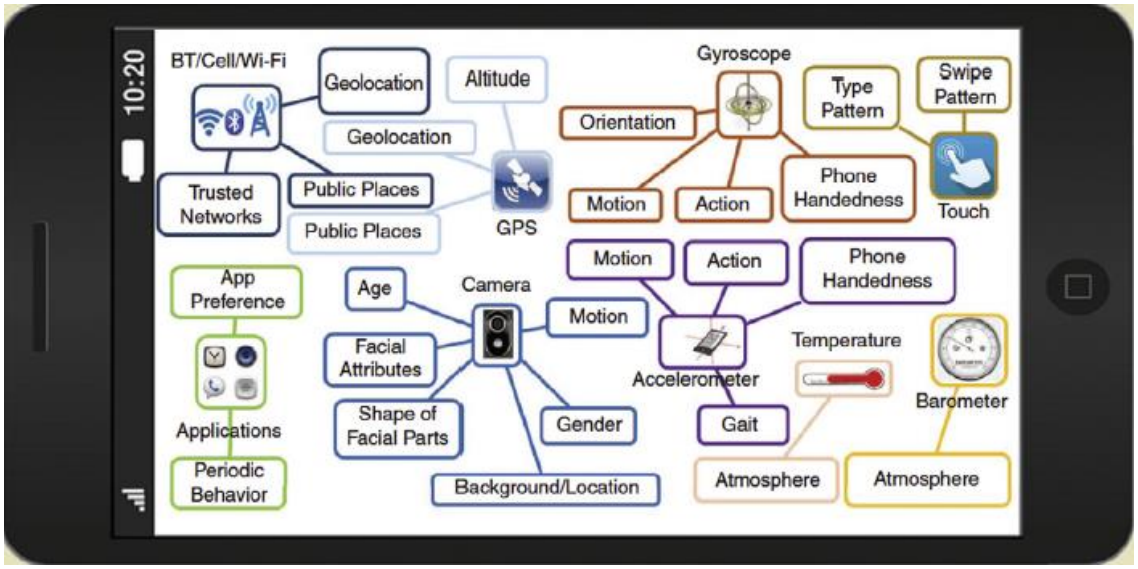

Figure 1. Physiological and behavioural biometrics for mobile devices [17]

The performance of a typical biometrics technique is measured by comparing the biometric sample of the current user with the existing reference template. The means of measurement are the ***false acceptance rate*** (FAR), ***false rejection rate*** (FRR) and ***equal error rate*** (EER), as shown in Figure 2.

•FAR refers to the percentage of access attempts by imposters that have been accepted by the system (incorrectly accepted). These are also called Type I errors or false positives (sometimes referred to as the impostor pass rate). In this context, high FAR values are often seen as a significant problem because they represent an intrusion into a protected system.

•FRR refers to the percentage of access attempts by legitimate users that have been rejected by the system (incorrectly rejected). These are also called Type II errors or false negatives (sometimes referred to as the false alarm rate). Generally, a low FAR indicates that the system is secure and a low FRR means the system is usable. The point at which the FAR and FRR are equal is called the EER, which means that a system is accurate. To be more accurate and perform better, a system needs a low EER.

In addition there are some other metrics such as:

•***True acceptance rate*** (TAR): the rate at which the system correctly verifies the claimed individual.

•***True rejection rate*** (TRR): the rate at which the system correctly rejects a false claim.

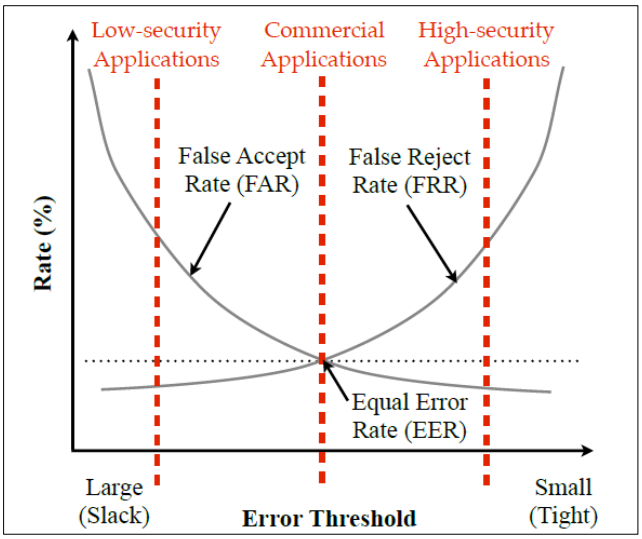

Figure 2: Biometrics performance metrics factors [7]

A confusion matrix is used to evaluate classifier performance, by collecting statistical information about the correctly and incorrectly classified samples [18].Two variables are used to understand and measure relevance [19]: precision and recall (see Figure 3). Precision refers to the fraction of relevant instances among the retrieved instances, whereas recall refers to the fraction of relevant instances that have been retrieved among the total amount of relevant instances [20]. Precision is referred to as the positive predictive value and recall as the true positive rate and sensitivity [19].

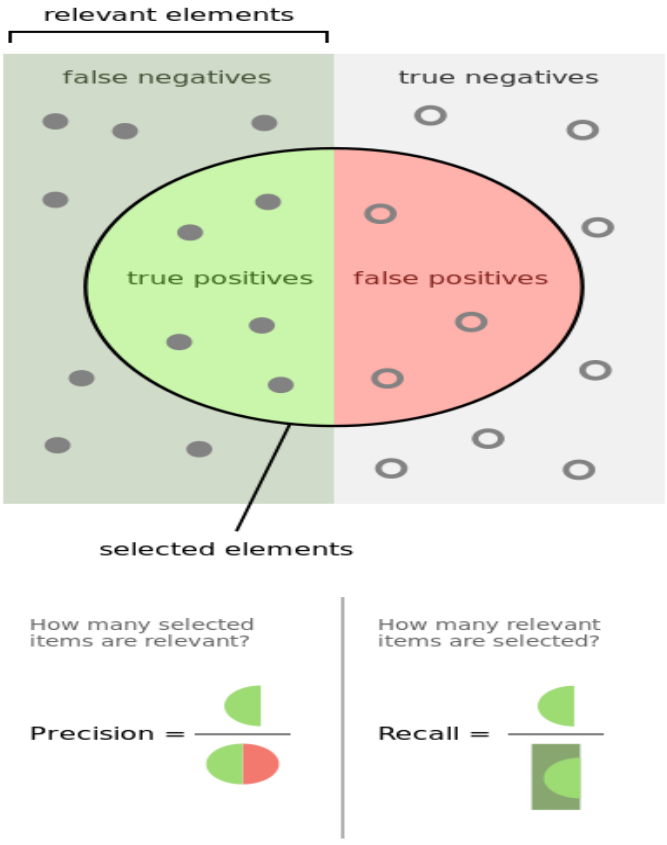

Figure 3. Precision and recall metrics [20]

3. Research methodology

Behavioural profiling (service utilization) attempts to identify and discriminate users based upon the way they interact with applications and/or services [10]; specifically, which applications they access, at what time of day, and for how long (see Figure 4). However, this technique is not expected to be unique and distinct enough to use for an identification system. It also suffers from privacy issues during behaviour monitoring, which affects the level of user acceptance.

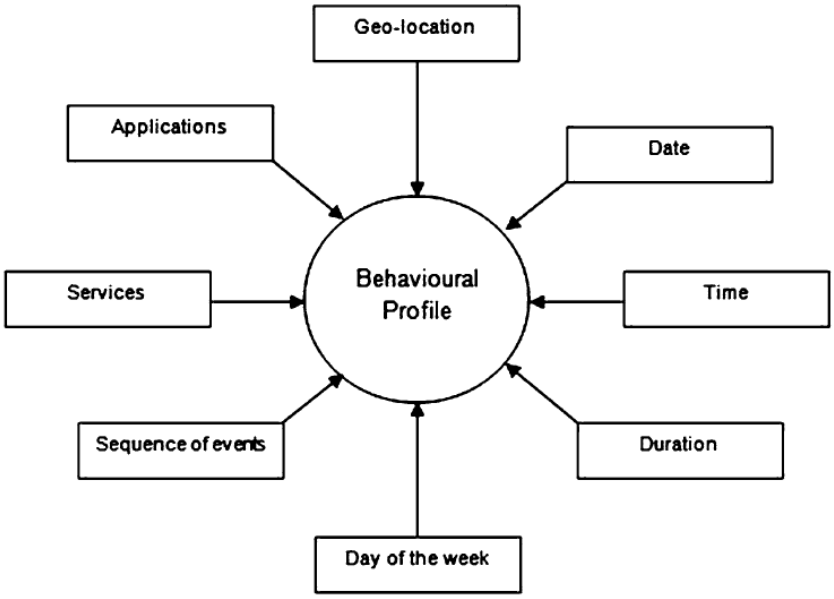

Figure 4. Attributes of behavioural profiling [10]

In this research paper, a systematic literature review [21] of transparent authentication for mobile devices is conducted to identify articles and papers that discuss this subject. In this review, the main research question is how to authenticate the mobile user in the background without the user being interrupted, in a transparent manner based on application or service usage. This systematic literature review is divided into two phases. In the first phase, a collection of papers is identified and analyzed based on their keywords and synonyms that relate to the review research question. The second phase provides a systematic overview of the methodology generated by all significant approaches published from 2008 to 2018.

To this end, all the search terms and keywords and their synonyms were identified and a search conducted that utilized Google Scholar's "all-in-one" search expression. By compiling using AND and OR, the following query was created to search titles, keywords and abstracts:

"allintitle: smartphones **OR** smart phones **OR** smartphone **OR** smart phone **OR** Mobile phones **OR** Mobile phone **OR** Mobile Devices **OR** Mobile Device **AND** Behaviour+Profiling **OR** behavioural+profiling **OR** behavioural **OR** Behaviour **OR** User+profiling"

To identify the most relevant papers for this search, the following filters were used:

- The paper must be on a behaviour profiling method.
- The paper focuses on smartphones.
- The paper is published between 2008 and 2018.
- The paper must be in English.

Different sources were used to conduct the systematic literature review: ACM, IEEE, Springer, ScienceDirect, and Google Scholar. Table 1 shows the final search results detailing the number of papers found in each database.

Table 1. Papers found in each database

Library	**Total *(papers)***
ACM	2
IEEE Xplore	3
SpringerLink	1
Google Scholar	3
Total	9

4. Results

Studies have proposed application usage aimed at providing transparent authentication. For example, Hayashi et al. [22] argue that device-centric continuous authentication cannot discriminate among data from different applications, meaning that they cannot make any inferences about the importance of the application currently being used. More specifically, the drawback of a device-centric approach, which is unaware of the task that the user is performing within an application, is that it can lead to a failure to deliver authentication control at the task level [23]. This leads to a higher authentication overhead.

Hayashi et al. [22] argue that an all-or-nothing access model is inefficient and suggest that a mobile user should be authenticated only when a sensitive application is started, since most applications do not require explicit authentication. In the context of a sensitive application concept, the authors created paper prototypes (i.e., a theoretical method) of two alternative access mechanisms: group accounts and an activity lock. The group account would provide access to some of the functionality that is normally available only when the phone is unlocked and is for sharing non-sensitive information or applications. Whereas, an activity lock can be activated by the device owner before handing the device to another user to share specific screens in an application. Configuring a group account on a device enables the device owner to share a specific set of applications with other users.

In the same context, the work of Riva et al. [24] is based on when the user should authenticate (as opposed to how) and for which applications. The authentication decision depends on the confidence and sensitivity levels of each application, which are provided by the user to protect sensitive applications from unauthorised use. The result of their prototype was a 42% reduction in requested explicit authentication, although this was conducted with only nine users. A similar but more extensive study was conducted on positive habits (i.e., familiar events) and negative habits (i.e., unfamiliar locations). Shi et al. [25] recorded a user's routine, such as location, phone calls, and application usage, in order to build a profile and assign a positive or negative score to each user's routine.

Among further studies in a similar context, Li et al. [26] introduce a behaviour profiling approach to identify mobile device misuse by focusing on the mobile user's application usage: general application usage, voice calls, and text messaging. The total EER was 7.03%. Later, these authors (Li et al., [27]) present a novel behaviour profiling framework, which is able to collect user behaviour to evaluate the system security status of the device continuously before sensitive services are accessed.

They investigate the sensitivity of the application concept, which is mapped using high-risk levels to render the framework more secure and transparent when the user requires access to high-value applications. This means that the system will reject user access after several attempts at using different applications, rather than an attempt to access a single application use. The authors conclude that the framework seems to distinguish mobile users through their application usage; in particular, by focusing on the names of applications and the location of usage. However, the main limitation is that the MIT Reality dataset used was created in 2004 with a small number of mobile applications, which creates difficulty in discriminating between users.

Saevanee et al. [34] examine the combination of three diverse biometric methods: keystroke dynamics, behavioural profiling and linguistic profiling. By employing this multimodality, they achieved a total EER of 3.3% from 30 virtual users (the dataset was not real, however, and was gathered from different datasets). To continue their work, Saevanee et al. [35] present a text-based authentication framework utilising the same modalities and introduce a security feature by allowing the user to set security levels for access to different applications. The researchers claim that this approach would reduce the number of intrusive authentication requests for high security applications by 91%.

Table 2. Systematic literature review results

Study	# of Subjects	Dataset	Features	Classification	Performance (%)
[22]	20, interview for 90 minutes.	structured interviews	-	-	-
[25]	50 for 12 days	-	SMS, Calls, Browser History, Location	-	-
[27]	22–76	MIT Reality	app name, Tel. number, cell, location, call (duration, time)	Neural Network	FRR:11.45, FAR:4.17
[28]	7,35,100	GCU,RiceLivelab, MIT Reality	Wi-Fi, CPU load, light, noise, magnetic field and rotation		-
[29]	NA	Private	app usage, time, location, HDI, bandwidth	Bayesian	NA
[30]	37–76	MIT Reality	GPS location, WIFI, Bluetooth	Developed model	Precision:85, Recall:91
[31]	200 for 30 days	-	Text(n-grams), application usage, Wi-Fi, and location.	Maximum likelihood and SVM with a RBF kernel.	1% - 5% EER
[32]	30	4different datasets	-	-	-
[33]	76	11 Applications	Time of usage, application name, action with each application	SVM,GB,KNN	26% (GB)

Fridman et al. [31] propose a 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). To evaluate this framework, the authors collected a dataset from 200 users' Android mobile devices for 30 days, which is considered a large dataset in the transparent authentication literature. After one minute of the user using the device, the ERR was 5%, whereas after 30 minutes the EER was 1%. Despite this work's promising results, battery consumption was the main issue. More recently, Alotaibi et al. [33] proposed a novel behaviour profiling approach for mobile security in a study involving data collected from 76 users using 11 mobile applications over a one-month period. The proposed approach was examined by utilising three classifiers: a support vector machine (SVM), a random forest (RF), and gradient boosting (GB). The findings show that the gradient boosting classifier achieved good results compared with the other classifiers, with an average EER of 26.98%. This suggests that this approach could allow mobile users to be discriminated based on behavioural profiling when they interact with and utilise mobile applications.

5. Challenges

With the rapid growth of smartphones for use in daily life, securing the sensitive data stored upon them makes authentication of paramount importance. In particular, smartphones are used to perform activities which are considered sensitive and confidential, and the risks are high in the event of privacy breaches and the loss of sensitive data. After the point of entry, the user of the device can, by using techniques such as a PIN or password, perform almost all tasks with different risk levels without having to re-authenticate periodically to re-validate their identity. Current point-of-entry authentication mechanisms also consider all applications on a mobile device to have the same level of importance and do not apply any further access control rules.

Although a number of studies have investigated the feasibility of using behavioural biometrics to secure a mobile device [15], there is a lack of investigation of behavioural profiling, as shown in Table 2. Although the introduction of such a system has the basis for solving the authentication problem in a secure and usable way, it also raises a number of further issues that need to be considered and solved in order for the system to operate effectively. This section highlights several of these issues in order for them to be taken into account during the development stage. First, although a large number of datasets exists for physiological traits, there is a lack of standard datasets regarding behavioural profiling needed in order to test and validate a proposed approach [36, 37].

Second, there is also the matter of privacy. First and foremost, will users allow the activity on their mobile phone to be monitored, such as sending emails or writing messages, since these data are considered personal and sensitive? One interesting development in this area has been Apple's introduction of a new feature to manage usage on iOS 12 (Screen Time) [37]. The main aim of this new feature is to provide management tools for customers to control how they spend time with apps and websites, by creating daily and weekly activity reports as shown in Figure 5. Screen Time for iOS 12 might also present an opportunity for parents/guardians to better understand and manage a child's device usage.

Third, based on seven biometric characteristics, behavioural profiling has been scored high in terms of universality and collectability, medium for acceptability, but low for uniqueness, performance, and permanence [10, 39]. Although the main advantage of a behaviour profiling authentication approach is its ability to produce continuous and transparent authentication by periodically checking user behaviour [39], data inconsistently considered a major weakness [36,37]. In addition, Energy Consumption [12] such as usage of CPU, memory and battery.

Figure 5. Screen Time for Apple – iOS 12[38]

6. Conclusion

With the growth of smartphones for use in our daily life, securing the sensitive data stored upon these devices makes authentication of paramount importance. In particular, smartphones are used to perform activities which are considered sensitive and confidential, and the risks are high in the event of privacy breaches and the loss of sensitive data. In addition, after the point of entry, using techniques such as a PIN or password, the user of the device can perform almost all tasks with different risk levels without periodically having to re-authenticate to re-validate their identity. The current point-of-entry authentication mechanisms also consider all applications on a mobile device to have the same level of importance and thereby do not apply any further access control rules. Consequently, there is a security benefit if authentication could be applied continuously and transparently (i.e., without obstructing the user's activities) to authenticate legitimate users and be maintained beyond the point of entry. This research study produced a systematic review of the research literature regarding behavioural profiling for smartphone security published over the last 10 years and suggests that there is a lack of research on behavioural profiling for mobile devices. Finally, the open problems for behavioural profiling authentication were highlighted in order for them to be addressed.

7. References

[1] L. O'Gorman, Comparing Passwords, Tokens, and Biometrics for User Authentication, Proceedings of the IEEE, vol. 91, no. 12, pp. 2019-2040, 2003.

[2] H. Wood, The Use of Passwords for Controlling Access to Remote Computer Systems and Services', Proceedings of American Federation of Information Processing Societies: 1977 National Computer Conference (AFIPS 77), Dallas, Texas, USA, 13-16 June 1977, pp. 27-33, 1977.

[3] K. Tam, S., Khan, A., Fattori, A. & L. Cavallaro, Copper Droid: Automatic Reconstruction of Android Malware Behaviours. In Proceedings of the 22nd Annual Network and Distributed System Security Symposium (NDSS'15), pp.1-15. 2015.

[4] S. Alotaibi, S. Furnell, and N. Clarke," MORI: An Innovative Mobile Applications Data Risk Assessment Model". In Journal of Internet Technology and Secured Transactions (JITST), Volume 5, Issues 3/4. 2016.

[5] N. Clarke, S, Karatzouni, and S. Furnell, "Flexible and transparent user authentication for mobile devices". IFIP Advances in Information and Communication Technology, 297/2009, pp.1-12. 2009.

[6] S. Alotaibi, S. Furnell, and N. Clarke, "A novel Taxonomy for mobile applications data". Int. J. Cyber-Security Digit. Forensics, 5 (3), 115-121. 2016.

[7] H. Crawford, K., Renaud, K., & T. Storer, A framework for continuous, transparent mobile device authentication. Computers & Security, 39, 127-136. 2013.

[8] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: reviewing the state of the art". Cluster Computing, 19(1), 455-474. 2016.

[9] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent Two-Factor Authentication". In IEEE Access, 6, pp.3267732686. DOI: 10.1109/ ACCESS.2018.2844548, 2018.

[10]N. Clarke," Transparent user authentication: biometrics, RFID and behavioural profiling". Springer Science and Business Media. 2011.

[11] S. Alotaibi, S. Furnell, and N. Clarke, "Transparent authentication systems for mobile device security: A review". In the 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 406-413). IEEE. 2015.

[12] A. Alzubaidi, & Kalita, J. Authentication of smartphone users using behavioral biometrics. IEEE Communications Surveys & Tutorials, 18(3), 1998-2026. 2016.

[13] IBG, How is biometric defined? International Biometric Group, http://www.biometricgroup.com/ reports/biome tric_definition.html [Accessed 7 May 2015]. 2010.

[14] A. Jain, P. Flynn, and A. Ross, Handbook of Biometrics, New York, Springer, 2007.

[15] A. Jain, A. Ross, and S. Prabhakar, S., An introduction to biometric recognition, Circuits and Systems for Video Technology, IEEE Transactions on Circuits and Systems for Video Technology , vol.14, no.1, pp. 4-20, 2004.

[16] J. Woodward, N. Orlans, N., and Higgins "Identity Assurance in the Information Age". McGraw-Hill/ Osborne, Berkeley, California. 2003.

[17] M., Patel, R. Chellappa, R., Chandra, D., & Barbello, B. Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), 49-61. 2016.

[18] K. Andrea, G. Shevlyakov, G., Vassilieva, N., and Ulanov, A. "A new measure of outlier detection performance". In International Workshop on Machine Learning and Data Mining in Pattern Recognition (pp. 190-197). Springer, Cham. 2014.

[19] Fawcett, T. An introduction to ROC analysis. Pattern recognition letters, 27(8), 861-874. 2006.

[20] Precision and recall: available on: https:// en.wikipedia.org/wiki/Precision_and_recall

[21] Alharbi, S., Weber-Jahnke, J. and Traore, I., August. The proactive and reactive digital forensics investigation process: A systematic literature review. In International Conference on Information Security and Assurance (pp. 87-100). Springer, Berlin, Heidelberg. 2011.

[22] E. Hayashi, O. Riva, K. Strauss, A., Brush, & Schechter, S. Goldilocks and the two mobile devices: going beyond all-or-nothing access to adevice's applications. In Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM.2012.

[23]De Luca, A., Hang A., Brudy, F., Lindner C., & Hussmann, Touch me once and I know it's you!Implicit authentication based on touch screen patterns, in ACM CHI, pp.987–996. H., 2012.

[24] O. Riva, C., Qin, K., Strauss, K, K., & Lymberopoulos, D. Progressive authentication:Deciding when to authenticate on mobile phones. In Proceedings of the 21st USENIX Conference on Security Symposium, ser. Security'12. Berkeley,CA, USA: USENIX Association. 2012.

[25] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y.Xiong, "Sen Guard: passive user identification onsmartphones using multiple sensors." 2011 IEEE 7thInternational Conference on Wireless and MobileComputing, Networking and Communications(WiMob), Shanghai, China. Pp.141- 148, 2011.

[26] F. Li, N. L. Clarke, M. Papadaki, and P.Dowland, “Misuse detection for mobile devicesusing behaviour profiling,” International Journal ofCyber Warfare and Terrorism (IJCWT), 1(1), pp.41-53.IJCWT, vol. 1,, no. 1, pp.41–53, 2011.

[27] F. Li, N. Clarke, M. Papadaki, and P. Dowland,“Active authentication for mobile devices utilisingbehaviour profiling. International journal ofinformation security, 13(3), pp.229-244, 2014.

[28] Kayacik, H., Just, M., Baillie, L., Aspinall, D.,& Micallef, N., Data driven authentication: On theeffectiveness of user behaviour modelling withmobile device sensors, in Proceedings of theMobile Security Technologies Workshop. 2014.

[29] Bassu D, Cochinwala M, Jain A. A new mobilebiometric based upon usage context. In:Technologies for homeland security (HST), IEEEinternational conference on. IEEE; 2013. p. 441–6.2013

[30] Gupta A, Miettinen M, Asokan N, Nagy M.Intuitive security policy configuration in mobiledevices using context profiling. In: Privacy,security, risk and trust (PASSAT), 2012international conference on and international con-fennec on social computing (SocialCom). IEEE; 2012. p. 471–80. 2012.

[31] Fridman, L., Weber, S., Greenstadt, R., andKam, M., Active authentication on mobile devicesvia stylometry, application usage, web browsing,and GPS Location. In arXiv preprint arXiv, pp.1–10.2015.

[32] H. Khan and U. Hengartner, “Towardsapplication-centric implicit authentication onsmartphones,” in ACM HotMobile, 2014.

[33] S. Alotaibi, S. Furnell, and N. Clarke, “A NovelTransparent User Authentication Approach forMobile Applications. (Under review).

[34] H. Saevanee, N.L. Clarke, and S.M. Furnell,“Multi-modal behavioural biometric authenticationfor mobile devices,” In Proc. IFIP InformationSecurity and Privacy Conference (SEC), pp.465-474, 2012.

[35] H. Saevanee, N. Clarke, S. Furnell, and V.Biscione, “Text-based active authentication formobile devices”. In ICT Systems Security andPrivacy Protection. Berlin Heidelberg: Springer,pp.99-112. 2014.

[36] Neal, T. J., & Woodard, D. L. Surveyingbiometric authentication for mobile device security.Journal of Pattern Recognition Research, 1, 74-110.2016.

[37] Mahfouz, A., Mahmoud, T. M., & Eldin, A. S.A survey on behavioral biometric authentication onsmartphones. Journal of Information Security andApplications, 37, 28-37. 2017.

[38] Apple, 2018: iOS 12 introduces new features to reduce interruptions and manage Screen Time, https://www.apple.com/newsroom/2018/06/ios-12-introduces-new-features-to-reduce-interruptions-and-manage-screen-time/ available on June 4, 2018.

[39] W. Meng, D.S. Wong, S. Furnell, and J. Zhou,“Surveying the development of biometric userauthentication on mobile phones,” IEEECommunications Surveys & Tutorials, 2015.

