A Novel Behaviour Profiling Approach to Continuous Authentication for Mobile Applications

Saud Alotaibi[1], Abdulrahman Alruban[1,2], Steven Furnell[1,3,4] and Nathan Clarke[1,3]
[1]*Centre for Security, Communications and Network Research, Plymouth University, Plymouth, U.K*
[2]*Computer Sciences and Information Technology College, Majmaah University, Al Majma'ah, Saudi Arabia*
[3]*Security Research Institute, Edith Cowan University, Perth,Western Australia*
[4]*Centre for Research in Information and Cyber Security, Nelson Mandela University, Port Elizabeth, South Africa*

Keywords: Transparent Authentication, Behaviour Profiling, Mobile Applications, Mobile Security, Usable Security Biometric Authentication, Smartphones, Tablets.

Abstract: The growth in smartphone usage has led to increased user concerns regarding privacy and security. Smartphones contain sensitive information, such as personal data, images, and emails, and can be used to perform various types of activity, such as transferring money via mobile Internet banking, making calls and sending emails. As a consequence, concerns regarding smartphone security have been expressed and there is a need to devise new solutions to enhance the security of mobile applications, especially after initial access to a mobile device. This paper presents a novel behavioural profiling approach to user identity verification as part of mobile application security. A study involving data collected from 76 users over a 1-month period was conducted, generating over 3 million actions based on users' interactions with their smartphone. The study examines a novel user interaction approach based on supervised machine learning algorithms, thereby enabling a more reliable identity verification method. The experimental results show that users could be distinguished via their behavioural profiling upon each action within the application, with an average equal error rate of 26.98% and the gradient boosting classifier results prove quite compelling. Based on these findings, this approach is able to provide robust, continuous and transparent authentication.

1 INTRODUCTION

Smartphones have evolved and become a necessity in our everyday life; we use them to contact each other, transfer money, and to store sensitive information (Saevanee et al. 2014). Since smartphones contain high-risk applications and sensitive data, such as personal and financial information, suitably robust security is needed on mobile devices and this makes authentication of paramount importance. Currently, a user can perform almost all tasks without having to re-authenticate or re-validate after point-of-entry authentication. This presents additional demands in terms of usability and security (Clarke, 2011; Alotaibi et al. 2016).

It is commonly acknowledged that biometric authentication is a reliable solution to authenticating users using convenient and trusted methods (Clarke et al., 2009, 2016; Zhang et al., 2018). Most biometric authentication systems are capable of providing a wide range of transparent authentication approaches to achieve a high level of balance between usability and security (Alotaibi et al. 2015). In this context, behavioural biometrics is often presented as a suitable authentication method and, indeed, is commonly used for transparent and continuous authentication while ensuring usability (Clarke, 2011; Hatin et al., 2017). One type of behavioural biometric is behaviour profiling. The main aim in this case is the transparent verification of mobile users based on the way they interact with the required service whilst using their smartphone (Clarke, 2011; Meng et al., 2015). This approach compares the current user's activities with a historical profile of usage that is built utilising a machine learning method (Mahfouz et al., 2017).

This research study considers the use of a be-

Alotaibi, S., Alruban, A., Furnell, S. and Clarke, N.
A Novel Behaviour Profiling Approach to Continuous Authentication for Mobile Applications.
DOI: 10.5220/0007313302460251
In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, pages 246-251
ISBN: 978-989-758-359-9

haviour profiling approach to authenticate legitimate users and detect imposters in a continuous and transparent manner, which is maintained beyond point of entry, without the explicit involvement of the user. Although several studies exploring a behaviour profiling approach to smartphone use have been conducted, many have been conducted with relatively small trial groups and in artificial conditions. This study involves a sizeable population of users, with data collection during genuine day-to-day usage." In this study, a total of 3,015,339 actions were accumulated (with an average of 22,457 actions per day). In this dataset, the long total usage day was 1230 days and 35 was the short total usage day. The study also employed four types of classifier to assess the performance of the system.

The next section presents related work and the state of the art of smartphone behaviour profiling biometrics. This is followed by an outline of a novel behaviour profiling approach to smartphone security, including the data collection phase, experimental methodology, and the feature extraction process in section 3. Section 4 presents the experimental results and section 5 concludes the paper.

2 RELATED WORK

Although a limited number of studies have focused on behavioural profiling-based authentication for mobile devices, some investigative efforts have been made in the literature to introduce behavioural profiling as a behavioural biometrics authentication approach to providing transparent authentication (Alotaibi et al., 2015). For instance, Li et al. (2011) introduced a behaviour profiling approach to identify mobile device misuse by focusing on the mobile user's application usage. This work used the MIT Reality Mining dataset (Eagle & Pentland, 2006). The following data were collected from 100 smartphone users for 9 months: application information (app name, date, duration of usage and cell ID), voice call data (including date, time, number called, duration, and cell ID), and text message data (date, time, number texted and cell ID) (Meng et al., 2015; Mahfouz et al., 2017). This research achieved a total equal error rate (EER) of 7.03%. Later, the authors presented a novel behaviour profiling framework that was able to collect user behaviour to evaluate the system security status of a device in a continuous manner before sensitive services were accessed (Li et al., 2014). They investigated the sensitivity of the application concept, which is mapped to high-risk levels to make the framework more secure and transparent when the user requires access to high-risk applications. The authors concluded that the approach seems able to distinguish mobile users through their application usage; in particular, by focusing on the names of applications and the location of usage, which are considered valuable features.

Among further studies in a similar context, Saevanee et al. (2012) examined the combination of three diverse biometric methods: keystroke dynamics, behavioural profiling and linguistic profiling. Using this multimodality, the researchers achieved a total EER of 3.3% from 30 virtual users (the dataset was not real and was gathered from different datasets). To continue their work, Saevanee et al. (2014) presented a text-based authentication framework utilising the above modalities and introduced a security aspect by allowing the user to set security levels for access to different applications. The researchers claimed that this approach would reduce the number of intrusive authentication requests for high-security applications by 91%.

In other recent work, Fridman et al. (2015) proposed a parallel binary decision-level fusion architecture for active authentication. The 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 through GPS (outdoors) or Wi-Fi (indoors). To evaluate the framework, the authors collected a dataset from 200 users' Android mobile devices over a period of 5 months. After 1 minute of the user using the device, the EER was 5%, whereas the EER was 1% after 30 minutes.

In the same context, Neal and Woodard (2017) introduced associative classification to authenticate mobile device users by analysing the performance of applications. Bluetooth and Wi-Fi data were collected from 189 college-level students over 19 months. Three time intervals (5, 15, and 30 min) were selected and association rules were extracted from each data type separately and combined as features. The experimental results revealed up to 91% accuracy, with application and Bluetooth data being more accurate than Wi- Fi data. Prior to that, Shi et al. (2011) recorded users' routines, such as location, phone calls, and application usage, in order to build a profile and assign a positive (e.g., good behaviour, such as a phone call to a known number) or negative score for each user's routine, using a dataset based on 50 users for a period of 12 days or more. The dataset contained SMS, phone call, browser history and location, without demonstrating the finding of this study.

3 EXPERIMENTAL METHODOLOGY

The main aim of this section is to present the methodology of a novel behavioural profiling approach to user identity verification, which is maintained beyond point of entry, without the explicit involvement of the user. In addition, this section examines the proposed approach based on supervised machine learning algorithms.

3.1 Mobile Data Collection Dataset

This experiment enlisted 100 participants at the University of Plymouth and collected app log data, such as a timestamp for the application used by the participant and the name of the user action for each application (read, send, etc.). The dataset collection was carried out from February to July 2017. Each participant engaged in the study for at least 1 month, during which time they were all simply asked to use their device as normal. For the purpose of the data collection, a code was developed to extract log files from a backup file from the participants' devices by utilising the Android Debug Bridge (ADB), which is a command line tool that allows communication between a connected Android device and a computer. The backup file was extracted and a code run on SQLite to extract a log file from the backup file extracted for each application.

During the data collection phase, applications were selected and collected. Some applications, such as Facebook, online mobile banking, and Chrome, are fully encrypted, and there was no means of collecting user data without compromising the user's privacy by asking the participant to root his/her device. For this reason, in order to protect the users' privacy, only 11 applications were collected: Phone Call, SMS, Download, YouTube, WhatsApp, Browser, Google Play, Email, Viber, Google Photo, Camera, and Yahoo mail. Consequently, the collectively applications have been offered enough of a basis for profiling enough of the users' interactions.

At the end of the data collection, the 76 users had completed the process and the analysis phase was ready to begin. Each user's data were stored in an individual text file, each record containing the following fields: the date (in two forms: human time and a timestamp e.g., 2016-06-28 20:22:30, 1467141750071), application name, action type, and extra information, such as message/email length and call duration. A total of 3,015,339 actions with total daily usage of 22,457 were accumulated. In this context, the long total usage day was 1230 days, and 35 was the short total usage day. This, in turn, means that the large dataset sample size might lead to a high degree of accuracy, which would have a positive impact on the conclusions drawn from the proposed approach.

3.2 Data Pre-Processing and Feature Extraction

The main purpose of the data pre-processing phase is to improve the quality of the data to allow for reliable statistical analysis by converting raw data that are derived from data extraction and extracting discriminative user information. More specifically, feature extraction is a crucial phase that allows the classifier to identify users based on extracting a discriminative set of features following analysis of raw data drawn from the users. The extracted feature sets for each participant are labelled and stored as a sequence of comma-separated values (CSV) files. In this research study, seven features were extracted from the data collected from the participants' interactions with their mobile device. These features were determined as they generic metadata for almost every action that the user could perform.

- Application name
- Action name
- Length of message/email
- Call duration
- Day of the week
- Hour of the day
- Time between every two consecutive user actions.

3.3 Modelling

With a dataset labelled as the input in the previous phase, machine learning was utilised to construct a model that can identify pattern similarities by training machines on the new dataset after feature extraction (Narudin et al., 2016). Using a machine learning classifier, the predictable model created is able to authenticate the mobile user based on his/her behaviour. Supervised learning methods were chosen in this experiment due to the labelled known data and known responses. Three classifiers were selected in this research study: a support vector machine (SVM), random forest (RF), and gradient boosting (GB), to identify the most efficient machine learning classifier based on the classifier output. The selections of these algorithms were made based on their popularity in solving such a problem (Narudin et al., 2016).

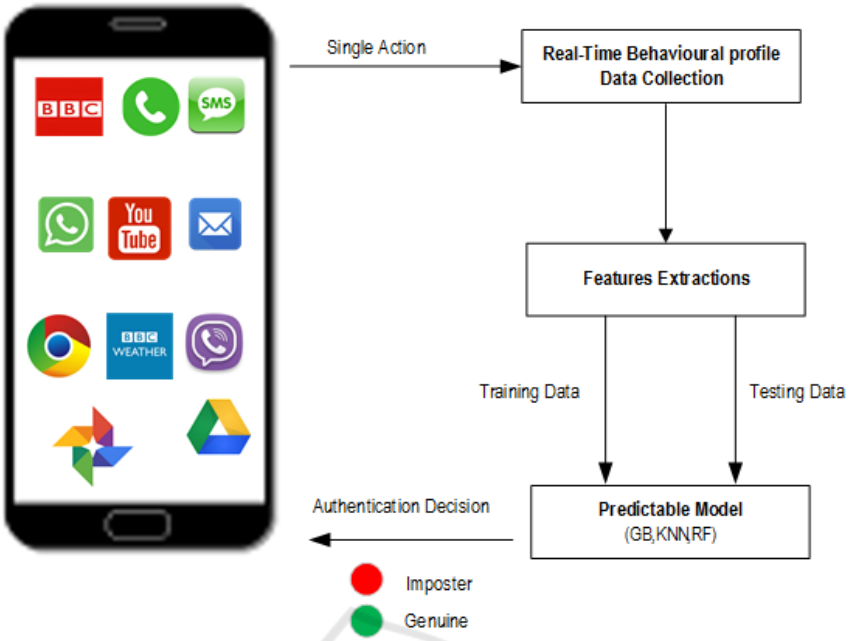

Figure 1: Block diagram of the proposed approach.

4 EXPERIMENTAL ANALYSIS AND DISCUSSION

Table 1 displays the performance results of the three selected classifiers, showing that the GB classifier, which achieved the lowest EER (26.98%), was quite successful. Given that an authentication decision was made on each user action within each application, with some actions taking less than 1 second, the experimental results are promising and thereby support the proposed idea of basing the authentication decision on historical behavioural profiling of the smartphone user. However, having transparent authentication for each user action would not be a logical approach due to some of the factors that have to be taken into account, such as the time taken to produce the authentication decision, memory space requirements, computational overheads, and the usability of the proposed system.

Table 1: Performance of the classification algorithms.

Classifier	EER (%)
GB	**26.98**
RF	28.70
KNN	30.53

Based on the performance of the classification algorithms presented in Table 1, a more detailed analysis of the GB algorithm result was undertaken. Figure 2 shows a histogram distribution of the EER for the 76 participants after applying the GB classifier and shows that only a few participants achieved a good EER result, although, on average, the EER was 26.98%. For instance, four participants (71, 44, 52, and 57) produced an EER of less than 10% (2.5, 4.4, 4.4, and 9.1, respectively). Participant 34 had the highest EER (36.01%), whereas participant 71 had the lowest (2.5%).

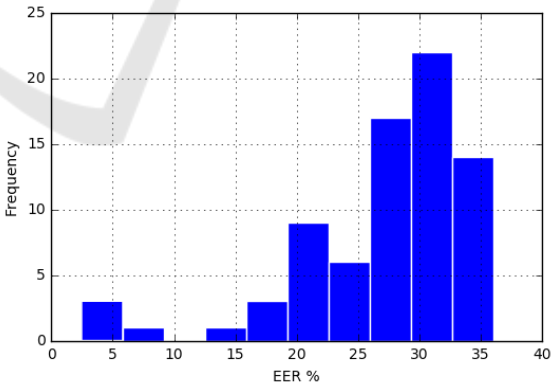

Figure 2: Histogram showing the distribution of the EER after applying the GB classifier

In order to investigate the features ranking, the feature importance approach was applied, utilising the random forest algorithm. The training set was fed into the algorithm to perform multiclass classification and then compute each feature contribution weight to use for the classification decision. The main aim of

feature importance is to quantify the importance of each of the extracted features to understand which has the most significant impact on the classification task (Hooker et al., 2018). Consequently, feature importance provides a high level of insight into a model's behaviour, which leads to improved model prediction. The feature importance technique was applied to all feature extractions for participant 71 (i.e., the user with the lowest EER), as illustrated in Figure 3, which shows the names of the features and their relative importance. It is clear from the figure that two features, application and action, were the most important (both were 41%). The third important feature, the day of the week, has a weight of 13%, while the two remaining features registered about 5% in total. This suggests that application, action and day of the week are the three most important features, forming 95% of the decision weight for participant 71.

This analysis was supported by plotting the application feature distribution of the user with the lowest EER (71), the user with the highest EER (34) and the population of the dataset, as depicted in Figure 4. It can be seen that participant 71 behaved differently from the other participants, while the behaviour of participant 34, who had the highest EER, was almost identical to the pattern for the rest of the population. This suggests that participant 71 used an almost unique application in comparison with the others. This is also consistent with the action feature type. As Figure 6 shows, the same user (71) still behaved differently in comparison with participant 34. Finally, the distribution of the hour of the day feature shows almost the same pattern.

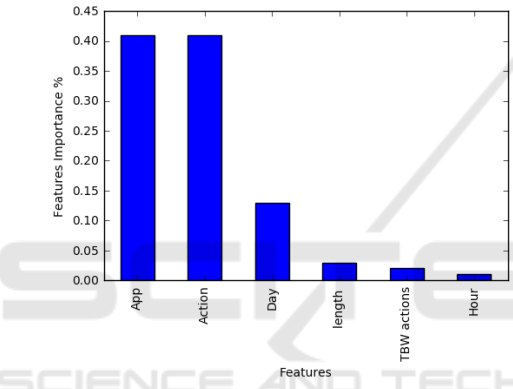

Figure 3: Features importance results.

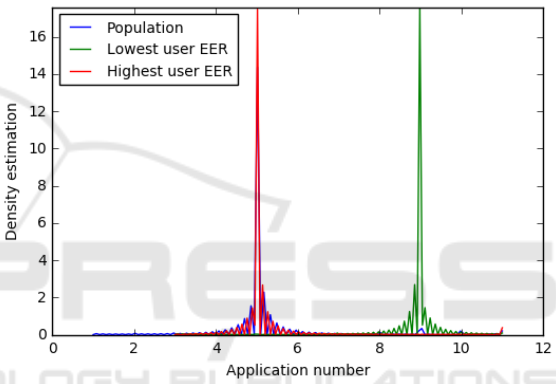

Figure 4: Application feature comparison.

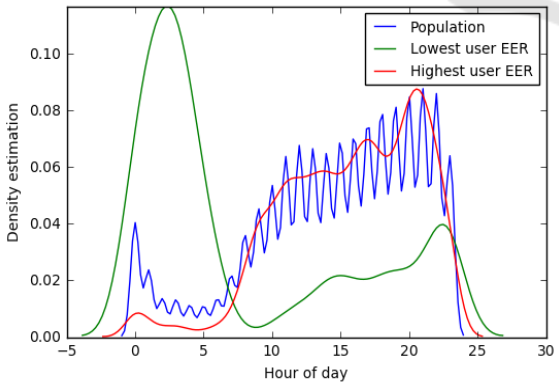

Figure 5: Hour of the day feature comparison.

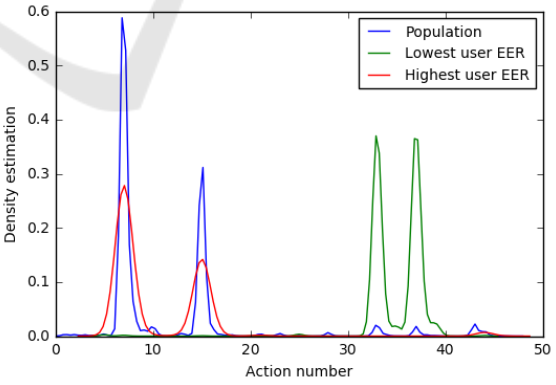

Figure 6: Action feature comparison.

4 CONCLUSIONS

This study presented a novel behavioural profiling approach to verifying the user in terms of mobile application security and providing robust user identification. In this study, three supervised machine learning algorithms were selected to evaluate the proposed approach and to determine the ideal classifier based on EER value. The experimental results show that the significance of this research lies in having successfully applied continuous user verification for mobile applications in a manner that fulfils both security and usability requirements.

Although the authentication decision is based on action resolution, the experimental results are still promising. Making an authentication decision on each user action might lead to an unusable system which does not present transparent authentication. For future work, solutions could be suggested and tested to improve the usability of the approach in relation to the security requirements. For instance, it would be beneficial to test the impact of different time windows on performing the verification process and how this affects the overall accuracy of the model.

REFERENCES

Alotaibi, S., Furnell, S. and Clarke, N. (2015). "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.

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

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

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

Clarke, N. (2011)."Transparent user authentication: biometrics, RFID and behavioural profiling". Springer Science and Business Media.

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 arXiv, pp.1–10.

Eagle, N., and Pentland, A. (2006). Reality mining: sensing complex social systems. Personal and ubiquitous computing, 10(4), 255-268.

Hatin, J., Cherrier, E., Schwartzmann, J., and Rosenberger, C. (2017)."Privacy preserving transparent mobile authentication". In International Conference on Information Systems Security and Privacy (ICISSP). pp. 354-361.

Hooker, S., Erhan, D., Kindermans, P. J., and Kim, B. (2018). "Evaluating Feature Importance Estimates". ArXiv preprint arXiv: 1806.10758.

Li, F., Clarke, N., Papadaki, M., and Dowland, P. (2011). "Misuse detection for mobile devices using behaviour profiling". IJCWT, vol. 1, no. 1, pp.41– 53.

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.

Mahfouz, A., Mahmoud, T. M., and Eldin, A. S. (2017). "A survey on behavioral biometric authentication on smartphones". Journal of Information Security and Applications, 37, 28-37.

Meng, W., Wong, D., Furnell, S., and Zhou, J. (2015)." Surveying the development of biometric user authentication on mobile phones". IEEE Communications Surveys and Tutorials (Volume: 17, Issue: 3). pp. 1268 – 1293.

Narudin, F. A., Feizollah, A., Anuar, N. B., and Gani, A. (2016). "Evaluation of machine learning classifiers for mobile malware detection". Soft Computing, 20(1), 343-357.

Neal, T. J., and Woodard, D. L. (2017). "Using associative classification to authenticate mobile device users". In Biometrics (IJCB), 2017 IEEE International Joint Conference on (pp. 71-79). IEEE.

Saevanee, H., Clarke, N., and Furnell, S. (2012). "Multi-modal behavioural biometric authentication for mobile devices". In Proceedings of the Information Security and Privacy Research, IFIP Advances in Information and Communication Technology - IFIP AICT. Springer Boston. pp. 465-474.

Saevanee, H., Clarke, N., Furnell, S., and Biscione, V. (2014). "Text-based active authentication for mobile devices". In ICT Systems Security and Privacy Protection. Berlin Heidelberg: Springer, pp.99-112.

Shi E, Niu Y, Jakobsson M, and Chow R. (2011). "Implicit authentication through learning user behavior". In: Proceedings of the 13th international conference on information security. ISC'10. Berlin, Heidelberg: Springer-Verlag. p. 99–113. ISBN 978-3-642-18177-1.

Zhang, J., Tan, X., Wang, X., Yan, A., and Qin, Z. (2018). "T2FA: Transparent Two-Factor Authentication". In IEEE Access, 6, pp.32677-32686. DOI: 10.1109/ACCESS.2018.2844548