Incoming Call Implicit User Authentication
User Authentication via Hand Movement Pattern

Aleksandr Eremin and Konstantin Kogos
Institute of Cyber Intelligence Systems, NRNU MEPhI, Kashirskoe sh., 31, 115409, Moscow, Russian Federation

Keywords: Implicit Authentication, Hand Movement, Incoming Call Authentication, Behavioural Biometrics.

Abstract: This paper focuses on implicit authentication during answering an incoming call based on user's hand movement. This approach allows to increase usability of authentication against common PIN or graphical password. It increases the security level as well. Unlike other researches in this area, our work considers the problem of answering a question, whether it is the owner of the phone, who is interacting with the device right now. The paper shows that user's hand movement provides all necessary information for authentication and there is no need for user to enter a PIN or graphical password.

1 INTRODUCTION

Smartphones have become indispensable in our daily lives. These devices have become more than personal assistants. Users make purchases, store their photos, contacts, personal accounts – and all of that with the only device. It leads us to the conclusion that the data stored on your mobile phone and services, which are accessed via a mobile phone gain its value, as it contains sensitive information. As Consumer Reports says, smartphone thefts rose from 1.6 to 3.1 million during one year (Tapellini, 2014).

If an attacker seizes user's phone, he gets almost full access to all information that is of particular value for the user: personal communication and contacts, accounts on different services, including online banking, data on movements, photos, etc. In addition, an attacker is able to act on your behalf: make and answer calls, conduct correspondence in social networks and e-mail, etc. Therefore it is becoming an increasingly urgent problem to provide mobile phone user authentication.

The growing popularity of smartphones, progress in their performance and abilities opens new horizons for both attackers and defenders. A lot of authentication methods were used and are still in a use providing protection for mobile phones users.

All authentication methods can be divided into three groups by the authentication factor used during authentication process (Smith, 2002):

- the knowledge factor – something the user knows;
- the ownership factor – something the user has;
- the inheritance factor – something the user is.

The *knowledge factor* in mobile devices is represented by different passwords, patterns or combinations of points on a photo or a picture. Such methods are rather weak as users usually choose easy-memorized passwords or patterns or associate them with a shape or a letter they form on a screen (Løge, 2015).

The *ownership factor* is related to different peripheral devices that the owner uses with his phone. These devices are smart watches, fitness trackers, Bluetooth headphones, etc. The idea of the method is rather obvious: if the phone is connected to the device, there is no reason to worry: the phone is near the owner. However, such method still cannot provide full protection of user's information on the phone.

Methods based on the *inheritance factors* are now gaining more and more popularity due to the fact that these factors are part of the user which means it is hard to steal it. Yet this methods still requires additional user actions: take a photo, spell a phrase, and place a finger on a fingerprint scanner.

Figure 1 shows how these factors corresponding with existing methods of mobile phone user authentication.

Eremin, A. and Kogos, K.
Incoming Call Implicit User Authentication - User Authentication via Hand Movement Pattern.
DOI: 10.5220/0006555200240029
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 24-29
ISBN: 978-989-758-282-0

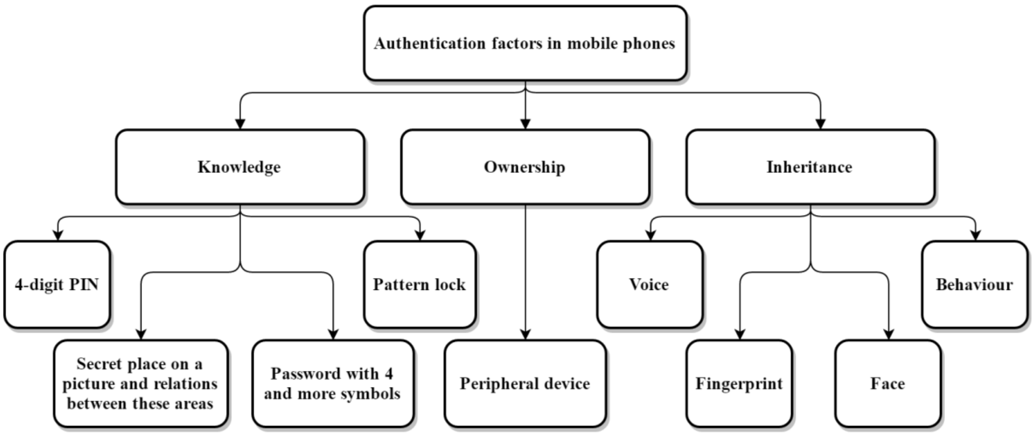
Authentication factors in mobile phones
Knowledge
Ownership
Inheritance
4-digit PIN
Secret place on a picture and relations between these areas
Password with 4 and more symbols
Pattern lock
Peripheral device
Voice
Fingerprint
Face
Behaviour

Figure 1: < in mobile phones.

Behavioural biometrics is of a special interest for us for several reasons. Unlike aforesaid factors, behavioural biometrics doesn’t require additional actions from the user except his natural movements and actions: gait, keystrokes, and characteristic movements like picking up a phone. The recent progress in the methods of machine learning makes it possible to process bigger amounts of data and as a consequence make more precise predictions. Moreover, modern smartphones are equipped with lots of sensors which can provide all necessary information for such authentication methods. This means that there is no need in additional sensors or other hardware, and all data can be gathered and processed with the help of one program.

The main purpose of this research is to review existing methods of user authentication and suggest a new approach to authentication based on behavioural biometrics.

The remainder of this paper is organized as follows. Section 2 contains an overview of existing approaches to behavioural biometrics and related work. Section 3 introduces used sensors and the data obtained from them. Section 4 describes feature extraction used in this research. Obtained results of implementation and evaluation are presented in section 5. Conclusions and further research are discussed in Section 6.

2 RELATED WORK

In (Shrestha, 2013) user should wave his hand several times in front of the surface of the phone's screen to unlock the phone or make a call. Light sensor built into the front panel of the device determines the motion parameters by measuring amount of light falling on it. Next, the collected data is processed by the system; the system compares it with the stored template, and, depending on the result of comparison an outgoing call is performed or not.

In (Yang, 2015) the movement of the hand with the phone is used to unlock the phone. The subjects were invited to shake the phone for 10 seconds and had two modes: a normal mode, the data obtained consisted of 100 measurements, with an interval of 200 ms. 100 measurements were also obtained in the fast mode with an interval of 10-20 ms. After that, the data was processed by the system and a "template" of the movement for each user was created. After that it was enough for user to shake the phone to unlock it. The research demonstrates that the user had to shake the phone for 3 seconds to unlock it, which is longer than the time entered the PIN-code, but users appreciated the comfort, safety and accessibility of this authentication method.

In (Krishnna, 2015) a way to interact with the phone was suggested for purposes of the alarm: if, for example, a woman realizes that she is in danger, it is enough to shake the phone and the call will be sent to the appropriate service, indicating the device's location.

In some cases there is a necessity to authenticate a user answering an incoming call. This happens in case a non-legitimate person’s answer causes a significant owner’s loss. For example, the bank assistant calls the depositor to check whether a strange transaction made from his account was actually made by depositor, not a thief. If a thief answers such call, he can easily confirm a transaction leaving the depositor and the bank without money.

Such a problem of user authentication can be solved by entering a password, but this solution requests additional actions from a user. In

(Maghsoudi, 2016) it is shown how hand movement analysis can be used in user identification. All necessary data was collected by built-in sensors of the smartphone. In this case there is no need user entering anything, all necessary authentication information is being collected while user's hand with a phone is moving towards user's ear. That's why an authentication method without any extra user actions can be suggested providing authentication of a person answering an incoming call.

The problem of incoming call authentication was considered in (Conti, 2011). In this paper, the researchers proposed to replace the input of the password with the characteristics of the hand movement when answering an incoming call. Data, as in previous works, was obtained from built-in sensors (accelerometer and orientation sensor). For user authentication, Dynamic Time Warping Distance and Dynamic Time Warping Similarity algorithms were used. The basic idea of this approach is to obtain the distance between the coordinates of the vector of characteristics of the legitimate user and the coordinates of such vectors of the user in relation to which authentication is performed. The closer the vector of the current user to the legal user's vector, the more likely he is a legitimate user. This approach is notable for its simplicity. Using the training sample of 10 people's 50 lifts of the phone, the system missed the attacker in 4.4% of cases, and the legal user was blocked in 9.3% of cases. These study shows that the movement of the hand when answering an incoming call is unique for each person.

In (Buriro, 2017), a user authentication method based on the "micromovements" of his hand right after unlocking the smartphone on the Android OS is presented. To receive data, built-in smartphone sensors (accelerometer, gyroscope, magnetometer, gravity sensor and orientation sensor) are used. In addition, a low-pass filter and a high-pass filter are applied to the data obtained from the accelerometer. Thus, 7 data sources are used. The data acquisition process starts immediately after receiving the USER_PRESENT event at intervals of 2, 4, 6, 8 and 10 seconds. Then the following features were calculated:

- mean;
- mean absolute deviation;
- median;
- standard error of the mean;
- standard deviation;
- skewness;
- kurtosis.

After this, feature vectors were formed, which were fed to the input of various algorithms of machine learning. It is worth noting that in this paper the task of user identification was considered, so, the classification problem was solved using the machine learning algorithm. The authors gained the following results: in 96% of cases the system correctly identified the user using the Random Forest algorithm.

3 DATA ACQUISITION AND FEATURE SELECTION

The analysis showed that the movement of the hand when answering an incoming call is unique for each person and the information about this movement can be used for user authentication. To perform it, it is necessary to obtain data from the sensors of the mobile phone, pre-process it and select features for learning the algorithm.

3.1 First Look at the Problem

The problem of a mobile phone user authentication when answering an incoming call has several limits and speciality:

- limited time to perform authentication (having no answer, the caller will simply "drop" the call);
- limited operational memory of the device;
- the method used must be simple and user-friendly.

Based on these limits, a method of authentication based on behavioural biometrics was proposed, in which the user would not need to perform any additional actions, except for placing the phone to his ear, as he usually does answering an incoming call. This action becomes a source of the behavioural biometrics data of the user.

We would like to focus your attention on the fact that only standard sensors (gyroscope, accelerometer, touch screen) are needed, and most of modern smartphones are equipped with these sensors.

3.2 Sensors Used and Data Obtained

In order to describe the movement of the phone in space, it is necessary to obtain data from the sensors of the phone. An event is generated in the Android OS when a state of any sensor is changed. According to the Android documentation, each sensor generates such an event every 200 milliseconds. This frequency is sufficient to obtain the required amount of data, even about a short movement, such as raising your hand with the phone towards your ear.

The following sensors were used:

- accelerometer (measures the acceleration in m/s^2, with which the phone moves on all three axes, including the force of gravity);
- gyro (measures the rotation rate of the phone in rad/s around each of the axes);
- magnetometer (measures the ambient geomagnetic field for all three axes in μT);
- orientation sensor (measures the degree of rotation around each of the three axes);
- gravity sensor (measures the force of attraction applied to the phone on all three axes).

All sensors generate data about the position of the phone in three axes: X, Y and Z, which are located as shown in Figure 2.

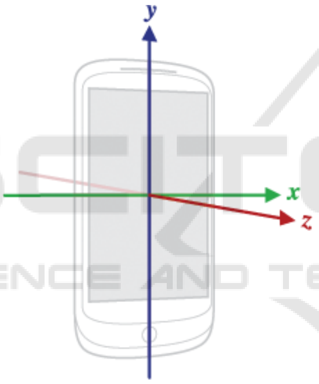

Figure 2: Sensors' axes.

The received data is saved for further processing into files, one file for each sensor. These files are available only to the developed application.

The process of obtaining data is carried out for two seconds, since this interval is enough to place the phone to your ear.

4 FEATURE EXTRACTION

In our research, we used features that authors of (Buriro, 2017) used in their work, because these features describe the hand movement dynamic clearly. These features are:

- mean;
- mean absolute deviation;
- median;
- standard error of the mean;
- standard deviation;
- skewness;
- kurtosis.

Moreover, we added two more features to gain more accurate results as it helps to describe the movement more precisely. These features describe the exact position of the phone at the exact moments of the motion (the coordinates obtained from the sensors mentioned above). These features are:

- the coordinates of the device at the beginning of the movement (when accepting the call):
- the coordinates of the device at the end of the movement (when the device is placed near the ear).

It will be shown further how the addition of these features influenced the accuracy.

As the result, feature vector has the following structure (a concatenation of the features computed from different axes separately):

$$v = ([\bar{x}, \bar{y}, \bar{z}, MAD_x, \dots][\bar{x}, \bar{y}, \bar{z}, MAD_x, \dots] \dots) \qquad (1)$$

Square brackets contain the features obtained from one sensor. The length of the vector is 135 (5 sensors, 3 coordinates, 9 features for every sensor).

5 IMPLEMENTATION, RESULTS AND ANALYSIS

In this paper, the user authentication task is solved when answering an incoming call. In contrast to (Maghsoudi, 2016, Buriro, 2017), in which the data of several users was used and the classification problem was solved, the problem in question belongs to problems of anomaly detection, since there are no data of other classes except the "legitimate user" class in the training sample.

Due to the limits of implementing the authentication method, as the use of a smartphone on the Android OS, it was decided to use WEKA, data analysis software (Weka 3) that is written in the Java programming language.

During the testing, the above described algorithms of machine learning were compared by several parameters and a suitable algorithm for the proposed authentication method was chosen.

To evaluate the performance of algorithms we use following characteristics:

- TPR – true positive rate;
- FPR – false positive rate:
- FNR – false negative rate;
- ACC – accuracy.

It should be noted that in order to improve the quality of this authentication method, it is necessary to minimize the number of type II errors with a satisfactorily low number of type I errors.

5.1 Training Set and Testing Set

A training set was created containing 50 vectors of features, i.e. 50 hands rising with the phone to the ear were obtained and processed. This size of training set seems to be sufficient, as more movements will negatively affect the usability of this method. In addition, it will be further shown that with the increase in amount of objects in the training set, the quality of the algorithm stops to grow after a certain amount.

A test set contained 50 legitimate user movements (not used in the training set) and 50 movements of 10 other people who pretended to be "intruders".

The appropriate parameters of the algorithms were chosen experimentally to improve the quality of the algorithms.

5.2 Implementation

WEKA allows to solve anomaly detection problem with the help of two algorithms of machine learning, One-Class SVM and One-Class Classifier. Let us consider their features in details.

5.2.1 One-Class SVM

One-Class SVM (OC-SVM) is one of the examples of SVM. The idea is to divide the space of objects by a hyperplane in such a way that objects of one class are on the same side of the hyperplane. In the case of a one-class support vectors machine, the method tries to separate sample objects from the origin, while the dimensionality of the space can be increased in order to distinguish the objects of the target class from the anomalies. In this case, some of the objects are defined as anomalous (the proportion of such objects in the training sample is characterized by the parameter ν), and then the problem is reduced to the classification problem. Most often, when using SVM to solve the problem of detecting anomalies, the RBF-kernel is used.

5.2.2 One-Class Classifier

A One-Class Classifier (OCC) was proposed in (Hempstalk, 2008) and implemented in Weka. Its peculiarity lies in the fact that this classifier is a kind of "wrapper" for standard classifiers, including a Naïve Bayes or the method of k-NN. This becomes possible due to the fact that the artificial data is generated, this data has a different distribution than the "normal" data, and so, it becomes some sort of anomaly. Thus, these artificial data play the role of the second class, and the problem of detecting anomalies also reduces to the classification problem.

5.3 Evaluation

There were several algorithms that were tested. Here in this work we show only algorithms with best results we obtained while testing them.

While evaluating algorithms we realized, that having a training set consisting of 25 movements and greater the accuracy of algorithms stops to grow. It is rather clearly shown on Figure 3.

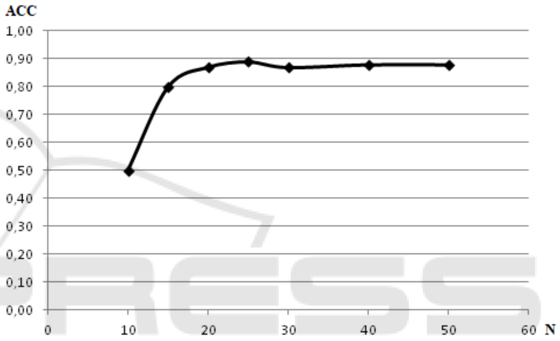

Figure 3: Accuracy dependency of training set size using One-Class Classifier with Naive Bayes.

That leads us to the assumption that having 25 movements in training set is quite enough to train a model with satisfactory results. That means that the user doesn’t have to perform too much movements to train a model and the usability of the method is quite good at this point.

During the experiments, an assumption that addition of “exact position” features improves the results of the algorithms was tested. Table 1 shows that the addition of it improves the accuracy in case of One-Class Classifier with Naïve Bayes (OCC-NB). In addition, having these extra features, One-Class Classifier with Random Forest (OCC-RF) decreased the number of FN with the same amount of FP that leads to the usability growth having a stable level of security. Talking about One-Class SVM (OC-SVM), its FPR decreased while FNR increased. This means that the security of authentication provided with this method has grown, but it led to fall in usability as the user is detected as an intruder more often.

Table 1: Evaluation results.

Alg.	Before extra features addition			After extra features addition		
	FNR	FPR	ACC	FNR	FPR	ACC
OCC-NB	0,34	0,1	0,78	**0,2**	**0,02**	**0,89**
OC-SVM	0,34	0,18	0,74	0,18	0,35	0,74
OCC-RF	0,76	0,1	0,73	0,44	0,08	0,74

This far the best results were obtained with One-Class Classifier using Naïve Bayes. Only 2 percents of testing movements were recognized as user's while it was intruder who performed the movement (FPR).

6 CONCLUSIONS AND FURTHER RESEARCH

As a result, it was determined that adding features that clearly characterize the position of the phone at a particular time improves the accuracy of the algorithm. The obtained accuracy allows drawing a conclusion about the possibility to perform an incoming call user authentication with the characteristics of user's hand movement.

The purpose of further research is to improve the performance of the chosen algorithm. For this it is proposed to break the interval of motion into segments and consider them independently of each other (Maghsoudi, 2016). In addition to this, we will consider the possibility of adding new features (extra points defining the position of the phone during the movement). At the same time, it is necessary to reduce the sample size required for training to increase the usability of the developed method. Gathering more representative testing set is another goal to achieve.

ACKNOWLEDGEMENTS

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Professional Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

REFERENCES

Tapellini, D., 2014. *Smart phone thefts rose to 3.1 million in 2013*. URL: http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

Smith, R. E., 2002. *Authentication: From Passwords to Public Keys,* Williams Publishing House. Moscow.

Løge, M. D., 2015. *Tell Me Who You Are and I Will Tell You Your Unlock Pattern*, Master of Science in Computer Science. Norwegian University of Science and Technology.

Shrestha, B., 2013. Wave-to-Access: Protecting Sensitive Mobile Device Services via a Hand Waving Gesture. In *Proceedings of the 12th International Conference on Cryptology and Network Security*.

Yang, L., Guo, Y., Ding, X., et al., 2015. Unlocking smartphone through handwaving biometrics. In *IEEE Transactions on Mobile Computing.*

Krishnna, G., Durga, V., Dheepika, B. et al., 2015. Mobile Waving Pattern: Android Based Unlocking Mobile Waving Pattern for Emergency Support System. In *International Journal of Innovative Research in Computer and Communication Engineering.*

Maghsoudi, J., Tappert, C., 2016. A Behavioral Biometrics User Authentication Study Using Motion Data from Android Smartphones. In *Proceedings of European Intelligence and Security Informatics Conference.*

Conti, M., Zachia-Zlatea, I., Crispo, B., 2011. Mind How You Answer Me! In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security.*

Buriro, A., Crispo, B., Zhauniarovich, Y., 2017. Please Hold On: Unobtrusive User Authentication using Smartphone's built-in Sensors. In *Proceedings of IEEE International Conference on Identity, Security and Behavior Analysis.*

Weka 3: Data Mining Software in Java. URL: http://www.cs.waikato.ac.nz/ml/weka/.

Hempstalk, K., Frank, E., Ian, H., 2008. One-Class Classification by Combining Density and Class Probability Estimation. In *Proceedings of the 12th European Conference on Principles and Practice of Knowledge Discovery in Databases and 19th European Conference on Machine Learning.*