Kosareva Anastasiia,
Pavlo Rehida

ISSUES AND METHODS OF BIOMETRIC AUTHENTICATION

Abstract. This paper dials with biometric authentication methods, such as fingerprint recognition, face recognition, their advantages and disadvantages and additional biometry such as behavior keystroke-based authentication method, taking in consideration existing solution. Also own developed solution based on neural network learning is presented and described.

Key words: biometrics, authentication, user behavior, keystroke, neural networks.

Fig.: 3. Tabl.: 1. Bibl.: 4.

Relevance of the research topic: Since humanity is surrounded with gadgets and store all personal data on such devices as smartphones, it is crucial to keep user’s information safe and secure. Behavior authentication, which can be added as secondary authentication method, is getting more and more relevant, imperceptible and accurate over time. Those characteristics can help to authenticate user invisibly and accurately.

Formulation of the problem: The less personal gadget is defended from threats coming from outside, the more probability of data to be stolen. Using password as the only method of authentication is not so secure as it used to be. Nowadays it is very important to add another level of biometric authentication, which is not based on physiological characteristics, which can be face recognition, fingerprint recognition, iris or retina recognition systems, but those have to be reliable and unobtrusive.

Analysis of recent researches and publications: The main idea of keystroke based biometric authentication is validating authorized or unauthorized users not on what they write in different text inputs but how they write it. It is important to extract the pattern of typing on specific gadget and provide this data as an additional way of authentication, where behavior authentication system uses received pattern. Resent publication show researches in keystroke-based method of authentication by dividing them into two groups: static and dynamic typing. The example of those methods can be typing already known login and password for static method and entering not a specific string, where user can type random text for dynamic method. Figure 1 shows the basic algorithm of user authentication based on keystroke pattern which is get from dynamic-based experiment.

Now existing approaches should be considered.

First solution that will be mentioned was recreated by Matthias Trojahn and Frank Ortmeier [2] in *A mixture approach based on analysis of keystroke and handwriting* where keystroke-based method and handwriting patter based the form of authentication on smartphones and tablets. Two experiments were performed to collect user data such as typing the sentence which contains two or more words and to enter the password using provided devices on Android platform. For the first experiment 18 subjects were involved and they were asked to type the sentence 10 times. For the second approach 16 subject were recruited to enter the password 8 times. Authors used Kstar, Decision trees, Multilayer perceptron or (MLP) and other technologies based on neural networks as classifiers.

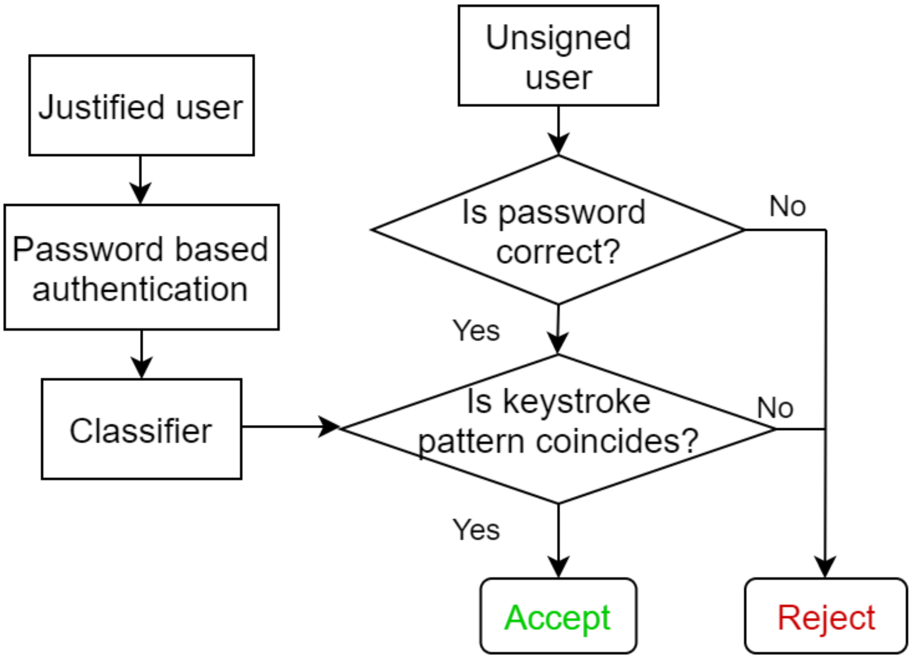


Fig. 1. General algorithm of keystroke-based authentication method

Second solution was introduced by Kambourakis et al. [3] which is *Using speed of finger movement*. The main idea of this method is to improve the analyzing stage of traditional-based keystroke dynamics. Such features were used as inter-time (the time between releasing the previous key and pressing next one), hold-time (the time between press-release state of a single key), speed and distance. 20 subjects were recruited to collect the data by recurring typing of several strings (12 times to be accurate). Were chosen such classifiers as MLP which already has been mentioned, k-NN, Random Forest.

Third solution – *Using sensors with a virtual software keyboards to identify users* – was recreated by Gascon et al. [4]. Authors developed such approach where they used virtual keyboard application for the Android smartphone platform and collected behavioral biometrics based on keystroke method, also orientation sensor, accelerometer and gyroscope were implemented. Static typing method was used in this research since recruiters were asked to type pre-defined short text string. The participants were divided into two groups where first group contained 303 volunteers who were asked to type the text only once. Second group contained only 12 users, who were already authorized, and they were asked to enter the same text 10 times, it was enough to collect keystroke pattern of each participant. Volunteers were limited with T seconds while typing. For example, if there were no symbols entered in T_{stop} seconds, program understood that user finished writing. Program collects and analyze all motions and gestures which are related to typing.

In table 1 mentioned typing motion approaches are summarized and can be compared.

Table 1

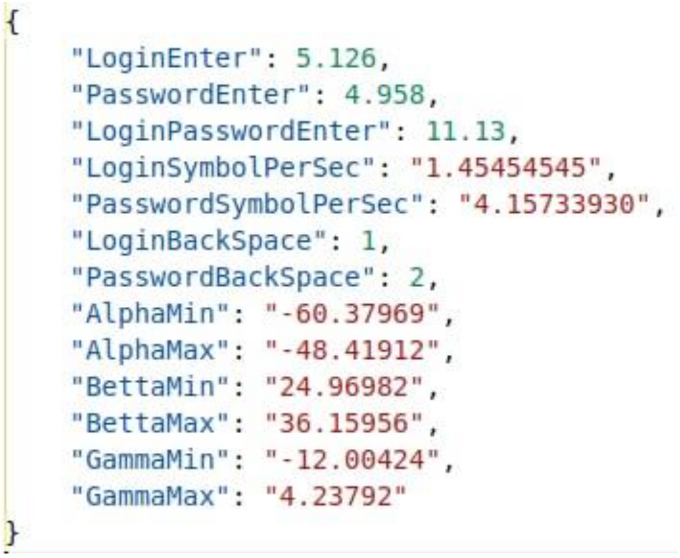
Examples of keystroke-based authentication solutions

Study	**Collected data**	**Used classifiers**	**Used features**	**Results**			
				EER	**FAR**	**FRR**	**Memory con-sumption**
M. Trojahn, F. Ortmeier [2]	16	MLP, K-star, J48, Bayes Net	Pressure on screen, finger size	1 exp.: 2%; 2 exp. 13.5%	2.03% at J48	2.67% at J48	-
G. Kambourakis et al. [3]	20	MLP, k-NN, Random Forest	Speed, distance, inter-time, hold-time	-	1st phase: 10.4%-16.8% 2nd phase: 8.93%	-	-
Gascon et al. [4]	315	LSVM (linear support vector machines)	iFFT Spline Features, iFFT Signal Features, Simple Statistics	-	Unautho-rized users: 35%, authorized users: 1%	Unautho-rized users: 58%, authorized users: 92%	-

Selection of unexplored parts of the general problem: Despite ongoing research in the use of neural networks in conjunction with behavior biometrics, this topic is still not fully disclosed and requires further consideration and study. Nevertheless, more attention should be paid to the bundle of behavioral biometrics and built-in sensors such as gyroscope, accelerometer, etc.

Setting objectives: The purpose of this article is to provide an open-source behavior authentication method, which is based on keystroke methods, uses gyroscope sensor for providing smartphone orientational angles to each of the X, Y, Z axes. Collected data is sent to neural network which learns to accept and reject users using their behavior pattern. Authors invites other stakeholders to refine offered open-source solution to promote the idea and devote more researches and developments to it.

Presentation of the open-source solution: The open-source solution is developed by React Native framework based on JavaScript programming language which makes it possible to use the program on Android and iOS smartphone platforms. BrainJS neural network is used to provide users authentication by collected datasets and is working on the developing nodeJS server. Datasets contains such information as time for entering login and password separately and together, the amount of entered symbols per second as typing speed for each text input, how many times backspace button was pressed and minimum and maximum orientational angle based on gyroscope sensor information. The dataset example is provided on figure 2.



```
{
    "LoginEnter": 5.126,
    "PasswordEnter": 4.958,
    "LoginPasswordEnter": 11.13,
    "LoginSymbolPerSec": "1.45454545",
    "PasswordSymbolPerSec": "4.15733930",
    "LoginBackSpace": 1,
    "PasswordBackSpace": 2,
    "AlphaMin": "-60.37969",
    "AlphaMax": "-48.41912",
    "BettaMin": "24.96982",
    "BettaMax": "36.15956",
    "GammaMin": "-12.00424",
    "GammaMax": "4.23792"
}
```

Fig. 2. Dataset example

Figure 3 demonstrates the algorithm of the open-source solution which was described. Since this method also uses password authentication, bcrypt encryption npm library was used to provide secureness of the stored password (it is assumed that the user is already registered in the system). The main advantage of this encryption method is that while comparing entered string with the stored one, it hashes entered data and combine it to already hashed stored information which makes it harder to attacker to steal the credentials data. The hashing function gets the output as the cost and the 128-bit salt value concatenated with the result of the encryption loop.

Conclusion: The paper demonstrates promising approaches to contemporary biometric authentication methods, namely behavioral keystroke-based authentication methods combining with other ways of recognizing users, such as hand-waving recognition methods, touchscreen recognition methods. Existing approaches have been considered and described to form the general problem and to set the objectives. Also, article is demonstrating authors approach to behavior keystroke-based authentication.

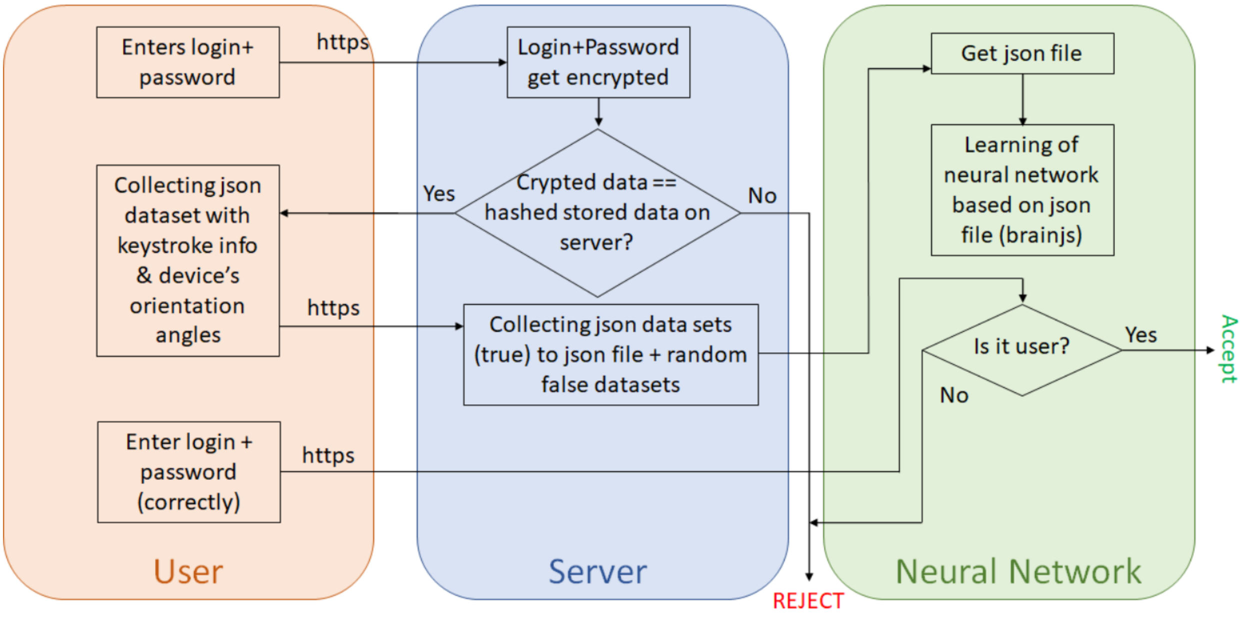

Enters login+ password
https
Login+Password get encrypted
Get json file
Learning of neural network based on json file (brainjs)
Collecting json dataset with keystroke info & device's orientation angles
Yes
Crypted data == hashed stored data on server?
No
https
Collecting json data sets (true) to json file + random false datasets
Is it user?
Yes
Accept
No
Enter login + password (correctly)
https
User
Server
Neural Network
REJECT

Fig.3. Algorithm of open-source solution

References

1. Alzubaidi A. and Kalita J. (2016). *Authentication of smartphone users using behavioral biometrics*". IEEE Commun. Surv. Tutor. (pp. 1–10).

2. M. Trojahn and F. Ortmeier (2013). *Toward mobile authentication with keystroke dynamics on mobile phones and tablets*. In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on. IEEE (pp. 697–702).

3. G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis (2014). *Introducing touchstroke: keystroke-based authentication system for smartphones*. Security and Communication Networks (pp. 1–13).

4. H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck (2014). *Continuous authentication on mobile devices by analysis of typing motion behavior*. In Sicherheit (pp. 1–12).