Surveys

Continuous user authentication on smartphone via behavioral biometrics: a survey
https://link.springer.com/article/10.1007/s11042-022-13245-9

09 June 2022; Rayani, Changder

The smartphone can act as an intelligent personal assistant with integrated sensors and actuators to simplify their daily needs. (+1 article)

The deployed and most widely used entry-point authentication methods experiencing several vulnerable limitations (+1) Deployed and current entry-point authentication mechanisms of the smartphone have been experiencing several security breaches from malicious insiders (+6).

Creating a large dataset for continuous authentication is very difficult for researchers because many users may not show interest in making their confidential behavioral traits public.

Public Datasets: (https://link.springer.com/article/10.1007/s11042-022-13245-9/tables/1)

Dataset	#Users	Sensors	Activities
MIT Reality	100	Bluetooth, GPS, Keystroke	passive (apps usage)
MOBIO	150	Touch, Microphone	audio, video based
LiveLab	34	GPS, Accelerometer, Bluetooth, WiFi	passive (apps usage)
Touchalytics	41	Touch	scrolling
GCU	7	Accelerometer, Gyroscope, WiFi, Light	
Antal	51	Touch	scrolling
UMDAA-01	50	Touch, Camera	
UMDAA-02	48	Touch, Accelerometer, Gyroscope, Camera	
HMOG	100	Touch, Accelerometer, Gyroscope, Magnetometer	
Sherlock	50	Accelerometer, Gyroscope, WiFi, Bluetooth, GPS, Light	
MSC	6	Accelerometer, Gyroscope, WiFi, Bluetooth, GPS, Light	

Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey
https://ieeexplore.ieee.org/document/9179700

28 August 2020; Abuhamad

Hodně zdrojů na attacks, porovnání starčích surveys

Behavioral biometrics & continuous user authentication on mobile devices: A survey
https://www.sciencedirect.com/science/article/pii/S1566253520303493?via%3Dihub

February 2021; Stylios.

A survey on behavioral biometric authentication on smartphones
https://www.sciencedirect.com/science/article/pii/S2214212617302417

December 2017; Mahfouz

Touch-dynamics based Behavioural Biometrics on Mobile Devices – A Review from a Usability and Performance Perspective
https://dl.acm.org/doi/abs/10.1145/3394713

2020; Ellavarason

A survey on touch dynamics authentication in mobile devices
https://www.sciencedirect.com/science/article/pii/S0167404816300256

June 2016; Teh, Zhang

Touchscreen based authentication

Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication

https://ieeexplore.ieee.org/document/6331527

16 October 2012; Frank

41 users

Dataset - http://www.mariofrank.net/touchalytics/index.html

reading and image viewing behavior on smart phones

+ kNN: The classifier takes every new observation and locates it in feature space with respect to all training observations. The classifier identifies the training observations that are closest to the new observation. Then, it selects the label that the majority of the closest training observations have. This procedure requires no explicit training phase. For huge datasets, the limitation of this method can be that not all data can be stored. In our case, this is not a problem as our feature space is comparably low-dimensional and, to keep classes balanced, we store only as many samples from the negative class as there are samples of the legit user.

+ SVM: In contrast to kNN it generalizes from the observed data, i.e., it forgets the individual observations after training and only saves the decision hyperplane. SVM performed better.

Our classifiers treat every stroke individually. The estimation of the authenticity of the user is thus a highly volatile random variable. Instead of individually classifying all strokes and taking the majority vote as the final decision, we combine the classifier output at an earlier stage. For SVM, we average the continuous scores of projecting the individual test observations on the vector orthogonal to the decision hyperplane. For kNN, we sum up the number of positive and negative labels of all nearest neighbors of all involved strokes and put the threshold on the ratio of these counts.

BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics

https://www.sciencedirect.com/science/article/pii/S1570870518306899?via%3Dihub

1 March 2019; Yang

45 users
clicking operation, vertical sliding operation, horizontal sliding operation, and oblique sliding operation
OCSVM
Accuracy 95%

Addressed that capturing behavioral data from unauthorized users in advance were practically not possible. Thus, validating a smartphone user with a binary or multiclass classifier was illogical. Hence, the authors had implemented continuous touchscreen authentication framework on smartphone using One-Class SVM (OCSVM) and iForest classifiers.

Their experiment captured several touch operations from the WeChart app, including clicking, vertical sliding, horizontal sliding, and oblique sliding operations. Their experiment had computed the confidence level (+2) and accuracy of different touch operation sequences using the Bayesian theorem (BT) and expectedprob algorithm. Experiment results on 3 and 9 consecutive touch operations had shown the best accuracy.

To enable stable verification, we choose four types of touch operations which are common and frequent. We extract features and build a model for each type of touch operations respectively. To calculate the recognition rate of an operation sequence, BehaveSense extracts the confidence level of each type of touch operations using Bayesian theorem and computes the accuracy of a touch operation sequence with an improved expectedprob algorithm.

Novelty detection:

- https://www.sciencedirect.com/science/article/pii/S0165168403002020
- https://ieeexplore.ieee.org/document/7877899

clicking operation (Co), vertical sliding operation (Vs), horizontal sliding operation (Hs), and oblique sliding operation (Os).

Filter Standardized MinMaxScaler

Preprocessing

Before feature extraction, we need to filter out exceptional operation (sliding up and down) and transform the data into normalized format. In particular, to eliminate exceptional operations, we compute the distances between start point (x0, y0) and other points (xi, yi) i = 1,2, ..., n of each sliding operation, and filter out these sliding operations where distances don't follow an ascending order. Moreover, as the range of user properties is different from each other, performance, we choose the MinMaxScaler and Standardized method to scale their values to [0, 1].

4.3 podrobne sbirani predevsim scrolling eventu

Local Outlier Factor (LOF), EllipticEnvelope needs to know distribution of samples. OCSVM and iForest do not. According to the result, we set these parameters as nu = 0.1, kernel = 'rbf', and gamma = auto. iForset max_samples = n, and contamination = 0.1

To efficiently identify different users, we still need to quantify the similarity between two touch operation sequences. In addition, the accuracy of different touch operations varies a lot and the touch operation with higher accuracy is more trustable. Therefore, before calculating the accuracy of an operation sequence, we should first compute the confidence level of each touch operation.

Information revealed from scrolling interactions on mobile devices

https://www.sciencedirect.com/science/article/pii/S0167865515000355

15 April 2015; Antal

Continuous User Authentication by the Classification Method Based on the Dynamic Touchscreen Biometrics

https://ieeexplore.ieee.org/document/8711941

13 May 2019; Leyfer

14 users
Pressure, x coordinate, y coordinate, duration of the gesture, timestamp, finger down, finger up, finger move
RF and Gradient Boosting
AUC: 0.96

Implemented a continuous authentication approach to recognize the user through single-touch and multi-touch gestures. The experimental results on RF and Gradient Boosting classifiers had shown a similar AUC score of 0.96. In contrast to learning time, the gradient boosting classifier was 2.6 times faster than the RF classifier.

Exploring a statistical method for touchscreen swipe biometrics

https://www.researchgate.net/publication/321657537_Exploring_a_statistical_method_for_touchscreen_swipe_biometrics

October 2017; Pozo

190 Users
Vertical stroke features and horizontal stroke features
GMM with UBM
EER between 15% and 22%

Statistical-based touchscreen authentication system to recognize the genuine user through single-touch gestures (such as horizontal and vertical touch strokes). Their system had utilized Sequential Forward Floating Search (SFFS) algorithm and Gaussian Mixture Models (GMM) with Universal Background Model (UBM) to select the best features and similarity matching, respectively. Their experiment had shown EER between 15% and 22% with 30 to 40 training samples.

Benchmarking Touchscreen Biometrics for Mobile Authentication

https://ieeexplore.ieee.org/document/8353868

03 May 2018; Fierrez, Pozo

41 users
swipe gesture features and signature features
SVM with RBF kernel and GMM with UBM
EER: 3.1% to 4.3% (frank dataset)

Evaluated swipe-gesture and signature features with three authentication models to recognize the user: discriminative, statistical, and fusion models.

Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms

https://ieeexplore.ieee.org/document/6712758

16 January 2014; Serwadda

Scrolling (horizontal and vertical scrolls), 10 different verifiers. SVM, RF, Logistic regression. Comparing a few studies.

Performance Analysis of Touch-Interaction Behavior for Active Smartphone Authentication

https://ieeexplore.ieee.org/document/7335628

23 November 2015; Shen, Zhang

Graphical Password-Based User Authentication With Free-Form Doodles

https://ieeexplore.ieee.org/document/7362167

22 December 2015; Martinez-Diaz, Fierrez

Touch-Stroke Dynamics Authentication Using Temporal Regression Forest

https://ieeexplore.ieee.org/document/8713391

13 May 2019; Ooi, Teoh

190/41 users
28 hand-engineered features
TRF
EER: 1.8% / EER: 1.1%

TouchWB: Touch behavioral user authentication based on web browsing on smartphones

https://www.sciencedirect.com/science/article/pii/S1084804518301723?via%3Dihub

1 September 2018; Meng, Wang.

48 users
single-touch features, touch-movement features, multi-touch features
PSO-RBFN
FAR: 2.22% FRR: 2.54% AER: 2.38%

Touch gesture-based authentication on web browsing apps. Captured single-touch, touch-movement, and multi-touch features. Evaluated several classifiers, such as J48, NB, Kstar, RBFN and BPNN. FAR of 8.43% and 6.87% for free gestures and web browsing activity.

SocialAuth: Designing Touch Behavioral Smartphone User Authentication Based on Social Networking Application

https://www.researchgate.net/publication/333812999_SocialAuth_Designing_Touch_Behavioral_Smartphone_User_Authentication_Based_on_Social_Networking_Applications

June 2019; Meng

50 users

single-touch features, touch-movement features, multi-touch features
SVM
FAR: 2.89% FRR: 3.24% AER of 3.07%

Touch behavioral authentication approach on social networking apps of the smartphone. SVM classifier had shown AER as 6.02% and 3.07% for free touches and touch gestures. Investigated behavioral inconsistency of the user during long-term authentication. User's touch behavior had more consistent in long-term authentication.

Active Authentication on Smartphone using Touch Pressure

https://dl.acm.org/doi/10.1145/3266037.3266113

October 2018; Kudo

21 users
Pressure, velocity, stroke duration, touch coordinates (x and y)
Online AROW
EER 0.014 %

Investigated the usability of the smartphone in sitting, standing, and prone postures with and without touch pressure feature using the online AROW (Adaptive Regularization of Weight Vector) learning method. Their experiment on the device's usability with touch pressure feature had successfully reduced EER.

Dynamic Authentication of Smartphone Users Based on Touchscreen Gestures

https://link.springer.com/article/10.1007/s13369-017-2758-x

04 August 2017; Alghamdi

20 users
tapping, scrolling, drag, and zoom
k-NN
EER: 0%

Examined several touch gestures, including tapping, scrolling, drag, and zoom. Unlike k-NN and RF classifiers, their experiment on single-touch gestures with the MVP classifier had produced the best EER. Moreover, their experiment on combining three to five sequential gestures with the k-NN classifier had obtained AER of 0%.

Enhancing touch behavioral authentication via cost-based intelligent mechanism on smartphones

https://link.springer.com/article/10.1007/s11042-018-6094-2

20 May 2018; Meng

60 users
timing of touch inputs, press down, press up, touch coordinates (x and y), touch pressure and touch size
SVM
FAR: 4.95% FRR: 4.37% AER: 4.66%

Noticed that behavioral authentication with the sole machine learning model could reduce the system usability. Thus, the authors had implemented a cost-based intelligent mechanism that could adaptively select the less costly algorithm from the classifier pool for user authentication. Their experiment on touch behavioral authentication had shown the best authentication score with the cost-based intelligent mechanism than the sole machine learning model.

Simulated Cloud Authentication Based on Touch Dynamics with SVM

https://ieeexplore.ieee.org/document/8628762

31 January 2019; Gunn

5 users
System time, event time, activity id, action id, point id, touch coordinates (x and y), pressure, contact size, phone orientation
SVM
Accuracy: 98.997 %

Identified that most of the mobile applications were associated with the cloud for storing users' data. The attacker can gain access to the user's data by performing several attacks (+2). Thus, a simulated distributed cloud authentication framework using touch dynamics had been presented. Investigated several behavioral traits: touch dynamics, keystroke data, and their fusion. Their experiment on feature selection using the random forest classifier had discarded the phone orientation feature. Their experiment on touch dynamics with SVM classifier had shown outstanding authentication score than RF and LSTM-RNN.

User authentication via touch pattern recognition based on isolation forest
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8317378

2018; Filippov

Zajímavé jen protože využívá iForest

Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones
https://www.usenix.org/conference/soups2014/proceedings/presentation/xu

Keystroke based authentication

Typing pattern on a smartphone's virtual keypad - digraph, trigraph, pressure, finger size, hold time, and keystroke latency.

Multi-Model authentication using keystroke dynamics for Smartphones

https://ieeexplore.ieee.org/document/8576226

16 December 2018; Cilia

24 users
digraph and trigraph
SVM with gaussian RBF kernel
EER: 0.44%

Investigated the performance of digraph and trigraph features during different modes of smartphone operation with full-sentence and full-session datasets. The authors reported that their experiment on the full-sentence dataset had shown better results with trigraph features. Moreover, their experiment on the full-session dataset had shown better results with digraphs. However, their study addressed that trigraph features require more computation than digraphs.

Keystroke dynamics-based user authentication using long and free text strings from various input devices

https://www.sciencedirect.com/science/article/pii/S0020025514009062?via%3Dihub

1 July 2015; Kang

35 users
sequence index, start key, end key, down-down time
R+A measure
Average EER: 1.90%

Implemented a keystroke-based authentication approach on several devices using long and free reference text strings. The authors had evaluated several one-class classifiers, such as the mean and variance equality test (MV test), Kolmogorov–Smirnov statistic (K–S statistic), Cramér–Mises criterion (C–M criterion), the distance between two digraph matrices (digraph distance; DD), relative measure (R measure), absolute measure (A measure), the linear combination of the R and A measures (R+A), the product combination of the R and A measures (RA), Gaussian density estimator (Gauss), Parzen window density estimator (Parzen), k-NN, and support vector data description (SVDD).

Their experiment on soft and touch keyboards with CM criterion (statistical measure) had shown the best authentication scores. Moreover, experimental results on PC keyboard with RA measure had shown the best authentication score. The authors reported that when the size of the reference and test sets had increased from 100 to 1000, then EER had reduced.

Keystroke Active Authentications Based on Most Frequently Used Words

https://dl.acm.org/doi/10.1145/2713579.2713589

Darabseh; 04 March 2015

28 users
flight time latency, diagraph time latency, and word total time duration
Statistic test
FAR: > 3%

Examined four features on the most frequently used words: duration, flight time latency, digraph time latency, and word total time duration. Their experiment on active authentication with digraph time latency had shown the lowest EER than other features. Their experiment on the word total duration feature had shown the highest EER due to inconsistent word size. The authors inferred that the digraph time latency feature could reduce the error rate in keystroke-based authentication.

Securing smartphones via typing heat maps

https://ieeexplore.ieee.org/document/7684753

27 October 2016; Inguanez

32 users
diagraph, position, surface area, velocity, euclidean slide distance features
MLP
Accuracy: 94.81% FAR: 6.33%

Investigated the significance of several keystroke features individually: digraph, position, area, velocity, and slide. Their experimental results had shown the highest FAR of 32.68% for the digraph feature and the lowest FAR of 17.03% for the slide feature. Further, their experiment on combined features had shown FAR of 6.33%. In contrast to digraph, combined features had reduced FAR of 26%.

The Applicability of Fuzzy Rough Classifier for Continuous Person Authentication

https://ieeexplore.ieee.org/document/7861645

23 February 2017; Temper

25 users
Di-Graph, pressure, size and speed
VQNN
Accuracy: 98.2%

Discussed that an attacker could easily capture static authentication methods. Moreover, a single behavioral biometric did not guarantee reliable human identification. Thus, continuous authentication using keystroke dynamics and touch gestures on a self-made banking app was presented.

Their experiment with Vaguely Quantified Nearest Neighbours (VQNN) had achieved 98.2% of authentication accuracy.

Keystroke-based Continuous Authentication while listening to Music on Your Smart-phone

https://ieeexplore.ieee.org/document/8249029

08 January 2018; Primo

27 users
key interval latency
R Measure
EER: 4.29%

Discussed how user contexts could impact the performance of keystroke-based authentication on the smartphone. Thus, the author had presented a continuous authentication approach based on keystroke behavioral biometrics while listening to music on the device. Their experiment had evaluated three latencies with digraphs: key hold, key interval, and keypress latencies. While listening to the music, their experiment on R measure with three latencies had shown the lowest EER. For non-music apps, their experiment had shown the highest EER.

One-class naïve Bayes with duration feature ranking for accurate user authentication using keystroke dynamics

https://link.springer.com/article/10.1007/s10489-017-1020-2

24 August 2017; Ho

51/118 users
keystroke's index order, dwell time, and flight time
SITS and ONENB
FAR: 0% FRR: 35.34%

Introduced a keystroke dynamics authentication based on feature ranking for accurate user authentication. Their approach focused on the typing speed information of the user because most users had different typing patterns. The authors had implemented the speed inspection in the typing skills (SITS) algorithm that calculates keystroke index data. Experimenting on the CMU dataset with the SITS&ONENB method had achieved the best performance results compared to other methods. Experiment results had shown FAR of 0%. Their approach had achieved FRR of 35.34% and 48.88% for when the imposter was unfamiliar and familiar with the password, respectively.

Understanding Keystroke Dynamics for Smartphone Users Authentication and Keystroke Dynamics on Smartphones Built-In Motion Sensors

https://www.researchgate.net/publication/323779574_Understanding_Keystroke_Dynamics_for_Smartphone_Users_Authentication_and_Keystroke_Dynamics_on_Smartphones_Built-In_Motion_Sensors

March 2018; Lee

22 users
down-time, flight-time, size of the fingertip, coordinate values on the touch screen, accelerometer samples, Game-Rotation samples and gyroscope samples (x, y and z axis)
MD
EER: 7.89%
Addressed that pattern drawing and PIN (Personal Identification Number) authentication methods were leaked due to shoulder surfing attacks. Moreover, the smartphone's fingerprint sensor had failed to scan the user's fingerprint at certain conditions. Thus, the authors had introduced a multifactor authentication approach that authenticates a user by combining PIN, keystroke dynamics, and motion data.

Unlike ED and OCSVM, their experiment on MD had shown the EER of 8.94% and 7.89% for without and with motion data, respectively. Their approach with MD distance metric had achieved the best authentication performance than OCSVM.

Continuous Transparent Mobile Device Touchscreen Soft Keyboard Biometric Authentication

https://ieeexplore.ieee.org/document/8710764

13 May 2019; Dee

4 users
Key location, pressure
Distance metric
Accuracy: 100%

Discussed that interaction with a smartphone's keyboard could offer a consistent data stream to authenticate the user continuously and transparently. Thus, a continuous authentication scheme using keyboard biometrics was implemented. Their scheme had created user profiles by using raw data. User profiles were n-gram approximations to model Markov processes. User profiles had optimized using a prefix tree that improves profile authentication computations. Their experiment on the Nexus 7 device with distance metric had achieved an accuracy of 80%, 90%, and 100% in 2, 3, and 4 seconds, respectively.

A parameterized model to select discriminating features on keystroke dynamics authentication on smartphones
https://dl.acm.org/doi/abs/10.1016/j.pmcj.2019.02.001

Mar 2019; Lee

22 users
time between key press and release, size, coordinate (x and y), mean, root mean square, sum of positive values, sum of negative values, standard deviation
MD
AR: 1% FRR: 11.111% EER: 6.0555%

Introduced a parameterized keystroke dynamics authentication approach for smartphones to improve the performance of authentication. The authors had designed the Android app on the Nexus 5X device and collected keystroke and motion behavioral samples from 22 users. The authors had extracted 62 features from keystroke and 540 features from motion samples. Further, the authors had applied the feature selection method on extracted features, such as median and interquartile range (IQR). Their approach had used the MD metric to train and test the normalized features. Their experiment on MD metric with tuned parameters ($\Gamma = 0.15$, $\Delta > 0.7419$) had achieved the best FAR of 1%, FRR of 11.111% and EER of 6.0555%.

User authentication on smartphones using keystroke dynamics
https://dl.acm.org/doi/abs/10.1145/3368691.3368725#:~:text=It%20is%20also%20known%20as,42%20users%20with%202142%20records.

December 2019; Hriez

42 users
Key hold time, Down-down time, Up-down time, Keypress pressure, Finger area, Average hold time, Average finger area, Average pressure and statistical features
RF
Accuracy: 94.26%

Presented a user identification approach based on keystroke dynamics of the smartphone. The authors had used a public dataset. Each user had typed two sessions of data. In both sessions, users had typed the same passphrase 30 times. The dataset had included 71 features, such as Key hold time, Down-down time, Up-down time, Keypress pressure, Finger area, Average hold time, Average finger area, and Average pressure. Besides, the authors had extracted 19 statistical features from the dataset. The authors had implemented NB, Bayesian Network, J48, k-NN, RF, and MLP classifiers for training and testing the features. The authors had evaluated their approach with a 10-fold cross-validation technique. With 71 features, their experiment had shown accuracy of 78.93%, 91.94%, 69.02%, 72.98%, 93.04% and 86.26% for NB, BN, J48, k-NN, RF and MLP, respectively. With 90 features, their experiment had achieved an accuracy of 80.81%, 92.48%, 72.41%, 70.59%, 94.26% and 87.49% for NB, BN, J48, k-NN, RF, and MLP, respectively. The authors had reported that adding statistical features improved the authentication accuracy of the smartphone user. Their approach had shown the best authentication results with RF classifier.

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9123909

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8024638

Keystroke Dynamics on Android Platform
https://www.sciencedirect.com/science/article/pii/S221201731500119X

2015; Antal

Comparing anomaly-detection algorithms for keystroke dynamics
https://ieeexplore.ieee.org/abstract/document/5270346

2009; Killouhry

PC keyboard data while typing password. 14 different outlier detectors used.

Scaled Manhattan, Nearest Neighbor, Outlier Count(Z-Score), OCSVM

Authentication of Smartphone Users Using Behavioral Biometrics
https://ieeexplore.ieee.org/document/7423666

02 March 2016; Alzubaidi

Motion based authentication

Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning
https://arxiv.org/abs/1708.09754

30 Aug 2017; Lee

35 users
Acc, Gyro (Mag, Ori, Light dropped for low Fisher score)
Time domain feature and Frequency domain features
KRR (what about change to SVR), SVM ok but much higher complexity
Accuracy: 98.1%, FRR: 0.9%, FAR: 2.8%

We segment the sensor data streams into a series of time windows, and compute statistics from both the time domain and the frequency domain (DFT) for the sensor data values in a time window.

Mean: Average value of the sensor stream
Var: Variance of the sensor stream
Max: Maximum value of the sensor stream
Min: Minimum value of the sensor stream
-Ran: Range of the sensor stream
Peak: The amplitude of the main frequency of the sensor stream (energy of sensor)
Peak f: The main frequency of the sensor stream
-Peak2: The amplitude of the secondary frequency of the sensor stream
Peak2 f: The secondary frequency of the sensor stream

For each feature, we test whether this feature derived from different users is from the same distribution. We use the Kolmogorov-Smirnov test (KS test) to test if two data sets are significantly different. accPeak2 f and gyrPeak2 f are “bad” features.
Next, we try to drop redundant features, by computing the correlation between each pair of features. We calculated the Pearson’s correlation coefficient between any pair of features. We drop Ran from our feature set.

Context: (1) The user uses the smartphone without moving (standing/sitting). (2) The user uses the smartphone while moving. (3) The smartphone is stationary (e.g., on a table). user uses it; (4) The user uses the smartphone on a moving vehicle. Contexts (3) and (4) are easily misclassified as context (1), since (1), (3) and (4) are all relatively stationary (e.g., when moving at a stable speed). So combined contexts (1), (3) and (4) into one stationary context, and left (2) as the moving context. Android: https://developer.android.com/guide/topics/location/transitions

Augmented PIN Authentication through Behavioral Biometrics

https://www.mdpi.com/1424-8220/22/13/4857

June 2022; Nereni, Favarelli, Chiani

12 users
PCA
5% EER for 4-digit PIN

RAW data, normalized

The smartphone movements are recorded during the PIN insertion through built-in motion sensors. Then, an anomaly detection-based system evaluates whether these movements represent an inlier (i.e., the smartphone owner typed the PIN), or an anomaly (i.e., an attacker typed the PIN). We implement and test our authentication method using four common anomaly detection algorithms: Principal Component Analysis (PCA), Kernel Principal Component Analysis (K-PCA), One-Class Support Vector Machine (OC-SVM), and Local Outlier Factor (LOF).

Accelerometer, Gravity, Gyroscope, Linear Acclereation, Rotation Vector (3D), Orientation sensor (deprecated sensor, taken only M = sqrt(pitch^2 + roll^2)), pressed digit. All sensors are sampled during a keystroke (pressing a digit). Anomaly detection is independently computed for every press and mean of all sequence is used after for final decision.

Before proceeding with the anomaly detection, the features (raw sensor data) are centered and normalized by subtracting the offset (mean) and dividing each row element-wise by the scaling factor (std).

~Using Feature Fusion Strategies in Continuous Authentication on Smartphones

https://ieeexplore.ieee.org/document/8979415

03 February 2020; Li

50 users
Acc, Gyro, Mag
Statistics features and Frequency features; CMIM feature selection
OCSVDD with RBF
BER: 1.47% (serial fusion), BER: 1.79% (parallel fusion)

mean, median, maximum, minimum, standard deviation, range, 25%, 50%, and 75% quartiles, kurtosis, and skewness; energy, entropy, peak1, freq_peak2, and peak2

Their experiment had investigated two feature fusion strategies: serial (Combine vectors into one long) and parallel feature fusion. No much difference, serial a bit better.

~Modeling interactive sensor-behavior with smartphones for implicit and active user authentication
https://ieeexplore.ieee.org/document/7947694

Linear acc + gyr

K-S test feature selection

Nice feature extraction, but uses activity aware context

-Implicit Sensor-based Authentication of Smartphone Users with Smartwatch
https://dl.acm.org/doi/10.1145/2948618.2948627

June 2016; Lee

Viz Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning; 2017

-A Behavioral Biometrics User Authentication Study Using Motion Data from Android Smartphones
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7870220

2016; Maghsoudi

60 users
Acc, Gyro
average, variance
MLP
Accuracy: 92.7%

Presented a behavioral biometric approach against malicious activity on smartphones using accelerometer and gyroscope data. Their experiment with MLP and SVM classifiers had shown the best accuracy than NB, k-NN.

-Mobile sensor-based biometrics using common daily activities
https://ieeexplore.ieee.org/document/8249001

08 January 2018; Yoneda

51 users
Acc, Gyro
Average Absolute Difference, Time Between Peaks, Average Resultant Acceleration, Binned Distribution, and Average
RF
Accuracy: 99.7%, EER: 9.3%

Presented a sensor-based user identification system on smartphones based on daily activities using accelerometer and gyroscope sensors.

-Sensor-based continuous authentication using cost-effective kernel ridge regression
https://ieeexplore.ieee.org/document/8367817

28 May 2018; Li

100 users (HMOG)
Acc, Gyro, Mag
Time domain feature and Frequency domain features
KRR-TRBF
EER: 3.0%

Feature used?

We are among the first to apply the data rotation augmentation approach on a continuous authentication system, which creates additional data based on the raw data from data collection and improves the robustness of the system. Then, 135 sensor-based features are extracted in both time and frequency domains within a time window on the augmented data. From these features, the most discriminable ones are selected by the minimum-Redundancy MaximumRelevance (mRMR), and with the selected features, we use the kernel ridge regression with truncated Gaussian radial basis function kernel (KRR-TRBF) to train the classifier in the enrollment phase.

Since the raw readings may contain abnormal values or missing values, the module processes outliers and fills missing values. More specifically, the values of a time window from the first to the fourth quartiles are removed in the training or testing data, and the missing values will be replaced by the latest previous values. Users may prefer their own ways holding the smartphones, and the sensors may generate non-diverse data for each user. By simulating different smartphone holding gestures for users, we apply rotation to the collected raw data to achieve data augmentation.

-Adaptive phone orientation method for continuous authentication based on mobile motion sensors
https://ieeexplore.ieee.org/abstract/document/8995241

13 February 2020; Wang

15 users
Acc, Gyro, Mag
-
OCSVM
FRR: 2.25%

Investigated how different phone orientations affect the performance of continuous authentication via motion sensors.

-Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing
https://www.sciencedirect.com/science/article/pii/S1084804518300717

2018; Ehatisham-ul-Haq

Recognizes smartphone users on the basis of their physical activity patterns using accelerometer, gyroscope, and magnetometer sensors of smartphone. Noise preprocessing.

Was de-noised using an average smoothing filter of size 1 x 3.

Acc, Gyr, Mag [x, y, z, M]

-Biometric authentication technique using smartphone sensor
https://ieeexplore.ieee.org/document/7429906

10 March 2016; Laghari

Using accelerometer of the smartphone, we have used the concepts of signal matching for identification mechanism

-SenSec: Mobile security through passive sensing
https://ieeexplore.ieee.org/abstract/document/6504251

Convert the raw sensory data into behavior text representation as sequences of behavior labels. Each behavior label is considered as a "word" in the language. We then train a continuos n-gram language model

-Multi-sensor authentication to improve smartphone security
https://ieeexplore.ieee.org/document/7509970

no preprocessing; using SVM

-Identifying Smartphone Users based on their Activity Patterns via Mobile Sensing
https://www.sciencedirect.com/science/article/pii/S1877050917317593

-ICAuth: Implicit and Continuous Authentication When the Screen Is Awake
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8761435

2019; Wu

142 users
Motion and Behavior Profiling
Flf
RF
Accuracy: 96.85%, FPR: 4.01%, and FNR: 2.95%

Malo podrobnosti, neco bezi na pozadi a sbira senzory

Their framework had captured raw data from fine-grained sensors (such as accelerometer, magnetometer, orientation sensor, and gyroscope) and coarse-grained sensors (which includes contextual information such as light, gait, proximity, and battery). The authors had extracted 200

features from raw data using the Gradient boosting decision tree (GBDT) algorithm. Further, the authors selected 50 best features using the fisher score ranking for user classification.

Secure privacy-preserving protocols for outsourcing continuous authentication of smartphone users with touch data
https://ieeexplore.ieee.org/document/6712742

2014; Govindarajan

Continuous Authentication based on Hand Micro-movement during Smartphone Form Filling by Seated Human Subjects
https://www.scitepress.org/Papers/2021/102258/102258.pdf

2021; Ray

Score level fusion of multiple modalities

Multimodal Multimodal continuous authentication

BB-MAS dataset

https://ieee-dataport.org/open-access/su-ais-bb-mas-syracuse-university-and-assured-information-security-behavioral-biometrics

Captures routine usage traits of the same user across different devices (desktop, tablet, and Android mobile phones). It involves several user behaviors while logging the data like sitting, walking on the corridor, and walking up and down a staircase. We are interested in authenticating users utilizing three modalities (from each dataset) namely acceleration, gyroscope, and swipe which are logged from mobile devices while each user is sitting and typing/writing.

An introduction to biometric recognition

https://ieeexplore.ieee.org/document/1262027

30 January 2004; Jain

Mostly talking about HW.

+You Are How You Touch: User Verification on Smartphones via Tapping Behaviors

https://ieeexplore.ieee.org/document/6980382

2014; Zheng, Bai

80 users

One class

Writing 5 predefined PIN in a loop (4-digit and 8-digit) with right index finger

All users used single device

Gyroscope, Accelereometer, Pressure, Size

Employ a simple outlier removal process to all the collected raw data (on long inter key). Between each key-press and key-release, we record raw data of timestamps, acceleration, angular acceleration, touched-size, and pressure.

Magnitude at down/up, max/min/mean during press. Key hold time and inter key interval.

Using the dissimilarity score between two feature vectors, we further verify if our extracted features of a user remain relatively stable over multiple repetitions, in comparison with those of the other participants.

As the first step, we compute a target user's template as an average feature vector over its N PIN tapping actions (N = 150). At the same time, each feature's standard deviation is computed based on these N actions. Suppose the new data sample's feature vector is X = {X1, X2, ..., Xi, ..., Xn}, where Xi represents the ith feature dimension; and the target user's template is represented similarly as T = {T1, T2, ..., T n}. The dissimilarity score is the accumulated deviation from the two vectors over all

$$D(\mathbf{X},\overline{\mathbf{T}}) = \sum_i \left\| \frac{X_i - \overline{T}_i}{\sigma_i} \right\|,$$

normalized features . By dividing σi, we give higher weights to those features that have smaller variation within the target user, because they more reliably reflect the target user's specific pattern. This is a standard procedure mostly seen in outlier removal (also known as standard score or z-score in statistics).

Decision is based on nearest neighbor – if min distance to trained data < threshold

~Touch Gesture Data based Authentication Method for Smartphone Users

https://dl.acm.org/doi/10.1145/2987386.2987410

October 2016; Park

94 users, single smartphone
Touch and Motion; Heuristic Search Procedure selection + correlation
FLF fusion
RF
EER: 0.7%, Accuracy: 90.64%

3s okoli vlevo vpravo

Each user draws a triangle 20 times on a touchscreen. Touchscreen data contain touching time, x-coordinate, y-coordinate, size of touch points and pressure values of each touch points. Accelerometer sensor and the gyroscope sensor are utilized to collect sensor data. Sensor data need to be collected and synchronized with touchscreen events. After the raw data are collected, 48 types of features are extracted from the data for classification.
We used Heuristic Search Procedure to select the whole set of features. Features whose correlation coefficient values are more than a certain threshold are eliminated. In order to choose a proper feature, the information gain (IG) score of each feature is calculated and the features are ranked with their IG scores

Author had evaluated Naïve Bayes, Logistic, MLP, simple logistic, SMO, J48, and Random Forest classifiers. RF classifier had achieved the best EER.

+Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns

https://ieeexplore.ieee.org/document/7791164

22 December 2016; Kumar

28 users, web browsing
Touch, and Motion; correlation feature reduction
FLF fusion
RF
Accuracy: 93.33%

+HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users

https://ieeexplore.ieee.org/document/7349202

2015; Sitova

100 users; free text typing
acc, gyro and (mag - poorly), touch , and keystroke; FS / MRMR
Scaled Manhattan with Fisher score ranking
EER: 7.16% (walking), and EER: 10.05% (sitting)

Captured hand micro-movements and orientation patterns through touchscreen, virtual keyboard, accelerometer, gyroscope, and magnetometer. The feature vectors trained and verified with Scaled Manhattan (SM), Scaled Euclidian (SE), and OCSVM classifiers.

During training, we evaluated two feature selection methods: Fisher score ranking, and minimum-Redundancy Maximum-Relevance (mRMR). Our preliminary experiments showed that Fisher score performed better for HMOG features, while mRMR performed well with tap features. For HMOG and tap templates, we evaluated the interquartile outlier removal (i.e., different subsets of the values from the first and fourth quartile are removed). Experiments with SM verifier showed that outlier removal does not improve authentication accuracy. Our motivation for using PCA are: (1) to remove correlation between features to meet the assumptions in SE and SM, and (2) to reduce dimensionality by using only those principal components, which explain most of the variance

Evaluating multi-modal mobile behavioral biometrics using public datasets
https://www.sciencedirect.com/science/article/pii/S0167404822002620

August 2022; Ray-Dowling, Hou

Acc, Gyr, Swipe

Pracuje nad dvěma dostupnými datasety. Porovnává využití dat ze senzorů s dotyky (v době dotyku, nonstop). Porovnává dva různé features vectory. Používá SLF. Neřeší rychlost ověření, dobré výsledky kvůli velkému oknu.

There are two cases of feature extraction from such motion events. In the first case we extract features from a time window of 500 ms. However, in our pilot studies, we try 50 ms, 100 ms, 200 ms, and 500 ms time windows where 500 ms produces the best results. The second case is driven by the availability of swipes where features are extracted from all the motion events that fall within each swipe. In both cases, we extract three kinds of features:

- medians of the motion events
- 2017; Shen features
- HMOG features

In case of swipes, we have extracted Frank et al.s (2012) Touchalytics features (Frank et al., 2012), which measure the distance, movement, and temporal attributes of swipes.

We do not perform any feature selection method because we want to evaluate the public data on the entire feature set as proposed and experimented in the original state of art.

We train an SVM classifier for each of acceleration, gyroscope, and swipe modalities for both datasets. Using SVM (OC RBF, BC RBF), we perform score-level fusion for single modality-based authentication and likelihood ratio-based score fusion to combine multiple modalities. We split each user's data into training and testing sets. A 10-fold shuffling is performed. We train the SVM using one genuine user and 50% random users from the impostor set.

We perform grid searches to tune several parameters: k (sliding window: these are the number of the consecutive scores generated by an SVM per modality which are fused by averaging the distance scores to reach a final decision); n (step size of k); binary SVM parameters C and gamma; one-class SVM parameters gamma and nu; the Kg (genuine Gaussian components) and Ki (impostor Gaussian components) in the likelihood ratio-based score-level fusion.

In the single modality experiment, we utilize swipe data and train one binary SVM per user to measure the authentication performance of that genuine user against all impostors. To improve the performance, we apply a score-level fusion by averaging the distance scores of k consecutive swipe readings (scores) from the binary classifier and calculate an EER for each user.

Likelihood Ratio (LR)-based Fusion for multiple modalities. First we train an SVM classifier for each of acceleration, gyroscope, and swipes. In case of the two modalities fusion, we take the two dimensional vectors of match scores of acceleration and gyroscope from their respective SVM classifiers and create genuine and impostor distributions. Similar genuine and impostor distributions

are created during the fusion of all three modalities (acceleration, gyroscope, and swipes). LR, which is defined as the ratio of the genuine to the impostor distribution, is then used as a new match score for a test sample.

LR fusion: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4359389

Fusion can be performed at four different levels of information -- sensor, feature, match score, and decision levels. Score fusion techniques can be divided into the following three categories:

- Transformation-based score fusion: scores are first normalized to a common domain and then combined. Choice of the normalization scheme and combination weights requires extensive empirical evaluation
- Classifier-based score fusion: Scores from multiple matchers are treated as a feature vector and a classifier is constructed to discriminate genuine and impostor scores
- Density-based score fusion: based on the likelihood ratio test and it requires explicit estimation of genuine and impostor match score densities

Consider K different matchers, and $X = [X_1, X_2, \ldots X_K]$ their scores.

Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication

https://ieeexplore.ieee.org/ielaam/10206/8114524/8006292-aam.pdf

2017; Shen

102 users
Acc, Gyro, Mag, Ori
Descriptive features and Intensive features; relative MI between the feature fi and a user's identity
HMM
EER: 4.74% (hand-hold), EER: 6.64% (table-hold), and EER: 9.73% (hand-hold-walk)

Data ze senzorů v době dotyku. Zajímavé příznaky.

To quickly and accurately characterize users' touch habit by sensor behavior, we focus on the behavior of four motion sensors from touch-tapping and single-touch-sliding actions, which contain the behaviors from accelerometer, gyroscope, orientation, and magnetometer.

Gravity Filtering.

Wavelet De-noising: A sensor signal usually contains non-stationary noise, which makes signals exhibit multiple peaks. This would lower the accuracy of feature modeling for authentication. Thus we applied a wavelet-based de-noising method to mitigate the signal mutation, instead of the traditional Fourier analysis method, since the latter converts a signal in the frequency domain at a certain time point, but the mutation and noise usually affect the entire spectrum of the signal.

- select suitable wavelet functions to decompose the signals into N levels, and extract low-frequency coefficients of every level and high-frequency coefficient of the Nth level
- employ threshold analysis to filter decomposed signals
- use an inverse wavelet transform on the filtereddecomposed signals to reconstruct the original sensor signal

Features: For each touch action, we first extract four sensors' data in the duration of that action, and obtain three data sequences for each sensor, which respectively represent the data from the (X, Y, Z) axes of that sensor.

Then we characterize these data sequences by two feature sets: descriptive features and intensive features. Descriptive features characterize the motion patterns of touch actions with meaningful statistics. For instance, the range of a y-axis gyroscope series. Intensive features depict the intensity and complexity of touch actions. For example, the energy of a sensor-data sequence is calculated by summing up the squared magnitudes of FFT (Fast Fourier Transform) components, which is a metric of action intensity; the entropy of a sensor-data sequence is calculated with Shannon entropy, which measures the complexity of a touch action.

Mutual information and Fisher Score for feature ranking.

Along with the preliminary analysis of the distribution of sensor-event timings, the process appears to be stochastic and is best analyzed as a Markov process. Thus the Hidden Markov Model (HMM) employed.

~Increasing Accuracy of Hand-Motion Based Continuous Authentication Systems

https://ieeexplore.ieee.org/document/8796725

15 August 2019; Bhattarai

100 users (HMOG)
Acc, Gyro
Mean, standard deviation of readings during the tap, difference in before and after tap, difference of the readings during before the tap
fuzzy OCSVM
EER: 5.8% (for walking) EER: 3.7% (for sitting)

Selection: We used four filter based approaches: Fisher score, Chi-Square, F-score, and Gini Index. With Forward Selection One Class SVM

Identified that one-time authentication methods could be susceptible to masquerade attacks. The results of their experiment on fuzzy OCSVM with feature selection technique had obtained the lowest EER as 5.8% and 3.7% for walking and sitting, respectively.

--- feature selection: https://dl.acm.org/doi/10.1145/3136625

The fuzzy membership value is a real number between 0 and 1 and it accounts for the membership of a training point towards the class

The fuzzy membership is defined as a function of distance between the class center and the data point, i.e., each data points is assigned weights based on its distance from the class center and using these weights, SVM creates an optimum hyperplane.

~A continuous smartphone authentication method based on gait patterns and keystroke dynamics

https://link.springer.com/article/10.1007/s12652-018-1123-6

2018; Lamiche

20 users
gait and keystroke dynamics; sequential floating forward selection
FLF
MPL
FAR: 1.68%, FRR: 7%, EER: 1% and Accuracy: 99.1%

Used keystroke dynamics. The raw data from the accelerometer sensor had resampled through linear-interpolation that corrects the uneven time interval issues. Their approach had used a feature level fusion method to combine both modalities that generate the final feature vector. Further, they had implemented the SFFS algorithm, which minimized redundant features and computational complexity. The authors had evaluated SVM, RF, random tree (RT), NB, and MLP classifiers with 10-fold cross-validation technique. The authors reported that change of user environmental conditions not affected the performance of the system. Further, the authors had tested their framework against Zero-effort attack, and Minimal-effort mimicking attack.

~AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones

https://www.sciencedirect.com/science/article/pii/S2214212618304435

February 2019; Buriro

85 users
Mean, Standard Deviation, Skewness, Kurtosis; correlation-based feature selection + Attribute Selected Classifier
FLF
RF
TAR: 99.35%

Additionally, we applied High Pass Filter (HPF) and Low Pass Filter (LPF) to obtain HPF and LPF acceleration readings. By applying HPF, we obtained exact acceleration applied on the device by the user, and by LPF, we obtained the apparent transient forces acting on the device due to the users' activity. Thus, we used 3 variants of accelerometer sensors, i.e., Raw, LPF and HPF

Data from accelerometer, gyroscope, gravity, magnetometer, and touchscreen sensors in several postures: sitting, standing, and walking. The authors had extracted 97 and 31 features from phone-pickup movement behavior and touch-based slide-to-unlock, respectively. The authors had combined these features using feature-level fusion. To avoid redundant features, they had used a correlation-based feature selection (CFS) technique. Moreover, they had used Attribute Selected Classifier (ASC) to perform in parallel both features selection and automatic classification. The authors had implemented six base classifiers: BayesNET, NB, SVM, k-NN, J48, and RF.

~DAKOTA: Sensor and Touch Screen-Based Continuous Authentication on a Mobile Banking Application

https://ieeexplore.ieee.org/document/9367144

2021; Incel

45 users

Touch, mag, gyr, acc; sequential backward selection

Vypadá to že řeší jen scrolls

126 features for each scroll event. PCA, Before applying PCA, we also normalized the features using min-max scaling since their ranges were different from each other. we also applied feature selection to see each feature's importance in the biometric model of each user. We compare the results with the selected features to the results when PCA is used to transform features. We applied the sequential backward selection method

~A Framework for Continuous Authentication Based on Touch Dynamics Biometrics for Mobile Banking Applications

https://www.researchgate.net/publication/352562061_A_Framework_for_Continuous_Authentication_Based_on_Touch_Dynamics_Biometrics_for_Mobile_Banking_Applications

June 2021; Estrela

51 users (25 users for evaluation); m-bank simulator

Sensors: accelerometer, gyroscope, magnetometer, orientation, linear acceleration, and gravity (axs)

Touch: DD, DU, UD, UU, Avg DU, Pressure, Avg Pressure, Size, avg size

Login: (1) Capture location and password typing / interaction; (2) Calculate accuracy for the location pattern and calculate F1 score for the password typing pattern / interaction – two models involved. (3) Fuse the two models output by finding its mean. (4) Generate alert if score <90%.

For the creation of a feature ranking, the Random Forest (RF) algorithm was used.

Models: Random Forest, Support Vector Machine, Extreme Gradient Boosting, Gradient Boosting, Naive Bayes Bernoulli, Naive Bayes Gaussian. OCSVM only for location pattern.

RF, NBG best results

Continuous user identification via touch and movement behavioral biometrics

https://ieeexplore.ieee.org/document/7017067

2014; Bo, Zhang

"sellf learning"

Tiny perturbation of the whole device will be captured by motion sensors when a user touches the screen.

BrainRun: A Behavioral Biometrics Dataset towards Continuous Implicit Authentication
https://www.mdpi.com/2306-5729/4/2/60

2019; Papamichail

2218 users; playing brain run Dataset

-Continuous Authentication Using One-class Classifiers and their Fusion
https://arxiv.org/abs/1710.11075

2018; Kumar

Compares the performances of several one-class classifiers (OCC) with binary classifiers (BC). Among experiments performed on individual OCC, BC and fusion of multiple OCCs, the kNN (k-Nearest Neighbor) BC produces the best result of 94.22% accuracy.

It is possible to build behavioral biometrics-based continuous authentication systems without using samples from impostor class. Such systems can be implemented by using OCC and their fusion. The SV 1C and LOF achieved comparable error rates and outperformed half of the eight MCC. The fusion of OCC could not improve the performance of the system significantly.

S3: An AI-Enabled User Continuous Authentication for Smartphones Based on Sensors, Statistics and Speaker Information
https://www.mdpi.com/1424-8220/21/11/3765

Cely framework

An HMM-based multi-sensor approach for continuous mobile authentication
https://ieeexplore.ieee.org/document/7357626

2015; Roy

Implement an HMM (Hidden Markov Model)-based multi-sensor system, which is evaluated on their own dataset of 42 volunteers. The user activity includes reading Wikipedia articles and filling out a questionnaire through which they log modalities like swipe, tap, acceleration, and gyroscope.

-A flick biometric authentication mechanism on mobile devices
https://ieeexplore.ieee.org/document/7281144

2015; Shih

-Evaluation of Motion-Based Touch-Typing Biometrics for Online Banking
https://ieeexplore.ieee.org/document/8053504

2017; Buriro

-Touch to Authenticate — Continuous Biometric Authentication on Mobile Devices
https://ieeexplore.ieee.org/abstract/document/7812943

2015; Temper

-At Your Fingertips: Considering Finger Distinctness in Continuous Touch-Based Authentication for Mobile Devices
https://ieeexplore.ieee.org/document/7527779

04 August 2016; Ali

6 users, reading and browsing pictures
Motion (acc), Touch
SLF fusion
SVM with RBF
Accuracy: 98%

To rika jen ze je fajn pridat accelerometer

-Adaptive Threshold Scheme for Touchscreen Gesture Continuous Authentication Using Sensor Trust
https://ieeexplore.ieee.org/document/8029487

2017; Smith-Creasey

6 users
Touch, Motion, and Behavior Profiling
Slf
Rf
FRR: 5.64%, FAR: 5.59%

Uses anchors (category based on time of day and location). Data collected on the background nonstop on kernel level.

Implemented an adaptive continuous authentication framework on smartphone using touchscreen sensor, inertial sensors, proximity, ambient lighting, gravity, pressure sensor, Wi-fi, Bluetooth, cellular, user activity, and GPS data. The authors had created user profiles using behavioral data and constructed the kernel density estimation (KDE) and histograms 5-fold cross-validation technique for training each anchor. Their framework had adopted a RF classifier. Their experiment with an adaptive threshold scheme with activity anchors on the MSC dataset.

-CASTRA: Seamless and Unobtrusive Authentication of Users to Diverse Mobile Services
https://ieeexplore.ieee.org/document/8399501

2018; Shila

15 users
Gait, and Behavior profiling
SLF
K-means clustering, OCSVM and RF

Detection rate: 99%

Captured behavioral profiling trait to record location and mobility patterns. The authors had recorded STILL, IN-VEHICLE, and WALKING.activities. The authors had implemented K-means clustering to learn location and mobility patterns, OCSVM to learn gait patterns, and RF to learn physical proximity patterns. Their experiment with adaptive and weighted trust score fusion had manifested 99% detection rate.

Deep Learning

A SIAMESE NEURAL NETWORK FOR BEHAVIORAL BIOMETRICS AUTHENTICATION
https://openreview.net/pdf?id=MG8Zde0ip6u

Towards continuous authentication on mobile phones using deep learning models
2019; Volaka

Deepauth: A framework for continuous user re-authentication in mobile apps
2018; Amini

Risk-driven behavioral biometric-based one-shot-cum-continuous user authentication scheme
2021; Buriro

Learning human identity from motion patterns
2016; Neverova

Actions speak louder than (pass) words: Passive authentication of smartphone users via deep temporal features
2019; Deb

AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors
https://ieeexplore.ieee.org/document/9007368

24 February 2020; Abuhamad

84 users
Acc, Gyro, Mag , Ele
Multi-LSTM model
EER: 0.09

Addressed that point-of-entry authentication methods were compromised with several vulnerabilities. Thus, the authors introduced a deeplearning-based continuous authentication. The authors had implemented the RNN with LSTM models and evaluated with different LSTM units ranging from 16 to 256.

SCANet: Sensor-based Continuous Authentication with Two-stream Convolutional Neural Networks

https://dl.acm.org/doi/10.1145/3397179

2020; Li

100 users for own dataset + 82 BrainRun

Investigating the combination of acceleration and gyroscope over one-class SVM, they achieve an EER of 2.35% as the best performance on their own dataset.

Smartphone Continuous Authentication Using Deep Learning Autoencoders

https://ieeexplore.ieee.org/document/8476929

30 September 2018; Centeno

100/20 users
Acc
-
Deeplearning auto encoders
EER: 2.2%

Discussed that the real applicability of earlier works (+3) on continuous authentication had limited due to less recognition rate. Their approach had implemented deep learning autoencoders.

Mobile Based Continuous Authentication Using Deep Features

https://www.sigmobile.org/mobisys/2018/workshops/deepmobile18/papers/Mobile_Based_Continuous_Authentication.pdf

Continuous Authentication using Inertial-Sensors of Smartphones and Deep Learning

https://hdms.bsz-bw.de/frontdoor/deliver/index/docId/6506/file/Masterthesis_BuechHolger_20190628.pdf

https://github.com/dynobo/ContinAuth

Attacks

Smudge attacks on smartphone touch screens

Beware, your hands reveal your secrets!

A pilot study on the security of pattern screen-lock methods and soft side channel attacks

Boosting the guessing attack performance on android lock patterns with smudge attacks

On the effectiveness of pattern lock strength meters
https://link.springer.com/article/10.1007/s11042-022-13245-9#Sec19

__ Uvodni kecy

Continuous and transparent multimodal authentication: reviewing the state of the art
https://dl.acm.org/doi/10.1145/3025453.3025461

On the practicality of motion based keystroke inference attack
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.298.6345&rep=rep1&type=pdf

2012; Cai, Chen

Android Smudge Attack Prevention Techniques

A formal classification of internet banking attacks and vulnerabilities.

E-banking Overview: Concepts, Challenges and Solutions.

Defending Touch-based Continuous Authentication Systems from Active Adversaries Using Generative Adversarial Networks
https://arxiv.org/abs/2106.07867

https://github.com/midas-research/GANTouch-TBIOM/

2021; Agrawal

Resource

Resource Usage Analysis of a Mobile Banking Application using Sensor-and-Touchscreen-Based Continuous Authentication
https://www.scilit.net/article/77535f2097ec7c0e9da70bbf6e6295f7

Adaptive

Adaptive Algorithms in Accelerometer Biometrics
https://ieeexplore.ieee.org/document/6984853

Long time influence
https://www.semanticscholar.org/paper/Long-term-influence-of-user-identification-based-on-Watanabe-Kun/b413b46372fcddf540df352b05f3b8c2825f03e4

Pitfall

Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics
https://dl.acm.org/doi/pdf/10.1145/3052973.3053032

2017; Oxford

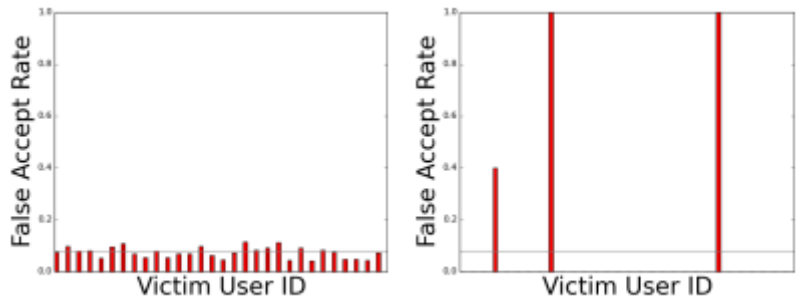
However, this process of optimizing the mean ERR often overlooks the security implications of different distributions of these errors, which may even lead to reduced security. There is a big difference between random errors (that will prolong, but not prevent the eventual detection of an attacker) and systematic errors (that can lead to an attacker perpetually escaping detection).

Blind optimization of the EER might also lead to unrealistic expectations regarding the system's real-world performance

As systems are usually evaluated on a static dataset, training, operation and the presence of attackers have to be simulated based on this data. Authors frequently choose to sample training data

randomly from the entire set, which would not be possible in actual operation. In addition, authors often include some data of the eventual attacker in the negative class, a decision which is unrealistic outside of some insider threat environments.

Continuous authentication provides a unique challenge as errors accumulate over the runtime of the system. Without knowing the exact distribution, an FAR of 10% could signify all attackers being detected 90% of the time (resulting in eventual detection), or 10% of the attackers never being detected while all others are exposed immediately (called systematic false-negatives).



(a) Random Errors (b) Systematic Errors

These types of errors are more problematic from a security perspective, as the undetected attackers can then access the compromised system for a virtually unlimited time.

Attacker Model: A common choice is to train a binary classifier with one user's samples as the positive class and samples from all other users as a single combined negative class. In practice, it is impractical to assume that reference data for each potential attacker is available and including this data may lead to overestimating the classifier's performance. A different approach trains a generic attacker model from other users (again, combining them into a negative class), but withholding samples from the actual attacker. A more straight-forward approach is to perform anomaly detection, new samples are then classified.

Selection of Training Data: The first part of the recorded data as training data, and the remaining samples as test data.

Sample Aggregations: Single measurements of a feature vector are often noisy. Samples can either be combined before classification (e.g., by computing the component-wise mean of several feature vectors) or afterwards (e.g., by majority votes).

A Gini Coef of 0 indicates a maximal equality of values (i.e., every resident having the same income), while a value close to 1 represents maximal inequality (i.e., one resident earning all the income).

In some scenarios, adding distinctive features could actually reduce the security of a system, despite the lower average error, by adding systematic false negatives. As a result, researchers should take great care to not blindly strive for the lowest average EER but to also take into account how changes to features or classifiers influence their system's error distributions.

Common Evaluation Pitfalls in Touch-Based Authentication Systems

https://www.semanticscholar.org/reader/cbf6956df6ce82d5c3cdd66c143565378d9d62d8

1) Small Sample Size (limited number of users; missing longitudinal data). Availability of long term data does not affect EER in a significant way. Increasing the number of users in the model has a non-negligible effect on the EER: while we obtain EER=9.14% for n=40, increasing the number of users has a large benefit, reaching EER=8.41% for n=400

2) Phone models mixing: Different phone for training (victim would use same phone). Combined (not divided phone models) approach leads to an overestimation of performance. Swipes belonging to similar phone models tend to be more similar. It is undesirable to mix different phone models in data collection

3) Non-contiguous training data selection: using randomized training instead session dedicated

- Random? Merge all user data and choose randomly for train/test
- Contiguous? Combine samples – first portion for train, reminder for testing
- Dedicated Session? Choose some session for training, some for testing
- Intra Session? Choose session, half of the session for train, second half for test

Performance seems to be overestimated compared to the most realistic dedicatedSessions

4) Attacker data in training: nonrealistic; clarify the negative class consists of legitimate users

- Exclude Attacker? Divide other users into two groups, one for train, second for test
- Include Attacker? Divide other users into two groups, test/train both

The fewer users are considered, the more the presence of attacker data impacts the classifier. IncludeAtk can lead to an artificial performance gain of between 0.3% and 6.9%

https://www.semanticscholar.org/paper/Evaluating-Behavioral-Biometrics-for-Continuous-and-Eberz-Rasmussen/2b3ee94ac514ac49b457dcfac7a9be6f0faf661d

5) Aggregation window size – aggreagting multiple swipes gives attacker time in the window

Increasing the aggregation window size leads to lower EERs: an EER of 8.2% obtained on single swipes drops more than a quarter (5.9%) when aggregating two swipes, and drops to less than 3% at 12 swipes.

Scaling - The training and testing samples of both the user and the attackers are scaled by subtracting the mean and dividing by the standard deviation of this training data. Positional feature normalized to the screen resolution.

Classification - Following scaling, we fit a classifier to our training data for each user. We then classify the samples in the testing set, which gives us a probability for each sample. This probability is in turn used for both sample aggregation and threshold selection.

Sample aggregation - For this optional step, instead of treating samples independently, we group a set of consecutive samples together and take their mean probability estimation

Threshold selection - Taking the distance scores for the testing samples (both user and attacker samples), we compute the EER for each user. This is done by finding the distance score threshold where the FAR and FRR are equal. The mean EER for a given systém is the average EER across all users

Code + Data

https://github.com/ssloxford/evaluation-pitfalls-touch