The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 5 (2019) 16–20

www.elsevier.com/locate/icte

DriverAuth: Behavioral biometric-based driver authentication mechanism for on-demand ride and ridesharing infrastructure

Sandeep Gupta, Attaullah Buriro*, Bruno Crispo

DISI, University of Trento, Trento, Italy

Received 13 September 2017; accepted 24 January 2018
Available online 3 February 2018

Abstract

On-demand ride services and the rideshare infrastructure primarily focus on the minimization of travel time and cost. However, the safety of riders is overlooked by service providers. For driver authentication, existing identity management methods typically check the driving license, which can be easily stolen, forged, or misused. Further, background checks are not performed at all; instead, social profiles and peer reviews are used to foster trust, thereby compromising the safety and security of riders. Moreover, the present mechanism seems ineffective in discontinuing a malicious driver from offering the services. In this paper, we present DriverAuth—a fully transparent and easy-to-use authentication scheme for drivers that is based on common behavioral biometric modalities, such as hand movements, swipes, and touch-strokes while the drivers interact with the dedicated smartphone-based application for accepting the booking. A preliminary study of behavioral biometric-based approaches offers a usable verification mechanism on smartphones that could be a potential solution to improve the safety of riders in the emerging on-demand ride and the rideshare infrastructure.

Keywords: On-demand ride infrastructure; Smartphones; Human factors; Rider safety

1. Introduction

On-demand rides and the rideshare infrastructure are innovative means for people to reserve various transportation options readily and as needed, using their smartphones. Uber, Lyft, and BlaBlaCar are gaining immense popularity among consumers despite some misdeeds [1] reported against them, such as assaults or abuse towards riders. The reason behind their popularity is primarily the convenience and cost-effectiveness, i.e., from the rider's perspective, it is easy and convenient to book a ride from their smartphones. While this infrastructure has improved the quality of life of riders, it has also raised concerns about the rider's safety. Service providers offer the services by means of smartphone-based applications and assume that users have identified themselves correctly while using it. In the case of any unforeseen incidence, service providers have to typically rely on the information provided by the driver, which might be false (typically, the human factors) owing to their unclean police record [2].

The most common form of verification used by service providers is based on the documents issued by the government [3]; however, these documents can be forged easily. Inadequate background checks on the drivers by the service providers compromises the safety of riders which is no longer an issue of drivers who act maliciously.[1]

Modern identity management solutions, e.g., trust-based mechanisms [4], can be designed by integrating popular social network platforms such as Facebook, LinkedIn, Twitter, and Google+. However, many privacy-conscious users are not so keen on sharing all their movements and actions on social networking sites [5]. Moreover, a fraudulent driver could easily

* Corresponding author.
E-mail addresses: sandeep.gupta@unitn.it (S. Gupta), attaullah.buriro@unitn.it (A. Buriro), bruno.crispo@unitn.it (B. Crispo).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

[1] https://www.recode.net/2017/11/14/16647706/uber-class-action-lawsuit-riders-sexual-assault-rape-violence-background-checks.

https://doi.org/10.1016/j.icte.2018.01.010

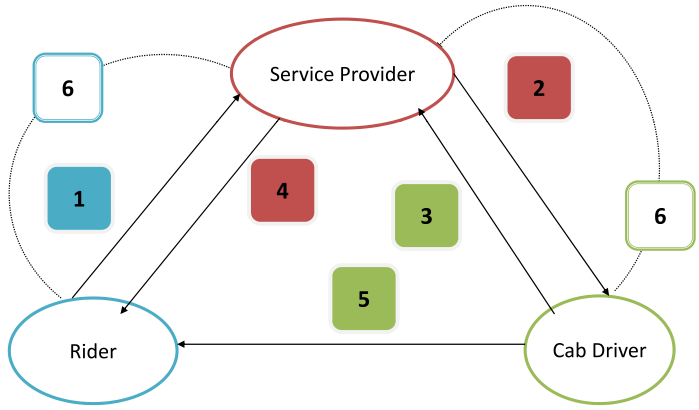

Fig. 1. App-based booking system.

create a fake profile on these social network platforms [6], defeating the whole purpose of this form of authentication.

Using biometrics for a driver's authentication becomes an interesting and feasible option especially owing to the increased popularity of mobile applications as a common method to access these services.

In this paper, we propose a seamless and transparent authentication scheme to verify the drivers remotely that can be easily integrated to the service providers' dedicated smartphone applications. The scheme exploits the driver's interactions with the smartphone while accessing the rideshare application to accept a new booking request. We assume that during the interaction, the drivers hold their smartphones in their hands and/or tap or navigate through the application to view the booked rides. The proposed scheme profiles the hand movements, taps, and swipes to profile the driver. Later, the service provider uses that information to verify the identity of the drivers.

The main contributions of the paper are listed below:

1. The introduction of seamless and transparent authentication scheme, DriverAuth, based on person-specific behavioral biometrics, i.e., hand movements, swipe gestures, and touch typing, collected during the interaction with the dedicated application, to accept a new booking request.
2. The proposal for proactive management by service providers by recording and associating a driver's misconduct if reported with their behavioral-biometrics-based identity establishment mechanism.

2. Design goals

We propose a seamless and unobtrusive behavioral-biometric-based driver authentication scheme. The idea is based on the fact that the drivers need to interact with the application to facilitate the rides booked by people. In the course of this interaction, the drivers are supposed to navigate, swipe, and/or touch type, through the dedicated application. All the smartphones currently available in the market are equipped with sensitive sensors, i.e., accelerometer, gyroscope, touchscreen, etc. These sensors are used to collect movements and touch-based data to profile the very-specific user behavior. Our server-based authentication scheme collects the gestures, i.e., hand-movement, touch type, and swiping, of a driver transparently, during their interaction with the application, to prepare their profile, and uses the gestures to train the classifier. After reaching the sufficient number of training observations, it notifies the service provider about the availability of the behavioral biometric modality for the identity confirmation of drivers and riders.

DriverAuth offers the advantages as follows.

i. **Transparency**: the proposed authentication scheme is fully transparent, as all the authentication steps are performed in the background.
ii. **No requirement of additional hardware**: the scheme uses the existing built-in hardware available in all commercially available smartphones on the market today.
iii. **Higher Security and Usability**: the proposed scheme is secure by mimicking the very personal invisible phone movements and touch timings, and swiping is difficult. The scheme is highly usable as well because it performs its operation in the background without bothering the drivers.

3. App-based ride booking system

3.1. System overview

In spite of different service providers have their own dedicated application for the users but the core functionalities are common in those applications. We refer to this core in the rest of the paper when we mention about the application. The application-based on-demand ride-booking system primarily consists of three stakeholders, i.e., (a) the service provider, (b) the rider, and (c) the driver, as shown in Fig. 1.

The interaction among these three stakeholders is described as follows:

1. A customer accesses the application and types the destination where he/she wants to go at a particular time. The service provider accepts the request from a customer and fetches his/her credentials, i.e., name, location, mobile number, address, and other ancillary data.

2. The service provider checks the availability of a driver in that area or nearby and informs an available driver to pick up the customer from the location at the time requested with the customer details.
3. The driver acknowledges the service provider for accepting the ride.
4. The service provider notifies the customer and messages the cab number, arrival time, and the driver's details.
5. The driver calls the customer typically 15 min prior to the pick-up time to confirm the rider's location.
6. Both the customer and the driver can share their feedback about each other to the service provider.

3.2. Threats posed by human factors

In this system, the identity of the drivers and the riders is hidden in their smartphones. Anyone possessing a stolen smartphone can pose a threat to any of them, besides the vehicle security. We explain the possible threats, involving human factors, associated with the on-demand ridesharing systems.

(1) **The cab-driver**: The business model allows a person over 21 years with at least one year of driving experience to become a commercial driver. Any driver with a valid driving license and proof of vehicle registration and insurance can become eligible to drive a 4- or 6-door vehicle and can register freely [7] to become a driver. Several misdeeds have been reported where the drivers assaulted or abused the riders. Similarly, a person with malicious intentions can impersonate a legitimate driver by stealing/cloning his smartphone without the knowledge of the service provider and can be a threat to riders.

(2) **The rider**: A person with hideous intentions can pose a threat to the driver or could be a prankster who books the ride just for fun. The service providers with existing identification methods would most likely not be able to track such a person with hideous intentions who can pose a threat to the driver or could be a prankster who books the ride just for fun. The service providers with existing identification methods would most likely not be able to track such a person and deny them the chance to repeat their prank. The authentication system that we propose for drivers can be applied to the riders' authentication as well. However, while drivers have a contract and an incentive to enroll in our authentication method, riders, especially if one-shot, may object based on privacy concerns. This limitation to the voluntary use of our scheme can be overcome by explaining the advantages in the security increase of all ecosystems and also the introduction of some incentive schemes to early adopters.

This business model lacks usability and a secure authentication mechanism, where the service provider could discontinue a driver who misbehaves with the rider, as he/she could either seek employment from similar or other service providers or reapply using fake identification. Similarly, the provider is unable to distinguish between a genuine rider and a prankster or someone who misbehaves with a driver earlier and is seeking the ride again.

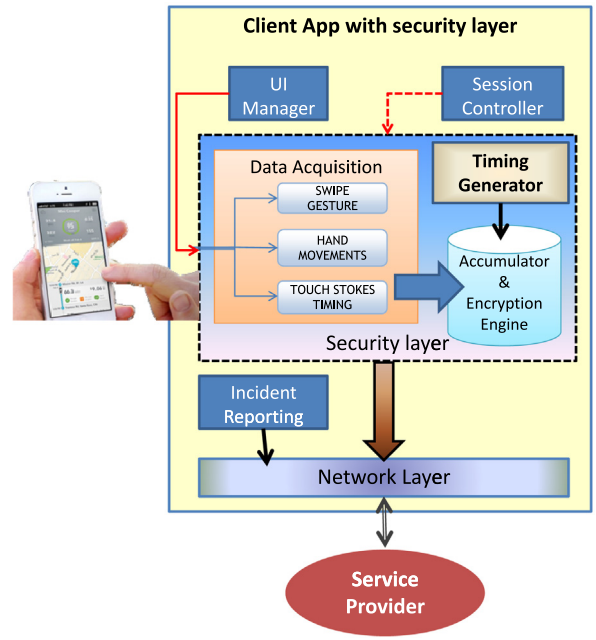

Fig. 2. Client app with security layer.

4. The solution

Our solution, DriverAuth, uses the client–server architecture. In our scheme, we stitched a transparent security layer at the client side, capturing various behavioral biometrics modalities including the hand movements [8], swipe and hand-movement gestures [9,10], and touch-stroke timing differences [8,11], while the user holds the phone and interacts with the on-demand rideshare application. Simultaneously, the captured data is processed at the server side to establish the identity of the driver and to maintain the historical data of any misbehavior if reported against the driver.

4.1. Client application

In our experiment, we collected three modalities, namely, hand movements, swipe gestures, and touch-stroke timings unobtrusively and successfully identified and distinguish between the users. The client application is extensible to include other modalities as well and in the future, we will include the gait, grip, voice, and other behavioral modalities.

In the client application, we stitched a security layer consisting of a data acquisition module, an accumulator/encryption engine, and a timing generator along with the incident reporting module as shown in Fig. 2. As soon as the user starts interacting with the application, the session manager invokes the security layer. The data acquisition activates the required sensors to collect the required data of the modality as determined by

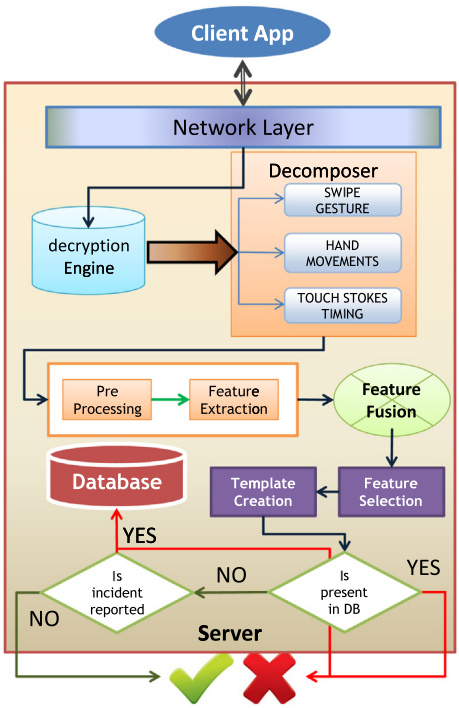

Fig. 3. Server application.

the User-Interface (UI) manager and transfers the data to the accumulator and encryption engine for the set duration. The accumulator stores the data collected from various sensors and the encryption engine encrypts this data using industry standard encryption algorithm. Once sufficient data is collected, it is packetized and sent to the network layer. The network layer sends the data to the service provider for further processing to establish the identity of the user.

4.2. Server application

Fig. 3 shows the main components of the server application. It primarily consists of (1) a decryption engine, (2) a decomposer, (3) a signal preprocessing and feature-extraction module, (4) a feature fusion, (5) a feature selection, (6) a template creation, and (7) a database.

The decryption engine decrypts the user data as received from the client application. The data stream is decomposed into individual modalities i.e., hand movements, swipe gestures, and touch stroke for the preprocessing of raw data and various statistical features, such as mean, standard deviation, skewness, and kurtosis that are extracted for each individual modality. As the proposed scheme used the multimodal mechanism, the features are fused and selected based on merit entailing the selection of only the productive features for user identification. The drivers' template is created based on the selected feature subset and is then stored in the main database as the training template. Subsequently, the similar procedure is applied to the testing data to formulate the testing template and is matched with the training samples to verify the identity of the claimant.

Table 1
Behavioral biometrics modalities.

Modalities	Data collected	Sensors/APIs used
Hand movements (User holds the smartphone)	Time-offset, x-y-z acceleration, x-y-z gyroscope	Real-time clock, accelerometers, gravity, magnetometer, orientation, gyroscopes sensors
Swipe gesture (User swipes on the screen)	Time offset, x-y position, pressure, size	Real-time clock, touchscreen Velocity tracker
Touch-strokes (User typing)	Time intervals, track velocity	Real-time clock, touchscreen

Whenever a user interacts with the client application, the input sample is compared with the template stored in the database, which was created during the training phase and for the purpose of matching, standard machine learning classifiers are used. Hence, the driver is authenticated based on their behavioral patterns. The authentication mechanism is transparent to the driver, and their data becomes extremely easy to collect since their permission or cooperation is not required. Additionally, the person-specific invisible biometric behaviors become extremely tedious to impersonate.

4.3. Behavioral biometrics modalities description

DriverAuth leverages all the available 3-dimensional sensors i.e., the accelerometer, the gravity, the orientation, the magnetometer, and the gyroscope along with the touchscreen. In addition, it also derives two more sensory readings from the accelerometer by applying two filters, i.e., a low-pass filter (LPF) and high-pass filter (HPF) [12]. The list of chosen modalities, the extracted features, and the sensors used are summarized in Table 1.

5. Conclusion

The paper has proposed a behavioral-biometric-based authentication scheme in the context of on-demand ride and the rideshare services. The approach can be extremely useful to verify drivers remotely, i.e., distinguishing between a genuine driver and an impostor, at the time every new ride-booking. This scheme can be extended to verify the intended riders as well (provided the prior user consent is taken to avoid any privacy related issues). The scheme is unobtrusive as verification is performed in the background and is invisible to the driver.

In addition, the proposed scheme has shown resistance to mimicry attacks as the invisible person-specific behavioral modalities, i.e., hand movements, swipe gestures, and touch types can be extremely difficult to imitate. Further, this additional security layer makes the system secure against presentation-, shoulder-surfing-, and random-attacks. Lastly, the scheme is easy to implement and integrate with the existing infrastructure as it does not require any additional hardware and explicit user input.

Owing to space limitations, we will report the detailed methodology and the results of an extended empirical evaluation in a future paper. We will also explore the impact of its extension in terms of more modalities, i.e., grip, gait, voice, etc., and we will evaluate them in terms of their accuracy, performance, and usability.

Acknowledgment

This work has been partially supported by the NeCS ITN project under the Marie Sklodowska-Curie Grant Agreement No. 675320.

Conflict of interest

The authors declare that there is no conflict of interest in this paper.

References

[1] Reported list of incidents involving uber and lyft http://www.whosdrivingyou.org/rideshare-incidents.

[2] Uber driver background checks not good enough, http://www.bbc.com/news/technology-34002051.

[3] Wael Jabbar Abed Al-Nidawi, Mahdi Athab Maan, Marini Othman, Review on national electronic identification system, in: 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), IEEE, 2015.

[4] Michael Frutiger, Eric Overby, D.J. Wu, Is social network platform integration valuable for an online service? A Randomized Field Experiment and Archival Data Analysis. 2014.

[5] Kang Ruogu, Stephanie Brown, Sara Kiesler, Why do people seek anonymity on the internet?: Informing policy and design, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2013.

[6] Correa Denzil, LeandroAraújo Silva, Mainack Mondal, Fabrício Benevenuto, Krishna P. Gummadi, The many shades of anonymity: Characterizing anonymous social media content, in: ICWSM, 2015, pp. 71–80.

[7] Uber needs partners like you. https://get.uber.com/p/legacy-cl-base/.

[8] Attaullah Buriro, Bruno Crispo, Filippo Del Frari, Jeffrey Klardie, Konrad Wrona, Itsme: Multimodal and unobtrusive behavioral user authentication for smartphones, in: International Conference on Passwords, Springer International Publishing, 2015, pp. 45–61.

[9] Attaullah Buriro, Bruno Crispo, Filippo DelFrari, Konrad Wrona, Hold and sign: A novel behavioral biometrics for smartphone user authentication, in: Security and Privacy Workshops (SPW), 2016 IEEE, IEEE, 2016, pp. 276–285.

[10] Attaullah Buriro, Sandeep Gupta, Bruno Crispo, Evaluation of motion-based touch-typing biometrics in online financial environments. in: 16th International Conference of the Biometrics Special Interest Group, Darmstadt, Germany 2017.

[11] Attaullah Buriro, Bruno Crispo, Filippo Del Frari, Konrad Wrona, Touchstroke: Smartphone user authentication based on touch-typing biometrics, in: International Conference on Image Analysis and Processing, Springer, Cham, 2015, pp. 27–34.

[12] Attaullah Buriro, Behavioral biometrics for smartphone user authentication, (Dissertation), University of Trento, 2017.