CableAuth: A Biometric Second Factor Authentication Scheme for Electric Vehicle Charging

Jack Sturgess[†], Sebastian Köhler[†], Simon Birnbach, and Ivan Martinovic
Department of Computer Science, University of Oxford, Oxford, UK
{firstname.lastname}@cs.ox.ac.uk

***Abstract*—Electric vehicle charging sessions can be authorised in different ways, ranging from smartphone applications to smart cards with unique identifiers that link the electric vehicle to the charging station. However, these methods do not provide strong authentication guarantees. In this paper, we propose a novel second factor authentication scheme to tackle this problem. We show that by using inertial sensor data collected from IMU sensors either embedded in the handle of the charging cable or on a separate smartwatch, users can be authenticated implicitly by behavioural biometrics as they unhook the cable from the charging station and plug it into their car at the start of a charging session. To validate the system, we conducted a user study (n=20) to collect data and we developed a suite of authentication models for which we achieve EERs of 0.06.**

***Keywords*—authentication, electric vehicle, charging, EV, IMU, smartwatch, wearable authentication**

I. Introduction

The adoption of electric vehicles (EV) is happening at a rapid pace. However, in comparison to vehicles with combustion engines, the refilling of an EV battery takes substantially more time. To make the charging process as convenient and quick as possible for the driver, manufacturers have worked on different payment approaches to enhance the user experience. Almost all charging stations nowadays allow cashless payments via so-called external identification means [24]. Examples range from scanning a QR code printed on the charging station, to making payments via a mobile app, to simply tapping a contactless card on the card reader attached to the charging station. The card used can be either a contactless debit or credit card, or an RFID/NFC enabled smart card issued by the charging station operator. Regardless of the form of payment used at the charging station, compared to walking to the counter at a petrol station, these approaches already save the driver time.

To further enhance the convenience for the driver and improve the user experience, new payment methods, such as AutoCharge [10] and Plug & Charge [18] have been developed. Both technologies enable the driver to pay automatically for the charging session without any interaction. Once the charging cable is plugged into the vehicle, the payment information linked to the vehicle is sent to the charger and after the charging session is completed, the user is automatically billed. In the case of AutoCharge, the unique identifier used for the authorisation of the charging session is the ID of the Electric Vehicle Communication Controller (EVCC), or to be more precise the Media Access Control (MAC) address [12], [19]. In contrast, Plug & Charge offers a more secure approach that relies on digital signatures and a complex Public Key Infrastructure (PKI) [13].

Unfortunately, all of the aforementioned payment methods lack sufficient security implementations. For example, researchers found that RFID smart cards can easily be copied [7]. A similar problem exists for AutoCharge. Recent research has shown that it is possible to wirelessly extract the MAC address from an ongoing charging communication [2]. Since the MAC address of a vehicle is static and cannot be changed without the replacement of the EVCC, a leaked MAC address might not be usable for AutoCharge after the compromise. While Plug & Charge promises higher security guarantees, it is still possible that an adversary with physical access to the vehicle can extract the certificate to masquerade the victim and pay for their own charging [11].

Although these payment methods lack adequate security, they are widely used due to the increased convenience for the user. To overcome this problem, academic literature in the field of mobile payments has proposed using inertial data from the inertial measurement unit (IMU) sensors of the smartphone or smartwatch used for the payment as a second factor [21], [23].

In this paper, we adapt these approaches and propose an implicit second factor for authentication to overcome the security limitations of current payment methods used for electric vehicle charging.

Contributions.

- We propose a novel second factor authentication scheme for EV charging that does not require any additional user interaction.
- We show that when a user unhooks and plugs in an EV charging cable, the gestures made (as measured by inertial sensors in the handle) provide a biometric that is capable of implicitly authenticating the user.
- We also show that these gestures can be collected with the IMU on a smartwatch, providing a second option for system implementation that does not require any changes to existing hardware.
- We make the code and data required to reproduce our results available at http://github.com/jacksturgess.

[†] Joint first authors. These authors contributed equally.

Symposium on Vehicles Security and Privacy (VehicleSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-88-6
https://dx.doi.org/10.14722/vehiclesec.2023.23041
www.ndss-symposium.org

II. Related Work

Security and Privacy in EV Charging. With the increasing reliance on electric vehicles and their integration into the smart grid as an energy buffer, the security of the EV charging infrastructure has developed into an active field of research [14], [3]. Security issues that have been uncovered range from the physical layer of the charging station [2], [15], [8] to vulnerabilities in the software [9], [20], [4]. Researchers have also shown that the payment methods available for vehicle owners lack adequate protection. For example, Dalheimer [7] showed that the smart cards issued by charging point operators can easily be cloned. However, even the new payment methods, such as AutoCharge and Plug & Charge, do not provide sufficient security [2]. Hence, research related to privacy preservation and secure payment and authentication schemes that use a Trusted Platform Module (TPM) have attracted particular attention [11], [27]. In contrast to previous works that require additional hardware, such as a TPM, and the adjustment of the charging protocol, our proposed system can be deployed straightforwardly.

Gesture Biometrics for User Authentication. The ubiquity of IMU in consumer devices such as smartphones and smartwatches has enabled research into gesture-based authentication. For this type of user authentication, the user executes one or more gestures while a device equipped with inertial sensors gathers the unique biometric features necessary to identify that user. These gestures can be implicit gestures that the user performs as part of a regular activity, or they can be explicit gestures that the user performs exclusively for the purpose of authentication. Explicit gestures proposed in related work range from full arm motions [25] to punching the air [17] to simple hand gestures, such as giving someone a thumbs up [26]. However, while explicit gestures show a lot of promise due to strong performance results, they can be very cumbersome to execute and require additional effort by the user. To solve this issue, recent work has explored the use of implicit gestures—such as typing [1], picking up a phone or answering a call [16], [6], and payment gestures [21], [23], [22]—to authenticate users.

In particular, in the area of mobile payments, gesture biometrics based on inertial sensor data have been used to authenticate payments. The authors in [21] used various sensors (including IMU) on a smartphone during the tap gesture of a mobile payment to authenticate the user. A similar approach was used in [23], where the payments were authenticated using wrist-worn sensors (on a smartwatch). While our work is closely related to these, to the best of our knowledge no work has been done that considers IMU sensors that are attached to a charging cable, nor the gestures inherent in handling such a cable, to authenticate the user.

III. System Design

A. System Model

In this paper, we propose a novel approach that utilises the motion data from an IMU sensor in the handle of a charging cable of an electric vehicle charging station as a second factor to authenticate the payment for a charging session. Our system uses the unique movements of the charging cable handle when it is unhooked from the charging station and plugged into the vehicle. As such, the most important component for our system is the IMU sensor, which consists of an accelerometer and a gyroscope and is integrated into the handle of the charging cable. Due to the high current flow during a DC fast-charging session, modern charging cables are equipped with temperature sensors that are regularly polled by the charging station. We argue that the same communication channel can be used to access the IMU sensor, making the implementation of our system simple.

It is worth mentioning that our system does not require the user to perform any additional actions for the second factor to work (*i.e.*, it is an implicit factor). Therefore, our system provides an additional layer of security without affecting the user experience. We assume that the user's primary factor remains uncompromised during an initial training phase in which the user's normal charging sessions are used to provide the necessary training data for our system.

To start a charging session, the user unhooks the charging cable from the charging station and plugs it into the charging port of their vehicle. We extract from this procedure two separate gestures: the *unhook* gesture and the *plug-in* gesture. Once the cable is plugged into the vehicle—*i.e.*, no movement of the charging cable is recorded and the circuit of the Proximity Pilot (PP) between the charging station and the vehicle is closed—we consider the procedure to be completed.

We assume that the primary factor used for the authentication of a charging session is one of the following:

- An external means of identification, such as a smart card issued by the charging station operator, or a debit or credit card. Before the charging session, the card needs to be tapped against a card reader on the charging station.
- A unique identifier of the vehicle, for example the MAC address of the Electric Vehicle Communication Controller (EVCC). Once the car is connected to the charging station, the unique identifier is transmitted to the charging station via a communication channel in the charging cable. This process is also known as AutoCharge [10].
- A certificate that is installed in the vehicle as part of the Plug & Charge [18] standard. Similar to AutoCharge, the charging session is authorised once the charging cable is connected to the vehicle.

Widespread deployment of our system would require the embedding of IMU sensors into the handles of charging cables that are hardwired to a charging station. As an interim solution, and to ensure compatibility for charging stations that do not get upgraded or for user-owned portable cables that need to be plugged into a charging station, we also consider a parallel model using the inertial sensor data collected on wrist-worn IMU sensors in commercial off-the-shelf smartwatches.

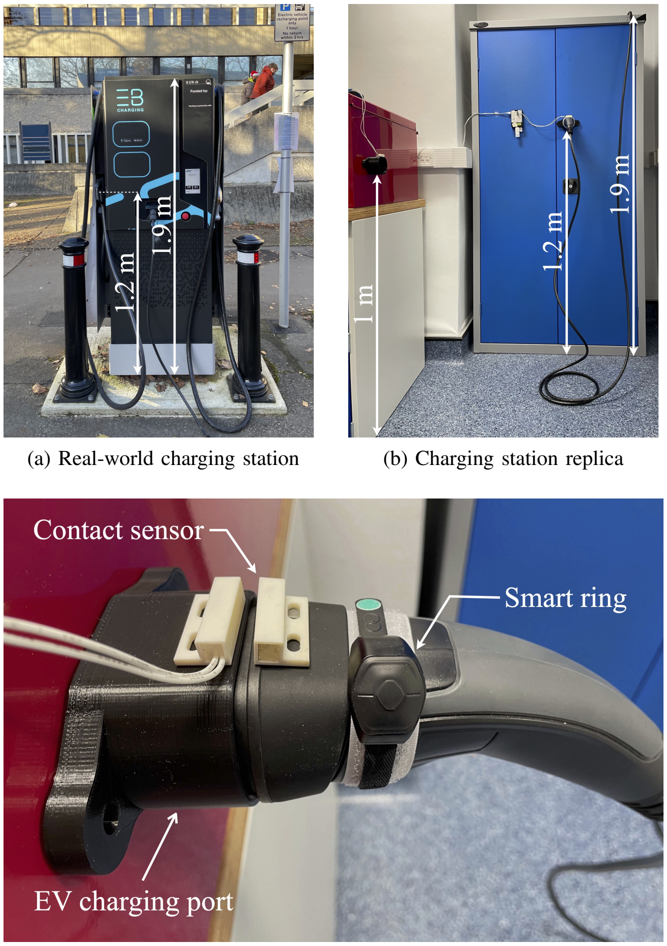
B. Threat Model

We consider two types of attackers: an attacker who has access to the vehicle of the victim, and another one who is attempting to pass their own vehicle as that of the victim.

The first type of adversary has possession of the electric vehicle of the victim (and any authorisation card that may be required to initiate charging sessions), has unlocked the vehicle, and is attempting to charge the vehicle at a publicly accessible charging station. For the case where the system uses a user-worn smartwatch instead of an IMU integrated into the charging cable for verification, we assume that the attacker has further obtained and unlocked the victim's smartwatch. The adversary may have stolen the vehicle, the card, and the smartwatch, or they may have borrowed them from the legitimate user. In either case, our goal is to prevent anyone other than the legitimate user from using the default payment method associated with the vehicle to pay for charging.

The second type of attacker has obtained the credentials used by the vehicle to identify itself to the charger. This could be a stolen certificate, a stolen or copied smart card [7], or—in the case of a less secure system, such as AutoCharge—as simple as the vehicle's unique identifier. The adversary may have obtained these credentials through prior physical access to the legitimate user's vehicle, through wireless eavesdropping on the vehicle's communication with another charger [2], or by launching a live relay attack if the victim's vehicle is charging nearby [5]. For this type of attacker, we only consider a system that uses an IMU integrated into the handle of the charging cable, as the use of a user-worn smartwatch would prevent the vast majority of these types of attacks [23]. Again, our goal is to authenticate the legitimate user, and to prevent any non-legitimate users from charging their vehicle using the victim's payment method.

In this work, we focus on the use of gesture biometrics to secure electric vehicle charging. We do not consider attacks on the charger itself or the payment infrastructure. Tampering of devices or biometric templates, malware, or denial of service attacks are similarly out of scope for this paper.



(a) Real-world charging station

(b) Charging station replica

(c) Charging cable handle with the smart ring attached

Figure 1: Real-world charging station and lab replica.

IV. Experiment Design

A. Experiment Setup

To collect data, we set up a replica charging station in our laboratory (see Figure 1b). We took measurements from a real-world DC fast-charging station (see Figure 1a) to ensure that our fake charging station replicates a real charging station as closely as possible with regards to the positions of the cable and cable holder. The cable (including its handle) used in our experiment was a real-world Type-2 charging cable to make certain that the users' cable-handling gestures were as realistic as possible. On the vehicle side, we chose to replicate a Volkswagen ID.3, as its size and the height of its charging port are a commonly found combination. We used a 3D printer to manufacture both the cable holder of the charging station and the charging port of the car.

For the collection of the inertial sensor data, we used a smart ring[1] attached on top of the cable handle. We chose to use the smart ring due to its small form factor and because it added a negligible weight to the handle. This allowed us to closely mimic an integrated IMU sensor within the handle, without adding other factors that could influence the handling of the cable. Henceforth, we will consider the smart ring IMU to be an integral part of the handle and we will refer to its data as the *handle data*. As an additional source of inertial sensor data, for comparison, the user wore a smartwatch[2] on their dominant hand with which they handled the charging cable. Our devices provided motion data from four sensors: the accelerometer, gyroscope, linear accelerometer, and gyroscope rotation vector (GRV). The linear accelerometer measures acceleration with the force of gravity excluded and the GRV is an approximation of the orientation of the device. We collected data from all four of these inertial sensors from each of the handle and the watch throughout the experiment at sampling rates of 100 Hz and 50 Hz, respectively.

In order to obtain ground truth for the cable *unhook* and *plug-in* events, we used magnetic contact switches mounted on top of the cable holds at both the charger and the car replicas, as well as a magnet mounted on top of the cable handle. Please refer to Figure 1c for a graphical depiction of both the handle and contact switch installation.

[1] Genki Wave, https://genkiinstruments.com/products/wave

[2] Samsung Galaxy Watch, https://www.samsung.com/uk/watches

B. User Study

For our experiment, we recruited 20 participants (students and staff; 12 male and 8 female) by distributing fliers at our university. Every participant was compensated for taking part in our study. This project was reviewed and received clearance by the responsible research ethics committee at our university.

Each participant attended three data collection sessions. The first two sessions were separated by a break of two minutes and the final session occurred after a longer break of at least fifteen minutes after the second session. In each session, participants would emulate ten full charging periods for a total of thirty charging periods across the three sessions. During each charging period, participants first unhooked the handle from the charger, before plugging it into the car charging port. They then briefly left the room with the charger, before coming back to put the cable back into the cable holder of the charger.

V. Methods

A. Data Processing

We collected inertial sensor data from both the handle and watch IMUs. At time t, each accelerometer sample is given in the form (t, x, y, z), the same for each gyroscope and linear accelerometer sample, and each GRV sample is given as a quaternion in the form (t, x, y, z, w). We express a *plug-in* or *unhook* gesture using time-series of samples within a fixed window. To retrieve the gestures, we segmented 4-second blocks of sensor data by using the timestamps collected from the associated contact switch as the midpoints. We found that a 4-second window size was enough to encapsulate the entirety of the movements for each gesture without overlap. To find the optimum parameters for each type of gesture, we compared the performances of gestures bounded by different (smaller) window sizes and offsets, where the offset is the time between the contact switch timestamp and the end of the window. For a timestamp T_0, a window size s, and an offset o, we retrieved a gesture with start time T_S and end time T_E, where $T_E = T_0 - o$ and $T_S = T_E - s$.

B. Feature Extraction

Whenever a gesture was retrieved, we applied a low pass filter to the data to reduce noise and then reduced it to a feature vector containing 220 features ready for classification. To extract the features from the gesture, we processed the following five dimensions for each sample: the filtered x-, y-, and z-values, the energy of those filtered values, and the energy of the unfiltered (raw) values, where the energy of $\{x, y, z\}$ is given by $\sqrt{x^2 + y^2 + z^2}$. As GRV samples are expressed as quaternions, for those we processed only the four filtered values. In total, we processed each gesture in 19 dimensions. For each gesture, we extracted the following ten statistical features in each dimension: *minimum*, *maximum*, *mean*, *median*, *standard deviation*, *variance*, *inter-quartile range*, *kurtosis*, *skewness*, and *peak count*. We also calculated the *mean* and *maximum velocities* along each axis, the *displacement* along each axis, and the *Euclidean displacement* from each of its accelerometer, gyroscope, and linear accelerometer vectors, adding another 30 features for a total of 220. (For further details on our settings and hyper-parameters, see our publicly available code, referenced in our Contributions in Section I.)

C. Classification

We used random forest classifiers in each of our models, as these have been shown to be efficient, able to estimate the importance of features, and robust against noise [23]. To balance relevance with learning time, we included 100 trees in each forest. For the other random forest hyperparameters, we found that the defaults provided by the sklearn Python library were suitable. To reduce the impact of random generation on our results, we trained and tested each classifier ten times with different randomisation seeds and averaged the outcomes.

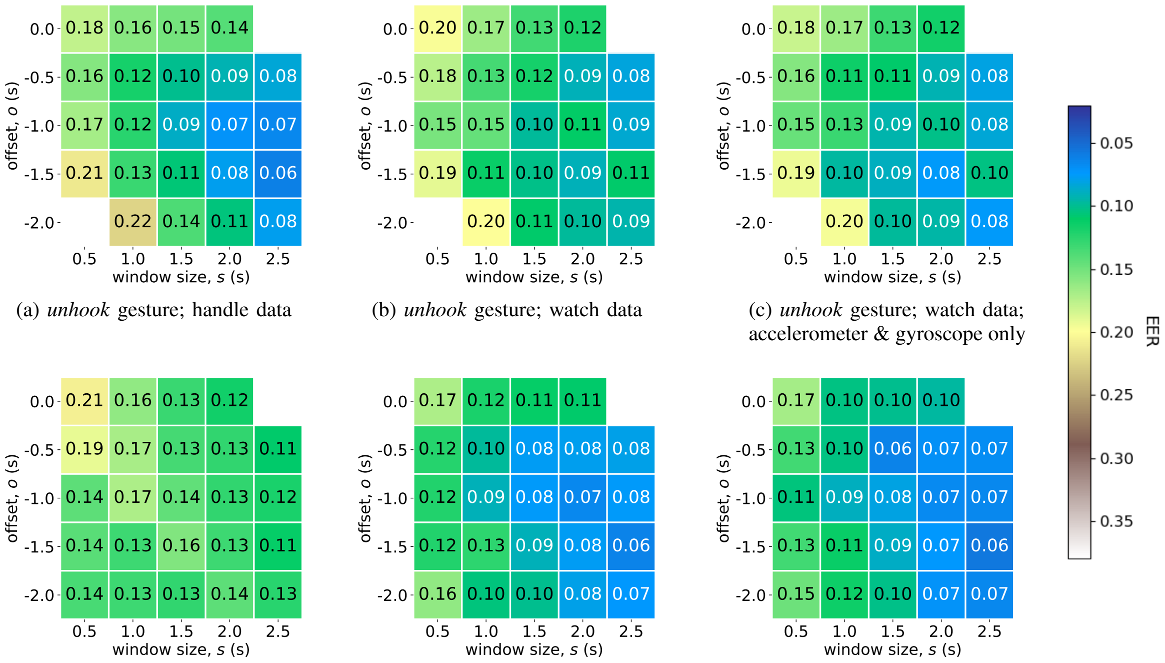
Authentication Model. For our main authentication model, we trained a set of classifiers that are user- and gesture-dependent– *i.e.*, a separate template is generated for each user and each classifier considers a single type of gesture, either *unhook* or *plug-in*. In each classifier, we took the legitimate user's gestures as the positive class and all other users' gestures of the same type as the negative class. As this is an authentication use-case, we ensured that the training data precedes the testing data by taking the gestures collected in users' first and second data collection sessions as training data (analogous to the enrolment phase, where the user template is created) and those collected in the third session as testing data.

In [23], the authors claimed that the linear accelerometer and GRV sensor data were detrimental to their classifiers, and that improved results were achieved when only the accelerometer- and gyroscope-derived features were included in the feature vector. To test this claim, and to see its impact on our results, we also trained a set of classifiers using smartwatch data from the accelerometer and gyroscope only. For these classifiers, each feature vector contained 120 features.

Combined-Gesture Model. In our main authentication model, we considered the *unhook* and *plug-in* gestures in separate classifiers. We also wanted to investigate whether combining these gestures would enable us to authenticate the user better (since both gestures are performed in the same arm movement as the user unhooks and plugs in the charging cable). The combination of the two gestures represents a composite gesture formed of two sources of data, one taken as a window around the *unhook* contact switch timestamp and the other as a window taken around the *plug-in* timestamp. This gave us two sets of window parameters to modify to find the ideal settings. For each pair of parameters, we concatenated the respective feature vectors into a single feature vector containing 440 features and then trained and tested user-dependent classifiers as per the main authentication model.

D. Performance Metrics

In each model, the *true positives* is the number of times that the positive class (*i.e.*, the legitimate user) is correctly accepted; the *true negatives* is the number of times that the negative class (*i.e.*, any other user) is correctly rejected; the *false positives* is the number of times that the negative class is wrongly accepted; and the *false negatives* is the number of times that the positive class is wrongly rejected. To quantify our models, we find the decision threshold where the false acceptance rate (FAR) is equal to the false rejection rate (FRR); this is called the equal error rate (EER). The EER is a measure of performance when considering both security and usability and is commonly used as a metric in authentication systems.



(a) *unhook* gesture; handle data

(b) *unhook* gesture; watch data

(c) *unhook* gesture; watch data; accelerometer & gyroscope only

(d) *plug-in* gesture; handle data

(e) *plug-in* gesture; watch data

(f) *plug-in* gesture; watch data; accelerometer & gyroscope only

Figure 2: Average EERs for our authentication model by window size and offset, for *unhook* (top) and *plug-in* (bottom) gestures using inertial sensor data collected on the handle (left) and the smartwatch (centre) and only the accelerometer and gyroscope data collected on the smartwatch (right).

VI. Results

A. Authentication Model

Figure 2 shows the average EERs for our authentication model. Each window shows the average EER of 10 instances of the same classifier (with different randomisation seeds) trained and tested on gesture data segmented into a time window of a given size and offset.

We see that the handle data yields the best EERs when classifying the *unhook* gesture, and the smartwatch data is best for the *plug-in* gesture. By examining the output logs of our classifiers, we see that the most influential features for the classifiers using handle data were derived from (i) the x-value of the gyroscope data and (ii) the extrema in the GRV data. The x-axis of the handle-mounted IMU in our setup pointed directly forwards, towards the nozzle of the handle, so the x-value of the gyroscope corresponds with the angular velocity of the side-to-side tilt of the handle. The GRV extrema describe orientation. Together, these suggest that the freehand 'wobble' of the handle when held was discriminative between users and likely explains why these classifiers performed better for the *unhook* gesture than the *plug-in* gesture, since users were more deliberate and had a target to aim for when plugging in the charger compared to when withdrawing it. For the smartwatch, the predominant features were those derived from the x-value of the accelerometer data. The x-axis of the smartwatch also pointed towards the end of the handle, indicating that push and pull speeds were discriminative. In the user study, users positioned themselves relative to the charging unit rather than the car, meaning that pulling the handle out of the charging unit was a low-effort movement, whereas pushing the handle into the car socket elicited a change in pose as well as additional force–this likely explains why the classifiers using smartwatch data performed better for the *plug-in* gesture.

There is a slight improvement in the smartwatch results when we omit the linear accelerometer- and GRV-derived features from the classifiers, which confirms the claims made by related work (see Section V-C).

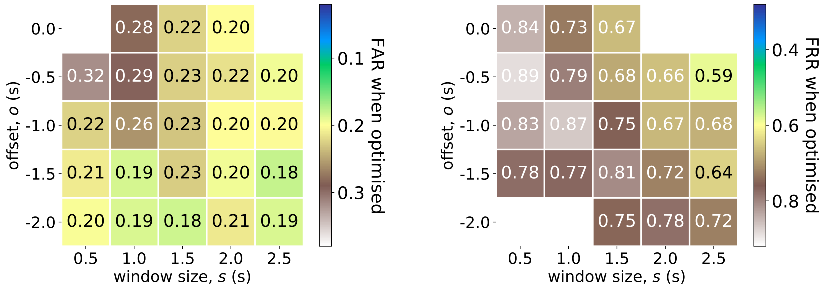
The optimum window parameters are $\{s = 2.5, o = -1.5\}$ (*i.e.*, a window of 2.5 seconds of sensor data starting 1 second before the corresponding contact switch timestamp and ending 1.5 second after it), where our model can authenticate the user with an EER of 0.06 for either gesture. Our results show that if the IMU is embedded into the handle of the cable then the *unhook* gesture is more effective at distinguishing between users, or if a smartwatch is used then the *plug-in* gesture is more effective.

B. Combined-Gesture Model

We constructed a set of classifiers that were trained and tested on data from both gestures together. We chose the best window parameters for *plug-in* and the best for *unhook* and made a classifier for each respective pair. Table 1 shows the results for these classifiers. The strongest results in the table are emboldened. Unfortunately, instead of improving on the results in Figure 2, the combined classifiers yielded EERs that were roughly the mean of the EERs of the single-gesture classifiers of the two component gestures in their respective window parameters. We find no benefit in combining the gestures.

Device	Parameters for *unhook* Gesture	Parameters for *plug-in* Gesture					
		$\{s = 1.5, o = -1.0\}$	$\{s = 2.0, o = -1.0\}$	$\{s = 2.0, o = -1.5\}$	$\{s = 2.5, o = -0.5\}$	$\{s = 2.5, o = -1.0\}$	$\{s = 2.5, o = -1.5\}$
Handle	$\{s = 2.0, o = -1.0\}$	0.13	0.11	0.12	**0.09**	0.10	0.10
	$\{s = 2.0, o = -1.5\}$	0.13	0.11	0.12	**0.09**	0.10	0.11
	$\{s = 2.5, o = -1.0\}$	0.12	0.11	0.11	**0.09**	**0.09**	0.10
	$\{s = 2.5, o = -1.5\}$	0.12	0.11	0.12	**0.09**	**0.09**	0.10
Watch	$\{s = 2.0, o = -1.0\}$	0.13	0.12	0.13	0.12	0.11	0.12
	$\{s = 2.0, o = -1.5\}$	0.11	0.11	0.12	0.10	**0.09**	0.10
	$\{s = 2.5, o = -1.0\}$	0.11	0.10	0.11	0.11	0.11	0.11
	$\{s = 2.5, o = -1.5\}$	0.13	0.12	0.13	0.11	0.12	0.12

Table 1: Average EERs for our combined-gesture model by *unhook* and *plug-in* window parameters.



(a) FARs

(b) FRRs

Figure 3: Average FARs when optimised to minimise false negatives and FRRs when optimised to minimise false positives for our authentication model by window size and offset, for *unhook* gestures using data from the handle.

C. *Second Factor Optimisation*

Our model is designed to be a second factor to an existing authentication system. As such, we can tune our classifiers to the needs of that system and then measure the strict improvement that we provide to it. The decision threshold, θ, is the score at which the classifier chooses to assign to a sample the positive class rather than the negative. To optimise a classifier, we adjust θ to modify the trade-off between security and usability; a larger θ is more resilient to false positives, whereas a smaller θ favours usability.

To evaluate the security gains that our model could provide without imposing any burden on usability (*i.e.*, by negating the likelihood of causing false negatives, which would cause the user to need to re-authenticate), we find for each classifier the θ such that the FRR is less than 0.01% and then measure the FAR at that point. Figure 3a shows the average FARs when optimised for usability. We see that our model can provide a strict improvement to the existing system by adding a layer of false acceptance detection with a FAR of 0.18.

Alternatively, to evaluate the impact on usability that our model would have on the system if tuned to maximise security gains, we find for each classifier the θ such that the FAR is less than 0.01% and then measure the FRR at that point. Figure 3b shows the average FRRs when optimised for security. We see that by adding a heavy-duty (and completely implicit) layer of security, we would impose an FRR of 0.59. This means that if our system were the primary authentication factor, an attacker would rarely be successful, and instead of needing to manually approve the charging session on their phone 100% of the time, the user would only need to do so 59% of the time.

VII. Conclusion

In this paper, we demonstrated that an IMU sensor embedded in the handle of an electric vehicle charging cable (or a smartwatch worn by the user) provides sufficient data to use the unique movements made by the user while unhooking and plugging the cable into the vehicle at the start of a charging session to authenticate the user. Our models achieved EERs of 0.06 and we showed that they could further be tuned to favour either security or usability so as to provide a strict improvement to an existing authentication system in each case.

Acknowledgements

This work was supported financially by Mastercard; armasuisse S+T; and the Engineering and Physical Sciences Research Council [grant number EP/P00881X/1]. The authors would like to thank these organisations for their support and the anonymous reviewers for their feedback.

References

[1] A. Acar, H. Aksu, A. S. Uluagac, and K. Akkaya. "A Usable and Robust Continuous Authentication Framework using Wearables", *IEEE Transactions on Mobile Computing (TMC)*, 2020.

[2] R. Baker and I. Martinovic. "Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging", *USENIX Security Symposium (USENIX)*, 2019.

[3] K. Bao, H. Valev, M. Wagner, and H. Schmeck. "A Threat Analysis of the Vehicle-to-grid Charging Protocol ISO 15118", *Computer Science-Research and Development*, Vol. 33, 2018.

[4] CISOMAG. "Schneider Electric Patches 13 Vulnerabilities Affecting Its EVlink Charging Stations", https://cisomag.com/schneider-electric-vulnerabilities-fixed, accessed December 2022.

[5] M. Conti, D. Donadel, R. Poovendran, and F. Turrin. "EVExchange: A Relay Attack on Electric Vehicle Charging System", *European Symposium on Research in Computer Security (ESORICS)*, 2022.

[6] M. Conti, I. Zachia-Zlatea, and B. Crispo. "Mind How You Answer Me!", *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, 2011.

[7] M. Dalheimer. "Ladeinfrastruktur für Elektroautos: Ausbau statt Sicherheit", https://media.ccc.de/v/34c3-9092-ladeinfrastruktur_fur_elektroautos_ausbau_statt_sicherheit, accessed December 2022.

[8] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and Regan Zane. "Electromagnetic Sensor and Actuator Attacks on Power Converters for Electric Vehicles", *IEEE Security and Privacy Workshops*, 2020.

[9] S. Dudek. "Examining Log4j Vulnerabilities in Connected Cars and Charging Stations", https://www.trendmicro.com/en_us/research/21/l/examining-log4j-vulnerabilities-in-connected-cars.html, accessed December 2022.

[10] EVgo Services LLC. "Evgo: Electric Vehicle (EV) Charging Stations - EV Fast Chargers", https://www.evgo.com/autocharge, accessed December 2022.

[11] A. Fuchs, D. Kern, C. Krauß, and M. Zhdanova. "TrustEV: Trustworthy Electric Vehicle Charging and Billing", *ACM Symposium on Applied Computing*, 2020.

[12] ISO 15118-2. "Road Vehicles - Vehicle to Grid Communication Interface - Network and Application Protocol Requirements", ISO, 2014.

[13] ISO 15118-20. "Road Vehicles - Vehicle to Grid Communication Interface - Part 20: 2nd Generation Network Layer and Application Layer Requirements", ISO, 2014.

[14] J. Johnson, T. Berg, B. Anderson, and B. Wright. "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses", *Energies*, Vol. 15, 2022.

[15] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic. "BROKENWIRE: Wireless Disruption of CCS Electric Vehicle Charging", arXiv:2202.02104 [cs.CR], 2022.

[16] W. H. Lee and R. B. Lee. "Implicit Sensor-based Authentication of Smartphone Users with Smartwatch", *ACM Hardware and Architectural Support for Security and Privacy (HASP)*, 2016.

[17] G. C. Liang, X. Y. Xu, and J. D. Yu. "User Authentication on Wearable Devices Based on Punch Gesture Biometrics", *International Conference on Information Science and Technology*, Vol. 11, 2017.

[18] M. Mültin. "The basics of Plug & Charge", https://www.switch-ev.com/blog/basics-of-plug-and-charge, accessed December 2022.

[19] Open Fast Charging Alliance. "Autocharge - Automatic Charging Start and Authorization of Electric Vehicles", https://github.com/openfastchargingalliance/openfastchargingalliance/blob/master/autocharge-final.pdf, accessed December 2022.

[20] Pen Test Partners. "Smart Car Chargers. Plug-n-play for Hackers?", https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers, accessed December 2022.

[21] B. Shrestha, M. Mohamed, S. Tamrakar, and N. Saxena. "Theft-Resilient Mobile Wallets: Transparently Authenticating NFC Users with Tapping Gesture Biometrics", *Annual Conference on Computer Security Applications (ACSAC)*, 2016.

[22] J. Sturgess, S. Birnbach, S. Eberz, and I. Martinovic. "RingAuth: Wearable Authentication using a Smart Ring", arXiv:2301.03594 [cs.CR], 2023.

[23] J. Sturgess, S. Eberz, I. Sluganovic, and I. Martinovic. "WatchAuth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch", *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2022.

[24] V2G Clarity. "Secure and User-friendly EV Charging - A Comparison of Autocharge and ISO 15118's Plug & Charge", https://www.dropbox.com/s/b9bq211cul69cax/Whitepaper-Autocharge-vs-ISO15118-Plug-and-Charge.pdf, accessed December 2022.

[25] J. Yang, Y. Li, and M. Xie. "MotionAuth: Motion-based Authentication for Wrist Worn Smart Devices", *IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, 2015.

[26] X. Yu, Z. Zhou, M. Xu, X. You, and X. Li. "ThumbUp: Identification and Authentication by Smartwatch using Simple Hand Gestures", *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2020.

[27] D. Zelle, M. Springer, M. Zhdanova, and C. Krauß. "Anonymous Charging and Billing of Electric Vehicles", *International Conference on Availability, Reliability and Security*, 2018.