

Inferring User Height and Improving Impersonation Attacks in Mobile Payments using a Smartwatch

Jack Sturgess, Simon Eberz, Ivo Sluganovic, and Ivan Martinovic

Department of Computer Science, University of Oxford, Oxford, UK
{firstname.lastname}@cs.ox.ac.uk

Abstract—In this paper, we show that as a user makes mobile payments with a smartwatch, the height of the user can be inferred purely from inertial sensor data captured on the watch (with R^2 scores of up to 0.77). Besides unwanted information exposure, we also show that users of a similar height are more difficult to distinguish between in terms of their tap gesture data and that an attacker who chooses a victim of a similar height can improve the success chance of impersonation (by increasing the false acceptance rate by up to 20.6%).

Index Terms—smartwatch, tap gesture, privacy, authentication

I. INTRODUCTION

Modern smartwatches offer a plethora of embedded sensors for health monitoring, location- and context-awareness, and security, including inertial sensors such as accelerometers and gyroscopes. While these sensors in particular can provide benefits in terms of activity recognition [6, 11, 13] and implicit authentication [5, 15], they also introduce a risk to privacy where users' secrets [8, 14, 16], interactions [10], activities [6], or physical attributes [12] might be inferred unwittingly.

Mobile payment systems—such as Google Pay—continue to grow in popularity as users seek fast and convenient means to make payments. While these tap-and-pay systems were initially deployed only on smartphones, their functionality has more recently been extended to smartwatches as well, enabling users to pay with a simple tap gesture on NFC-enabled payment terminals.

We recently conducted a user study in which participants wore a smartwatch and made mobile payments at point-of-sale terminals, during which we collected wrist motion data from the accelerometer and gyroscope [15]. We used the data to show that the tap gesture performed when making a payment is a biometric that can implicitly authenticate the user. We also showed that the user's intent-to-pay can be inferred since the tap gesture can be recognised amongst a large dataset of wrist-captured activity data.

In this work, we consider the privacy implications of this wrist motion data. Having shown that tap gestures can be used in an authentication use-case, we investigate whether we can infer users' age, sex, and height from these same gestures and how an attacker might capitalise on such inferences.

Contributions.

- From tap gestures composed of up to 4 seconds of inertial sensor data, we find that we cannot accurately infer users' age or sex, but that we can infer users' height.

- We show that users of a similar height are more difficult to distinguish between based on their tap gesture data, and therefore that an impersonator can gain an advantage in attacks by choosing a victim of a similar height.

II. RELATED WORK

Authentication. Prior works have shown that inertial sensor data from a smartwatch can be used to authenticate the user. Some works employ explicit gestures, made by the user solely for the purpose of authentication, such as MotionAuth [19] (full arm gestures), ThumbUp [20] (hand and finger gestures), and work by Liang *et al.* [7] (a punch gesture). Other works authenticate the user implicitly—*i.e.*, without dedicated effort, as he performs other tasks. Johnston *et al.* [5] present a gait-based system to identify or authenticate users as they walk, using 10-second windows of wrist motion data. WatchAuth [15] authenticates users as they make mobile payments and uses activity recognition to infer whether the payment is intentional, using as little as 0.5-second windows of wrist motion data. Nassi *et al.* [9] use wrist motion data to verify handwritten signatures and other authors [2, 3, 4, 18] present approaches to authenticate the user from free handwriting, using 5- to 60-second windows of data.

Privacy Risk. Several works use inertial sensor data from a smartwatch to infer alphanumeric inputs, potentially leaking secret information. Wang *et al.* [17] combine wrist motion data with a linguistic model that matches common short letter sequences to infer contextual inputs (English words) being typed on a keyboard. Liu *et al.* [8] and Wang *et al.* [16] present models that can infer PIN inputs on a keyboard or the keypad of a point-of-sale terminal or cash machine. Sen *et al.* [14] show that the location of touchscreen taps on a smartphone screen (and thus the keys tapped on its virtual keyboard) held in the same hand as the watch can be inferred by the watch using wrist motion data. Ardüser *et al.* [1] combine wrist motion data with audio recordings (for segmentation) to infer text characters written on a whiteboard with the same hand.

Other works use inertial sensor data from a smartwatch to recognise object interactions and hand-related activities. Object Hallmarks [10] combines smart meter data with wrist motion data to identify which user in a shared environment used a certain object, such as a faucet or light switch. The authors later showed that wrist motion data alone can be used to track object usage [11]. Sen *et al.* [13] use wrist motion

data to determine whether a smartwatch user is playing table football. Laput *et al.* [6] identify 25 different hand-related activities using wrist motion data.

Riaz *et al.* [12] collect inertial sensor data from four measuring devices worn simultaneously by users on the ankle, wrist, back, and chest as they do controlled walking tasks, segment the data into single steps by peak analysis, and infer users' age range, sex, and (discretised) height range from a single step using random forest classifiers, achieving accuracies of 83.50%, 87.16%, and 84.78%, respectively. They found that, of the four sensors, the wrist data contributed the least.

III. OBJECTIVES AND ASSUMPTIONS

A. System Model

We consider a system model in which a user is wearing a smartwatch and using it to make NFC-enabled payments at point-of-sale terminals. We assume that the watch has an accelerometer and gyroscope and that we collect timestamped data from each; we do not collect any non-inertial sensor data.

Using the collected data, we create distinct age-, sex-, and height-inferring models. We collect data from users interacting with different terminal types and positions to ensure that the resultant models are generalised and terminal-agnostic. We also create a separate height-inferring model based on the data from interactions only with a single terminal to compare the performance when using fixed-height, standardised terminals; for this model, we choose the foremost terminal, shown in the bottom right corner of Figure 1, because its position matches the standardised terminals mounted on British railway stations. Finally, we create an authentication model that authenticates users based on the tap gestures and we use this to compare the impersonation attackers detailed in our threat model.

B. Threat Model

For our inference models, we assume that the adversary has obtained tap gesture data—perhaps exfiltrated by some background malware and segmented by the adversary (since tap gestures are recognisable), or collected by a legitimate payment app and misused by an unscrupulous payment provider.

For our impersonation attack, we consider two classes of adversary: one *naïve* and one *informed*. In each case, we assume that the adversary has stolen a legitimate user's smartwatch, has it in an unlocked state (*e.g.*, by having previously shoulder-surfed the PIN, if it uses one), is wearing it, and is attempting to make a payment at an unstaffed point-of-sale terminal. The naïve attacker selects victims at random, whereas the informed attacker selects victims that are similar in height. For an attacker of height h , we consider a victim of height v to be similar in height iff $h - 1 \text{ cm} \leq v \leq h + 1 \text{ cm}$.

IV. METHODS

A. User Study

We captured wrist motion data from 16 users as they interacted with seven terminals: six in fixed positions and one 'freestyle' terminal that was picked up by the user, as if



Fig. 1: The equipment used in our experiment: six point-of-sale fixed terminals, an NFC reader connected to a Raspberry Pi for timestamp collection, and a Samsung Galaxy Watch running Tizen 4.0.

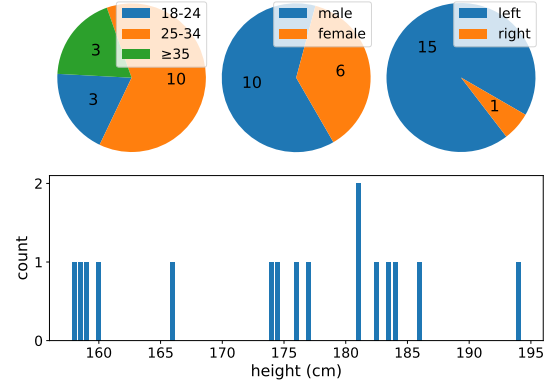


Fig. 2: The distribution of age (top-left), sex (top-centre), on which wrist they wore the smartwatch (top-right), and height (bottom) of users in our study ($n=16$).

handed it by a merchant. The set up is shown in Figure 1. Each participant attended 3 sessions, performing 10 tap gestures on each terminal per session. Participant demographics are shown in Figure 2 and further details can be found in [15].

B. Sensor Module

Our watch offered four inertial sensors: an accelerometer, a gyroscope, a linear accelerometer (derived from the accelerometer excluding gravity), and a gyroscope rotation vector (GRV; a fusion of other readings to estimate orientation). The sensors measure wrist motion along three axes that are relative to the frame of the watch: the x -axis corresponds with arm extension or withdrawal; the y -axis, with side-to-side arm waving; and the z -axis, directly up- and downwards through the watch face. We collect data from each at a sampling rate of 50 Hz.

C. Data Processing

Each sample at time t is given in the form (t, x, y, z) , giving the measurement along each axis; each GRV sample is given as a quaternion in the form (t, x, y, z, w) . We express a tap gesture using series of inertial sensor data samples within a time window. We also collect a timestamp each time the watch establishes an NFC connection with the NFC reader. For an NFC contact point timestamp T_0 , a window size s , and an offset o , we retrieve a tap gesture with start time T_S and end time T_E , where $T_E = T_0 - o$ and $T_S = T_E - s$.

D. Feature Extraction

We apply a low pass filter to the data of each windowed gesture to reduce noise and then extract a feature set. From samples from the first three sensors we take the filtered $\{x, y, z\}$ values, the norm of these values, and the norm of the unfiltered values and from GRV samples we take the filtered $\{x, y, z, w\}$ values to give us, overall, 19 dimensions in which we process the following statistical features: *minimum*, *maximum*, *mean*, *median*, *standard deviation*, *variance*, *inter-quartile range*, *kurtosis*, *skewness*, and *peak count*. For each gesture, we also calculate the *mean* and *maximum velocities* along each axis, the *displacement* along each axis, and the *Euclidean displacement* from each of the first three sensors. This gives our feature set a total of 220 members.

E. Classification

Inference Models. We employ three separate supervised learning approaches. Each classifier or regressor is trained and tested on features extracted from tap gestures and labelled with age range, sex, or height. The age and sex classifiers are trained on the tap gestures of all other users (in a leave-one-out manner). For our age-inferring model, we have a multi-class classification problem with three age classes (18 to 24, 25 to 34, and 35 and over). For our sex-inferring model, we have a binary classification problem. For our height-inferring model, we have a regression problem with height values between 158 cm and 194 cm (rounded to the nearest 0.5 cm). To see whether inferring height is more effective when using standardised terminals, we develop both multi- and single-terminal models; the latter uses training and testing data collected from users interacting with only one terminal.

In each model, we use random forests and apply stratified 10-fold cross-validation to preserve class proportionality in our training and testing sets and to reduce bias towards the more populous class. We train and test each classifier or regressor ten times with different forest randomisation seeds and average the outcomes to reduce the impact of random generation on our results.

Authentication Model. To see the impact of the height of the attacker on the success of the attack, we train an authentication model. We restrict our attention to tap gestures that could be used in-store (*i.e.*, those that end at or before the NFC contact point, when the payment provider would decide whether to approve the payment). We develop a separate classifier for each victim-attacker pair: we use data collected in the user's first and second data collection sessions and data from other (non-attacker) users to form the training set, and data from the user's third data collection session and data from the attacker for the testing set. This ensures that the user's training data necessarily precedes the testing data, analogous to the enrolment phase preceding an authentication phase, and that the attacker's data is not included in the training set. Again, we repeat each classifier ten times with different forest randomisation seeds and present the average.

F. Performance Metrics

Inference Models. In our classification models, the *true positives* is the number of times that the positive class (*i.e.*, the correct age range or sex of the user who performed the tap gesture) is correctly chosen; the *true negatives* is the number of times that the negative class (*i.e.*, an incorrect age range or sex) is correctly rejected; the *false positives* is the number of times that the negative class is wrongly chosen; and the *false negatives* is the number of times that the positive class is wrongly rejected. To quantify the performance of these models, we calculate the F-measures. To quantify the performance of our regression models, we use the coefficient of determination (R^2) to measure how correct the predicted values are.

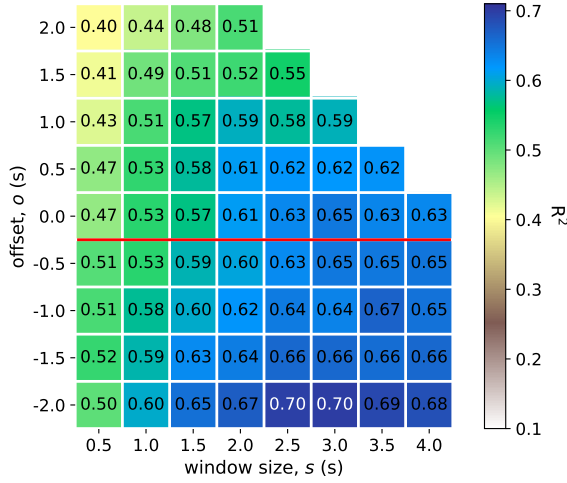
Authentication Model. In our authentication model, the positive class in each victim-attacker pair consists of the user's gestures and the negative class consists of the other users' gestures (including the attacker's). To quantify the performance of these models, we use the equal error rate (EER), where the false acceptance rate (FAR) and the false rejection rate cross over. The informed attacker measures success by how much he can raise the FAR.

V. RESULTS

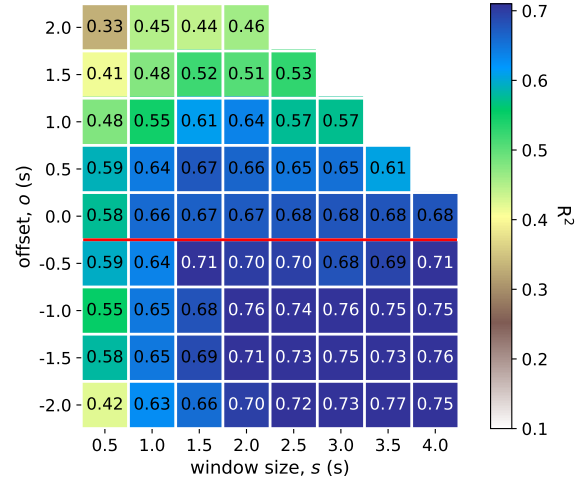
A tap gesture can be split into three phases: *reaching* (where the user moves the watch towards the terminal), *alignment* (where the user aligns the watch face to find the NFC contact point), and *withdrawal* (where the user pulls the watch away). We observed that the alignment phase typically began 0.5 to 1.5 seconds before the NFC contact point and ended up to 1 second after, depending on user reaction times. We consider matrices for each model showing metrics for classifiers and regressors trained and tested on feature vectors extracted from tap gestures of differently-sized sliding time windows by window size and offset. We include only the matrices for the height-inferring models and summarise the others. Each window is averaged over 10 random forests with different seeds. Tap gestures that occur fully before the NFC contact point (*i.e.*, those above the red lines in Figure 3, where $o \geq 0$) contain data from the reaching and alignment phases only.

Age-inferring Model. For our age-inferring model, we have poor results in all windows with F-measure scores ranging between 0.18 and 0.21 and no discernible patterns across window sizes or offsets. We find that we cannot infer users' age from our tap gesture data.

Sex-inferring Model. For our sex-inferring model, we have results that are better but still poor with F-measure scores ranging between 0.33 and 0.40 and that present a trend where larger window sizes yield better scores. Had we collected more data from participants before and after each tap gesture then, following this trend, the scores for larger windows might have become viable; however, the scope of this work is to infer private information from tap gestures, so we restrict our attention to windows containing 4 seconds of data or less. We find that we cannot infer users' sex from our tap gesture data.



(a) multi-terminal height-infering model



(b) single-terminal height-infering model

Fig. 3: Average R^2 scores for our multi- and single-terminal height-infering models by window size and offset. Tap gestures that end at or before the NFC contact point are above the red line.

multi-terminal height $\{s = 2.5, o = -2\}$		single-terminal height $\{s = 3.5, o = -2\}$	
Feature	#	Feature	#
Acc-x-mean	100	Acc-x-median	100
Acc-unf-pkcount	100	Acc-fil-median	100
Acc-x-median	92	Acc-x-kurtosis	100
Acc-x-velomax	75	Acc-x-maximum	100
Acc-x-disp	66	Acc-unf-pkcount	95
Acc-x-velomean	36	Gyr-y-kurtosis	3
Acc-x-minimum	10	Gyr-z-median	2
Acc-z-median	10		
Acc-y-minimum	5		
Acc-unf-median	3		

TABLE I: Modal top-five features of our height-infering models by Gini importance in the best performing windows, $\{s = 2.5, o = -2\}$ and $\{s = 3.5, o = -2\}$. Features are given in the format sensor-axis-statistic; *fil* and *unf* are the magnitudes of the filtered or unfiltered $\{x, y, z\}$ values, *velo* is velocity, and *disp* is displacement.

We note that sex correlates well with height, with the average height of our male participants being 182 cm and that of our female participants being 19 cm shorter, which may indirectly benefit the sex-infering classifiers (compared with the age-infering classifiers) to explain the improvement in F-measure scores.

Height-infering Models. For our height-infering model, we have much stronger results that show that we are able to infer users' height from our tap gesture data in certain windows. We see in Figure 3a that the withdrawal phase elicits movements that are the most distinctive, with optimum parameters $\{2.5 \geq s \geq 3, o = -2\}$, where we achieve R^2 scores of 0.70. We observed that, in the withdrawal phase, users unconsciously erect their back and pull away their arm at an angle roughly proportional to their height (in contrast with the reaching phase, where movements are adapted to the position of the terminal). The heights of the participants

range from 158 cm to 194 cm (with an average of 175 cm) and of the terminals, 95 cm to 120 cm (with an average of 106 cm). We see in Figure 3b that, when we restrict our attention to the wrist motion data collected from interactions with only a single, fixed-height (95 cm) terminal, our results improve; this suggests that for repeated interactions with the same terminal or with terminals in standardised positions, we can more effectively infer the user's height. Here, for $\{s = 3.5, o = -2\}$, we achieve an R^2 score of 0.77.

We hypothesised that movement along the vertical axis would be the most distinctive when inferring users' height. We note that the sensor axes are relative to the frame of the smartwatch; this means that inferring height is not as simple of comparing displacement in the z -axis, because traversal in the downward direction (from the external reference frame) is measured by the watch along whichever axis is facing downwards given its current orientation. Since each user started each gesture facing the terminals with his smartwatch arm either at his side or across his chest, it is most likely that downward travel was measured on the x - and y -axes for smooth gestures made on inclined terminals. For the rear terminals, tilted near vertically, taller users were able to lower the watch to the terminal with the x - and z -axes facing downwards, whereas shorter users approached them from the side with the x - and y -axes down. To see which features are most informative to our models, we select the best performing window parameters in each model and sum the top five features, sorted by Gini importance, in each of the ten regressors for those windows; we present the features and tallies in Table I. Comparing the multi- and single-terminal features, we see that only accelerometer features are ranked highly and most pertain to the x -axis, likely owing to it being the common axis in downward movement. Furthermore, we see that some of the features were tallied 100 times; this means that in all ten folds of all ten randomly-seeded forests for that

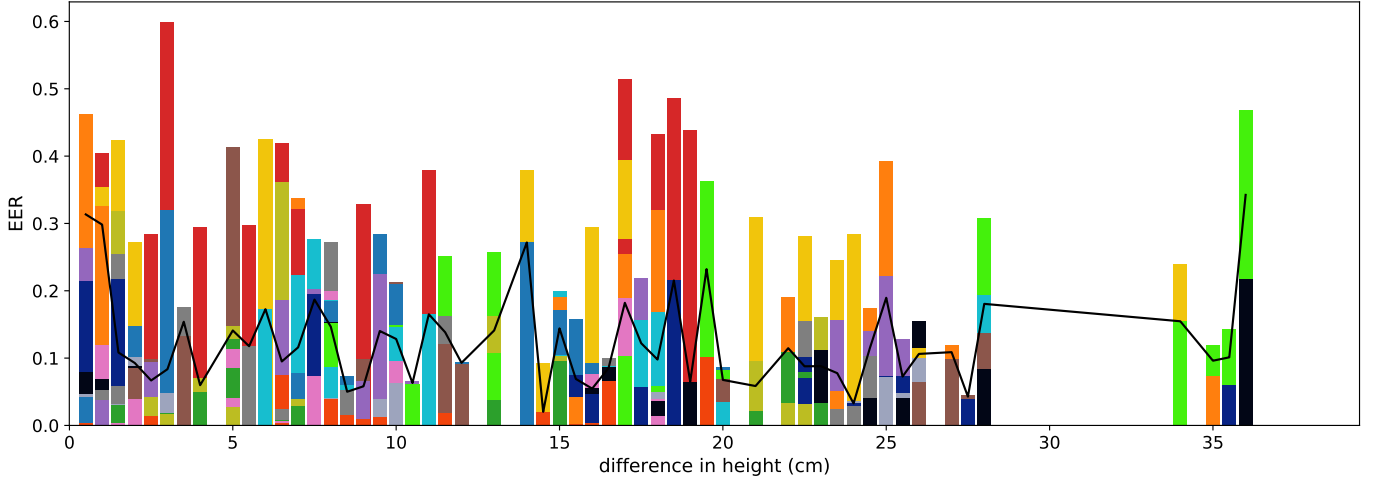


Fig. 4: Average EERs for each victim in our authentication model against each attacker by their difference in height with parameters $\{s = 2.5, o = 0\}$. Each colour corresponds to a different victim. The average per difference is indicated with the running black line.

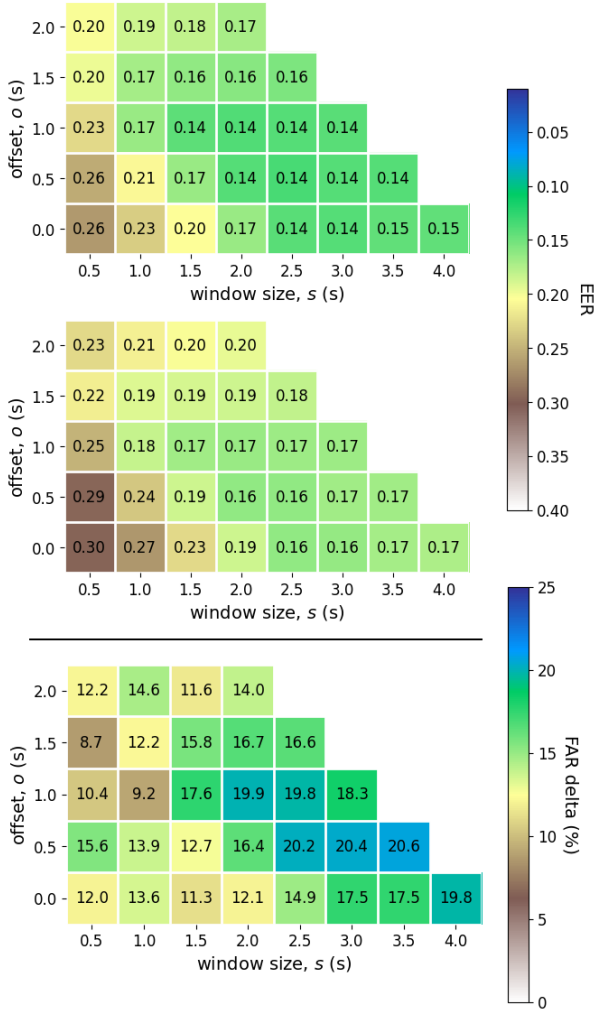


Fig. 5: Average EERs for our naïve (top) and informed (middle) attackers and the increases in EERs (and therefore FARs) from the naïve to the informed attacker as a percentage gain (bottom) by window size and offset.

window, every regressor ranked those features among their top five, strongly asserting their importance as discriminators.

Authentication Model. For our authentication model, we train a different classifier for each victim-attacker pair (and repeat each ten times with different seeds) and present the average (over both pairings and seeds) per window. For in-store usage, we focus only on offsets $o \geq 0$, where the tap gestures end at or before the NFC contact point. Figure 5 shows the average EERs for our victim-attacker pairs by window size and offset; the top heatmap shows the average results for the naïve attacker (*i.e.*, all pairings) and the middle heatmap shows the average results for the informed attacker (*i.e.*, only pairings where the attacker and victim are similar in height). We see that the EERs are monotonically greater in the middle heatmap, indicating that the classifiers have a greater false acceptance rate when the victim and attacker are similar in height. The bottom heatmap in Figure 5 shows the increases in the EERs (and therefore in the FARs) from the naïve to the informed attacker as a percentage gain and therefore the impact of the attacker selecting a victim that is similar in height. Interestingly, the impact is greatest in those windows that are most performant in terms of authentication and height inference (where $o \geq 0$). In [15], we found that the optimum window parameters for in-store authentication are $\{s = 2.5, o = 0\}$; here, we see that an informed attacker can passively improve the FAR, and the chance of success of impersonation, by 14.9% for those parameters.

Figure 4 shows the EERs for our authentication model with $\{s = 2.5, o = 0\}$, where each victim-attacker pair is arranged by their difference in height and the results for each victim are shown in the same colour. We see that, with the exception of two victims (shown in yellow and red, with diagonal hatching) and a few outlier results, the average EERs steadily decrease as the difference in height increases (indicated with the black line). The two exceptional users performed notably minimalistic gestures during the user study, which present fewer gesture properties and typically yield poorer EERs in

all attacker pairings. A noteworthy counter-trend is presented by the tallest user in our study (shown as a victim by the light green bar with dots): the rightmost outlier shows that when the tallest user is the victim of the shortest user the EER is 0.47, but *vice versa* the EER is 0.22; indeed, the light green bar is usually larger than its converse. This suggests that this user is particularly susceptible to impersonation, although our data are too few to conclude whether this is due to his height.

VI. LIMITATIONS AND FUTURE WORK

The chief limitation of this work is the size of the dataset (unfortunately, our experimental work was ended abruptly by national lockdowns in 2020). Having samples from 16 users provides a reasonable basis for our study and demonstrates its feasibility, but future work would benefit from a larger dataset with a broader spectrum of participant height values to enable more fine-grained analysis. In particular, with a larger dataset, future work might explore whether difference in height (between victim and attacker) is directly proportional to the increase in FAR—and, moreover, whether a payment provider could use this information to infer the height of an impersonator in retrospective fraud analysis. Future work might also explore the observed counter-trend presented by the tallest user.

VII. CONCLUSION

In this paper, using wrist motion data obtained from users performing mobile payments with a smartwatch, we showed that users' height can be inferred with R^2 scores of up to 0.77 and that an informed attacker who selects victims that are similar in height to him has a greater chance of success when attempting to impersonate the victim's tap gestures than a naïve attacker who selects victims at random. We showed in our previous work that tap gestures can be used to authenticate users and infer intent-to-pay; we showed in this work that those same gestures do not leak users' age or sex.

ACKNOWLEDGEMENT

The authors would like to thank the Engineering and Physical Sciences Research Council (under grant EP/P00881X/1) and Mastercard for financially supporting this work and the anonymous reviewers for their feedback.

REFERENCES

- [1] L. Ardüser, P. Bissig, P. Brandes, and R. Wattenhofer. "Recognizing Text using Motion Data From a Smartwatch", *IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, 2016.
- [2] F. Ciuffo and G. M. Weiss. "Smartwatch-based Transcription Biometrics", *IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*, 2017.
- [3] I. Griswold-Steiner, R. Matovu, and A. Serwadda. "Handwriting Watcher: A Mechanism for Smartwatch-driven Handwriting Authentication", *IEEE International Joint Conference on Biometrics (IJCB)*, 2017.
- [4] I. Griswold-Steiner, R. Matovu, and A. Serwadda. "Wearables-driven Freeform Handwriting Authentication", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, Vol. 1, 2019.
- [5] A. H. Johnston and G. M. Weiss. "Smartwatch-based Biometric Gait Recognition", *IEEE International Conference on Biometrics Theory, Applications, and Systems (BTAS)*, 2015.
- [6] G. Laput and C. Harrison. "Sensing Fine-Grained Hand Activity with Smartwatches", *Conference on Human Factors in Computing Systems (CHI)*, 2019.
- [7] 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 (IST)*, Vol. 11, 2017.
- [8] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang. "When Good Becomes Evil: Keystroke Inference with Smartwatch", *ACM Conference on Computer and Communications Security (CCS)*, 2015.
- [9] B. Nassi, A. Levy, Y. Elovici, and E. Shmueli. "Handwritten Signature Verification using Hand-worn Devices", *ACM Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, Vol. 2, 2016.
- [10] J. Ranjan and K. Whitehouse. "Object Hallmarks: Identifying Object Users using Wearable Wrist Sensors", *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, 2015.
- [11] J. Ranjan and K. Whitehouse. "Towards Recognizing Person-Object Interactions using a Single Wrist Wearable Device", *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, 2016.
- [12] Q. Riaz, A. Vögele, B. Krüger, and A. Weber. "One Small Step for a Man: Estimation of Gender, Age and Height from Recordings of One Step by a Single Inertial Sensor", *Sensors*, Vol. 15, 2015.
- [13] S. Sen, K. K. Rachuri, A. Mukherji, and A. Misra. "Did You Take a Break Today?: Detecting Playing Foosball using Your Smartwatch", *IEEE International Workshop on Sensing Systems and Applications using Wrist Worn Smart Devices*, 2016.
- [14] S. Sen, K. Grover, V. Subbaraju, and A. Misra. "Inferring Smartphone Keypress via Smartwatch Inertial Sensing", *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017.
- [15] J. Sturgess, I. Sluganovic, S. Eberz, and I. Martinovic. "WatchAuth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch", arXiv: 2202.01736 [cs.CR].
- [16] C. Wang, X. Guo, Y. Wang, Y. Chen, and B. Liu. "Friend or Foe?: Your Wearable Devices Reveal Your Personal PIN", *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, 2016.
- [17] H. Wang, T. T.-T. Lai, and R. R. Choudhury. "MoLe: Motion Leaks through Smartwatch Sensors", *International Conference on Mobile Computing and Networking (MobiCom)*, 2015.
- [18] R. Wijewickrama, A. Maiti, and M. Jadhwal. "Write to Know: On the Feasibility of Wrist Motion Based User-Authentication from Handwriting", *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2021.
- [19] 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.
- [20] 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.