Under Pressure: Pushing Down on Me: Touch Sensitive Door Handle to Identify Users at Room Entry

Christian Tietz, Eric Klieme, Rachel Brabender,
Teresa Lasarow, Lukas Rambold and Christoph Meinel
Hasso Plattner Institute, University Potsdam, Potsdam, Germany

Keywords:
behavior biometrics, identification, door handle, touch interactions.

Abstract:
Each day we open a door using physical keys or tokens like RFID or smart cards. While we all are used to these methods they have problems of security and usability. These tokens and keys can easily be stolen or taken by other persons which results in a security problem. The problem in usability is that users need a significant amount of time to take out their tokens to unlock and open the door. In this paper, we propose a new approach for door handle access control. We developed a prototype by attaching pressure sensors to the door handle that measure resistive and capacitive touch interactions with the door handle. We demonstrate the feasibility of identification with a door handle with a visual and classification analysis. The classification algorithms used are K-NN, SVM, Random Forests, AdaBoost and MLP achieving a maximum accuracy of 88% using the Random Forests.

1 INTRODUCTION

Currently, authentication at door and gate access points is mostly achieved by using mechanical keys or radio-frequency tags (RFID). Each verification key permits users to access associated areas. The problem with such physical tokens is that they can easily be cloned or stolen. For example, one can find a wide variety of instructions to duplicate mechanical keys without a locksmith (Marsh et al., 2014). Furthermore, there exist smartphone apps that let people easily scan their physical keys with the camera, store it in the cloud or share them with family & friends and easily order duplicates that are sent to you by mail (Wendt, 2015). Also, RFID tags are not secure as research showed that it was possible to open millions of doors without authorization in a hotel (Pinkert and Tanriverdi, 2018) or clone a key of a Tesla Model S (Greenberg, 2018).

To make access control more secure, biometrics can be used. For example, fingerprint (Odiete et al., 2017), palmprint (A. Kumar and Jain, 2003), hand contour (Schmidt et al., 2010), voice (Wahyudi and Syazilawati, 2007), face recognition (Alam and Yeasin, 2019)(Varasundar and Balu, 2015) and combinations of them (Brunelli and Falavigna, 1995)(Bigun et al., 2005) are ways to unlock a door. These methods are also having some problems. Fingerprints can be photographed and forged (ChaosComputerClub, 2013) or iris recognition can be bypassed with a simple photo (ChaosComputerClub, 2017).

Both, the possession- and biometric-based methods have a usability problem. All these methods require an additional authentication effort besides opening the door, e.g. interacting with the lock or the biometric scanner terminal. Recent research showed that users like the idea of just using the door handle without any additional interaction (Mecke et al., 2018). They compared physical keys, a gait-based system, and a vein scanner integrated into the door handle as methods in a Wizard-of-Oz study and analyzed the perception of users. The results showed that users like seamless interaction with the vein scanner and the door handle because it is faster than a key, more comfortable, easy to use and secure.

In this work, we propose a proof of concept for physical access control based on the user's behavior while using the door handle. A normal door handle is enhanced with resistive and capacitive pressure sensors instead of a real vein scanner. Using touch sensors is new in the field of door

handle access control.

We give a summary of existing research in this area in Section 2. Then, we present our door handle prototype and the data collection approach in Section 3 and 4. Afterwards, we go over the data extraction and pre-processing (Section 5), followed by a first data exploration in Section 6. We finish the paper with an evaluation of the identification results and the conclusion (Sections 7 and 8).

2 RELATED WORK

In the field of access control using door handles, there is already some prior work done. We divided them into two parts: image-based and sensor-based evaluation.

2.1 Door Handle Authentication using Images

Aoyama et al. (Aoyama et al., 2013) proposed a system for analyzing the user's finger knuckles on the door handle. The door is set up with a camera and an infra-red-light source that records an image of the four-finger knuckles while interacting with the door handle. From the hand image, they detect and extract the knuckles as ROI (region of interest). They used 900 images from 90 subjects (10 images per person, 5 left, and 5 right hands). The algorithms used are knuckling recognition methods: BLPOC, pCode and LGIC and their proposed one. The best result is achieved by middle and ring finger combination with an EER (Equal-Error-Rate) of 1.54%.

A similar approach was presented by Kusanagi at al. (Kusanagi et al., 2017). They used a camera to get the images of the finger knuckles from above and not from the front. They also extracted the finger knuckles ROI from the image. Their database was created from 28 participants who also used both, left and right hand 5 times each. This for two sessions. In a total of 560 images. They also came up with a new proposal and compared them to the existing BLPOC, CompCode and LGIC algorithms. They evaluated each finger individually and in combination. The best result is achieved with a combination of all four knuckles resulting in an EER of 2.36%.

2.2 Door Handle Authentication using Sensors

Garcia et al. (Garcia et al., 2016) investigated hand dynamics and the door handle movement when opening a door. They used two smartphones that are attached to the hand and the door handle to collect data from 20 participants. Each participant opened the door ten times. They extracted 170 features (85 from hand and 85 from door handle) with statistical (e.g. mean, median, root mean square level) and physical (e.g. movement intensity, dominant frequency energy) features. The authentication algorithm was SVM with 92% accuracy to identify users using a 50-50 train test split.

Ishida et al. (Ishida et al., 2017) looked into the door opening and closing of a refrigerator. They attached pressure, accelerometer and gyroscope sensors to the door handle. Their features are acceleration, angular velocity and pressure values of gripping the handle. On seven participants, an accuracy of 91.9% is reached.

2.3 Summary

There are already approaches in using the door handle behavior to identify and authenticate users that work quite well by analyzing finger-knuckles or using smartphone sensors. The finger-knuckle approach requires a camera that needs to be integrated into or above the door. This makes it complicated for a more realistic, real-world user study. When using sensors, a complete smartphone was attached to the door handle which has an impact on how users are gripping and using the door handle.

Thus, in this work, we build a new prototype that attaches pressure sensors to the door handle and can easily be installed to real doors to analyze the user's behavior by using their pressure on the door handle.

3 TOUCH-SENSITIVE DOOR HANDLE PROTOTYPE

Our prototype uses four silicon-based sensor stripes of Tacterion[1]. These stripes measure touch (capacitive) and applied force (resistive) data. The material and their size of 90x9 mm makes them suitable for uneven surfaces like a

[1]https://www.tacterion.com/development-kit

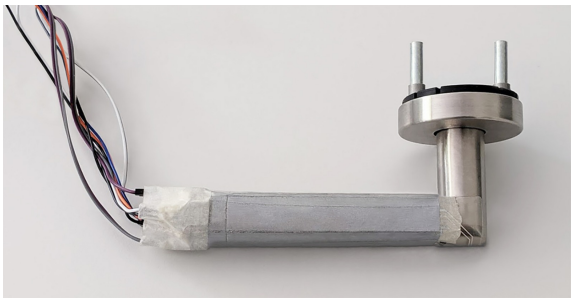

Figure 1: The final protoype from our door handle with the lengthwise attached sensor stripes. The positions of the sensor stripes are Top, Bottom, Back and Front.

cylindrical door handle. In total, the sensors produce eight values per reading.

All four sensors are attached to a door handle on top (To), on the front (Fr), the back (Ba) and the bottom (Bo) of the door handle and are fixed by regular masking tape. It has a silver color to keep the genuine look to not disturb participants. The resulting prototype is shown in Figure 1.

4 DATA COLLECTION

To our knowledge, no similar work has been done and no available data set can be used. Therefore, we describe our user study and some preliminary considerations in this section.

4.1 Preliminary Considerations

There are a lot of different factors that might influence our behavior of opening a door. These factors can be approaching the door from different directions like from left, from right or frontal. The position of the door handle (left or right) the used hand or opening the door by pushing or pulling might be important, too. The door opening can also change over multiple days or if people are emotional, angry or in a hurry. Users might talk to other people, having something in their hands or using different types of door handles. All these can influence the behavior and bring randomness to it.

For this proof of concept work, we decided to use the most common factors. Participants will approach the door from frontal and opening it by pushing using their preferred hand. The recording is done in a supervised manner without distractions and special emotions.

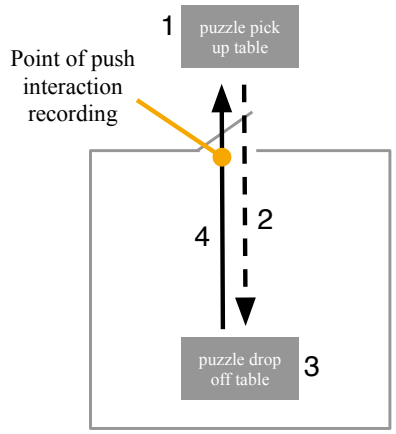

Figure 2: The running direction of the user study. The data was collected when the users leave the room and push the door.

4.2 User Study

We conducted a supervised user study to record their door handle behavior using the most common parameters discussed in Section 4.1. Each participant got an explanation of the study's purpose and procedure which has to be agreed and signed in a consent form. Afterward, they follow the procedure shown in Figure 2.

The participant starts outside the room and takes a piece of a puzzle that was prepared in advance (1). The puzzle serves as distraction task. Then, they walk inside (2) and put the piece of the puzzle at the correct position inside(3). Finally, they leave the room by pushing the door open(4). At this time, we record their door handle behavior. This completes one round which is repeated 30 times. The participants answer a questionnaire after finishing all rounds. We asked for information about gender, their preferred hand that could correlate to the recorded data and their thoughts and views about this authentication concept in the questionnaire. 25 people took part in the study.

5 DATA EXTRACTION and PRE-PROCESSING

Our prototype generates data with a frequency of 30Hz which results in 8x30 data points per second. The data were recorded and stored per user

with no separation of stand by phases and door opening phases.

To detect the door handle usages in the stream of data, we use the resistive sensors values. They have a clear zero line when there is no interaction in comparison to the capacitive sensors that are always showing low non-zero values. The values of the resistive sensors are numbers in the interval [0, 4095]. For a given raw signal, we assign to each timestamp a *"0"* when all resistive sensors' values are under 500 and *"1"* if at least one is over 500. Afterward, sequences of consecutive *"1"s* are combined into intervals (see Algorithm 1) with the index of the first and last *"1"* as interval borders.

Algorithm 1 Building intervals of consecutive 1s.

```
function BUILDINTERVALS(list)   ▷ list of 0, 1
    intervals ← []
    start ← 0
    for all i in list do
        if i+1 = |list| or list[i] ≠ list[i+1] then
            if list[i] = 1 then
                intervals ← intervals + [(start, i)]
            end if
            start ← i+1
        end if
    end for
    return intervals
end function
```

If two neighboring intervals are very close to each other (< 100 timestamps, roughly 3 seconds) then the two intervals are fused into one as described in Algorithm 2.

Finally, each interval is extended by two seconds by subtracting 30 time-units from the beginning index and adding 30 time-units to the end. These final intervals are then used to extract the door opening samples from the data stream into a matrix with eight rows where each row represents one sensor. Each sample can have a different length. We interpolate each sample to the maximum length of all samples.

6 DATA EXPLORATION

After collecting and pre-processing the data, we have a visual look on it to see how each sensor contributes to distinguishing users.

Algorithm 2 Fusing nearby intervals.

```
function FUSEINTERVALS(intervals)
    fusedIntervals ← []
    lastInterval ← intervals[0]          ▷ tuple
    i ← 1
    while i < |intervals| do
        (start, end) ← intervals[i]
        if |start − lastInterval[1]| < 100 then
            lastInterval = (lastInterval[0], end)
        else
            fusedIntervals.append(lastInterval)
            lastInterval ← (start, end)
        end if
        if i = |intervals| − 1 then
            fusedIntervals.append(lastInterval)
        end if
        i ← i+1
    end while
    return fusedIntervals
end function
```

6.1 Comparing Time Series of the same User

In the first visualization, we compare all samples of the same user by plotting all samples in the same plot. We create one plot for each sensor, thus, resulting in eight single time series plots. The plots for one of our 25 users are shown in Figure 3. In general, the plots for the other users look similar and with at most two outliers. We can see that the capacitive sensors (on the left) seem to be more characteristic and expressive than the resistive ones. Another point that can be seen is that all the samples in the plot have the same structure which shows that the door opening is not random and follows a pattern.

6.2 Comparing the Time Series of Different Users

In a second visualization, we compare the time series of two different users. We take two samples of one user and one from another user and show one of the plots in Figure 4. We see that the patterns of user1 and user2 are similar and differ in the amplitude. For the back (BaC) and front (FrC) capacitive sensor, the sample of user2 is between the samples of user1. On the other side, the sensors for bottom and top (BoC and ToC) show a clear visible separation of user1 and user2. This indicates that some sensors are better suited for distinguishing the users than others. Again,

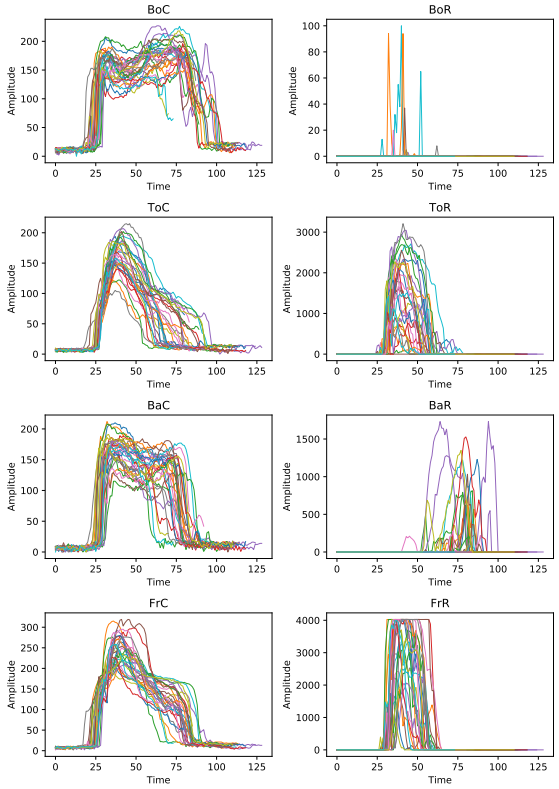

Figure 3: This figure shows all door opening samples of one user for each sensor: Bottom (Bo), Top (To), Back (Ba) and Front (Fr) with their capacitive (C) and resistive (R) values, respectively.

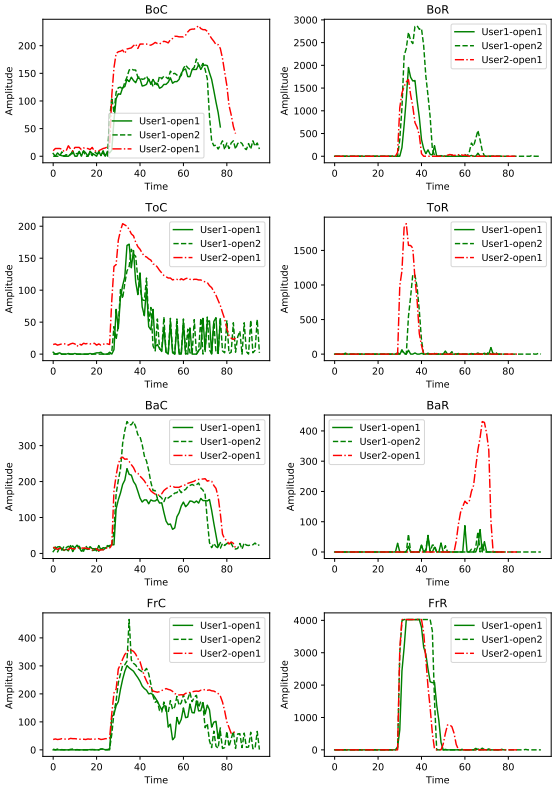

Figure 4: This figure shows the door opening from two samples of one user and one sample of a second participant for each sensor: Bottom (Bo), Top (To), Back (Ba) and Front (Fr) with their capacitive (C) and resistive (R) values, respectively.

the plots of the other users show the same results with some plots showing a clear separation between the users in all eight plots.

7 IDENTIFICATION RESULTS

In this work, we will do only a very first evaluation of our data by analyzing the identification performance with a closed-world assumption. Different groupings of sensors are evaluated using five-fold cross-validation and the common classifiers: K-NN (k-nearest neighbors), SVM (support vector machine), Random Forests, Ada Boost and MLP (multi-layer perceptron).

7.1 Evaluation per Sensor

For the first evaluation, we applied all classifiers to each sensor individually to see how good each sensor is to distinguish the users. Figure 5 and Figure 6 show the results (the mean accuracy of the five-fold cross-validations runs) for each of the resistive and capacitive sensors, respectively.

The plots show that the performance of the resistive Sensors is significantly lower than the capacitive sensors (best: 34.1% vs 74.6%) which correlate to the data exploration observation. The top sensor (ToR) performs best for all resistive sensors while it is different for the capacitive sensors. The best result is given by the front Sensor (FrC). In all cases, the random forest classifier gives the best results on our dataset.

7.2 Evaluation of Sensor Groups

In the second evaluation, we grouped the sensors under three categories: resistive only, capacitive only and all sensors. Figure 7 shows the mean accuracies of the cross-validations.

The combination of all resistive sensors improves the identification result up to 57%. That's better but still inferior to one capacitive sensor. Grouping all capacitive sensors achieved an accuracy of 88.6% Again, the best overall classifier is

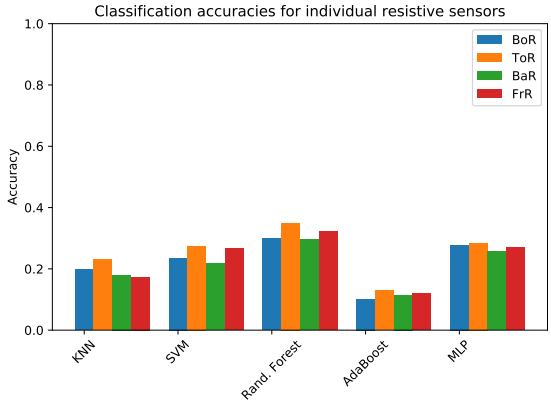

Figure 5: The evaluation results for each of the resistive sensors. The best accuracy is 34% from the top sensor (ToR) using the random forest classifier.

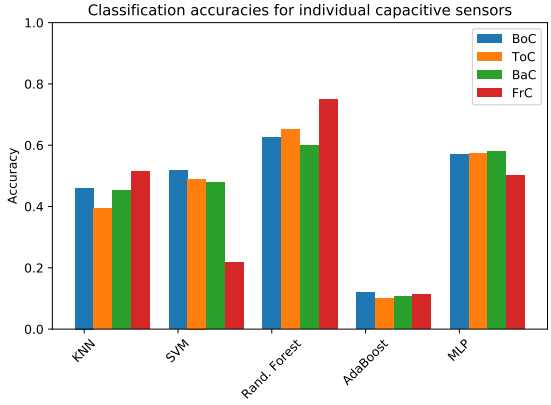

Figure 6: The evaluation results for each of the capacitive sensor. The best accuracy is 74% using from the front sensor (FrC) using the random forest classifier.

the random forest. The combination of all sensors reaches an accuracy of 88.3% which gives a similar result as the capacitive sensors only.

One reason why capacitive sensors perform better than resistive is that they have a higher resolution than the resistive ones ($[0, 2^{14}]$ vs $[0, 2^{12}]$) and a longer time of interaction. This gives more significant data points per sample and, therefore, are much more discriminative.

In our current identification procedure, the data of the resistive sensors do not provide any information to increase the identification result and therefore could be ignored to increase the computation speed. However, the data is needed for other tasks, e.g. detecting a door handle interaction (see Section 5).

Overall, we summarize that we can use touch-sensitive door handles to identify users with a good precision of over 88%.

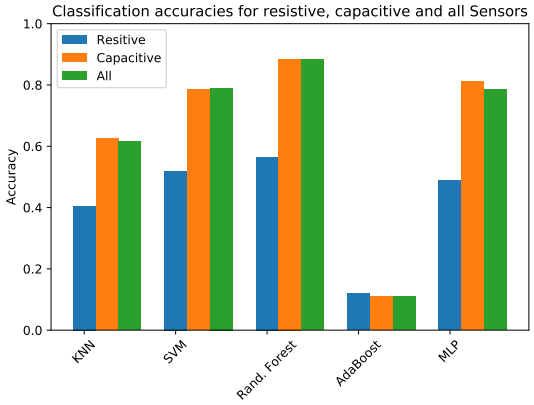

Figure 7: This Figures shows the accuracies of the evaluation results of combined resistive sensors, combined capacitive and the combination of all sensors.

7.3 Qualitative Evaluation

The evaluation of the questionnaire gives insights about the participant's opinion to the door handle authentication system.

First, we look into the answers to the question of how comfortable the usage of our prototype is. The participants answered this question using a 1 to 5 scale where five means the prototype was indistinguishable from using a normal door handle. None of the participants reported difficulties in using the system and they evaluate the comfort with a mean of 4.54.

In a second question, we asked them whether they think if such a door handle technology is an acceptable method for authentication. The participants could answer with *yes* or *no* question to this question. 60% of the participants answered with *yes*. Besides, the users could also add a reason for their answer. They think that a smart door handle is easier and faster to use than using a physical key and can provide more security because it can not be easily stolen. On the other hand, some participants are not convinced that such a method can provide more security. They have concerns about the precision and the uniqueness of the door handle behavior.

8 CONCLUSION and FUTURE WORK

In this paper, we evaluate a system for identifying users at the door opening using their touch behavior. By building a prototype and a user study, we recorded the capacitive and resistive data of 25

participant's door handle behavior. Data exploration and classification showed that the capacitive sensors are more suited for identifying users with an accuracy of 88% and using the random forest classifier. The majority of the participants agreed that this could be an acceptable authentication method but also mentioned concerns about the precision and uniqueness of the door handle behavior.

The next steps are to extend the user study over multiple days to analyze the robustness over the time of this method as well as analyzing the influences of different hands. For example, does the door opening behavior change when we use the other hand, etc. We will also add an accelerometer to the door handle to analyze the door's opening and closing movement. Another step is to analyze the single phases of the door opening process such as *pushing down the door handle, pushing* or *pulling open or closing the door*, etc. to improve the user authentication at the door opening.

REFERENCES

A. Kumar, D. C. M. Wong, H. C. S. and Jain, A. K. (2003). Personal Verification Using Palmprint and Hand Geometry Biometric. In Kittler, J. and Nixon, M. S., editors, *Audio- and Video-Based Biometric Person Authentication*, pages 668–678.

Alam, S. and Yeasin, M. (2019). Person identification with visual summary for a safe access to a smart home. *CoRR*.

Aoyama, S., Ito, K., and Aoki, T. (2013). A multi-finger knuckle recognition system for door handle. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–7. IEEE.

Bigun, J., Fierrez-Aguilar, J., Ortega-Garcia, J., and Gonzales-Rodriguez, J. (2005). Combining biometric evidence for person authentication. In *Advanced Studies in Biometrics*, pages 1–18. Springer.

Brunelli, R. and Falavigna, D. (1995). Person identification using multiple cues. In *IEEE Transactions on Pattern Analysis and Machine Intelligence*, volume 17, pages 955–966.

ChaosComputerClub (2013). Chaos computer club breaks apple touchid. [Online; posted 30-07-2019].

ChaosComputerClub (2017). Chaos computer clubs breaks iris recognition system of the samsung galaxy s8. [Online; posted 30-July-2019].

Garcia, F. T., Krombholz, K., Mayer, R., and Weippl, E. (2016). Hand dynamics for behavioral user authentication. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pages 389–398. IEEE.

Greenberg, A. (2018). Hackers can steal a tesla model s in seconds by cloning its key fob. [Online; posted 09-October-2018].

Ishida, A., Murao, K., Terada, T., and Tsukamoto, M. (2017). A user identification method based on features of opening/closing a refrigerator door. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 533–538. IEEE.

Kusanagi, D., Aoyama, S., Ito, K., and Aoki, T. (2017). A practical person authentication system using second minor finger knuckles for door security. *IPSJ Transactions on Computer Vision and Applications*, 9(1):8.

Marsh, G., Borer, K., Salzbank, Z., Kim, J., and Pruitt, P. (2014). Systems and methods for duplicating keys. US Patent 8,682,468.

Mecke, L., Pfeuffer, K., Prange, S., and Alt, F. (2018). Open sesame! user perception of physical, biometric, and behavioural authentication concepts to open doors. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia*, MUM 2018, page 153–159, New York, NY, USA. Association for Computing Machinery.

Odiete, J., Agbeyangi, A., and Olatinwo, O. (2017). An automated door control system using biometric technology. *IOSR Journal of Computer Engineering (IOSR-JCE) 2278-0661*, 19:20–25.

Pinkert, R. and Tanriverdi, H. (2018). Wie hacker in hotelzimmer eindringen koennen. [Online; posted 25-April-2018].

Schmidt, D., Chong, M. K., and Gellersen, H. (2010). Handsdown: hand-contour-based user identification for interactive surfaces. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries*, pages 432–441.

Varasundar, M. and Balu, R. (2015). Web-based online embedded door access control and home security system based on face recognition. In *International Conference on Circuits, Power and Computing Technologies*.

Wahyudi, W. A. and Syazilawati, M. (2007). Intelligent voice-based door access control system using adaptive-network-based fuzzy inference systems (anfis) for building security. *Journal of Computer Science*, 3:274–280.

Wendt, J. (2015). Apps ersetzen den schluesseldienst. [Online; posted 5-Januar-2015].