Using tap sequences to authenticate drivers

Andrew L. Kun
University of New Hampshire
Electrical and Computer Eng. Dept.
Durham, NH, USA
andrew.kun@unh.edu

Travis Royer
University of New Hampshire
Electrical and Computer Eng. Dept.
Durham, NH, USA
tth3@unh.edu

Adam Leone
University of New Hampshire
Computer Science Department
Durham, NH, USA
aai28@unh.edu

ABSTRACT
Most vehicles only require a key to authenticate the driver. However, with vehicles becoming portals to digital information, many drivers might find this authentication method inadequate. In this paper we explore using tap sequences on the back of the steering wheel to authenticate drivers. Our results indicate that drivers can learn to use an authentication system that uses such taps, and that the system could provide good protection from shoulder-surfing attacks.

Categories and Subject Descriptors
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

General Terms
Measurement, Design, Experimentation, Human Factors

Keywords
Usability, driver identification, driver authentication

1. INTRODUCTION
Security has rarely been a priority of vehicle manufacturers. Most of today's vehicles only require a single authentication factor, a key, to confirm a user's access to its resources. Little work has been done to add a second factor to vehicle security or attempt to confirm the user's identity and access privileges through different channels. However, vehicle security is becoming more of a problem than it used to be in the past. Decades ago thieves could steal our cars, which was bad enough. Today, with our cars becoming portals to digital information, a thief who steals our car might also gain access to our personal information. Even worse, for some professionals, such as law enforcement officers, the car is a portal to remote databases [2] which need to remain secure.

Thus, our long term goal is to provide additional security layers for accessing the car's functions. The goal of the work in this paper is an exploration of one such layer: using taps on the back of the steering wheel. In general, taps are characterized by tap location, by how much pressure we exert when tapping, and by the time between individual taps. In this paper we will explore location and pressure. Specifically, we will explore the feasibility of using three pressure sensors, allowing for taps using three different locations, and allowing the exertion of a different pressure with each tap. We propose three hypotheses:

(H1) Participants can enter sequences of 2-8 taps with three locations to authenticate themselves.

(H2) Participants can enter sequences of 2-8 taps even when each tap is also characterized by low or high pressure.

(H3) A participant sitting next to the driver cannot simply observe the taps (with or without pressure) and then replicate them (i.e. shoulder-surf).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the authors must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

AutomotiveUI '13, October 28 - 30 2013, Eindhoven, Netherlands
Copyright is held by the authors. Publication rights licensed to ACM.
ACM 978-1-4503-2478-6/13/10…$15.00.
http://dx.doi.org/10.1145/2516540.2516567

2. RELATED RESEARCH
A number of researchers have explored the use of biometrics in authenticating drivers. In recent work, Wu and Ye developed a system to identify a driver prior to vehicle use by mapping the veins in his fingers and using an artificial neural network [10], adding a second authentication factor to a vehicle by means of biometrics. Their system worked well in driver identification, achieving an average success rate of 99.2%. Issues arise, however, in regards to the aging of the driver and the changing of finger vein distribution over time.

Reiner and Ferscha used a posture recognition system for driver identification [8], examining pelvic bone distance as a biometric trait for the driver. The system utilized a pressure pad within the seat, thus requiring no active cooperation between the driver and the system. However, changes in clothing thickness, or large objects in the driver's back pocket, could cause the system to fail.

Wakita et al. developed a system to identify drivers by their behavioral patterns while operating a vehicle [9]. They examined variables such as velocity, acceleration patterns, and distance to the lead vehicle, in creating a driver model. Their system worked with 73% accuracy. However, while the system might be useful to automatically change the settings of the family car for different members of the family, it cannot be used to authenticate drivers prior to actual driving.

Our use of the steering wheel as an input location for in-vehicle human-computer interaction builds on promising results by a number of research efforts. In prior work, our group conducted a driving simulator experiment in which drivers initiated speech input to an in-vehicle computer by pressing a glove-mounted switch to the steering wheel [5]. We found that participants were comfortable using this interaction technique. More recently, Murer et al. installed buttons on the back of a steering wheel to allow text input [4]. Their work explored the back of the steering wheel as an interface location, finding that physical feedback was important to users due to the fact that they could not see the buttons. Using more than just buttons, Pfeiffer et al. explored the use of a multi-touch surface on the front of the steering wheel [6] and Pfleging et al. combined interactions on this multi-touch surface with speech-speech interaction [7].

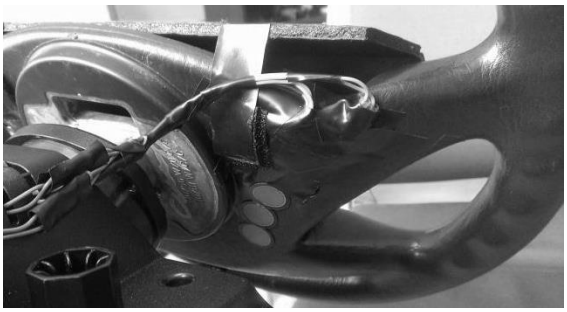

Figure 1. Force sensing resistors on steering wheel.

While tapping has not been explored as a way to identify a driver, Henderson et al. developed a system to identify a user tapping on a piezoelectric sensor attached to a smart card [1]. And in general, patterns of acceleration have been used in security applications, such as by Mayrhofer and Gellersen, who paired two wireless devices that were shaken together by a user [3].

3. EXPERIMENT

3.1 System design

We placed three force sensing resistors (FSRs), on the back of a steering wheel, as shown in Figure 1. The steering wheel was attached to a desk, as shown in Figure 2.

The active area of the sensors is 0.5 inches (about 1.25 cm) in diameter, sized appropriately for finger-touch applications. They are polymer thick film devices which exhibit a drop in resistance when pressure is applied to the active area of the sensor. The sensors are printed onto a flexible substrate, allowing them to be bent as needed. There is also an adhesive on the back of the sensors which allowed for easy mounting to the steering wheel. The FSRs are numbered from top to bottom; these numbers are used to describe which FSRs to tap for a sequence (see Table 1).

The sensors were connected to the analog input pins of an Arduino UNO. The success or failure of authentication, as well as prompts to enter tap sequences, were provided by status lights controlled by the Arduino.

A user authenticates herself by tapping the FSRs according to a hardcoded sequence. We used 15 such sequences in this experiment (see Table 1). Once the sequence is complete (detected by the system as a sufficiently long pause in FSR activity), the system compares the sensor number for each tap of the input sequence to the sensor number for the corresponding tap of the hardcoded password. Optionally, the system also compares the pressure applied to the sensor (low or high) for each tap to hardcoded reference pressures. If the user tapped the correct sequence of FSRs (and optionally applied the correct pressures) then the authentication was successful; otherwise the authentication failed.

3.2 Participants

The experiment was completed by 13 participants. Due to a technical problem we did not record FSR pressure data for one participant and decided to discard his data. The remaining 12 participants (5 female) were University of New Hampshire students between the ages of 19 and 23, with one participant of age 37. They were recruited through email advertisement and received $15 in compensation.

3.3 Tasks

Each participant performed the following three tasks:

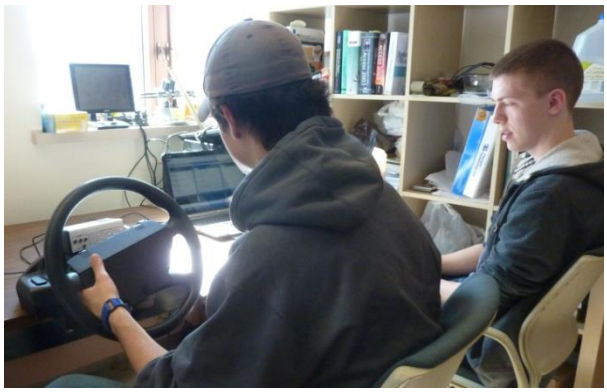

Figure 2. Participant (left) and experimenter. The participant's left hand is placed on the steering wheel, with his fingers on the FSRs.

3.3.1 Tap location task (TLT)

Participants entered six sequences of taps using the FSRs. The sequences are described as ordered lists of FSRs to tap (see Table 1), with each FSR occupying a different location. Participants received the list of sequences in writing, and could refer to the list throughout the task. We ignored the pressure of taps (as long as they exceeded a threshold), as well as their timing (as long as the time between consecutive taps did not exceed a timeout).

3.3.2 Tap location and pressure task (TLPT)

In this task participants entered the same six tap sequences as in the TLT. Again, participants could refer to the list of sequences throughout the task. However, in this task participants also had to pay attention to the pressure of each tap. Specifically, our system differentiated between low and high pressure taps (see Table 1).

3.3.3 Shoulder-surfing task (SST)

In this task an experimenter was seated in front of the steering wheel and the participant was seated on his right. The experimenter entered tap sequences and the participant was instructed to "steal" these sequences. The seating arrangement meant that the steering wheel occluded the experimenter's hand, making it difficult for the participant to steal a tap sequence.

The experimenter entered three different sequences (see Table 1), repeating each sequence five times: a two-tap sequence without pressure, a five-tap sequence without pressure, and a two-tap sequence with pressure. The experimenter told the participant how many taps the upcoming sequence consisted of and if pressure mattered. After entering a sequence five times the experimenter switched seats with the participant, and the participant would attempt to enter the sequence. Participants were allowed a maximum of five attempts to steal the sequence. This process was repeated for each of the three sequences.

Table 1. Tap sequences used in the three tasks.

Seq.	TLT	TLPT	SST
1	3-1	3_L-1_L	1-3
2	1-2-3	1_H-2_H-3_H	3-1-3-3-2
3	2-2-3	2_L-2_L-3_L	2_H-1_L
4	3-2-1-2-3	3_L-2_H-1_L-2_H-3_L	
5	1-2-3-1-2-3	1_L-2_L-3_L-1_H-2_H-3_H	
6	1-1-2-1-2-2-3-2	1_L-1_L-2_H-1_L-2_H-2_H-3_L-2_H	

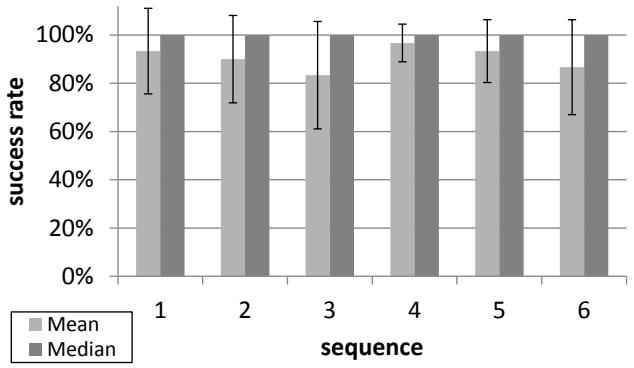

Figure 3. Mean and median success rate for each sequence. Error bars: ±1 SD.

3.4 Procedure

After completing consent and personal information forms, participants completed the three tasks. For TLT and TLPT participants first trained on sequences 1-3 and after becoming comfortable with them, they entered each sequence five times. Next, this procedure was repeated for sequences 4-6. For SST participants completed the task without training. After completing the three tasks participants completed a questionnaire.

3.5 Design

Since incorporating pressure into taps is more difficult than simply tapping, and since shoulder-surfing is more difficult than entering a sequence, we elected not to counterbalance the order of task presentation.

We measured and calculated the following independent variables:

- For the TLT and the TLPT we counted the number of times participants entered the correct sequence. We then calculated the mean and median success rate for each of the six sequences, by averaging success rates over the 12 participants. Finally, we calculated the individual overall success rate for each participant, by averaging their success rates over the six sequences.
- For the SST we counted the number of attempts that it took each participant to enter the correct sequence (minimum 1, maximum 5). We also noted if the participant was unsuccessful in all five attempts. Finally, we counted the number of participants who were able to enter the correct sequence in a maximum of five attempts.
- For all three tasks we asked participants to indicate their level of agreement with preferential statements on a 5-point Likert scale.

4. RESULTS

4.1 Entering known and "stolen" sequences

Figure 3 shows the mean and the median success rate for the six sequences in the TLT (no pressure). All six sequences had a mean success rate above 80%, with four at 90% or higher. For all six sequences the median success rate was 100%. This high median was due to the fact that 9 of the 12 participants had success rates of 93% or higher, averaged over all six sequences. The other 3 participants had success rates between 70% and 77%.

Figure 4 shows the mean and the median success rate for the six sequences in the TLPT (with pressure). The mean success rate ranged from 35% to 95%. The median success rate ranged from 40% to 100%.

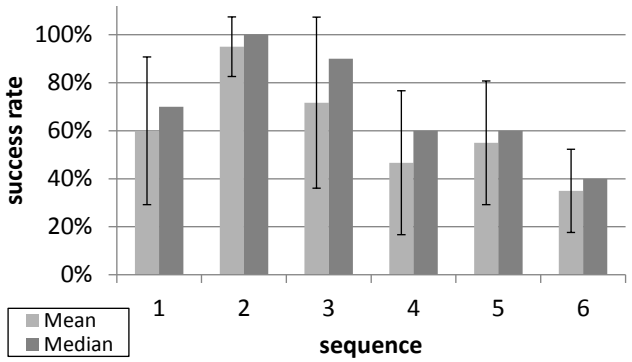

Figure 4. Mean and median success rate for pressure-enabled sequences. Error bars: ±1 SD.

Figure 5 shows the number of participants who were able to steal a sequence entered by the experimenter. Eight of 12 participants were able to steal the 2-tap sequence. On average, it took these 8 participants 2.6 attempts to successfully enter the 2-tap sequence. However, no participants were able to steal the 5-tap sequence, even though this sequence did not include pressure. Only two participants could steal the 2-tap sequence with pressure.

4.2 Preferential statements

The responses to the preferential statements completed after testing help us understand how well the system functions from the viewpoint of a new user. Nine of 12 users agreed that the pressure sensors were in a comfortable location and were comfortable to use with their left hand even though 7 of these 9 were right-handed.

Eight of 12 participants agreed that "the login process [entering tap sequences] was easy". Similarly, 8 of 12 agreed that the process was reliable. Note that for these two statements we did not explicitly identify the process as one that uses pressure or not. When we asked specifically about entering sequences with pressure, only 4 of 12 participants felt that the process was easy, mirroring the results in Figure 4, which indicate that participants had a difficult time entering sequences with pressure.

Regarding shoulder-surfing, none of the participants agreed that it was easy to steal the driver's password by watching him log in, although 50% felt that it was easy to differentiate between the two tap pressures. Four of 12 participants thought that the front of the steering wheel would have been a better sensor position, even at the cost of reduced security; however, 10 of 12 participants considered the tested location to have a good balance between usability and security.

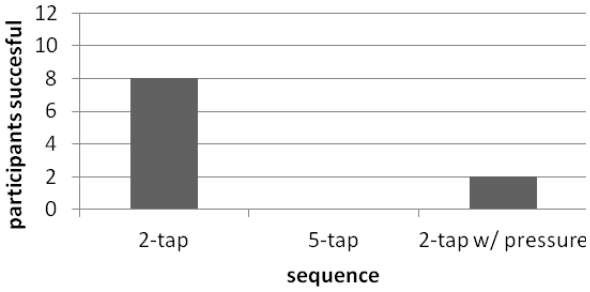

Figure 5. Number of participants to successfully steal a secret 2-tap, 5-tap, and 2-tap w/ pressure sequence.

5. DISCUSSION

We started this study by proposing three hypotheses. We now consider each hypothesis in light of our results.

> (H1) Participants can enter sequences of 2-8 taps with three locations to authenticate themselves.

We tested H1 through the TLT. The results in Figure 3 indicate that participants can indeed enter sequences of 2-8 taps. In fact, 9 of 12 (75%) of our participants were successful in over 90% of their attempts. For these 9 participants the average success rate for each of the six sequences is over 93%. These results support H1.

Still, participants made errors, and this happened even on the two simplest sequences (#1 and #2 in Table 1). Sometimes they missed the sensors entirely, other times they hit more than one sensor at a time, or their fingers rested on a sensor between taps instead of hovering above the sensors. Thus, our results also indicate that there is a need to improve system implementation to help users avoid these errors.

> (H2) Participants can enter sequences of 2-8 taps even when each tap is also characterized by low or high pressure.

We tested H2 through the TLPT. The data presented in Figure 4 indicates that the addition of pressure made it difficult for participants to successfully enter the sequences. It is worth noting that participants needed more time to learn the TLPT than the TLT.

We conducted a paired-samples t-test to assess the effect of including pressure in the tap sequence on participants' overall success rate. We define the overall success rate for a participant as the average success rate on all 30 attempts of entering a sequence in a task (TLT or TLPT). We found that the mean overall success rate was 91% for the TLT (no pressure) and only 61% for the TLPT (with pressure). This large effect size (30%) was highly significant ($p<.001$). Thus, our results do not support H2: adding pressure, at least in our implementation, made it unreasonably difficult to enter sequences.

> (H3) A participant sitting next to the driver cannot simply observe the taps (with or without pressure) and then replicate them (i.e. shoulder-surf).

The data from the twelve participants shows a clear difference in security based both on the number of taps and the pressure evaluation. When a two-tap password was entered, 67% of the participants were able to figure out the password within five attempts. This could be largely attributed to the fact that there are only $3^2=9$ combinations possible at this sequence length. Increasing the number of taps in the sequence to 5 made it impossible for our participants to "steal" the sequence. Similarly, adding pressure to the 2-tap sequence made the task of "stealing" the sequence very difficult, with only 2 participants succeeding in 5 tries. These results support H3 if it is applied to a sequence of "reasonable" length (e.g. 5 taps) or to a shorter sequence that also includes pressure. Of course, our participants had a difficult time correctly entering sequences with pressure. Thus, at least in this implementation of the system, more security can best be achieved with increasing the number of taps in a sequence.

6. CONCLUSIONS

In this paper we explored the feasibility of using taps on the back of the steering wheel to be used for driver authentication in vehicles. Specifically, we conducted an experiment in which participants reproduced tap sequences on three pressure sensors mounted on the back of a steering wheel. We found that participants can successfully input reasonably long tap sequences (up to 8 taps) and that long tap sequences (e.g. those of at least 5 taps) should be difficult to steal in a shoulder-surfing attack. However, we also found that our participants had difficulty reproducing tap sequences in which taps were also characterized by high or low pressure on the sensor. It is quite possible that these difficulties can be blamed on our implementation. Namely, in our system participants had to learn a hardcoded threshold between high and low pressure. It is possible that a user-defined threshold would be more appropriate. Furthermore, our algorithm rigidly identified each tap as having either high or low pressure based on this threshold. A better implementation could identify the user's intent, e.g. based on pressure differences between adjacent taps. Nevertheless, our results are encouraging, as they indicate that the back of the steering wheel is a reasonable space to explore when designing interfaces for driver authentication.

7. ACKNOWLEDGMENTS

This work was supported by the US Department of Justice under grants 2009D1BXK021 and 2010DDBXK226.

8. REFERENCES

[1] Henderson, N.J., and Hartel, P. 2000. Pressure sequence – a novel method of protecting smart cards. *Conference on Smart Card Research and Advanced Applications* (Bristol, UK).

[2] Kun, A.L., Miller, W.T., and Lenharth, W.H. 2004. Computers in police cruisers. *IEEE Pervasive Computing, 3*(4). 34-41.

[3] Mayrhofer, R., and Gellersen, H. 2007. Shake Well Before Use: Authentication Based on Accelerometer Data. *Pervasive 2007* (Toronto, Canada).

[4] Murer, M., Wilfinger, D., Meschtscherjakov, A., Osswald, S., and Tscheligi, M. 2012. Exploring the back of the steering wheel: Text input with hands on the wheel and eyes on the road. *AutomotiveUI 2012* (Portsmouth, NH, USA).

[5] Palinko, O. and Kun, A. 2009. Comparison of the Effects of Two Push-To-Talk Button Implementations on Driver Hand Position and Visual Attention. *Driving Assessment 2009* (Big Sky, MT, USA).

[6] Pfeiffer, M., Kern, D., Schoning, J., Doring, T., Kruger, A., and Schmidt, A. 2010. A multi-touch enabled steering wheel: exploring the design space. *CHI 2010* (Atlanta, GA, USA).

[7] Pfleging, B., Schneegass, S., Schmidt, A. 2012. Multimodal interaction in the car: combining speech and gestures on the steering wheel. *AutomotiveUI 2012* (Portsmouth, NH, USA).

[8] Reiner, A., and Ferscha, A. 2008. Supporting implicit human-to-vehicle interaction: Driver identification from sitting postures. *The First Annual International Symposium on Vehicular Computing Systems* (Trinity College Dublin, Ireland).

[9] Wakita, T., Ozawa, K., Miyajima, C., Igarashi, K., Itou, K., Takeda, K., Itakura, F. 2006. Driver Identification Using Driving Behavior Signals. *IEICE Transactions on Information and Systems, E89-D* (3). 1188-1194.

[10] Wu J. and Ye S. 2009. Driver identification using finger-vein patterns with Radon transform and neural network. *Expert Systems with Applications, 36* (3). 5793-5799.