VibraPass - Secure Authentication Based on Shared Lies

Alexander De Luca
University of Munich
Amalienstr. 17
80333 Munich, Germany
alexander.de.luca@ifi.lmu.de

Emanuel von Zezschwitz
University of Munich
Amalienstr. 17
80333 Munich, Germany
zezschwitz@cip.ifi.lmu.de

Heinrich Hußmann
University of Munich
Amalienstr. 17
80333 Munich, Germany
heinrich.hussmann@ifi.lmu.de

ABSTRACT
Authentication in public spaces is a risky task. Frauds on cash machines (ATMs) are not uncommon nowadays. The biggest group of attacks is observation attacks, which focus on recording the input done by the users. In this work, we present VibraPass, a system created to be resilient against observation attacks using tactile feedback provided by the users' own mobile devices. In this way, secret information is shared between the terminal and the users to add an overhead of 'lies' to the input which makes it hard for attackers to steal the real PIN or password. We present an evaluation, which shows that VibraPass has the potential to replace current authentication systems due to increased security combined with reasonable input speed and error rates.

Author Keywords
Security, Public Terminals, Authentication, Lie Input

ACM Classification Keywords
H5.2. Information interfaces and presentation (e.g., HCI): User Interfaces-Input devices and strategies, evaluation.

INTRODUCTION
Interaction with public terminals and large public displays becomes more and more part of our everyday's life. There are several services that require interaction with public terminals. Examples are train ticket vending machines, quick check-in counters or ATMs.

Despite their many advantages like efficient in- and output capabilities, they comprise severe privacy and security risks. A successful attack on an ATM, for instance, can grant access to the user's bank account. Due to their location and mostly unlimited availability, they can be manipulated, for instance to record the input done by a user. The most common attacks are based on camera recordings or simple shoulder-surfing [5].

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. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
CHI 2009, April 4–9, 2009, Boston, MA, USA.
Copyright 2009 ACM 978-1-60558-246-7/09/04...$5.00.

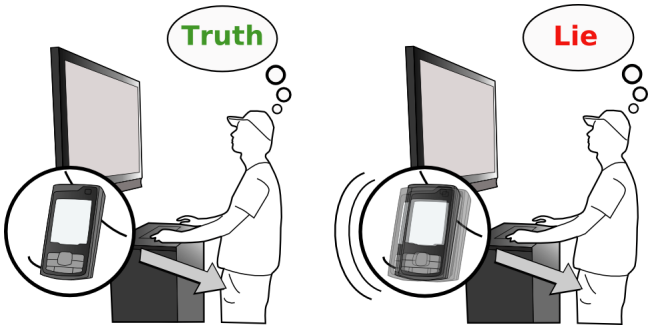

Figure 1: VibraPass. When the mobile phone vibrates, the user enters a false character, if not, a correct one.

The most important interaction with public terminals is authentication, which is carried out nowadays mainly either by PIN or passwords. In order to safeguard authentication against attacks, we developed VibraPass, a system to increase the security of public authentication, which will be presented in this paper. Enhanced security is achieved by utilizing the vibration function of the user's mobile devices as an invisible communication channel. This way, an overhead consisting of 'lies' can be enforced by the terminal to make it hard for attackers to spy on the real input done by the users, which makes it resilient against any form of observation attacks. We conducted a formal evaluation that shows promising results for VibraPass.

RELATED WORK
Private and secure interaction with public terminals has been approached in many different ways, mostly reduced to solving the problem of authentication. The approaches can be roughly divided in three categories.

The first one tries to solve the problem on a software level. That is, software is designed in a way that makes it hard for onlookers to spy on the input. Examples for this approach are the *Spy-resistant (software) keyboard* by Tan et al. [9] and the *PIN-entry method* developed by Roth et al. [6]. Similar to VibraPass, both add additional steps (overhead) to the input to hide it from onlookers. The weakness of software based solutions is that they are not resilient against attacks based on visual recordings.

Using additional input hardware is characteristic for the second category. The most famous example is probably biometric authentication as tested by Coventry et al. [1] on ATMs.

Other work in this field has been performed by evaluating the appropriateness of eye-tracking for authentication on public terminals [3]. *Tactile PIN Entry* by Deyle et al. [2] and *Undercover* by Sasamoto et al. [7] use tactile feedback for authentication (like VibraPass) given by devices attached to the terminal. For instance, *Undercover* uses the movement of a ball that can only be felt by the user holding it. This movement has to be interpreted as different number pad layouts that are used to define a password picture within a set of five pictures. The main problem of the approaches using additional fixed hardware is that the hardware can be manipulated since public terminals are generally publicly available to everyone. Compared to these approaches, VibraPass is resilient against this kind of manipulation since the mobile device is possessed by the users.

Private interaction with public displays based on hardware owned by the users is the last category. This hardware cannot (or hardly) be manipulated by attackers since it is carried by the users. For instance in [4], mobile phones with acceleration sensors are used to authenticate with public terminals. Sharp et al. [8] developed a system that utilizes the users' PDAs to interact with public terminals. While the information on the terminal is blurred, interaction takes place on the PDA that displays a non blurry version.

CONCEPT

To enable secure authentication on public terminals, VibraPass introduces the lie overhead. PINs and Passwords are enriched with 'lies', i.e. redundant interactions that do not contribute to the actual authentication and confuse an observer. This additional information is randomly mixed with the real PIN/password. The knowledge about lies is shared secretly between the terminal and the user. Therefore, the terminal can extract the real password from the input.

In VibraPass, this knowledge is shared utilizing the users' mobile devices. Each current mobile phone, PDA and the like is equipped with vibration functionality. That is, they provide a tactile output channel, which is an appropriate way to transport simple messages like 'true' or 'false'.

VibraPass works as follows: (1) The user connects her mobile device to the terminal. This is necessary each time the user wants to interact with a terminal. (2) The terminal creates a random sequence of lies based on the lie overhead. The randomization prevents attacks based on knowledge of the order of lies. An example sequence of lies for a four-digit PIN could be "0,1,0,0,1,0" (0 means truth and 1 means lie/vibration). (3) The user enters her PIN or password. Every time the mobile device vibrates, the terminal indicates to the user that for the next input she should lie (figure 1 right). When the device remains quiet, the next part of the real password/PIN should be input (figure 1 left).

As mentioned before, VibraPass provides enhanced security for public authentication while relying on basic input mechanisms of the terminal. That is, no additional hardware (besides a communication module like Bluetooth) is necessary on terminal side. Theoretically, VibraPass could be used to enter arbitrary amounts of information on public terminals. Due to its nature of adding overhead to the input it seems more suitable for short authentication tokens.

Doing the input directly at the mobile device would require transmitting the password/PIN and would make it vulnerable to man-in-the-middle attacks. In VibraPass, no sensitive data is transmitted but only 'vibrate' commands. Thus, cracking the input in one time would require a synchronized camera and sniffing attack.

The main weakness of VibraPass is that repeated observations can lead to successful attacks by analyzing the differences between inputs. The highest success rate for an attack can be assumed if the lie overhead is known by the attacker. For instance, two recordings can lead to breaking a four-digit PIN when the smallest overhead is used. In real world situations this threat is minimal since manipulated terminals are usually quickly repaired and users mostly do not interact twice with the same terminal within a short time.

EVALUATION

VibraPass has been evaluated with a lightweight prototype written in JavaSE (terminal) and JavaME (mobile application). Bluetooth has been used for communication. A public terminal has been set up in a public corridor of our labs consisting of a 42 inch screen and a keyboard connected to it. Two cameras, one pointing at the keyboard and the other recording the whole interaction from the right side, were installed as well as two microphones (co-located with the cameras). The recordings have been used for usability as well as security analysis. Participants were equipped with a Nokia N80 mobile phone placed in the pockets of their trousers. Synchronization between the user and the terminal has been achieved by sending the vibration signal immediately with the release of the previous button. No participant had major issues with this approach.

User Study Design

VibraPass was evaluated using a repeated measures within participants factorial design. The independent variables were *PwType* (random PIN, random password, user generated PIN, user generated Password), *PwLength* (4 and 8) and *LieOverhead* (0%, 30%, 50%, 100%). The lie overhead of 0% represents the control condition since it is identical to standard PIN/password entry without lying.

The task was to authenticate with the terminal using every combination of the independent variables (*PwType x PwLength x LieOverhead* = 32 authentication sessions). The order of *PwType* was counterbalanced between the participants, while the order of *PwLength* and *LieOverhead* has been randomized to minimize learning effects.

Procedure

At the beginning, the prototype was explained in detail to each participant. They were encouraged to train until they felt familiar with it. When the participants felt ready, they were

asked to define two private passwords and two private PINs (each length 4 and 8). Randomized passwords/PINs were provided on printed lists. Randomized passwords were generated using a vowel as every second letter to increase readability and memorability**.** Each password/PIN was only used once not to influence the results. In the next step, the participants were equipped with the mobile device, which was already connected to the terminal via Bluetooth.

At the beginning of each authentication session, the terminal informed the current participant, which password to choose from the lists and created a randomized lie sequence based on the current lie overhead. Every key press, correction, error etc. were logged. For each authentication session, there was a maximum of three tries to fill in the right authentication token. Changing to the next session took place whenever the previous one had been filled out correctly or failed three times. In the end, each participant had to fill out a questionnaire. Ratings were given using Likert scales from 1 (don't agree) to 5 (highly agree).

Hypotheses

Based on first evaluations of VibraPass, the following main hypotheses were stated: (H1) VibraPass is more secure to observation attacks than standard PINs/passwords. (H2) Error rate increases a) the higher the lie overhead and b) the longer the password. (H3) Interaction time increases a) the higher the lie overhead and b) the longer the password.

Participants

The study was conducted with 24 volunteers with an average age of 23 years, eight of them female. All of them own mobile phones with vibration functionality. Choosing 24 participants allowed perfect counterbalance of *PwType* to minimize learning effects. Thus, Results are based on 768 authentication sessions performed by 24 participants.

Results

Error Rate

Performance in sense of low error rates is crucial for authentication since tries are limited on public terminals. For instance, most ATMs confiscate the users' bank card once the PIN has been wrongly input three times. Therefore, we have to differentiate between two types of errors: basic errors that indicate that at maximum two tries of the authentication session failed, and critical errors, which indicate that the authentication session failed completely.

Out of the 768 authentication sessions, 63 (8%) were performed with at least one wrong input (including critical errors). Four of them (0.5%) using a *LieOverhead* of 0%. 19 (2.5%) sessions ended in critical errors. None with a lie overhead of 0% or 30% created a critical error. 557 out of the 576 (96.7%) sessions using a lie overhead bigger than 0% could be completed successfully.

Even though error rates for VibraPass are quite low, it is worth taking a closer look at which levels of the independent variables influence critical errors.

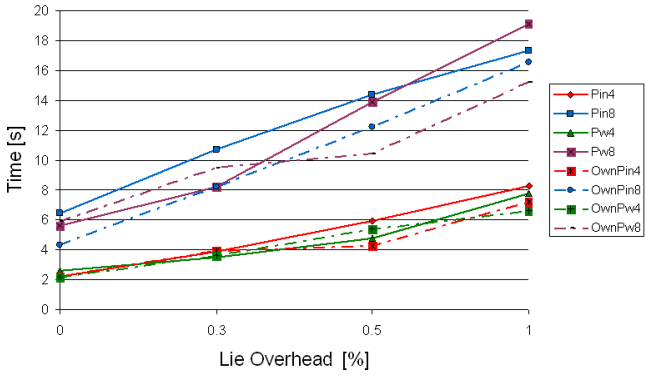

Figure 2: Average interaction times for different combinations of LieOverhead, PwType and PwLength.

A 4 x 2 x 4 (*PwType x PwLength x LieOverhead*) within participants analysis of variance of critical errors showed significant main effects for *PwLength* ($F_{1,23}$ = 9.70,p<.05) and *LieOverhead* ($F_{3,69}$ = 7.24,p<.05). No significant interaction effects could be found. Post hoc tests revealed that the difference in the occurrence of critical errors using *PwLength* of 8 (15 out of the 19 critical errors) compared to 4 critical errors with *PwLength* 4 is significant (p<.05). No critical errors occurred using levels of 0% and 30%. Thus, the 19 critical errors all occurred with lie overhead of 50% (5 out of 19) and 100% (14 out of 19). The post hoc tests revealed significant differences between *LieOverhead* level 100% and 0% and between level 100% and 30%. These results mainly support hypothesis (H2) a) and b) with the exception that 30% did not create any critical errors.

Interaction Speed

Interaction time has been measured for each authentication session from the first key press to releasing the last key. Failed sessions were excluded from the analysis. Figure 2 depicts the average interaction times for all combinations. It shows that mostly interaction time increases when *LieOverhead* is increased. It also shows the increase of time needed for authentication with *PwLength* of level 8 (upper four lines) compared to level 4 (lower four lines). Nevertheless, when comparing the time needed for four-digit random PINs with lie overhead 0% (mean: 2.23s; sd:0.86s) to four-digit random PINs with lie overhead 30% (mean: 3.91s; sd:1.70s), the time needed for the more secure variant is still within a reasonable range.

A 4 x 2 x 4 (*PwType x PwLength x LieOverhead*) within participants analysis of variance showed significant main effects for *PwLength* ($F_{1,13}$ = 131.35; p<.001) and *LieOverhead* ($F_{3,39}$ = 107.59; p<.001). A significant interaction effect was found for *PwLength x LieOverhead* ($F_{3,39}$ = 21.06; p<.001). Post hoc comparisons showed significant differences (p<.001) in interaction speed between *PwLength* with level 4 (mean: 4.65s; se:0.33s) and level 8 (mean: 11.14s; se: 0.72s). Comparing the different levels of *LieOverhead* showed significant results as well (all p<.001). These results confirm hypothesis (H3) a) and b). Regarding interaction effects of *PwLength x*

LieOverhead, results show that changing *PwLength* influences interaction time when increasing *LieOverhead*. This result is significant for all levels of *PwLength x LieOverhead* (all $p<.05$, most $p<.001$).

Security Evaluation

We evaluated the security of VibraPass based on a worst case scenario. We set up two video cameras, one filming the keyboard from above and one filming the users from the right side. Two microphones were used to record the audio part (e.g. audible vibration). To make the attacks even more efficient, we assumed that the attacker knows as well the lie overhead as the length of the input and we chose a mobile phone with a very loud vibration alert.

The video recordings were analyzed abiding to strict rules to ensure mostly unbiased results. The question was how many passwords and PINs could be stolen by an attacker. It should be highlighted that it is next to impossible to have such optimal conditions in the real world since public terminals are usually located in rather crowded and noisy places and that this decision has been made to evaluate the security of VibraPass with a worst-case scenario.

Out of the 749 successful authentication sessions, 100% with a lie overhead of 0% could be identified (192 sessions). VibraPass enhanced authentication sessions only revealed the true password/PIN in 32.5% of the cases (181 out of 557). The main reason for successful attacks was audible vibrations, for example due to keys in the pockets of the participant (140 out of 181). Only 41 attacks (7.3%) would have been successful without a perfect audio recording. A 4x2x4 (*PwType x PwLength x LieOverhead*) within participants analysis of variance showed only a significant main effect for *LieOverhead* ($F_{3,39} = 28.53$; $p<.001$) and no interaction effects. Post-Hoc tests revealed that only the differences between *LieOverhead* 0% (100% successful attacks) and all *LieOverhead* > 0% were significant (all $p<.05$). These results support hypothesis (H1). We argue that in real world use, the number of successful attacks is more likely to be what we found without hearable vibrations.

The most interesting finding is reasons for the other successful attacks, 'bad lies'. Examples for bad lies include repeated pressing the same key, confused waiting before pressing and using characters as lies for PINs.

User Preferences

In the questionnaire, participants were asked to rate their preferences regarding the levels of lie overhead. The results showed that all participants preferred either a low lie overhead of 30% (13 participants) or the medium lie overhead of 50% (11 participants). Lie overhead of 0% as well as 100% were favored by none of the participants. As a reason for liking 30% - 50%, most participants mentioned they found it still very easy to use but more secure. One participant called the medium lie overhead a "*good trade-off between usability and security*". The analysis of the participants' answers regarding security and ease-of-use encourage the use of a lie overhead between 30% - 50%, depending on the password length. Security for 30% was rated 3.6 compared to 2.3 for standard authentication. Regarding ease-of-use, both were considered fairly easy (4.7 for 0%, 4.2 for 30%, 3.2 for 50% and 2.1 for 100%).

CONCLUSION AND FUTURE WORK

The evaluation showed that VibraPass has the potential to increase security while providing low error rates and fast input speed. VibraPass with a lie overhead between 30% and 50% seems an appropriate trade-off between usability and security. It highly increases security but still provides a reasonable input speed with low error rate. In fact, in sense of error rates lie overhead 30% performed as good as standard password and PIN since it did not result in any failed authentication session. It also provides an input speed close to standard PIN and password entry. The qualitative data collected from the participants supports this conclusion.

During the study, some starting points for future work became apparent. For instance, real world issues like users without trousers and thus without pockets (e.g. women wearing skirts) were found. The most interesting finding is on the quality of lies. The security evaluation showed that all successful attacks besides hearing the vibration were due to 'bad lies' like repeated pressing of the same character. Therefore, we are planning to conduct a long-term study to find out whether lies can improve after repeated use of the system and if they have influence on the recall of PINs.

REFERENCES

1. Coventry, L., De Angeli, A., Johnson, G. Usability and biometric verification at the atm interface. In *Proc. CHI '03*.
2. Deyle, T., Roth, V. Accessible authentication via tactile pin entry. *CG Topics*, Issue 3, Mar. 2006.
3. Kumar, M., Garfinkel, T., Boneh, D., Winograd, T. Reducing shoulder-surfing by using gaze-based password entry. In *Proc. SOUPS '07*.
4. Patel, S.,Pierce, J. Abowd, G. A gesture-based authentication scheme for untrusted public terminals. In *Proc. UIST '04*.
5. Rogers, J. Please enter your 4-digit pin. *Financial Services Technology*, U.S. Edition, Issue 4, Mar. 2007.
6. Roth, V., Richter, K., Freidinger, R. A pin-entry method resilient against shoulder surfing. In *Proc. CCS '04*.
7. Sasamoto, H., Christin, N., Hayashi, E.. Undercover: authentication usable in front of prying eyes. In *Proc. CHI '08*.
8. Sharp, R., Scott, J., Beresford, A.R. Secure mobile computing via public terminals. In *Proc. Pervasive '06*.
9. Tan, D., Keyani, P., Czerwinski, M. Spy-resistant keyboard: more secure password entry on public touch screen displays. In *Proc. OZCHI '05*.