LookUnlock: Using Spatial-Targets for User-Authentication on HMDs

Markus Funk
TU Darmstadt / Siemens CT
Darmstadt, Germany
funk@tk.tu-darmstadt.de

Karola Marky
TU Darmstadt
Darmstadt, Germany
marky@tk.tu-darmstadt.de

Iori Mizutani
University of St. Gallen / Siemens CT
St. Gallen, Switzerland
iori.mizutani@unisg.ch

Mareike Kritzler
Siemens CT
Berkeley, CA, USA
mareike.kritzler@siemens.com

Simon Mayer
University of St. Gallen / Siemens CT
St. Gallen, Switzerland
simon.mayer@unisg.ch

Florian Michahelles
Siemens CT
Berkeley, CA, USA
florian.michahelles@siemens.com

ABSTRACT

With head-mounted displays (HMDs), users can access and interact with a broad range of applications and data. Although some of this information is privacy-sensitive or even confidential, no intuitive, unobtrusive and secure authentication technique is available yet for HMDs. We present LookUnlock, an authentication technique for HMDs that uses passwords that are composed of spatial and virtual targets. Through a proof-of-concept implementation and security evaluation, we demonstrate that this technique can be efficiently used by people and is resistant to shoulder-surfing attacks.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5971-9/19/05.
https://doi.org/10.1145/3290607.3312959

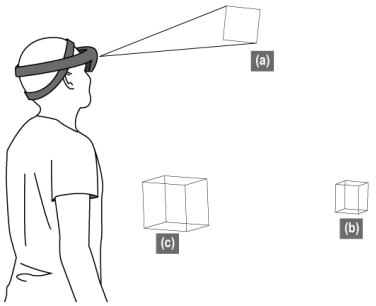

Figure 1: A user is using the LookUnlock concept to enter graphical passwords in the environment using a head-mounted display.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**;

KEYWORDS

Augmented Reality; Usable Security; Authentication; Head-Mounted Displays; Spatial Passwords

ACM Reference Format:
Markus Funk, Karola Marky, Iori Mizutani, Mareike Kritzler, Simon Mayer, and Florian Michahelles. 2019. LookUnlock: Using Spatial-Targets for User-Authentication on HMDs. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI'19 Extended Abstracts), May 4–9, 2019, Glasgow, Scotland UK.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3290607.3312959

INTRODUCTION & BACKGROUND

Smart eye-ware, such as head-mounted displays (HMDs), has become more usable and less bulky over the past decades. This enables HMDs to be used in many real-world scenarios and across a variety of use-cases, such as assembly assistance [2], navigation [8] and programming smart environments [4]. HMDs are used to provide Augmented Reality (AR) feedback or data that is only visible to the wearer. This data might be confidential or privacy-sensitive and must therefore be protected from unauthorized access.

To authenticate users in such settings, an obvious method would be textual passwords. However, gesture-based text entry on HMDs is very cumbersome and voice-based entry cannot be used since bystanders could easily hear the password. More convenient methods require an additional text entry device, such as a smart haptic glove [5] or a Twiddler [6], which is often impractical. Biometric authentication, such as fingerprints, is another possibility for authenticating users on HMDs, but also introduces privacy concerns and security risks [7] that can lead to adoption issues. Existing work for authentication on HMDs thus focuses on biometric approaches [9], out-of-band authentication using an additional device (e.g., a wristband [11]), or the combination of several wearable computing devices to create novel authentication mechanisms [1]. Recently, transferring traditional unlock approaches to virtual environments was proposed [3].

In this paper we present *LookUnlock*, a graphical authentication mechanism based on head-gaze tracking and spatial mapping. LookUnlock enables authentication on HMDs without the need of an additional device by using passwords that are constructed from spatial and virtual objects – a password in our system is thus a set of spatial and/or virtual objects that a user focuses on in the correct sequence. We present design considerations to decide under which circumstances different variants of LookUnlock are most effective, and provide a security evaluation.

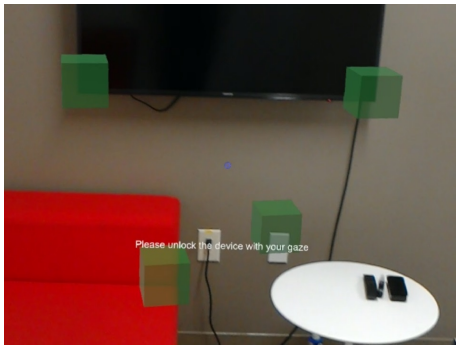

Figure 2: A spatial password that sticks to objects in the physical world. (Here depicted in green for a better visibility)

Figure 3: A virtual password consisting of free-floating virtual objects.

LOOKUNLOCK: SPATIALLY-AWARE PASSWORDS

LookUnlock uses head-gaze tracking and spatial mapping for entering passwords on HMDs. The graphical LookUnlock passwords can be defined by: (1) using objects that are available in the physical world (*Spatial Passwords*), (2) objects in the virtual world (*Virtual Passwords*) or (3) a combination of physical and virtual objects (*Hybrid Passwords*).

Spatial Passwords. Spatial passwords consist of a sequence of different spatial targets, i.e. the individual characters of a spatial password are 3D coordinates in the user's physical environment. – these locations can (but do not need to) overlap with physical objects in the environment. They thus add an additional layer of protection in scenarios where an HMD should only be used at a specific place.

To set a spatial password, the user selects spatial targets in the environment by navigating the HMD's cursor onto an object or surface in the environment and performing an enter action (e.g., an AirTap gesture of the HoloLens). In response, our system creates an invisible 3D cube of a predefined size that is created at the position where the cursor and the model of the room intersect (see Figure 2). To perform an unlocking procedure, the user enters the spatial password by placing the cursor over the previously defined spatial targets using the head-gaze.

Virtual Passwords. Virtual passwords consist of virtual targets, i.e. 3D models of objects that spawn at random positions in the proximity of the user (see Figure 3). Virtual targets are not aligned with any physical object and therefore their positions can be randomized. This means that each time a virtual password is entered, the virtual targets are spawning at different positions in the 3D space. This creates an additional level of security against observers, however it also increases the difficulty for the user to find the correct virtual unlock target. In contrast to spatial passwords, purely virtual passwords can be used independently from the environment where the password was defined. Setting a password and unlocking are analogously to spatial passwords, but 3D models of objects are required as virtual targets.

Hybrid Passwords. Hybrid passwords combine spatial targets and virtual targets and enable the user to define any combination of target types. An example for a four-character hybrid password is a password that consists of three spatial targets around the visual features of a door and a virtual target (e.g., the virtual hydrant; see Figure 4).

As the combination of virtual and spatial real-world targets also depends on the location where the spatial targets have been defined in, this variant also only works in those very environments where the password has been defined (or replicas thereof).

Mitigation of Brute-Force Attacks

Brute-forcing targets by scanning the entire room with the cursor or trying all combinations of virtual and spatial is a security risk for LookUnlock passwords.

Figure 4: A hybrid password combines virtual and spatial targets.

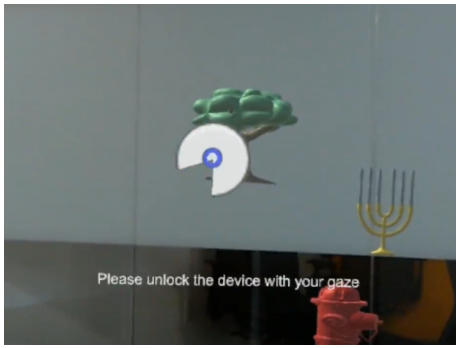

Figure 5: A dwell to unlock approach prevents involuntarily logging in false targets.

[1]Microsoft HoloLens: https://www.microsoft.com/en-us/hololens

Spatial Passwords. To mitigate brute-force attacks on spatial passwords, LookUnlock limits the available time in-between entering spatial targets. In an informal preliminary user test we found that a timeout of 3000*ms* represents a good trade-off between security and usability of the system. However, we did not implement a time limit for finding the *first* spatial target of a password since we cannot be certain that a user is actively trying to perform an unlock action prior to the first spatial target.

Virtual Passwords. LookUnlock uses the *dwell-to-select* approach (inspired by Yu et al. [10]) to (1) mitigate brute-force attacks and to (2) enable the selection and entering of a target as part of the same user action. The user selects a virtual target by moving the cursor on top of it. While the cursor is on top of the target, over the time of 1500ms, a circle starts building up to indicate the selection progress (see Figure 5). If the cursor is still on the virtual target after 1500ms, the target is entered and the virtual target is checked for correctness. If the entry was incorrect, the system prevents the user from entering another virtual target and aborts the entry process. If the entered virtual target was correct, the password is either complete or the next virtual target can be selected and entered.

Hybrid Passwords. For hybrid passwords, combining the brute-force prevention techniques for spatial targets and virtual targets would give away the type of the next expected target. However, being able to mix spatial and virtual targets is one of the main factors that make hybrid passwords more resistant against attacks. We therefore chose to implement the same brute-force mitigation technique as for entering *virtual passwords*, i.e. the *dwell-to-select* approach.

EVALUATION: SHOULDER SURFING

In order to evaluate LookUnlock, we created a prototype for the Microsoft HoloLens[1]. Since bystanders in the user's proximity might observe the definition and entering of passwords, we conducted a user study to investigate LookUnlock's protection against such "shoulder surfing" attacks.

Method and Procedure

We designed the study according to a repeated measures design with the used password type as the only independent variable. As dependent variables, we measured the number of trials and whether guessing the password was successful. We counterbalanced the order of the password types according to the Balanced Latin Square.

To provide a more realistic scenario in which the bystander can move around, the experimenter interacted live with LookUnlock. Our study's procedure was as follows: After welcoming the participant, we described the purpose of the study and familiarized the participant with all three LookUnlock password types. Then, we explained that the task in this study is to attack these 4-objects long passwords and try to guess them by observing the experimenter. To prepare for this password attacking task, we showed how the experimenter enters one password of each password type that is known to the participant.

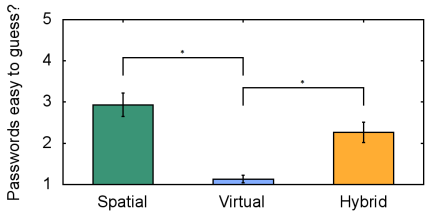

Figure 6: The average responses of the Likert scale questionnaire indicating the perceived difficulty for guessing the password according to the different password types. All error bars depict the standard error. The * indicates a significant difference between the variants ($p < .05$).

While participants were allowed to observe the password entry process by the experimenter as often as they wished, they were given only three attempts to enter the correct password after their observation. We counted the number of trials and recorded if guessing the password was successful or not. To increase the chances of a successful guess, we told the participant which LookUnlock password type is used in each condition. In the hybrid condition, we additionally asked the participant to guess for each element whether it is a virtual or a spatial target. When the participant confirmed that the rules were understood, performed three test rounds: one for each password type. In the study, we use three passwords per password type resulting in nine different passwords. After trying to guess all passwords of one password type, we asked the participant to fill in a questionnaire. We repeated this procedure for all three password types.

Results

We recruited 15 participants (13 male, 2 female) who were between 23 and 63 years old ($M = 33.2$, $SD = 10.12$) years old and were mostly students and researchers. The participants were not reimbursed.

Overall, in the study each password type was attempted to be hacked 135 times. Considering the quantity of correctly guessed passwords, the spatial passwords were the most vulnerable with 8 successful attempts (5.9%), followed by the the hybrid passwords with 5 successful attempts (3.7%). The virtual passwords could not be guessed at all. A one-way repeated measures ANOVA showed a statistically significant difference in the amount of correctly guessed passwords, $F(2, 28) = 1.2$, $p = .028$. The post-hoc test revealed a significant difference ($p < .05$) between the spatial and virtual passwords. The effect size estimate shows a large effect ($\eta^2 = .225$). To account for multiple testing, all post-hoc tests were Bonferroni-corrected. At the end of each test in the hybrid condition, we asked the participants to identify for each of the four password characters whether it is a virtual or a spatial target. The types of 153 out of 180 elements were guessed correctly (85%).

We also asked participants to rate the perceived difficulty for guessing each password type on a 5-point Likert scale with *1 = "very difficult"* and *5 = "very easy"*. The virtual passwords were perceived as the most difficult ($M = 1.13$, $SD = .35$) followed by the hybrid passwords ($M = 2.27$, $SD = .96$) and the spatial passwords ($M = 2.93$, $SD = 1.1$). A one-way repeated measures ANOVA showed a statistically significant difference in the perceived difficulty, $F(2, 28) = 24.844$, $p < .001$. The post-hoc test revealed a significant difference ($p < .05$) between the virtual and both other password types. The effect size estimate shows a large effect ($\eta^2 = .611$). Figure 6 graphically depicts the results.

DISCUSSION AND CONCLUSION

In this paper, we presented LookUnlock, a technique for leveraging spatial awareness and head-gaze for user authentication on HMDs. We presented three types of passwords: spatial passwords, virtual passwords, and hybrid passwords.

Through a user study we assessed the resistance of all LookUnlock password types to shoulder surfing attacks. We found that spatial passwords were the most vulnerable while virtual passwords were not guessable in a total of 135 attempts. Also, we told the attackers details about each used password type, e.g., the number of objects used for a password, and the password type. Therefore, the attackers can be considered as trained experts with prior knowledge about password parameters. In reality the training level of attackers might vary more, which might yield different (and presumably worse) success rates. LookUnlock passwords might suffer from users tending to choose certain targets more likely than others, analogously to other graphic and textual authentication methods. Therefore, the impact of environment features needs to be investigated.

REFERENCES

[1] Andrea Bianchi and Ian Oakley. 2016. Wearable authentication: Trends and opportunities. *it-Information Technology* 58, 5 (2016), 255–262.

[2] Sebastian Büttner, Markus Funk, Oliver Sand, and Carsten Röcker. 2016. Using Head-Mounted Displays and In-Situ Projection for Assistive Systems: A Comparison. In *Proceedings of the 9th ACM International Conference on PErvasive Technologies Related to Assistive Environments*. ACM, 44. https://doi.org/10.1145/2910674.2910679

[3] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS.

[4] Valentin Heun, Shunichi Kasahara, and Pattie Maes. 2013. Smarter objects: using AR technology to program physical objects and their interactions. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. ACM, 961–966. https://doi.org/10.1145/2468356.2468528

[5] Yi-Ta Hsieh, Antti Jylhä, Valeria Orso, Luciano Gamberini, and Giulio Jacucci. 2016. Designing a Willing-to-Use-in-Public Hand Gestural Interaction Technique for Smart Glasses. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 4203–4215.

[6] Kent Lyons, Thad Starner, Daniel Plaisted, James Fusia, Amanda Lyons, Aaron Drew, and EW Looney. 2004. Twiddler typing: one-handed chording text entry for mobile phones. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 671–678. https://doi.org/10.1145/985692.985777

[7] Caroline Lancelot Miltgen, Aleš Popovič, and Tiago Oliveira. 2013. Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems* 56 (2013), 103–114.

[8] Umair Rehman and Shi Cao. 2015. Augmented Reality-Based Indoor Navigation Using Google Glass as a Wearable Head-Mounted Display. In *Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference on*. IEEE, 1452–1457. https://doi.org/10.1109/SMC.2015.257

[9] Stefan Schneegass, Youssef Oualil, and Andreas Bulling. 2016. SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 1379–1384. https://doi.org/10.1145/2858036.2858152

[10] Chun Yu, Yizheng Gu, Zhican Yang, Xin Yi, Hengliang Luo, and Yuanchun Shi. 2017. Tap, Dwell or Gesture?: Exploring Head-Based Text Entry Techniques for HMDs. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 4479–4488. https://doi.org/10.1145/3025453.3025964

[11] Ruide Zhang, Ning Zhang, Changlai Du, Wenjing Lou, Y Thomas Hou, and Yuichi Kawamoto. 2017. AugAuth: Shoulder-Surfing Resistant Authentication for Augmented Reality. In *Proc. of the 2017 IEEE International Conference on Communications*.