Design Considerations for Secure and Usable Authentication on Situated Displays

Ludwig Trotter
Lancaster University
Lancaster, United Kingdom
LMU Munich
Munich, Germany
l.k.trotter@lancaster.ac.uk

Nigel Davies
Lancaster University
Lancaster, United Kingdom
n.a.davies@lancaster.ac.uk

Sarah Prange
University of Applied
Sciences Munich
LMU Munich
Munich, Germany
sarah.prange@hm.edu

Florian Alt
University of Bundeswehr Munich
University of Applied
Sciences Munich
LMU Munich
Munich, Germany
florian.alt@unibw.de

Mohamed Khamis
University of Glasgow
Glasgow, United Kingdom
mohamed.khamis@glasgow.ac.uk

Submitted to MUM '18 poster track. Do not cite, do not circulate.

Abstract

Users often need to authenticate at situated displays in order to, for example, make purchases, access sensitive information, or confirm an identity. However, the exposure of interactions in public spaces introduces a large attack surface (e.g., observation, smudge or thermal attacks). A plethora of authentication models and input modalities that aim at disguising users' input has been presented in the past. However, a comprehensive analysis on the requirements for secure and usable authentication on public displays is still missing. This work presents 13 design consideration suitable to inform practitioners and researchers during the development process of authentication systems for situated displays in public spaces. It draws on a comprehensive analysis of prior literature and subsequent discussion with five experts in the field of pervasive displays, human-computer-interaction and usable security.

Author Keywords

Authentication; Touch; Gaze; Mid-Air Gestures; Public Displays.

ACM Classification Keywords

H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous; See [http://acm.org/about/class/1998/]: for full list of ACM classifiers. This section is required.

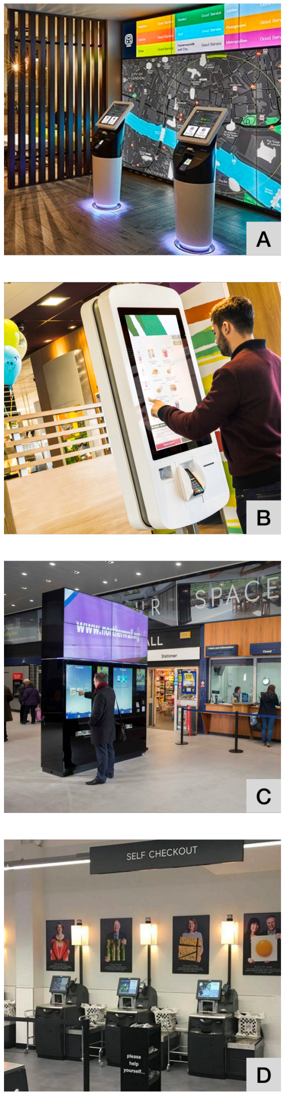

Figure 1: Users often need to authenticate on public displays e.g., self-service hotel receptions (A), food ordering systems (B), ticket machines (C), and self-service checkouts (D)

Introduction & Background

There is an increasing need for users to authenticate on terminals in public spaces. On the one hand, the portfolio of digital consumer services in public spaces is being permanently expanded. On the other hand, employees are more and more replaced by situated self-service terminals [21]. Examples include, but are not limited to, systems like self-service hotel receptions (see figure 1.A), interactive food ordering systems (see figure 11.B), ticket machines (see figure 1.C), and self-service checkouts in supermarkets (see figure 1.D).

However, prior research has highlighted challenges for designing interactions with displays in public spaces [7]. The public nature of the environment introduces the need for authentication mechanisms that are resilient against intrusion, and theft of user credentials [11, 14, 24]. For example, an attacker could shoulder-surf a user during authentication to observe the password [14], exploit smudge traces caused by oily residue on the screen [4, 25] or use a thermal camera to uncover heat traces [1, 23].

While a lot of work focused on identifying threats [1, 4, 11, 14] and proposed a myriad of authentication schemes disguising users' input on personal devices [3, 9, 16, 17, 28] and situated displays [10, 12, 16], a comprehensive analysis of the requirements for secure and usable authentication on public displays is still missing as of today.

The contribution of this work is three-fold: We (i) conducted an extensive literature review and discussed potential challenges with domain experts, (ii) identified a set of design considerations targeting domain specific challenges that can support researchers and professionals during the design and development of secure authentication schemes, and (iii) briefly discuss and outlook on how to apply these considerations for future work.

Requirement Analysis & Design Considerations

We carried out an analysis of related literature, aiming to understand the challenges for secure and usable authentication on situated displays (i.e., public internet terminals, check-in counters, ticket vending machines, and cash machines) in public and semi-public spaces. From these, we formulated design considerations to help professionals and researchers in developing authentication schemes for situated displays.

Approach

This work draws on a comprehensive literature review across various research domains. We reviewed a total of 118 peer-reviewed scientific papers within the research field of pervasive displays, multimodal interaction techniques and usable security and subsequently discussed results with five experts in the field of pervasive displays, human-computer-interaction and usable security.

The existing literature revealed an importance of the following aspects: Exposure of hardware (physical access), exposure of users' input (i.e., visual accessibility), associated threats (e.g, skimming), the target group, the user behaviour, and the users' expectations.

By clustering these aspects, we derived design considerations along the following three dimensions: *Security & Privacy*, *Usability* and *Accessibility*.

Security & Privacy

As a result of the screen's exposed location [7], interactions on the display should be designed from ground up to be secure. Abstracting the "secure by design pattern" introduced by Dougherty et al. [13] for software engineering, malicious behaviour (e.g., shoulder surfing or video attacks) of vicious third-parties is taken for granted, thus the input scheme should ***(1) disguise user input "by design"*** and

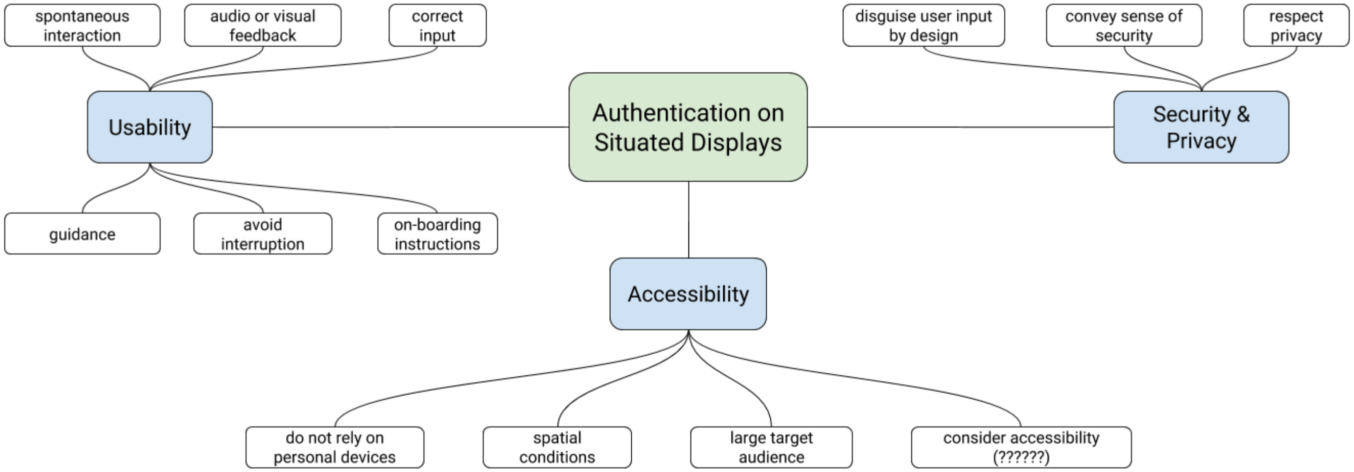

Figure 2: We propose a set of design considerations for secure & usable authentication on situated displays, evolving around the dimensions usability, security & privacy and accessibility.

not rely on the user to protect their input. Schemes that employ cues that users respond to during the authentication [5, 17, 28], hence overwhelming attackers as they are required to observe both, the cue on the screen as well as a user's response, appear to be very promising. Following recommendations by Davies et al., the system should further ***(2) respect the peoples' need for privacy*** [8], thus not expose their privacy directly (e.g., by leaking information in the public) or indirectly (e.g., through tracking for advertising purposes). When choosing an input modality, it should be considered that an input technique not only needs to be easy to use and secure but able to ***(3) convey a sense of security***.

Usability

The usage scenarios on public displays are characterised by short interactions with frequently changing users [6, 22, 27] of a broad target group (self service baggage drop off, payments on a kiosk terminal, withdrawing money form a cash machine). Therefore, the authentication scheme and input modalities should be ***(4) suitable for spontaneous interaction*** and in particular not require users to perform a calibration of sensor hardware [26] (e.g., motion sensors or eye-trackers) prior to their authentication attempt.

Furthermore, users may also need guidance when approaching a display. On-boarding [29] (e.g., explaining input gestures or modalities) and the guidance of users to the correct interaction spot [2] are crucial for the users' experience. Thus, appropriate means to ***(5) provide on-boarding instructions*** (e.g., StrikeAPose presented by Walter et al. [29]) and to ***(6) guide users to the interaction sweet-spot*** (e.g., GravitySpot presented by Alt et al. [2]) should be considered.

Prior studies indicated that obscuring the input does not only have an effect on the observer, but also on the legitimate users that were trying to authenticate. Thus, an authentication method should employ suitable ***(7) audio or visual feedback***. Previous work, which has shown that users can easily get frustrated during interaction on public displays, but are willing to correct errors if sufficient modalities are provided. Thus, authentication schemes should ***(8) allow users to correct their input***. [18].

Additionally, an ideal authentication system should ***(9) not interrupt the users' interaction flow*** [19, 20], but provide a seamless interaction experience (e.g., not require to change the mean of interaction, or require the user to switch devices).

Accessibility

Since public displays (e.g, cash machines) are subject to be used from a diverse target group, the system should employ means for interaction ***(10) suitable for a large target audience*** (e.g., different age groups) and ***(11) consider accessibility*** (e.g. adjusting the height of screens or enable multiple input techniques) [**?**].

Likewise, the spatial situation around public displays is as diverse as the user-base, thus input modalities should be ***(12) adapted to spatial conditions*** (e.g., areas limited interaction space may not be suitable for mid-air gestures). Furthermore, authentication mechanisms on public displays ***(13) should not rely on users' personal devices or sensors***, since users may not own or always carry their mobile [15] or devices suffer from low battery or functional defects.

Discussion

We do not claim that the design considerations presented are comprehensive, nor do all need to be applied. Especially since in some cases its application may introduces trade-offs between usability and security. Depending on the employed technologies and the use-case, some aspects might be less important, or do not apply. Thus, all aspects need to be assessed on a case-by-case basis. For example, a terminal in a shopping mall where users can access discounts or personalised navigation may employ a scheme that focuses on usability (in particular allowing for easy and spontaneous interaction **(4)**), but may be less secure since it does not exploit highly sensible data **(2)**). A system that relies on touch input may not need means to introduce the modality or guide a user to an interaction spot **(6)**. However, we believe that our set of design considerations set provides a solid foundation for researchers as well as practitioners to facilitate an informed decision-making process.

While the proposed design considerations mainly address the development of future systems, the presented considerations can further be used for critical evaluations of *existing concepts*. For example, in traditional PIN based authentication schemes (e.g., on cash machines), a user's input is masked on the screen by replacing letters with asterisks. However, the input modality does not disguise the actual input **(1)**, but relies on the user (e.g., to shield the PIN pad with his hand).

Likewise, the considerations can motivate the *adoption of existing schemes* (e.g., authentication schemes which were developed in another context). The cue-based authentication scheme SwiPIN, presented by von Zezschwitz et al. [28], as an example, disguises input **(1)** by employing cues that users respond to during the authentication. It proved to overwhelm attackers by requiring them to observe both, the cue shown on the screen as well as users' response to the cue. While it was designed for the use on mobile phones, its underling design might be suitable to be adopted for use on situated displays in public spaces.

Conclusion

This work presented 13 design considerations that aim to guide practitioners and researchers when designing and evaluating interaction models for authentication on situated displays. The design guidelines derived from a literature review and subsequent discussion with expert in the domain. For future work, we aim to apply the design considerations described in this work in an exemplary application to compare input modalities for secure authentication on situated displays.

Acknowledgements

This research was partially funded by the UK EPSRC under grant number EP/N023234/1 (PETRAS IoT Research Hub - Cybersecurity of the Internet of Things) and by the Bavarian State Ministry of Education, Science and the Arts in the framework of the Centre Digitisation.Bavaria (ZD.B). This research was supported by the Deutsche Forschungsgemeinschaft (DFG), Grant No. AL 1899/2-1.

REFERENCES

1. Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA. DOI: http://dx.doi.org/10.1145/3025453.3025461

2. Florian Alt, Andreas Bulling, Gino Gravanis, and Daniel Buschek. 2015. GravitySpot: Guiding Users in Front of Public Displays Using On-Screen Visual Cues. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software &#38; Technology (UIST '15)*. ACM, New York, NY, USA, 47–56. DOI: http://dx.doi.org/10.1145/2807442.2807490

3. Florian Alt, Mateusz Mikusz, Stefan Schneegass, and Andreas Bulling. 2016. Memorability of Cued-recall Graphical Passwords with Saliency Masks. In *Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia (MUM '16)*. ACM, New York, NY, USA, 191–200. DOI: http://dx.doi.org/10.1145/3012709.3012730

4. Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10)*. USENIX Association, Berkeley, CA, USA, 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009

5. Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2012. Counting Clicks and Beeps: Exploring Numerosity Based Haptic and Audio PIN Entry. *Interact. Comput.* 24, 5 (Sept. 2012), 409–422. DOI: http://dx.doi.org/10.1016/j.intcom.2012.06.005

6. Harry Brignull and Yvonne Rogers. Enticing people to interact with large public displays in public spaces. In *Proc. INTERACT '03*. 17–24.

7. Nigel Davies, Sarah Clinch, and Florian Alt. 2014a. *Pervasive Displays - Understanding the Future of Digital Signage*. Morgan and Claypool Publishers.

8. Nigel Davies, Marc Langheinrich, Sarah Clinch, Ivan Elhart, Adrian Friday, Thomas Kubitza, and Bholanathsingh Surajbali. 2014b. Personalisation and Privacy in Future Pervasive Display Networks. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2357–2366. DOI: http://dx.doi.org/10.1145/2556288.2557287

9. Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into My Eyes!: Can You Guess My Password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 7, 12 pages. DOI: http://dx.doi.org/10.1145/1572532.1572542

10. Alexander De Luca and Bernhard Frauendienst. 2008. A Privacy-respectful Input Method for Public Terminals. In *Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges (NordiCHI '08)*. ACM, New York, NY, USA, 455–458. DOI:http://dx.doi.org/10.1145/1463160.1463218

11. Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. 2010. Towards Understanding ATM Security: A Field Study of Real World ATM Use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, New York, NY, USA, Article 16, 10 pages. DOI: http://dx.doi.org/10.1145/1837110.1837131

12. Alexander De Luca, Emanuel von Zezschwitz, and Heinrich Hussmann. 2009. Vibrapass: Secure Authentication Based on Shared Lies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 913–916. DOI: http://dx.doi.org/10.1145/1518701.1518840

13. Chad Dougherty, Kirk Sayre, Robert Seacord, David Svoboda, and Kazuya Togashi. 2009. *Secure Design Patterns*. Technical Report CMU/SEI-2009-TR-010. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9115

14. Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA. DOI: http://dx.doi.org/10.1145/3025453.3025636

15. R. Grignani. 2005. Where's the phone? A study of mobile phone location in public spaces. *IET Conference Proceedings* (January 2005), 142–142(1). http://digital-library.theiet.org/content/conferences/10.1049/cp_20051557

16. Mohamed Khamis, Regina Hasholzner, Andreas Bulling, and Florian Alt. 2017a. GTmoPass: Two-factor Authentication on Public Displays Using GazeTouch passwords and Personal Mobile Devices. In *Proceedings of the 6th International Symposium on Pervasive Displays (PerDis '17)*. ACM, New York, NY, USA, 9. DOI: http://dx.doi.org/10.1145/3078810.3078815

17. Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017b. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction (ICMI 2017)*. ACM, New York, NY, USA, 5. DOI: http://dx.doi.org/10.1145/3136755.3136809

18. Mohamed Khamis, Ludwig Trotter, Markus Tessmann, Christina Dannhart, Andreas Bulling, and Florian Alt. 2016. EyeVote in the Wild: Do Users Bother Correcting System Errors on Public Displays?. In *Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia (MUM '16)*. ACM, New York, NY, USA, 57–62. DOI: http://dx.doi.org/10.1145/3012709.3012743

19. Ville Mäkelä, Jobin James, Tuuli Keskinen, Jaakko Hakulinen, and Markku Turunen. 2017. “It's Natural to Grab and Pull”: Retrieving Content from Large Displays Using Mid-Air Gestures. *IEEE Pervasive Computing* 16, 3 (2017), 70–77. DOI: http://dx.doi.org/10.1109/MPRV.2017.2940966

20. Ville Mäkelä, Mohamed Khamis, Lukas Mecke, Jobin James, Markku Turunen, and Florian Alt. 2018. Pocket Transfers: Interaction Techniques for Transferring Content from Situated Displays to Mobile Devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 135, 13 pages. DOI: http://dx.doi.org/10.1145/3173574.3173709

21. James Manyika, Michael Chui, Mehdi Miremadi, Jacques Bughin, Katy George, Paul Willmott, and Martin Dewhurst. 2017. *A Future That Works: Automation, Employment, and Productivity*. Executive summary. McKinsey&Company.

22. Daniel Michelis and Jörg Müller. 2011. The Audience Funnel: Observations of Gesture Based Interaction With Multiple Large Displays in a City Center. *International Journal of Human–Computer Interaction* 27, 6 (2011), 562–579. DOI: http://dx.doi.org/10.1080/10447318.2011.555299

23. Keaton Mowery, Sarah Meiklejohn, and Stefan Savage. 2011. Heat of the Moment: Characterizing the Efficacy of Thermal Camera-based Attacks. In *Proceedings of the 5th USENIX Conference on Offensive Technologies (WOOT'11)*. USENIX Association, Berkeley, CA, USA, 6–6. http://dl.acm.org/citation.cfm?id=2028052.2028058

24. Volker Roth, Kai Richter, and Rene Freidinger. 2004. A PIN-entry Method Resilient Against Shoulder Surfing. In *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*. ACM, New York, NY, USA, 236–245. DOI: http://dx.doi.org/10.1145/1030083.1030116

25. Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2014. SmudgeSafe: Geometric Image Transformations for Smudge-resistant User Authentication. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, USA, 775–786. DOI: http://dx.doi.org/10.1145/2632048.2636090

26. Mélodie Vidal, Andreas Bulling, and Hans Gellersen. 2013. Pursuits: Spontaneous Interaction with Displays Based on Smooth Pursuit Eye Movement and Moving Targets. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '13)*. ACM, New York, NY, USA, 439–448. DOI: http://dx.doi.org/10.1145/2493432.2493477

27. Daniel Vogel and Ravin Balakrishnan. 2004. Interactive Public Ambient Displays: Transitioning from Implicit to Explicit, Public to Personal, Interaction with Multiple Users. In *Proceedings of the 17th Annual ACM Symposium on User Interface Software and Technology (UIST '04)*. ACM, New York, NY, USA, 137–146. DOI: http://dx.doi.org/10.1145/1029632.1029656

28. Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1403–1406. DOI: http://dx.doi.org/10.1145/2702123.2702212

29. Robert Walter, Gilles Bailly, and Jörg Müller. 2013. StrikeAPose: Revealing Mid-air Gestures on Public Displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 841–850. DOI: http://dx.doi.org/10.1145/2470654.2470774