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

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 considerations 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 fields of pervasive displays, human-computer-interaction and usable security.

Author Keywords
Authentication; Public Displays; Input Modalities; Design Considerations; User Interface Design.

CCS Concepts
• Human-centered computing → Ubiquitous and mobile computing theory, concepts and paradigms; • Security and privacy → Domain-specific security and privacy architectures;
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 [22]. 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 [8]. The public nature of the environment introduces the need for authentication mechanisms that are resilient against intrusion, and theft of user credentials [12, 15, 25]. For example, an attacker could shoulder-surf a user during authentication to observe the password [15], exploit smudge traces caused by oily residue on the screen [5, 26] or use a thermal camera to uncover heat traces [1, 24].

While a lot of work focused on identifying threats [1, 5, 12, 15] and proposed a myriad of authentication schemes disguising users’ input on personal devices [3, 10, 17, 18, 29] and situated displays [11, 13, 17], 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 [8], interactions on the display should be designed from ground up to be secure. Abstracting the “secure by design pattern” introduced by Dougherty et al. [14] 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
not rely on the user to protect their input. Schemes that employ cues that users respond to during the authentication [6, 18, 29], 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 people’s need for privacy [9], 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 [7, 23, 28] of a broad target group (self service baggage drop off, payments on a kiosk terminal, withdrawing money from 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 [27] (e.g., motion sensors or eye-trackers) prior to their authentication attempt.

Furthermore, users may also need guidance when approaching a display. On-boarding \([30]\) (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. \([30]\)) 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 [19].

Additionally, an ideal authentication system should (9) not interrupt the users' interaction flow [20, 21], 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) [4].

Likewise, the spatial situation around public displays is as diverse as the user-base, thus input modalities should be adapted to spatial conditions (e.g., areas limited in interaction space may not be suitable for mid-air gestures). Furthermore, authentication mechanisms on public displays (12) should not rely on users’ personal devices or sensors, since users may not own or always carry their mobile [16] 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 their application may introduce 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 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. [29], 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 ob-
serve 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 underlying 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 experts 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


