Understanding Shoulder Surfing in the Wild: Stories from Users and Observers

Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, Florian Alt
Media Informatics Group, LMU Munich, Germany
{malin.eiband, mohamed.khamis, emanuel.von.zezschwitz, hussmann, florian.alt}@ifi.lmu.de

ABSTRACT
Research has brought forth a variety of authentication systems to mitigate observation attacks. However, there is little work about shoulder surfing situations in the real world. We present the results of a user survey (N=174) in which we investigate actual stories about shoulder surfing on mobile devices from both users and observers. Our analysis indicates that shoulder surfing mainly occurs in an opportunistic, non-malicious way. It usually does not have serious consequences, but evokes negative feelings for both parties, resulting in a variety of coping strategies. Observed data was personal in most cases and ranged from information about interests and hobbies to login data and intimate details about third persons and relationships. Thus, our work contributes evidence for shoulder surfing in the real world and informs implications for the design of privacy protection mechanisms.

Author Keywords
Shoulder Surfing; Privacy; Mobile Devices

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: User Interfaces—*Input devices and strategies*; K.6.5 Computing Milieux: Security and Protection—*Authentication*

INTRODUCTION
At the time of submission of this paper, at least 4640 academic publications indexed on Google scholar are concerned with research on shoulder surfing[1]. The vast majority of these articles (about 4000) have been published since 2007, the year the iPhone entered the market. Not only since then, shoulder surfing – that is the act of observing other people's information without their consent (see Figure 1) – has served as a fundamental motivation behind much of the work that has been conducted in the area of usable privacy and security. In particular, there is a plethora of work on authentication systems that aim to mitigate shoulder surfing on mobile devices (e.g., [3, 8, 11, 18, 39, 45]).

CHI 2017, May 06 - 11, 2017, Denver, CO, USA

ACM 978-1-4503-4655-9/17/05$15.00
DOI: http://dx.doi.org/10.1145/3025453.3025636

Figure 1. A shoulder surfing situation in a cafe.

At the same time, surprisingly little is known about the phenomenon of shoulder surfing itself. To date, there are no detailed investigations of shoulder surfing incidents and their real-world implications. In fact, findings from Harbach et al. [20] in 2014 showed that only in eleven out of 3410 situations (0.3 %), smartphone users perceived a shoulder surfing risk. Hence, one might wonder, *how much of a threat is shoulder surfing for the user?*

To answer this question, this work contributes the results of an exploratory survey (N=174) that collects actual stories from both perspectives: *users* (the person being shoulder surfed) and *observers* (the shoulder surfer). Stories are not restricted to authentication, but focus on visual privacy in general.

The analysis of the stories revealed that shoulder surfing was mostly casual and opportunistic. There were no stories indicating observation out of malicious intent and/or with technical equipment. Shoulder surfing was most common among strangers, in public transport, during commuting times, and involved a smartphone in almost all cases. Observations uncovered a broad range of mostly personal content, such as information about a user's interests, hobbies, relationships, sexual preferences, third persons, and login data. Except for two cases, users did not report serious consequences of shoulder surfing. However, both users and observers expressed negative feelings in the respective situation, such as embarrassment and anger or guilt and unease. Users reacted with vari-

[1] https://scholar.google.de/scholar?q=%22shoulder+surfing%22, *accessed 2016/09/20.*

ous coping strategies, like turning the device away, shielding content with their body, or adapting their way of interaction. However, shoulder surfing often went unnoticed: Users were aware of it in only 7 % of the incidents reported by observers.

The contribution of this work is threefold: First, we provide evidence for shoulder surfing in the wild by collecting experiences from users and observers. Second, we identify and discuss seven main findings that help the community to better understand the nature and implications of shoulder surfing. Third, we derive implications of these results on the design of future privacy protection mechanisms.

RELATED WORK

The observability of knowledge-based authentication mechanisms has been discussed for over a decade [35, 49]. As established authentication methods like Android unlock patterns [46] and text-based input [37] are very easy to observe, most prior work focused on investigating and proposing alternative authentication concepts which conceal the entered secret and make the authentication process observation-resistant. A literature review indicates that improved observation-resistance is usually achieved by visual overload (e.g., [18, 45, 40]), indirect input (e.g., [12, 49]), multiplexed input (e.g., [35, 44]) or by establishing a second, non-observable, communication channel (e.g., [4, 11, 26, 36, 51]). That is, the presentation style or interaction concept are usually modified in a way that makes the input harder to observe. The performance of these concepts is mostly evaluated in the lab where authentication is performed by participants and observation attacks are simulated by the experimenter [50]. Hence, the real-world vulnerability of authentication methods and the real-world risks of shoulder surfing have not yet been evaluated systematically.

However, shoulder surfing is not limited to the observation of password input. The Ponemon Institute [23] investigated the feasibility of shoulder surfing attacks in business office environments and found that "sensitive information can be displayed on laptops, tablets and smartphones, as well as in paper documents that are left in plain sight on desks, printers and conference tables and at other office locations or outside meeting sites". The authors report that 91 % of all attacks were successful. While 12 % of the observed information was indeed based on login credentials (e.g., passwords), personal information about consumers and employees (28 %), contact lists (17 %) and financial information (8 %) was also frequently observed. Overall, 28 % of the attacks were performed on unprotected computer screens. In another study [21], 85 % of the participants acknowledged that they had already observed sensitive information on computer screens they were not authorised to see. In addition to direct observation, threats to visual privacy have recently been discussed in the context of surveillance cameras [38], corneal reflections [53], drones [48] and life logging cameras [22].

In contrast to the manifold work which was published to protect the authentication process, general visual privacy concepts have not been in focus of research and related work is quite sparse. Besides the use of physical privacy foils which limit the angle of view [34], adaptive sensor-based approaches (e.g., [2, 7, 28, 54]) and static software-based approaches (e.g., [14, 41, 47]) have been discussed. Sensor-based approaches are usually checking the user's surrounding and indicate bystanders. If potential observers are detected, the user is either informed (e.g., [2, 7]) or the user interface is adapted (e.g., [7, 28, 54]). Such adaptions imply reducing the screen's lightness or selectively hiding information [41]. In addition, individual user characteristics can be exploited to improve visual privacy for specific content. Eiband et al. [14] proposed to utilise the user's handwriting to protect private text-messages on mobile devices. Von Zezschwitz et al. [47] suggested to use graphical distortion filters to protect personal images stored in photo galleries of smart phones. Distortion filters were applied so as to make the images' content easy to recognise for the user but hard to understand for observers.

Despite the effort of improving visual privacy and observation-resistance of authentication mechanisms, the real-world threat of shoulder surfing in everyday life is still largely unknown. Harbach et al. [20] performed an experience sampling field study to evaluate the risk perception of smartphone users in the wild. They reported that shoulder surfing was rarely perceived as a relevant risk. However, the authors acknowledged that critical environments (e.g., public transport) might have been under-sampled. Trewin et al. [43], who investigated the risk perception of users accessing different kinds of specific data (e.g., company data, banking information) on mobile devices, found that shoulder surfing risks were frequently perceived. In line with this finding, Little and Briggs [29] revealed that most users show stress reactions when viewing sensitive data in public environments. Indeed, mobile devices are often used in public context and provide a wide range of applications [5, 6] which may be exposed to the danger of unauthorised observation.

We argue that it is crucial to understand the nature of everyday shoulder surfing scenarios to inform the design of solutions and to understand if shoulder surfing is restricted to certain data types (e.g., authentication) or if it is a general problem.

ONLINE SURVEY

We collected a large number of diverse experiences from both users and observers to investigate shoulder surfing in the wild. For this exploratory approach, we used an online survey[2].

Design and Method

Shoulder surfing is a potentially sensitive topic, since content is observed without the other person's knowledge or consent. Prior work has shown that asking sensitive questions in self-report should be done in an indirect and anonymity-preserving way in order to minimise social desirability bias [30, 31]. We also wanted to avoid a particular context or use case to minimise recall bias as much as possible and to capture diverse experiences.

We therefore decided to collect *stories* about shoulder surfing based on the *critical incident technique* [16], which allows for "generating a comprehensive and detailed description of a content domain" [52]. The questionnaire was designed in

[2] http://www.medien.ifi.lmu.de/team/malin.eiband/shouldersurfing-questionnaire.pdf

an iterative process and tested repeatedly in prestudies with small participant samples. The critical incident was presented as a sketch of an intentionally generic shoulder surfing situation among two stick-figures that we called "Cas" (the user) and "Vic" (the observer), shown in Figure 2, alongside a short description. We did not mention the term "shoulder surfing" itself throughout the survey. We also avoided words and expressions with a negative connotation like "peeking" or "victim" to not give participants the impression that their behaviour is judged and thus possibly discourage them from telling the truth. Instead, we used neutral terms like "looking" and "user". The stick-figures should allow to tell a story anonymously, if a participant wanted to. We chose unisex names instead of commonly used placeholders like "Alice" and "Bob" because the results of the pretests suggested that gender might influence recall. The pretests also indicated that examples could sometimes not be completely avoided in order to illustrate questions or statements. In these cases, we tried to minimise bias by giving a very broad range of examples and included validity checks to identify participants who copied text from the questions.

Questionnaire Structure

The questionnaire consisted of 1) a free text entry for participants' stories, 2) a section asking for specific details about the story told in the first part, and 3) demographic questions.

In the first part, the shoulder surfing sketch and the description were displayed. Participants had to state whether they knew of a situation like the one depicted. If their answer was "Yes", they were asked to report any real life experiences with such an incident as detailed as possible via free text entry.

In the second part, we enquired about specific details, such as the context of the situation, the type of content displayed on the screen, the gender of both user and observer, etc. We also asked participants to state the feelings and reactions of user and observer and to optionally reveal their role (e.g., user or observer). This allowed us to indirectly derive further insights about the situation. We used multiple choice where appropriate, but most of the questions allowed for free text entry.

In the last part, participants filled in demographic data and had to indicate their honesty on a 5-point Likert scale. This question was included as previous work suggested that self-report of honesty helps identifying invalid data [46].

Participants

The survey was distributed in Egypt, Germany and the US. It was framed as "Privacy on mobile devices" without mentioning the term "shoulder surfing" so as to minimise self-selection bias in the sample. Participants were mainly recruited via mailing lists and social media. More than two thirds of the participants (70 %) were female. 75 % were German, 16 % Egyptian, the rest came from a variety of countries including the US, Bulgaria, India, Italy, Romania, Russia and South Korea. Participants' age ranged from 16–57 years, with a mean of 25 years (*SD*=6 years). About two thirds of the sample (67 %) were students. All data was stored anonymously. Participants were compensated with vouchers or credit points for their studies.

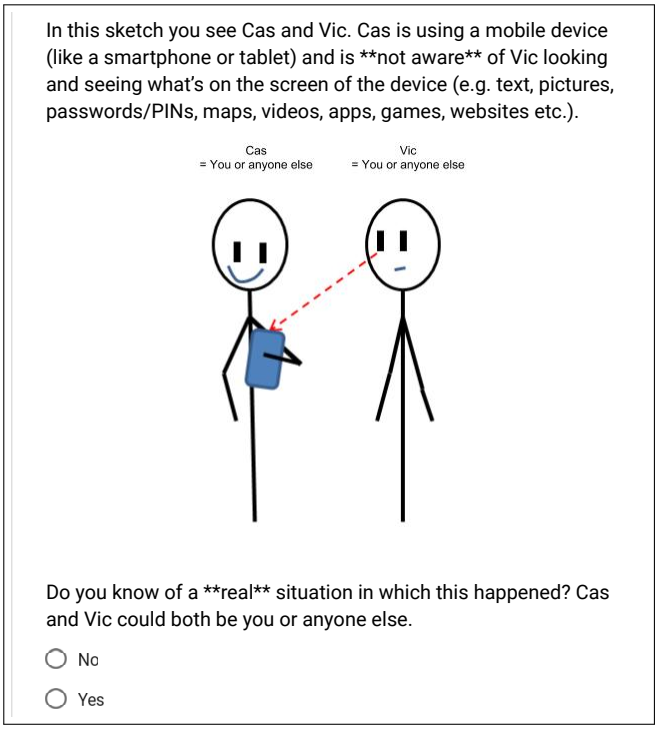

Figure 2. Screenshot of the first part of the online questionnaire.

Limitations

Self-report is a common tool to gather a general understanding of user perceptions in diverse research areas and established practice also in many security and privacy studies [1, 25]. However, we are aware that self-reported data is susceptible to inaccurate statements, influence by wording or recall bias [33]. For example, we cannot be sure whether an incident in our survey was reported because it happened recently or because participants felt it was serious. Moreover, when asking people to self-report potentially sensitive experiences, social desirability can be a source of error [42]. Also, since the study was posted online, our participant sample might have been biased by self-selection.

Although we cannot completely rule out any of these limitations, we countered them in various ways: We followed an indirect questioning approach allowing for anonymity. The questions were designed in a careful, iterative way using multiple pretests. To identify invalid responses, we included validity checks such as a question asking for the honesty of the participants, and manually inspected all collected data before analysis as explained in detail in the next section. The framing of the study also invited participants without shoulder surfing experiences. The subset of those with shoulder surfing experiences was identified post-hoc. Finally, research about shoulder surfing in the wild is not concluded with a single study and that our results may not generalise, given our rather homogeneous sample. Still, we are confident that our exploration gives directions for future work on specific issues.

INDUCTIVE CODING AND INTERRATER AGREEMENT

A total of 176 participants completed our online survey. Each statement was manually inspected before the coding process. P102 and P157 both indicated 1=*strongly disagree* when

Code	Count
Role:	**174**
– I was the observer	84
– I was the user	58
– I was neither	22
– I prefer not so say	4
– I don't know of any incident	6
Relationship:	**170**
– strangers	126
– friends	11
– acquaintances	10
– colleagues	8
– family	3
– couple	3
– other	9
Gender:	**151**
– male observed female	44
– male observed male	38
– female observed female	37
– female observed male	32

Table 1. Role of participants, the relationship between user and observer, and gender. Most stories were reported by observers, users and observers were mostly strangers, and there was no correlation between gender and role.

asked whether they were completely honest when answering the questions. Their answers were therefore removed from the data. We also checked whether participants copy-pasted from the questions and whether their answers to the second part of the questionnaire were coherent with the story told in the first part. From the remaining 174 response sets, we derived a codebook with 15 main categories from the collected answers to the open-ended questions. Each category was further refined by up to 21 subcategories, yielding 160 categories in total. A randomly chosen subset of 10 % of the answers was then coded independently by two raters. Agreement among raters was calculated using Cohen's κ [10] and Byrt et al.'s prevalence-adjusted bias-adjusted κ (PABAK) [9], which are appropriate indices given two raters and nominal data [13]. Statements could belong to more than one category. For instance, the statement

> *"In public places and on public transport many people are not aware that what they're doing on their phone is quite visible to people [...] nearby [...]"* (P174)

was coded as *Location: public open spaces* and *Location: public transport*. For this reason, comparisons were reduced into 2×2 contingency tables based on whether a code was present or absent in the report of each rater. Both κ and PABAK were then calculated for each of the 160 categories. For κ, interrater agreement was "substantial" to "(almost) perfect" [27] for 70 % of the subcategories. κ ranged from 0.00 (e.g., *Location: narrow, crowded places*) to 1.00 (e.g., *Time of day: evening*). The range of values was smaller for PABAK, where agreement ranged from 0.62 (*Motivation Observer: I don't know*) to 1.00 (e.g., *Device: smartphone*). For PABAK, "substantial" to "(almost) perfect" agreement was reached for 98 % of the categories. We assume that the

Code	Count
Location:	**193**
– public transport	130
– theatre hall / lecture hall	13
– at work / university	10
– cafe, restaurant, bar	9
– narrow / crowded places	8
– public open spaces	7
– other	16
Activity:	**189**
– on the way	72
– commuting	69
– working / studying	16
– other	32
Time of day:	**158**
– morning	57
– evening	40
– afternoon	34
– midday	13
– all day	14
Device:	**175**
– smartphone	157
– tablet	8
– laptop	7
– ebook reader	3

Table 2. Context of shoulder surfing in everyday life. Shoulder surfing mostly happened in public transport, during commuting time, and involved a smartphone.

broad κ range was caused by effects of prevalence in the respective categories, a known problem with κ [15]. Therefore, no categories were excluded. All remaining discrepancies were discussed until a consensus was reached. Assuming that the final agreement generalises [19], half of the remaining statements was then coded by the first, the other half by the second rater.

RESULTS

The following sections present the insights gathered from the analysis of the cleaned data, that is the remaining 174 response sets, based on the coding. The percentages are calculated based on the total number of collected code instances in the respective category. Participants' quotes are translated to English where necessary.

Users and Observers

Table 1 shows the code instances related to the participants' role and the relationship between user and observer. Six participants (3.4 %) stated in the first part of the questionnaire that they did not know of a shoulder surfing incident. 32 stories (18.4 %) were reported by participants who preferred to remain anonymous or stated having been neither user nor observer, but had, for example, witnessed the incident as a bystander. In 142 out of 174 cases, we could identify the participants role (user or observer): 58 of the collected stories (33.3 %) were told from the user perspective, 84 (48.3 %) from the observer perspective. Only six out of these 84 observers (7.1 %) were noticed by the person they observed.

In most cases (74.1 %), user and observer were strangers, in about a quarter (25.9 %) observer and user were acquainted. These cases included shoulder surfing among friends (6.5 %), colleagues (4.7 %), family members (P4, P163, P170; 1.7 %) and couples (P19, P93, P94; 1.7 %), or incidents in which the observer was the participants' boss (P143, P153; 1.2 %). There was no correlation between gender and role.

Context

The code instances regarding contextual information are shown in Table 2. Shoulder surfing mostly happened in public transport: More than two thirds (67.4 %) of our participants referred to a situation that occurred while travelling on the subway, bus, train, etc., which is linked to the finding that user and observer were mostly strangers. For example, P1 said that she had *"often tried to look at the phones of strangers in the train"*. P76 generalised this statement:

> *"Such a thing happens in public transport in particular. People are deliberately or unconsciously observed by others while having, e.g., their smartphone in their hand. This goes from quick glances to real staring."*

P161 had a similar impression:

> *"In the subway [...] Everyone next to you or behind you can look [at] your phone, you can look at [everyone's] phone there from the correct position."*

Most commonly, user and observer were sitting side by side (33.9 %). In 36.5 % of the cases user and observer had been commuting. For instance, P8 said that she *"[commutes] frequently by train, where you often see people looking at the phones of strangers and reading along."* This is supported by the fact that shoulder surfing happened mostly during the times of the day when people typically commute: in the morning (36.1 %), afternoon (21.5 %) and evening (25.3 %).

Shoulder-surfed devices were mainly smartphones (89.7 %). Only few participants reported incidents involving a tablet (4.6 %), laptop (4.0 %) or ebook reader (1.7 %). 21.8 % of the participants mentioned that shoulder surfing occurs regularly.

Content

Table 3 shows the code instances related to the observed data. The content observers saw on a display was mostly text (46.6 %), followed by pictures (24.1 %) and games (12.6 %), and was personal in the majority of the incidents (83.6 %). Most commonly observed was communication via instant messaging such as WhatsApp (41.8 %), followed by Facebook (17.5 %), email (7.9 %) and news (7.4 %).

The insights observers gained from other people's devices were broad-ranging: *"Resolution and font size as well as the orientation of the device made it possible to follow everything that was on the device and happening there [...]"* (P50). Observers uncovered details about a user's interests and hobbies, weekend plans, work or studies, online shopping, appointments, and in some cases even about his or her sex life and sexual preferences. In most cases, shoulder surfing revealed information about a user's relationships (34.3 %), including data about third persons. For example, P6 was able to see someone's apartment in a video chat.

Code	Count
Content (general):	**253**
– text	118
– pictures	61
– games	32
– credentials	15
– videos	8
– other	19
Content (concrete):	**189**
– instant messaging	79
– Facebook	33
– email	15
– news	14
– PIN	9
– password	4
– online shopping	4
– unlock pattern	3
– other	28
Uncovered Information:	**171**
– personal:	**143**
– relationships / third persons	49
– interests / hobbies	23
– plans	17
– credentials	12
– work / studies	8
– sex life	5
– general	18
– other	11
– non-personal:	**23**
– games	15
– other	8
– other	5

Table 3. Type of content and information observed. Content was mostly text in the form of instant messages, and personal. There was a broad range of information uncovered by shoulder surfing.

In 5.9 % of the incidents, participants reported shoulder surfing of authentication data (PINs, unlock patterns, passwords and user names). For instance, take P173's statement:

> *"One time I was on the train when I was opening my phone using the pattern [...] which is provided as security feature in [Android], when I noticed this guy trying to figure out my pattern. When I asked him [did] you see what I drew, he said 'I think I know your pattern' ".*

Moreover, the stories suggest that non-personal information revealed details about the user. From the source the user read news from, P11 and P23 uncovered information about political views and interest in particular countries and topics. P14 reported learning "*what kind of books*" a neighbouring flight passenger reads.

Motivation for Shoulder Surfing

The code instances regarding the observers' motivation can be found in Table 4. Our analysis indicates that observers rarely shoulder surfed out of reasons other than curiosity and boredom (33.6 % each). P82, for instance, said that *"[it hap-*

Code	Count
Motivation Observer:	**134**
– curiosity	45
– boredom	45
– inadvertently	12
– device was in line of sight	8
– reaction to stimulus	6
– habit	4
– other	14

Table 4. Reasons for shoulder surfing. Observers acted out of curiosity and boredom in most cases.

pened out of] boredom, because I cannot read a book while standing". Similarly, P19 stated that she was *"[bored], [since my] own smartphone was out of battery"*. P1 admitted that she shoulder surfed *"to compare [my] own life with the life of others because [I] don't have many friends and [do] not know what other people do"*. Only few observers shoulder surfed deliberately and regularly, for example:

> *"I always look at displays when you get the opportunity, you get to know many things."* (P10)

> *"[...] I like to read [other people's WhatsApp chats]. Romantic drama, shopping lists, film recommendations ... wherever you look!"* (P43)

In other cases, shoulder surfing occurred inadvertently (e.g., P34, P40, P71) or as response to a stimulus such as light or sound coming from the device (e.g., P20, P68).

There were no cases in which our analysis indicated shoulder surfing with technical equipment or out of malicious intent, such as getting a particular piece of information from the user as leverage for the future.

Feelings

Participants were asked to state both the user's and the observer's feelings in the shoulder surfing situation. User feelings were reported 41 times, observer feelings 90 times. The code instances are shown in Table 5.

User Feelings

Our analysis indicates that feelings of users who noticed being observed were negative in the majority of cases (90.2 %), among them anger, unease, pressure, and embarrassment. For example, P116 described the following incident:

> *"I just had googled sex toys. Then I went to my parents' bowling night. I then wanted to google something quickly and my phone froze after the first letter and at exactly that moment, the person sitting next to me at the table looked at my display. There was written 'inflatable dildo'. One of the most embarrassing moments in my life [...] I wished the ground would open and swallow me up."*

Other participants stated that users felt *"violated in [their] privacy"* (P11), *"harassed"* (P15), *"that someone is not minding [their] own business"* (P148), *"very bad and uncomfortable"* (P159), or *"vulnerable"* (P173).

Code	Count
User's Feelings:	**41**
– positive feelings:	**1**
– amused	1
– negative feelings:	**37**
– observed / spied on	13
– uneasy / embarrassed	12
– harassed / pressed	6
– angry / outraged	6
– other	3
Observer's Feelings:	**90**
– positive feelings:	**13**
– amused	8
– superior	4
– proud	1
– negative feelings:	**24**
– uneasy	10
– guilty /ashamed	10
– annoyed	4
– curious / interested	26
– neutral	13
– bored	7
– other	7

Table 5. Feelings of users and observers. Shoulder surfing evoked negative feelings for both parties.

Moreover, participants expressed negative feelings through criticism of the observer's behaviour, for example, P156: *"[He felt] Hopefully like an idiot"*, and P173: *"[He was] proud of himself that nosey bastard!"* P166 summarised her thoughts as follows:

> *"People [...] [looking] at your phone and [...] [reading] your conversations or [focusing] on anything you are doing [...] is totally unacceptable."*

Observer Feelings

Interestingly, in more than a quarter of the cases (26.7 %), participants described the observer's feelings as negative, too. For instance, P176 stated that he *"felt bad. This was [another person's] device."* and P163 remarked:

> *"My sister is on [WhatsApp] and I [had] nothing to do at that moment, so I [looked] at her screen. [...] when I [realised] it [was] so unmoral, I turned my eyes away."*.

In other stories, the observer's feelings were described as *"a bit more ashamed as if [...] reading along another person's newspaper"* (P59), *"a little bit guilty"* (P161), *"not comfortable, like [they] would not accept the privacy"* (P67), or *"very wrong"* (P146). P95 said:

> *"[...] If I catch myself staring at someone's display, I – particularly when it comes to sensitive content – quickly look away"*.

However, 14.4 % of the feelings were positive, like amusement or pride. Also, some observers were unconcerned about shoulder surfing other people's devices in public:

"Since I don't look at my phone a lot in the train [...] I now and then look at the phone of my neighbour. I don't see anything reprehensible about it. If something is top secret, you don't handle it in public." (P45)

Reactions

We asked participants to state both the user's and the observer's reactions during the incident, given that the user noticed the observer. User reactions were reported 64 times, observer reactions 41 times.

User Reactions

The code instances related to the user reactions are shown in Table 6. Although the observer was sometimes just ignored (7.8 %), shoulder surfing provoked a reaction in most cases (92.2 %). Reactions occurred in a variety of ways, either emotionally (20.3 %) or proactively (71.9 %), for example, by protecting content from the observer's view. Coping strategies included turning the display or the whole body away from the observer (43.5 %), switching the device or the screen off, or putting the device away (13 % each). Interestingly, users tended to behave differently depending on their relationship to the observer: If the observer was known to them, users did not react with obvious rejection (e.g., by hiding the display with their hands), but rather subtly by changing their way of interacting with the device (e.g., quicker scrolling).

Moreover, some participants stated being alert when using their mobile device in public, like P68:

"Everytime I take the subway I look at people and, if they play a game, secretly watch what they are playing. For this reason I'm always watchful when I'm doing something on my [smartphone], and look up frequently to see whether someone is looking."

Others do not access sensitive data at all when in public:

"[...] I don't do things that require higher security when I'm on the way (online banking, entering credit card details, etc.)" (P62)

"[In public transport] you often notice that people look at other (or my) smartphones. In these situations, I often use other, 'harmless' apps or even stop using my smartphone." (P11)

P108 and P166 expressed a certain helplessness:

"Afterwards it occurred to me that eventually everyone could have observed [...] what I'm typing and on which page I'm on, but I also wouldn't have known how to keep my input secret." (P108)

"[...] you can't really prevent them [looking] except by not using your phone." (P166)

Emotional reactions included angry looks and verbal complaints about the observer's conduct. However, participants also stated positive experiences where shoulder surfing led to a conversation between user and observer (e.g., about a game the user played), or triggered a humorous response (P93):

[Addressing the observer] *"Shall I send [the message] like that?"* – [Observer] *"Yes, that's fine."*

Code	Count
Reaction User:	**64**
– ignored the observer	5
– proactive reaction:	**46**
– turned display / body away	20
– put device away	6
– turned device off	6
– changed way of interacting	6
– hid display with hands	3
– avoided using sensitive data	2
– other	3
– emotional reaction:	**13**
– angry look	4
– talked to observer (positive)	4
– talked to observer (negative)	3
– humorous / relaxed	2

Table 6. User reactions to shoulder surfing. If they noticed being observed, most users tried to protect their content from the observer and to prevent further shoulder surfing.

Observer Reactions

Observers mostly simply looked away from the device without further reaction (61 %). Some observers did not take notice of the user's reaction and kept on looking (12.2 %). Others engaged in a conversation with the user (14.6%).

Consequences

Shoulder surfing did not have unpleasant or severe consequences except for two cases. Take P104's statement of the following incident, for example:

"I sat in the bus on the way to a friend who lives in a neighbourhood said to be less safe. Apart from me there were only two young men in the bus who sat [...] directly behind me [...] I looked for the address [of my friend on Google Maps] [...] They saw this and then started talking about where I might be going. When getting off the bus, they [...] said that they could show me the way [...] it was getting dark already and [...] I had a bad feeling [about it], since they made a somewhat aggressive impression [...]"

MAIN FINDINGS AND DISCUSSION

In this section, we identify and discuss the main findings from the analysis of the 174 stories collected in the online survey.

Shoulder Surfing is Real – But Goes Unnoticed

The great majority, 168 of our 174 participants (97 %), claimed to know of a shoulder surfing situation in everyday life. Moreover, 21 % of the participants mentioned that shoulder surfing occurs regularly, although we did not explicitly ask them to report this detail. Leaving aside the incidents reported by persons who were not directly involved in the shoulder surfing incident, we collected 58 (33 %) stories from users and 84 (48 %) stories from observers. Only six out of these 84 observers stated being noticed by the user – about 7 %. Since stories by users could *only* be reported *if* the user had noticed the observer, we argue that stories reported by observers are better indicators of how often shoulder surfing gets noticed. Hence, we conclude:

Finding 1: Shoulder surfing exists to a substantial amount in real life. However, users are not aware of being observed in the majority of cases.

Similar observations were made in related work through the simulation of shoulder surfing attacks in offices [23].

Observers are not always Evil

The great majority of observers were strangers motivated by curiosity and boredom (34 % each). Moreover, in many cases (27 %) shoulder surfing went along with negative feelings such as guilt or unease on the side of the observer. The incidents we collected were all simple, one time observations without technical equipment such as video cameras.

Finding 2: Observers are opportunistic and rarely act out of reasons other than curiosity and boredom. Moreover, they often associate their conduct with negative feelings.

While we cannot exclude the occurrence of premeditated attacks in the wild, this indicates that real-world shoulder surfing is mostly not based on malicious intent. Since the majority of observers in our survey were strangers (74 %), this finding complements the work by Muslukhov et al. [32], which suggests that insiders (e.g., friends and family) pose a higher threat to users compared to strangers. In addition, shoulder surfing may be a more serious risk in the business context [23].

Personal Data Leakage Causes User Concern

The information uncovered by observers was personal in the vast majority of cases (79 %) and affected a broad range of private details, even of very intimate nature (e.g., sexual preferences). Although data leakage did mostly not have serious consequences, almost all users who had noticed being shoulder surfed expressed negative feelings like anger or embarrassment (90 %) and tried to protect their data through a variety of coping strategies.

Finding 3: Shoulder surfing affects a broad range of personal information and evokes negative feelings on the side of the user.

This suggests that shoulder surfing has a substantial influence on the user experience of mobile device usage in public, which is in line with prior work by Little and Briggs [29] who found that people respond with stress when their personal data is exposed publicly. It also indicates that mechanisms are required which ensure visual privacy throughout the interaction (e.g., [14, 47]).

Text, Pictures and Games are Most Observed Content

Content most commonly observed was text (47 %), followed by pictures (24 %) and games (13 %). In particular, shoulder surfing mostly affected communication via instant messaging, such as WhatsApp (42 %) and social network activities, for instance, on Facebook (18 %).

Finding 4: Text is observed in most cases, followed by pictures and games. This involves instant messaging and social network activities in particular.

This correlates with mobile device usage investigated in previous work that showed that mobile devices are still communication tools in the first place [5]. Moreover, it again confirms the need for visual privacy-protection concepts.

Shoulder Surfing Affects Credentials

We collected 15 stories (9 %) in which shoulder surfers observed login data. While in most of these cases (12 out of 15) the user was entering an authentication PIN or unlock pattern, there were also cases in which the user was authenticating on a regular website with a user name and password.

Finding 5: Shoulder surfing puts authentication credentials such as PINs, passwords and patterns at risk.

Previous work reported cases in which it was *likely* to be shoulder surfed during authentication [20], and the feasibility of shoulder surfing in the workplace [23]. We report the first evidence of real situations where authentication data was shoulder surfed on mobile devices in the wild. In particular, this finding confirms assumptions made in previous work about observation attacks (e.g., [11, 18, 45]).

Coping Strategies Depend on User/Observer Relation

As previously mentioned, most users did not notice the observer. However, *if* they did, the majority of them took action to prevent further shoulder surfing (46 out of 64 reactions – 72 %). We found that coping strategies tend to differ depending on the relationship between user and observer: If users know the observer, they are likely to react in a more subtle way (e.g. by scrolling quickly) than if the observer is a stranger, where strategies are more obvious (e.g., turning the phone away).

Finding 6: Users adapt their coping strategies against shoulder surfing based on their relation to the observer.

This suggests that users are not only concerned about their privacy, but also about the social implications of their reaction, in particular if the observer is known to them. The importance of social acceptability of security measures has been highlighted in the literature [1]. Moreover, our finding is in line with previous work, which reported that users are sometimes hesitant to unlock their phones in front of friends [32].

It is not Only the User's Own Privacy at Stake

Personal information revealed by shoulder surfing was most commonly related to a user's relationships (49 out of 143 cases – 34 %). In more than a third of these cases (18 out of 49), the uncovered personal piece of information did not concern the users themselves, but third persons they were communicating with (e.g., names, interests, insight into an apartment via video chat in one case).

Finding 7: Shoulder surfing leaks personal information about third persons through the content with which the user interacts.

This is crucial in the business context and has been emphasised as challenge for the security of sensitive information when people work while commuting [24].

DESIGN IMPLICATIONS FOR PRIVACY PROTECTION

From the findings discussed in the previous section, we derive the following implications to guide researchers and practitioners in designing feasible privacy protection systems and improving the experience of using mobile devices in public:

1. **Privacy protection should cover the broad range of information that is leaked by shoulder surfing.** While Finding 5 supports the need for observation-resistant authentication schemes, Finding 3, 4 and 7 show that due to the popularity of instant messaging and social networks, text and pictures are most prone to shoulder surfing in public. Thus, research should extend its current focus on credentials to systems that protect other types of data. Examples for such systems are [14], [47] and [54].

2. **Privacy protection should be lightweight, fast, and easy.** Since shoulder surfing is often casual without serious consequences (Finding 2), users might not be willing to deal with excessive overhead for the benefit of privacy. Prior work has shown that users value usability more than security [17]. Systems for visual privacy thus have to be designed and evaluated not only for the protection but also for the usability they provide.

3. **Privacy protection should not have to be initiated by the user in a shoulder surfing situation.** Finding 1 shows that most users are unaware of being observed. In contrast to approaches taken in prior work (e.g., [11, 45]), where protection is switched on and off by the user, this suggests that automatically triggering protection or alerting the user (like in [2]) is more effective. For this purpose, a system could rely on contextual information to determine, for example, whether a user is currently riding public transportation.

4. **Privacy protection should be socially acceptable**. Finding 6 suggests that, as with other security systems [1], social acceptability has an impact on visual privacy protection. In order to avoid social implications, in particular in cases in which the user is acquainted with the observer, solutions need to be designed and evaluated with social acceptability in mind.

CONCLUSION AND FUTURE WORK

Shoulder surfing has motivated an abundance of studies and systems in the past, in particular in the area of usable security and privacy. To date however, the real-world relevance and implications of shoulder surfing itself were still underexplored. This work contributes to the literature the results of an online survey (N=174), in which we collected stories from both users and observers about their experiences with shoulder surfing. The received reports provide insight into various aspects of the nature of shoulder surfing. For example, observations are usually casual and opportunistic, but uncover a broad range of personal information (e.g., authentication data, interests, dating) and thus evoke negative feelings for both users and observers. Users react with diverse coping strategies that depend on their relationship to the observer. However, in most cases shoulder surfing goes unnoticed. Thus, our findings improve understanding of shoulder surfing in the wild and inform a set of implications for feasible privacy protection mechanisms. In future work, we want to 1) find ways to quantify shoulder surfing in the field, 2) investigate the existence and the frequency of malicious shoulder surfing attacks, and 3) examine usable ways to protect sensitive data in public. Additionally, in-depth interviews could be a beneficial next step to learn more about some of the specific issues presented in this work.

REFERENCES

1. Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (1999), 40–46. DOI: http://dx.doi.org/10.1145/322796.322806
2. Mohammed Eunus Ali, Anika Anwar, Ishrat Ahmed, Tanzima Hashem, Lars Kulik, and Egemen Tanin. 2014. Protecting Mobile Users from Visual Privacy Attacks. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 1–4. DOI: http://dx.doi.org/10.1145/2638728.2638788
3. Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical Passwords in the Wild: Understanding How Users Choose Pictures and Passwords in Image-based Authentication Schemes. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 316–322. DOI: http://dx.doi.org/10.1145/2785830.2785882
4. Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2011. The Phone Lock: Audio and Haptic Shoulder-surfing Resistant PIN Entry Methods for Mobile Devices. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '11)*. ACM, New York, NY, USA, 197–200. DOI: http://dx.doi.org/10.1145/1935701.1935740
5. Matthias Böhmer, Brent Hecht, Johannes Schöning, Antonio Krüger, and Gernot Bauer. 2011. Falling Asleep with Angry Birds, Facebook and Kindle: A Large Scale Study on Mobile Application Usage. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI '11)*. ACM, New York, NY, USA, 47–56. DOI: http://dx.doi.org/10.1145/2037373.2037383
6. Barry Brown, Moira McGregor, and Donald McMillan. 2014. 100 Days of iPhone Use: Understanding the

Details of Mobile Device Use. In *Proceedings of the 16th International Conference on Human-computer Interaction with Mobile Devices & Services (MobileHCI '14)*. ACM, New York, NY, USA, 223–232. DOI: http://dx.doi.org/10.1145/2628363.2628377

7. Frederik Brudy, David Ledo, Saul Greenberg, and Andreas Butz. 2014. Is Anyone Looking? Mitigating Shoulder Surfing on Public Displays Through Awareness and Protection. In *Proceedings of the International Symposium on Pervasive Displays (PerDis '14)*. ACM, New York, NY, USA, Article 1, 6 pages. DOI: http://dx.doi.org/10.1145/2611009.2611028
8. Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the Security of Gaze-based Cued-recall Graphical Passwords Using Saliency Masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 3011–3020. DOI: http://dx.doi.org/10.1145/2207676.2208712
9. Ted Byrt, Janet Bishop, and John B. Carlin. 1993. Bias, Prevalence and Kappa. *Journal of clinical epidemiology* 46, 5 (1993), 423–429.
10. Jacob Cohen. 1960. A Coefficient of Agreement for Nominal Scales. *Educational and Psychological Measurement* 20, 1 (1960), 37–46.
11. Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hußmann, and Matthew Smith. 2014. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2937–2946. DOI: http://dx.doi.org/10.1145/2556288.2557097
12. Alexander De Luca, Katja Hertzschuch, and Heinrich Hußmann. 2010. ColorPIN: Securing PIN Entry Through Indirect Input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1103–1106. DOI: http://dx.doi.org/10.1145/1753326.1753490
13. Michael E. Dewey. 1983. Coefficients of Agreement. *The British Journal of Psychiatry* 143, 5 (1983), 487–489.
14. Malin Eiband, Emanuel von Zezschwitz, Daniel Buschek, and Heinrich Hußmann. 2016. My Scrawl Hides It All: Protecting Text Messages Against Shoulder Surfing With Handwritten Fonts. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 2041–2048. DOI: http://dx.doi.org/10.1145/2851581.2892511
15. Alvan R. Feinstein and Domenic V. Cicchetti. 1990. High Agreement but Low Kappa: The Problems of Two Paradoxes. *Journal of Clinical Epidemiology* 43, 6 (1990), 543–549.
16. John C. Flanagan. 1954. The Critical Incident Technique. *Psychological Bulletin* 51, 4 (1954), 327–360.
17. Simson Garfinkel and Heather Richter Lipford. 2014. *Usable Security:History, Themes, and Challenges*. Morgan & Claypool. 124– pages. DOI: http://dx.doi.org/10.2200/S00594ED1V01Y201408SPT011
18. Jan Gugenheimer, Alexander De Luca, Hayato Hess, Stefan Karg, Dennis Wolf, and Enrico Rukzio. 2015. ColorSnakes: Using Colored Decoys to Secure Authentication in Sensitive Contexts. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 274–283. DOI: http://dx.doi.org/10.1145/2785830.2785834
19. Kevin A. Hallgren. 2012. Computing Inter-rater Reliability for Observational Data: An Overview and Tutorial. *Tutorials in Quantitative Methods for Psychology* 8, 1 (2012), 23–34.
20. Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 213–230. https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach
21. Brian Honan. 2012. Visual Data Security White Paper. (2012).
22. Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1645–1648. DOI: http://dx.doi.org/10.1145/2702123.2702183
23. Ponemon Institute. 2016. Global Visual Hacking Experimental Study: Analysis. (2016). multimedia.3m.com/mws/media/1254232O/global-visual-hacking-experiment-study-summary.pdf
24. Iron Mountain. 2013. Protecting sensitive company information from the commuter snoopers. (2013). http://www.ironmountain.co.uk/Company/Company-News/News-Categories/Press-Releases/2013/October/8.aspx
25. Amy K. Karlson, A.J. Brush, and Stuart Schechter. 2009. Can I Borrow Your Phone?: Understanding Concerns When Sharing Mobile Phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 1647–1650. DOI: http://dx.doi.org/10.1145/1518701.1518953

26. Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 2156–2164. DOI: http://dx.doi.org/10.1145/2851581.2892314

27. J. Richard Landis and Gary G. Koch. 1977. The Measurement of Observer Agreement for Categorical Data. *Biometrics* 33, 1 (1977), 159–174. DOI: http://dx.doi.org/10.2307/2529310

28. Shiguo Lian, Wei Hu, Xingguang Song, and Zhaoxiang Liu. 2013. Smart Privacy-preserving Screen Based on Multiple Sensor Fusion. *IEEE Transactions on Consumer Electronics* 59, 1 (2013), 136–143. DOI: http://dx.doi.org/10.1109/TCE.2013.6490252

29. Linda Little and Pam Briggs. 2009. Private Whispers/Public Eyes: Is Receiving Highly Personal Information in a Public Place Stressful? *Interacting with Computers* 21, 4 (2009), 316 – 322. DOI: http://dx.doi.org/10.1016/j.intcom.2009.06.002

30. Diogo Marques, Tiago Guerreiro, and Luis Carriço. 2014. Measuring Snooping Behavior with Surveys: It's How You Ask It. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems (CHI EA '14)*. ACM, New York, NY, USA, 2479–2484. DOI: http://dx.doi.org/10.1145/2559206.2581240

31. Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on Mobile Phones: Prevalence and Trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 159–174. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/marques

32. Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2013. Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*. ACM, New York, NY, USA, 271–280. DOI: http://dx.doi.org/10.1145/2493190.2493223

33. Delroy L. Paulhus and Vazire Simine. 2009. The Self-report Method. In *Handbook of Research Methods in Personality Psychology*, Richard W. Robins, R. Chris Fraley, and Robert F. Krueger (Eds.). Guilford Press, 224–239.

34. George Probst. 2000. *Analysis of the Effects of Privacy Filter Use on Horizontal Deviations in Posture of VDT Operators*. Ph.D. Dissertation. Virginia Polytechnic Institute and State University.

35. 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

36. Hirokazu Sasamoto, Nicolas Christin, and Eiji Hayashi. 2008. Undercover: Authentication Usable in Front of Prying Eyes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. ACM, New York, NY, USA, 183–192. DOI: http://dx.doi.org/10.1145/1357054.1357085

37. Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia (MUM '12)*. ACM, Ulm, Germany. DOI: http://dx.doi.org/10.1145/2406367.2406384

38. Jeremy Schiff, Marci Meingast, Deirdre K. Mulligan, Shankar Sastry, and Ken Goldberg. 2009. *Respectful Cameras: Detecting Visual Markers in Real-Time to Address Privacy Concerns*. Springer London, London, 65–89. DOI: http://dx.doi.org/10.1007/978-1-84882-301-3_5

39. 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

40. Desney S. Tan, Pedram Keyani, and Mary Czerwinski. 2005. Spy-resistant Keyboard: More Secure Password Entry on Public Touch Screen Displays. In *Proceedings of the 17th Australia Conference on Computer-Human Interaction (OZCHI '05)*. Computer-Human Interaction Special Interest Group (CHISIG) of Australia, Narrabundah, Australia, 1–10. http://dl.acm.org/citation.cfm?id=1108368.1108393

41. Peter Tarasewich, Jun Gong, and Richard Conlan. 2006. Protecting Private Data in Public. In *CHI '06 Extended Abstracts on Human Factors in Computing Systems (CHI EA '06)*. ACM, New York, NY, USA, 1409–1414. DOI: http://dx.doi.org/10.1145/1125451.1125711

42. Roger Tourangeau and Ting Yan. 2007. Sensitive Questions in Surveys. *Psychological bulletin* 133, 5 (2007), 859–883. DOI: http://dx.doi.org/10.1037/0033-2909.133.5.859

43. Shari Trewin, Cal Swart, Larry Koved, and Kapil Singh. 2016. Perceptions of Risk in Mobile Transaction. In *2016 IEEE Security and Privacy Workshops (SPW)*. 214–223. DOI: http://dx.doi.org/10.1109/SPW.2016.37

44. Wouter van Eekelen, John van den Elst, and Vassilis-Javed Khan. 2014. Dynamic Layering Graphical Elements For Graphical Password Schemes. In *Proceedings of the Chi Sparks 2014 Conference: HCI Research, Innovation, and Implementation*. The Hague University of Applied Sciences, The Hague, The Netherlands, 65–73.

45. Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hußmann. 2015a. 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

46. Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hußmann. 2015b. Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2339–2342. DOI: http://dx.doi.org/10.1145/2702123.2702202

47. Emanuel von Zezschwitz, Sigrid Ebbinghaus, Heinrich Hußmann, and Alexander De Luca. 2016. You Can't Watch This!: Privacy-Respectful Photo Browsing on Smartphones. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 4320–4324. DOI: http://dx.doi.org/10.1145/2858036.2858120

48. Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying Eyes and Hidden Controllers: A Qualitative Study of Peoples Privacy Perceptions of Civilian Drones in the US. *Proceedings on Privacy Enhancing Technologies* 2016, 3 (2016), 172–190. DOI: http://dx.doi.org/10.1515/popets-2016-0022

49. Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. Design and Evaluation of a Shoulder-surfing Resistant Graphical Password Scheme. In *Proceedings of the Working Conference on Advanced Visual Interfaces (AVI '06)*. ACM, New York, NY, USA, 177–184. DOI: http://dx.doi.org/10.1145/1133265.1133303

50. Oliver Wiese and Volker Roth. 2015. Pitfalls of Shoulder Surfing Studies. In *NDSS Workshop on Usable Security 2015 (USEC'15)*. Internet Society, 1–6.

51. Christian Winkler, Jan Gugenheimer, Alexander De Luca, Gabriel Haas, Philipp Speidel, David Dobbelstein, and Enrico Rukzio. 2015. Glass Unlock: Enhancing Security of Smartphone Unlocking Through Leveraging a Private Near-eye Display. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1407–1410. DOI: http://dx.doi.org/10.1145/2702123.2702316

52. Lorette K. Woolsey. 1986. The Critical Incident Technique: An Innovative Qualitative Method of Research. *Canadian Journal of Counselling* 20, 4 (1986), 242–254.

53. Yi Xu, Jared Heinly, Andrew M. White, Fabian Monrose, and Jan-Michael Frahm. 2013. Seeing Double: Reconstructing Obscured Typed Input from Repeated Compromising Reflections. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*. ACM, New York, NY, USA, 1063–1074. DOI: http://dx.doi.org/10.1145/2508859.2516709

54. Huiyuan Zhou, Vinicius Ferreira, Thamara Alves, Kirstie Hawkey, and Derek Reilly. 2015. Somebody Is Peeking!: A Proximity and Privacy Aware Tablet Interface. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. ACM, New York, NY, USA, 1971–1976. DOI: http://dx.doi.org/10.1145/2702613.2732726