Securing Personal Items in Public Space

Stories of Attacks and Threats

Sarah Prange*
Bundeswehr University, LMU Munich
Munich, Germany
sarah.prange@unibw.de

Lukas Mecke*
Bundeswehr University, LMU Munich
Munich, Germany
lukas.mecke@unibw.de

Michael Stadler
University of Applied Sciences
Munich, Germany
michael.stadler@hm.edu

Maximilian Balluff
University of Applied Sciences
Munich, Germany
m.balluff@hm.edu

Mohamed Khamis
University of Glasgow
Glasgow, UK
Mohamed.Khamis@glasgow.ac.uk

Florian Alt
Bundeswehr University
Munich, Germany
florian.alt@unibw.de

ABSTRACT

While we put great effort in protecting digital devices and data, there is a lack of research on usable techniques to secure personal items that we carry in public space. To better understand situations where ubiquitous technologies could help secure personal items, we conducted an online survey (N=101) in which we collected real-world stories from users reporting on personal items, either at risk of, or actually being lost, damaged or stolen. We found that the majority of cases occurred in (semi-)public spaces during afternoon and evening times, when users left their items. From these results, we derived a model of incidents involving personal items in public space as well as a set of properties to describe situations where personal items may be at risk. We discuss reoccurring properties of the scenarios, potential multimedia-based protection mechanisms for securing personal items in public space as well as future research suggestions.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**;
• **Security and privacy**;

KEYWORDS

usable security, personal items, public space, everyday life, online survey, real world stories

ACM Reference Format:
Sarah Prange, Lukas Mecke, Michael Stadler, Maximilian Balluff, Mohamed Khamis, and Florian Alt. 2019. Securing Personal Items in Public Space: Stories of Attacks and Threats. In *18th International Conference on Mobile and Ubiquitous Multimedia (MUM 2019), November 26–29, 2019, Pisa, Italy*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3365610.3365628

*Both authors contributed equally to this research.

MUM 2019, November 26–29, 2019, Pisa, Italy

ACM ISBN 978-1-4503-7624-2/19/11…$15.00
https://doi.org/10.1145/3365610.3365628

1 INTRODUCTION

Much of the research in usable security and privacy is based on the assumption that attackers get physical access to users' personal devices, such as smartphones, tablets, or laptops. Subsequently, to mitigate the risk of attackers gaining access to sensitive data that is either stored on the device itself or can be accessed by means of the device, researchers are developing an ever-increasing number of authentication concepts (e.g., [5, 20]). The main focus of these works is to ensure that the attacker is unable to find the user's login credentials through, for example, shoulder surfing [6], smudge attacks [2, 16], guessing attacks, or thermal attacks [1].

At the same time, little research exists on understanding the context and circumstances under which personal devices are stolen. Undisputedly, though, theft of personal items occurs frequently. For example, in Germany about 600 smartphones are stolen every day[1]. We argue that we should take a step back and first understand *how* attackers get access to personal items. Attackers do not only steal personal items to access sensitive information, but also for monetary value (e.g., selling a stolen smartphone on the black market). Knowledge about how attackers get access to personal devices is valuable because by understanding such situations, we can design better protective mechanisms to prevent theft or allow users to find their stolen/lost items.

The objective of our research is to (a) obtain an understanding of the context in which attackers (might) get physical access to users' personal devices and (b) to derive requirements for designing mechanisms that prevent attackers from getting access to the device in the first place. This is valuable in the context of authentication as well: if a personal device is able to understand that it is in the hand of an attacker, appropriate security measures could be taken, such as switching to a secure authentication mechanism, that would require too much effort and thus be inappropriate for daily use.

Our research approach is: Firstly, we conducted an online survey (N=101) where we asked participants to describe in detail a situation in which a personal item was at risk or even attacked. Secondly, we analysed these situations for common themes and derived opportunities for the design of systems capable of securing personal items in public space. Such mechanisms may involve the personal items, the owners, or group members and/or bystanders. Thirdly we derive open questions and opportunities for future research.

All sources were last accessed August 30, 2019
[1] www.presseportal.de/pm/55928/3348558

2 BACKGROUND & RELATED WORK

Prior work on securing personal items mainly focuses on users' digital possessions (i.e., data), which may be protected through several authentication factors – mainly knowledge-based, token-based, or biometric [12]. A number of authentication mechanisms aiming at being more secure while at the same time being more usable have been investigated in prior work [16, 20]. Further, methods to reduce authentication overhead have been introduced, for example, SnapApp [3].

However, we see a a main risk in how potential attackers may gain access to the personal item itself. 127,376 cases of pick-pocketing were reported at German police departments in 2017[2]. Especially in locations such as bars, bags are particularly at risk when placed over a chair or on the floor [17]. Some devices hence employ "anti-theft features", mainly addressing the issue of returning and/or finding the device (in particular smartphones) once it got lost. Examples include Google's *find my device*[3] or Apple's *find my iPhone*[4]. Examples for securing other items include anti-theft systems for bikes[5] or security cables to lock laptops[6]. Moreover, patents for anti-theft mechanisms have been granted (e.g., for portable electronic devices [21], vehicles [14], or detection of theft or burglaries [10]).

Moreover, to securely store and carry personal items, several protection features have been applied to bags. Examples include, but are not limited to, the use of cut resistant, waterproof or RFID blocking material or hidden or locking zippers (e.g., *Bobby Original Anti-Theft Backpack*[7], *Secura® Premier Anti-Theft Satchel*[8]). However, while many devices already employ authentication mechanisms, the need for ubiquitous security mechanisms for personal items as physical objects is under-investigated. Secured bags have been proposed as a possible solution, but those still do not actively avoid or intervene in potential attacks. With our work, we obtain an understanding of potential attacks to guide the use of ubiquitous multimedia to design more suitable security mechanisms for personal items.

3 ONLINE SURVEY

3.1 Design and Method

With our work, we investigate attacks and risks for personal items. We hence decided to collect *real world stories* from users in an online survey. To achieve this, we loosely followed the critical incident technique [7] and questions were designed in such a way that both, victims and bystanders, could report on stories. For other threats, this methodology already provided valuable insights [6]. Note, that there is no IRB at our institution. However, we made sure to comply with the study, ethics and privacy regulations of our local university.

3.2 Questionnaire Structure

The questionnaire consisted of three parts (refer to Appendix A): 1) a free text entry field for a detailed description of the scenario, 2) voluntary open-ended questions about details of the scenario (e.g., time, location), and 3) demographic questions. We also included a 5-point Likert item about participants being honest in their answers. Participants could fill in the questionnaire multiple times if they had multiple scenarios to share.

Gender	75	Female
	25	Male
	1	Not stated
Mean Age	27.93	
Occupation	68	Student
	26	Employee
	7	Other or not stated
Nationality	92	German
	9	Other or not stated

Table 1: Demographics of participants who filled in our online questionnaire (N=101).

3.3 Participants

We ran the survey in spring 2018 in a large German city. It was distributed via a university mailing list and participants were self-selected. We excluded 8 scenarios due to being not honest (i.e., participants did not partially or fully agree to being honest) or describing no scenario (e.g., P73: "*I can't remember such a situation*"), resulting in a total of 101 scenarios. The reported mean age was 27.93 (compare Table 1) and most participants were female (75%). Participants were mainly students (68%) and almost all were German (92%). Participants could win one of three €20 gift vouchers.

3.4 Limitations

Our study sample is biased towards young people, students and females. In addition we only received one scenario from the viewpoint of an attacker. This may cause bias in our qualitative insights. Due to our data being self-reported, our insights are limited to parts of scenarios participants were willing to share and/or recalling correctly and may also have been influenced by our wording [13]. Participants may also have modified their answers due to social desirability [18]. However, we took great care to avoid bias in the questions (e.g., we avoided the term "victim" in favour of "owner") and most participants indicated they were honest in their answers.

4 ANALYSIS & DATASET

4.1 Coding Process

The dataset used for analysis consisted of 101 answers; each including a *scenario description*, answers to *detail questions* and *demographic* information. We applied qualitative content analysis to the descriptions as well as the detail questions. Two researchers independently applied in-vivo coding to all answers and merged their codes afterwards. Focused coding was applied to derive categories from the in-vivo codes (e.g., codes such as "in a backpack" and "carried" were grouped to "item storage"). Finally, axial coding was applied to find relations between the discovered categories. We noticed that categories could be associated with one of two models: either describing properties of the environment or steps occurring in the event of an incident. We report on both derived models in Sections 5 (*environmental properties*) and 6 (*incident model*), respectively. Participants' quotes were translated from German.

[2] www.bundespolizei.de/Web/DE/02Sicher-im-Alltag/01Vorsicht-Taschendiebstahl/04Statistik/statistik_node
[3] www.google.com/android/find,
[4] support.apple.com/kb/PH19297?viewlocale=en_EN
[5] www.indiegogo.com/projects/boomerang-v2-bike-anti-theft-safety-system
[6] https://www.kensington.com/p/products/security/keyed-locks/
[7] www.xd-design.com/us-us/bobby-anti-theft-backpack-grey
[8] www.lewisnclark.com/secura-rfid-blocking-anti-theft-satchel/

Time	
• afternoon	29
• evening	17
• night	16
• noon	15
• forenoon	12
• during the day	7
• morning	3
• other	5
Location	
• public transport	16
• university/work/library	12
• public road/place	10
• station/airport	10
• food court/bar	8
• city	5
• sports facility	4
• disco	3
• other	11
Artefacts	
• smartphone	32
• wallet	29
• bag/backpack/suitcase	27
• bike	14
• clothes	6
• camera	4
• money	4
• laptop	3
• car	3
• keys	3
• other	8
Protected	
• yes	45
• no	43
• other	8
Companions	
• alone	53
• not alone	45
• other	2

Table 2: *Properties of potentially dangerous environments* (Section 5), as found from the collected situations. Counts indicate the number of scenarios the respective manifestation was mentioned in. For details refer to Section 4.2.1.

Action	
• leave item	22
• have item with them	21
• (shortly) leave unattended	18
• forget item	12
• secure item	11
• distraction/sleep	9
• accident	3
• other	2
• unclear	15
Incident	
• theft	45
• no attack	25
• damage	8
• raid	3
• other	2
• unclear	20
Reaction	
• emotional reaction	31
• none	23
• confront attacker	15
• search	15
• none (no incident)	10
• file a complaint (police)	5
• return to owner	5
• increase vigilance	4
• alert owner	4
• other	2
Reaction time	
• delayed reaction	40
• instant reaction	23
• no reaction (no incident)	10
• no reaction	2
• unclear	25
Consequence	
• none	34
• loss	30
• damage	8
• partial loss	7
• unclear	23

Table 3: Number of scenarios mentioning phases of our *incident model* (Section 6). For Details refer to Section 4.2.2.

4.2 Results

We quantified both, scenarios and detail questions, and in this section report on the results. For quantification, one scenario could contribute to multiple manifestations in the same category if more than one was mentioned (e.g., the manifestations "wallet" and "money" would be separately counted towards the category "Artefacts" if both were mentioned in one scenario). Manifestations that were mentioned less than 3 times over all scenarios were summarised as "other". In cases where the manifestation of a category could not unambiguously be determined, we marked it as "unclear".

4.2.1 Environmental Properties. Results relating to environmental properties are illustrated in Table 2. We found the scenarios being relatively evenly spread over different *times* with a light tendency to occurring later in the day. Except for a few cases (e.g., work), only public places were given as *locations* in the scenarios. The affected *artefacts* were mainly smartphones, wallets and bag-like objects. Notice, that this includes several situations where those things were affected simultaneously (e.g., P33: "*I forgot a bag containing my wallet on a chair in my unlocked office*"). There were also a large number of scenarios involving bikes. Scenarios were almost evenly split between cases where personal items were *protected* (e.g., P55: "*My bike was stolen [...] although it was locked*") or left unsecured as well as between the owner being alone or having *companions*.

4.2.2 Phases of Incident Situations. Results relating to observed phases of incident situations are illustrated in Table 3. Our scenarios included many situations in which participants either left items unattended (for a short duration) or where items were intentionally left and secured (e.g., locking a bike to an object). The most common *incident* was theft. In 25 cases no incident occurred (i.e., there was no attack on personal items (e.g., theft or damage)). Many participants described to have *reacted* emotionally on incidents. In some cases, the attacker was confronted or a lost item searched (15 occurrences each). In 23 cases no reaction was shown/described. This was oftentimes linked to a long *reaction time*, i.e., the participant only noticed the incident after a certain delay (40 occurrences). Instant reactions were only shown by 23 participants. In most cases there were no consequences. However those cases are closely followed by a total of 30 cases where an artefact was lost (including stolen in the sense of lost for the owner). In some cases items were damaged or partial loss occurred (e.g., P13: "*[...] I found my ransacked bag in a bush [...]. Except for my phone and cash everything was still there*").

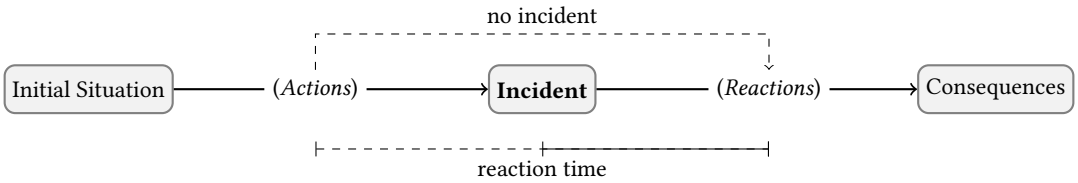

Figure 1: Incident model: From an initial situation, an incident (i.e., an attack on a personal item/artefact) may occur. This can either be triggered by an action (e.g., leaving an item unattended) or arise from the situation itself (e.g., crowded environment). After an incident, the consequences (e.g., loss of the artefact) can be influenced by the owner or bystanders according to their reaction. This also holds if no incident occurred but a personal item was at risk nonetheless (e.g., forgotten or lost). In both cases, a further influencing factor is the reaction time (i.e., the time until a reaction is shown).

5 PROPERTIES OF POTENTIALLY DANGEROUS ENVIRONMENTS

From analysing scenarios and questions, we identified a set of entities, actions, and properties to describe dangerous environments.

5.1 Entities

5.1.1 Actors. As actors we describe all people who can influence the situation by taking an *action* or remaining passive. We observed three groups of possible actors: The victim or *owner*, the (potential) *attacker(s)*, and *bystanders*, with both attackers and bystanders being either acquaintances, strangers or both (multiple bystanders). Notice how also the absence of actors (e.g., no attacker) and the number of people can influence the situation (e.g., bystander effect [9]).

5.1.2 Artefacts. Under the term *artefacts*, we collect the set of possibly endangered personal items. Those can be described by their *type* (e.g., purse or phone), *value* (monetary or sentimental) and *storage* (e.g., backpack, carried etc.). The latter also includes measures taken to protect the item (e.g., attaching a lock).

5.2 Actions

All actors can influence the current situation by performing either *actions* or *reactions*. In this context we also consider taking no (re)action (e.g., ignoring an incident) as a (re)action. Notice, how actions taken can be influenced both, by the current environment as well as the acting party's mental model. This includes assumptions (e.g., P3: "*We expected that during daytime [...] nobody would try to steal something*") and habits that lead to a certain behaviour.

5.3 Environmental Properties

Apart from the entities and the actions taken, the environment itself has properties that may influence the situation as well as the actors' mental model. Those include the *time* (e.g., P3: "*[...] daytime (it was noon/early afternoon) [...]*"), *weather* (e.g., P85: "*in a cold winter night [...]*"), *location* and *semantic context* (e.g., vacation, parties). There may be more *contextual* factors having an influence (e.g., Schmidt et al. [15]) that we did not observe in our sample.

6 INCIDENT MODEL

From the reported scenarios, we derived a model of incidents (cf. Fig. 1), consisting of three main *phases* with *transitions* between; allowing for optional actions and reactions. In this section, we provide further detail about those phases and their interplay.

6.1 Initial situation

The initial situation is the prerequisite for an incident. It can be described via the properties of potentially dangerous environments (compare Section 5). Depending on the initial situation and actions taken, different incidents are (not) possible.

6.2 Actions

Starting from the initial situation, an incident can happen due to the owner putting an artefact at risk (e.g., P95: "*The mobile of our exchange pupil was stolen from her backpack at a lake. She was in the water at that time*"). In other cases, no action is required and an incident can arise from the situation itself without active involvement of the owner (e.g., P63: "*A man asked me for the time and I read it from my clock. Suddenly he approached me and embraced me for giving the answer while at the same time searching the pockets of my jacket for valuables.*"). Finally, it is also possible that a user's action does not lead to an incident (i.e., an active attack), but only puts items at risk (e.g., P9: "*After paying, we left the building and I accidentally left my phone [...]. There was a risk that one of the visitors would steal my phone. Luckily nothing happened*").

6.3 Incident

We only consider a situation an "incident" in case an actual attack happened or was attempted. This includes for example theft, robbery and damage to objects. Notice, however, that the absence of an attack does not necessarily imply that there are no negative consequences (e.g., P107: "*I once slipped on an icy sidewalk [...] and the phone in my pocket was damaged when I fell*").

6.4 Reactions

After an incident, there is another window of opportunity for reactions by all actors. While the attacker may try to secure the item or retreat from the situation, both owner and bystanders have the opportunity to intervene (e.g., by stopping the attacker or draw the owner's attention to a forgotten item, e.g., P29: "*Forgot phone on the bar when getting pizza from a good restaurant. Another client alerted the personnel and handed it over.*"). Both, for actions and reactions, the *reaction time* may influence the outcome (e.g., in case of damage, intervention may not be possible shortly afterwards or returning to a forgotten item may be too late).

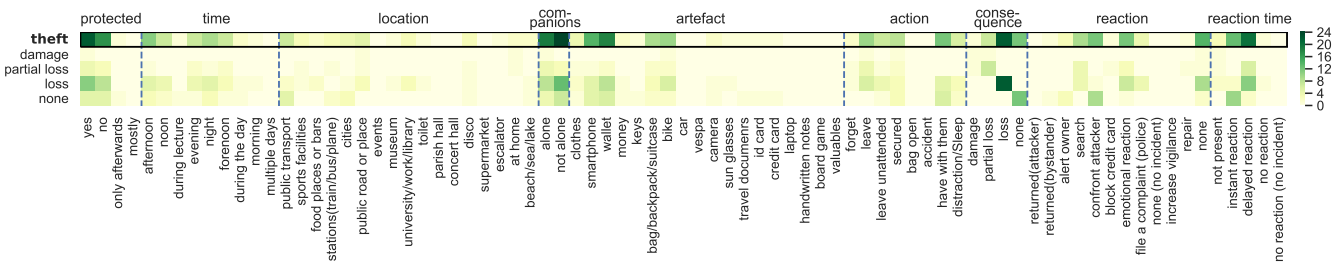

Figure 2: Co-occurrence of situational properties (left) and phases in our incident model (right) with potential consequences (y-axis) for situations with (attempted) theft. First line indicates overall co-occurrence of theft with all properties, the following lines denote the outcomes of situations with (attempted) theft w.r.t all properties (refer to Appendix B, Fig. 3 for full list).

6.5 Consequences

Depending on the previous factors, the situation may result in one of several outcomes. Consequences can be divided in cases where factual damage or loss occurred (e.g., P44: "*My bike was stolen*") and situations in which damage could be averted (e.g., P87: "*[...] A man managed to grab in her backpack. [...] She turned and loudly said "Hey!". The man walked away and immediately left the subway [...].*") or the initial state restored (e.g., P8: "*[...] both students managed to repair the plug, so that the incident had no negative consequences.*").

7 DESIGN OPPORTUNITIES

In prior sections, we described properties and sequences of events for situations in which incidents involving personal belongings occurred or were probable. In this section, we elaborate on some reoccurring patterns in those scenarios and, based on those, discuss design opportunities for possible ubiquitous security mechanisms.

7.1 Don't Forget Me: Items remind Owners

In our results, we found multiple scenarios in which users left their personal items *unattended*, accidentally as well as intendedly (compare Table 3, category *Action*). This may be due to a lack of awareness (e.g., P35: "*After having lived in Japan for a while - where it is common to leave personal belongings [...] to reserve spots [...] - I habitually left my wallet on the table several times [...]*"), false optimism (e.g., P12: "*There was a sign indicating that no liability is accepted [...], but of course one would not expect something to be taken away*") or urgent reasons (e.g., P62: "*I left my bag in the train and went for the toilet*"). However we found that instantly reacting to an incident often allowed for loss to be prevented, whereas loss occurred more often in situations where the owner reacted with a delay (compare Fig. 2, category *reaction time*).

Multimedia-based solutions can help by intervening before or after an item is left (cf. our model, Fig. 1). For instance, context detection can be used to assess the initial situation, predict potential risks (e.g., based on collected incident data) or media can be used to increase awareness in general. A possible security mechanism for personal items could also detect situations in which items were left behind or unattended to foster reactions (e.g., using proximity sensing technology like Bluetooth). As a result, sound or mobile notifications could be used to draw the owner's attention, hopefully leading them to take their personal belongings and/or increase their awareness for future, similar situations.

7.2 One For All and All For One: Involving Bystanders and Group Members

We encountered several scenarios of users being in groups (i.e., at least two people) when facing situations where personal items were at risk (about half of the participants stated to not be "alone", compare Table 2, category *Companions* and more cases of loss occurring in groups, compare Fig. 2, category *Companions*). Hence, we envision possible security mechanisms for personal items could at least address one of the group members to not only secure their own, but also the others' items. Moreover, in situations where the group is small, but bystanders are present, a security mechanism could involve them to protect personal items (assuming that bystanders are trusted parties). To enrich the motivation to take care of others' belongings (i.e., increase security of each and everyone's items), a reward system could be developed.

As an example, such situations often happen on trains: a passenger wants to leave the seat with personal items (e.g., P89: "*owner has to go to the toilet and leaves backpack on their seat on the train.*"). Hence, they may ask fellow travellers to look after their belongings. This not only calms absent owners, but also warns bystanders and potential attackers. Possible rewards for helpful fellow passengers may include, but are not limited to, free seat reservations or coffee.

7.3 Summary

To summarise, we see multiple starting points for security mechanisms protecting personal items, namely (1) the artefacts themselves, (2) the owners, and (3) group members and/or bystanders.

8 FURTHER RESEARCH OPPORTUNITIES

Based on the previous considerations, we see the following aspects to consider in future research to a) gain a deeper understanding / validating our current model of potentially dangerous situations and b) investigate possible security mechanisms for personal items.

8.1 Understanding Critical Situations

To gain insights with regards to potentially dangerous situations, we conducted an online survey. For more in-depth insights, interviews could provide more details about scenarios. However, self-reported data may be subjective and/or biased. Further research could hence consider more "objective" approaches, including, but not limited to, observations in-the-wild or in-depth analysis of crime statistics.

8.2 Designing Security Mechanisms

8.2.1 Context Detection. As a prerequisite for interventions or activating potential security mechanisms, a system requires knowledge about its context. We envision such systems to detect the context and environment, in particular with respect to the properties we describe in Section 5. This could be used to identify critical situations and nudge users to take measures against potential attackers.

8.2.2 Sensitivity. For potential security mechanisms, it is important to strike a good balance between reacting overly sensitive to non-threatening situations (e.g., a legitimate user opening their bag) and not reacting in the case of a real incident. It also remains to be investigated what behaviour users would expect (e.g., overly sensitive vs rather relaxed) and how to best match this.

8.2.3 Protection. Adding protection to artefacts can potentially prevent incidents (e.g., P3: "*Retrospectively, all valuables could have been securely stored in a locker [to prevent the incident].*"). However we also saw a high occurrence of loss for items that were protected (compare Fig. 2). Further research might explore which kinds of protections are effective and how to nudge users to use them.

8.2.4 Intervention. An open question is the appropriate reaction or intervention of a technical solution in case of a detected attack. From the scenarios, we find confronting the attacker or alerting the owner of an item to be common (compare Table 3, category "Reaction") and successful (compare Fig. 2) approaches. Further exploration can be done towards transferring this to technical solutions, e.g., sending a notification or nudging bystanders to intervene.

From a safety perspective there is also the question whether or not in certain situations an intervention should take place at all, as it can impose an actual safety risk, e.g., as stated by P2: "*[After the incident] my mother realised, that things could have gone way differently if [the attackers] would have been armed.*"). For such cases, covert interventions might be further investigated.

8.2.5 Communication & Awareness. Following up on using interventions, another open question is communicating threats. There are several options for technical actors to realise communication. However traditional methods like alarms (e.g., at cars) may be insufficient as bystanders cannot decide if the alarm was triggered by chance or due to an actual attack (see also *Sensitivity* above). This leaves room for further exploration for effective output modalities and communication interfaces (compare e.g., security indicators [8, 11, 19]).

8.2.6 Consequences. As a result of an attack, a security mechanism could still be useful by helping to cope with whatever happened (e.g., repair damage, search for forgotten devices[9]). However, further research should investigate if this is desired by users (i.e., victims of attacks on personal items).

9 DISCUSSION

9.1 Potentially Dangerous Situations

In our reports, we found reoccurring characteristics of situations in which incidents happened. These included crowded locations (e.g., subways) or (semi-) public spaces where items were left unattended (e.g., swimming at lakes). This knowledge may serve further research in multiple ways. On one hand, it can be used to understand potentially dangerous situations and inform the design of usable mechanisms to protect personal belongings in such scenarios. On the other hand, the introduced vocabulary can be used to describe more situations, similar to those collected in this work, and the given dimensions can be a starting point for further exploration.

[9] e.g., www.njoiii.com/the-attic-loft/

9.2 Reasons for Incidents

We found that incidents may happen due to several reasons, both with and without the (active) involvement of the legitimate owner. Some participants reported they left items unattended. In other scenarios, participants did not do anything in particular (e.g., parking their car, leaving their bike locked) or were just present at a certain location. In this work, we provide a model (refer to Section 6) to better understand *how* incidents happen and at which points a (technical) *intervention* is possible. This serves to inform further mechanisms to aid users protect their belongings, as any or all steps in the event chain can be addressed to counteract potential threats.

9.3 When and How to Secure CRAVED Items

Our results align with previous work stating that items attracting thieves oftentimes fulfil the *CRAVED* acronym: *concealable*, *removable*, *available*, *valuable*, *enjoyable* and *disposable* [4]. Namely we found many cases in which smartphones and wallets being "CRAVED" were actually stolen (compare Fig. 2, category *artefact*). While these items may be *valuable* and *enjoyable* by design, we see great potential in designing security mechanisms that protect items from being *removable*. Finally, researchers should consider that the protection mechanism is not more expensive than the item itself.

10 CONCLUSION

With this work, we take first steps to understand situations in which personal items are at risk and why this is the case. We conducted an online survey (N=101), where we collected real world stories from users' personal items being exposed to incidents like theft or damage or generally at risk. From the reported scenarios, we derived a) properties of potentially dangerous environments and b) an incident model. We suggest opportunities for designing security mechanisms for personal items and discuss directions for future research. We hope our work to be useful for further investigating threats on personal items as well as support designers and practitioners building usable security mechanisms.

ACKNOWLEDGMENTS

Work on this project was partially funded 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 Number 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 2017 Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3751–3763. https://doi.org/10.1145/3025453.3025461

[2] 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

[3] Daniel Buschek, Fabian Hartmann, Emanuel von Zezschwitz, Alexander De Luca, and Florian Alt. 2016. SnapApp: Reducing Authentication Overhead with a Time-Constrained Fast Unlock Option. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 3736–3747. https://doi.org/10.1145/2858036.2858164

[4] Ronald Victor Gemuseus Clarke and Barry Webb. 1999. *Hot products: Understanding, anticipating and reducing demand for stolen goods*. Vol. 112. Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, London.

[5] 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. https://doi.org/10.1145/2556288.2557097

[6] 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 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 4254–4265. https://doi.org/10.1145/3025453.3025636

[7] John C Flanagan. 1954. The critical incident technique. *Psychological bulletin* 51, 4 (1954), 327.

[8] Saranga Komanduri, Richard Shay, Lorrie Faith Cranor, Cormac Herley, and Stuart Schechter. 2014. Telepathwords: Preventing Weak Passwords by Reading Users' Minds. In *23rd USENIX Security Symposium (USENIX Security 14)*. USENIX Association, San Diego, CA, 591–606. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/komanduri

[9] Bibb Latané and John M Darley. 1970. *The unresponsive bystander: Why doesn't he help?* Appleton-Century-Crofts, New York.

[10] Jerome H Lemelson. 1982. Theft detection system and method. US Patent 4,337,462.

[11] Lukas Mecke, Sarah Prange, Daniel Buschek, and Florian Alt. 2018. A Design Space for Security Indicators for Behavioural Biometrics on Mobile Touchscreen Devices. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. ACM, New York, NY, USA, Article LBW003, 6 pages. https://doi.org/10.1145/3170427.3188633

[12] L. O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (Dec 2003), 2021–2040. https://doi.org/10.1109/JPROC.2003.819611

[13] Delroy L Paulhus and Simine Vazire. 2007. The self-report method. *Handbook of research methods in personality psychology* 1 (2007), 224–239.

[14] William R Reagan. 1979. Auto theft detection system. US Patent 4,177,466.

[15] Albrecht Schmidt, Michael Beigl, and Hans-W Gellersen. 1999. There is more to context than location. *Computers & Graphics* 23, 6 (1999), 893 – 901. https://doi.org/10.1016/S0097-8493(99)00120-X

[16] 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. https://doi.org/10.1145/2632048.2636090 schneegass2014ubicomp.

[17] Aiden Sidebottom and Kate Bowers. 2010. Bag theft in bars: An analysis of relative risk, perceived risk and modus operandi. *Security Journal* 23, 3 (01 Jul 2010), 206–224. https://doi.org/10.1057/sj.2008.17

[18] Roger Tourangeau and Ting Yan. 2007. Sensitive questions in surveys. *Psychological bulletin* 133, 5 (2007), 859.

[19] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, and William Melicher. 2017. Design and Evaluation of a Data-Driven Password Meter. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3775–3786. https://doi.org/10.1145/3025453.3026050

[20] 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. https://doi.org/10.1145/2702123.2702212

[21] Paul J Wehrenberg. 2007. Acceleration-based theft detection system for portable electronic devices. US Patent 7,218,226.

A QUESTIONNAIRE

A.1 Part 1 Scenario

(1) Please describe, with as much detail as possible, a situation that you experienced yourself, which endangered a personal item. Relevant are situations in which personal items got either stolen or damaged, especially also situations where only the opportunity existed. You could have either been the owner of the item or merely observed the owner.

A.2 Part 2 Detail questions

(1) What item was the focus of the scenario?
(2) Who was the owner of the item?
(3) Was the owner alone or in a group?
(4) At which location did the scenario happen?
(5) How familiar was the owner with the location of the scenario?
(6) How many and which people (e.g., friends, neutral, active or passive observers, attacker) where present?
(7) Describe the behaviour/the activity of the owner and the other people present.
(8) Did the owner take any precautions to protect the item? If so which?
(9) During which time of the day did the scenario occur?
(10) Do you think the owner had knowledge of the risk or did gain knowledge during the scenario?
(11) How did the owner and the people present react?

A.3 Part 3 Demographic questions

(1) Gender (male/female/own answer)
(2) Age
(3) Nationality
(4) Occupation
(5) I was completely honest with my answers during this questionnaire (five point Likert scale)

B FULL CO-OCCURRENCE TABLE

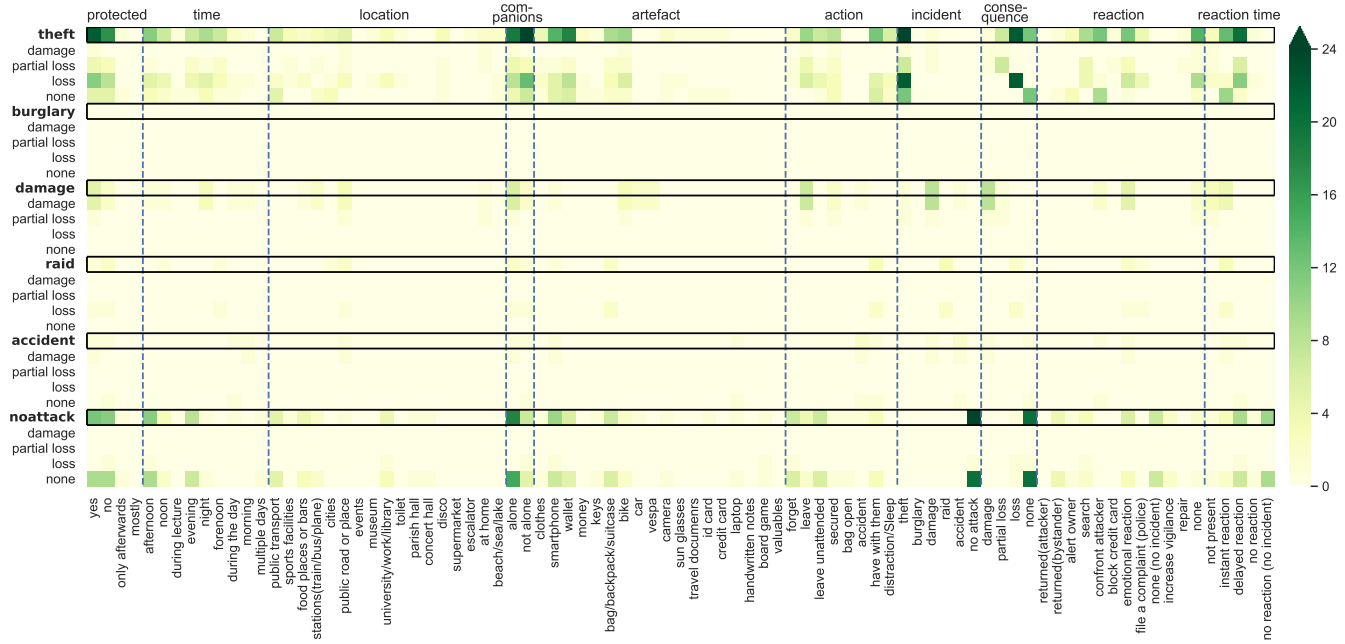

Figure 3: Co-occurrence of situational properties (left) and phases in our incident model (right) with incidents (y-axis, bold). Below each incident is the three way co-occurrence of property, incident and consequence. As an example: the first cell denotes the number of scenarios where theft happened while the item was protected (i.e., theft and protected co-occurred). The cells below illustrate the number of scenarios for each potential outcome (consequence) of this situation (i.e., mostly loss in this case).