



Marky, K., Macdonald, S., Abdrabou, Y. and Khamis, M. (2023) In the Quest to Protect Users from Side-Channel Attacks – A User-Centred Design Space to Mitigate Thermal Attacks on Public Payment Terminals. In: 32nd USENIX Security Symposium, Anaheim, CA, California, 9-11 Aug 2023, pp. 5235-5252. ISBN 9781939133373.

There may be differences between this version and the published version. You are advised to consult the published version if you wish to cite from it.

<http://eprints.gla.ac.uk/300251/>

Deposited on: 08 June 2023

In the Quest to Protect Users from Side-Channel Attacks – A User-Centred Design Space to Mitigate Thermal Attacks on Public Payment Terminals

Karola Marky^{1,2}, Shaun Macdonald², Yasmeen Abdrabou³, Mohamed Khamis²
¹*Ruhr-University Bochum, Germany*, ²*University of Glasgow, United Kingdom*,
³*Lancaster University, United Kingdom*

Abstract

Thermal attacks are an emerging threat that enables the reconstruction of user input *after* interaction with a device by analysing heat traces. There are several ways to protect users from thermal attacks that require different degrees of user involvement. In this paper, we first present a structured literature review to identify 15 protection strategies. Then, we investigate user perceptions of these strategies in an online study ($N = 306$). Our results show that users intuitively use protection strategies that also work against other side-channel attacks. Further, users are willing to sacrifice convenience for the sake of verifying a strategy's efficacy. Yet, an ideal holistic defence from thermal attacks is one that is readily integrated into user interfaces by manufacturers in a way that the user can verify it. Further, users like resourceless strategies that fit their habits. We use the literature review and study results to identify a user-centred design space for thermal attack protection. We conclude the paper with specific recommendations for users, device manufacturers and interface providers to better protect individuals from thermal attacks.

1 Introduction

Thermal attacks can identify user input, such as credentials or sensitive data, based on heat traces left on interface surfaces [41]. These heat traces can be collected after user interaction meaning *after* users have left [10, 15, 27, 41]. Further, thermal attacks allow reconstructing the order of the user input, for instance, to determine a user's PIN [1]. This makes thermal attacks different from other side-channel attacks, such as shoulder surfing, because the attacker does not need to be present at the same time as the user, or smudge attacks that do not reveal the input order. Several studies demonstrated proof-of-concept attacks for common devices, such as smartphones [1], ATMs [41], and keyboards [2, 3, 10].

Researchers proposed numerous possibilities to defend users from thermal attacks, ranging from user-based solutions (e.g., wearing gloves [27]) to manufacturer-based solutions

(e.g., heating the interface [1]). While several of these solutions are promising for delivering effective protection, protection success often relies on assumptions about specific user behaviour, such as extra tasks they must perform, or extra items they must bring. Human factor investigation in related domains, such as e-mail encryption [44, 51] or passwords [48], show that users cannot always be relied on when security-critical tasks interfere with convenience. Further, even if a protection mechanism is secure in theory, missing user trust might result in insecure behaviour because users do not believe that the mechanism will protect them [23]. Consequently, the proposed protection mechanisms in the literature need further investigation, which motivates our first research question:

RQ₁: What are protection strategies against thermal attacks?

We first contribute the results of a structured literature review to identify 15 protection strategies in the scientific literature. Next, we investigated user perceptions of protection strategies to identify which strategies are suitable for usage specifically considering the following research question:

RQ₂: What are the user perceptions towards protection strategies against thermal attacks in public payment scenarios?

For this, we conducted an online survey ($N = 306$) which presented different protection strategies to prospective users in a public payment terminal scenario, such as withdrawing money from an ATM or buying transport tickets on a vending machine. Our results show that intuitively users would use strategies that are not present in the literature, such as waiting at an ATM or observing their surroundings. These strategies also work for other side-channel attacks, such as shoulder surfing. Our results further show that users prefer automatic protection (e.g., by a physical cover), but would sacrifice convenience for the sake of verifying protection efficacy. Strategies known from other domains, such as two-factor authentication or privacy-enhancing keyboards – that shuffle PIN pad keys – were also welcomed. User specifically considered aspects such as uncertainty of effective protection, ease-of-use and effort, but also privacy aspects and hygiene, when evaluating strategies.

We use the results from the literature review and the user study to inform a user-centred design space for mitigating thermal attacks on public payment terminals. Our design space considers the *protection strategy* which can be: (1) thermal masking (i.e., adding additional heat traces), (2) heat trace manipulation (i.e., using complex credentials), (3) heat trace reduction (i.e., making heat traces fade), (4) heat trace prevention (i.e., using methods that do not leave heat traces), (5) environment manipulation (i.e., designing an environment that makes thermal attacks difficult) or (6) thermal image feed manipulation (i.e., modifying thermal cameras). The design space further considers *who* is responsible for using or deploying the mechanism, the *effort* and *resources* required by users, *verifiability* and *universality* (i.e. whether a strategy only works for specific devices or generally protects users).

Finally, we conclude with actionable protection guidelines specifically for each actor: the device manufacturer, the users, but also the thermal camera manufacturer.

Research Contributions:

1. **Literature Review & User Investigation:** We present the first study ($N = 306$) that investigates protection strategies in the scientific literature from the users' point of view, showing which strategies users perceive as effective and which properties of a strategy impact whether users are willing to use it.
2. **User-Centred Design Space:** We present the first design space for protection against thermal attacks based on the scientific literature. Our design space is user-centred to specifically focus on the victims of the attacks and also consider their degree of involvement in protection.
3. **Actionable Solutions:** Based on our investigation, we present actionable solutions for device manufacturers, users, and camera manufacturers that help to defend individuals from the emerging threat of thermal attacks.

2 Background and Related Work

Our work is driven by prior work in thermal attack protection strategies and investigated thermal attack parameters.

2.1 Investigated Protection Strategies

Researchers proposed different ways to mitigate thermal attacks. Some introduced touchless interaction via gaze [4, 19, 29, 30, 50], gestures [12, 25], biometrics [12, 13, 26] or multi-modal interactions [7, 29–31, 34]. Other research investigated heat trace manipulation techniques, such as masking, using additional heat traces [1], obfuscation [3, 27], distortion [35], or using different input device materials [27].

Alternative Input: Gaze, Gestures & Biometrics. Some input techniques are resistant to thermal attacks by design, as they do not leave any heat traces. Examples include hands-free

authentication using gaze [19, 29, 30, 50]. Mid-air gestures are another form of touchless interaction that leaves no heat traces. Several studies investigated mid-air gestures for knowledge-based and for biometric authentication [6, 12, 13, 25, 26]. While thermal attacks were not specifically addressed by the aforementioned research, others explicitly motivate their work by citing resistance to thermal attacks, such as gaze dwelling and mid-air gestures with shuffled interface layouts [4].

Alternative Input: Multimodal Interaction. Multimodal interaction refers to combining multiple input modalities. This complicates thermal attacks by splitting the attacker's attention into multiple input channels. For example, in a multimodal authentication scheme that requires gaze and touch (cf. [29]), a thermal image alone is not sufficient to reconstruct credentials as it only captures the touch interactions. Kumar *et al.* [34] presented a multimodal method for entering PINs by gaze and touch via a virtual keypad on a touch display. The users initiated input by touching any location, then used eye gaze to select the keys bearing the PINs, before terminating input by lifting their finger off the display.

Manipulating Heat Traces. Other work has investigated specific strategies to manipulate heat traces. It has been shown that touching or rubbing the interface with the hand palm after interacting completely distorts interaction-based heat traces [1, 36, 52]. Next, having a non-conductive material between the interface and the user's hand, e.g., gloves [27], has also been shown to be effective against thermal attacks by reducing heat traces. Reducing heat traces by blowing can work, yet was shown to be unreliable [35, 36]. Finally, another option for manipulating heat traces is shuffling the placing of the keys on a touchscreen, e.g., by randomly changing the layout of a keypad. Investigations show that this effective against thermal attacks [33, 37, 45].

2.2 Thermal Attack Parameters

This section presents how thermal attacks were studied in the literature and what impacts the success of thermal attacks.

Thermal Camera & Capture Timing. Thermal camera sensitivity (TS) is an essential aspect of thermal attacks. Prior work investigated the variance in efficacy between different high-end and off-the-shelf cameras with different TS values on attack success. For instance, Mowery *et al.* [41] used an A320 FLIR camera with $TS < 0.05^\circ$, finding that PINs entered on an ATM were still visible 90 seconds after entry. Similarly, Optris PI 450 cameras which $TS = 0.04^\circ$ were used to demonstrate thermal attacks [1, 10] showing heat traces were visible for up to 60 seconds and that PINs and keyboard passwords could be identified within 30 seconds with a success rate of 72% to 100%, depending on input characteristics, e.g., duplicates [1, 10]. Similarly, FLIR Systems SC620 cameras with $TS = 0.04^\circ$ were used to show that pressed keys can be revealed up to 60 seconds after interaction [27]. The aforementioned

Strategy	Description	Source
Biometrics	Biometrics are used to authenticate because they do not leave heat traces	[14, 20, 40]
Blowing	Users blow on the interface to cool down left heat traces	[35, 36]
Feed Filtering	The feed of the thermal camera is manipulated to obfuscate input interfaces, e.g., keyboard	[9, 10, 38]
Input Modality	The input modality is changed to a touchless alternative, such as gaze, or a computer mouse	[1, 15, 16, 21, 28, 30, 31, 34]
Heated Element	A heated element behind or below the interface obfuscates user input	[1]
Gloves	Gloves serve as non-conductive barrier between the user's finger and the interface such that no heat traces are left	[27]
Graphical Cues	The authentication is based on graphical cues, e.g., credentials consist of a series of images where users have to choose from	[2, 28, 32]
Improve Credentials	Credentials (e.g., passwords) are made more complex to complicate thermal attacks by overlapping characters or longer input	[1, 2, 10]
Materials	Materials with low thermal conductivity are used for interfaces, such that heat traces decay faster	[10, 27, 41, 45, 52]
Multimodal/Multi-factor Auth	Additional (non-touch-based) input modalities or factors are used such that the thermal image is not sufficient for successful attacks	[29-31]
PEKs	A privacy enhancing keyboard that shuffles the layout of the input keys is used, e.g., scrambling digits of a PIN	[4, 33, 37, 45]
Physical Cover	A physical element covers the interface until heat traces decayed	[52]
Priming Hands	Users touch something cold before interaction to leave fewer heat traces that decay faster	[3]
Resting Fingers	Users cover the interface with their hand after interaction to leave additional heat traces	[1, 36, 52]
Thimblettes	Rubber thimblettes serve as non-conductive barrier between the user's finger and the interface such that no heat traces are left	[27]

Table 1: An overview of the 15 different protection strategies from the literature.

studies used high-end cameras (~5000\$). However, affordable off-the-shelf cameras are also effective for thermal attacks, such as ~400\$ FLIR C2 cameras with $TS=0.07^\circ$ [2, 3].

Device & Material of Attacked Device. Further critical aspects of attack success are the attacked device and the interface material, as these play an integral role in heat transfer. Early research demonstrated the success of thermal attacks on ATMs via visual inspection of thermal images with the naked eye to determine the credentials [41]. The feasibility was also shown for PINs on touch-based smartphones [1] and passwords depending on the keyboard [27]; Acrylonitrile Butadiene Styrene (ABS) keycaps are less vulnerable to thermal attacks than Polybutylene Terephthalate (PBT) keycaps *et al.* [10]. Abdrabou *et al.* [2] found that thermal attacks against graphical passwords were more successful on a gorilla glass touchscreen than a laptop's touchpad. In follow-up work, they found laptop keyboards were more vulnerable to thermal attacks on text passwords than gorilla glass [3].

Input Length & Characteristics. Several studies investigated and compared input characteristics and their effect on the success of thermal attacks. Overlapping input reduces the thermal attack success against Android patterns from 100% to 16.67% [1]. Comparisons of touch gestures and touch taps for entering cued recall graphical passwords show that touch taps are more challenging to reveal (23.61%) [2]. The longer the input, the harder the attack (36%), as the heat traces fade during the time taken to finish entering the input. This factor could be particularly impactful when choosing passwords [3, 10]. Finally, how many traces were left on the surface as a result of hand temperature of the user's way of typing impact attack success. Most successful attacks featured a substantial difference between the temperatures of the users' hands and the device; the hand temperature impacts the success of thermal attacks [3]. Further, hunt-and-peck typists are more vulnerable than fast typists (92% vs 83%) [10].

In sum, related work has investigated different input techniques and multimodal interactions, as alternatives to touch-based interactions, to resist thermal attacks. These alternatives, however, require additional hardware and introduce new in-

terfaces. In this paper, we present a holistic investigation of different kinds of protection strategies that can also be used to protect existing interfaces, such as PIN keypads or keyboards.

3 Strategies for Thermal Attack Protection

To answer **RQ₁** (*What are protection strategies against thermal attacks?*), we conducted a literature review to identify research that investigated thermal attacks in the context of interfaces. We conducted a literature search as follows:

1) *Keywords and Search Space:* We iteratively developed the keywords with two expert researchers with extensive research experience in thermal attacks. During the development of the keywords, the experts considered alternative connotations present in the literature. The final search query was: (*thermal AND attack**) OR (*thermal AND (imaging OR camera-based OR residue-based OR transfer) AND attack**) OR (*thermal AND sequence AND analysis*). As for the search space, we used the top 10 publication venues in "Human Computer Interaction" and the top 10 in "Computers Security & Cryptography" according to Google Scholar's ranking system (date accessed: April 06, 2022). We set the time frame for publication to 2011 and onward because the earliest work about thermal attacks from Mowery *et al.* [41] is from 2011.

2) *Exclusion Criteria:* A paper was excluded if the keyword did not appear in the paper's full text. Further, papers that did not include a protection mechanism that targets thermal attacks were excluded (e.g., papers that discuss thermal attacks only as related work). In this step, we identified five relevant publications [1, 24, 32, 35, 42].

3) *Forward and Backward Search:* Each paper identified in Step 2 was processed in two cycles of forward and backward searches to identify relevant literature outside the search space. Again, research published before 2011 was not considered. We excluded bachelor, master and PhD theses, white papers and papers not written in English. We further excluded papers based on the criteria in Step 2 and papers that mention a thermal attack in the context of data centres (over-heating attack) or chemical structures. In the backward search, we identified

10 relevant papers, eight of them duplicates, resulting in two new papers. In the forward search, we identified 31 relevant papers, 10 of them duplicates, resulting in 22 new relevant papers. In total 24 additional papers were identified in this step [2–11, 15, 16, 21, 27, 28, 30, 31, 33, 34, 36, 37, 41, 45, 52], bringing the total to 29 papers.

4) *Extraction of Strategies*: Two researchers jointly extracted 15 protection strategies from the resulting list of 29 papers. Table 1 provides descriptions of the strategies.

4 Methodology

To investigate the users' perspective, we conducted an online survey with 306 participants. In this study, we specifically investigated **RQ₂** (*What are the user perceptions towards protection strategies against thermal attacks in public payment scenarios?*), which we split into the following sub-questions:

RQ_{2.1} – How do users wish to be protected against thermal attacks on public payment terminals?

RQ_{2.2} – What are the properties of protection strategies considered by users when evaluating strategies?

Study Procedure & Pre-Studies. First, the participants were informed about the study and what will be asked of them. Then we informed them they could abort the study at any time, about handling of data, and their rights as participants. To proceed, participants had to express consent. We then introduced the concept of thermal attacks, including two informational videos¹. The first showed a person entering their PIN at an ATM, then leaving, before a second person uses a handheld thermal camera to observe four heat traces and infer the PIN code. The second showed a similar scene happening with a mobile phone. Both show typical threat models from prior work and do not suggest any mitigation. Participants were asked three multiple-choice questions about thermal attacks. They could go back and forth multiple times to check their understanding of thermal attacks but were not shown if their answers were correct. These multiple-choice questions were part of our attention checks.

Next, participants were asked how they would intuitively protect themselves from thermal attacks. Following this they were asked who, in their understanding, is responsible for protecting users from thermal attacks. Then, 14 protection strategies were described to the participants (see Table 7 in Appendix A)² identified in the literature search (see Table 1). We asked whether they intended to use each strategy and if they trusted it would protect them. To minimise bias, these strategies were presented in a random order and neutral manner; each strategy works was described and included an example based on the interaction with an ATM scenario, as this

is a security-focused and commonly known interface which is also vulnerable to attacks [41]. Strategies that apply to ATMs can also apply to other public payment terminals featuring keypads, such as ticket machines, automated kiosks and self-service checkouts. The section concluded by letting the participants rank the strategies based on their personal preferences. All questions in this section had an optional free-text field where participants were asked to explain their answers. The free-text field for the final ranking was mandatory. Finally, the participants provided demographics, were thanked for their participation and were redirected to their reimbursement platform.

We iteratively developed our questionnaire which was first tested in a pre-study with five experts. Based on the pre-study, the order and wording of the questions were improved. Second, we conducted a second pre-study with 44 participants to determine the study duration and further improve the wording of our questions and the instructions. In this run, participants' free-text responses were too limited, so the number of these questions was reduced. For the final questionnaire, the reader is referred to Appendix A. The questionnaire had two attention check items to ensure validity of the data. Ethical approval was granted by the institution for this study.

Recruitment & Participants. We recruited 348 participants through the online recruitment platform Prolific, targeting a minimum sample of >100 as per the central limit theorem, then recruiting beyond as resources allowed. We reimbursed them with an hourly rate of £8.89p, using the Prolific cost calculator based on pre-study completion time³ (completion time exceeded pre-study indications, leading to a slight rate adjustment). From 348 participants, 42 were excluded from the results based on failed attention checks. The remaining 306 participants had a mean age of 27.62 ($max = 72, min = 18, SD = 9.23$). 50.6% described themselves as male, 47.7% as female, four (1.31%) preferred to self-describe and one preferred not to say. Participants were recruited with no geographic restriction from 24 countries. Forty-five were from South Africa, 37 from Mexico, 209 from Europe (most prominently Poland (N=67), Portugal (60), South Africa (45), Mexico (37) and Italy (22)), and 15 from 5 other countries. Participants' technical proficiency was assessed with the Affinity for Technology (ATI) scale [22], resulting in a mean score of 4.00 ($SD = 0.61, \alpha = 0.64$).

Data Analysis. We analysed the study results in the following ways. For the *quantitative data*, we applied statistical testing when the data met assumptions for the respective statistical method (see Section 5.1). To understand the reasons why participants may feel certain strategies were usable or trustworthy, the *qualitative results*, i.e. open-ended answers, were processed in two ways. First, to analyse how participants intuitively protect against thermal attacks, we followed a semi-open coding approach with the protection strategies

¹Links to videos: 1. <https://rb.gy/ixyxt> 2. <https://rb.gy/kbcli>

²We excluded feed filtering after the pre-study due to feedback from participants, because this does not impact users.

³Prolific Cost Calculator www.prolific.co/researchers#pricing 15/05/23

described in Table 1 as initial codebook (see Table 5 in Appendix B). Since the participants added strategies different from those in the literature, one coder first familiarised with all statements to propose codes for new strategies. This was discussed with a second researcher. Next, the first researcher applied the codebook to all statements. This coding was then reviewed by the second researcher and disagreements were resolved in a review meeting.

For the remaining open-ended answers, we applied thematic analysis by Braun and Clarke [17, 18]. First, we conducted open-coding, assigning codes to meaningful and pertinent concepts. Due to the scale of the data set (4824 responses), an initial codebook was generated by two researchers independently over an identical 15.5% subset of the data. Both researchers conferred and established a synthesised codebook between them, normalising the names of semantically similar codes. This codebook, comprised of 15 codes (see Table 6 in Appendix B) which encompassed the factors that shaped participant preference and trust for protection strategies, was then used to code the remainder of the data set, with no major additions or alterations required. As before, the first researcher applied the codebook to all statements, which was then verified by the second researcher, and disagreements were resolved. After this, both researchers grouped the codes into five main themes.

Limitations. Our study aimed to understand user perspectives on a set of protection strategies; how much users would trust them to protect from thermal attacks and how willing they would be to use them. This approach came with natural limitations. First, surveys result in self-reported data, which may be subject to biases and incorrect self-assessments. In particular, in the context of our survey, which presented thermal attacks as a potential security threat, participants may have felt more obliged to display willingness to consider and use strategies than they would in real-world settings, and may have exaggerated the value they placed on security and trustworthiness. Ratings and responses regarding these strategies should be considered with this context in mind.

Second, some participants gave feedback on strategies with which they did not have personal experience, relying instead on the descriptions and figures presented in the survey, while some others may have had first-hand experience. Thus, ratings for trust and usability should be taken in the context that some participants may have misunderstood strategies they had not experienced, or would have rated them differently if they did have that personal experience. It was, however, valuable to capture lay-users' impressions of strategies with which they may not be familiar, as it allows better understanding of the negative perceptions or misconceptions about a strategy that could prove an obstacle to its adoption, or *vice versa*.

Finally, the average age and distribution of our sample was a limitation. While we had a wide overall age range, between 18 and 72, the mean age and standard deviation suggest the majority of the data set skews below 40 years old. This is

relevant, as ATMs, the thermal attack scenario presented in this paper, are a legacy technology commonly used across all adult ages. Particularly in regard to strategies which propose new ATM technologies or interactions, a more representative sample may reveal a different distribution of feedback and ratings reflective of the older age groups' priorities, and the results of this work should be understood with this in mind.

5 Results

5.1 RQ_{2.1} – Protection from Thermal Attacks

This section reports the quantitative results regarding responsibility, preferred strategies and usage intention, and how participants intuitively protect from thermal attacks.

Responsibility: We asked participants who was responsible for protecting users from thermal attacks using a multiple-choice item of options taken from the pre-study. Most participants felt the responsibility lay with users (47.4%) or interface manufacturers (40.2%), while far fewer felt thermal camera manufacturers were responsible (3.6%) or 8.8% suggested alternative answers (the user and manufacturer jointly (5.8%), all actors (1.6%), no-one (0.6%) and law-makers (0.3%)).

After a one-way chi-squared test of independence confirmed a significant difference in distribution, six *post hoc* pairwise chi-squared tests were conducted, confirming that significantly more respondents felt users or interface manufacturers were responsible for mitigating thermal attacks than thermal camera manufacturers or others (see Table 2). This may indicate users are divided on whether they wish for mitigation strategies they can action, or for interfaces to automatically protect them. Interestingly, despite thermal cameras being a single point of failure that enables thermal attacks, more users felt that vulnerable interfaces should be changed, perhaps viewing the cameras as immutable.

Intuitive Strategies: Before presenting participants with strategies from the literature, we asked how they would intuitively protect themselves. Their suggestions are shown in Table 3. Most prominently participants described thermal masking equivalent to the resting fingers strategy: “*before leaving ATM, I could press random keys that are not in my password so heat trace would show them as well*” (P99). Several suggested heat trace prevention strategies using gloves, or other protection objects, such as a “*piece of paper*” (P191), “*some sort of stick or pen*” (P63), or “*stylus*” (P212). Using multi-factor authentication was suggested by 11 participants (3.9%). Some proposed strategies are known also from shoulder-surfing literature. In particular, 24 participants proposed making sure that no-one suspicious uses the ATM after them and paying close attention to the user's surroundings, while 82 suggested waiting until the heat traces disappear, with responses ranging from “*20 seconds more*” (P184) to “*2 minutes before leaving*” (P193) (prior work has found thermal attacks can be effective

Who did respondents (N=306) consider responsible for mitigating thermal attacks?			
Users	Interface Manufacturers	Camera Manufacturers	Others
145 - 47.4%	123 - 40.2%	11 - 3.6%	27 - 8.8%
Was this distribution of responses significant? - Chi-squared test of independence			
Factor	χ^2	df	p
Responsibility Distributions	295.69	3	<.0001
Post hoc significant contrasts in responsibility - 6 Chi-squared tests - Bonferroni corrected $\alpha = 0.0083$			
Contrast	χ^2	df	p
User - Interface Manufacturer	1.806	1	0.179
User - Camera Manufacturer	115.1	1	<.0001
User - Other	80.95	1	<.0001
Interface Manufacturer - Camera Manufacturer	93.61	1	<.0001
Interface Manufacturer - Other	61.44	1	<.0001
Camera Manufacturer - Other	6.737	1	0.009

Table 2: Summary and significance statistics of respondents’ perception of who is responsible for mitigating thermal attacks.

Intuitive Suggestions	N	Intuitive Suggestions	N
Thermal Masking	137 44.8%	Observe Surroundings	24 7.8%
Waiting	82 27.0%	Alternate Authentication	11 3.6%
Gloves	56 18.3%	Cooling Element	7 2.3%
Non-Suitable Strategy	43 14.0%	Update Credentials	5 1.5%
Clean the Interface	35 11.4%	Use Secure Facility	4 1.3%
Protection Object	33 10.8%	Other	8 2.6%

Table 3: Prevalence of intuitive strategy suggestions.

for up to 60 or 90 seconds [1, 41]). Some strategy suggestions would not effectively protect against thermal attacks, most prominent of which was cleaning the screen, sometimes with alcohol or wet wipes (N=35). These strategies, however, work against smudge attacks. Eight suggestions were made by three or less participants: automated surveillance by ATMs, avoiding ATM use, or keeping less money in the account. Ten participants made no suggestion.

Strategy Ranking: Participants were asked to rank the 14 strategies “in order of personal preference”. The distribution of these rankings, their median rank and interquartile ranges can be seen on Fig. 1, while motivations for preferences (as well as their intended usage and trust) are further explored in the thematic analysis. Two verifiable software solutions, PEKs and multi-factor authentication, shared the highest median ranking of 4. Integrated hardware solutions, such as biometrics, heated elements, materials or physical covers, ranked lower with median rankings between 6 and 7. Similarly, user-centered strategies like resting fingers and improving one’s credentials ranked a median 6th and 7th respectively. Input modality also ranked a median 7th. While gloves and thimblettes both had a median rank of 9, suggesting a dislike of strategies which required users to bring protection objects. Two strategies shared a median rank of 10, graphical cues and priming hands. Finally blowing on the interface was the lowest ranked strategy, with a median of 13, a strategy which has shown showing a low efficacy in prior work [35, 36], and which participants took many issues with (see Sec. 5.2.4).

A Kruskal Wallis test found a significant difference in ranking between mitigation strategies ($\chi^2 = 736.9$, $df = 13$, $p < 0.0001$) and a *post hoc* Dunn test with Bonferroni correction was used to find significant contrasts between strategy

pairs, which are shown in full on Fig. 1. Both PEKs and multi-factor authentication were ranked significantly higher than most strategies, while graphical cues, blowing and priming hands were ranked significantly lower. Data inspection suggested that participant ratings for usage and trust were correlated with strategy ranking, confirmed by a pair of Pearson’s product-moment correlation tests which found that ratings for both strategy usage ($cor = 0.580$, $df = 4282$, $p < 0.0001$) and trust ($cor = 0.486$, $df = 4282$, $p < 0.0001$).

Trust Perceptions: To investigate the participants’ trust perceptions, we let them rate the statement “I am confident that my credentials are protected from a thermal attack by this strategy” for each strategy on a 5-point Likert scale of *Strongly Disagree* to *Strongly Agree*. 52% or more of participants agreed or strongly agreed to trust 10 of 14 strategies (see Fig. 2 for distribution of responses to all strategies).

One might expect fully verifiable strategies to be more trusted than partially or unverifiable methods. This bore out as four of the top six trusted strategies were fully verifiable: PEK (91% of participants agreed/strongly agreed they trusted this strategy), multi-factor authentication (79%), physical covers (63%) and biometric (63%). Of the other two, resting fingers (68%) was partially verifiable and heated element was not verifiable (63%). Of the strategies trusted by less than 50% of participants, three were partially verifiable (blowing, priming hands, improving credentials) and one was fully verifiable (gloves). Similarly to participants views on responsibility, there was no clear pattern for if manufacturer or user-enacted strategies were more trusted - they varied case-by-case.

A Kruskal Wallis test found a significant difference in trust between strategies ($\chi^2 = 15.1$, $df = 13$, $p < 0.0001$). A *post hoc* Dunn test with Bonferroni correction then identified significant contrasts between strategy pairs (see Fig. 2). PEK was significantly more trusted than all others, while multi-factor authentication was more trusted than all strategies except PEK and resting fingers. Blowing and priming hands were significantly less trusted than all other strategies, except each other. Two strategies significant contrasted with strategies outside of these four: gloves, which was significantly less trusted than five more strategies (biometric, heated element,

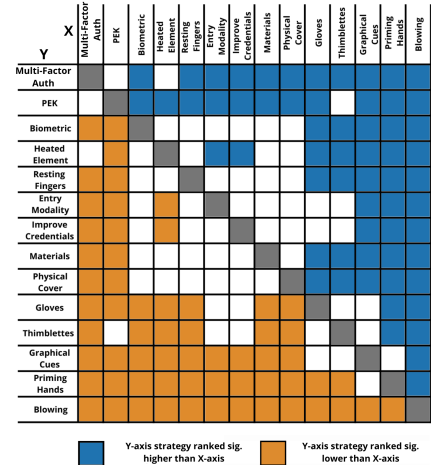
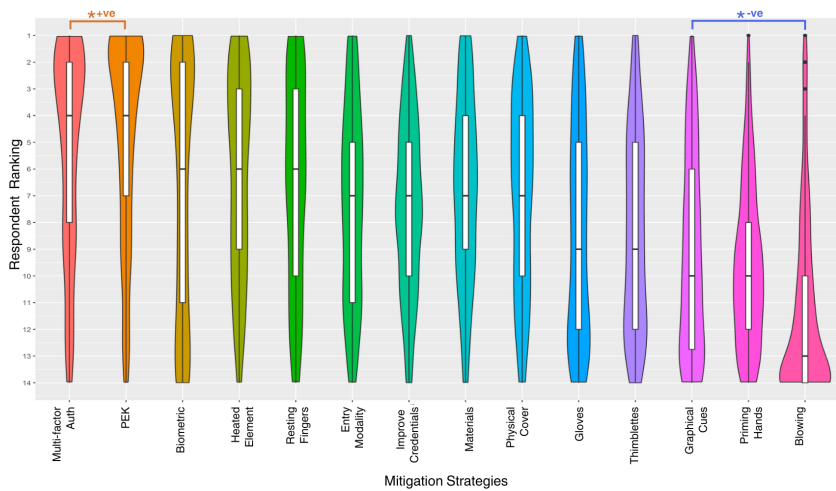


Figure 1: Left: Distribution of participant mitigation strategy rankings from 1 (Best) to 14 (Worst). The +ve group strategies significantly higher ranked than most others, vice versa for -ve group. Right: Significant contrasts in participant rankings.

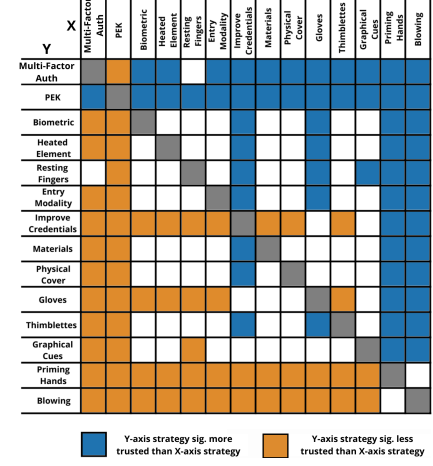
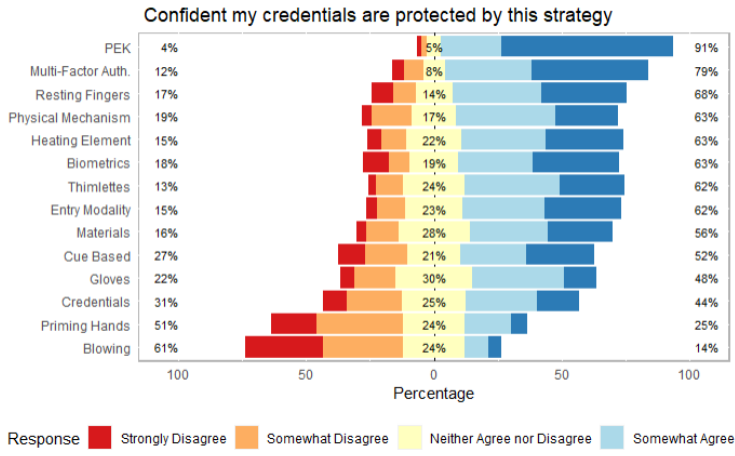


Figure 2: Left: Participant Likert scale responses when asked if they would trust each strategy, ordered from most to least preferred. Right: Significant contrasts in participant trust between thermal attack mitigation strategies.

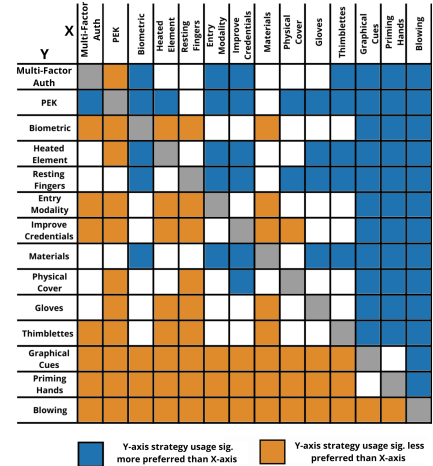
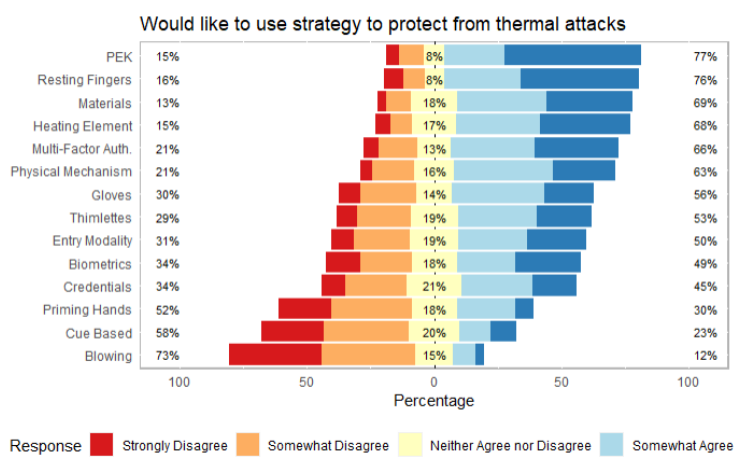


Figure 3: Left: Participant Likert scale responses when asked if they would use each strategy, ordered from most to least preferred. Right: Significant contrasts in preferred usage between thermal attack mitigation strategies.

resting fingers, input modality and thimblettes), and improve credentials, which was less trusted than those five strategies and two more (materials and physical cover).

Usage Intention: To investigate participant's willingness to use different strategies, we let them rate the statement "*I would like to use the described strategy to protect myself from thermal attacks*" on the same 5-point Likert scale. 50% or more of participants agreed or strongly agreed that they would like to use 10 out of the 14 strategies (see Fig. 3 for distribution of responses to all strategies).

Usage intention seemed partially informed by how much effort users would to use a strategy as three of the four strategies that most participants agreed they would use required no extra interactions from user: the PEK (77% agreed or strongly agreed they would like to use it), conductive materials (69%) and heating element (68%) and all of these required no user resources (see Table 4). This was not a universal trend, however, as resting fingers, despite requiring user interaction, was rated second highest for usage preference (76%). Also less preferred than these other strategies, a slight majority of participants did report they would like to use two strategies that require users to bring protection objects, gloves (56%) and thimblettes (53%). The strategies rated lowest for usage preference both required extra interaction from the user: priming hands (30%) and blowing on the interface (12%).

A Kruskal Wallis test revealed a significant difference in usage intention ratings between mitigation strategies ($\chi^2 = 760.0, df = 13, p < 0.0001$). Following this finding, a *post hoc* Dunn test with Bonferroni correction was conducted to identify the significant contrasts between strategies responsible for this difference (see Fig. 3 for a matrix showing every significant contrast). The most consistent contrasts were between three strategies rated least usable (blowing, graphical cues and priming hands), and the other twelve strategies with which they all contrasted negatively. PEK also positively contrasted with all but two strategies, resting fingers and conductive materials, and negatively contrasted with none.

Differences in Trust and Usage Intention: Some strategies which were noticeably rated as less or more usable than they were trustworthy. Examples include conductive materials, which 69% of participants said they would use, but 56% were confident it would actually protect them, or multi-factor authentication, which was the second most trusted strategy by participants (79%), but fifth most usable strategy (66%). Most notably, while 52% trusted graphical cues to protect them, only 23% were happy to use them.

5.2 RQ_{2.2} – Properties of Mitigation

In this section, we provide the results of the thematic analysis to gain a deeper insight on what properties of strategies participants consider to be important. Throughout the qualitative results, we provide numbers to give the reader an impression on how often a topic was mentioned.

5.2.1 Theme 1: Clear verification of efficacy is essential

When explaining their trust evaluation, participants particularly considered uncertainty, and the efficacy of protection.

Uncertainty: Several participants mentioned uncertainty regarding efficacy during trust evaluation among all kinds of strategies. Participants were conscious of methods that they felt were or were not verifiable and user perception of verifiability impacted trust perception. Thus, a lack of clarity on verifiability could obstruct use of otherwise viable strategies.

Mostly in connection with partially verifiable strategies, such as blowing (57.1%), materials (43.8%), heated elements (28.1%), physical covers (27.6%), and resting fingers (24.5%), participants stated they did not trust they would be protected due to uncertainty about effectiveness. For example, regarding blowing P59 wrote: "*I'm not sure that blowing on the keypad would make enough heat to disguise the keys which had been touched*", while P10 worried that the physical cover strategy would have adverse effects that worsened its efficacy, writing: "*I feel like if you cover the keypads, the amount of time that it takes to dissipate the heat would increase*". In these cases the inability for users to confirm if the strategy has been successful can lead to doubt, worry and a lack of trust.

Additionally, it is possible that fully verifiable strategies, which are effective by design, are not necessarily perceived as such. Several participants (27.2%) identified that gloves can be partially verifiable based on thickness and were unsure of the efficacy of gloves, citing concerns that they might be "*too thin*" (P129) to be effective and and uncertainty about "*how much heat the gloves leave behind*" (P41).

Only few participants mentioned uncertainty in the context of fully verifiable strategies, such as PEKs (3.5%), and 9% multi-factor authentication (9%). P249 expressed concerned uncertainty about how PEKs work: "*It won't work if the attackers have already learned the sequence*".

Efficacy: Most participants felt that verifiable strategies, namely PEKs and multi-factor authentication, were provably effective or understood they were effective by design. This was particularly true if they had prior experience with them in other contexts, for example P93 wrote, regarding multi-factor authentication, that it was "*a great idea, as I mentioned in the beginning, used widely in my country with great success*".

5.2.2 Theme 2: Strategies not requiring extra interactions or resources are preferred

When explaining their usage intention, participants considered the following attack properties:

Automatic Protection: Participants praised strategies with automatic protection. When discussing heating elements, P73 wrote: "*It doesn't require any work from me, which is great*" and P75 stated that "*It's better if the manufacturers help the users when their data is in peril*", while P250 described the

physical cover as “*a reliable solution provided to me by the manufacturer*”. This contrasts the results from the first theme as some manufacturer-based strategies are not verifiable.

Ease-of-Use: Of course, a protection strategy should also be easy-to-use, which is why the resting fingers strategy formed an exception to the trend of automatic protection. Participants valued that it was “*simple to implement*” (P114), and felt it was convenient and practical, with P153 commenting “*It’s quicker, doesn’t need any materials, and I’m pretty sure it can actually confuse the heat traces*”.

Some strategies were rated as noticeably less or more usable than trustworthy. Despite being trusted by the majority of participants, graphical cues were overall ranked 12th among strategies. The new interaction was seen as complex, with P115 commenting “*the strategy is effective, but it replaces the action of entering the PIN code with a more complex one, so I personally would not adopt it*” and others worrying about forgetting their details: “*I just wouldn’t be able to remember these*” (P75). Others simply felt the interaction would be “*tiresome*” (P24), “*annoying*” (P73) and worried about accessibility: “*I think it’s too complex and it will put a strain on people with vision problems*” (P206). Overall, participant responses to graphical cues demonstrate how severe usability concerns can undermine a majoritively trusted strategy.

Effortlessness: Participants had a variety of problems with methods requiring user effort in terms of actions or resources. Some simply disliked the extra effort required: “*I am not sure - it is a lot of work to me. I am too lazy for that*” (P162, on thimblettes). Others questioned the effort related to availability. For example, when discussing the priming hands strategy P18 wrote: “*Could work but it would require the person to carry around something cold, or have the luck of having something cold close-by*”. The new actions required to facilitate strategies could also spark concern, with P21 stating that blowing was “*strange and unsanitary*”. Opinions were split on thimblettes, with some participants describing them as convenient: “*it’s more portable and easy to equip*” (P14), while P135 felt they were “*easy to carry and store inside our purses or pockets*”. Others described them as inconvenient, with P77 stating that “*carrying around such a specific item would be cumbersome*”. By contrast, few participants (4.59%) described gloves as convenient, while inconvenience was mentioned more frequently (27.5%), citing similar complaints.

5.2.3 Theme 3: Trust is a dominant factor

There is an indication that trust above all else determines whether participants want to use a strategy meaning that high trust can overcome issues with effort or ease-of-use.

While usability and practicality concerns can undermine effective strategies in the eyes of users, results suggest that a high level of trust can overcome these concerns. The PEK and multi-factor authentication were the two most trusted strategies, with 91% and 79% of participants agreeing or

strongly agreeing that they were confident they protected them, respectively (see Fig. 2). Additionally, participants also majoritively reported they would like to use these strategies, 77% for the PEK and 66% for multi-factor authentication.

Despite these positive quantitative results, qualitative analysis revealed a large proportion of participants had concerns about the inconvenience and impracticality of PEKs and multi-factor authentication. Participants cited that the PEK would prevent familiar ATM usage (“*Seems extremely effective, but my PIN is partially in my muscle memory*” - P103) and that need for “*extra layer of steps*” (P103) and a smartphone during multi-factor authentication could be “*annoying*” (P151) or “*not that convenient if you forget your device*” (P205).

The PEKs and multi-factor authentication were, however, still the joint-highest ranked strategies, despite these prevalent usability concerns. They were also the most often described as effective or trusted among all 14 options, cited as such in over 75% of participant written responses. This suggests that, when the level of participant trust in a strategy is high enough, it becomes the dominant factor in their willingness to use it and their preference for it. This is well illustrated by P99’s comments about the PEK: “*I could easily be mistaken and enter my PIN number incorrectly. But I think that idea is the best and [it] would be almost impossible for thief to know my PIN number*”, and by P240 regarding multi-factor authentication: “*I use something like this already. It’s annoying to have to confirm my identity every time but definitely is a good way to protect you from further withdrawals*”.

5.2.4 Theme 4: No new attack vectors

Participants considered security aspects, e.g., privacy, ask for holistic defence. Further, participants did not only consider digital threats but also threats to their health.

Holistic: Few participants considered other threats, e.g., smudge attacks, when evaluating trust. For instance, P137 wrote regarding the thimblettes strategy that “*I think it would still leave some kind of marks when pressing a certain combination of buttons*”, regarding the physical cover P120 wrote: “*won’t stop remote camera attacks*” and P53 wrote, regarding resting fingers: “*I think its still dangerous, because still your fingerprint its still there even if you put the extra heat, I am really not sure about using [this] one*”. This indicates that users may want a holistic defence that works also for smudge attacks and real-time observation. Many intuitive strategies also considered this, specifying attending to one’s surroundings before authenticating.

Privacy: Many participants expressed privacy concerns despite the efficacy of biometrics, such as P189: “*Although you might be protected from thermal attacks, it’s a bit scary imagining ATMs and therefore banks having so much of your biometric information and not knowing what they will do with it. Especially since we know corporations have been known*

to sell their customers data”. Others, like P159, worried that if biometrics could be used to access bank accounts, it would lead to dangerous situations: “I just hope nobody chops off my finger or removes my eye to scan with.”

Hygiene: A smaller theme that emerged was concern about strategies that participants felt were unsafe due to being unhygienic. In particular, blowing was considered inappropriate, especially in the context of the COVID 19 pandemic. P43 raised their concerns, writing “COVID is still not gone, and there’s plenty of other illnesses that could be transmitted this way.”, and P128 wrote: “although it seems easy I don’t feel that it’s a very ‘clean’ method because it leaves other’s people’s virus, for example, much easier in the keypad. Does not feel very hygienic.” Similar concerns were shared about other strategies that required sharing an interface, such as priming hands, a trait also shared by normal ATMs.

5.2.5 Theme 5: Protection should be integral

Participants also considered the universality, viability, and accessibility when evaluating the strategies.

Universality: We found participants were mindful of the restricted use cases for some strategies, versus others which were universally applicable, as shown in Table 4. Participants expressed concern that restricted strategies were specific to ATMs. P78 felt that while a physical cover “might be perfect for an ATM. I am not so sure about a mobile phone” and P150 expressed a similar concern about heating elements: “I don’t know how that would apply to phones”.

Viability: There was also concern that strategies that would require system-wide change of ATMs or infrastructure, such as priming hands, materials, physical cover or input modality, would be too costly or unreliable for manufacturers to implement, even if they were effective. P172 highlighted cost concerns, writing that changing ATM materials “would mean rebuilding the ATM machines almost from scratch, it could be really effective but also really expensive”, while P69 worried about the reliability of implementing the input modality strategy: “I think this solution would end up being really over-engineered and the ATM wouldn’t work half of the time”. Overall, while this concern was not raised by the majority of participants, we found some users were very aware of the restrictive nature of non-universal strategies and raised valid questions about the practicality of methods which require the overhauling of society-wide systems.







Accessibility: Strategies that feature new technologies, such as biometrics, or learning an interaction paradigm, like PEKs or graphical cues, prompted concerns about accessibility for disabled or elderly people. Regarding graphical cues, P41 wrote: “This is way too complex even for me, let alone the millions of elderly people who use ATMs every day” and, when discussing PEKs, P59 wrote: “This is all well and good for people who have good vision, but for partially sighted or

those with dyslexia or other letter recognition issues, it may prove problematic”. No participant specifically mentioned their own status as elderly or disabled when commenting on accessibility, meaning some concerns about others’ ability to use certain systems may be assumptions, but it highlights users scrutinising strategies they perceive to be inaccessible.




6 User-Centred Design Space

This section proposes a user-centred design space for protection against thermal attacks on public payment terminals informed by our literature review and the user study. We used the list of the protection strategies and the descriptions from the study as input. Two researchers familiarised themselves with the data, proposed the dimensions of the design space, and developed a codebook that was finalised in a review meeting. Next, they independently applied the codebook, compared their coding and agreed on final code allocations. The inter-rater reliability was 0.92, referring to almost perfect agreement. The final allocation was verified by a third researcher. Based on the results, we identified six design space main dimensions (see Table 4 for an overview on how the protection strategies are located within the design space).

Dimension 1 – Protection Strategy: This dimension describes the protection strategy referring to *how* the users are protected from thermal attacks.

- 1)  **Thermal Masking:** Additional heat traces obfuscate the original input.
- 2)  **Heat Trace Manipulation:** Heat traces are modified to obfuscate the input without leaving additional traces.
- 3)  **Heat Trace Reduction:** Left heat traces are reduced.
- 4)  **Heat Trace Prevention:** Characteristics of the input are changed to make it difficult or impossible to leave heat traces or biometrics.
- 5)  **Environment Manipulation:** The environment is altered to make it difficult or even impossible for attackers to use thermal cameras.
- 6)  **Image Feed Manipulation:** Similar to how printers prevent its users from printing money, manufacturers of thermal cameras could prevent the misuse of thermal cameras by integrating models that detect and obfuscate input interfaces in the thermal camera’s feed.

Dimension 2 – Actor: All protection strategies outline an actor responsible for using or deploying the mechanism:

- 1)  **User:** The user is responsible for protection.
- 2)  **Device Manufacturer:** The protection mechanism can be built into an input device by its manufacturer.
- 3)  **Camera Manufacturer:** The protection mechanism is built into a thermal camera by obfuscating user input on interfaces in the thermal camera feed making it infeasible to use the thermal camera maliciously.

Strategy	Protection Method	Actor	User Effort	User Resources	Verifiability	Universality
<i>Biometrics</i>	🔒 Heat Trace Prevention	👤 Device Manufacturer	👤 Interaction-based	❌ None	✅ Complete	📍 Restricted
<i>Blowing</i>	🔒 Heat Trace Reduction	👤 User	👤 Habit-based	❌ None	⚡ Partial	🌐 Universal
<i>Feed Filtering</i>	📷 Image Feed Manipulation	📷 Camera Manufacturer	👤 None	❌ None	🚫 Not	🌐 Holistic
<i>Input Modality</i>	🔒 Heat Trace Prevention	👤 Device Manufacturer	👤 Interaction-based	📱 Hardware	✅ Complete	📍 Restricted
<i>Heated Elements</i>	🔒 Thermal Masking	👤 Device Manufacturer	👤 None	❌ None	🚫 Not	📍 Restricted
<i>Gloves</i>	🔒 Heat Trace Prevention	👤 User	👤 Habit-based	🔪 Protection object	⚡ Partial	📍 Restricted
<i>Graphical Cues</i>	🔒 Heat Trace Prevention	👤 Device Manufacturer	👤 Interaction-based	❌ None	✅ Complete	📍 Restricted
<i>Improve Credentials</i>	🔒 Heat Trace Manipulation	👤 User	👤 Interaction-based	❌ None	⚡ Partial	🌐 Universal
<i>Materials</i>	🔒 Environment Manipulation	👤 Device Manufacturer	👤 None	❌ None	🚫 Not	📍 Restricted
<i>Multi-Factor Auth</i>	🔒 Heat Trace Prevention	👤 User, 👤 Device Manufacturer	👤 Habit-based	📱 Software, 📱 Hardware	✅ Complete	🌐 Holistic
<i>PEKs</i>	🔒 Heat Trace Manipulation	👤 Device Manufacturer	👤 Interaction-based	❌ None	✅ Complete	📍 Restricted
<i>Physical Cover</i>	🔒 Environment Manipulation	👤 Device Manufacturer	👤 None	❌ None	⚡ Partial	🌐 Universal
<i>Priming Hands</i>	🔒 Heat Trace Prevention	👤 User, 👤 Device Manufacturer	👤 Habit-based	❌ None	⚡ Partial	📍 Restricted
<i>Resting Fingers</i>	🔒 Thermal Masking	👤 User	👤 Habit-based	❌ None	⚡ Partial	🌐 Universal
<i>Thimblettes</i>	🔒 Heat Trace Prevention	👤 User	👤 Habit-based	🔪 Protection object	✅ Complete	📍 Restricted
<i>Observation</i>	🔒 Environment Manipulation	👤 User	👤 Habit-based	❌ None	✅ Complete	🌐 Holistic
<i>Secure Environment</i>	🔒 Environment Manipulation	👤 User	👤 Habit-based	❌ None	⚡ Partial	🌐 Holistic
<i>Waiting</i>	🔒 Heat Trace Reduction	👤 User	👤 Habit-based	❌ None	✅ Complete	🌐 Holistic

Table 4: An overview of the protection strategies and how they manifest each of the six different design space dimensions.

Dimension 3 – User Effort: This dimension outlines the effort needed from the users to employ the protection strategy.

- 1) 🧑🏻 *Habit-based:* Users have to use the protection strategy every time.
- 2) 🧑🏻 *Interaction-based:* Users configure the mechanism once and then use it every time they interact. Users cannot forget or neglect the strategy, because the mechanism is part of the interaction.
- 3) 🧑🏻 *No Effort:* Users are automatically protected when interacting with a system.

Dimension 4 – User Resources: This dimension describes the resources needed by the users.

- 1) 🔪 *Protection object:* Additional items required by the users, such as gloves [27] or rubber thimblettes [27].
- 2) 📱 *Software:* Users require a specific software installed on one of their devices, e.g., for multi-factor authentication and other alternative authentication schemes [37].
- 3) 📱 *Hardware:* Users need specific personal hardware, such as eye-tracking glasses, to use a protection strategy [28].
- 4) ❌ *None:* Users do not require any resources to be protected from thermal attacks. Examples for this are filtering interactions from the camera feed [9] and using interfaces that feature materials that do not retain heat traces [10, 41].

Dimension 5 – Universality: Universality distinguishes to which degree mechanisms can be used for different interfaces.

- 1) 🌐 *Holistic:* The protection mechanism also protects against different kinds of side-channel attacks, such as shoulder-surfing and smudge attacks.
- 2) 🌐 *Universal:* The protection mechanism equally protects all kinds of devices and interfaces against thermal attacks.
- 3) 📍 *Restricted:* The protection mechanism can only be used for a specific subset of input devices, e.g., thimblettes [27] cannot be used on touchscreen devices.

Dimension 6 – Verifiability: Verifiability describes to which degree users who understand the strategy can verify that ef-

fective mitigation has been applied.

- 1) ✅ *Complete:* Users are assured they are protected from thermal attacks.
- 2) ⚡ *Partial:* Users can verify that a protection mechanism is present, but not its efficacy.
- 3) 🚫 *Not verifiable:* Users cannot verify the mechanism.

7 Discussion

This section discusses the design space and the user study results to inform users and manufactures on how to protect best against thermal attacks on public payment terminals.

7.1 How to defend users from thermal attacks?

Participants evaluated the range of different protection strategies that were used to inform the proposed design space. Overall, they tended to prefer *effective* strategies that are *verifiable* and ideally *automatic*, meaning the device manufacturer defends the users. Participants were willing to sacrifice convenience for the sake of verifying the efficacy of protection. The question is, how can these user perceptions and preferences inform actionable solutions that offer *effective* and *holistic* protection. For this, we must first discuss the prevalence of the threat. Thermal attacks have been demonstrated as a viable threat to touch-based interfaces [1, 10, 15, 27, 41], yet most investigations were based on thermal images taken in ideal lab conditions. Outside the lab, however, it might be challenging for attackers to successfully carry out such an attack, as thermal images need to be taken within a specific time-frame after interaction [1, 27, 41] from a specific angle [10, 52]. Consequently, thermal attacks are likely limited to a situations and environments where attackers have enough time to capture the images within the required angle range. Below, we consider this when discussing protection.

Large-scale changes of infrastructure are unrealistic. As noted by participants, protection has to be *viable* and *effective*, changing the hardware of world-wide device infrastructure, e.g., ATMs, to *automatically* protect users from thermal attacks would be challenging [39]. Secure environments, such as banks, may not require change as the secure environment makes it challenging to conduct attacks [45]. PIN-pads in supermarkets may be equally secure, because the environment setup makes it challenging to take thermal images unless attackers are queuing up [45]. Consequently, interfaces outside would be the most vulnerable to thermal attacks (among personal devices). This rules out a change of hardware for old devices, although changes could be gradually incorporated by newer models. Heated elements might be difficult, as study participants worried about not being able to verify their efficacy and they require additional energy or computation-intensive processes [1]. Using different materials is also not verifiable, but more doable, only requiring changes to some components (e.g., the keys [10]). Priming hands has two issues, users (a) cannot verify it and (b) might simply forget to do it, as reflected in our results. Consequently, physical covers that protect the interface until heat traces disappear seem among the most viable manufacturer-based solutions, in case a change of hardware is possible. Such covers could also wipe away fingerprints. PEKs and multi-factor authentication were placed at the top of the ranking and users familiar with them liked the protection offered. As also stated by our participants, some manufacturers already offer this solution. If the interface is a touchscreen, only the software has to be updated. Initial investigations on the efficacy of PIN-PEKs against thermal attacks and usability are promising [33]. Further, PEKs also defend against smudge and shoulder-surfing attacks, which helps with the property of *holistic* defence.

Intuitive strategies rely on habits. Our evaluation shows that users intuitively might use a range of realistic strategies for defence from thermal attacks. Most intuitively used strategies also work across a range of devices, making them universal. The effectiveness of resting the fingers has already been investigated in the literature [1, 52]. The strategies of waiting, observing environments, and resting fingers also rely on users to actively perform them, ideally as part of an authentication routine that users acquire as a habit, if motivated to do so. Further studies are needed, however, to judge if this is realistic, because users might forget to do it or perceive it as an obstacle as security is frequently a secondary task. Further, acquiring new security habits for personal devices may be challenging as they are used in a variety of contexts. Thus, users might not perform the protection at home, but elsewhere. Either way, the threat of thermal attacks on personal devices, and data that can be captured to harm users, needs further investigation. Because users rarely authenticate and then immediately leave devices

unattended [15], habit-based strategies might be more important when interacting with public devices.

Everyday items might be usable as protection objects. Interestingly, several participants intuitively wanted to use protection objects (e.g. gloves or stylus). On the other hand, opinions on these objects were divided, because additional objects might not be available during interaction. Some users, however, may already carry items that might serve as protection objects. For instance, wearing gloves during interaction is becoming popular for finger tracking as products like Sensoryx [49] that are increasingly integrated into extended reality headsets. Consequently, users might already wear gloves. This could, however, restrict interaction with touchscreens. Further, protection objects might help regarding hygiene requirements, because interfaces do not need to be touched by bare hands. Since the opinions regarding protection objects were diverse, we argue that they might work for a subset of users, yet do not ensure protection.

Biometrics are not the silver bullet. Biometrics perfectly protect from thermal attacks and placed high in participants' strategy rankings, together with PEKs and alternative authentication. Although effective, biometrics have privacy implications, which was also mentioned by participants. Fingerprints, for instance, might be stolen or linked to a person's identity [46]. Many biometric schemes allow users to authenticate without necessarily ensuring their consent, which may raise ethical issues [47]. While switching to biometric authentication may seem appealing, current implementations require a knowledge-based scheme for fallback authentication because biometric authentication is rather probabilistic. This is due to variations in the user's environments, such as non-ideal lighting conditions for capturing the user's face, or wet/dirty fingers [43]. Thus, biometric authentication can be attacked by forcing its users to use their fallback mechanism that is vulnerable to thermal attacks, e.g., using bypass attacks [47].

Holistic protection is needed. There is little awareness among users of thermal attacks [15], making it unlikely that users will employ strategies to protect themselves. Further, as stated above, many strategies that are actionable with current devices rely on user habits. This results in two assumptions regarding the user behaviour in the security chain of protection from thermal attacks, that are also present in many other security mechanisms: (1) users have to be aware that they need to act if they want to be defended from thermal attacks, and (2) users need to know which actions from them are needed. As demonstrated by countless usable security studies, such assumptions are not realistic. Further, the threat is not severe enough to justify millions of users acquiring new habits that work only against this threat. Given this, we argue once again for *holistic* protection mechanisms

that cover a range of different side-channel attacks. Many interfaces for mobile banking apps, for instance, already integrate information to make sure that no-one is around when authorising a transaction.

Should thermal camera manufacturers protect users? The literature proposed manipulating the feed of the thermal camera to obfuscate user interfaces [9, 10, 38]. Less than four percent of our study participants considered the camera manufacturer to be responsible for protection. While it has been demonstrated that such protection is effective, it may add noise to the camera feed, impeding the task the thermal camera user is attempting. Therefore, work in that direction should aim to minimise the impact on the camera utility, e.g., obfuscating interfaces only when heat traces are detected. While skilled attackers may use custom firmware to circumvent feed filtering, integrating protection into thermal cameras might reduce the risk as laymen would no longer be able to use thermal cameras maliciously.

7.2 Final Recommendations

In this section, we provide actionable recommendations for users and device manufacturers that consider a wide range of users and (camera) manufacturers to fit their individual circumstances rather than providing one single solution that demands one-size-fits-all.

For Users: Overall, users should ideally follow strategies that holistically and proactively defend them in vulnerable scenarios. Each user need not utilise all these recommendations, but a subset of the strategies their habits allow.

1. Enter credentials of important accounts in secure environments only, such as banks.
2. Use holistic strategies, e.g. observing the environment and making sure that no-one is around.
3. In public places, resting your fingers on the interface for a few seconds, or simply putting the device away in a pocket or purse is effective after entering sensitive input.
4. If your habits allow it, use protection objects to enter credentials of important accounts.
5. Use multi-factor authentication for important accounts.
6. Make sure to protect all authentication factors (e.g., PIN and card in the ATM scenario) because attackers need all of them to impersonate you.

For Device Manufacturers: We offer recommendations to manufacturers based on the type of device to protect users automatically or enable users to protect themselves.

1. For static devices: design environments that preclude thermal, but also other side-channel attacks.
2. Augment devices to offer automatic and verifiable protection on the device that is holistic and suited to the interface's implementation, such as PEKs for software interfaces, or physical covers for hardware interfaces.

3. Use software-based solutions to notify users to observe their surroundings, e.g., in financial transaction apps.

For Camera Manufacturers: Camera manufacturers should enact both recommendations to protect users.

1. Integrate methods that prevent the misuse of the camera, but also minimise the impact on the camera's utility (e.g., obfuscate interfaces in the camera's feed only when heat traces are visible).
2. Clearly notify users when obfuscation is taking place.

8 Conclusion and Future Work

This paper investigated protection against the emerging threat of thermal attacks. For this, first a literature review was conducted to identify 14 strategies. Through an online survey ($N = 306$), we collected user perceptions of thermal attack protection, specifically investigating how users are willing to protect themselves from thermal attacks. Overall, the following kinds of strategies were preferred: (1) those with effective and verifiable protection, (2) those with an effort-less, automatic defence done by the device manufacturer, (3) those with low user effort and no additional resources, and (4) those highly trusted to deliver efficacy even if convenience has to be sacrificed. We used the literature review and user study results to propose a user-centred design space for thermal attack protection. Finally, we discuss actionable precautions that users and (camera) manufacturers can take.

Future work should follow several directions: First, the long-term usage of thermal attack protection in realistic out-of-lab settings specifically focusing on efficacy should be investigated. Further, the realisations of specific strategies need further investigation, particularly the impact of camera feed filtering, the usage of physical covers, and habit-based strategies. For the latter, investigations in the users' daily contexts in-the-wild are required to investigate realistic settings. Finally, a more holistic investigation should not only consider the efficacy of thermal attack protection but also the protection from other side-channel and social engineering attacks, such that the burden on users is kept as low as possible.

Acknowledgments

This work was supported by the EPSRC(EP/V008870/1), and the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which is also funded by the EPSRC (EP/S035362/1). Furthermore this work was co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

- [1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. Stay Cool! Understanding Thermal Attacks on Mobile-Based User Authentication. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, CHI '17, page 3751–3763, New York, NY, USA, 2017. ACM.
- [2] Yasmeen Abdrabou, Yomna Abdelrahman, Ahmed Ayman, Amr Elmougy, and Mohamed Khamis. *Are Thermal Attacks Ubiquitous? When Non-Expert Attackers Use Off the Shelf Thermal Cameras*. ACM, New York, NY, USA, 2020.
- [3] Yasmeen Abdrabou, Reem Hatem, Yomna Abdelrahman, Amr Elmougy, and Mohamed Khamis. Passphrases Beat Thermal Attacks: Evaluating Text Input Characteristics Against Thermal Attacks on Laptops and Smartphones. In *IFIP Conference on Human-Computer Interaction*, pages 712–721. Springer, 2021.
- [4] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismael, and Amr Elmougy. ENGAGE: Resisting Shoulder Surfing Using Novel Gaze Gestures Authentication. In *Proc. of the International Conference on Mobile and Ubiquitous Multimedia*, MUM '18, page 469–473, New York, NY, USA, 2018. ACM.
- [5] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismail, and Amr Elmougy. Just gaze and wave: Exploring the use of gaze and gestures for shoulder-surfing resilient authentication. In *Proc. of the ACM Symposium on Eye Tracking Research & Applications*, ETRA '19, New York, NY, USA, 2019. ACM.
- [6] Yasmeen Abdrabou, Nadeen Mourad, and Amr Elmougy. Exploring the Scalability of Behavioral Mid-Air Gestures Authentication. In *Proc. of the International Conference on Mobile and Ubiquitous Multimedia*, MUM 2018, page 351–357, New York, NY, USA, 2018. ACM.
- [7] Yasmeen Abdrabou, Ken Pfeuffer, Mohamed Khamis, and Florian Alt. GazeLockPatterns: Comparing Authentication Using Gaze and Touch for Entering Lock Patterns. In *ACM Symposium on Eye Tracking Research and Applications*, ETRA '20 Short Papers, New York, NY, USA, 2020. ACM.
- [8] Hassoumi Almoutar, Pourang Irani, Vsevolod Peysakhovich, and Christophe Hurter. Path Word: A Multimodal Password Entry Method for Ad-Hoc Authentication Based on Digits' Shape and Smooth Pursuit Eye Movements. In *Proc. of the ACM International Conference on Multimodal Interaction*, ICMI '18, page 268–277, New York, NY, USA, 2018. ACM.
- [9] Norah Alotaibi, Md Shafiqul Islam, Karola Marky, and Mohamed Khamis. Advanced Techniques for Preventing Thermal Imaging Attacks. In *International Conference on Intelligent User Interfaces*, IUI '22 Companion, page 18–21, New York, NY, USA, 2022. ACM.
- [10] Norah Alotaibi, John Williamson, and Mohamed Khamis. ThermoSecure: Investigating the Effectiveness of AI-Driven Thermal Attacks on Commonly Used Computer Keyboards. *ACM Trans. Priv. Secur.*, 26(2), mar 2023.
- [11] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks. In *Proc. of the ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '13, page 1–6, New York, NY, USA, 2013. ACM.
- [12] Ilhan Aslan, Andreas Uhl, Alexander Meschtscherjakov, and Manfred Tscheligi. Mid-Air Authentication Gestures: An Exploration of Authentication Based on Palm and Finger Motions. In *Proc. of the International Conference on Multimodal Interaction*, ICMI '14, page 311–318, New York, NY, USA, 2014. ACM.
- [13] Md Tanvir Islam Aumi and Sven Kratz. AirAuth: Evaluating in-Air Hand Gestures for Authentication. In *Proc. of the International Conference on Human-Computer Interaction with Mobile Devices & Services*, MobileHCI '14, page 309–318, New York, NY, USA, 2014. ACM.
- [14] Roman Bednarik, Tomi Kinnunen, Andrei Mihaila, and Pasi Fränti. Eye-movements as a biometric. In *Scandinavian Conference on Image Analysis*, pages 780–789. Springer, 2005.
- [15] Paul Bekaert, Norah Alotaibi, Florian Mathis, Nina Gerber, Aidan Christopher Rafferty, Mohamed Khamis, and Karola Marky. Are Thermal Attacks a Realistic Threat? Investigating the Preconditions of Thermal Attacks in Users' Daily Lives. In *Nordic Human-Computer Interaction Conference*, NordiCHI '22, New York, NY, USA, 2022. ACM.
- [16] Omair Shahzad Bhatti, Michael Barz, and Daniel Sonntag. EyeLogin - Calibration-Free Authentication Method for Public Displays Using Eye Gaze. In *ACM Symposium on Eye Tracking Research and Applications*, ETRA '21 Short Papers, New York, USA, 2021. ACM.
- [17] Virginia Braun and Victoria Clarke. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

- [18] Virginia Braun and Victoria Clarke. *Successful Qualitative Research: A Practical guide for Beginners*. SAGE Publications, London, 2013.
- [19] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. Look into My Eyes! Can You Guess My Password? In *Proc. of the Symposium on Usable Privacy and Security*, SOUPS '09, New York, NY, USA, 2009. ACM.
- [20] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. Touch Me Once and i Know It's You! Implicit Authentication Based on Touch Screen Patterns. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, page 987–996, New York, NY, USA, 2012. ACM.
- [21] Rainhard Dieter Findling, Tahmid Quddus, and Stephan Sigg. Hide My Gaze with EOG! Towards Closed-Eye Gaze Gesture Passwords That Resist Observation-Attacks with Electrooculography in Smart Glasses. In *Proc. of the International Conference on Advances in Mobile Computing & Multimedia*, MoMM2019, page 107–116, New York, NY, USA, 2019. ACM.
- [22] Thomas Franke, Christiane Attig, and Daniel Wessel. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human-Computer Interaction*, 35(6):456–467, 2019.
- [23] Batya Friedman, Peter H. Khan Jr, and Daniel C. Howe. Trust Online. *Communications of the ACM*, 43(12):34–40, 2000.
- [24] Yang Gao, Wei Wang, Vir V. Phoha, Wei Sun, and Zhanpeng Jin. EarEcho: Using Ear Canal Echo for Wearable Authentication. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 3(3), sep 2019.
- [25] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. NDSS, 2017.
- [26] Eiji Hayashi, Manuel Maas, and Jason I. Hong. Wave to Me: User Identification Using Body Lengths and Natural Gestures. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 3453–3462, New York, NY, USA, 2014. ACM.
- [27] Tyler Kaczmarek, Ercan Ozturk, and Gene Tsudik. Thermanator: Thermal Residue-Based Post Factum Attacks on Keyboard Data Entry. In *Proc. of the ACM Asia Conference on Computer and Communications Security*, Asia CCS '19, page 586–593, New York, NY, USA, 2019. ACM.
- [28] Christina Katsini, Yasmeen Abdrabou, George E. Raptis, Mohamed Khamis, and Florian Alt. *The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions*, page 1–21. ACM, New York, NY, USA, 2020.
- [29] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proc. of the CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '16, page 2156–2164, New York, NY, USA, 2016. ACM.
- [30] Mohamed Khamis, Regina Hasholzner, Andreas Bulling, and Florian Alt. GTmoPass: Two-Factor Authentication on Public Displays Using Gaze-Touch Passwords and Personal Mobile Devices. In *Proc. of the ACM International Symposium on Pervasive Displays*, PerDis '17, New York, NY, USA, 2017. ACM.
- [31] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. Gaze-TouchPIN: Protecting Sensitive Data on Mobile Devices Using Secure Multimodal Authentication. In *Proc. of the ACM International Conference on Multimodal Interaction*, ICMI '17, page 446–450, New York, NY, USA, 2017. ACM.
- [32] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-Based Authentication on Situated Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(4), dec 2018.
- [33] Daniel Kirkwood, Cagdas Tombul, Calum Firth, Finn Macdonald, Konstantinos Priftis, Florian Mathis, Mohamed Khamis, and Karola Marky. PIN Scrambler: Assessing the Impact of Randomized Layouts on the Usability and Security of PINs. In *Proc. of the International Conference on Mobile and Ubiquitous Multimedia*, MUM '22, page 83–88, New York, NY, USA, 2022. ACM.
- [34] Chandan Kumar, Daniyal Akbari, Raphael Menges, Scott MacKenzie, and Steffen Staab. TouchGazePath: Multimodal Interaction with Touch and Gaze Path for Secure Yet Efficient PIN Entry. In *Proc. of the International Conference on Multimodal Interaction*, ICMI '19, page 329–338, New York, NY, USA, 2019. ACM.
- [35] Duo Li, Xiao-Ping Zhang, Menghan Hu, Guangtao Zhai, and Xiaokang Yang. Physical Password Breaking via Thermal Sequence Analysis. *IEEE Transactions on Information Forensics and Security*, 14(5):1142–1154, 2019.

- [36] Duo Li, Xiao-Ping Zhang, Guangtao Zhai, Xiaokang Yang, Wenhan Zhu, and Xiao Gu. Modeling Thermal Sequence Signal Decreasing for Dual Modal Password Breaking. In *Proc. of the IEEE International Conference on Image Processing, ICIP*, pages 1703–1707, 2018.
- [37] Zhen Ling, Melanie Borgeest, Chuta Sano, Jazmyn Fuller, Anthony Cuomo, Sirong Lin, Wei Yu, Xinwen Fu, and Wei Zhao. Privacy enhancing keyboard: Design, implementation, and usability testing. *Wireless Communications and Mobile Computing*, 2017, 2017.
- [38] Shaun Alexander Macdonald, Norah Mohsen Alotaibi, Md Shafiqul Islam, and Mohamed Khamis. Conducting and Mitigating Portable Thermal Imaging Attacks on User Authentication Using AI-Driven Methods. In *Proc. of the Augmented Humans International Conference, AHs '23*, page 357–359, New York, NY, USA, 2023. ACM.
- [39] Shaun Alexander Macdonald, Habiba Farzand, Norah Alotaibi, Md Shafiqul Islam, and Mohamed Khamis. Change Policy or Users? Mitigating the Security Risks of Thermal Attacks. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23-28, 2023, Hamburg, Germany*, volume 1, pages 1–3. ACM, 2023.
- [40] Fabian Monrose and Aviel Rubin. Authentication via Keystroke Dynamics. In *Proc. of the ACM Conference on Computer and Communications Security, CCS '97*, page 48–56, New York, NY, USA, 1997. ACM.
- [41] Keaton Mowery, Sarah Meiklejohn, and Stefan Savage. Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks. In *Proc. of the USENIX Conference on Offensive Technologies, WOOT'11*, page 6, USA, 2011. USENIX Association.
- [42] Toan Nguyen and Nasir Memon. Tap-based User Authentication for Smartwatches. *Computers & Security*, 78:174–186, 2018.
- [43] Sarah Prange, Lukas Mecke, Alice Nguyen, Mohamed Khamis, and Florian Alt. Don't Use Fingerprint, it's Raining! How People Use and Perceive Context-Aware Selection of Mobile Authentication. In *Proc. of the International Conference on Advanced Visual Interfaces, AVI '20*, New York, NY, USA, 2020. ACM.
- [44] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J. Hyland. Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In *Symposium on Usable Privacy and Security, SOUPS*, pages 3–4. ACM, 2006.
- [45] Gurvinder Singh, Sergey Butakov, and Bobby Swar. Thermal Print Scanning Attacks in Theretail Environments. In *International Siberian Conference on Control and Communications, SIBCON*, pages 1–6. IEEE, 2019.
- [46] Martin Stokkenes, Raghavendra Ramachandra, and Christoph Busch. Biometric authentication protocols on smartphones: An overview. In *Proc. of the 9th International Conference on Security of Information and Networks, SIN '16*, page 136–140, New York, NY, USA, 2016. ACM.
- [47] Christian Tiefenau, Maximilian Häring, Mohamed Khamis, and Emanuel von Zezschwitz. "please enter your pin" - on the risk of bypass attacks on biometric authentication on mobile devices. *CoRR*, abs/1911.07692, 2019.
- [48] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujjo Bauer, Nicolas Christin, and Lorrie Faith Cranor. I added '! ' at the end to make it secure": Observing Password Creation in the Lab. In *Proc. of the Symposium on Usable Privacy and Security, SOUPS*, 2015.
- [49] VROne. VRFREE - Haptic VR glove review. <https://www.vrone.co.uk/vr-accessories/vr-gloves/vrfree-haptic-vr-glove>. [Online; accessed 7-Feb-2023].
- [50] Roman Weiss and Alexander De Luca. PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability. In *Proc. of the Nordic Conference on Human-Computer Interaction: Building Bridges, NordiCHI '08*, page 383–392, New York, NY, USA, 2008. ACM.
- [51] Alma Whitten and J. Doug Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*, pages 169–184, 1999.
- [52] Wojciech Wodo and Lucjan Hanzlik. Thermal Imaging Attacks on Keypad Security Systems. In *Prod. of the International Joint Conference on e-Business and Telecommunications, ICETE*, pages 458–464, 2016.

A Online Study

In this section, we provide texts and questions used in the online study. Text presented to participants is in *italic letters*.

1. Familiarisation

- By Text: *Thank you for agreeing to participate in our study. The purpose of this questionnaire is to investigate perceptions on the mitigation strategies against thermal attacks. Thermal attacks are a type of hack, where attackers use a thermal camera to take pictures of the heat residue you leave on devices that you interact with. For instance, thermal attacks can be used to capture your credit card pin code by taking pictures of*

ATM or payment terminal keypads after you have used them. Thermal attacks can also be used to capture the code or pattern you use to unlock your smartphone, your computer password, digital doorlock codes, home safe codes, and more. Studies have shown that usable heat traces can be captured up to a minute after you have typed in your PIN code or password. You will get more detailed information about thermal attacks in the next sections.

- By Video: The participants watched two videos that demonstrate thermal attacks, including thermal images.

2. **Explaining terminology:** Participants were explained the terminology used in the questionnaire. In this questionnaire, we will use some words that are worth defining for the sake of clarity:

- **Credentials:** this refers to PIN codes, passwords, and any other secret login information.
- **Device:** this refers to the item being attacked, whether it is an ATM, a laptop, a smartphone, a payment terminal in a store, or something else.
- **Interface:** this refers to the part of the device that you are interacting with when entering your credentials. For an ATM or a payment terminal it is the keypad, for a smartphone it is the touch screen, for a laptop it is the keyboard.

3. **Understandability & Attention Check Quiz:**

- A thermal attack describes inferring sensitive data (e.g., a password) based on heat traces on a surface (e.g., a smartphone). Please state whether this statement is true or false.
- Thermal attacks can be carried out after the user entered data (e.g., after they left their phone unattended). Please state whether this statement is true or false.
- For carrying out a thermal attack the user has to be present while the thermal image is captured. Please state whether this statement is true or false.

4. **Responsibility Question:** Who, in your opinion, is responsible to protect you from thermal attacks? (multiple-choice)

- I am responsible
- The manufacturer of the interface (e.g., ATM or smartphone) is responsible
- The manufacturer of the thermal camera is responsible
- Other, please specify:

5. **Intuitive Protection:** How would you protect yourself from a thermal attack when using an ATM? Please describe how you would protect yourself from a thermal attack when you withdraw money from an ATM. (open-ended)

6. **Evaluation of strategies:** For each strategy, we provided a description, an example connected to the ATM scenario, a visual depiction, and asked three questions.

In this section you will be presented with 14 strategies and asked to evaluate them. Each strategy is described, followed by a scenario that explains how the strategy could be used. We are interested in your intuitive opinion on these strategies. There are no right or wrong answers. We further do not evaluate your performance. You will first be asked to evaluate the strategies individually. Then, you will be asked to rank all different groups of strategies in order of your personal preference.

- **Usage Intention:** I would like to use the described strategy in the ATM scenario to protect myself from thermal attacks. (5-point Likert scale)
- **Trust Perception:** I am confident that my credentials are protected from a thermal attack by this strategy. (5-point Likert scale)
- **Explanation:** We would like to know why you answered the questions above the way you did. The more details, the better. (open-ended)

We used the descriptions for the strategies provided in Table 7 in randomised order. The descriptions included two simple attention check items.

7. **Ranking the strategies:** Please rank the strategies by personal preference by using drag and drop. Drag the blue rectangles with the strategies to the list on the right. In the bottom of the page, participants could read the descriptions (see Table 7) again in case they forgot how a strategy worked.

Ranking Explanation: Please explain your ranking of the strategies.

8. **Demographics:** The survey was concluded with demographic questions. Then, participants for redirected to Prolific for reimbursement.

B Codebooks

This section provides the codebooks used to analyse the open-ended responses. For analysing intuitive strategies, we used the list of codes in Table 5. The remaining questions were coded with the 15 codes listed below in Table 6.

Table 5: Table displaying the qualitative codebook of 18 codes to code the intuitive protection strategies.

Code	Description	#	%
biometrics	Usage of biometric authentication	0	0%
blowing	Blowing on the interface	0	0%
feed_filtering	Filtering the thermal camera feed	0	0%
input_modality	Using touchless input modalities	0	0%
heated_element	Having a heated interface	0	0%
gloves	Wearing gloves	56	18%
graphical_cues	Using cue-based authentication	0	0%
improve_credentials	Change characteristics of credentials	0	0%
materials	Using materials with less thermal conductivity	0	0%
multi-factor_auth	Using 2FA or multi-factor authentication	11	3.9%
PEKs	Using PEKs	0	0%
physical_cover	Having a physical cover after interaction	0	0%
priming_hands	Touching something cold before interaction	0	0%
resting_fingers	Rest the hand or fingers on the interface after interaction	137	45%
thimblettes	Wearing rubber thimblettes	0	0%
new_observation	Observe the surroundings	24	7.8%
new_secure_environment	Entering credentials in secure environments	3	1%
new_waiting	Waiting until heat traces decayed	82	27%
new_protection_objects	Using an object to not leave heat traces	33	11%
non_suitable_strategy	The strategy does not protect against thermal attacks	45	14%

Table 6: Table displaying the qualitative codebook of 15 codes describing the benefits or problems with the proposed thermal mitigation strategies and their prevalence across the total of 4284 responses (306 participants x 14 strategies).

Code	Description	#	%
efficacy	Participant stated/trusted that the strategy works	1506	35.2%
efficacy_issues	Participant does not trust/believe strategy will work	649	15.1%
efficacy_in_theory	Participant understands why strategy would work in theory	217	5.07%
verifiability	Participant believes the user should verify efficacy	5	0.12%
uncertainty	Participant felt uncertainty about if strategy works	628	14.7%
other_attacks	Concern that attackers could still exploit information to perform other side-channel attacks or steal fingerprints	46	1.07%
other_attacks_hygiene	Using strategy is unhygienic or unsafe/lead to danger	220	5.14%
effortlessness	Participant considers strategy convenient or practical	295	6.89%
effortfulness	Participant considers strategy inconvenient or impractical	810	18.9%
ease-of-use	Participant considers strategy to be simple, easy or efficient	167	3.90%
complexity	Strategy is complicated, strange or uncomfortable to use	352	8.22%
viability	Concerned strategy would be technologically unreliable	113	2.64%
resources_needed	Dislikes that strategy requires bringing a protection object	207	4.83%
automatic	Participant believes the system/bank responsible for security issue	107	2.50%
discreetness	Comments on the discreetness of a strategy	68	1.58%

Table 7: Descriptions of strategies and scenarios used in the online study.

Strategy	Description	Scenario
Wearing gloves	You wear gloves to minimise the heat traces you leave on the device. Gloves work as an insulating barrier between your fingers and the device.	You walk up to an ATM to withdraw money. Before you enter your credentials (PIN code), you put on your gloves. After your credentials have been entered (or after you have finished withdrawing money) you can take your gloves off.
Using rubber thimblettes	You wear a rubber thimblette to minimise the heat traces you leave on the device. Rubber works as an insulating barrier between your finger and the device.	You walk up to an ATM to withdraw money. Before you enter your credentials (PIN code) you put your rubber thimblette on the finger you intend to use to enter your credentials. After your credentials have been entered (or after you have finished withdrawing money) you take off your rubber thimblette.
Resting fingers on interface	You use your fingers to leave extra heat traces on the interface after you have entered your credentials.	You walk up to an ATM to withdraw money. You enter your credentials (PIN code). After your credentials have been entered, you rest your fingers on the keypad for a few seconds.
Changing your credentials	You use credentials that are more difficult to hack using thermal imaging. Overlaps, repetition, special characters, and longer credentials can be used to obscure the order in which the characters have been typed. This makes it more difficult for hackers to decipher your credentials using thermal images.	You walk up to an ATM to withdraw money. You enter your credentials (PIN code). Because you have used repetitions in your pincode and made it longer, it is mathematically more difficult for an attacker to decipher the order of the numbers in your pin code.
Priming your hands	You briefly touch something cold to lower the temperature of your fingers before entering your credentials. The thing you touch could either be a cooling element installed on the device, or a cold surface next to you. By priming your hands in this way you minimise the heat traces your fingers leave when entering your credentials.	You walk up to an ATM to withdraw money. The manufacturer of the ATM has installed a cooling element next to the keypad so you can prime your hands. You touch the cooling element for a few seconds before entering your credentials.
Blowing on the interface	Your breath is used to manipulated heat traces on the interface after you have entered your credentials, by blowing on the interface.	You walk up to an ATM to withdraw money. You enter your credentials (PIN code). After your credentials have been entered, you blow on the keypad.
Heating element behind the interface	There is a heating element below the interface you use to enter your credentials. The extra heat from the heating element adds extra heat traces.	You walk up to an ATM to withdraw money. You enter your credentials (PIN code). After your credentials have been entered a heating element behind the keypad slightly heats up the keypad.
Using materials with lower thermal conductivity	The device is made of materials that dissipate heat faster.	You walk up to an ATM to withdraw money. You enter your credentials (PIN code) on the metal keypad. After your credentials have been entered, the heat traces you left quickly dissipate because the keypad is made of metal.
Cover	A cover automatically covers the interface for a set period of time after you have entered your credentials. Since heat traces naturally dissipate over time, the longer an attacker waits before taking the thermal image, the more the traces has dissipated. When the cover retracts and reveals the interface again, the heat traces are no longer visible.	You walk up to an ATM to withdraw money. You enter your credentials (PIN code). A cover automatically slides over the keypad for 30 seconds before it retracts again.
Privacy enhanced keyboards	A Privacy Enhanced Keyboard (PEK) is an interface for entering your credentials that only works on touchscreens. There are many types of PEKs, but the most common one shuffles the position of the characters in the keyboard.	You walk up to an ATM to withdraw money. You enter your credentials (PIN code) on the touch keypad. Each time you interact with the ATM, the order of the keys is different.
Alternative input modality	Instead of using your fingers to directly interact with the interface, you use an alternative. This can take many forms: gaze input (the direction in which you look with your eyes), a stylus, or a computer mouse.	You walk up to an ATM to withdraw money. The ATM is installed with an alternative entry modality (e.g., gaze). You enter your credentials using your gaze.
Graphical credentials	Instead of using traditional character-based credentials, you use graphical ones. For instance, credentials consist of a series of images. The user is presented with a set of images and has to chose the first image from their credentials. Then a new set of images appears and the user has to pick the second image from their credentials, and so forth.	You walk up to an ATM to withdraw money. The ATM uses graphical credentials. You enter your credentials.
Additional authentication factor(s)	You use a secondary device to verify your identity after entering your credentials. For instance, a text or email that is sent to you with a unique code which you then have to enter on the device you entered your credentials on.	You walk up to an ATM to withdraw money. You enter your credentials (pincode). After that, your bank sends you a text with a 6-character one-time password. You then enter that pincode on the ATM.
Biometric authentication	You use your own biometrics as credentials, instead of character based credentials, such as finger prints, iris information, or a face ID. When you want to access the device, you interact with it in the way that the particular biometric authentication scheme requires (touch finger print reader, hold device up to your face, etc), and the device unlocks.	You walk up to an ATM to withdraw money. The ATM has a fingerprint reader. You place your finger on the reader.