Are Thermal Attacks a Realistic Threat? Investigating the Preconditions of Thermal Attacks in Users' Daily Lives

Paul Bekaert
2517073B@student.gla.ac.uk
University of Glasgow
Glasgow, United Kingdom

Norah Alotaibi
n.alotaibi.3@research.gla.ac.uk
University of Glasgow
Glasgow, United Kingdom

Florian Mathis
University of Glasgow
Glasgow, United Kingdom
florian.mathis@glasgow.ac.uk

Nina Gerber
nina.gerber@tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

Aidan Rafferty
2314722R@student.gla.ac.uk
University of Glasgow
Glasgow, United Kingdom

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

Karola Marky
karola.marky@itsec.uni-hannover.de
Leibniz University Hannover
Hannover, Germany
University of Glasgow
Glasgow, United Kingdom

ABSTRACT

Thermal attacks refer to the possibility of capturing heat traces that result from interacting with user interfaces to reveal sensitive input, such as passwords. The technical feasibility and effectiveness of thermal attacks have already been demonstrated. Yet, several preconditions have to be met for successful thermal attacks. In this paper, we investigate user awareness of thermal attacks and to which extent the attack's preconditions are met in the users' daily lives. We present results from an online study with 101 participants showing that users are frequently at risk of thermal attacks based on their behavior, e.g., due to leaving devices unattended, or their choice of authentication method. Further, only 7 of our 101 participants had heard of thermal attacks. Based on our results, we discuss the implications on user security, operators of public spaces, and the development of thermal attack-resistant input methods.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; *Privacy protections*.

KEYWORDS

thermal attacks, usable security, usable privacy, side-channel attacks

ACM Reference Format:
Paul Bekaert, Norah Alotaibi, Florian Mathis, Nina Gerber, Aidan Rafferty, Mohamed Khamis, and Karola Marky. 2022. Are Thermal Attacks a Realistic Threat? Investigating the Preconditions of Thermal Attacks in Users' Daily Lives. In *Nordic Human-Computer Interaction Conference (NordiCHI '22), October 8–12, 2022, Aarhus, Denmark*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3546155.3546706

NordiCHI '22, October 8–12, 2022, Aarhus, Denmark

1 INTRODUCTION

Thermal attacks are a type of side-channel attack that takes advantage of heat traces left following an interaction with a user interface [1]. Adversaries can use thermal cameras to examine these heat traces to reconstruct key presses and even infer key press order [1]. Hence, adversaries can obtain authentication credentials, such as PINs [1, 4, 21] passwords [3, 12], or other typed information [4] with little effort. Despite the recent prevalence of alternative authentication schemes that resist thermal attacks by relying on biometrics (e.g., fingerprint or face recognition) or additional hardware (e.g., smartwatches), current implementations of said schemes still use the knowledge factor, i.e., PINs or patterns, as fall back methods. This means that attackers can employ bypass attacks [26] to force users of these schemes to use their a fall back method that is vulnerable to thermal attacks as we discuss further in section 5.1. Thermal attacks reveal more information than other types of side-channel attacks. Unlike smudge attacks [5], thermal attacks reveal the order of touchscreen taps and button presses. A thermal image of a PIN pad, for example, taken after a user has authenticated, will show the highest temperature at the last entered digit and the lowest temperature at the first entered digit which can be used to determine the order of digits. Furthermore, these attacks can also been done without the victim's presence, which makes it less likely a victim will know they have been attacked. Prior work has argued that thermal attacks are likely going to become "ubiquitous" [3] due to two main factors: First, thermal cameras became remarkably affordable, e.g., there are thermal cameras for less than $200[1]. Second, there are no technical prerequisites for carrying out thermal attacks. Adversaries can infer PINs, passwords, and sensitive content by visually inspecting the images produced by

[1] https://www.amazon.com/dp/B0728C7KND/ last accessed 09 April 2022.

these low-cost thermal cameras [3, 4]. Consequently, the technical requirements to execute thermal attacks are well-known. However, what remains under-explored is to which extent thermal attacks can actually be carried out in users' daily lives based on the their behavior and expectations.

In this paper, we explore to which extent the preconditions of thermal attacks are met in users' daily lives. We explore users' behavior when interacting with (mobile) devices in different scenarios and environments in a mixed-methods online study with N=101 participants. Further, we explore users' security perceptions of different scenarios and environments as well as their awareness of thermal attacks. Studying users' awareness of potential threats, e.g., thermal attacks, is important as previous work showed that users only apply protection mechanisms against risk they are aware of [11]. Our study shows that many users are aware of smudge attacks [5], shoulder surfing attacks [8], and what thermal cameras are. However, most of our participants reported to not consider thermal attacks as a realistic threat in their daily life. They also wrongly assumed that PINs and passwords would protect them against such attacks.

Furthermore, behaviors that put users at risk of thermal attacks are quite common. While users considered realistic mitigation strategies, at the time of our research, the majority did not use them. We conclude by discussing means to better defend users from thermal attacks considering holistic knowledge about other types of social engineering and side-channel attacks.

2 BACKGROUND & RELATED WORK

We build on two strands of previous work: research on thermal attacks and on understanding security and privacy risk awareness.

2.1 Thermal Attacks

Heat traces are best described as a temperature gradient caused by a thermal energy exchange at a contact point. Thermal cameras are capable of detecting these heat traces on user interfaces, such as keyboards and mobile phones [1, 4, 21]. This could be used maliciously to deduce sensitive information, which resulted in an area of research focused on assessing and mitigating the security threats of thermal attacks. Thermal attacks are carried out as follows: after a user has provided input on a user interface, an attacker uses a thermal camera to capture a thermal image of the interface. These are inconspicuous attacks, as they are carried out without the victim's presence, however the thermal camera needs to be in close proximity to the interaction. Thermal attacks are effective on a wide range of devices, as we discuss below.

2.1.1 Attacks against Keyboards and Keypads. The earliest form of thermal attack research investigated the feasibility of thermal attacks on keypad locks of a safe using a thermal camera costing between $5,000 and $10,000 USD [31]. It is possible to recover the keys pressed as long as the thermal image is taken within approximately five to ten minutes after a valid key code entry [31]. This time window would allow an attacker plenty of time after the user had left the device after entering their code, highlighting the threat that thermal attacks pose to the security of keypad PINs. Another study by Mowery et al. investigated the effectiveness of thermal attacks against keypads used in ATMs using high-end thermal cameras [21]. They used image processing techniques and visually inspected the thermal images to gather information. Image processing was more accurate than visual inspection. The effectiveness of thermal attacks is influenced by individual differences in body heat, keypress techniques as well as keypad material. Heat residue faded substantially faster for individuals with a light touch or a low body temperature, and plastic keypads were found to be more vulnerable to thermal attacks than metal keypads. Further research by Li et al. explored the effectiveness of low-cost thermal cameras that currently cost less than $200 to extract data from ATM keypads [17]. Another stream of research investigated thermal attacks on common computer keyboards [12]. Entire sets of keypresses could be recovered as late as 30 seconds after initial password entry, while partial sets can still be viable to recover after one minute. Abdrabou et al. [4] investigated thermal attacks against keyboards and touchscreens to capture text input. Passphrases and complex entries were found to be less vulnerable to thermal attacks. Text passwords typed into laptop keypads are less vulnerable than those typed into smartphone touchscreens. Further, the hand temperature has a major influence on the success of the attack, with those with warmer hands being more vulnerable to thermal attacks than others.

2.1.2 Attacks against Touchscreens and Touchpads. Recent work into thermal attacks has revealed that they also pose a threat to touchscreen and touchpad authentication. Abdelrahman et al. [1] investigated the effectiveness of thermal attacks in recovering PINs and patterns from touchscreen smartphones considering duplicate key presses and pattern overlaps and the age of the heat traces. Abdrabou et al. [3] investigated how effectively everyday users could conduct thermal attacks using an affordable thermal camera (less than US$450) on tap and gesture inputs on smartphones and laptop touchpads. The results showed that participants were able to recover 60.65% of gestures and 23.61% of touch tap passwords overall, while attack success on touchscreens (43.06%) and touchpads (41.2%) were.

2.2 Preconditions

In summary, it is clear that thermal attacks can pose a serious threat. Not only can thermal attacks recover passwords of various types after entry on a variety of devices, but they can also be conducted by anyone who has access to a relatively cheap thermal camera. In this paper, we investigate the severity of this threat by surveying users about their behavior when interacting with devices that have been shown to be vulnerable to thermal attacks. Based on previous work [1, 3], we investigate the following preconditions for thermal attacks:

- **P1:** In case of attacking authentication using thermal attacks, the used scheme must use the knowledge factor (e.g., alphanumeric password, pattern, or PIN).
- **P2:** The device has to be left unattended without presence of the user within a short time frame of providing input.
- **P3:** The device has to be left in the user's vicinity in a way that strangers have access to it.
- **P4:** The lack of awareness of thermal attacks, while not strictly required, makes it more likely that users will think their devices are secure in situations where they are not, thereby increasing their vulnerability to the attack.

P5: Thermal attacks are more likely to be successful if the user interacts minimally (or does not interact at all) after the sensitive input is provided, e.g., not using the keyboard anymore after authenticating.

2.3 Security and Privacy Risk Awareness

The second stream of research that is related to our work studies the security and privacy risk awareness of users. Researchers used surveys to investigate risk awareness of shoulder surfing [8], internet usage [10], password composition [28], mobile device usage [7, 27], and wearable computing [6, 9]. Overall, everyday users are often unaware of security and privacy risks associated with technology usage. Harbach et al. showed that users are only willing to spend limited effort on security, referred to as their "compliance budget" [10]. Hence, users will only defend themselves from risks that they are aware of. Asking participants which risks they are aware of from a list can provide misleading results about risk awareness, which we took into account when designing our own questionnaire. Researchers found that users rarely make use of additional security measures and that many users sometimes leave their phones unattended around others [7]. Such situations could be exploited by thermal attackers. In this paper, we extend this body of knowledge by contributing an awareness study of thermal attacks.

3 METHODOLOGY

In line with previous research that investigated security and privacy risk awareness, e.g., [6], we opted for an online study. As survey provider, we used Qualtrics and distributed the survey link through the online recruitment platform Prolific, which is specifically designed for use in research and has found wide-spread application in academia (e.g., [19, 20]). Research has shown that Prolific produces data quality comparable to Amazon Mechanical Turk (Mturk) with the benefit that Prolific participants are much more diverse than participants from MTurk [23]. We compensated participants with £3.75 for completing our survey, the standard fee for surveys hosted on Prolific which take 30 minutes to complete[2].

3.1 Survey Items

We designed an initial set of survey items based on previous work into thermal attack effectiveness and user awareness of other security and privacy risks [6] which was discussed between two researchers. We ensured that all items were worded in a neutral way which did not lead users into thinking that the authentication methods they use were insecure, to avoid biasing responses. Next, we tested the items in an internal pilot study to improve the clarity and order of our items and finalized the items after a second pilot study distributed on Prolific during which we collected feedback from participants. The results from these pilot studies are not included in the result section.

3.2 Survey Procedure

The survey took on average around 30 minutes to complete and consisted of open ended, multiple choice and Likert scale items. The survey was split into sections, once a participant completed a section they could not go back to change previous answers, to prevent them from using information learned in later sections of the survey to change their responses to earlier questions. We employed two attention checks which would allow us to discard unhelpful data from our analysis. Ethical approval was granted before the launch of our online survey.

3.2.1 Welcome, Consent & Demographics. Participants were first informed they could withdraw their consent at any time, that no personal or identifiable information would be collected and that their responses would be anonymized. The information sheet also detailed what would be required of participants that wish to take part and how their responses would be used. Next, the participants confirmed to have read and understood the study's consent form. Then, we collected demographic data consisting of gender, age, highest education level and self-reported technical expertise level.

3.2.2 Part I: Devices and Authentication Methods. We started the survey by asking participants which authentication mechanisms they used at the time of the survey. Next, we investigated the participants' experiences and usage of specific devices that have been identified as being vulnerable to thermal attacks, namely touchscreen devices [1, 3], keyboards [12] and keypads [21, 30, 31]. For each of these devices, we asked users to provide examples of devices they either owned or frequently used, authentication methods they used and reasoning behind their choices.

After assessing the participants' usage of devices and authentication methods, we assessed the participants' security considerations of authentication methods used on mobile devices, keyboards, and keypads. We specifically asked whether participants felt that passcodes, PINs or authentication patterns offered sufficient security for mobile devices and whether they felt that passwords and PINs offered sufficient security for devices with keyboard or keypad input. We also asked participants to provide a reasoning for their assessment. Each device and authentication mechanism asked about in each question was carefully chosen, as each combination had been identified in past literature as being vulnerable to thermal attacks. To conclude this survey part, we asked participants to provide methods that attackers could use to bypass touchscreen and keyboard/keypad authentication.

3.2.3 Part II: Scenarios and Environments. This survey part consisted of questions about scenarios in which participants had left their devices unattended for a short period of time around other individuals in the past. The next set of questions considered how attackers could exploit unattended scenarios to obtain authentication credentials.

We then asked questions about the risks that users associate with authenticating in public environments. This included their perceived security and privacy risks while using mobile devices in public environments, providing authentication details into a public computer, and providing authentication details via keyboard or keypad devices, such as Chip-and-PIN machines. We focused on these devices as they have been shown to be vulnerable to thermal attacks. We further asked for precautions participants employ to protect their security and privacy in public environments.

3.2.4 Part III: Thermal Attacks. In this survey part, we specifically introduced thermal cameras to participants. We first captured the

[2]https://www.prolific.co/pricing/, price from 9 September, 2021.

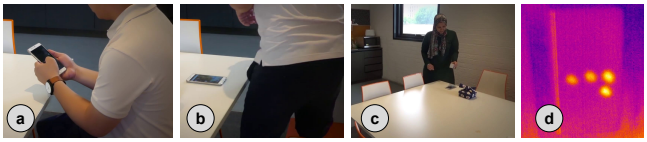

Figure 1: After responding to questions about authentication and security behaviors, participants watched a video demonstrating thermal attacks that is adapted from a video teaser [2] of a paper on thermal attacks [1].

participants' knowledge and experiences considering thermal cameras. Further, we asked about (malicious) use cases for thermal cameras.

In this part, we further investigated 1) the participants' awareness of thermal attacks, 2) their perceptions of attack feasibility, and 3) their opinion of the likelihood and severity of thermal attacks and protection strategies. For this, the participants were presented with a video which shows a person conducting a thermal attack on someone else's smartphone (Figures 1a - 1c). The was adapted from the teaser video of a CHI 2017 paper on thermal attacks [1] with a permission from the authors [2]. We asked participants whether this was a familiar scenario, what they believed the person on the right (the attacker) was doing and how they would describe their behavior. Next, we presented a thermal image of a smartphone screen that had also been part of the presented video (Figure 1d). We then asked participants how they believe the image was created and if they could infer the PIN shown by the heat traces. We then asked participants to estimate how long after authentication the image was taken, and how long they believed it would take for the heat traces shown in the image to disappear.

In the final part, we first explained what thermal attacks are and unveiled to participants that the video demonstrated a thermal attack. Next, we asked participants if they have ever been made aware of thermal attacks before this survey, and if so where from. Then, we asked if participants consider thermal attacks to be a serious security threat to mobile devices and if they consider PINs to be susceptible to thermal attacks. Participants were then asked to rank risks of thermal attacks (low/medium/high risk) to each of four common authentication mechanisms (PIN, password, fingerprint recognition, authentication patterns).

Further, we also asked for input interfaces that would be immune to thermal attacks. We then asked participants about mitigation strategies that could be used to protect touchscreen devices from thermal attacks and which, if any, they were already employing and why. We also asked participants if they could identify any other input interfaces which would be vulnerable to thermal attacks, any mitigation strategies that would protect them, and any they were already employing and why. Our final question asked users for an honest account of whether they had researched thermal attacks while completing our survey, and what questions their search helped them answer.

3.3 Data Analysis

Since the majority of our survey questions were open ended and gathered qualitative data, we decided to analyze our responses using open coding [16]. First, two researchers familiarized themselves with the dataset. Next, one researcher proposed a codebook after reading all responses. The codebook was discussed with a second researcher. One coder coded all open-ended responses. The coding was verified by a second researcher by reviewing all code allocations. Disagreements were solved by discussion. Unless otherwise stated, percentages for codes were calculated by taking the ratio of the number of participants who mentioned the code and the number of respondents who completed our survey (N=101). Questions were mostly open ended, with some Likert scale and multiple choice questions. Some of our questions had responses with multiple codes assigned; therefore, it is not necessarily the case that the sum of the percentages reported for a question will equal 100%.

3.4 Participants

Our survey was completed by 101 participants (51 female, 50 male). Participants were aged from 18 to 62 years (M=31, SD=9.7), Most of our participants were of European nationalities (85.2%), and most frequently from the United Kingdom (42.6%). Participants were also from the US, Mexico, Indonesia, Australia, and South Africa. Participants rated their technical expertise level as good (49.5%), average (37.6%), and excellent (12.9%). Most frequently, participants had been educated to graduate level (31.7%), followed by undergraduate (27.7%), high school (22.8%), and post-graduate level (17.8%).

4 RESULTS

In this section, we present the results of our investigation based on the different survey parts.

4.1 Authentication Preferences and Threat Awareness

The majority of participants (53.5%) reported to use fingerprint recognition for authenticating on **devices with touchscreens**. More than a third (38.6%) mentioned to use PINs, followed by face recognition (24.8%), alphanumeric passwords (4.95%), and patterns (4.95%). Eleven percent of participants reported to not secure their devices.

When asked to explain their choice, the majority of participants (55.4%) referred to convenience/usability, followed by security (31.7%). Of those who reported not using any authentication, five participants (4.95%) mentioned they perceive the unlock mechanisms as unnecessary, and three (2.97%) mentioned usability issues. The most popular authentication method for technical **devices with keyboards** (e.g., laptops, desktop PCs) were alphanumeric passwords (62.4%) followed by PINs (18.8%), fingerprint recognition (4.95%), and face recognition (1.98%). 20.8% did not lock at least one of their devices with a keyboard/keypad attached. The most frequently stated reasons for this choice were convenience/usability (28.8%) and security/privacy (22.8%). A third of the participants (36, 35.6%) thought that password or PIN authentication offers sufficient security for their devices with keypad or keyboard input. However, 29 participants believed that this heavily depends on the context, e.g., the practices users follow regarding passwords (11.9%), such as their strength, reuse, or how well they are kept secret. 26 participants (25.7%) felt that these authentication methods were

not secure, with 15 (14.9%) justifying their choice with reasons including that they can be guessed, hacked or attacked (9.9%). Five participants (4.95%) were unsure or did not know whether these methods offered sufficient security.

The majority of participants (62.4%) could not describe methods which could be used by an attacker to bypass authentication mechanisms on keyboard or keypad devices. However, 21 participants (20.8%) were aware of malicious software as a means of bypassing these mechanisms, with 8 participants (7.9%) naming key-loggers or describing their function in their response.

4.2 Unattended Scenarios

In this section, we asked whether our participants had ever left their device unattended for a short time with others around, and to describe this situation if they had.

The majority of participants (59, 58.4%) reported to have left their **touchscreen device** unattended around others. Of those, 46 (77.97%) mentioned the locations, with libraries and hospitality settings being most common (17), followed by working/university environments (14), at home (28.3%), at parties (19.6%), and at trusted people's homes (8.7%). Thirty participants (63.8%) mentioned the people who they left their devices around, mostly friends (24/30,80%), and family/partner (14/30, 46.7%).

4.3 In Public Authentication

4.3.1 Authenticating on a Mobile Device In Public Spaces. The most frequently mentioned risk when unlocking mobile device in the public was shoulder surfing (66.3%), followed by physical theft (17.8%), and the risk of an attacker first shoulder surfing authentications and then stealing the device (11.8%). Other risks mentioned include using public Wi-Fi's (7.9%), and that authentications could be recorded (4.95%). Eleven participants (10.9%) reported to be not aware of any risks of authenticating on their device mobile device in public spaces.

Unsurprisingly, participants most frequently mentioned to take precautions which would help in preventing shoulder surfing,such as preventing observers from seeing what is being typed on screen (25, 24.8%) and using alternative authentication mechanisms which are perceived to be harder to shoulder surf (24, 23.8%).

4.3.2 Providing Authentication Details into a Public Computer. The most frequently mentioned risk in this scenario was the possibility of authentication details being saved on the device or websites (29.7%), followed by shoulder surfing (22.8%), various types of malware being installed on the device (21.8%) including spyware and key-loggers, and the fact that others will have access to the device (15.8%).

Participants most frequently described to take precautions which fell into the category of secure browsing or usage habits (44.6%), such as using VPNs, only visiting secure sites, private browsing/clearing of browsing data, and avoiding completing sensitive transactions on public computers. Other precautions mentioned include avoiding to leave their device unattended and to ensure they are logged out properly (21.8%), avoiding the use of public Wi-Fi (19.8%), being aware of surroundings (11.9%), and using strategies or techniques to combat shoulder surfing (7.9%), such as shielding the screen or keyboard.

4.3.3 Providing Authentication Details via Keypad or Keyboard in Public. Most participants (78, 77.2%) perceived shoulder surfing as the most pressing threat when using a keyboard in public, while some participants explicitly mentioned that they are worried about fake ATM machines (15.8%) or ATMs that are recorded by cameras (15.8%). Other named risks include theft of cards, money or authentication details, theft of both their PIN and bank card, and key-loggers (5.9% each), being subjected to physical attacks or harm (2.97%), or hackers and scammers (1.98%). 7.92% did not percieve a threat or know of any.

Participants most frequently reported to take precautions against shoulder surfing, such as covering PIN entry (65.4%) or paying more attention on the surroundings (29.7%).Some participants (9.9%) reported to take no precautions or were unsure about this. Only two precautions which have been proposed in the literature for mitigating thermal attacks [12] were mentioned. One participant each referred to wearing gloves and pressing extra buttons after authentication, but none of them related those precautions to the risk of thermal attacks.

4.4 Thermal Camera Considerations

After concluding the questionnaire sections concerning behavior and authentication, participants proceeded to answer questions on their familiarity with thermal imaging. The majority of participants knew about thermal cameras (85.1%). The most common characteristic was that it detects or senses heat or temperature in some way (73.3%). The majority of participants had never used a thermal camera before (91.1%). In terms of price estimates, participants most often felt thermal cameras would cost in the range of £500-£1500 (38.6%), followed by £15-£249 (30.7%), £249-£499 (12.9%) and over £1500 (8.9%).

Participants most frequently described thermal cameras being used for safety and security purposes (24.8%), for places such the home, banks, airports. The next most popular uses were by the emergency services (18.8%), such as by firefighters to find people in buildings, followed by to improve vision at night or in low light and dark conditions (17.8%). Medical uses were also described (12.9%), along with finding people in emergency situations (10.9%), measuring heat or temperature for non-medical purposes (10.9%), finding people or animals (9.9%), finding missing persons (7.9%), and for conducting wildlife, agricultural or nature activities such as hunting (5.9%).

4.5 Thermal Attack Scenario

4.5.1 Scenario: Conducting Thermal Attacks. After viewing the video demonstration on thermal attacks [2], 64.4% reported that the person on the right was spying on the other person's screen. Participants also felt the person was reading personal information on the screen, such as notifications (11.9%), holding an object above or placing it on the phone or desk (8.9%) and taking a picture of or scanning the screen (7.9%). Some participants thought the person on the right was showing no malicious action (10.9%).

When asked which security or privacy risks they could identify from the scenario presented, the risk mentioned the most was unauthorized access to the device (58.4%). This was followed by phone theft (14.9%), the risk that the phone is left unlocked or

unattended (12.9%) or theft of data or personal information (7.9%). Only two participants (1.98%) described thermal attacks as a risk present.

4.5.2 Smartphone Image: Perceived Effectiveness of Thermal Images. The vast majority of participants recognized that the picture showed a thermal image (88.1%). Nine participants (8.9%) provided vague answers or did not interpret the question correctly, and three participants did not know how the image was created.

4.5.3 Thermal Attack Scenario. Only a few participants (6.9%) said they had been made aware of thermal attacks before taking our survey, with 93.1% of participants unaware. 83.2% of participants believed thermal attacks pose a serious threat to mobile devices. 81.2% believed that PINs are not secure given thermal attacks are possible. 16.8% believed that thermal attacks do not pose a serious threat to mobile devices, and that PINs are secure (18.8%).

Participants were split over the likelihood of being a victim of a thermal attack (mean=2.85, SD=1.68). Participants were asked to provide their assessment of the level of risk thermal attacks pose towards four common authentication mechanisms by allocating a risk rating (low, medium, or high) to each. For authentication patterns, the most common risk rating was high, selected in 64.4% of cases. For fingerprint recognition, the most popular rating was low (74.3%). The difference in risk ratings given to passwords, however, were less discrete, with the most popular rating being high (47.5%), followed closely by medium (40.6%). PINs received a high risk rating in 83.2% of cases.

Biometrics were the most frequently mentioned unlock mechanism seen as immune to thermal attacks, with 81 participants (80.2%). These included face-ID (46.5%), fingerprints (33.7%) retinal/iris/eye (15.8%), and voice recognition (4.95%). Some participants also perceived passwords which were longer or contained repeated or complex characters to be immune (3.96%).

4.5.4 Mitigation Strategies. When asked about mitigation strategies, one-fifth of participants mentioned obscuring heat signatures physically, e.g., by adding extra types. Further, 20.8% mentioned not leaving their device unattended. Participants further mentioned using alternative authentication mechanisms (19.8%), such as face-ID or fingerprint, covering their screen (7.9%), authenticating using objects instead of their fingers (6.9%). Participants mentioned touchscreens could be adapted to dissipate heat traces by changing temperature after the user has authenticated (5.9%).

We then asked participants which of these mitigation strategies they were already employing; the majority of participants (62.4%) was not employing any strategy.

4.5.5 Impact of Thermal Attack Knowledge. We finally asked participants whether they would change their behavior based on the information they learned during the study. The majority of participants reported they were either somewhat or extremely likely (N=54, 53.5%) to change their behavior as a result of what they had learned about thermal attacks from taking our survey, with somewhat or extremely unlikely being chosen by 28 participants (27.7%). Nineteen (18.8%) were neither likely nor unlikely.

Finally, participants were asked to describe these behavioral changes, if any. Overall, 66 participants (65.3%) described changes they would make to protect themselves against thermal attacks. The difference mentioned most frequently was to stop leaving their devices unattended, being more cautious when they do, and keeping their devices close (26.7%). This was followed by adopting authentication mechanisms they believe are thermal attack resistant or using these mechanisms more often (18.8%). However, 29 participants (28.7%) provided answers suggesting they had no intention of making changes.

5 DISCUSSION

Thermal attacks require specific preconditions to be executed successfully. Further, users will only defend themselves from risks that they are aware of [11]. In our survey study, we captured the user's awareness of thermal attacks, their behavior when interacting with devices, and preferences of authentication schemes. Overall, we can conclude that users are not aware of thermal attacks; they commonly behave in a way that puts them at risk and prefer authentication methods that have been demonstrated to be susceptible to thermal attacks.

5.1 Authentication Methods Vulnerable to Thermal Attacks Remain Popular

Research into thermal attacks has demonstrated their threat towards a variety of authentication schemes [1, 12]. The results of our survey show that these remain a popular choice among users (Section 4.1). About half of our participants made use of either PINs, patterns to secure touchscreen devices. Almost two-thirds of participants made use of passwords to secure their devices with keyboards.

Despite the risk thermal attacks pose towards these authentication mechanisms, most often, participants believed they offer sufficient security for their devices. Of those who did not believe they offered sufficient security, none of these participants suggested thermal attacks as a reason behind their choice of authentication scheme. Further, most participants were unaware of any methods to breach these authentication mechanisms based on PINs or patterns on smartphones and passwords or PINs on keyboard devices.

Participants considered PINs, patterns, and passwords to be at the highest risk from thermal attacks, which is consistent with related work [1, 12]. In most cases, participants felt that thermal attacks would pose no or low risk to fingerprint authentication and face recognition. However, this is not necessarily true in reality, as some of the most popular implementations of fingerprint and face recognition on smartphones require a backup authentication method which is often a PIN. It is, therefore, possible that an attacker intentionally attempts to login using their incorrect biometrics multiple times to activate the backup authentication [26], on which they could conduct a thermal attack.

This suggests not only a lack of awareness of the threat of thermal attacks but a lack of awareness of how these mechanisms could be attacked in general. Based on that, we can conclude that the preconditions **P1** (*the authentication scheme must use the knowledge factor (e.g., alphanumeric password, pattern, or PIN)*) and **P4** (*awareness*) for thermal attacks are fulfilled for a majority of users.

5.2 Devices Are Left Unattended In Locations Where Thermal Attackers Could Roam.

Our findings show that more than half of participants leave their touchscreen devices unattended around others (Section 4.2). Devices are frequently left in public places, such as hospitality settings or working and education environments.

When asked about ways in which attackers could exploit these unattended scenarios to gain unauthorized access to their devices, participants failed to recognize that thermal attacks could be used for this purpose. Participants described a variety of methods, including physical theft, malware installation, and using passwords that had already been shoulder surfed. Two participants (1.98%) showed awareness of smudge attacks [5], but none of our participants described thermal attacks.

Overall, this supports the preconditions **P2** and **P3** that require the devices to be left unattended in a specific spot unattended. However, one might argue that many participants left their devices with others, such as friends and family. While this could be a protection method, previous work highlighted the possibility of insider threats [22]. This supports the precondition **P4** (*awareness*). If there is only minimal interaction in such situations, precondition **P5** is also given.

5.3 Thermal Attacks Are Not Recognized as a Public Authentication Risk

When asked to describe the risks present while authenticating in public environments, none of our participants described thermal attacks. However, participants described a variety of risks linked to the presence of other people, such as shoulder surfers, the possibility of others installing malware on the device, and the fact that others have access to the device in general, but none of our participants were aware that thermal attackers could be present and could exploit this shared access to recover their authentication details. While this does not support precondition **P4** (*awareness*) directly related to thermal attacks, the participants were overall aware of more well-known attacks, such as shoulder surfing. The high awareness of shoulder surfing and the high adoption of precautions designed to prevent it shows that shoulder surfing is a risk which users perceive as relevant and protect themselves against. This is understandable, as shoulder surfing has been found to be a privacy threat that is common in everyday life [8], and so our participants are likely to have experienced shoulder surfing themselves.

However, we also found that some participants were aware of risks but showed a lack of concern for them by not adopting precautions to mitigate them. Nineteen participants identified shoulder surfing as a risk of unlocking their mobile devices in public, and over half of these participants did not adopt precautions, showing a lack of concern. This is consistent with the findings from prior work [32] that found participants are aware of the privacy risks of smart home devices but were not concerned about them in their daily lives. This suggests that educating users about the risk of thermal attacks may not necessarily lead to them adopting mitigation strategies against them if they do not feel concerned about thermal attacks.

5.4 The Affordability and Availability of Thermal Cameras are Underestimated

Most of our participants had heard of thermal cameras before and were able to describe various characteristics of them, but the overwhelming majority had never used one before. The majority of participants did overestimate the price of a thermal camera compared to reality. Therefore, it is possible that many people do not consider thermal attacks as a relevant risk due to their perception of thermal attacks being more expensive to carry out than they actually are, and thus less likely a threat.

5.5 There is little Awareness of Thermal Attacks

When presented with a scenario showing a person conducting a thermal attack on an unattended smartphone, more than half of participants recognized that the activity of the attacker was negative or malicious, but only two participants were able to recognize a thermal attack. Some participants suggested that the person was only curious or that their behavior was normal or neutral, suggesting they would not be concerned. This supports the claim that most participants lacked awareness of thermal attacks as a threat and lacked understanding of how they are conducted.

When we informed participants about what thermal attacks are, only seven participants (6.9%) said they had heard of them before taking our survey. However, 22 participants (21.8%) provided thermal attacks as malicious use of thermal cameras, which is interesting, as this suggests that some participants could imagine thermal attacks being possible, but had not actually heard of them before or seen evidence of them being possible.

Most participants believed thermal attacks pose a serious threat to the security of mobile devices and that PINs are not secure, given thermal attacks are possible. However, large proportions of participants felt extremely unlikely or somewhat unlikely to fall victim to a thermal attack, and in a large number of cases, participants agreed or strongly agreed that a thermal attack would require significant technical expertise to conduct. This again supports **P4**.

5.6 There is little awareness of Mitigation Strategies and an Overestimation of Biometrics' Effectiveness

Sixteen participants believed that making use of fingerprint or face recognition biometrics would prevent thermal attacks on a touchscreen, and 12 participants made use of these as a mitigation strategy against thermal attacks. As stated above, a thermal attack would still be possible on the fallback authentication [26].

In most cases, participants mentioned mitigation strategies that they believed would protect touchscreens from thermal attacks, some of which have been recommended in previous work to protect against keyboards and keypads, such as wearing gloves [12] or adding extra types after entering your password [12, 30]. However, a large number was unaware of mitigation strategies overall. Wearing gloves is not always practical and hence does not offer a viable solution. Further keypresses might still be recognized. Hence, defending users from thermal attacks requires more in-depth research on possible mitigation strategies.

Methods that raise in-situ awareness of other types of attacks can be adapted to for thermal attacks. For example, detecting that the user's behavior is likely to make them vulnerable to attacks (e.g., because they typed a password and then left their device idle) can trigger the system to alert the user. There has been many studies on different ways to raise awareness of side channel attacks [24, 33]

6 LESSONS LEARNED AND RECOMMENDATIONS

Our study shows that the preconditions of thermal attacks can be met in users' daily lives. Intuitive mitigation strategies might be impractical or not effective. We conclude with five lessons learned and future research directions.

(1) **Thermal attacks are a realistic threat:** Based on the preconditions of thermal attacks that are met in the users' daily lives, we conclude that thermal attacks are a realistic threat that probably is limited in occurrence because attackers are not yet aware of it. Thermal cameras are somewhat affordable to anyone, and there are many opportunities to carry out thermal attacks.
(2) **Lack of awareness and misunderstandings put the users at risk:** The results of our survey have uncovered that there exists a general lack of awareness about thermal attacks, a lack of effective mitigation strategies and many thermal attack misunderstandings among the general public. People also put themselves at risk of thermal attacks by leaving their devices unattended in places where thermal attacks could take place.
(3) **Public environments have a high risk of thermal attacks:** Our results show that people put themselves at risk of thermal attacks in public environments, where also other side-channel attacks might occur. Operators of such environment, therefore could make people aware of the risks of their actions, for instance, by information signs and warning in public user interfaces.
(4) **Thermal attack education is necessary among users and thermal camera manufacturers, and likely to be successful:** The fact that over half of our participants indicated to adapt their behavior after learning of thermal attacks through our study is promising. Informative education materials on thermal attacks, similar to other attacks should be developed and distributed. Our results suggest that methods aiming to improve thermal attack awareness and provide thermal attack education would be effective in encouraging the public to take the threat seriously and protect themselves, as it seems that our survey managed to encourage the majority of our participants to do so, even though it was not designed to carry out this specific purpose. While we focused on users in this study, similar to how manufacturers of printers integrate mechanisms to prevent using printers to forge money bills, manufacturers of thermal cameras may also program their cameras to distort, block or prevent taking thermal images of input interfaces, such as keyboards.
(5) **The development of usable attack-resistant authentication schemes is required:** Most authentication schemes are not resistant against thermal attacks. Mitigation strategies might be difficult to use or ineffective. This creates a demand for authentication schemes that are usable and resilient against many types of side-channel attacks. Prior work proposed authentication methods that are resilient to thermal attacks by design (e.g., gaze-based input [13–15]); however, they are often not widely adopted. Other examples include schemes that resist smudge attacks [25, 29]. Alternatively, methods that predict vulnerability to thermal attacks based on typing behavior may provide a means to resist attacks while maintaining high usability.

7 CONCLUSION

In this work, we conducted an online study with 101 participants to investigate the risk of thermal attacks in users' daily lives. Our results suggest that users frequently leave their touchscreen devices unattended. Furthermore, users are often at risk of thermal attacks due to their authentication method, allowing attackers to use thermal traces to reconstruct previously entered PINS and passwords. Despite the threat of thermal attacks in users' daily lives, only seven participants (6.93%) had heard of thermal attacks. This lack of awareness suggests that users do not apply any countermeasures to thermal attacks as they are unaware of such novel threats. Future research may extend our work to support users' understanding and awareness of thermal attacks and develop thermal attack-resistant input methods that protect users' privacy and security when leaving devices unattended. Furthermore, our sample is skewed towards a Western, Educated, Industrialized, Rich, and Democratic population (WEIRD [18]). Future work is called to broaden the participant recruitment and conduct cross-country/cross-culture comparisons to highlight the potential differences in users' awareness of thermal attacks. We concluded with five lessons learned and recommendations, such as educating users about thermal attacks and developing usable attack-resistant authentication schemes, to advance research in this area and eventually protect users against thermal attacks.

ACKNOWLEDGMENTS

This work was supported by the University of Edinburgh and the University of Glasgow jointly funded PhD studentships, by an EPSRC New Investigator award (EP/V008870/1) and by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, Denver Colorado USA, 3751–3763. https://doi.org/10.1145/3025453.3025461
[2] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. https://www.youtube.com/watch?v=a2Q64XmZpc4&ab_channel=MohamedKhamis last accessed 9 September 2021.
[3] Yasmeen Abdrabou, Yomna Abdelrahman, Ahmed Ayman, Amr Elmougy, and Mohamed Khamis. 2020. Are Thermal Attacks Ubiquitous?: When Non-Expert Attackers Use Off the shelf Thermal Cameras. In *Proceedings of the International Conference on Advanced Visual Interfaces*. ACM, Salerno Italy, 1–5. https://doi.org/10.1145/3399715.3399819

[4] Yasmeen Abdrabou, Reem Hatem, Yomna Abdelrahman, Amr Elmougy, and Mohamed Khamis. 2021. Passphrases Beat Thermal Attacks: Evaluating Text Input Characteristics Against Thermal Attacks on Laptops and Smartphones. In *IFIP Conference on Human-Computer Interaction*. Springer, 712–721.

[5] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies* (Washington, DC) *(WOOT'10)*. USENIX Association, USA, 1–7.

[6] Xavier Bellekens, Andrew Hamilton, Preetila Seeam, Kamila Nieradzinska, Quentin Franssen, and Amar Seeam. 2016. Pervasive eHealth services a security and privacy risk awareness survey. In *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*. 1–4. https://doi.org/10.1109/CyberSA.2016.7503293

[7] Frank Breitinger, Ryan Tully-Doyle, and Courtney Hassenfeldt. 2020. A survey on smartphone user's security choices, awareness and education. *Computers & Security* 88 (Jan. 2020), 101647. https://doi.org/10.1016/j.cose.2019.101647

[8] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, Denver Colorado USA, 4254–4265. https://doi.org/10.1145/3025453.3025636

[9] Sandra Gabriele and Sonia Chiasson. 2020. Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–12. https://doi.org/10.1145/3313831.3376651

[10] Marian Harbach, Sascha Fahl, and Matthew Smith. 2014. Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In *2014 IEEE 27th Computer Security Foundations Symposium*. IEEE, Vienna, 97–110. https://doi.org/10.1109/CSF.2014.15

[11] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. 213–230. https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach

[12] Tyler Kaczmarek, Ercan Ozturk, and Gene Tsudik. 2019. Thermanator: Thermal Residue-Based Post Factum Attacks on Keyboard Data Entry. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. ACM, Auckland New Zealand, 586–593. https://doi.org/10.1145/3321705.3329846

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

[14] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-based Authentication on Situated Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 174 (Dec. 2018), 21 pages. https://doi.org/10.1145/3287052

[15] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*. 13–19.

[16] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. Chapter 11 - Analyzing qualitative data. In *Research Methods in Human Computer Interaction (Second Edition)*, Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser (Eds.). Morgan Kaufmann, Boston, 299–327. https://doi.org/10.1016/B978-0-12-805390-4.00011-X

[17] Duo Li, Xiao-Ping Zhang, Menghan Hu, Guangtao Zhai, and Xiaokang Yang. 2018. Physical password breaking via thermal sequence analysis. *IEEE Transactions on Information Forensics and Security* 14, 5 (2018), 1142–1154.

[18] Sebastian Linxen, Christian Sturm, Florian Brühlmann, Vincent Cassau, Klaus Opwis, and Katharina Reinecke. 2021. How WEIRD is CHI?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 143, 14 pages. https://doi.org/10.1145/3411764.3445488

[19] Diogo Marques, Tiago Guerreiro, Luis Carriço, Ivan Beschastnikh, and Konstantin Beznosov. 2019. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300819

[20] Florian Mathis, Kami Vaniea, and Mohamed Khamis. 2021. *Observing Virtual Avatars: The Impact of Avatars' Fidelity on Identifying Interactions*. Association for Computing Machinery, New York, NY, USA, 154–164. https://doi.org/10.1145/3464327.3464329

[21] Keaton Mowery, Sarah Meiklejohn, and Stefan Savage. 2011. Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks. (2011), 8. http://cseweb.ucsd.edu/~smeiklejohn/files/woot11.pdf

[22] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2013. Know your enemy: the risk of unauthorized access in smartphones by insiders. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI '13)*. Association for Computing Machinery, New York, NY, USA, 271–280. https://doi.org/10.1145/2493190.2493223

[23] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153–163.

[24] Alia Saad, Michael Chukwu, and Stefan Schneegass. 2018. Communicating Shoulder Surfing Attacks to Users. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 147–152. https://doi.org/10.1145/3282894.3282919

[25] Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2014. Smudgesafe: Geometric image transformations for smudge-resistant user authentication. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 775–786.

[26] Christian Tiefenau, Maximilian Häring, Mohamed Khamis, and Emanuel von Zezschwitz. 2019. "Please enter your PIN" - On the Risk of Bypass Attacks on Biometric Authentication on Mobile Devices. arXiv:1911.07692 http://arxiv.org/abs/1911.07692

[27] S. Trewin, C. Swart, L. Koved, and K. Singh. 2016. Perceptions of Risk in Mobile Transaction. In *2016 IEEE Security and Privacy Workshops (SPW)*. 214–223. https://doi.org/10.1109/SPW.2016.37

[28] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, San Jose California USA, 3748–3760. https://doi.org/10.1145/2858036.2858546

[29] Emanuel von Zezschwitz, Anton Koslow, Alexander De Luca, and Heinrich Hussmann. 2013. Making Graphic-Based Authentication Secure against Smudge Attacks. In *Proceedings of the 2013 International Conference on Intelligent User Interfaces* (Santa Monica, California, USA) *(IUI '13)*. Association for Computing Machinery, New York, NY, USA, 277–286. https://doi.org/10.1145/2449396.2449432

[30] Wojciech Wodo and Lucjan Hanzlik. 2016. Thermal Imaging Attacks on Keypad Security Systems:. In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications*. SCITEPRESS - Science and Technology Publications, Lisbon, Portugal, 458–464. https://doi.org/10.5220/0005998404580464

[31] Michal Zalewski. 2005. Cracking safes with thermal imaging. https://lcamtuf.coredump.cx/tsafe/

[32] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. (2017), 17.

[33] Huiyuan Zhou, Khalid Tearo, Aniruddha Waje, Elham Alghamdi, Thamara Alves, Vinicius Ferreira, Kirstie Hawkey, and Derek Reilly. 2016. Enhancing Mobile Content Privacy with Proxemics Aware Notifications and Protection. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1362–1373. https://doi.org/10.1145/2858036.2858232