Conducting and Mitigating Portable Thermal Imaging Attacks on User Authentication using AI-driven Methods

SHAUN ALEXANDER MACDONALD, NORAH ALOTAIBI, MD SHAFIQUL ISLAM, and MOHAMED KHAMIS, University of Glasgow, UK

Thermal cameras have become portable enough to integrate into wearables, such as glasses, and can be used maliciously to infer passwords observing heat traces left on keyboards, keypads and screens. While prior work showed how AI-driven approaches can be used to further enhance the effectiveness of these attacks, we use similar approaches to detect vulnerable interfaces and obfuscate heat traces to defend against thermal attacks. At our Augmented Humans 2023 demo, attendees will have the chance to use a thermal camera to observe thermal traces on a keyboard, and observe how machine learning can both automatically identify keys pressed based and identify, then obfuscate, thermal images of a keyboard to prevent thermal attacks. This demo will provoke thought and discussion about the security risks presented by discrete, wearable thermal cameras and how these risks can be mitigated by both designers and users.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; **Privacy protections**; • **Computing methodologies → Computer vision**; **Machine learning**.

Additional Key Words and Phrases: Thermal Attacks, Usable Security, Machine Learning

ACM Reference Format:
Shaun Alexander Macdonald, Norah Alotaibi, Md Shafiqul Islam, and Mohamed Khamis. 2023. Conducting and Mitigating Portable Thermal Imaging Attacks on User Authentication using AI-driven Methods. In *Augmented Humans Conference (AHs '23), March 12–14, 2023, Glasgow, United Kingdom.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3582700.3583698

1 INTRODUCTION

Thermal cameras have become increasingly affordable and portable in recent years, and are on the cusp of easily augmenting users in the wild [10]. Consumers can purchase a thermal camera for only $150 to discretely augment their smartphones, and researchers have successfully integrated thermal cameras into wearable glasses and displays [2, 3, 10] (see Figure 1). This raises security concerns, however, as thermal cameras have been shown capable of enabling *thermal attacks* [1, 8, 9, 16]. This category of effective side-channel attacks functions by capturing a thermal image of a keyboard, keypad or touchscreen following user authentication, which then reveals heat traces that indicate the keys or areas pressed, and in what order, allowing deduction of the user's password or pattern. A near future where thermal cameras can be discretely worn and used therefore poses new security risks for commonly used interfaces, like ATMs, keyboards and smartphones; risks which designers must understand and be prepared to account for.

In the course of three ongoing research projects we are investigating the security and privacy risks of thermal imaging and how they can be mitigated, in order to tackle this emerging problem space. Prior work has shown thermal attacks can be used to identify passwords are visually inspected by non-experts [4, 17] or more accurately when analysed following image processing [1, 16]. Our research builds on prior work by assessing how machine learning, an increasingly accessible technology, may be used by attackers to automate the identification of authentication interfaces and deduction of passwords, codes or patterns from thermal traces. Our approach is to then leverage machine learning in a defensive capacity by automatically identifying vulnerable interfaces and mitigate thermal attacks upon them,

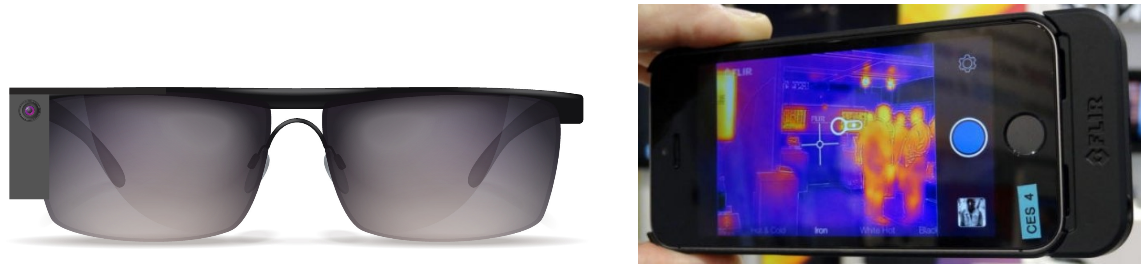

Fig. 1. Examples of how thermal cameras are becoming more portable, discrete and usable in everyday scenarios Left: Illustration of possible future wearable thermal camera, based on current research prototype [10]. Right: Thermal camera smartphone add-on [13].

while not otherwise inhibiting the function of thermal cameras. This Augmented Humans demonstration will raise awareness of potential ubiquity of thermal attack risk, demonstrate our mitigation approaches and enable attendees to explore this topic from several angles. They will be able to experience performing thermal attacks and observe how machine learning can automate the detection of, and attacks on, vulnerable interfaces. Additionally, attendees will be able to try user-centered mitigation strategies and observe their efficacy, as well as observe how machine learning can enable automated obfuscation of thermal feeds featuring sensitive interfaces.

2 MOTIVATION AND IMPACT

First investigated in 2011 by Mowery [16], research in the years since have repeatedly found thermal imaging effective at conducting side-channel attacks on keyboards [8], keypads [14] and touchscreens [1]. Unlike shoulder surfing attacks which require real-time observation of user authentication, thermal attacks can be conducted in the window of time after the victim has entered their details and then left their device unattended, making them easier to perform. Prior work has found passwords can be retrieved by a thermal image taken within 60 seconds [12, 16], and consistently from images taken within 30-40 seconds [1, 12, 17]. Furthermore, the order in which regions of interest were touched (be it keys or areas of a touchscreen) can be identified by observing which heat traces are least intense to most intense [1, 16].

While this threat was previously somewhat inhibited by the cost and form factor of thermal cameras, it is now poised to become far more accessible and commonplace concern. Thermal cameras are available for as little as $150, can discreetly augment smartphones and recently also Humans. For example, Faltaous *et al.* and Abdelrahman *et al.* have demonstrated its imminent potential to augment wearable glasses and goggles [2, 3, 10]. Wearable, portal and discrete thermal cameras present an increased security risk in many common real-world scenarios, from public keypads on ATMs, to keyboards in office spaces and smartphones left unattended after being unlocked, without an attacker having to take any overt or noticeable action to indicate they are performing a thermal attack.

This means that, while user-centered mitigation strategies have been proposed, such as pressing one’s hand against the interface to leave masking heat traces [1], priming one’s hands with a cold object [5], or wearing gloves [12], it is also prudent to consider hardware-centered interventions to automatically mitigate this risks. Prior work has investigated changing authentication interfaces to increase resilience to thermal attacks. For example alternative authentication schemes could be employed, such as biometrics [6], mid-air gestures [11], or using a privacy enhanced keyboard (PEK) [15]. Such solutions would, however, require changing to a wide variety of new and legacy interfaces that are distributed on a societal scale, making them impractical to apply or enforce. Instead we propose a solution targeting a single point of failure, by preventing thermal cameras themselves from being used in thermal attacks.

Work by Alotaibi *et al.* has demonstrated the ability for a deep learning object detection model, Mask RCNNs, to automatically detect keyboards and key-presses in a thermal image [7, 8]. This demonstration will display our current research, utilising the same automatic detection to create thermal cameras systems which obfuscate authentication interfaces, preventing thermal attacks as they happen and whether or not they were detected by the potential victim. This solution could form inform future policy or thermal camera design in order to largely eliminate the risk of thermal attacks. In addition to displaying our research and implementation, this demonstration will also raise awareness of ubiquitous thermal attacks, allowing attendees to consider human-centered and system-centered mitigation solutions when designing secure interactions between augmented humans and authentication interfaces.

3 DEMONSTRATION ACTIVITIES AND REQUIREMENTS

The thermal attacks demonstration at Augmented Humans will house two setups consisting in total of two laptops, two external monitors, two external keyboards, one Raspberry Pi, one hand-held FLIR thermal camera, and one OPTRIS thermal camera attached to the table edge by an adjustable arm. Both setups will feature the ability for attendees to interact with the demonstration, as well as additional elements which the demonstrators will present to the attendees.

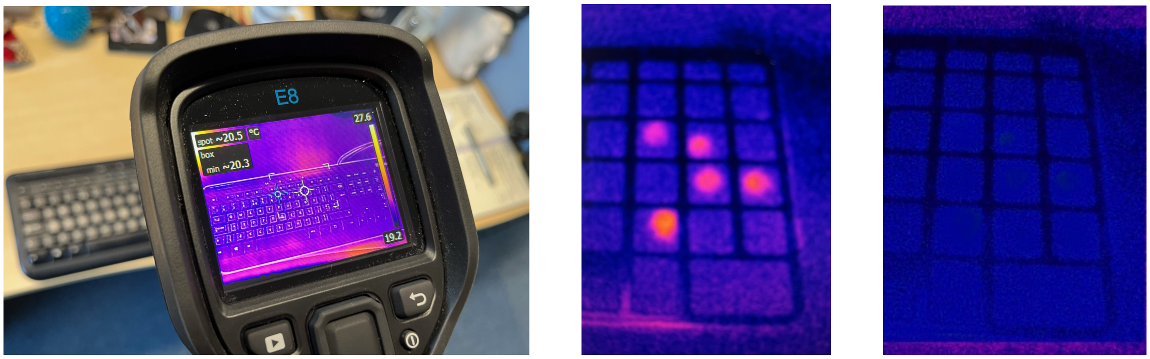

Fig. 2. Setup 1 - Left: The handheld FLIR thermal camera used in, pointed as a keyboard. Middle: Heat traces captured following key presses on a keyboard. Right: Heat traces preemptively obfuscated following identification by machine learning.

The first setup will allow attendees to go hands-on with a portable FLIR thermal camera (see Figure 2) and experience how it can enable people augmented with this technology to observe passwords after they have been entered. Attendees will be able enter example passwords on the external keyboard and then use the camera to see the heat traces they left and identify the keys pressed. Additionally, they will be able try out two thermal attack mitigation strategies proposed in prior work that users can enact themselves: swiping their hands along the keys after entering a password to mask it with additional heat traces and priming their hands on a cold surface (in this case an ice pack) to reduce the thermal traces they leave. They can then observe how these actions impact the thermal image on the camera. Via an external monitor will show how YOLO, a deep learning model running on a Raspberry Pi [1], can use the FLIR to identify keyboards in real time. Due to limitations, we will not be able to conduct live machine learning detection of the keys pressed during the demo, but will display prior examples of thermal images of heat traces on keyboards and how they were identified with machine learning on a laptop.

[1] GitHub Repository for YOLO model: github.com/MdShafiqu/Thermal-Imaging-Project

The second setup will feature an OPTRIS thermal camera mounted via an arm in a fixed position above the desk, facing down to the second external keyboard. The second external monitor and laptop will show the live thermal video feed from the camera which will be used to demonstrate our real-time obfuscation algorithm. As in the first setup, attendees will be able to leave thermal on the keyboard and observe them via the camera feed. However, once the demonstrator activates the obfuscation, attendees will instead observe how the Mask RCNNs deep learning model automatically detects the keyboard [8], allowing application of a filter which hides thermal traces (see Figure 3.) Attendees will be able to move the keyboard around the desk and observe how the obfuscation tracks it in real-time. Due to limitations in processing power the real-time demonstration will not run smoothly, but will still effectively demonstrate the obfuscation technique and how it dynamically can track and detect the keyboard as it moves.

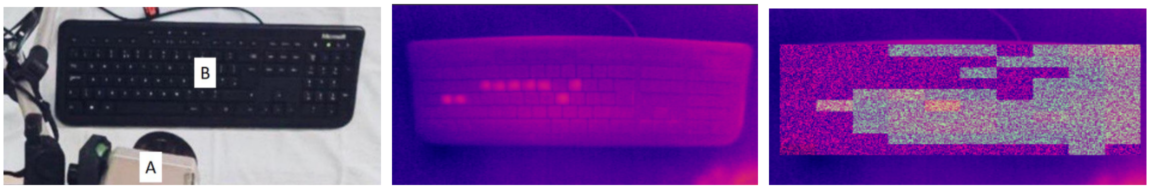

Fig. 3. Setup 2 - Left: An OPTRIS Camera (A) pointing toward an external keyboard (B). Middle: A thermal image of heat traces left on the keyboard following authentication. Right: Pixelation obfuscation filter applied automatically after the machine learning model detects the keyboard.

4 CONCLUSION

As thermal cameras have become highly affordable and portable and can now be integrated into wearable form factors, suggesting a future where they can easily augment users in the wild. Our work on thermal attacks on user authentication draws attention to the security risks of this imminent future and how machine learning can be used to both enhance and prevent these attacks. This interactive demonstration should provoke thought and discussion within the attendees of Augmented Humans 2023 about the security challenges posed by thermal cameras and provide future directions in the form of both user-focused and system-focused mitigation strategies.

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).

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay cool! Understanding thermal attacks on mobile-based user authentication. *Conference on Human Factors in Computing Systems - Proceedings* 2017-May (2017), 3751–3763. https://doi.org/10.1145/3025453.3025461

[2] Yomna Abdelrahman, Pascal Knierim, Pawel W. Wozniak, Niels Henze, and Albrecht Schmidt. 2017. See through the fire: Evaluating the augmentation of visual perception of firefighters using depth and thermal cameras. In *UbiComp/ISWC 2017 - Adjunct Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*. 693–696. https://doi.org/10.1145/3123024.3129269

[3] Yomna Abdelrahman, Albrecht Schmidt, and Pascal Knierim. 2017. Snake view: exploring thermal imaging as a vision extender in mountains. (2017), 1067–1071.

[4] 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 *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3399715.3399819

[5] 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. July (2021), 712–721. https://doi.org/10.1007/978-3-030-85610-6

[6] Yasmeen Abdrabou, Khaled Kassem, Jailan Salah, Reem El-Gendy, Mahesty Morsy, Yomna Abdelrahman, and Slim Abdennadher. 2018. Exploring the usage of EEG and pupil diameter to detect elicited valence. In *Intelligent Human Systems Integration: Proceedings of the 1st International Conference on Intelligent Human Systems Integration (IHSI 2018): Integrating People and Intelligent Systems, January 7-9, 2018, Dubai, United Arab Emirates*. Springer, 287–293.

[7] Norah Alotaibi, Md Shafiqul Islam, Karola Marky, and Mohamed Khamis. 2022. Advanced Techniques for Preventing Thermal Imaging Attacks. In *International Conference on Intelligent User Interfaces, Proceedings IUI*. 18–21. https://doi.org/10.1145/3490100.3516472

[8] Norah Alotaibi, John Williamson, and Mohamed Khamis. 2021. *ThermoSecure: Investigating the effectiveness of AI-driven thermal attacks on commonly used computer keyboards*. Technical Report. https://doi.org/x

[9] Paul Bekaert, Norah Alotaibi, Florian Mathis, Nina Gerber, Aidan Christopher Rafferty, Mohamed Khamis, and Karola Marky. 2022. Are Thermal Attacks a Realistic Threat? Investigating the Preconditions of Thermal Attacks in Users' Daily Lives. In *NordiCHI '22*. Aarhus, 1–9. https://doi.org/10.1145/3546155.3546706

[10] Sarah Faltaous, Mark Wittpoth, Yomna Abdelrahman, and Stefan Schneegass. 2022. HeatGoggles : Enabling Ubiquitous Touch Input through Head-Mounted Devices using Thermal Imaging. *21th International Conference on Mobile and Ubiquitous Multimedia (MUM 2022), November 27â•fi30, 2022, Lisbon, Portugal* 1, 1 (2022), 6–9. https://doi.org/10.1145/3568444.3570597

[11] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS.

[12] Tyler Kaczmarek, Ercan Ozturk, and Gene Tsudik. 2019. Thermanator: Thermal residue-based post factum attacks on keyboard data entry. *AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (2019), 586–593. https://doi.org/10.1145/3321705.3329846 arXiv:1806.10189

[13] Pierre Lecourt. 2015. Flir ONE. https://www.flickr.com/photos/13815526@N02/16051311760/in/photostream/

[14] Duo Li, Xiao Ping Zhang, Menghan Hu, Guangtao Zhai, and Xiaokang Yang. 2019. Physical password breaking via thermal sequence analysis. *IEEE Transactions on Information Forensics and Security* 14, 5 (2019), 1142–1154. https://doi.org/10.1109/TIFS.2018.2868219

[15] Zhen Ling, Melanie Borgeest, Chuta Sano, Jazmyn Fuller, Anthony Cuomo, Sirong Lin, Wei Yu, Xinwen Fu, and Wei Zhao. 2017. Privacy Enhancing Keyboard : Design , Implementation , and Usability Testing. *Wireless Communications and Mobile Computing* 2017 (2017), 1–15.

[16] Keaton Mowery, Sarah Meiklejohn, and Stefan Savage. 2011. Heat of the moment: Characterizing the efficacy of thermal camera-based attacks. *5th USENIX Workshop on Offensive Technologies, WOOT 2011* (2011), 1–8.

[17] Wojciech Wodo and Lucjan Hanzlik. 2016. Thermal imaging attacks on keypad security systems. *ICETE 2016 - Proceedings of the 13th International Joint Conference on e-Business and Telecommunications* 4, Icete (2016), 458–464. https://doi.org/10.5220/0005998404580464