Macdonald, S. A., Farzand, H., Alotaibi, N., Islam, M. S. and Khamis, M. (2023) Change Policy or Users? Mitigating the Security Risks of Thermal Attacks. In: 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), Hamburg, Germany, 23-28 Apr 2023.

Copyright © 2023 The Authors. Reproduced under a Creative Commons Attribution 4.0 International License.

For the purpose of open access, the author(s) has applied a Creative Commons Attribution license to any Accepted Manuscript version arising.

https://eprints.gla.ac.uk/294369/

Deposited on: 15 March 2023

Enlighten – Research publications by members of the University of Glasgow
https://eprints.gla.ac.uk

Change Policy or Users? Mitigating the Security Risks of Thermal Attacks

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

Attacks on passwords by thermal cameras are a poignant example of how emerging technologies can pose unforeseen security risks. Despite being easy to perform and effective, thermal attacks are not commonly understood or counteracted, hence a strategy to mitigate this is required. In this paper, we propose an AI-driven strategy to obfuscate vulnerable interfaces in the view of thermal cameras automatically, then discuss the advantages and limitations of attempting to enforce such a system-centred solution as policy, versus instead attempting to shape user behaviour.

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

ACM Reference Format:

Shaun Alexander Macdonald, Habiba Farzand, Norah Alotaibi, Md Shafiqul Islam, and Mohamed Khamis. 2023. Change Policy or Users? Mitigating the Security Risks of Thermal Attacks. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 3 pages.

1 INTRODUCTION

When new technology becomes available to the general public, it can bring novel and unconsidered security risks. For example, with the introduction of the iPhone in 2007, shoulder surfing became prevalent [7, 9] but various methods such as multimodal authentication [11] assist in overcoming this threat. Similarly, thermal cameras have become increasingly inexpensive, portable and discrete. This is a concern, as they can be effectively used to steal passwords, passcodes and patterns by observing the heat trace left on keyboards [3, 4, 10], keypads [15] or touchscreens [1, 2] after use. The risk posed by *thermal attacks*, and how they can be mitigated, is not well understood by the general public, prompting consideration of how to protect users, either by shaping user behaviour or mitigating the risk at a system level. This paper presents our work, investigating thermal attacks and how they can be mitigated, as a case study, discussing the benefits and drawbacks of designing solutions intended to be instituted as public policy versus user-centred solutions.

2 THE SECURITY THREAT OF THERMAL ATTACKS

The threat of thermal cameras being used to infer passwords was identified in 2011 [15] and researchers have since demonstrated the efficacy of these *thermal attacks* on keyboards [4], keypads [13] and touchscreens [1]. Due to the fact that heat is transferred from the user's fingertips to interfaces that they touch, thermal cameras can observe these residual heat traces on keyboards, keypads or phone screens after authentication. The order in which keys or areas were pressed can be inferred by the relative intensity of heat traces: warmer traces were pressed later, cooler traces earlier, and keys or areas pressed multiple times will be most intense [1, 15].

Thermal attacks work up to 60 seconds after authentication [10, 15], and are consistent under 30 seconds [1, 10, 16], making them hard to detect. Thermal cameras are also becoming more affordable and discrete, as they are available to consumers as a smartphone add-on for £155 [5], and researchers have integrated them into glasses [8]. Recent work shows that scenarios which allow for successful thermal attacks are common [6]. In summary, the availability of discrete

© 2023 Copyright held by the owner/author(s).

thermal cameras presents a societal security risk for which authentication systems and users are not prepared and therefore, mitigation strategies are necessary.

3 THERMAL MITIGATION AS PUBLIC POLICY OR USER-RESPONSIBILITY

Our research on thermal attacks can illustrate the benefits and limitations of designing system-centred, versus user-centred, mitigation policies. First, how could thermal attacks be mitigated by system-level policy change? Authentication interfaces can be made more resilient to thermal attacks in several ways, such as manipulating interface temperature [1], using specific materials [4, 15], or digital interfaces which shuffle key positions [12, 14]. This approach would, however, require the conversion or replacement of all preinstalled interfaces, and regulation of new interfaces being produced, making it a difficult policy to establish or enforce. This motivates instead to pursue a solution which is easier to implement, should it become policy: targeting just the thermal camera. We propose a system that obfuscates vulnerable interfaces in the view of thermal cameras in real time. It has been shown that machine learning can be used to identify authentication interfaces, such as keyboards, in thermal images and camera feeds [4]. Using this automatic detection, filters could be applied to the interface in view to obscure heat traces without otherwise inhibiting the camera's functionality (see Figure 1), similar to how printers are software-blocked from printing images of banknotes.

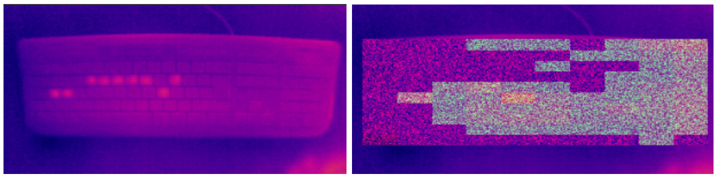

Fig. 1. **Left:** The threat: heat traces on a keyboard after a password is entered, as seen by a thermal camera. **Right:** By using machine learning to detect if a keyboard is in the camera's view, obfuscation filters can be automatically applied.

Alternatively, we could seek to encourage user behaviours resilient to thermal attacks. Research has identified effective examples, including masking heat traces by placing one's hand on the interface after use [1], wearing gloves [10] or using longer passwords with repeated characters [10, 13]. While a system-level solution will not be available to users until it becomes policy, users have agency over solutions which rely on their behaviour and can start using them immediately. The downside, however, is users can freely choose not to adopt these methods, just as people are free to choose '1111' as their PIN code. By contrast, a policy enforcing system-level mitigation would secure most people by default, while requiring no user effort. It would be fallacious to characterise that user-centred solutions are not requiring policy change, as informing users of this new behaviour and installing it in them is a challenge, which may call for a new policy, such as new public information campaigns. Overall, policy enforcing a system-level change may stand the best chance of mitigating a societal risk, in this case of thermal attacks but are subject to resources and negotiation between public and corporate bodies, which can delay or prevent implementation and limit the changes available. While user-centred behavioural change may not be an effective solution, it should still be encouraged as it can provide individuals with immediate agency and can act as a stop-gap solution while awaiting appropriate policy change.

4 ACKNOWLEDGEMENTS

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] 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*. ACM. https://doi.org/10.1145/3399715.3399819

[3] Yasmeen Abdrabou, Reem Hatem, Yomna Abdelrahman, and Amr Elmougy. 2021. Passphrases Beat Thermal Attacks: Evaluating Text Input Characteristics Against Thermal Attacks on Laptops and Smartphones. ACM, 712–721. https://doi.org/10.1007/978-3-030-85610-6

[4] Norah Alotaibi, John Williamson, and Mohamed Khamis. 2022. *ThermoSecure: Investigating the Effectiveness of AI-Driven Thermal Attacks on Commonly Used Computer Keyboards*. Technical Report. New York, NY, USA. https://doi.org/10.1145/3563693 Just Accepted.

[5] Amazon. 2023. *Amazon Listing - PerfectPrime IR203, (IR) Infrared Thermal Imager Camera*. Accessed: 2023-01-13.

[6] 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*. ACM, Aarhus, 1–9. https://doi.org/10.1145/3546155.3546706

[7] 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*. 4254–4265.

[8] 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

[9] Habiba Farzand, Karola Marky, and Mohamed Khamis. 2022. Shoulder Surfing through the Social Lens: A Longitudinal Investigation & Insights from an Exploratory Diary Study. In *Proceedings of the 2022 European Symposium on Usable Security*. 85–97.

[10] 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

[11] Mohamed Khamis, Karola Marky, Andreas Bulling, and Florian Alt. 2022. User-centred multimodal authentication: securing handheld mobile devices using gaze and touch input. *Behaviour & Information Technology* 41, 10 (2022), 2061–2083.

[12] Daniel Kirkwood, Cagdas Tombul, Calum Firth, Finn Macdonald, Konstantinos Priftis, Florian Mathis, Mohamed Khamis, and Karola Marky. 2022. PIN Scrambler: Assessing the Impact of Randomized Layouts on the Usability and Security of PINs. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 83–88. https://doi.org/10.1145/3568444.3568450

[13] 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

[14] 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.

[15] 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.

[16] 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