Thermanator: Thermal Residue-Based Post Factum Attacks on Keyboard Data Entry

Tyler Kaczmarek
tkaczmar@uci.edu
University of California, Irvine

Ercan Ozturk
ercano@uci.edu
University of California, Irvine

Gene Tsudik
gene.tsudik@uci.edu
University of California, Irvine

ABSTRACT

Being warm-blooded mammals, we humans routinely leave thermal residues on various objects with which we come in contact. This includes common input devices, such as keyboards, that are used for entering (among other things) secret information, such as passwords and PINs. Although thermal residue dissipates over time, there is always a certain time window during which thermal energy readings can be harvested from input devices to recover recently entered, and potentially sensitive, information.

To-date, there has been no systematic investigation of thermal profiles of keyboards, and thus no efforts have been made to secure them. This serves as our main motivation for constructing a means for password harvesting from keyboard thermal emanations. Specifically, we introduce `Thermanator`, a new post factum insider attack based on heat transfer caused by a user typing a password on a typical external keyboard. We conduct and describe a user study that collected thermal residues from 30 users entering 10 unique passwords (both weak and strong) on 4 popular commodity keyboards. Results show that entire sets of key-presses can be recovered by non-expert users as late as 30 **seconds** after initial password entry, while partial sets can be recovered as late as 1 **minute** after entry. Furthermore, we find that Hunt-and-Peck typists are particularly vulnerable. The take-away of our work is three-fold: (1) using keyboards to enter passwords is even less secure than previously recognized, (2) post factum (either planned or impromptu) thermal imaging attacks are realistic, and (3) we should either stop using keyboards for password entry, or abandon passwords altogether.

ACM Reference Format:
Tyler Kaczmarek, Ercan Ozturk, and Gene Tsudik. 2019. `Thermanator`: Thermal Residue-Based Post Factum Attacks on Keyboard Data Entry. In *ACM Asia Conference on Computer and Communications Security (AsiaCCS '19), July 9–12, 2019, Auckland, New Zealand.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3321705.3329846

1 INTRODUCTION

Insider attacks are very common, estimated to account for ≈28% of all electronic crimes in industry [11]. This includes some high-profile attacks, such as the 2014 Sony hack [22]. At the same time, it is well known that security of a system is based on its weakest link. Furthermore, it is often assumed that involvement of a fallible (or simply gullible) human user corresponds to this weakest link, e.g., as in Shoulder-Surfing and Lunch-Time attacks. However, other insider attacks that focus on stealing passwords by compromising the user environment, e.g., Acoustic Emanations [1, 7, 19] or Keyboard Vibrations [12], show that the weakest link is a consequence of a law of Physics. However, such insider attacks must occur instantaneously, in real time, in order to succeed. In other words, to exploit them, real-time adversarial presence (whether in person or via a nearby compromised recording device) is required which raises the bar for the attack. This prompts the question: *Are there any observable physical effects of password entry that linger and can therefore be collected* **afterwards***?*

Heat Transfer & Thermal Emanations. Any time two objects with unequal temperatures come in contact with each other, an exchange of heat occurs. This is unavoidable. Being warm-blooded, human beings naturally prefer environments that are colder than their internal temperature. Because of this heat disparity, it is inevitable that we leave thermal residue on numerous objects that we routinely touch, especially, with bare fingers. Furthermore, it takes time for these heated objects to cool off and lose heat energy imparted by human contact. It is both not surprising and worrisome that this includes our interactions with keyboards that are used for entering sensitive private information, such as passwords.

Based on this observation, we consider a mostly unexplored attack space where heat transfer and subsequent thermal residue can be exploited by a clever adversary to steal passwords from a keyboard some time after it was used for password entry. The main distinctive benefit of this attack type is that adversary's real time presence is not required. Instead, a successful attack can occur with after-the-fact adversarial presence: as our results show, many seconds later.

Expected Contributions. In this paper, we propose and evaluate a particular human-based side-channel attack class, called Thermanator. This attack class is based on exploiting thermal residues left behind by a user (victim) who enters a password using a typical external keyboard. Shortly after password entry, the victim either steps away inadvertently, or is drawn away (perhaps as a result of being prompted by the adversary) from the personal workplace. Then, the adversary captures thermal images of the victim keyboard. We examine the efficacy of Thermanator Attacks for a moderately sophisticated adversary equipped with a mid-range thermal imaging camera. The goal of the attack is to learn information about the victim password.

To confirm viability of Thermanator Attacks, we conducted a rigorous two-stage user study. The first stage collected password entry data from 31 subjects using 4 common keyboards. In the second stage, 8 non-expert subjects acted as adversaries and attempted

AsiaCCS '19, July 9–12, 2019, Auckland, New Zealand

ACM ISBN 978-1-4503-6752-3/19/07…$15.00
https://doi.org/10.1145/3321705.3329846

to derive the set of pressed keys from the thermal imaging data collected in the first stage. Our results show that even novice adversaries can use thermal residues to reliably determine the entire set of key-presses **up to 30 seconds** after password entry. Furthermore, they can determine a partial set of key-presses as long as a full minute after password entry. We provide a thorough discussion of the implications of this study, and mitigation techniques against Thermanator Attacks.

1.1 Organization

Section 2 describes assumed Thermanator Attacks and adversarial models. Section 3 describes our methodology, apparatus and subject recruitment. Study results are presented in Section 4 and their implications are discussed in Section 5. Section 6 discusses related work. We conclude the paper in Section 7. Appendix A provides background on thermodynamic concepts, modern keyboards and thermal cameras.

2 ADVERSARIAL MODEL & ATTACKS

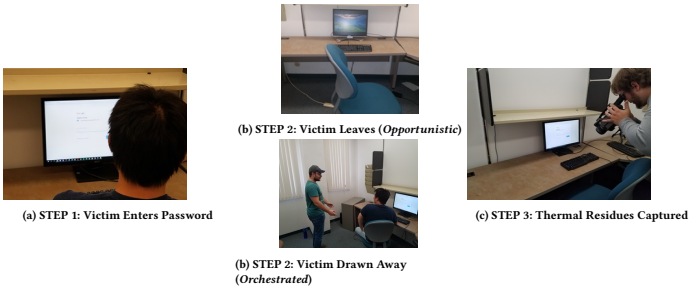

Figure 1: An Example Thermanator Attack

Thermanator is a distinct type of insider attack, where a typical attack scenario proceeds as follows (see also Figure 1):

STEP 1: The victim uses a keyboard to enter a genuine password, as part of the log-in (or session unlock) procedure.

STEP 2: Shortly thereafter, the victim either: (1) willingly steps away, or (2) gets drawn away, from the workplace.

STEP 3: Using thermal imaging (e.g., photos taken by a commodity FLIR camera) the adversary harvests thermal residues from the keyboard.

STEP 4: At a later time, the adversary uses the "heat map" of the images to determine recently pressed keys. This can be done manually (i.e., via visual inspection) or automatically (i.e., via specialized software).

REPEAT: The adversary can choose to repeat STEPS [1-4] over multiple sessions.

The two options in **STEP 2** correspond to two attack sub-types: *opportunistic* and *orchestrated*. In the former, the adversary patiently waits for the situation described in **STEP 2** case (1) to occur. Once the victim leaves (on their own volition) shortly after password entry, the adversary swoops in and collects thermal residues. This strategy is similar to Lunch-Time Attacks. In an *orchestrated* attack, instead of waiting for the victim to leave, the adversary uses an accomplice to draw the victim away shortly after password entry, as in **STEP 2** case (2).

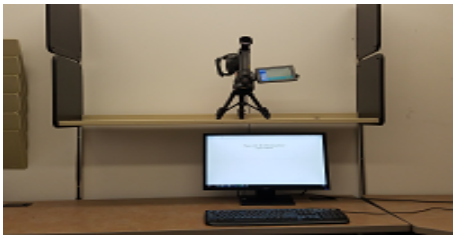

Figure 2: SC620 Apparatus Setup

3 METHODOLOGY

In this section we describe of the experimental apparatus, procedures, and subject recruitment methods.

3.1 Apparatus

The experimental setup was designed to simulate a typical office setting. It was located in a dedicated office in a research building of a large university. Figure 2 shows the setup from the subject's perspective. Equipment used in the experiments consisted of the following readily available (off-the-shelf) components:

I. FLIR Systems SC620 Thermal Imaging Camera[1]: This camera was perched on a tripod 24 $''$ above the keyboard.

II. Four popular and inexpensive commodity computer keyboards: (a) Dell SK-8115, (b) HP SK-2023 (c) Logitech Y-UM76A, and (d) AZiO Prism KB507.

The particular thermal camera that was used in our experiments was chosen to be realistic for a moderately sophisticated and determined adversary. We assume this type of adversary to be an individual, i.e., not an intelligence agency, a nation-state, or a powerful criminal organization. FLIR SC620 Thermal Imager costs approximately US$1,500 used (this model is about 6-7 years old). It automatically records images at the resolution of $640x480$ pixels, with $1Hz$ frequency. Its thermal sensitivity is $0.04K$. The four keyboards were chosen to cover the typical range of manufacturers represented in an average workplace.

3.2 Procedures

`Thermanator` was evaluated using a two-stage user study. The first stage was conducted to collect thermal emanation data, and the second – to evaluate efficacy of Thermanator Attacks. A given subject only participated in a single stage.

3.2.1 Stage One: Password Entry. Recall that Thermanator's goal is to capture thermal residues of subjects **after** keyboard password entry. This is accomplished by having FLIR SC620 take a sequence of images (60 total), one per second, for a total of one minute after initial password entry. This collection of 60 images does **not** represent the requirements for a single attack. In reality, the adversary would arrive as quickly as possible (after the victim leaves the workspace) and take a single thermal image. For strictly experimental purposes, a full minute of thermal data was captured to more accurately model adversaries arriving after some time has elapsed.

Each subject entered 10 passwords on 4 keyboards (40 passwords in total) and each entry was followed by one minute of keyboard

[1]See: http://www.FLIR.com for a full specification.

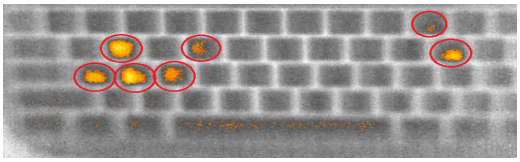

Figure 3: Thermal image of "passw0rd" 20 seconds after entry.

recording (60 successive images) by the FLIR. Each entry took between 10 and 20 seconds. The total duration of the experiment for a Stage 1 subject ranged between 50 and 60 minutes, based on the individual's typing speed and style. Both keyboards and passwords were presented to each subject in random order, in an attempt to negate any side-effects due to subject training or familiarity with the task.

We selected 10 passwords that included both "insecure" and "secure" categories. The former passwords were culled from the top 100 passwords by popularity that adhere to common password requirements, such as Gmail [2]. Whereas, "secure" passwords were created by randomly generating 8-, 10-, and 12-character strings of lower/uppercase letters as well as numbers and symbols that adhere to Gmail restrictions. Our selection criteria resulted in the following 10 candidate passwords:

- **[Insecure]:** "password", "12345678", "football", "iloveyou", "12341234", "passw0rd", and "jordan23",
- **[Secure]:** "jxM#1CT[", "3xZFkMMv|Y", and "6pl;0>6t(OvF".

3.2.2 Stage Two: Data Inspection. The second stage of the experiment has subjects acting as adversaries conducting Thermanator Attacks. Subjects were shown images obtained from the first stage of the experiment, e.g., Figure 3, and were instructed to identify the "lit" regions. Each subject was shown 150 recordings of password entries in random order. On average, a subject could process a single recording in 45 – 60 seconds. Total time for each Stage 2 subject varied in the range of 100 – 130 minutes.

3.3 Subject Recruitment Procedure

Subjects were recruited from the student body of a large public university using a unified Human Subjects Pool designated for undergraduate volunteers seeking to participate in studies such as ours. Subjects were compensated with course credit. Because of this, overwhelming majority of subjects were of college age: 18 – 25. The subject gender breakdown was: 16 male and 15 female. All experiments were authorized by the Institutional Review Board (IRB) of the authors' employer(s), well ahead of the commencement of the study. The level of review was: Exempt, Category II. No sensitive data was collected during the experiments and minimal identifying information was retained. In particular, no subject names, phone numbers or other personally identifying information (PII) was collected. All data were stored pseudonymously.

4 RESULTS

We now describe the results of Stage 2 analysis of thermal images obtained in Stage 1. We divide it into two categories:

- Hunt-and-Peck Typists — those who **do not** rest their fingertips on, or hover their fingers just over, the home-row of keys (i.e. "ASDF" on the left hand, and "JKL;" on the right hand.).
- Touch Typists – those whose fingertips routinely hover over, or lightly touch, the home-row.

The distribution of our Stage 1 subjects to these categories were: 18 hunt-and-peck typists and 12 touch typists. One subject had long acrylic fingernails and instead of typing with fingertips, this person tapped the keys with nail-tips. Since false nails do not have any blood vessels to regulate their temperature, this subject left almost no thermal residue. Consequently, this subject is not included in either Touch or Hunt-and-Peck typist populations.

As it turns out, our study results indicate that the category of the typist is the most influential factor for the quality of thermal imaging data. For each category, we separately analyze "secure" and "insecure" passwords types. Since we did not observe a significant statistical difference between results of different keyboards, results include all keyboards.

For full context, aggregate results (identification rates) from the entire subject population are shown in Figure 4. For clarity's sake, "insecure" passwords are split into two subcategories: alphabetical and alphanumeric. In each graph, "D = 0" refers to average latest time when Stage 2 subjects could correctly identify every keystroke of the entered password, while "D = 1" denotes average latest time when subjects could identify all-but-one keystroke, and so on. "D" is calculated as $D = |(K \cup P) \setminus (K \cap P)|$ where P is the set of pressed keys identified by Stage 2 subjects and K is the set of keys in the actual password. Note that this calculation includes both missed and mis-classified as pressed keys.

4.1 Hunt-and-Peck Typists

Our analysis of Hunt-and-Peck typists was straightforward. Because these typists do not rest their fingertips on (or hover right above) the keyboard home-row, it is readily apparent that each bright spot on the thermal image corresponds to a key-press. However, as discussed below, we encountered some challenges with "secure" passwords.

4.1.1 Insecure Passwords. As Figure 5 shows, analysis of Hunt-and-Peck typists entering "insecure" passwords is straightforward. In fact, in the best-case of "12341234" subjects could correctly recall every keystroke, on average, 45.25 seconds after entry. Even the weakest result, "football" was fully recoverable 25.5 seconds later, on average. This is in line with conventional thought. Hunt-and-Peck typists typically only use their forefingers to type. Because of this, they make contact with a larger finger over a large surface area. Also, since Hunt-and-Peck typists are generally less skilled, they take longer for each keystroke, resulting in longer contact time. These two factors combined yield high-quality thermal residue for Thermanator Attacks.

4.1.2 Secure Passwords. "Secure" passwords are more challenging to analyze. As shown in Figure 5 full recall was possible, on average, up to 31 seconds after recording started, in the best case, and 19.5 seconds, in the worst case. Performance of Stage 2 subjects was uniform in terms of password length: the shortest password was

[2] See: https://support.google.com for details

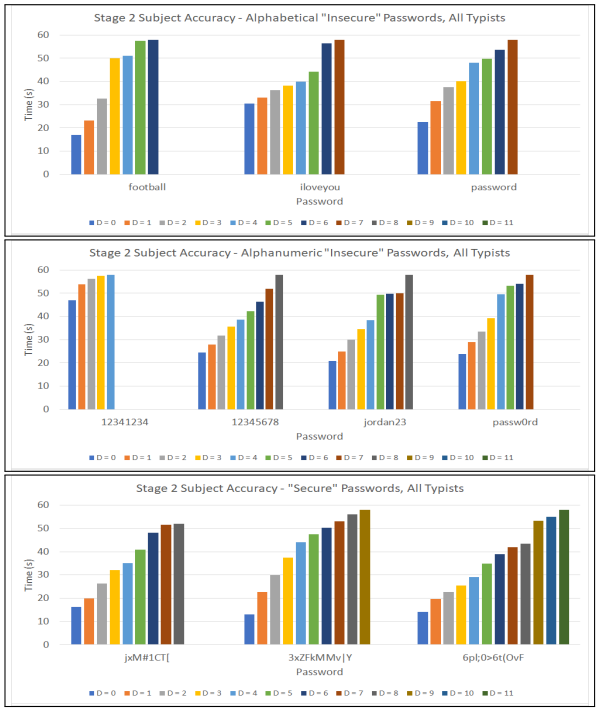

Figure 4: Stage 2 Subject Performance: Alphabetical and Alphanumeric "Insecure" Passwords, and "Secure" Passwords, All Typists

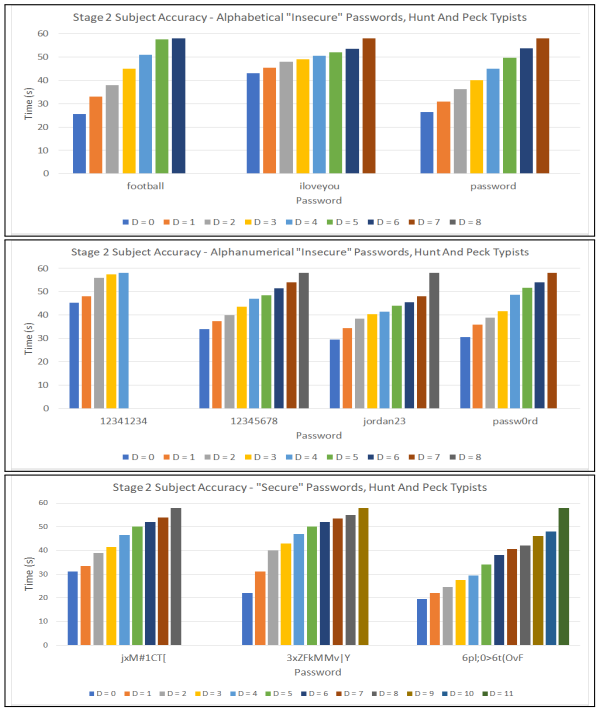

Figure 5: Stage 2 Subject Performance: Alphabetical and Alphanumeric "Insecure" Passwords, and "Secure" Passwords, Hunt-and-Peck Typists

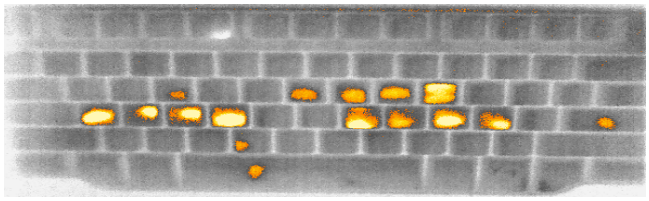

Figure 6: Password "iloveyou" Entered by a Touch Typist.

the easiest to analyze correctly. Anecdotally, this is not surprising. It was quite common for Hunt-and-Peck typists to look back and forth between the characters of a relatively complex "secure" passwords, and their keyboards. This resulted in longer completion times, which left longer time for keycaps to cool off before recording began.

4.2 Touch Typists

Analyzing data from Touch typists was a challenge for Stage 2 subjects. Since a typical Touch typist's fingers are constantly in contact with (or in very close proximity of) the home-row of the keyboard, there are two incidental sources of thermal noise. First, there is thermal residue on the 2 groups of 4 home-row keys: "asdf" and "jkl;" which results from the typist's fingertips. However, whenever typist's fingers rest on the keyboard for a long time, additional observed effects occur outside (though near) the home-row, on the following keys:

```
"qwertgvcxz","][poiuhnm,./"
```

Even though this secondary thermal residue was not as drastic as that on the home-row, it had a more pronounced effect on Stage 2 subjects. In many cases, a subject was uncertain whether a key was lit on the thermal image because it was actually pressed, or because it was simply close to the home-row. This uncertainty in turn led to mis-classification of some keys as unpressed. Also, mis-classification of home-row keys as pressed keys was not counted in the distance. We justify this choice in Section 5.

4.2.1 Insecure Passwords. While more difficult than analysis of "insecure" password for Hunt-and-Peck typists, Stage 2 subjects have moderate success analyzing Touch typists entering "insecure" passwords. As Figure 7 shows, the best average time for full recall was for password: "12341234" at 47.6 seconds, and the worst was for "jordan23", at 17.8 seconds. This follows the notion that Stage 2 subjects were hesitant to classify home-row-adjacent key-presses, e.g., "o", "r" and "n" in "jordan23". Furthermore, this supports the notion that a simple, repeated password such as "12341234" leaves ideal thermal residue.

4.2.2 Secure Passwords. Touch typists entering "secure" passwords were the most difficult for the Stage 2 subjects to analyze. As shown in Figure 7, full recall was only possible, on average, within the first 14.33 – 18.5 seconds. Surprisingly, the password with the smallest window for full recall was "jxM#1CT[". We believe that many Stage 2 subjects were hesitant to classify home-row-adjacent keys in this password as keystrokes (as opposed to thermal noise). This might explain why the window for full recall is so small.

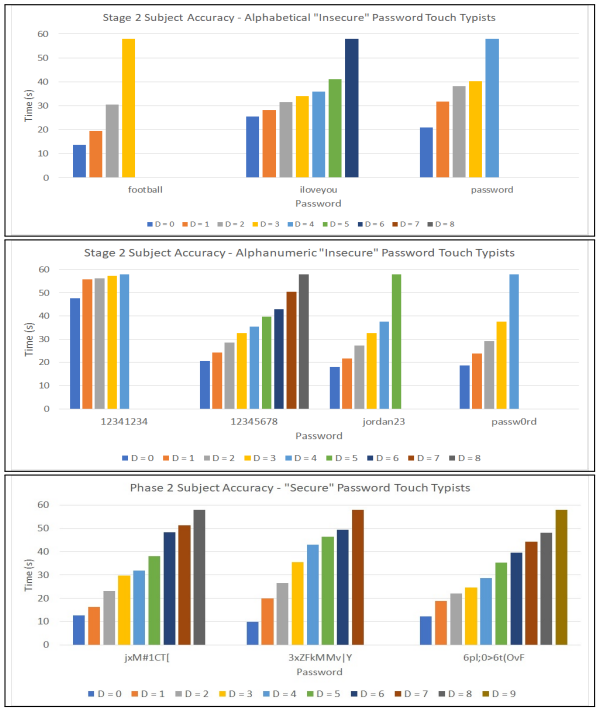

Figure 7: Stage 2 Subject Performance: Alphabetical and Alphanumeric "Insecure" Passwords, and "Secure" Passwords, Touch Typists

5 DISCUSSION

In this section, we break down our observations from Section 4 between two password classes, and among two categories of typists.

5.1 Results with Common Passwords

Stage 2 subjects were particularly adept at identifying passwords that are English words or phrases. Even though we could not reliably detect the exact sequence of pressed keys, ordering can be found indirectly by mapping the set of pressed keys to words. Furthermore, a list of distances between detected keys (characters) and possible words, can be used to reconstruct full passwords from incomplete thermal residues. Finally, the same list of distances can help determine when a key is pressed multiple times. These combinations highlight the threat posed by Thermanator Attacks to already insecure passwords.

5.2 Results with Random Passwords

However, strong results from Stage 2 subjects' identification of English-language words does not extend to secure passwords. First, inability to reliably determine the order of pressed keys can not be mitigated by leveraging the underlying linguistic structure. Moreover, it is unclear whether a given set of emanations represents the whole password, or if some information was lost. Finally, it is impossible to tell if a key was pressed multiple times. However, even with these shortcomings, our subjects managed to greatly reduce the password search space from 72^n to $72^{n-m} * m!$ where n is the total number of characters in the password, and m is the number of identified key-presses. This represents a reduction in search space by a factor of 10^{10} for an 8-character password where the individual keys have been identified.

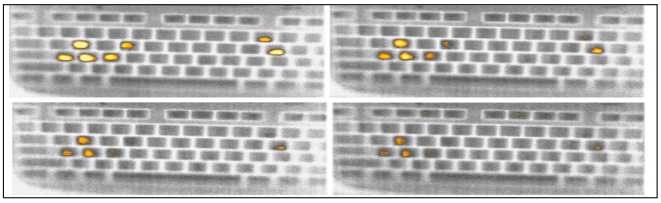

Figure 8: Password "passw0rd" thermal residue after 0 (top left), 15 (top right), 30 (bottom left), and 45 (bottom right) seconds after entry

5.3 Results with Hunt-and-Peck Typists

As described in Section 4.1, Hunt-and-Peck typists are particularly vulnerable to Thermanator Attacks. This is not surprising, given that these less-skilled typists tend to type more slowly, and primarily use their index fingers, which have greater fingertip surface area than ring or pinky fingers [14]. This results in greater heat transfer, due to longer contact duration with a larger contact area. Also, as seen from Figure 3, Hunt-and-Peck typists do not touch any keys that are not part of the password. Therefore, every observed key-press is part of the password.

5.4 Results with Touch Typists

For Touch typists, two factors confuse their thermal residues and make passwords harder to harvest. One is their habit to rest their hands on the home-row, which introduces potential false positives as Figure 6 shows. This is exacerbated by the possibility that any home-row key might actually be part of the password. Because of this, Stage 2 subjects were not penalized for classifying the home-row keys as pressed; they were instructed to identify all keys that looked to them as having been pressed.

Another issue is that Touch typists tend to use all fingers of both hands while typing. This causes two advantages over their Hunt-and-Peck counterparts. First, they touch individual keys for a shorter time, thus transferring less heat to the key-cap. Second, they type much more quickly and also use their ring and pinky fingers. Fingertips of these smaller fingers tend to have 1/2 of the surface area of larger index or middle fingers. Thus, they transfer half of the total heat energy due to conduction during a key-press [14]. Such factors make Touch typists much more resistant to Thermanator Attacks.

5.5 Ordering of Key-Presses

Unfortunately, inspection of thermal images by Stage 2 subjects did not yield any reliable key-press ordering information. This is due to *keystroke inconsistency* in the dynamics of Touch typists. Factors, such as the travel distance between keys and the particular finger used to press a key, result in small differences in the duration, and total surface area of, contact. Since each key-press is distinct, intensity of a given thermal residue does not correspond to its relative position in the target password. This holds even for Hunt-and-Peck typists, as evidenced by Figure 8. These inconsistencies

make reliable ordering of key-presses infeasible in our analysis framework.

However, as mentioned above, for insecure (language-based) passwords, dictionary tools can be used to infer the most likely key-press order and anagram solvers can be extended to find phrases such as "iloveyou", with relative ease. For random passwords, the adversary can utilize additional attack angles such as combining multiple side-channels. To assess viability of this approach, we conducted a pilot study of 10 users for the combination of `Thermanator` with a profile-less modified version of Compagno et al.'s [7] keyboard acoustics attacks. This *hybrid* attack, namely `AcuTherm`[3], is quite effective in reducing the password search space for random passwords without the help of dictionaries.

5.6 Mitigation Strategies

There are several simple strategies to mitigate or reduce the threat of Thermanator Attacks, without modifying any existing hardware. The most intuitive solution is to introduce *Chaff typing* right after a password is entered. This can be as simple as asking the users to swipe their hands along the keyboard after password entry. Another way is to avoid keyboard entry altogether and use the mouse to select (click on) password characters displayed on the on-screen keyboard.

If hardware changes are possible, other mitigation techniques might be appropriate. For example, a touch-screen would allow password entry without the use of a keyboard. Alternatively, common plastic keyboards could be replaced with metallic ones. Metals have much higher thermal conductivity than plastics. Thus, any localized thermal residues very quickly dissipate throughout the keyboard. A similar strategy was adopted to protect ATMs from thermal attacks [10].

6 RELATED WORK

Human-factors based attacks have been extensively studied over the past decade. Interesting side-channels have been discovered [3, 16, 17] and there has been a wealth of work on strategies to commit and mitigate Shoulder-Surfing Attacks [6, 9, 18].

Thermal side-channels have been shown to be an avenue for obtaining secrets (e.g., key-codes, PINs) with the work of Zalewski [25]. Mowery et al. [10] investigated the influence of material composition and camera distance on PIN recovery, using a US$17,950 thermal camera, on commercial PoS-style PIN pads. [15] explored the effectiveness of a low-cost thermal camera ($\approx US\$330$, attachable to a smartphone) to recover 4-digit PINs entered into rubber keypads. Lastly, [24] discussed the viability of thermal imaging attacks on various PIN-entry devices including a keyboard, digital door lock, cash machine and payment terminal. [4] and [5] showed that smartphones also were a target for thermal imaging attacks.

7 CONCLUSIONS

In this work, we presented a post factum insider attack, namely Thermanator, that exploited the thermal residue side-channel against password entry on external keyboards. Our experiments included 30 subjects entering 10 passwords on 4 commodity keyboards. Results showed that complete password key-set can be recovered as late as **30 seconds** after entry, and subsets thereof up to **1 minute**. We also found that Hunt-and-Peck typists are especially vulnerable. In addition, we discussed mitigation strategies and methods for discovering key ordering for insecure and secure passwords.

[3]Abstract available: https://www.blackhat.com/asia-19/briefings/schedule/index.html#acutherm-a-hybrid-attack-on-password-entry-based-on-both-acoustic%2Dand-thermal-side-channels-13927

REFERENCES

[1] Dmitri Asonov and Rakesh Agrawal. 2004. Keyboard acoustic emanations. In *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*. IEEE, 3–11.

[2] AC Burton. 1939. The range and variability of the blood flow in the human fingers and the vasomotor regulation of body temperature. *American Journal of Physiology-Legacy Content* 127, 3 (1939), 437–453.

[3] Aviv et al. 2010. Smudge Attacks on Smartphone Touch Screens. *Woot* 10 (2010), 1–7.

[4] Andriotis et al. 2013. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, 1–6.

[5] Abdelrahman et al. 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, 3751–3763.

[6] Brudy et al. 2014. Is anyone looking? mitigating shoulder surfing on public displays through awareness and protection. In *Proceedings of The International Symposium on Pervasive Displays*. ACM, 1.

[7] Compagno et al. 2017. Don't Skype & Type!: Acoustic Eavesdropping in Voice-Over-IP. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. ACM, 703–715.

[8] Dai et al. 2004. Comparison of human skin opto-thermal response to near-infrared and visible laser irradiations: a theoretical investigation. *Physics in Medicine & Biology* 49, 21 (2004), 4861.

[9] Kumar et al. 2007. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 13–19.

[10] Mowery et al. 2011. Heat of the moment: Characterizing the efficacy of thermal camera-based attacks. In *Proceedings of the 5th USENIX conference on Offensive technologies*. USENIX Association, 6–6.

[11] Mickelberg et al. 2014. US cybercrime: rising risks, reduced readiness key findings from the 2014 US State of Cybercrime Survey. *US Secret Service, National Threat Assessment Center. Pricewaterhousecoopers* (2014).

[12] Owusu et al. 2012. ACCessory: password inference using accelerometers on smartphones. In *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*. ACM, 9.

[13] Pyda et al. 2004. Heat capacity of poly (butylene terephthalate). *Journal of Polymer Science Part B: Polymer Physics* 42, 23 (2004), 4401–4411.

[14] Peters et al. 2009. Diminutive digits discern delicate details: fingertip size and the sex difference in tactile spatial acuity. *Journal of Neuroscience* 29, 50 (2009), 15756–15761.

[15] Sidhu et al. [n.d.]. Study of potential attacks on rubber PIN pads based on mobile thermal imaging. ([n. d.]).

[16] Song et al. 2001. Timing analysis of keystrokes and timing attacks on ssh.. In *USENIX Security Symposium*, Vol. 2001.

[17] Weinberg et al. 2011. I still know what you visited last summer: Leaking browsing history via user interaction and side channel attacks. In *Security and Privacy (SP), 2011 IEEE Symposium on*. IEEE, 147–161.

[18] Yamamoto et al. 2009. A Shoulder-Surfing-Resistant Image-Based Authentication System with Temporal Indirect Image Selection.. In *Security and Management*. 188–194.

[19] Zhuang et al. 2009. Keyboard acoustic emanations revisited. *ACM Transactions on Information and System Security (TISSEC)* 13, 1 (2009), 3.

[20] Jan Noyes. 1983. The QWERTY keyboard: A review. *International Journal of Man-Machine Studies* 18, 3 (1983), 265–281.

[21] Occupational Safety and Health Administration and others. 1999. OSHA technical manual. *Section VIII* (1999).

[22] David Robb. 2014. Sony hack: A timeline. http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/.

[23] Jeff Sauro. 2009. Estimating productivity: composite operators for Keystroke Level Modeling. In *International Conference on Human-Computer Interaction*. Springer, 352–361.

[24] Wojciech Wodo and Lucjan Hanzlik. 2016. Thermal Imaging Attacks on Keypad Security Systems.. In *SECRYPT*. 458–464.

[25] Michal Zalewski. 2005. Cracking safes with thermal imaging. http://lcamtuf.coredump.cx/tsafe/. Accessed: 2018-04-02.

A BACKGROUND

In this section we provide some background material on physical interactions that describe thermal phenomena observed in our experiments. We start with a glossary of terms, then describe the form factor and material composition of modern 104-key "Windows" keyboards and finish with a comparison of various thermal cameras available in the market.

A.1 Basic Thermal Terminology

- Joule (J) – Unit of energy Corresponding to 1 Newton-Meter ($N \cdot m$)
- Kelvin (K) – Base unit of temperature in Physics. The temperature T in Kelvin (K) minus 273.15 yields the corresponding temperature in degrees Celsius ($^\circ C$).
- Watt (W) – Unit of power corresponding to 1 Joule per second: ($\frac{J}{s}$)
- Conduction – Transfer of Thermal Energy caused by two objects in physical contact that are at different Temperatures.
- Convection – Transfer of Thermal Energy caused by submerging an object in a fluid.
- Heat Transfer Coefficient - Property of a fluid that determines rate of convective heat flow. Expressed in Watts per square meter Kelvin: $\frac{W}{m^2 K}$
- Specific Heat – Amount of Thermal Energy in Joules that it takes to increase temperature of 1kg of material by $1K$. Expressed in Joules over kilograms degrees Kelvin: $\frac{J}{kgK}$.
- Thermal Conductivity – Rate at which Thermal Energy passes through a material. Expressed in Watts per meters Kelvin: $\frac{W}{mK}$
- Thermal Energy – Latent energy stored in an object due to heat flowing into it.
- Thermal Source – Object or material that can internally generate Thermal Energy such that it can stay at constant temperature during a thermal interaction, e.g., a heat pump.

A.2 Heating via Thermal Conduction

Thermal Conduction is transfer of heat between any two touching objects of different temperatures. It is expressed as the movement of heat energy from the warmer to the cooler object. We are concerned with transfer of energy from a human fingertip to a pressed keycap. This transfer is governed by Fourier's Law of heat conduction which states that:

> *Heat transfer between two objects can be modeled by the equation:* $q = \frac{\mathcal{K}A(T_1 - T_2)t}{d}$*, where* $\mathcal{K}$ *is thermal conductivity*[4] *of the object being heated,* A *is area of contact,* T_1 *is initial temperature of the hotter object,* T_2 *is initial temperature of the cooler object,* t *is time, and* d *is the thickness of the object being heated.*

The relationship between an object's heat energy and its temperature is governed by the object's mass and specific heat, as dictated by the formula: $q = cm\Delta T$, where q is total heat energy, c is object's specific heat, m is object's mass and ΔT is change in temperature.

We consider the human body to be a thermal source, and we assume that any change in the fingertip temperature during the (very short) fingertip-keycap contact period is negligible, due to internal heat regulation [8]. Furthermore, we assume that:

- Average human skin temperature is $307.15K$ ($= 34^\circ C$) [2].
- Keyboard temperature is the same of that as that of the air, which, for a typical office, is OSHA[5]-recommended $294.15K$ ($= 21^\circ C$) [21].
- Keycap area is $0.00024025\ m^2$, keycap thickness is 0.0015 meter and keycap mass is $.4716g$ (See: Section A.4).
- Average duration of a key-press is 0.28s [23].

Therefore, for variables mentioned above, we have:

$\mathcal{K}$=0.25, A=0.00024025, T1=34, T2=21, t=0.28, and d=0.0015

Plugging these values into Fourier's Law, we get:

$$q = \frac{(0.25)(0.00024025)(34 - 21)(.28)}{0.0015}$$

which yields total energy transfer: $q = 0.1458$J. We then use total energy q in the specific heat equation to determine total temperature change: $0.1458 = (1000)(0.0004716)\Delta T$. This gives us a total temperature change of $\Delta T = 0.3092$. Therefore, we conclude that the average human fingertip touching a keycap at the average room temperature results in the keycap heating up by $0.3092K$.

A.3 Cooling via Thermal Convection

After a keycap heats up as a result of conduction caused by a press by a warm(er) human finger, it begins to cool off due to convective heat transfer with the air in the room. Convection is defined as the transfer of heat resulting from the internal current of a fluid, which moves hot (and less dense) particles upward, and cold (and denser) particles – downward. This interaction is governed by Newton's Law of Cooling. Its particulars are impacted by the shape and position of the heated object. In our case, there is a plane surface[6] facing towards the cooling fluid (i.e., a keycap directly exposed to ambient air) which is described by the formula:

$$T(t) = T_s + (T_0 - T_s)e^{-\kappa t}$$

where $T(t)$ is temperature at time t, T_s is temperature of ambient air, T_0 is initial object temperature, and κ is the cooling constant of still (non-turbulent) air over a $0.00024025m^2$ plane.

This comes with the additional intuitive notion that a surface convectively cools quicker when the temperature difference between the heated object and the fluid is higher. Similarly, it cools slower when the temperature difference is smaller. Finally, Newton's Law of Cooling is asymptotic, and cannot be used to find the time at which the object reaches the exact temperature of the ambient fluid. Thus, instead of finding the time when the temperatures are equal, we determine the time when the temperature difference falls below an acceptable threshold, which we set at $0.04K$. Plugging this into Newton's Law of Cooling results in:

$$t = -\frac{ln(\frac{0.3092}{0.04})}{0.037}$$

which yields $t = 55.7$ for total time for a pressed key to cool down to the point where it is indistinguishable from the room temperature.

[4] $\mathcal{K}$ should not be confused with K – degrees Kelvin.

[5] OSHA = Occupational Safety and Hazards Administration, a United States federal agency.

[6] The actual keycap surface can be slightly concave.

A.4 Modern Keyboards

Most commodity external keyboard models are of the 104-key "Windows" variety, shown in Figure 9. On such keyboards, the distance between centers of adjacent keys is about 19.05mm, and a typical keycap shape is an $\approx$ [15.5mm x 15.5mm x 1.5mm] rectangular prism, with an average travel distance of 3.55mm [20]; see Figure 10. All such keyboards are constructed out of Polybutylene Terephthalate (PBT) with density of $1.31g/cm^3$, resulting in an average keycap mass of .4716g [13]. PBT generally has the following characteristics: specific heat = $1,000\frac{J}{kgK}$ and thermal conductivity = $0.274\frac{W}{mK}$ [13].

Figure 9: Typical "Windows"-style Keyboard.

Figure 10: Typical Keycap Profile.

A.5 Thermal Cameras

In the past few years, many niche computational and sensing devices have moved from Hollywood-style fantasy into reality. This includes thermal imagers or cameras. In order to clarify their availability to individuals (or agencies) at different levels of sophistication, we provide the following brief comparison of several types of readily-available FLIR: **F**orward-**L**ooking **I**nfra-**R**ed devices. (See: Figure 11 for product images and https://www.flir.com/products for full product specifications.)

FLIR One – Price: About US$300. Thermal Sensitivity: 0.15K. Thermal Accuracy: ±1.5K or 1.5% of reading. Resolution:50x80. Image Capture: Manual, 1 image at a time. Video Capture: None

SC620 – Price: About US$1500 (used). Thermal Sensitivity: 0.04K Thermal Accuracy: ±2K or 2% of reading. Resolution: 640x480. Image Capture: Automatic, programmable to capture images by timer, or when specific criteria are met, at maximum rate of 1 image per second. Video Capture: None.

A6700sc – Price: About US$25,000. Thermal Sensitivity: 0.018K Thermal Accuracy: ±2K or 2% of reading. Resolution: 640x512. Image Capture: Automatic, programmable to capture images by timer or when specific criteria are met, at up to 100fps. Video Capture: High speed, up to 100fps.

X8500sc – Price: About US$100,000. Thermal Sensitivity: 0.02K: Thermal Accuracy: ±2K or 2% of reading. Resolution: 1280x1024 Image Capture: Automatic, programmable to capture images by timer or when specific criteria are met, at up to 180fps. Video Capture: High speed, up to 180fps.

Figure 11: FLIR Devices / Thermal Imagers: FLIR ONE(top left), SC620 (top right), A6700sc (bottom left) and X8500sc (bottom right).

Obviously, a sufficiently motivated organization or a nation-state could easily obtain thermal imagers of the highest quality and price. However, we assume that the anticipated adversary is of a mid-range sophistication level, i.e., capable of acquiring a device exemplified by SC620.

However, we note the adversary armed with a FLIR One (which is on the low-end of the spectrum for thermal imagers, and can be connected to any commodity smartphone without substantially altering the overall form factor) can collect thermal residues up to 20 seconds after entry. Whereas, the adversary with a A6700sc or X8500sc can do the same 139 seconds, and 136 seconds after entry, respectively. Also, since thermal residues decay at a logarithmic rate, future advances in thermal camera sensitivity will result in a exponential increase of collection time.