

## Towards robustness of keyboard-entered authentication factors with thermal wiping against thermographic attacks

Lothar Fritsch<sup>1</sup>, Marie Mecaliff<sup>2</sup>, Kathinka Wik Opdal<sup>3</sup>,  
Mathias Rundgreen<sup>4</sup>, Toril Sachse<sup>5</sup>


**Abstract:** Many authentication methods use keyboard entry for one of their authentication factors. Keyboards factors have been compromised exploiting physical fingerprints, substances from fingers visible on keys, with acoustic recordings through mobile phones, and through video reflections captured by high-resolution cameras used for video conferencing. Heat transfer from human fingers to keypads is an additional attack channel that has been demonstrated. There are few mitigation measures published against this type of attack. This article summarizes the feasibility of thermographic attacks against computer keyboards and against door pin pads, as well as the efficiency of the scrubbing technique deployed in order to counter thermographic attacks. For this purpose, a series of experiments with small, mobile thermal cameras were carried out. We report findings such as time intervals and other constraints for successful laboratory observation of authentication factors, describe scrubbing methods and report the performance of those methods.

**Keywords:** password hijacking, infrared camera, thermographic attack, thermal imaging, authentication factor, identity management, information security, scrubbing, thermal lock picking.

### 1 Introduction

PIN codes and passwords as well as touchscreen-entered patterns are widely used authentication factors. Their compromise can lead to the collapse of individual digital identities as well as to the degradation of whole identity ecosystems [Fr20]. The common feature of most solutions is the transfer of an authentication secret to a computer input device through physically pressing or moving fingers of the human hand over the device. This physical contact transfers body heat from the finger to the touched device. Such heat is measurable with thermography cameras which measure the infrared head emissions from object surfaces. Sensors are recently integrated in small devices such as the FLIR C5 pocket camera<sup>6</sup> and the hardened Android phone CAT S62 Pro<sup>7</sup>,

---

<sup>1</sup> Oslo Metropolitan University (OsloMET), Department of Computer Science, Postboks 4, St.Olavs plass, 0130 Oslo, Norway, lotharfr@oslomet.no,  <https://orcid.org/0000-0002-0418-4121>

<sup>2</sup> Institut National des Sciences Appliquées de Toulouse, France, mariemecaliff@gmail.com

<sup>3</sup> Oslo Metropolitan University (OsloMET), Department of Computer Science, s187533@oslomet.no

<sup>4</sup> Oslo Metropolitan University (OsloMET), Department of Computer Science, rundgreen@me.com

<sup>5</sup> Oslo Metropolitan University (OsloMET), Department of Computer Science, s341837@oslomet.no

<sup>6</sup> FLIR C5 thermal camera, <https://www.flir.com/products/c5/> as of 18.1.2022

<sup>7</sup> CAT S62 Pro mobile phone with thermal camera, <https://www.catphones.com/en-gb/cat-s62-pro-smartphone/>, as of 18.1.2022

which are available at prices below 1000 EUR. Both the price range as well as the deployability of the cameras outside laboratory settings increase the feasibility and likelihood of thermal attacks. We therefore investigated the feasibility of attacks and their prevention.

The remainder of the article is structured as follows: First, we summarize the background of the project by a summary of thermal attacks and their mitigation in academic literature. Next, we define our research questions and describe the experimental setup and the results of experimentation. Finally, we discuss our results and summarize open issues.

## 1.1 Background thermal hacking

**Attacks against PIN pads:** Point-of-sales attacks against PIN code security have been investigated by Singh. et al [SBS19] with the goal to investigate the influence of camera distance, time passed between entry and capture, angle of photography and ambient temperature. Li et al [Li19] built a demonstrator that extracts the sequence of typed keys from a numerical keypad in laboratory experiments. They found influence factors such as typing speed, ambient temperature and typing speed as well as the number of repetitive keys used. In a second publication, Li et al [Li18] present experimental results for three countermeasures that reduce attack success from 30% to 10% based on these observations (see Tab. 1). Mowery et al [MMS11] demonstrate automated extraction of keypad key patterns from 10.000 to 24 possible 4-digit PIN codes. They note influence factors such as keypad heat absorption, material reflectivity, ambient temperature and lightness of finger pressure during typing. However, they do not recommend countermeasures.

**Touch screens and pads:** Abdrabou et al [Ab20] experimented with the thermal capture of security patterns and gestures on touch screens and touch pads of mobile computers and device. They achieved experimental success rates ranging from 14.81% (touch pad taps) up to 60% (gestures). They note that tap patterns transfer less heat than gestures painted with sliding fingers. Temperature differences between different test participants' body temperatures were complicating analysis. No countermeasures were suggested. Complementary experimentation with mobile phone touch screens performed by Abdelrahman et al. [Ab17] investigated the automated extraction of touch PIN codes and authentication patterns from video sequences. They achieved success rates between 80% and 100 in lab settings, however noted that automated analysis suffers from overlapping lines in authentication patterns. The article proposes several countermeasures, summarized in Tab. 1.

**Computer keyboards:** Kaczmarek et al [KOT19] studied password entry on computer keyboards. They notice differences in heat traces left by different typing styles. Notably, typing with fingers sliding over keys that are not pressed as part of the passwords complicates password extraction. Strong reduction in password search complexity is found. The authors speculate about countermeasures, however, do not experiment with

them (see Tab. 1). Wodo et al [WH16] investigate a wide range of key pads and keyboards in an exploratory study. They note that materials, surfaces, ambient and keyboard temperatures as well as timing constraints influence thermal print visibility. They reference defense countermeasures, which are classified below.

**Known countermeasures.** Below, countermeasures against thermal attacks mentioned in the surveyed literature are listed and classified into types and maturity.

Countermeasure	Reference	Maturity
Block line of sight with shield	[SBS19], [AKSA17], [WH16]	Proposal
Reflective surface	[SBS19]	Proposal
Curved shape of keypad for diffusion	[SBS19]	Proposal
Delay entry transaction until cooled off	[SBS19]	Proposal
Minimum distance camera to keypad	[SBS19]	Proposal
Temperature control of keypad	[SBS19], [WH16]	Proposal
Materials with low heat conductivity	[SBS19], [KOT19]	Proposal
Blinding with illuminated keypad	[SBS19], [AKSA17]	Proposal
Wiping with CPU-generated heat	[AKSA17]	Proposal
Heating of surface	[AKSA17]	Proposal
Touch-to-heat wiping of thermal print	[SBS19], [Li19], [KOT19], [AKSA17], [Li18]	Proposal, <b>Experiment</b>
Blowing of warm air over keypad	[Li19], [Li18]	Proposal, <b>Experiment</b>
Randomized virtual pad on touchscreen	[SBS19], [AKSA17]	Proposal
Ambient light against key mapping	[Li19]	Proposal
Passwords with repetitive keys	[Li19], [AKSA17], [Li18]	Proposal, <b>Experiment</b>
Very long passphrases	[AKSA17]	Proposal
Add authentication factor or medium	[AKSA17], [WH16]	Proposal
Use temperate finger substitute for entry	[KOT19]	Proposal

Tab. 1: Countermeasures against thermal attacks

Our background summary in Tab. 1 clearly shows the lack of empirical validation of thermal attack countermeasures in published literature. Only for three of the measures, experiments of their effect have been published.

**Targets of attacks:** All attacks found in literature were deployed in laboratory settings. Most effort is put into attacking PIN pads, followed by touch-based patterns and then computer keyboards. Below, the mapping of literature on attack target is listed.

PIN pads: [SBS19], [Li19], [Li18], [MMS11], [WH16]

Touch screens: [Ab20], [AKSA17]

Touch pads (laptop):	[Ab20]
Keyboards:	[KOT19], [WH16]
Digital door lock:	[WH16]

The specification of countermeasures in the above publication falls short of detailed descriptions of how the countermeasures must be applied in order to succeed. Neither material specifications, light intensities, temperature intervals or descriptions of wiping movements are described in a level of detail that would allow for the reproduction of the experiments.

## 1.2 Research questions

In this article, we summarize the findings of experimentation that targeted two research questions:

1. Are IR fingerprints exploitable in a practical attack scenario with small thermal cameras? This research question investigates the practicability of attacks against a door PIN pad system.
2. How can IR attacks get mitigated with simple means for everyday application? Which methods that do not need technical modifications, and which work with minimal effort, can mitigate thermal attacks?

Digital door locks with PIN pads combine three experimental advantages: They are available indoors in controlled temperatures and lighting conditions. They do not move, but rest in locked position. And, most important, their users pass the door after PIN entry while leaving the PIN pad with thermal fingerprints behind. Thus, our feasibility study examines door locks with PIN pads as attack targets [RS21].

The empirical foundation of the proposed countermeasures against thermal attacks is weak. Therefore aims our second research question at systematic trials of easily applicable mitigation techniques in order to qualify how they work, and under which circumstances they are effective [Me21],[Wi21].

## 2 Experimentation and results

We carried out three studies with experiments in order to investigate the research questions: a feasibility test of thermal attacks against digital door locks with PIN pad [RS21], and experiments deploying countermeasures against thermal attacks against computer keyboard password entry [Wi21],[Me21]. In this section, we describe the experiments.

## 2.1 Practicability of attacks against digital door locks with PIN pads

First observations made by targeting operative door locks at OsloMET's buildings. Fig. 1 shows various types of indoor and outdoor PIN pads in thermal images. Note how shape, surface materials and heat emissions from internal electronics influence the visibility of the heat prints on key "5" in the middle of the key pads.

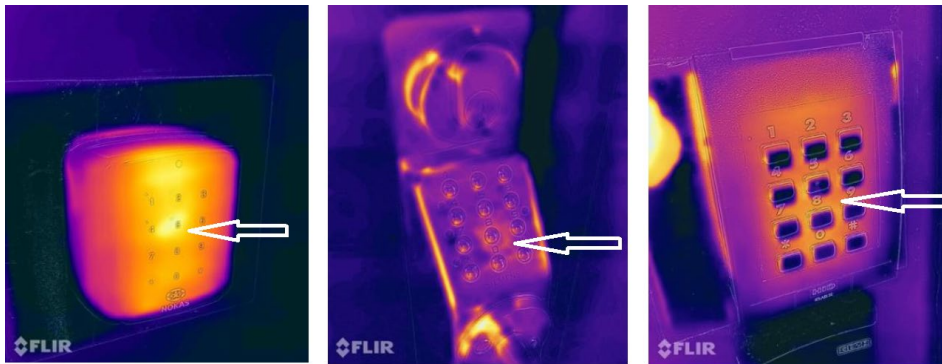


Fig. 1: Thermal image of various locks at OsloMET after pressing "5". Left: Internal heat obfuscates print. Center: round metal keys diffuse heat radiation on keys. Right: internal heat and plastic caps hide print [RS21].

As a consequence of these observations, a door lock was borrowed from a locksmithing shop in Oslo. It was set up in a lab where lighting conditions could be controlled. The lock's temperature was measured at room temperature and refrigerated in order to simulate outdoor measurement. Fig. 2 shows the lab setup.

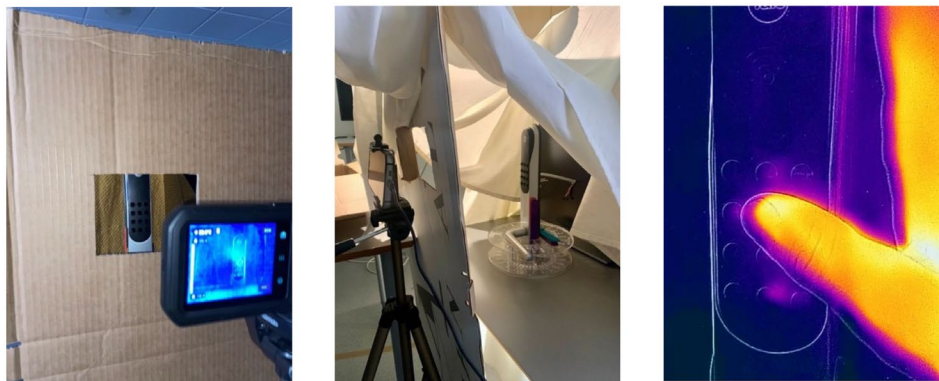


Fig. 2: Laboratory setup. Left: Camera positioning with mask. Center: shielding cloth against ambient light. Right: Thermal recording of PIN entry [RS21].

Experimentation was carried out by recording videos of PIN entries of a 4-digit and a 6-digit PIN for each temperature. Experiments were repeated for 10 rounds. Recordings

were done for 40 seconds after entry. Visibility of the heat prints was generally degraded after this time period. Visibility of PIN keys was measured by analyzing amplified color contrast values in the video still frames with the help of video editing software (5KPlayer for MacOS, Digiarty Software). Results show that the refrigerated lock shows heat prints longer than the lock at room temperature. Visibility of the PIN keys ranged from 3 seconds to 15 seconds. The average independent of temperature was 6.91 seconds (see Fig. 3). The longest visible print was detectable for 30,4 seconds.

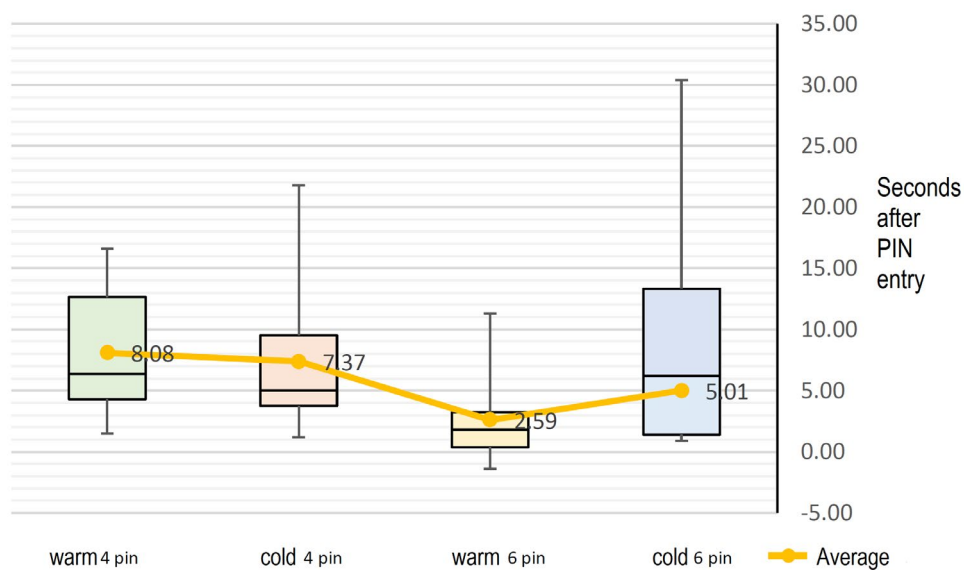


Fig. 3: Visibility of 4- and 6-digit PIN on lock at room temperature and refrigerated. Results obtained from contrast-enhanced video recordings. Average visibility: 6.91 seconds [RS21].

In summary, thermal lock-picking attacks on door lock PIN codes are feasible, however in specific contexts. The type of lock its surface materials, and ambient temperatures as well as ambient light will influence success. In warm environments, the time window between closing the door and the fading of the heat prints will be short. Some locks generate internal heat, which outshines the thermal prints.

## 2.2 Examination of wiping techniques on computer keyboards

The second research question investigated the applicability and the effectiveness of mitigation methods against thermal attacks. Reviewing the methods from literature (see Tab. 1), four methods were chosen for their ease of use, and their availability without modifications to the target keyboard:

- a) Application of flat hand to keyboard: Heat transfer from pressing a flat hand to the keyboard after password entry was used to camouflage pressed keys in a larger heat print.
- b) Hot gel pack: Applying a medical gel pack warmed up to body temperature, heat was transferred to the keyboard in order to camouflage keys pressed.
- c) Cold gel pack: Cooling the thermal fingerprints using a chilled medical gel pack applied to a keyboard with the intention to remove the thermal prints.
- d) Scrubbing: Moving hand randomly over the keyboard (once and repeatedly) with the intention to camouflage the pressed keys in additional thermal prints.
- e) Blowing: Applying warm air blown over the keyboard in order to conceal the thermal prints from password entry.

The experimental setup was built in an air-conditioned lab room at OsloMET. A PC keyboard was placed on a table. A camera tripod with the thermal camera was mounted next to the keyboard and calibrated. A refrigerator as well as hot and cold water and a water cooker/coffee maker were available for heating and cooling gel packs. Experiments were run several times, assessing the effect of the wiping method as well as the timing constraints of the visible artifacts. The lab setup is shown in Fig. 4.



Fig. 4: Experimental setup for password wiping studies [Me21].

In a first round of pre-experiments, camera calibration was done. Through small series of tests, cool-off time intervals for the keyboard were found. Issues arose when the team found out that different persons emit different amounts of heat. Two experimenters had relatively low surface temperatures of their fingertips, such that they after experimentation decided to standardize their hand temperatures with the help of a bottle with warm water heated to a controlled target temperature. For experimentation, two passwords of 8 and 16 characters length were chosen: ILOVEYOU and SMITTEVERTILTAK. The latter password contained double and tripe use of letters, which was found to have an impact on detectability of pressed keys. Experimentation was done in 10 rounds of measurements with timed typing, time measurements and interval photography using the thermal cameras.

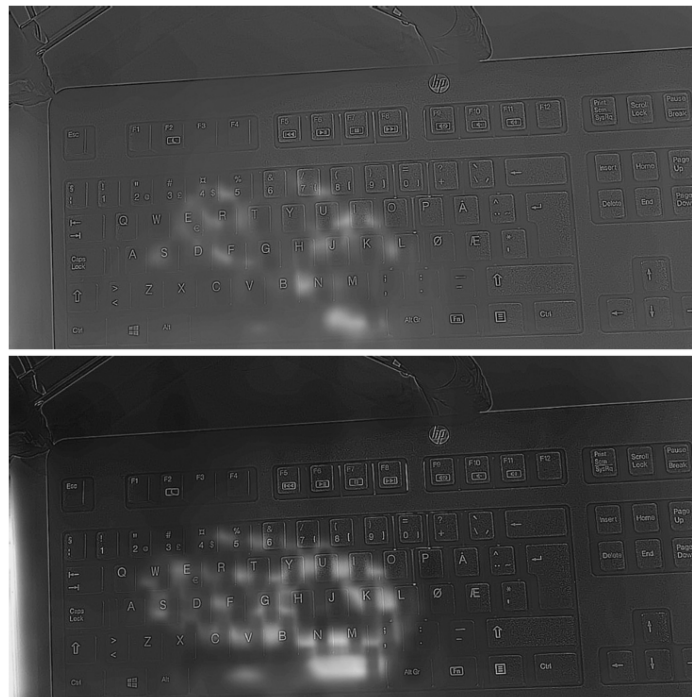


Fig. 5: Hand pressing technique. Top: 2.5s, bottom: 5s application [Wi21].

Not surprisingly, application time was a major determinant of wiping heat transfer. Fig. 5 shows the difference in transferred heat from 2.5 and 5 seconds of pressing the whole hand against a keyboard after typing a password. Individual keys were still identifiable after 2.5 seconds. In the experiments with moving hands or blowing air, speed or exposure time was equally relevant. As shown in Fig. 6 b), application of warm air from own lungs has a considerably higher wiping effect when blown for 5 seconds with higher pressure. The application techniques and their effect are summarized in Tab 2 below.



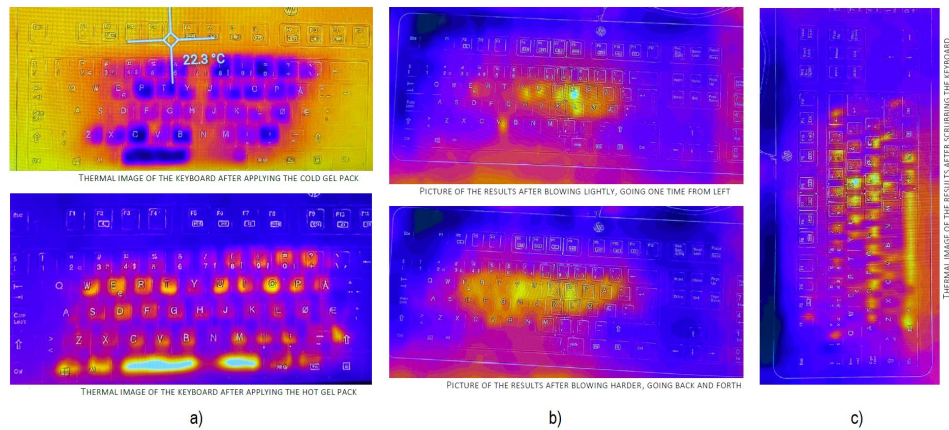


Fig. 6: Wiping: a) cold and hot gel pack; b) blowing warm air; c) wiping with hand [Me21].

In the course of experimentation it turned out that the wiping methods had to get applied much longer than the original password typing in order to securely transfer enough heat. Applications under 2.5 seconds revealed pressed keys, while application times of 5 seconds or more had a sufficient mitigation effect. Results will be discussed more in the next section of the article.

### 2.3 Summary of results

Results from experimentation show that any of methods a) to e) can mitigate the thermal attack. An application time of approx. 5 seconds will sufficiently wipe the thermal print. The different wiping techniques show different effects, and they require different preparations. Results are summarized in Tab 2.

Method	Application time	% keys identified	Preparation overhead
Cold gel pack	5s	31	Gel pack chilled to 8 C.
Hot gel pack	5s	31	Gel pack pre-heated to. 42 C
Moving hand slow	2s	44	Warming up hand if needed
Blowing	5s	59	Inhale and blow on keyboard
Pressing hand	5s	0	Warming up hand if needed
Moving hand once	5s	0	Warming up hand if needed
Moving hand once	2.5s	15	Warming up hand if needed
Moving hand multiple	5s	0	Warming up hand if needed
Moving hand multiple	10s	0	Warming up hand if needed
Control experiment (no wiping)		93	-

Tab 2: Effect and timing of wiping methods.

Various issues require care when wiping methods are applied. Moving hands is variable in speed and pressure applied. Self-discipline for slow movements is required. The same holds for the blowing method. A 5-second blow from the lungs is a practice many use once per year on the occasion of blowing the candles on birthday cakes, not when opening doors on a daily basis. Pressing the flat hand is a well-controllable movement, however it may suffer from the hand not being warm, due to either physiological conditions or recent exposure to cold environments. Finally, warm gel packs help standardizing temperature and application surface, are however items that need extra attention and preparation.

### 3 Discussion & conclusion

We showed that thermal attacks are a practical vulnerability that can get exploited in the area of PIN-protected door locks. This finding complements earlier research about practical point-of-sales-terminals as attack targets for payment card PIN theft. Further theoretical attacks target keyboard passwords and screen-lock patterns on mobile devices. However, the staging of attacks in these scenarios will require the attacker to have an opportunity to photograph devices shortly after passcode entry. We found that thermal prints are visible up to nearly one minute in thermal cameras.

Simple and practical countermeasures are available for individuals. They complement physical protection measures such as shielding, distance, heating and reflective surfaces. Hand pressing, hand movements, blowing hot air or the application of heat packs can effectively render thermal prints invisible, and thereby mitigate attacks. User-deployed wiping techniques should be part of security briefings and of user policies wherever keyboard-entered authentication factors are used. We suggest the inclusion of thermal wiping techniques into security awareness materials. One promising way of promotion will be the production of themed awareness gifts in the form of hand-warming heat packs with a thermal attack reminder as part of security awareness work.

**Future research.** Future research will investigate the social context for successful thermal attacks. Experimentation with secured campus access areas and their users will reveal the rates of succeeding with thermal photography versus being spotted and compromised in practical settings. Further attention should be used on authentication factors for digital identities, since the potential damage of compromise is large. PIN-pad enabled tokens can get compromised in similar ways as keyboards.

**Acknowledgement.** We thank OsloMET's research group for Universal Design, especially Professor Weiqin Chen, for providing laboratory space for experimentation.

---

## Bibliography

- [Ab20] ABDRABOU, YASMEEN ; ABDELRAHMAN, YOMNA ; AYMAN, AHMED ; ELMOUGY, AMR ; KHAMIS, MOHAMED: Are Thermal Attacks Ubiquitous? When Non-Expert Attackers Use Off the shelf Thermal Cameras. In: *Proceedings of the International Conference on Advanced Visual Interfaces*. New York, NY, USA : Association for Computing Machinery, 2020 — ISBN 978-1-4503-7535-1, S. 1–5
- [Ab17] ABDELRAHMAN, YOMNA ; KHAMIS, MOHAMED ; SCHNEEGASS, STEFAN ; ALT, FLORIAN: Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17*. New York, NY, USA : Association for Computing Machinery, 2017 — ISBN 978-1-4503-4655-9, S. 3751–3763
- [Fr20] FRITSCH, LOTHAR: Identification collapse - contingency in Identity Management. In: *Open Identity Summit 2020*. Bd. P305. Bonn : Gesellschaft für Informatik e.V., 2020. — Accepted: 2020-05-27T12:09:21Z — ISBN 978-3-88579-699-2
- [KOT19] KACZMAREK, TYLER ; OZTURK, ERCAN ; TSUDIK, GENE: Thermanator: Thermal Residue-Based Post Factum Attacks on Keyboard Data Entry. In: *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, Asia CCS '19*. New York, NY, USA : Association for Computing Machinery, 2019 — ISBN 978-1-4503-6752-3, S. 586–593
- [Li19] LI, DUO ; ZHANG, XIAO-PING ; HU, MENGHAN ; ZHAI, GUANGTAO ; YANG, XIAOKANG: Physical Password Breaking via Thermal Sequence Analysis. In: *IEEE Transactions on Information Forensics and Security* Bd. 14 (2019), Nr. 5, S. 1142–1154
- [Li18] LI, DUO ; ZHANG, XIAO-PING ; ZHAI, GUANGTAO ; YANG, XIAOKANG ; ZHU, WENHAN ; GU, XIAO: Modeling Thermal Sequence Signal Decreasing for Dual Modal Password Breaking. In: *2018 25th IEEE International Conference on Image Processing (ICIP)*, 2018, S. 1703–1707
- [Me21] MECALIFF, MARIE: *How to secure passwords against infrared camera attacks, Project report DATA3710* (Student report). Oslo : Department of Computer Science, Oslo Metropolitan University, 2021

- [MMS11] MOWERY, KEATON ; MEIKLEJOHN, SARAH ; SAVAGE, STEFAN: Heat of the moment: characterizing the efficacy of thermal camera-based attacks. In: *Proceedings of the 5th USENIX conference on Offensive technologies, WOOT'11*. USA : USENIX Association, 2011, S. 6
  
- [RS21] RUNDGREEN, MATHIAS ; SACHSE, TORIL: *Thermohacking, Project report DATA3710* (Student report). Oslo : Department of Computer Science, Oslo Metropolitan University, 2021
  
- [SBS19] SINGH, GURVINDER ; BUTAKOV, SERGEY ; SWAR, BOBBY: Thermal Print Scanning Attacks in Theretail Environments. In: *2019 International Siberian Conference on Control and Communications (SIBCON)*, 2019, S. 1–6
  
- [Wi21] WIK OPDAL, KATHINKA: *Hvor sikre er PIN-koder mot angrep basert på termografi?*, *Project report DATA3710* (Student report). Oslo : Department of Computer Science, Oslo Metropolitan University, 2021
  
- [WH16] WODO, WOJCIECH ; HANZLIK, LUCJAN: Thermal Imaging Attacks on Keypad Security Systems: In: *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications*. Lisbon, Portugal : SCITEPRESS - Science and Technology Publications, 2016 — ISBN 978-989-758-196-0, S. 458–464