Thermal Imaging Attacks on Keypad Security Systems

Wojciech Wodo and Lucjan Hanzlik
Department of Computer Science, Wroclaw Univeristy of Technology, Wybrzeze Wyspianskiego 27, Wroclaw, Poland

Keywords: Thermal Imaging Cameras, Thermal Imaging Attacks, Cash Machine, Cipher, Terminal, Keys, Access Code, PIN Number, Side Channel.

Abstract: The paper discusses the issue of thermal imaging attacks on a variety of keyboard devices, such as cash machines, payment terminals, combination locks or computer keyboards. The aim of the research was to obtain the entered code or password in the most non-invasive way. As it turned out, attacks based on images from thermal imaging cameras are very easy to carry out and work in almost every case, which calls for extra safety measures. The authors consider various attack scenarios and come up with recommendations for both manufacturers and users of electronic keyboard security systems.

1 INTRODUCTION

An observation of development of electronic and information systems in almost all areas of life makes one notice a replacement of old solutions based on mechanical or classic methods of verifying the authorization or identity. You no longer need a lock to secure a room, but a digital code; you do not pay in cash, but use a credit card and authorize the transaction by entering a PIN number. What is more, you no longer withdraw money after a long wait in a line at a bank, but use any of omnipresent cash machines instead, also validating the withdrawal by entering your PIN number. It is an understandable trend resulting from manufacturers' or contractors' urge to make things most convenient for their customers. However, transferring the area of security to the digital world results in new threats posed not by thieves who can steal physical property, but by cybercriminals who use sophisticated methods to steal not only the property, but also the identity of an online user.

1.1 State of the Art

Literature mentions various examples of side-channel attacks which use additional information from channels such as electromagnetic radiation, power consumption, or timing attacks to break security systems. This category of attacks is really difficult to fight because the designer of one particular component of a security system does not always influence other parts of it or the terms of its use. Owing to this fact, it was possible to carry out an attack to extract a RSA private key after unauthorized monitoring of processor computing time for particular mathematical operations. One of such weaknesses was described in a paper by Paul Kocher, the pioneer of side-channel attacks (Kocher, 1996). Other researchers carried out a power analysis using a microprocessor and achieved a data leakage from a smart card, which is mentioned in (Messerges et al., 1999). The issue of a simple power analysis – *SPA*, and a differential power analysis – *DPA*, has been researched also by the authors of this paper (Kocher, 1999). Using emissions of electromagnetic fields to break security systems was described in the iconic work by Van Eck (Eck, 1985); a series of papers on electromagnetic field analysis in the context of random number generators, smart cards and hard drives has been published by Cambridge University authors (Markettos et al., 2009; Li et al., 2005; Markettos et al., 2004).

In the case of attacks using a thermal imaging camera, two main publications can be mentioned: a strictly demonstrative study by Michal Zalewski (Zalewski, 2005) which describes cracking a combination lock in a safe, and a scientific work from the University of San Diego, California (Meiklejohn and Savage, 2011), in which the authors discuss the attack of capturing PIN numbers of customers using cash machines. The first work shows that attacks based on temperature distribution

Wodo, W. and Hanzlik, L.
Thermal Imaging Attacks on Keypad Security Systems.
DOI: 10.5220/0005998404580464
In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4: SECRYPT*, pages 458-464
ISBN: 978-989-758-196-0

examination on the surface of a digital lock after entering a PIN (touched by a human) are possible to carry out. The authors of the second work analyze details of the attack, consider various scenarios and automate the process of PIN recovery from fragments of recorded thermal imaging footage. However, they only focus on cash machine keyboards with plastic keys covered with rubber, claiming that due to the high conductivity of the metal used in other models of keyboards it was impossible to obtain any useful data.

1.2 Motivation

Taking into account the dates of the above mentioned publications describing thermal imaging attacks and their selective nature, we decided to examine what has been done to date by manufacturers of such sensitive devices as cash machines, safes or payment terminals in order to ensure their users' safety. We also took up a challenge to analyze attacks on devices made from metals with high conductivity and a high level of reflection of thermal radiation excluded from the study by the mentioned authors. The most important premise was to design and carry out attack scenarios in which the victim would be oblivious (no interaction with the victim), and the attacker would use stealth (the attacker is always hidden). We adapted this attitude because we deeply believe that in the digital era of today such criminals are the most dangerous and hardest to identify.

1.3 Structure of the Paper and Contribution

Chapter One constitutes an introduction to the subject of thermal imaging attacks, describing our motivation and discussing other works on the issue, proving that it poses a real threat. In *Chapter Two* of the work we present several scenarios of thermal imaging attacks devised by ourselves which we have simulated on various security devices, from computer keyboards and digital door locks to cash machines and payment terminals. Building on the observations from the previous chapter, in *Chapter Three* we give recommendations for manufacturers and users of electronic security systems, which could lower the potential threat of thermal imaging attacks. The last and binding part is *Conclusions* which constitutes a conclusion to our findings and suggests further areas of investigation with thermal imaging as a source of information for security breaches.

Figure 1: A micro camera in a cash machine case. Source: http://krebsonsecurity.com/.

2 ATTACK SCENARIOS

Undoubtedly, the majority of cash machine users know the technique of a skimmer's attack on ATM cards (Snapsupplies.com, 2014), i.e. copying ATM cards by installing skimming devices, micro cameras (Fig.1) or keyboard cover plates (Fig.2) recording the entered PIN number. These attacks, however, require an invasive interaction with the cash machine (a partial disassembly of its case or installation of additional parts); approaching the cash machine itself or any non-standard behavior at it may look suspicious to security guards or potential bystanders. Careless installation of skimming devices or cameras can be easily noticed and neutralized, with the skimmer traced owing to surveillance cameras footage.

Figure 2: A keyboard cover plate. Source: http://i.dailymail.co.uk/.

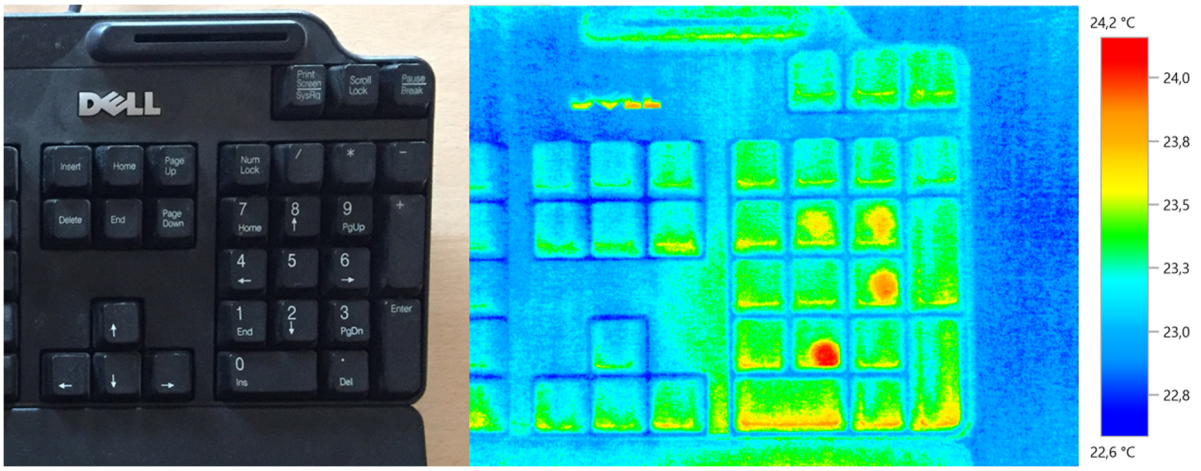

Figure 3: Attack on a computer keyboard, time: 5 seconds, PIN:8962.

Nowadays, prices and sizes of thermal imaging cameras are significantly lower than in the past and the devices no longer cost several thousand dollars. It is worth mentioning that some manufacturers produce special modules which are compatible with smartphones and enable thermal imaging in your own phone; e.g. *Seek Thermal* offers micro USB thermal imaging cameras for as little as ca. 250 USD. For comparison purposes we present our thermal imaging camera used in the research -- *Testo Thermal Image 890* which works with the frequency of 33 Hz and a standard 640 x 480 resolution, expanding to 1280 x 960 in the *Super Resolution* mode.

Our idea of the attack is to remain entirely anonymous for the victim with a simultaneous lack of modification in the attacked device (an oblivious attack). The adversary takes the role of a potential user of a chosen device and carries out a standard procedure of its use without giving rise to any suspicion. In the meantime, they record the thermal image of the keyboard using a smartphone with a thermal imaging camera. For a bystander it looks as if the adversary were queuing or checking something on their phone.

As part of our research, we carried out several dozen attacks on various available keyboard devices: cash machines, combination door locks, computer keyboards and payment terminals. Conclusions drawn from these attacks are also valid for other devices with a similar structure or made from similar materials, such as intercoms or parcel lockers.

2.1 Attack 1: Computer Keyboard

A basic attack which piqued our curiosity was a computer keyboard attack – an attempt to intercept a login password or an authentication code. We carried out an attack on a standard external keyboard by *Dell*. The password was entered by a fast-typing person and can be easily read using thermal imaging pictures (Fig.3). With a longer waiting time it is difficult to establish the order of the pressed keys, but it is still certain which were used to enter the password. In the case of built-in laptop keyboards, part of the keys are heated up by internal systems, so the temperature of some of them is much higher than the ambient temperature, sometimes even than human body temperature. In such cases it is impossible to identify the pressed keys in our attack scenario.

2.2 Attack 2: Digital Door Lock

We considered two types of combination door locks: with a protective film covering the keyboard and without it. The scenario of the attempt was fairly simple: we waited for an authorized person to approach the door, enter the code and go inside. At the same time we recorded thermal imaging footage. Even after a long break of 30 seconds, it was easy to decipher the code digits; with less waiting time it was not problematic even to establish the order of the digits (Fig.4).

2.3 Attack 3: Cash Machine

We carried out attacks on cash machines in cooperation with *Bank Zachodni WBK,* having been granted access to cash machines located in the most popular spots visited by bank customers every day. We considered the following three locations of those cash machines: in buildings (heated and soundproof), in semi-open spaces (mudrooms) and

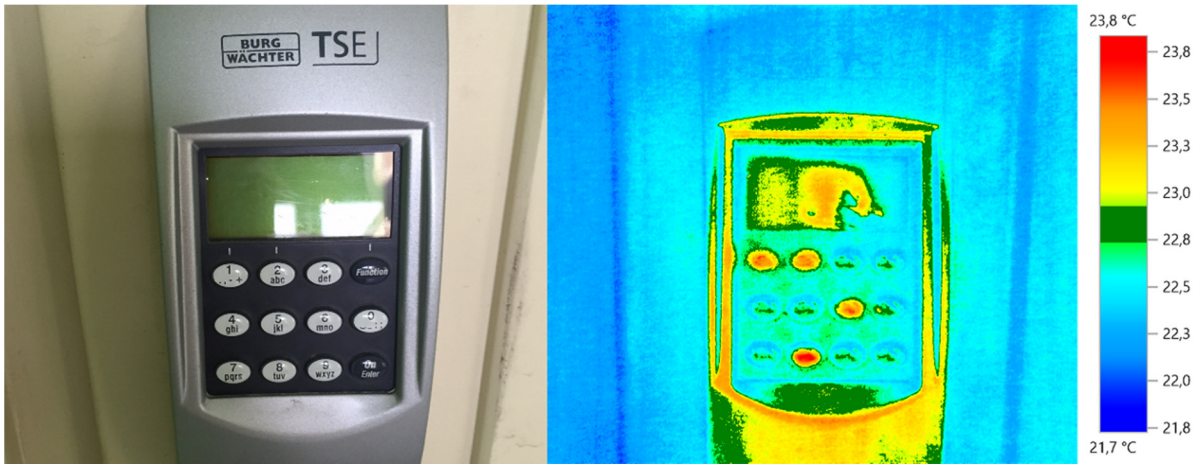

Figure 4: Attack on a combination door lock (no protective film), time: 5 seconds, PIN:1268.

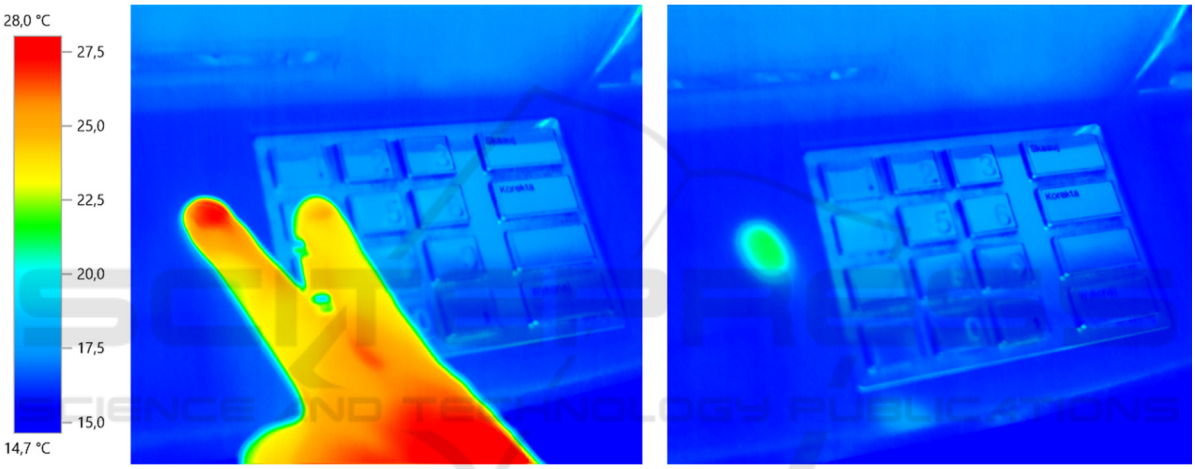

Figure 5: Attack on a cash machine (metal keyboard keys), time: 1 minute.

outdoors. It was crucial to take into consideration a variety of temperatures and weather conditions which could influence the heat flow and its retention on the touched parts of the cash machine. An additional aspect was the recording of sounds made by the cash machine while pressing its keys, crucial while entering a PIN number.

The first thing we examined was the average time of the user interaction with the cash machine, assuming a fast cash withdrawal scenario. The whole activity lasted 45 seconds, and counting from the moment of entering the PIN -- 25-30 seconds. When the user wanted a confirmation of the transaction, it added 10-15 seconds to the activity. It is worth mentioning that the used models of cash machines had metal keyboard keys.

All attempts to acquire thermal imaging with traces of the entered PIN ended up in a fiasco. Even in the case of holding two fingers simultaneously on a metal button and the case for ca. 1 minute, the result was inconclusive (Fig.5). Even though, the heat on the cash machine case was still visible.

Having figured out that the reason for the fiasco was very low emissive power of the metal used in the keys (e.g. aluminum), we designed a modification of the attack in which the keyboard was covered with a thin layer of an insulator before carrying out more attempted attacks. The mentioned insulator can be any spray creating a thin film on the sprayed surface, such as hair spray or sunburn spray. Another problem that we had to face was the fact that the presence of people generating heat influenced the measurement of the keys' temperature due to the effect of reflection of thermal radiation off the polished surface of the metal keys.

In further tests we utilized an information kiosk keyboard with polished metal keys just like in the case of the tested cash machines. In the first place

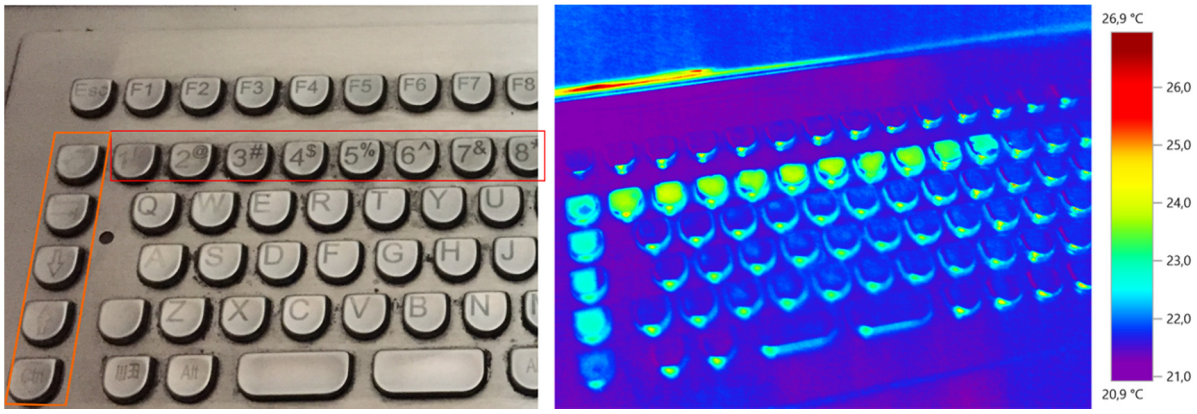

Figure 6: Attack on metal keys (orange box– keys covered with hair spray, red box – keys covered with nail polish), t. 5 s.

we tested various insulators, e.g. stretch foil, hair spray, transparent nail polish (Fig.6). Properties of the used materials and various layers which were created have proven that the most effective and durable solution was the nail polish. It creates a transparent, impalpable, durable and thick enough layer which retains heat and counters the reflection phenomenon. In the case of the other two solutions the effect was unsatisfactory – the hair spray created a layer which was too thin, did not retain the heat for long, and was prone to mechanical damage. The foil was easy to notice and did not protect the keyboard against the reflection phenomenon.

The next step was covering the 0-9 keys with a layer of nail polish and then carrying out an attack on the user's PIN number. We had no problem getting the correct sequence of the keys after a short time – the effect lingered for ca. one minute; after this time the sequence was a little blurry and we had to try out several combinations. At this stage of the research we noticed an opportunity for an attack by cooling a metal keyboard and recording the increased temperature of the keys pressed by the user. Such attacks can be carried out using compressed air. The effect does not linger long, therefore it can only be used in the next customer scenario. The advantage of this solution is that it does not leave any visible traces on the attacked device.

2.4 Attack 4: Payment Terminal

In the case of payment terminals, we focused on a more difficult device in our view – a battery-powered mobile payment terminal. As opposed to its fixed equivalent in which the keyboard is a peripheral device, the mobile payment terminal has an integrated structure. It means that the keyboard is located in the same case as the other electronics, and the temperature of the device is high owing to the heat generated by the microprocessor and other elements (similarly as in the case of the laptop, consider Attack 1). We decided to carry out two types of attacks: one utilizing the fact that the user comes from the outside where the temperature of their hand is lower than the temperature of the terminal, and one assuming that the customer has been in the building for some time and the temperature of their hand is comparable to the normal human body temperature. In both cases we can easily identify the keys pressed on the terminal (Fig.7). The worst case scenario is the situation when the temperature of the terminal is similar to the temperature of the customer's fingers; then the temperature of the keys changes and you are unable to identify the used keys.

3 ANALYSIS OF THE RESULTS AND RECOMMENDATIONS

The experimental attacks carried out by us clearly indicate that the most significant factor for security is the material of the keys used for entering the PIN code. If you use a material with high thermal conductivity, e.g. a metal, the heat from the user's finger can spread onto the whole button. However, owing to another property of the material, its emissive power (Wisniewski, 2012), thermal imaging does not show any thermal changes on the key's surface. All polished metals (especially aluminum) have a low emissivity factor, which causes problems in observing their thermal radiation. In the case of materials of high emissive power, such as plastics, ever brief contact with human skin results in heat spreading on the key's surface. Due to the fact that the key is surrounded by the air which is

an insulator, heat lingers on it for a longer time. Depending on the weather conditions and properties of the used material, this time will vary. Nevertheless, it is long enough to carry out the mentioned attacks (in some cases even one minute long). Furthermore, materials vary in absorption capacity and reflection or passing of heat radiation (Wisniewski, 2012). A particularly problematic phenomenon is reflection of thermal radiation of other objects off the material's surface. In such cases it may be difficult to establish whether the observed emission is due to the material or the user's heat reflection only.

The most effective security measures against thermal imaging attacks, as we have proven, is to heat up all the keys used to enter the PIN code. It can be done by putting a hand on their surface or stroking the surface of the keyboard several times. After such actions the thermal image shows heat on each of the keys, blurring information about the pressed ones.

Both physical and empirical information clearly indicate that using materials with low emissive power to manufacture device keys protects them from thermal imaging attacks. In cases of such keyboards we only suggest checking and rubbing the keyboard in order to remove a possible insulating layer spread by an adversary.

Another side channel turned out to be the sound made by the cash machine while pressing its keys, or the sound of the pressed keys itself. The volume intensity in both cases enables the queuing person to hear when the customer presses the keys. It is particularly dangerous while entering the PIN number because owing to the analysis of keystroke latencies you can deduce some information about the digits making up the code. It also facilitates the analysis of thermal imaging pictures, especially when their sequence is not entirely clear. The simplest example of the importance of audio surveillance is the use of a double digit in a PIN (e.g. 1449); in such cases, the recorded keystroke latency periods will be: long, short, and long again. The attacker immediately knows that the middle digit is a double one. We therefore suggest choosing PIN numbers without double digits and entering the code with intentional delay (Hanzlik and Wodo, 2013).

The case of customers of cash machines and payment terminals is particularly important to us because while in the first of the mentioned devices metal keyboards are quite common, they are highly unlikely to be used in payment terminals. If one of such key elements of payment systems is so prone to attacks based on PIN code extraction, you need to take other safety measures. First and foremost, you have to make provision against unauthorized attacks which use the victim's bank card to make a *PayPass* payment (utilizing *NFC chips*) (Hancke, 2005). Such transactions are made with no necessary authorization for limited amounts of money, yet in the case of obtaining the victim's PIN number (which is not so difficult, as we have proven) the safety measure is no longer valid. The only effective protection is preventing the card from starting the protocol by placing it in a special protective case – a *Faraday cage*. Owing to this step, no electromagnetic field can influence the card and initiate communication with it without our consent. What is more, it might be a good idea to dedicate a contactless card to a bank account with significant limits set for transfers and transactions.

4 CONCLUSIONS

As can be seen, thermal imaging attacks still pose a threat to users' safety. They can prove particularly

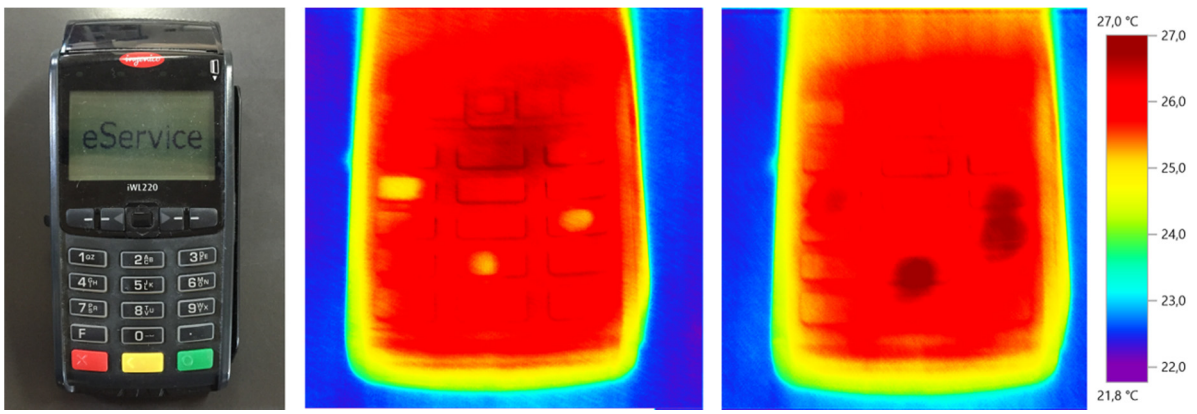

Figure 7: Attack on metal keys (orange box– keys covered with hair spray, red box – keys covered with nail polish), t. 5 s.

dangerous for people using contactless payment.

In the past, the PIN number itself was not enough as the card was necessary, too. Now, as we have proven earlier, owing to the *PayPass* contactless payment, it is enough to stand close to the victim and use their card to carry out the transaction. When you add the PIN code obtained in a thermal imaging attack to the equation, the limit set for the amount of money spent disappears completely (since it is authorized by the stolen PIN code). In order to avoid modern cybercriminals, you have to be extremely cautious and sensible while using technological devices. It is not enough to protect yourself against one threat only; you need to take safety measures against all forms of attacks, and this step requires knowledge and proactive behavior. The key action taken by manufacturers and providers of such modern devices should be raising users' awareness of potential threats and how to deal with them.

ACKNOWLEDGEMENTS

We would like to thank Mr. Janusz Rogula, PhD. Eng. of Institute of Power Engineering and Fluid Mechanics of Wroclaw University of Technology for lending measuring instruments necessary to carry out our research. We would also like to extend our gratitude to the authorities of Bank Zachodni WBK, in particular to Mrs. Monika Bejma and Mr. Rafal Wachowski, for their trust and sharing their cash machines as research tools. This research was supported by National Research Center grant PRELUDIUM no 2014/15/N/ST6/04375.

REFERENCES

Kocher, Paul, (1996). Timing Attacks on Implementations of Diffie-Hellman. *RSA, DSS, and Other Systems, Advances in Cryptology—CRYPTO'96*.

Messerges, Thomas S., Ezzy A. Dabbish, and Robert H. Sloan, (1999). Investigations of power analysis attacks on smartcards. In *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology (WOST'99)*.

Kocher, Paul, J. Jaffe, and B. Jun. (1999). Differential power analysis. *Proceedings of CRYPTO'99*, vol. 1666, pp. 388-397.

Van Eck, W. (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security 4*, 4.

Markettos, A. T. and S. W. Moore. (2009). The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators. In *Proceedings of Cryptographic Hardware and Embedded Systems (CHES). Lecture Notes in Computer Science 5747*, Springer, pp. 317-331.

Li, H., A. T. Markettos and S. W. Moore. (2005). A Security Evaluation Methodology for Smart Cards Against Electromagnetic Analysis. In *Proceedings of the 39th IEEE International Carnahan Conference on Security Technology (ICCST 2005)*, Las Palmas de Gran Canaria, Spain, pp. 208-211.

Markettos, A. T. and S. W. Moore. (2004). Electromagnetic Analysis of Synchronous and Asynchronous Circuits using Hard Disc Heads. *16th UK Asynchronous Forum*, Manchester, UK.

Zalewski, Mariusz. (2005). *Cracking safes with thermal imaging*, [online] Available at: http://lcamtuf.coredump.cx/tsafe. [Accessed 23 May 2016].

Meiklejohn, Sarah and Stefan Savage. (2011). Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks. *Proceedings of Workshop on Offensive Technologies (WOOT)*.

Snapsupplies.com. (2014). *ATM Skimming Devices,* [online] Available at: https://www.snapsupplies.com/Snap/Industry-News/ATM-Skimming-Devices_12.aspx. [Accessed 23 May 2016].

Stefan Wisniewski, Tomasz S. Wisniewski. (2012). Wymiana ciepla, *WNT*.

Hanzlik, L., W. Wodo. (2013). Identity security in biometric systems based on keystroking. *International Conference on Security and Cryptography (SECRYPT)*, Reykjavik, Iceland.

Hancke, Gerhard P., (2005). A practical relay attack on ISO 14443 proximity cards. *Technical report*, University of Cambridge Computer Laboratory.