2019 European Intelligence and Security Informatics Conference (EISIC)

HOTSPOT: Crossing the Air-Gap Between Isolated PCs and Nearby Smartphones Using Temperature

Mordechai Guri
Ben-Gurion University of the Negev, Israel
Cyber-Security Research Center
Air-gap research page: https://cyber.bgu.ac.il/advanced-cyber/airgap
Email: gurim@post.bgu.ac.il

Abstract—**Air-gapped computers are hermetically isolated from the Internet to eliminate any means of information leakage.**

In this paper we present HOTSPOT - a new type of air-gap crossing technique. Signals can be sent secretly from air-gapped computers to nearby smartphones and then on to the Internet - in the form of *thermal pings*. The thermal signals are generated by the CPUs and GPUs and intercepted by a nearby smartphone. We examine this covert channel and discuss other work in the field of air-gap covert communication channels. We present technical background and describe thermal sensing in modern smartphones. We implement a transmitter on the computer side and a receiver Android App on the smartphone side, and discuss the implementation details. We evaluate the covert channel and tested it in a typical work place. Our results show that it possible to send covert signals from air-gapped PCs to the attacker on the Internet through the thermal pings. We also propose countermeasures for this type of covert channel which has thus far been overlooked.

Index Terms—**Air-gap; covert-channels; exfiltration; thermal; temperature; smartphones.**

I. INTRODUCTION

Highly secured networks are protected by a wide range of security products including firewalls, anomaly detection systems and anti-malware programs. These networks are also kept in so-called air-gap separation, a measure in which there is no direct connection (physical or logical) between the internal network and the Internet. However, attackers are continuously finding innovative paths to infiltrate these targeted networks. Even so-called 'air-gapped' networks can be bypassed by highly motivated attackers [1], [2], [3], [4].

While compromising air-gapped networks has been shown feasible, the exfiltration of data from isolated networks is considered to be a challenging task. In order to leak data from air-gapped computers the attacker has to use non standard communication methods. Such methods use the electromagnetic [5], [6], [7], acoustic [8], [9] and optical [10], [11] mediums to encode information.

In this paper, we explore a new covert communication channel which relies on the computer temperature. We present a new attack model in which data can be exfiltrated from an air-gapped, network-less computer to the Internet via thermal signals, or 'thermal pings'. We implement a transmitter on the computer side and a receiver Android Application on the smartphone side, and discuss design and implementation. We evaluate the covert channel and test it in a typical workplace. We also propose countermeasures for this type of covert channel which thus far has been overlooked.

A. Scope of this Paper

In this paper, we demonstrate the feasibility of the PC-to-Smartphone thermal covert channel and examine the *physical layer* of this communication channel. The evaluation of various data modulation schemes for this channel is left for future work.

II. RELATED WORK

Air-gap covert channels are special communication methods that enable leakage of data from isolated, network-less systems. They are divided into six main categories: electromagnetic and electric, magnetic, acoustic, thermal, and optical. Guri and Elovici used the term *Bridgware* to describe a malware that employs non-standard covert channels to bridge the air-gap between the isolated network and the attacker [7].

A. Electromagnetic and Electric

Computer components are emitting electromagnetic radiation which can be used to carry information. Kuhn showed that it is possible to control the electromagnetic radiation generated by LCD screens [12]. In this technique, a malicious code sends radio signals with encoded data to the attacker equipped with a dedicated receiver. 15 year later Guri et al demonstrated malware that exfiltrate data from air-gapped computers to a smartphone in the same room via frequency modulation (FM) radio signals. They termed this attack as AirHopper [13], [14] and exploited the electromagnetic radiation emanated from screen cables. They showed hows the FM signals can also be received by a dedicated software defined radio (SDR) receiver [15]. Guri et al implemented GSMem [16] - a malware that leaks data from isolated computers to nearby mobile devices via cellular frequencies generated from the internal RAM bus lines. The same researcher presented an attack which generates electromagnetic signals from USB ports on desktop computers [17]. Recently, Guri et al presented PowerHammer [18] a new type of attack which uses the power-lines to exfiltrate data from isolated, network-less and air-gapped systems.

EISIC 2019, November 26-27, 2019, Oulu, Finland
978-1-7281-6735-0/19/$31.00 © 2019 IEEE

B. Magnetic

Magnetic covert channels are unique in that they can be used to bypass radio frequency (RF) blocking equipment. Guri et al presented a malware that can exfiltrate data from air-gapped computers via magnetic signals generated by the processors. In the ODINI attack [19], magnetic fields can evade Faraday cages and metal shields that used to block the electromagnetic radiation. Another type of this attack is MAGNETO [20] - malware that leaks information from isolated systems to nearby smartphones via CPU generated magnetic signals. They developed an application that used the magnetic sensors integrated in all modern smartphones.

C. Optical

In 2019 research explored the threat of leaking data via Keyboard LEDs with modern USB keyboards [21]. Guri et al showed how to use the hard drive read/write indicator LEDs in order to exfiltrate data [22]. Guri et al also presented a method to leak data via router and switch LEDs [11]. Fast flickering objects on the LCD screen [23] can also be used to carry hidden information. aIR-Jumper attack [24] is another way to communicate over air-gap. It uses the night vision IR LEDs in surveillance cameras to communicate with internal, isolated networks.

D. Acoustic

In acoustic based covert channels information is carried over sound. It is known that inaudible sound can establish a covert communication between two PC computers [25]. However, this method is limited to systems which are equipped with speakers and microphones. Fansmitter is a malware that uses the computer internal fans noise to encode and exfiltrate data [26]. In this method, the transmitting computer does not need to be equipped with audio hardware or an internal or external speaker. Guri et al also introduced a method that uses the hard disk drive (HDD) to generate covert noise which exfiltrate information to a nearby microphone [27]. More recently researchers presented an attack that covertly turns the speakers connected to a PC into a pair of eavesdropping microphones. In this attack two computers can communicate over air-gap via ultrasonic signals [28].

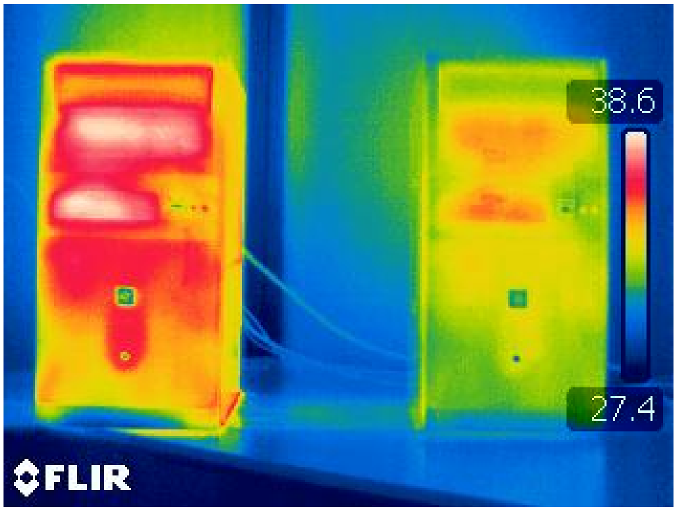


Fig. 1. The thermal view of two PCs taken with a thermal camera. The PC on the left is sending thermal pings with the HOTSPOT malware.

TABLE I
SUMMARY OF EXISTING AIR-GAP COVERT CHANNELS

Type	Method
Electromagnetic	AirHopper [13], [14] (FM radio) GSMem [16] (cellular frequencies) USBee [17] (USB bus emission) Funthenna [32] (GPIO emission)
Magnetic	MAGNETO [20] (CPU-generated magnetic fields) ODINI [19] (Faraday shields bypass) Hard-disk-drive [33]
Acoustic	Fansmitter [26] (computer fan noise) DiskFiltration [27] (hard disk noise) Ultrasonic [25], [34] MOSQUITO (speaker-to-speaker)
Thermal	BitWhisper [29] HOTSPOT (this paper) PC-to-Smartphone communication
Optical	LED-it-GO [22] (hard drive LED) VisiSploit [23] (invisible pixels) Keyboard LEDs [35] [21] Router LEDs [11]
Optical (infrared)	aIR-Jumper [24] (security cameras & infrared)

E. Thermal

BitWhisper [29] is a thermal based covert channel allowing an attacker to maintain covert communication between two close air-gapped workstations via temperature changes. The heat is generated by the processor of a standard computer and received by temperature sensors that are integrated into the motherboards. In a same principle, attackers can use the HVAC systems to deliver command and control (C&C) to air-gapped workstations and servers. Temperature-based covert channel in FPGA systems [30] and in multi-core platforms [31] have also been suggested. However these covert channels are dedicated to transferring data within the same physical platform and not between air-gapped systems. Unlike BitWhisper which works between two adjacent desktop computers, this paper discuss the thermal covert channel between a desktop computer and a nearby mobile phone.

Table I. summarizes the existing air-gap covert channels.

III. Attack Model

The adversarial attack model consists of a transmitter and a receiver. In these scenarios, the transmitter is a computer, and the receiver is a nearby mobile phone belonging to an employee or visitor.

In a first stage of the attack, the transmitter and receiver are compromised by an attacker. Infecting highly secure networks can be accomplished, as demonstrated by the attacks involving Stuxnet [36], Agent.Btz [37], and others [38], [39], [40]. In addition, mobile phones of employees can be identified, by social engineering techniques and other means. Employees are

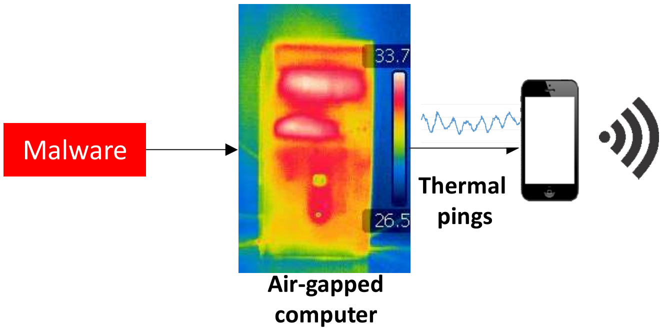


Fig. 2. The leakage scenario. Malware in the air-gapped computer causes heat fluctuations within the CPU and GPU. The heat is emitted in a form of thermal pings and received by a nearby smartphone. The signals are sent to the attacker via the Internet.

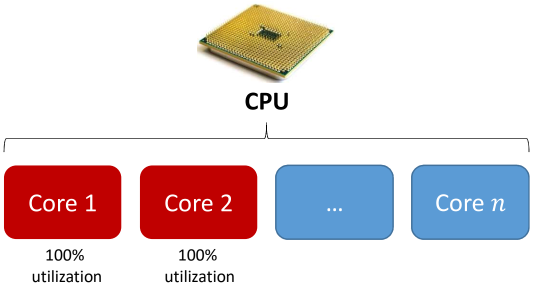


Fig. 3. The HOTSPOT heating code. In this case core #1 and core #2 are overloaded using busy loops.

assumed to carry their mobile phones around the workplace. These devices can then be infected either online, by exploiting a device's vulnerabilities, or by physical contact if possible. Various attack vectors, including using emails, SMS/MMS, malicious apps, and malicious websites [41], [42], [43], [44], [45] can be used to infect a mobile phone.

In the exfiltration phase, malware in the compromised computer transmits signals to the environment via thermal pings emitted from the CPU or GPU (as can be seen in Figure 2). A nearby infected mobile phone detects the transmission, demodulates and decodes the data, and transfers it to the attacker via the Internet.

IV. Transmission & Reception

A. Transmitter

As described in [29], due to the law of conservation of energy excess power dissipates as heat. This physical process known as Joule heating and is sometimes also referred to as ohmic heating or electrical resistance heating. When electric current pass through a conductor it emit heat which is proportional to the current and voltage in the wires. Complex electronic systems such as the central processing unit (CPU) and its cores requires varying amounts of power proportional to the workload of the processes and threads in the operating system. This workload directly affects the amount of heat generated by the CPU. Other heat sources in a computer include the graphics processing unit (GPU), the power-supply and various mechanical systems such as a hard disk drives (HDD) and optical drives (CD/DVD).

In our experiments, we used the CPU as a source of heat. In order to generate heat, we increased the workload of the CPU cores using a group of worker threads. Each thread was bound to a specific core after its creation. The threads executed busy loops to increase the utilization of the core to the maximum in a short period of time. Algorithm 1 shows the basic program used to overload each core for ms milliseconds. We used n worker threads and bound each thread to a specific core using the Linux *sched_setaffinity* system call [46]. Note that in addition to the CPU, other components on the computer can also be used to generate heat, including the HDDs, CDs/DVDs and GPUs. However, in this paper we evaluate the CPU as the main source of heat in a PC.

To transmit the data we used the On-Off Keying (OOK) modulation. Logical '1' is represented by emitting heat for a time period of x seconds, while logical '0' is represented by stopping heat emission for y seconds.

Algorithm 1 workload (*ms*)

```
$T1 \leftarrow getCurrentTime()$
while ($getCurrentTime() - T1 < ms$) do ;
end while
```

B. Receiver

We implemented a receiver as an application running on the Android OS. The *Thermo-Logger* receiver app samples the thermal sensor and performs signal processing. The temperature values were recorded with a Samsung Galaxy S7 (G930F) smartphone, running the Android OS version 8.0 (Nougat).

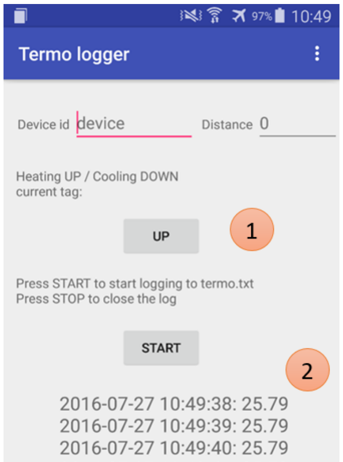
Modern smartphones are commonly shipped with three types of thermal sensors: (1) the battery temperature sensor, (2) the CPU temperature sensor(s), and (3) the ambient temperature sensor. We used the ambient temperature sensor to measure the thermal values as it appears to be the most sensitive to environmental temperature changes.

The main Thermo-Logger function runs in a separate thread. It is responsible for data sampling, signal processing and data demodulation. In our case we sampled the ambient thermal sensor using the Android environment sensors API. We used the type TYPE_AMBIENT_TEMPERATURE to sample the ambient temperature via the thermal sensor.

The *Thermo-Logger* app (Figure 4) samples and logs the ambient temperature every second (two in Figure 4). It then specifies the current change in temperature; UP for an increase in temperature, and DOWN for a decrease in temperature. The App logs the time and temperature to a CSV file for further analysis with MathWork MATLAB software.

V. Evaluation

Our experimental setup consists of a desktop computer and four smartphones for reception, each of which is installed with



Device id device

Distance 0

Heating UP / Cooling DOWN
current tag:

Press START to start logging to termo.txt
Press STOP to close the log

2016-07-27 10:49:38: 25.79
2016-07-27 10:49:39: 25.79
2016-07-27 10:49:40: 25.79

Fig. 4. The Thermo-Logger Android app.

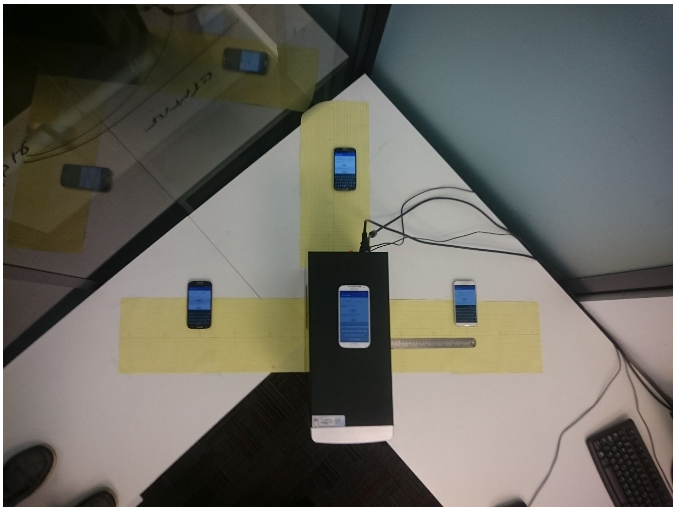


Fig. 5. The experimental setup.

the Thermo-Logger app (as seen in Figure 5). We used an off-the-shelf Desktop PC SilverStone FSP300-50HMN 300W with an Intel Core i7-4770 CPU 3.4GHz and four cores. During the tests, we overloaded the four cores to achieve the desired thermal effect. Because of the support in hyper-threading, each core was overloaded with two threads. With Intel's hyper-threading technology, for each processor core that is physically present, the operating system addresses two logical cores and shares the workload between them when possible.

Figure 6 graphs the thermal signals as received by a smartphone placed on the computer case. This represents the scenario in which a smartphone is placed on the workstation. This attack scenario can happen unintentionally, e.g., by an employee that places his/her phone on a workstation. It also can happen intentionally, e.g., by a malicious insider or visitor that places his/her phone on the computer. As can be seen, an increase of 0.5C in the temperature could be sensed by the smartphone after 10 seconds. This allows a single thermal ping to be sent from a computer in 10 seconds. More complex data transfer using OOK modulation works at a rate of a ping every 30 seconds (heating up) and a ping per 180 seconds (cooling down).

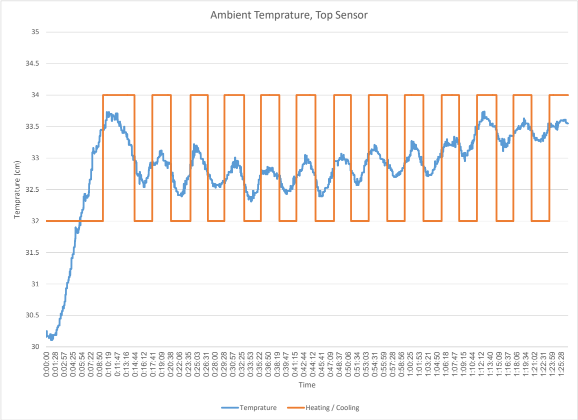


Fig. 6. The measurements from the smartphone placed directly on top of the computer.

Figures 7 and 8 graph the thermal signals received by smartphones placed on the right and left side of the computer case, respectfully, at distances of 10cm, 30cm, and 50cm from the computer case. This represents the scenario in which a smartphone was placed on the desktop near a compromised computer. As in the previous cases, this attack scenario can happen unintentionally or intentionally. As can be seen, at all three distances the thermal pings could be sensed by the smartphone. However, at distances of 30 and 50cm, the reception is much slower and takes between 60 and 120 seconds for each thermal ping. Note that the smartphone on the right side received the thermal pings faster than the smartphone on the right. This is because the heat diffusion hole is located on the right side of the computer case. The left side is blocked by the metal wall which absorbs the heat and prevents it from diffusing (Figure 9).

Figure 10 graphs the thermal signals received by a smartphone located behind the computer, at distances of 10cm, 30cm, and 50cm. As can be seen, at all three distances the thermal pings could be sensed by the smartphone. However, at all the distances it takes between 120 and 200 seconds for the smartphone to receive the increase in temperature. Note that a smartphone located behind the computer is an unusual scenario and is not likely to be part of a typical attack model.

A. Laptops

We also evaluated the thermal covert channel between a laptop and a nearby smartphone. In this case, we used the Dell Latitude 7480 laptop with an Intel Core i7-7600U. Our experiments showed that the thermal covert channel is effective at a range of 0-25cm. However , the thermal pings reach the smartphone only if it was positioned parallel to the laptop's

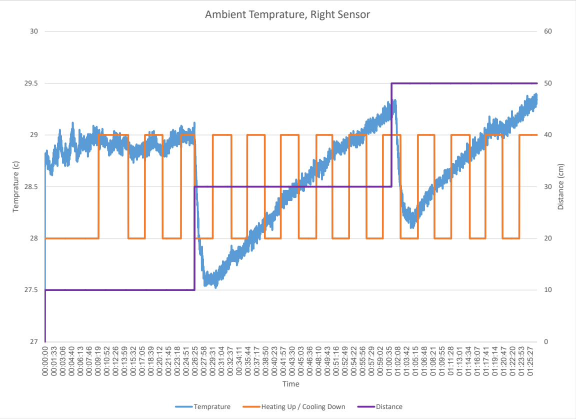


Fig. 7. The measurements from the smartphone placed on the right side of the computer case.

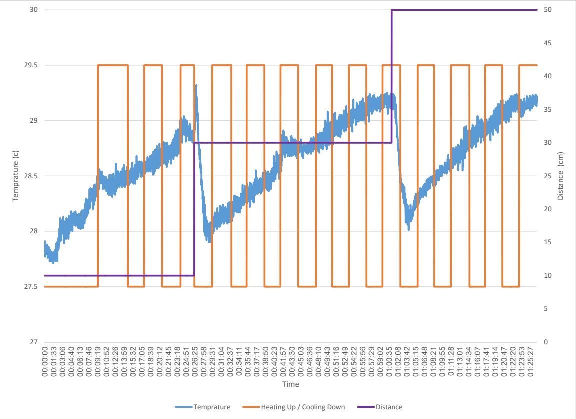


Fig. 8. The measurements from the smartphone placed on the left side of the computer case.

airflow hole (Figure 11). As can be seen in Figure 12 an increase of over 2C was measured from a smartphone located 25cm from the laptop, a case in which it takes 60 seconds to measure the two degree increase in the environmental temperature.

Given the results above, we consider three threat perimeters for the thermal covert channel (Figure 13). A distance of the 0cm where the smartphone is in direct contact with the compromised computer poses the greatest threat. Distances of 10-30cm between the computer and the smartphone represent a medium threat in which it takes tens of seconds for each ping to be transmitted. Distances of 30cm or greater between the computer and the smartphone pose the lowest threat, where the thermal pings take more than 60 seconds to reach the smartphone.

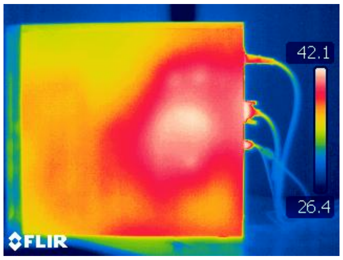


Fig. 9. The thermal view of the side wall of the computer during the thermal ping experiments.

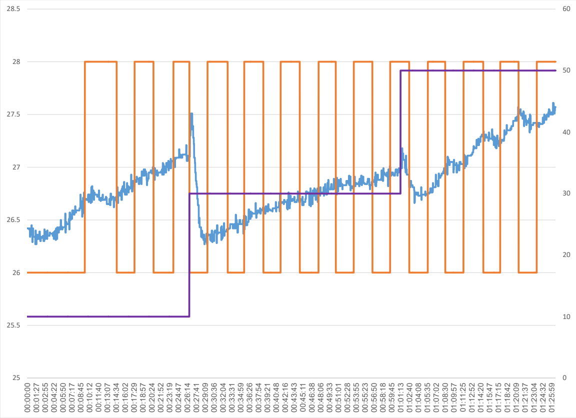


Fig. 10. The measurements from the smartphone placed behind the computer case.

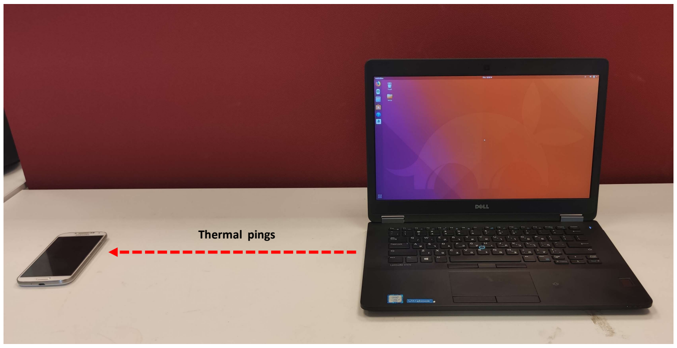


Fig. 11. The laptop experimental setup.

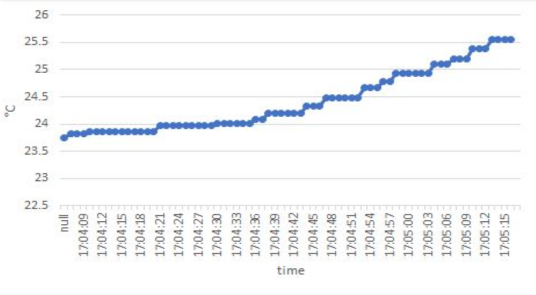


Fig. 12. The measurements from the smartphone placed 25cm from the laptop.

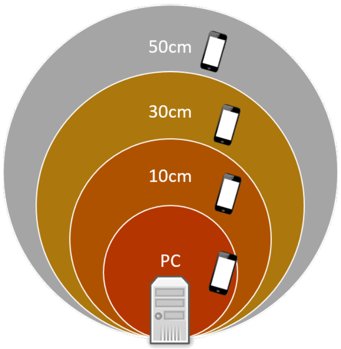


Fig. 13. The threat radius of the thermal covert channel.

VI. Countermeasures

TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) is a term used by the U.S. National Security Agency (NSA) and NATO to refer to spying on information systems through leaking emanations. The TEMPEST standard originally referred to the monitoring and shielding of devices that emit electromagnetic radiation (EMR). However, today many standards also refer to other types of emanations such as acoustic, magnetic and optical emissions. In the context of the HOTSPOT attack the 'zoning' approach may be taken. In this approach, electronic devices with different classification levels are kept at certain minimal distance. This effectively prevents signal propagation and reception between the two devices. In particular, the organization may define spatial regions where mobile phones are prohibited. However, enforcing minimal distances between electronic devices (e.g., workstations and smartphones) is not always possible. Another solution may be to detect anomalous thermal emissions using the workstation's internal sensor, e.g., the CPU/GPU and motherboard thermal sensors. However, the thermal sensors integrated in the computer are not considered trusted since malware (e.g., rootkits) can compromise the temperature values. Monitoring can also be done externally by a dedicated thermal sensor (hardware) placed near the computer. However, the application of external thermal monitors on a per computer basis is less practical due to cost and maintenance considerations. Thermal cameras can also be used to closely monitor the thermal behavior of a system. In this case, image processing and anomaly detection approaches may be used to identify covert thermal communication. However, such a solution is only relevant as a specialized forensic investigation tool and cannot be deployed on a wide scale.

Table II contains a list of the defensive approaches.

VII. Conclusion

In this paper, we show that a small amount of data can be exfiltrated from air-gapped computers to the Internet via heat. Given a malware running on a computer that generates heat fluctuations by regulating the utilization of the CPU and GPU, we show that the heat emitted from the computer can be sensed by a smartphone located up to a maximum distance of 50cm away from the computer. Binary data can be modulated on top of the thermal fluctuations, and then it can be decoded in the smartphone and sent to the attacker via the Internet. Although the covert channel is slow, it can be used to break through the hermetic isolation of sensitive computers. We propose defensive countermeasures to this currently overlooked air-gap covert channel.

TABLE II
Countermeasures

Countermeasure	Type	Cons
'Zones' approach	Prevention	Requires maintenance
Water cooling systems	Prevention	Cost
Heat and CPU monitoring	Detection	Can be evaded
Monitoring (thermal camera)	Detection	Cost and maintenance
Generate random thermal changes	Jamming	Cost and maintenance

References

[1] D. Goodin, "How "omnipotent" hackers tied to NSA hid for 14 yearsand were found at last," arc TECHNICA, Feb. 2015. [Online]. Available: https://arstechnica.com/information-technology/2015/02/

[2] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proc. IECON 2011 - 37th Annual Conf. of the IEEE Industrial Electronics Society*, Nov. 2011, pp. 4490–4494.

[3] B. Knowlton, "Military computer attack confirmed," NY Times, Aug. 2010. [Online]. Available: http://www.nytimes.com/2010/08/26/technology/26cyber.html

[4] S. Stasiukonis, "Social engineering, the USB way," Dark Reading, Jun. 2006. [Online]. Available: https://www.darkreading.com/attacks-breaches/social-engineering-the-usb-way/d/d-id/1128081

[5] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations." in *Information hiding*, vol. 1525. Springer, 1998, pp. 124–142.

[6] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," Ph.D. dissertation, University of Cambridge, 2002.

[7] M. Guri and Y. Elovici, "Bridgeware: The air-gap malware," *Commun. ACM*, vol. 61, no. 4, pp. 74–82, Mar. 2018. [Online]. Available: http://doi.acm.org/10.1145/3177230

[8] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *Journal of Communications*, vol. 8, no. 11, pp. 758–767, Nov. 2013.

[9] T. Halevi and N. Saxena, "A closer look at keyboard acoustic emanations: random passwords, typing styles and decoding techniques," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*. ACM, 2012, pp. 89–90.

[10] J. Loughry and D. A. Umphress, "Information leakage from optical emanations," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 3, pp. 262–289, 2002.

[11] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xled: Covert data exfiltration from air-gapped networks via switch and router leds," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018, pp. 1–12.

[12] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations." in *Information hiding*, vol. 1525. Springer, 1998, pp. 124–142.

[13] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*. IEEE, 2014, pp. 58–67.

[14] M. Guri, M. Monitz, and Y. Elovici, "Bridging the air gap between isolated networks and mobile phones in a practical cyber-attack," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 8, no. 4, p. 50, 2017.

[15] M. Guri and M. Monitz, "Lcd tempest air-gap attack reloaded," in *2018 IEEE International Conference on the Science of Electrical Engineering in Israel (ICSEE)*. IEEE, 2018, pp. 1–5.

[16] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "Gsmem: Data exfiltration from air-gapped computers over gsm frequencies." in *USENIX Security Symposium*, 2015, pp. 849–864.

[17] M. Guri, M. Monitz, and Y. Elovici, "Usbee: Air-gap covert-channel via electromagnetic emission from usb," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*. IEEE, 2016, pp. 264–268.

[18] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines," *ArXiv e-prints*, Apr. 2018.

[19] M. Guri, B. Zadov, and Y. Elovici, "Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," *IEEE Transactions on Information Forensics and Security*, 2019.

[20] M. Guri, A. Daidakulov, and Y. Elovici, "Magneto: Covert channel between air-gapped systems and nearby smartphones via cpu-generated magnetic fields," *arXiv preprint arXiv:1802.02317*, 2018.

[21] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "Ctrl-alt-led: Leaking data from air-gapped computers via keyboard leds," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1. IEEE, 2019, pp. 801–810.

[22] M. Guri, B. Zadov, and Y. Elovici, *LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED*. Cham: Springer International Publishing, 2017, pp. 161–184. [Online]. Available: https://doi.org/10.1007/978-3-319-60876-1_8

[23] M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "An optical covert-channel to leak data through an air-gap," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*. IEEE, 2016, pp. 642–649.

[24] M. Guri and D. Bykhovsky, "air-jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (ir)," *Computers & Security*, vol. 82, pp. 15–29, 2019.

[25] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *arXiv preprint arXiv:1406.1213*, 2014.

[26] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers," *arXiv preprint arXiv:1606.05915*, 2016.

[27] ——, "Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise (diskfiltration)," in *European Symposium on Research in Computer Security*. Springer, 2017, pp. 98–115.

[28] M. Guri, Y. Solewicz, and Y. Elovici, "Mosquito: Covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker communication," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 2018, pp. 1–8.

[29] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations," in *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*. IEEE, 2015, pp. 276–289.

[30] T. Iakymchuk, M. Nikodem, and K. Krzysztof, "Temperature-based covert channel in fpga systems," in *6th International Workshop on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)*. IEEE, 2011, pp. 1–7.

[31] R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, "Thermal covert channels on multi-core platforms," in *24th {USENIX} Security Symposium ({USENIX} Security 15)*, 2015, pp. 865–880.

[32] "funtenna - github," https://github.com/funtenna, 2016, (Accessed on 14/06/2018).

[33] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors," in *Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific*. IEEE, 2016, pp. 525–532.

[34] B. Carrara and C. Adams, "On acoustic covert channels between air-gapped systems," in *International Symposium on Foundations and Practice of Security*. Springer, 2014, pp. 3–16.

[35] J. Loughry and D. A. Umphress, "Information leakage from optical emanations," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 3, pp. 262–289, 2002.

[36] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[37] R. Grant, "The cyber menace," *Air Force Magazine*, vol. 92, no. 3, 2009.

[38] "The epic turla (snake/uroburos) attacks — virus definition — kaspersky lab," https://www.kaspersky.com/resource-center/threats/epic-turla-snake-malware-attacks, 2018, (Accessed on 12/03/2017).

[39] K. ZAO, "Red october diplomatic cyber attacks investigation," 2018.

[40] "A fanny equation: "i am your father, stuxnet" - securelist," https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/, 2018, (Accessed on 12/03/2017).

[41] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, N. Modadugu *et al.*, "The ghost in the browser: Analysis of web-based malware." *HotBots*, vol. 7, pp. 4–4, 2007.

[42] M. Cova, C. Kruegel, and G. Vigna, "Detection and analysis of drive-by-download attacks and malicious javascript code," in *Proceedings of the 19th international conference on World wide web*. ACM, 2010, pp. 281–290.

[43] A. K. Sood and R. J. Enbody, "Malvertising–exploiting web advertising," *Computer Fraud & Security*, vol. 2011, no. 4, pp. 11–16, 2011.

[44] T. R. Peltier, "Social engineering: Concepts and solutions," *Information Systems Security*, vol. 15, no. 5, pp. 13–21, 2006.

[45] C. Smutz and A. Stavrou, "Malicious pdf detection using metadata and structural features," in *Proceedings of the 28th annual computer security applications conference*. ACM, 2012, pp. 239–248.

[46] "sched_setaffinity(2) - linux man page," https://linux.die.net/man/2/sched_setaffinity, (Accessed on 05/04/2018).