Covert Channels Using Mobile Device's Magnetic Field Sensors

Nikolay Matyunin[1], Jakub Szefer[2], Sebastian Biedermann[1], and Stefan Katzenbeisser[1]

[1]Security Engineering Group, Technische Universität Darmstadt
{matyunin, biedermann, katzenbeisser}@seceng.informatik.tu-darmstadt.de

[2]Computer Architecture and Security Laboratory, Yale University
jakub.szefer@yale.edu

This paper presents a new covert channel using smartphone magnetic sensors. We show that modern smartphones are capable to detect the magnetic field changes induced by different computer components during I/O operations. In particular, we are able to create a covert channel between a laptop and a mobile device without any additional equipment, firmware modifications or privileged access on either of the devices. We present two encoding schemes for the covert channel communication and evaluate their effectiveness.

I. Introduction

Use of firewalls and intrusion detection systems are some of the common ways to protect computer systems from network attacks, or to prevent sensitive information from being sent out from a computer system. This way organizations can apply strict network security policies to prevent unauthorized accesses to sensitive data. Furthermore, many security-aware organizations install so-called air-gapped computers, where computers containing sensitive data are completely separated from other devices and the Internet. Usually, any network communication is forbidden on these computers and the use of removable media is limited.

To circumvent such security measures, attackers can use covert channels to establish communication between devices. We expect that security-aware organizations can also restrict the use of hardware in air-gapped networks or any other sensitive areas. For this reason, if a covert channel requires some dedicated equipment on either transmitter or receiver side, it may not be practically applicable. The goal of our work is thus to evaluate how attackers could create such covert channels which do not require special hardware.

Taking into account aforementioned requirements, we present a new covert channel based on using smartphone magnetic sensors, also called magnetometers. As the industrial cost of magnetic sensors is very low [14], they are integrated in most modern smartphones and wearable devices. At the same time, it has been recently shown in [3] that magnetometers are capable to detect magnetic fluctuations from hard drives and therefore can be used in side-channel attacks. In our work, we extend this approach to covert channels and show that magnetic sensors from off-the-shelf mobile devices are able to detect magnetic field fluctuations at distance of multiple centimeters from the target device.

The magnetic field covert channel is established between a sender and a receiver. The sender is assumed to be a typical computer equipped with a magnetic hard drive, and our experiments use a common Lenovo laptop. The receiver is assumed to be a modern smartphone with a magnetometer.

To emit the signal, we invoke basic input/output operations on the sender. While electromagnetic (EM) emanations caused by CPU and memory instructions have been used for covert channels earlier [4, 8], we explore the magnetic field emitted by the movements of the hard drive magnetic head. Our solution takes into account several available EM field sources and uses the combined signal as the channel for the covert communication. The setup is not limited to a specific hardware configuration, and the transmitter code runs in regular user space without having privileged access to the operating system.

To transmit data, we demonstrate the use of amplitude modulation encoding scheme and present the scheme based on periodic emanations, which appears to be more robust in a noisy environment.

To receive the signal, we implement an Android application which runs on any modern Android smartphone. As the use of magnetometer data does not need any explicit permissions granted by the user, this code can be a part of malware and run as a background process unbeknown to the user.

As a summary, we provide the following novel contributions to the field:

- We introduce using smartphone magnetic sensors to establish a covert channel. The presented solution does not require any dedicated equipment, firmware patching or even special permissions from the operating system.

- We propose using both electronic circuits and a movement of a hard drive magnetic head as sources of EM signals and introduce a modulation scheme, suitable for a majority of computer configurations without any hardware restrictions.
- We present the implementation of our covert channel, evaluate its practically achievable distance and corresponding bitrate, and compare our implementation with existing solutions.

II. Technical background

A. Magnetic field strength

The magnetic field is defined at a given point by its direction and strength, which is measured in Tesla (T). In particular, the magnetic field of the earth ranges between $25\mu T$ and $60\mu T$ at the surface [13]. It is directed roughly parallel to the surface and thus leads to additional noise on this plane during our measurements. More comprehensive information about magnetic fields can be found in books, such as [16].

In our experiments the emitted signal strength has been less than $100\mu T$ even directly at the source (nearly 1cm from the source). We observed average permanent noise fluctuations of $0.5\mu T$. Given the fact that the magnetic field strength quadratically depends on the distance from the source, theoretically the signal from a single source will be suppressed by noise at the distance of more than 20cm.

B. Magnetic field sensors

Modern smartphones are equipped with magnetic sensors, also called magnetometers. Magnetic sensors measure the ambient geomagnetic field for all three physical axes in μT. In Android devices, these values are accessed by using *Sensor* API class and oriented as follows: for default portrait device screen orientation, the X axis points to the right in the plane of screen, the Y axis is vertical and points up, and the Z axis points out of the front of the screen [1].

Unlike other components of the device, such as microphone, camera or Bluetooth module, the use of magnetometer in the application does not require explicitly granted permission from the user. Therefore, the code we use in our solution can be injected into an outwardly legitimate application and run silently from the user, making the electromagnetic channel suitable signal media for our attack scenario.

C. Electromagnetic emissions during I/O operations

We discover two sources of EM fluctuations during I/O operations, performed on the laptop. Any single writing or reading from the file leads to an EM peak, which can be measured at locations A and B indicated in Fig. 1.

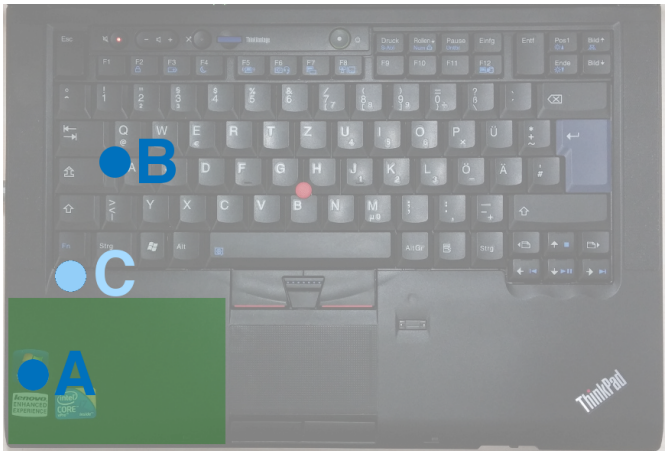

Fig. 1. The position of the hard drive (green), sources of EM signal A, B and intermediate point C.

The fluctuations at the point A are initiated by the movements of the hard drive magnetic head. To shift the head into another position, current is passed over the wires of a head actuator mechanism. As a result, the electromagnetic field arises and displaces the magnetic head.

As mentioned in [3], the hard disk magnetic platters themselves do not generate a magnetic field which is strong enough to be detected outside disk's chassis. However, we expect that the presence of these magnets can affect and interfere with electromagnetic field initiated by other sources.

The position B coincides with the location of the laptop's CPU. The signal is apparently generated by the circuits of the bus between CPU and RAM during data exchange, as was previously discovered in [8].

Fig. 2 shows the shape of a signal recorded at the positions A, B and at the intermediate point C. Signals clearly differ in both shape and amplitude. Even though the signal at point A is the strongest (one can see peaks up to $100\mu T$), it is shielded by the drive chassis. As a result, we could detect it only in close proximity to the hard drive. On the contrary, the signal at point B appears to be the most stable at a distance. One can also notice that at the intermediate point sharp peaks become smaller, but the main disturbance of nearly $5\mu T$ remains stable. This disturbance is observed even at a distance and may be caused by another signal source.

One can notice that produced peaks interfere with each other in the intermediate points. Therefore, it is reasonable to take into account all the discovered sources during exploration of the covert channel. As we do not focus on a specific shape and analyze the combined signal, our proposed method is suitable for different hardware configurations.

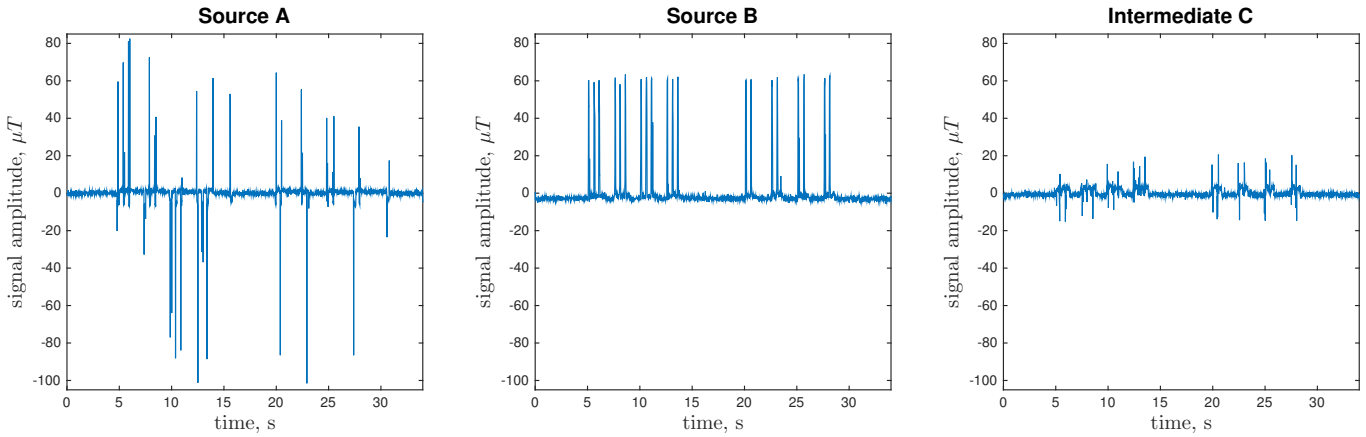

Fig. 2. Measured EM-fluctuations at points A, B and intermediate point C.

III. Magnetic Covert Channel Attacks

A. Attack model and test setup

We consider a basic covert channel scenario with two devices: a laptop containing sensitive target information to be extracted, and a smartphone, which serves as a receiver.

The laptop is considered to be a part of a security-aware network or be even isolated behind an air-gap. In any case, the attacker has no physical or network access to it and may not use existing communication channels. Instead, he wants to transmit data through the covert channel. We assume that at some point the laptop has been infected by the attacker's code. How the infection happens is outside the scope of this work. Our prototype code can be described as follows:

- it can be run in regular user's space without privileged access;
- it requires the rights to write data up to 1Mb both to RAM and to one specific file on the hard drive;
- currently, the implementation has less than 100 lines of code.

We do not rely on a specific hardware configuration and consider any commonly-used laptop as possible target. In our tests, we used an unmodified Lenovo T410 running Ubuntu 14.04.

We assume that the smartphone has at least temporary access to a lower-level security network and therefore is able to transmit data to the attacker at least once. As mentioned before, the device should be equipped with a receiver code, which does not require explicit permissions from the user and can be silently run in a background. We assume that at least for some time the device may be naturally located near the target laptop. In our experiments, we have been using an unmodified Nexus 4 smartphone running Android 5.1. Currently, our prototype implementation receives the raw EM-signal and sends it over the network to another workstation to decode the data, but the decoding can be easily implemented directly on a smartphone. Basic setup environment is shown in Fig. 3.

Fig. 3. Demonstration of the working environment. Smartphone is silently receiving EM-signal from the laptop at the distance of 12cm.

As the bandwidth of the covert channel is low compared to regular communication channels, such as TCP/IP network or Bluetooth, the attack scenario focuses on the transmission of small amounts of sensitive data up to several kilobytes, e.g. passwords or cryptographic keys. In our experiments we transmit raw binary data sequences and evaluate the corresponding bit error rate.

B. Basic signal generation

To generate a single peak in the signal, we write some amount of random data to a specific file on the hard drive. The use of a single write to the file as a base pattern of our modulation is based on the following considerations:

1. The operation affects both CPU ↔ RAM and RAM ↔ hard drive communications, producing EM fluctuations from several aforementioned sources at once.

2. Even the same I/O operations produce peaks of different shape and amplitude. We discovered that the single write of data to the RAM sometimes results in two consecutive peaks instead of a single one due to cache replacement algorithms. Therefore, we cannot fully control the shape of produced peaks even for basic operations.

3. The use of more complex peak patterns becomes not applicable far from the signal source. At distances where the signal strength is comparable to noise, specific shapes of peaks are not distinguishable, while the overall fluctuation of the field is still noticeable.

C. Signal retrieval

The emitted signal is to be retrieved and decoded by the code running on the smartphone. We implemented an Android application that receives 50 measurements per second from magnetic sensors, waits for a signal start sequence and decodes the signal.

The signal decoding is performed in two steps. First, we discover the direction of the signal based on three-dimensional data obtained from magnetic sensors. Second, we demodulate the data according to the encoding scheme. Based on the basic ability to emit a single peak, we propose two alternative schemes to encode the data and describe them in subsequent sections in detail.

D. Direction of the signal

The emitted magnetic fluctuation may have an arbitrary direction relative to the measurement axes at every particular point. Moreover, the signal vectors of different magnetic field sources have different directions and interfere with each other.

We propose the following approach to discover the most suitable direction for detection. As the transmission of data results in the disturbance of the magnetic field, it is reasonable to search for a direction with the biggest variance across the values inside a time frame. To achieve this, we apply Principal Component Analysis (PCA) [12] to the three-dimensional data and use the first component for subsequent signal decoding.

However, at a distance where the signal strength is comparable to noise, any random strong noise peak leads to the wrong choice of the direction. In this case, we follow the method proposed in [3] and use measurements received on z axis, since the earth's magnetic field may cause additional noise along x and y axes in case the phone lying on a table.

E. Information encoding — Amplitude modulation

As a first encoding method, we apply simple amplitude modulation of the signal. We emit a peak within a basic time frame of length t_0 to encode a 1 and perform no activity to encode a 0. The encoding is illustrated in the Fig. 4 (on the left). As mentioned, we could not precisely control the width and amplitude of peaks. This makes it difficult to use differential encoding schemes, based on changes in the produced peaks rather than on their level.

In this scheme, the bitrate is restricted by the duration of the basic time frame, e.g. $t_0 = 0.2s$ results in a bitrate of 5 bit/s. Therefore, the theoretical maximum bandwidth is limited by the fact that a basic time frame must exceed the time required to produce single peak. During our experiments, we were able to achieve an effective bitrate of up to 4 bit/s.

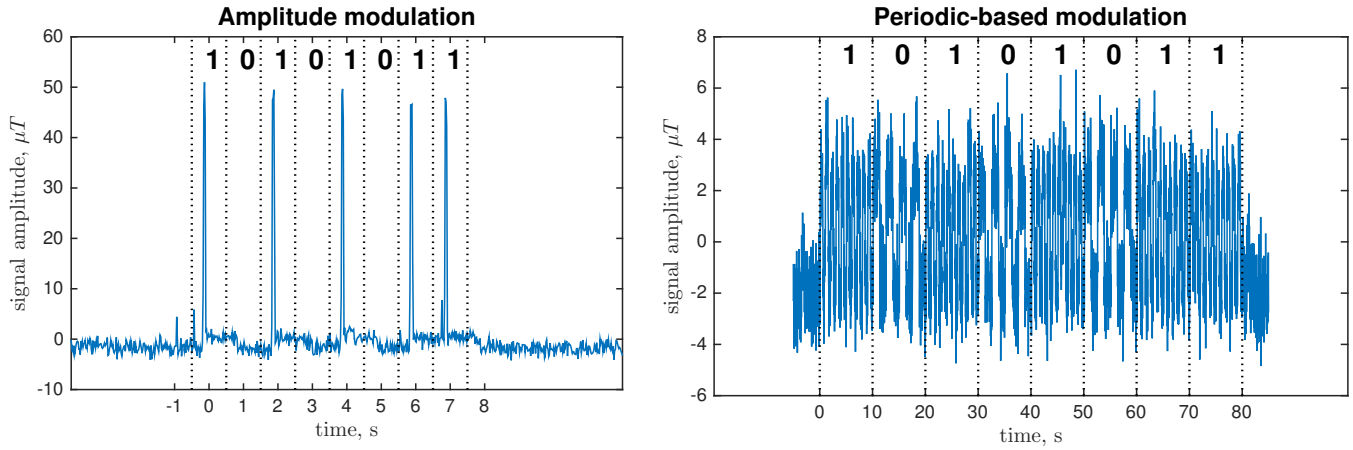

Fig. 4. Examples of two modulation schemes. Amplitude modulation: $t_0 = 1s$, bitrate is 1bit/s. Periodic-based modulation: $t_0 = 0.25s$, $t = 10s$, $p_0 = 5$, $p_1 = 3$, bitrate is 0.1bit/s.

On receiver's side, we calculate the cross-correlation between the recorded window of 4 basic frames and signals for every possible 4-bit sequence, previously recorded at the position close to the signal sources. The sequence which results in the highest correlation is considered as the decoded sequence.

In comparison to the simple detection of a local maximum within the time window, the proposed method does not require the evaluation of noise ratio threshold and naturally provides time synchronization correction, since cross-correlation lookup is performed in a small interval near the start time.

F. Information encoding — Periodic-based modulation

Although the amplitude modulation scheme provides good bandwidth, it shortly becomes not applicable at a distance. When the signal strength is comparable to noise, the detection of a single peak is no longer possible, while the average field disturbance caused by several consecutive peaks is still visually noticeable.

To overcome this problem, we propose a second encoding scheme based on periodic peak emissions and which is similar to square wave frequency modulation (SWFM) technique [17]. We choose two small primes p_0 and p_1 and a time frame t which divides both $2p_0$ and $2p_1$. Then, to encode a 0, we emit p_0 consecutive single peaks followed by p_0 basic time frames with no activity, and repeat this pattern $t/2p_0$ times within the time frame t. Similarly, we encode a 1 using periodically repeated p_1 consecutive peaks. The encoding scheme is illustrated in the Fig. 4 (on the right).

During decoding, we search for periodicity in the signal within a window of t basic frames using frequency analysis. More specifically, we perform the Fast Fourier Transform, detect peaks and choose the bit which corresponds to the peak frequency.

As we use t basic time frames to encode one bit, the maximum bitrate is limited by the length of the basic time frame (t_0) and the optimal value of t, which corresponds to the number of pattern repetitions to be correctly discovered. For this reason, the maximum bitrate can be evaluated only empirically.

Although the proposed method has a limited bitrate, it does not depend on the shape and amplitude of peaks and requires only the presence of noticeable periodic field disturbance during peak emission. Therefore, we consider this method as universal for different hardware configurations and signal sources of different nature.

IV. Feasiblity Analysis

In this section we evaluate the performance of our channel. First, we demonstrate the dependency of the signal strength on the distance by measuring the average amplitude of emitted peaks. This experiment allows us to evaluate the feasibility of the channel at certain distances independently of the encoding scheme. Second, we investigate the area outside the laptop in which the signal can be successfully decoded using both modulation schemes with a bit error rate (BER) of less than 30%, so that introduced errors could be corrected by an error-correcting code. This experiment allows to estimate the efficiency of both modulation schemes and indicates limits on the physical location of the receiver. Finally, we demonstrate how distance and increased bitrate gradually affect the error rate, again using both modulation schemes.

A. Average signal strength

To estimate the dependency of the signal strength on the distance, we emitted consecutive basic peaks and measured their average amplitude at a certain distance. Fig. 5 shows the strength of the signal at a specific distance from the source B along the axis parallel to the chassis of the laptop.

One can see the rapid attenuation of the signal amplitude, which conforms to the theoretical quadratic dependence between the strength of a magnetic field and the distance from the source. Single peaks become almost unnoticeable at a distance of 16cm and more, since their average amplitude is less than $2\mu T$, comparable to the amplitude of random noise peaks.

B. Presence of the signal

As shown in the previous section, the signal from a basic peak exceeds noise only in a very limited area. At the same time, even if the signal strength is comparable to noise, an overall disturbance of the field can be measured.

Fig. 6 demonstrates the area outside the laptop where we successfully decoded a signal with BER of less than

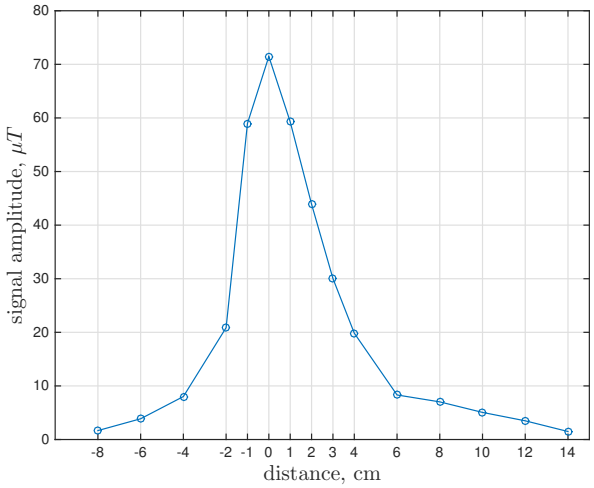

Fig. 5. Magnitude of the signal depending on the distance from the source B.

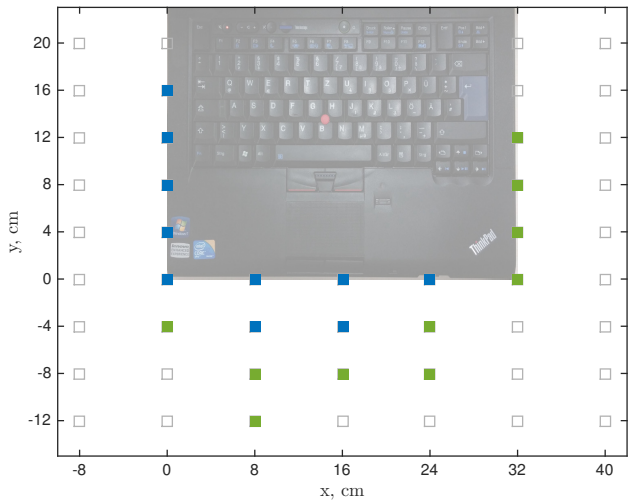

Fig. 6. Presence of the signal. Green marks show a successfully decoded signal using the periodic-based scheme. Blue indicate positions where both encoding schemes are feasible. White marks indicate no detectable signal. We use the following parameters: amplitude modulation: $t_0 = 0.5s$, bitrate 2bit/s; periodic-based modulation: $t_0 = 0.25s$, $t = 15s$, $p_0 = 3$, $p_1 = 5$, bitrate 0.067bit/s.

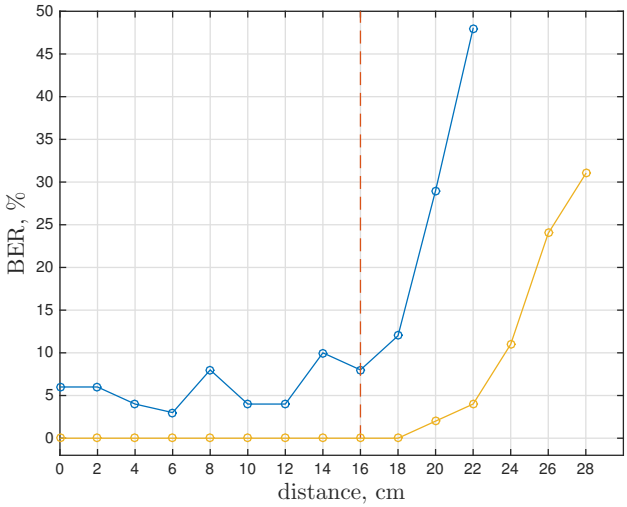

Fig. 7. BER depending on the distance from the point B. Area outside the laptop starts from 16cm. We use the following parameters: amplitude modulation (blue): $t_0 = 0.5s$, bitrate 2bit/s; periodic-based modulation (yellow): $t_0 = 0.25s$, $t = 15s$, $p_0 = 3$, $p_1 = 5$, bitrate 0.067bit/s.

30% using each decoding scheme. We consider this value of BER as practically suitable, since in this case decoding can be improved by using error-correcting codes.

The results show that the amplitude modulation scheme is applicable only to a very limited area up to 4cm in front of the laptop and directly near its left side. On the contrary, the periodic-based modulation is applicable in a comparably larger area up to 12cm in front of the laptop and close to its sides. Therefore, we consider the periodic-based modulation scheme as more practically suitable. We assume that laptop speakers located on the left and right sides impair the signal, therefore the available area on the sides of the laptop is relatively small.

C. Achieved distance and corresponding bit error rate

In this section we investigate how the distance from the source affects decoding bit error rate. Although in our attack scenario we suppose that a smartphone is placed near the laptop, we evaluate the bit error rate if the reciever is placed at the point B and moved towards the front of the laptop, to show how decoding is influenced by the attenuation of the signal strength.

Fig. 7 demonstrates that both schemes correctly decode transmitted data inside the chassis of the laptop. As mentioned before, the shape of peaks depends on the distance from the source. Therefore, noticeable errors occur even near the source for the amplitude modulation scheme, as it compares the signal with predefined patterns during the decoding. At the same time, different shapes of peaks do not affect the periodicity of the signal, and the periodic-based scheme demonstrates a robust BER of zero inside the laptop chassis. Outside the laptop, the level of the signal becomes comparable to noise and the BER immediately increases. Still, the periodic-based scheme shows less errors and is feasible up to roughly 28cm distance.

D. Bitrate and corresponding bit error rate

We conclude our experiments by investigating the dependency of the BER on the chosen bitrate. We consider points from the previous experiment, located on the line that starts at point B and continues in parallel to the side of the laptop. We choose a bitrate of 1, 2 and 4 bits per second for the amplitude modulation scheme and evaluate the BER at two points located at 2 and 4 centimeters outside the laptop. For the periodic-based modulation, we fixed $p_0 = 3$ and $p_1 = 5$ and chose three different time frames t corresponding to the bitrates of 1 bit per 7.5, 15 and 22.5 seconds. This choice allows to estimate the quality of decoding depending on the number of patterns being repeated to transmit one bit. The results are provided in Table I.

Using amplitude modulation, we get a similar BER when transmitting 1 and 2 bits per second. However, the BER is significantly higher for a bitrate of 4bit/s. We observed that decoding is mostly affected by small time shifts in the signal, since the exact time to produce one peak as well as its width are not easily controllable by the sender. Therefore, currently we see 4bit/s as a maximum bandwidth when using amplitude modulation.

We observed that the periodic-based scheme remains stable at the distance of 4cm if the consecutive patterns were repeated just a couple of times (in our case, 3 and 5

TABLE I
BIT ERROR RATE FOR DIFFERENT BITRATES

Amplitude modulation

Point	1bit/s	2bit/s	4bit/s
2cm	11	12	24
4cm	27	29	37

Periodic-based modulation

Point	1bit/22.5s	1bit/15s	1bit/7.5s
4cm	0	2	2
8cm	6	11	26

times for p_1 and p_0, according to the bitrate of 1bit/7.5s). However, at larger distances it becomes necessary to limit the bandwidth and increase the periodicity. Therefore, we consider a bitrate of 1bit/15s as practically suitable.

E. Summary

Out experiments show that the amplitude modulation scheme is applicable only in a very limited area of up to 4cm in front of the laptop. At this distance, the corresponding maximum bitrate is 2bit/s. Decrease of the bitrate to 1bit/s does not reduce the BER, as the decoding is mostly affected by the low signal strength compared to noise. Therefore, we consider 2bit/s as the optimal bitrate for this encoding scheme.

The periodic-based modulation scheme is applicable in a larger area of up to 12cm. The achieved BER is similar for bitrates of 1bit/22.5s and 1bit/15s. However, further increase of the bitrate by reducing the number of periodically repeated patterns leads to additional errors. As a result, we consider the periodic-based modulation scheme as more practically suitable, with the optimal bitrate of 1bit/15s.

V. COUNTERMEASURES

We propose several possible ways of preventing the presented covert channel from being established:

- Hard drives and other electronic components of the laptop can be shielded, so that the emitted EM-field is no longer discovered at a distance, or at least outside of the laptop chassis.
- The operating system can randomly perform I/O operations and thus make the transmitted covert signal undetectable among the continuously generated EM-field.
- On the smartphone, the use of magnetic sensors data can be forbidden without an explicit permission granted by the user. Additionally, the access to magnetometers can be restricted for processes executed in a background.

VI. RELATED WORKS

The use of EM emissions as a side-channel has been widely explored over last two decades. Many researches focused on EM side-channel attacks on cryptographic devices, such as smart cards, as the physical proximity to these devices is naturally achieved.

In particular, it was shown in [15] that EM analysis of smart card processors provides at least as much leaked information as power analysis. Later, Gandolfi et al. [7] and Agrawal et al. [2] showed that EM leakage information can be used to break cryptographic implementations, and presented successful attacks against different CMOS chips using low-cost equipment.

Zajic and Prvulovic [18] apply EM analysis to processors of modern desktops and laptops. They have shown that EM emanations caused by different CPU instructions can be successfully detected in radio-frequency spectrum at distances up to several meters, therefore both passive and active EM side-channel attacks on modern processors are feasible. Callan et al. [4] presented a methodology of measuring the available EM signal caused by various processor instructions. Although the potential use of EM side-channel is described in aforementioned works, the necessity of using dedicated equipment limits possible scenarios to establish EM-based covert channels.

Biedermann et al. [3] introduced the idea of using smartphone magnetic sensors to establish side-channel attacks on hard drives. Authors were able to fingerprint hard-drive activity based on the emitted electromagnetic field due to movements of the hard drive magnetic head.

Guri et al. [9] introduced a covert channel based on electromagnetic signals emitted by computer monitor cables, which can be detected by an FM receiver on a mobile phone. A bandwidth up to 60 Bytes per second was achieved at a distance of 1-7 meters. Although modern smartphones may not contain FM chips and display cables may not be present in air-gapped computer configurations, this work proves the feasibility of EM side-channel attacks without special equipment.

Recently, the same authors presented GSMem [8] — an EM covert channel between an air-gapped workstation and a cellular phone. SIMD memory-related instructions were used to produce multi-channel data paths and improve the signal power. Researchers modified the phone firmware to detect EM emanations in GSM frequency range at distances up to impressive 5.5 meters with bandwidth of 1-2 bits per second. Nevertheless, the necessity of modifying the phone firmware complicates the attack.

Apart from electromagnetic emissions, covert channels based on different sources were published. Covert transmission between air-gapped computers using sound waves in ultrasonic range was presented in [10, 11, 5]. Deshotels [6] applied this covert channel to mobile devices and achieved a bitrate of 345 bits per second. Guri et al. [9] presented covert channels based on thermal emissions,

detected by computer heat sensors at the distance up to 40cm, but the bitrate was comparably low (8 bit/hour).

VII. Conclusion and Future Work

In this work, we presented a new covert channel between mobile devices and a laptop. We proposed to transmit a signal using electromagnetic radiation which different components of the laptop emit during common I/O operations. Our modulation scheme uses a combined signal from several EM field sources and does not depend on a specific hardware configuration.

We showed that modern mobile devices can successfully discover and decode this signal at a distance of roughly 12cm from the laptop. Moreover, our proposed covert channel does not require additional equipment, can be run on any modern smartphone, does not need privileged access and can be easily implemented within malware.

Although the solution is attractive as it is widely applicable and easily deployable, the maximum available distance between sender and receiver remains short. An analysis of ways to increase the signal amplitude remains future work.

References

[1] Android API. Sensors overview. `https://developer.android.com/guide/topics/sensors/sensors_overview.html`, 2015. [Accessed: 24.10.2015].

[2] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi. The em side channel(s). In *Cryptographic Hardware and Embedded Systems*, volume 2523, pages 29–45. 2003.

[3] S. Biedermann, S. Katzenbeisser, and J. Szefer. Hard drive side-channel attacks using smartphone magnetic field sensors. In R. Bhme and T. Okamoto, editors, *Financial Cryptography and Data Security*, volume 8975 of *Lecture Notes in Computer Science*, pages 489–496. Springer Berlin Heidelberg, 2015.

[4] R. Callan, A. Zajić, and M. Prvulovic. A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events. In *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture*, MICRO-47, pages 242–254, Washington, DC, USA, 2014. IEEE Computer Society.

[5] B. Carrara and C. Adams. On acoustic covert channels between air-gapped systems. In *Foundations and Practice of Security*, pages 3–16. Springer, 2014.

[6] L. Deshotels. Inaudible sound as a covert channel in mobile devices. In *Proceedings of the 8th USENIX conference on Offensive Technologies*, pages 16–16. USENIX Association, 2014.

[7] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In *Cryptographic Hardware and Embedded Systems*, pages 251–261. 2001.

[8] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici. Gsmem: Data exfiltration from air-gapped computers over gsm frequencies. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 849–864, Washington, D.C., Aug. 2015. USENIX Association.

[9] 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*, pages 58–67. IEEE, 2014.

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

[11] M. Hanspach and M. Goetz. Recent developments in covert acoustical communications. In *Sicherheit*, pages 243–254, 2014.

[12] H. Hotelling. Analysis of a complex of statistical variables into principal components. *Journal of educational psychology*, 24(6):417, 1933.

[13] G. Hulot, C. Finlay, C. Constable, N. Olsen, and M. Mandea. The magnetic field of planet earth. *Space science reviews*, 152(1-4):159–222, 2010.

[14] W. Jones. A compass in every smartphone. *IEEE Spectrum*, 2(47):12–13, 2010.

[15] J.-J. Quisquater and D. Samyde. Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In *Proceedings of the Int. Conference on Research in Smart Cards: Smart Card Programming and Security*, pages 200–210, 2001.

[16] N. Rao. *Fundamentals of Electromagnetics for Electrical and Computer Engineering*. Pearson Education, 2011.

[17] B. Wilson and Z. Ghassemlooy. Pulse time modulation techniques for optical communications: a review. *IEE Proceedings J (Optoelectronics)*, 140(6):346–358, 1993.

[18] A. Zajic and M. Prvulovic. Experimental demonstration of electromagnetic information leakage from modern processor-memory systems. *Electromagnetic Compatibility, IEEE Transactions on*, 56(4):885–893, 2014.