A Case Study Exploring Side-Channel Attacks On Pet Wearables

Alla Levina, Vladimir Varyukhin, Dmitry Kaplun, Anna Zamansky and Dirk van der Linden

***Abstract*—IoT has long since come to the pet industry resulting in a proliferation of data-intensive devices including tracking anything from activity, health, to location. The resulting 'Internet of Pets' is generating large volumes of animal data which, due to the close link between the digital profile of companion animals held as pets (e.g., cats and dogs) and their caregivers holds significant security and privacy implications. In this case study we explore the vulnerability of such pet wearables to side-channel attacks, describing our implementation of an electromagnetic attack on a now discontinued dog activity tracker. We show how we were able to successfully exfiltrate data from the device during the Base64 encoding process and discuss what implications this holds for the security of these devices, given the lack of protection that animal data is afforded under extant existing data protection policy and legislation.**

***Index Terms*—Pet wearables; Side-Channel Attack; Electromagnetic Attack; Base64 encoding algorithm; Bluetooth; Traces.**

I. Introduction

Pet wearables are Internet of Things (IoT) devices worn by companion animals such as dogs and cats which capture activity, health, or even location data. The billion-dollar pet industry is catching up with the wearable hype and getting involved in the wearables market, with the number of available devices having grown significantly over the past years [1], [2]. While a large body of work exists on understanding the different aspects of human wearables' design and use (cf. [3]), research is only beginning to explore wearables for companion animals. With the growing popularity of these devices companion animals are starting to 'produce' large volumes of wellness and health data, which hold many privacy and security implications that require further research attention. Research so far has focused in particular on privacy considerations and expectations from the human users' side (cf. [4], [5], [6], [7], [8]) but as of yet little attention has been paid to the hardware security of these devices, notwithstanding a 2018 Kaspersky Labs [9] report which identified several vulnerabilities—in particular in the communication between the worn device and a caregiver's phone via the Bluetooth Low Energy (BLE) protocol.

To build on these findings and stimulate further attention to hardware security of pet wearables, we take a further step in the investigation of security aspects of pet wearables by considering Side-Channel Attacks (SCA). In particular, we demonstrate a successful SCA on a commercial dog activity tracker–obtaining information from its used Base64 encoding algorithm, by recording the traces of the device's central processor during data transfer. We provide a detailed description of our approach and discuss implications for how we should consider security of pet wearables.

II. Background

Side-channel attacks (SCA) are a powerful type of cryptographic attack which take advantage of physical leakage such as electromagnetic radiation or changes in power consumption. Early SCAs involved timing attacks to break Rivest–Shamir–Adleman (RSA), Diffie-Hellman (DH), and Digital Signature Standard (DSS) encryption by measuring execution time of different code branches and operations [10]. Later it was discovered that device power consumption leaks information about Data Encryption Standard (DES) and Advanced Encryption Standard (AES) by using both simple [11] and differential analysis [12]. Modern SCAs use many non-invasive ways to measure leakage, for example, electromagnetic signals [13], [14] or acoustic cryptanalysis [15], [16].

An electromagnetic field is formed during the operation of a device as a current flows through its hardware. If the design of a device is not well thought out, such unintentionally created fields may carry information about operations occurring during an observation, making it possible to 'read' data directly from the processor via the electromagnetic field. [17]. When using electromagnetic attacks special attention is paid to electromagnetic radiation, which is emitted by electrical circuits that consist of semiconductor elements such as transistors and diodes [18]. An attacker does not always know which frequencies are involved in the encoding process. We can use traces to determine the most frequently used frequencies during different execution periods–a non-aggressive attack. The use of filters always depends directly on the specific device and the noise level [19]. Encoding algorithms are vulnerable to simple electromagnetic analysis if there is a critical dependency of the definition of a specific key bit on the mathematical operation performed such as multiplication or exponentiation. By having a well-recorded trace, we can thus obtain the key by analyzing the record and identifying the multiplication operations performed [20].

There are cases where a simple electromagnetic attack is impossible or ineffective. Differential electromagnetic attacks

Manuscript received May 21, 2021; revised July 07, 2021.

The work of A. Levina and V. Varyukhin was supported by the Ministry of Science and Higher Education of the Russian Federation (Project 'Goszadanie' №075-01024-21-02 from 29.09.2021).

The work of D. Kaplun and A. Zamansky was supported by a grant from the Ministry of Science and Technology of Israel and RFBR according to the research project no. 19-57-06007.

Alla Levina is an Associate Professor, Saint Petersburg Electrotechnical University "LETI", 197376, Saint-Petersburg, Professora Popova str., 5, Russia, ablevina@etu.ru.

Vladimir Varyukhin is a Ph.D student, ITMO University, St. Petersburg, Russian Federation, vladimirrus13@mail.ru.

Dmitry Kaplun is an Associate Professor, Saint Petersburg Electrotechnical University "LETI", 197376, Saint-Petersburg, Professora Popova str., 5, Russia, dikaplun@etu.ru.

Anna Zamansky is a Senior Lecturer, University of Haifa, 3498838, Haifa, Mount Carmel, Aba Khoushy Ave. 199, Israel, annazam@is.haifa.ac.il.

Dirk van der Linden is a Lecturer, Northumbria University, Newcastle-upon-Tyne, Sutherland Building, 2 Ellison Pl, NE1 8ST, UK, dirk.vanderlinden@northumbria.ac.uk.

are used when the information received after applying simple electromagnetic analysis is insufficient. For example, symmetric encryption algorithms are most susceptible to such differential electromagnetic analysis. A distinctive feature of such an attack is that it is not necessary to have complete information about the device performing cryptographic operations [21]. By synthesizing and applying a combination of different types of attacks via side-channels (in terms of power, time, and electromagnetic radiation) we can increase the possibility of further analysis of the obtained traces. For example, a successful extraction of keys from the Elliptic Curve Digital Signature Algorithm (ECDSA) was demonstrated through an attack on mobile phones in 2016 [22]. Modern cryptographic software on mobile phones which implement the ECDSA has been shown to allow for the inadvertent revealing of their secret keys through physical channels: electromagnetic radiation and power consumption, which fluctuates depending on the secret information during cryptographic calculation. Another successful electromagnetic attack on ARM processor systems with the goal of cracking the key of the symmetric block algorithm AES has been shown using SCA [23].

Based on the above, it seems feasible that an electromagnetic SCA is a feasible strategy to extract information from pet wearables, and that the result of analyzing the received traces, that is, extracting secret information, will directly correlate with the quality of the equipment used to measure the electromagnetic signal [24], [25].

III. Case study: SCA on a Pet Wearable

A. The device

In this case study we analyzed a now discontinued dog activity tracker made by Jagger & Lewis [26]. The device contains several types of sensors, including accelerometer, gyroscope, hall sensor, and light and temperature sensors, and is equipped with Wi-Fi, Bluetooth, and a rechargeable battery. When the device interacts with a data processing server, it uses an API in JavaScript Object Notation (JSON) format, which is converted to Base64 encoding.

B. The electromagnetic attack

To demonstrate the SCA, we consider the JSON exchange between the device and server, showing our ability to restore the original JSON text by analyzing traces at the moment of encoding in Base64. As the Jagger & Lewis device is based on the ARM processor architecture, we know that the basic mathematical operations (addition, multiplication, shifts) cannot differ significantly from different versions of the processor family. This indicates a potential vulnerability to SCAs. A schematic representation of the conducted attack is given in Fig. 1, with the electromagnetic traces of the device's processor being the source data we capture.

We used the following equipment was to conduct the SCA:

- a type PXI-5114 digital oscilloscope [27] made by National Instruments (sample clock set to 250 MS/s, bandwidth 125 MHz), shown in Fig. 2;
- an antenna with which the measurements of electromagnetic fields from the device (probe) were made; and
- RFSA – Soft Front Panel software.

We chose this particular oscilloscope for its maximum bandwidth of 3 GHz as the Bluetooth signal range is in the range from 2.402 GHz to 2.48 GHz. This will allow us to record traces that directly describe the authentication processes using the BLE protocol. To further analyze the traces resulting from an electromagnetic attack, we used Soft Front Panel to record signals from the attacked device for subsequent visual analysis of the form as well for estimating its amplitude and temporal characteristics. We connected a probe to the oscilloscope's analog input to record electromagnetic radiation from the tracker and recorded the signal in various modes of the tracker: at the time of the Bluetooth search, at the time of pairing the device with the smartphone, and at the time of encoding data to Base64. All signals were collected separately.

The recorded signals were captured using an oscilloscope which carried out the sampling process on an analog-to-digital converter. To qualitatively implement an attack on electromagnetic radiation, it is required to carry out the processes of recording signals in neutral mode and in active / working mode. We also turned off all devices located at the location of the experiment with the exception of equipment that was directly required to conduct the attack to minimize third-party noise. The SCA was carried out in close proximity to the tracker CPU, at a distance of 0.1–0.2 cm as shown in Fig. 3. The signal from the tracker with its case intact was much weaker than the signal from when we opened its case, so we decided to make the final measures using the opened case. A sampling interval of 20 nanoseconds was selected as an interval for sampling. The Blackman window [28] acts as a typical window function for all records.

At the beginning of the SCA we investigated the frequency range of the device's Bluetooth operation. According to the device specification, its working range of operation was in the range from 2.402 GHz to 2.48 GHz. The results of the frequency analysis are presented in Fig. 4 while Fig.5 shows how dependent the measured signal strength is on the distance to the antenna.

We next had to remove traces in neutral mode to aid in reducing working trace noise. Several signal trace recording operations were performed for each of the following cases:

- in neutral mode;
- in the search mode for other devices via Bluetooth; and
- in the tracker preparing data to the server.

Traces recorded during the SCA are shown across Fig. 6, showing timelines on a scale of 20 nanoseconds of change in the amplitude of the electromagnetic signal recorded from the fitness tracker expressed in dB.

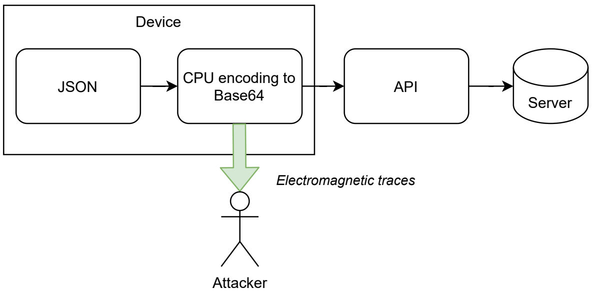


Fig. 1: The conducted electromagnetic attack

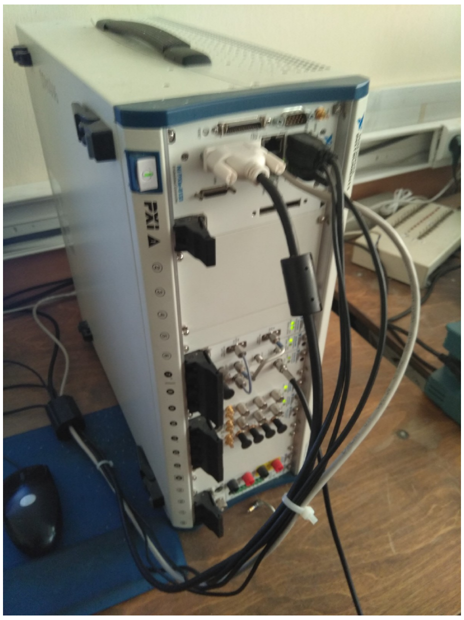
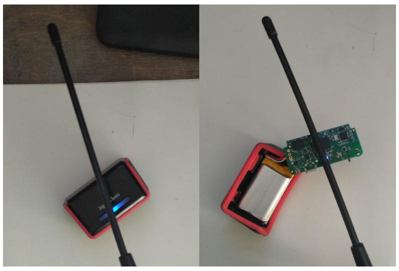


Fig. 2: The used digital oscilloscope type PXI-5114



(a) Case intact (b) Case opened

Fig. 3: Recording traces

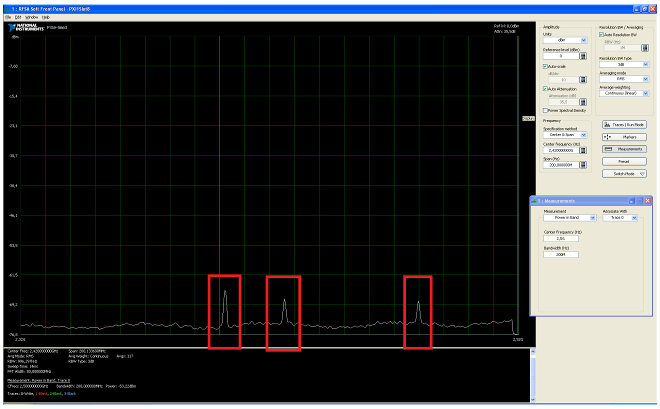


Fig. 4: Bluetooth frequency graph during tracker operation

Figure 6a shows the operation of the device in neutral mode, where a low signal activity can be observed due to lack of CPU processing activity. If the device is in a search mode, as shown in Fig. 6b, one can observe a significant change in the amplitude values of the signal emitted by the tracker. In this mode the CPU processes information related to the Bluetooth module's operation. In Fig. 6c, a significant change in the trace pattern is observed compared to the previous cases, representing the information being encoded into JSON format. It should be noted that the recorded traces contain side noise, as not all equipment interference could

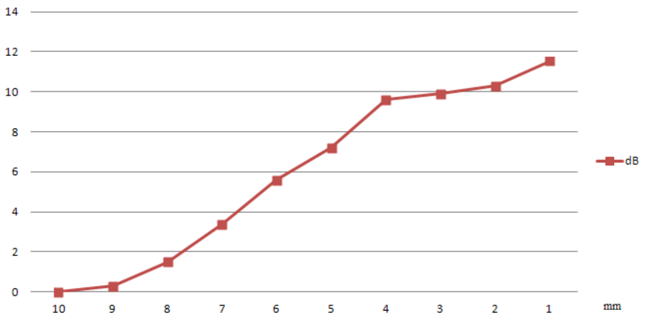
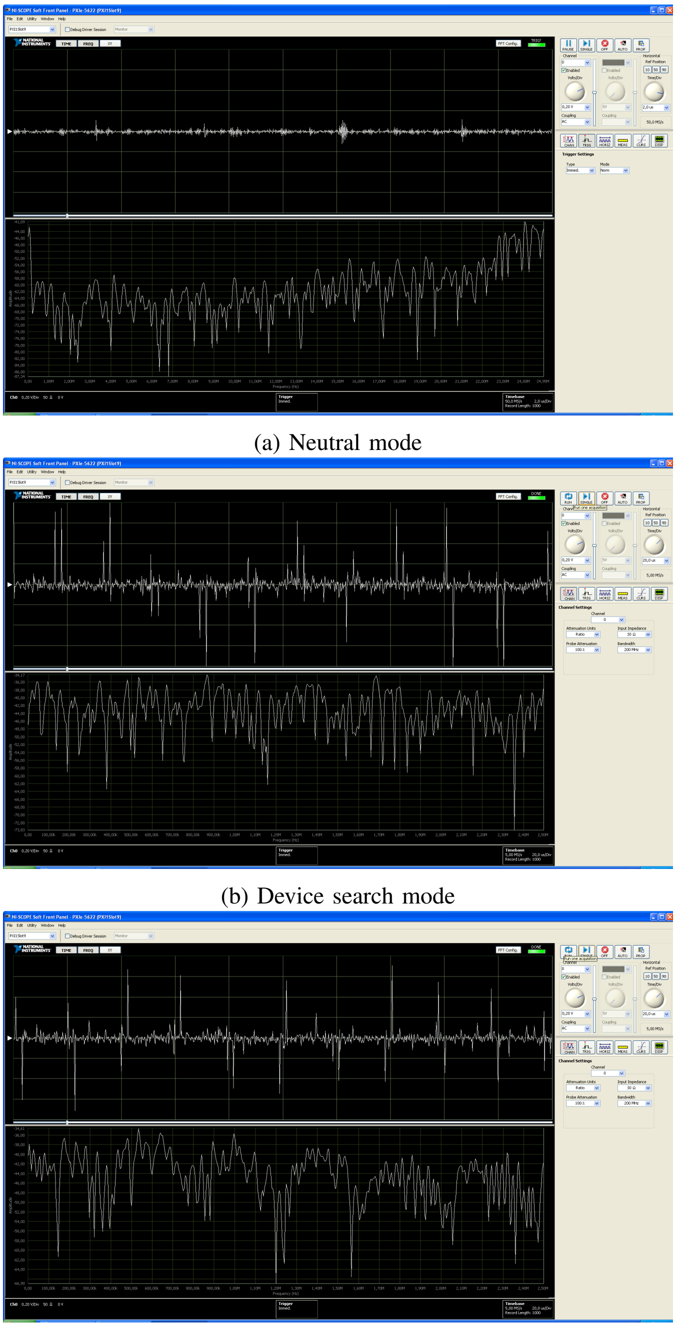


Fig. 5: Bluetooth signal strength gain from distance to antenna (gain in decibels, distance to antenna in millimeters



(a) Neutral mode

(b) Device search mode

(c) Data preparation mode for the server

Fig. 6: Tracker operation traces

be prevented. If the noise is comparable in amplitude with the "splash" of the signal, then a noise reduction procedure should be performed based on the previously recorded tracker signal in the "neutral" mode, in which the "clean" noise profile is recorded. The dependence of the delay time for receiving data on the distance is shown in Fig. 7.

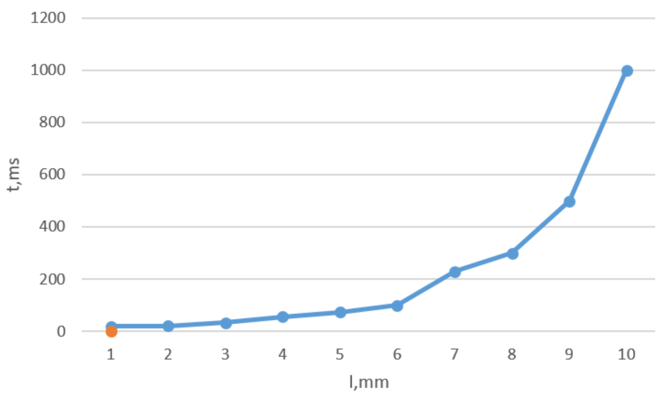


Fig. 7: Dependence of the delay time for receiving data on the distance to the antenna

To carry out a qualitative analysis of the SCA, it is necessary to understand which particular trace contains the relevant data encoding information. To correctly identify this trace the signal was recorded alternately in the neutral and encoding mode. One of the key problems in the analysis of traces measured via side channels is the precise determination of the time that the mathematical operations of encoding are performed. If this problem is not solved, it is impossible to decode the "secret" from the trace. The search for these time intervals can be carried out visually, as additional mathematical operations in the processor are displayed as "bursts", appearing as petals. Indeed, in the traces shown in Fig. 8, such points in time are visible– the signal amplitude becomes larger at the time of encoding data to the server compared to the signal in neutral mode.

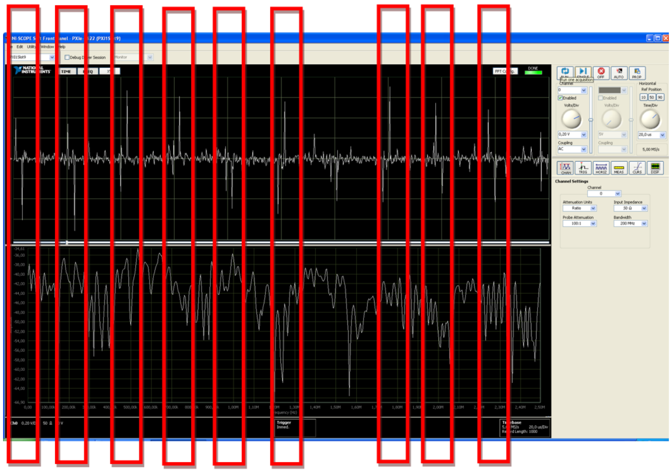


Fig. 8: "Bursts" of the tracker signal when connected to a device

It is efficient to perform the trace analysis using a window function since their level of spectrum sidelobs is less than the dynamic range obtained when recording a signal. Preliminary weighting of a signal sample by one of numerous time windows that smoothly descend at the edges of the range is traditionally used to reduce the level of sidelobes. Efficient window functions such as Kaiser, Hanning, Dolph-Chebyshev, or Kravchenko's atomic functions provide suppression of the 'tails' of the frequency response to -80/-.100 dB levels. However, the suppression of sidelobes is achieved by reducing the transform capability due to the expansion of the main lobe. Therefore we need to achieve a trade-off between the supression of sidelobes and the expansion of the main lobe. The basic frequency responses of window functions are given in Fig. 9, allowing to compare different windows with each other based on the normalized width of the frequency response main lobe $\triangle F_{0,5}$, the normalized width of the main lobe of the frequency response at the zero level ($\triangle F_{0}$.), and the maximum sidelobe level γ_{max}.

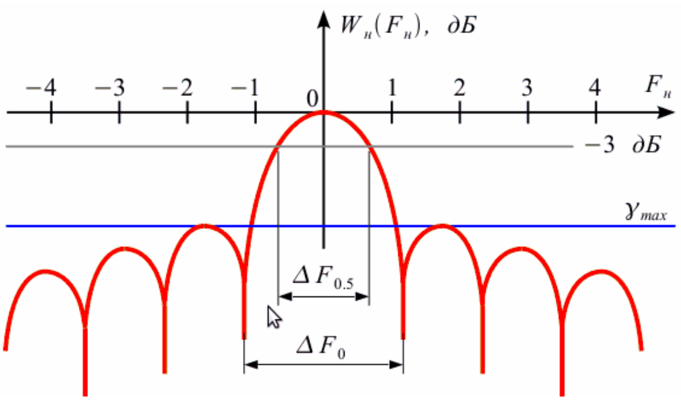


Fig. 9: Characteristics of window functions, from [28]

Based on the established properties of the main window functions, the Blackman window is the best solution given the trade-off described above. To perform further trace analysis, it is necessary to calculate the sidelobe levels of the obtained traces using the Blackman window with the sidelobe level: -58 dB (α=0.16) by the formula:

$$\begin{aligned} &\omega(\pi) = \alpha_0 - \alpha_1 \cos\tfrac{2n\pi}{N-1} + \alpha_2 \cos\tfrac{4n\pi}{N-1},\\ &\alpha_0 = \tfrac{1-\alpha}{2},\\ &\alpha_1 = \tfrac{1}{2},\\ &\alpha_2 = \tfrac{\alpha}{2}. \end{aligned} \tag{1}$$

Based on the results of the case study we can assume that this device uses the simplest data encoding algorithm, namely Base64, likely to ensure the smallest number of operations are performed to account for the tracker's low power. The basic operation that occurs in the central process at the time of encoding in Base64 is the shift operation, because it is required to implement the standard initial text content in blocks of 6 bits each. The traces measured during this operation, as shown in Fig. 8 show bright amplitude oscillations, which can be interpreted as register shifts. In the case study, we measured the following fragments encoded in Base64:

- ewoJInZlcnNpb24iIDogIjAuMS42IiwKCSJzb3VyY2UiIDogInRyYWNrZXIiLAoJInRvb2xVdWlkIiA
- ZXNzYWdlVHlwZSI6InNlbmRBbmltYWxQYXJhbXMiLAoJCSJhcmdzIjp7

After a manual conversion, the following JSON message fragments were extracted from Base64:

- { ”version” : ”0.1.6”, ”source” : ”tracker”, ”toolUuid”
- essageType”:”sendAnimalParams”, ”args”:{”

These results show that our assumption regarding the use of Base64 encoding was correct, as we successfully decoded the data. This shows that the SCA for each device is unique and depends on the specific implementation of the encoding or encryption algorithm, and may change with different devices due to different CPU architecture, location of physical elements, and so on.

IV. Concluding Outlook

This paper presented a case study demonstrating the capture and analysis of the Base64 encoding algorithm from a (once) commercially available dog activity tracker. We have shown that this device is vulnerable to SCAs by recording traces from its CPU when data was being transferred. Such vulnerabilities to SCAs hold significant security implications that need to be considered–also in the case of pet wearables that capture and process animal data. Given that the use of pet wearables is gaining more popularity and the amount of sensitive information they capture and hold is increasing, manufacturers need to pay due attention to their security–at the very least avoiding the use of algorithms that are easily susceptible to SCAs.

As similar devices use similar processors, other pet wearables should be examined for their resistance to SCAs, by conducting more fully fledged attacks implementing an electromagnetic attack using high quality equipment to obtain further secret information from devices, developing a “false tracker” using such secret information, and subsequently implementing a connection between a “false tracker” and a caregiver’s smart phone, in order to capture a caregiver’s personal data from their connected smartphone. Finally, future work should establish a comparative analysis of the security of the architecture of processors used in pet wearables.

References

[1] Gustov, V.; Levina, A. Electromagnetic Fields as a Sign of Side-Channel Attacks in GSM Module. IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021.

[2] Mostovoy, R.; Borisenko, P.; Sleptsova, D.; Levina, A.; Zikratiov, I. Side-Channel Attacks on the Mobile Phones: Applicability and Improvements. Advances in Intelligent Systems and Computing, 2019, 998, pp. 612–621

[3] Seneviratne, S.; Hu, Y.; Nguyen, T.; Lan, G.; Khalifa, S.; Thilakarathna, K.; Hassan, M.; Seneviratne, A. A survey of wearable devices and challenges. IEEE Communications Surveys & Tutorials. 2017, 19(4), 2573–2620.

[4] Zamansky, A; van der Linden, D.; Hadar, I.; Bleuer-Elsner, S. Log my dog: perceived impact of dog activity tracking. IEEE Computer. 2019, 52(9), 35–43.

[5] van der Linden, D.; Zamansky, A.; Hadar, I.; Craggs, B.; Rashid, A. Buddy’s Wearable Is Not Your Buddy: Privacy Implications of Pet Wearables. IEEE Security & Privacy. 2019, 17(3), 28–39.

[6] Zamansky, A.; van der Linden, D. Activity Trackers for Raising Guide Dogs: Challenges and Opportunities. IEEE Technology and Society Magazine. 2018, 37(4), 62–69.

[7] van der Linden, D; Davidson, B; Zamansky, A. The not so secret life of pets: pet owners’ privacy concerns for pet location data. In Proceedings of the Sixth Conference on Animal-Computer Interaction (ACI 2019), Haifa, Israel, 12–14 November 2019.

[8] van der Linden, D.; Williams, E.; Hadar, I.; Zamansky, A. Some might freak out – What if your dog’s activity tracker were to have a data breach?. In Proceedings of the Sixth Conference on Animal-Computer Interaction (ACI 2019), Haifa, Israel, 12–14 November 2019.

[9] Unuchek, R.; Sako, R. I know where your pet is. Kaspersky Lab Research Online, 2018. Available at: https://securelist.com/i-know-where-your-pet-is/85600/

[10] Kocher, P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Annual International Cryptology Conference (CRYPTO), Santa Barbara, California, USA, August 18–22, 1996.

[11] Bechtsoudis, A.; Sklavos, N. Side channel attacks cryptanalysis against block ciphers based on FPGA devices. Proceedings of IEEE Computer Society Annual Symposium on VLSI, Kefalonia, Greece, 5–7 July 2010.

[12] Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In: Annual International Cryptology Conference (CRYPTO), Santa Barbara, California, USA, August 15–19, 1999.

[13] NACSIM 5000 Tempest Fundamentals (Report): National Security Agency, February 1982.

[14] Genkin, D.; Pipman, I.; Tromer, E. Get your hands off my laptop: physical side-channel key-extraction attacks on PCs. Journal of Cryptographic Engineering. 2015, 5(2), 95–112.

[15] Backes, M.; Dürmuth, M.; Gerling, S.; Pinkal, M.; Sporleder, C. Acoustic side-channel attacks on printers. In Proceedings of the 19th USENIX Conference on Security (USENIX Security ’10), Washington, DC, USA, August 11–13, 2010.

[16] Genkin, D.; Shamir, A.; Tromer, E. Acoustic cryptanalysis. Journal of Cryptographic Engineering. 2017, 30(2), 392–443.

[17] Song, D.X.; Wagner, D.; Tian, X. Timing Analysis of Keystrokes and Timing Attacks on SSH. In Proceedings of the 10th USENIX Conference on Security (USENIX Security ’01), Washington, DC, USA, August 13–17, 2001.

[18] Levina, A.; Mostovoi, R.; Sleptsova, D.; Tcvetkov, L. Physical model of sensitive data leakage from PC-based cryptographic systems. Journal of Cryptographic Engineering, 2019, 9(4), pp. 393–400

[19] Kelsey, J.; Schneier, B.; Wagner, D. Key Schedule Weakness in SAFER+. In The Second Advanced Encryption Standard Candidate Conference, Rome, Italy, March 22–23, 1999.

[20] Shamir A.; Tramer E. Acoustic cryptanalysis: on nosy people and noisy machines. Presentation given at Eurocrypt 2004 Rump Session, Interlaken, Switzerland, May 2–6, 2004.

[21] Ometov, A.; Orsino, A.; Andreev, S.; Levina, A.; Borisenko, P.; Mostovoy, R. Mobile social networking under side-channel attacks: practical security challenges. IEEE Access. 2017, 5, 2591–2601.

[22] Genkin, D.; Pachmanov, L.; Pipman, I.; Tromer, E.; Yarom, Y. ECDSA key extraction from mobile devices via nonintrusive physical side channels In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24–28, 2016.

[23] Longo, J.; de Mulder, E.; Page, D.; Tunstall, M. SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Saint-Malo, France, September 13–16, 2015.

[24] Biham E.; Shamir A. A Power Analysis of the Key Scheduling of the AES Candidates. In Proceedings of the Second AES Candidate Conference, Rome, Italy, March 22–23, 1999.

[25] Chari S.; Jutla C.; Rao J.; Rohatgi P. A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards. In Proceedings of the Second AES Candidate Conference, Rome, Italy, March 22–23, 1999.

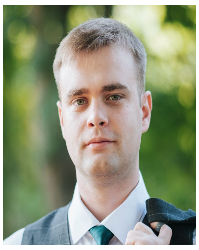
[26] Jagger & Lewis. Available online: https://www.jagger-lewis.com/en-en/home (accessed on 21 November 2020).

[27] PXI-5114 Specifications . Available online: https://www.ni.com/documentation/en/pxi-oscilloscope/latest/specs-pxi-5114/specs/ (accessed on 21 November 2020).

[28] Oppenheim, A.V.; Schafer, R.W.; Buck, J.R. Discrete-Time Signal Processing. Prentice Hall: Upper Saddle River, NJ, USA, 1999, pp. 468-471.

Alla Levina finished St. Petersburg State University mathematical faculty in 2005, in 2009 got Ph.D in St. Petersburg State University mathematical faculty, Russian Federation.

She is an Associate Professor at Saint Petersburg Electrotechnical University ”LETI”, Russian Federation. Her research interests include cybersecurity, cryptography, coding theory, and wavelet transformation.



Vladimir Varyukhin finished institute of electronics and lighting engineering National Research Mordovia State University in 2017, in 2019 got master degree in ITMO University, Russian Federation.

He is a Postgraduate student at ITMO University, Russia. His research interests include cryptography, cybersecurity, software engineering.

Dmitry Kaplun is an Associate Professor at Saint Petersburg Electrotechnical University ”LETI”, Russian Federation.

His research interests include digital signal processing, spectral analysis, FPGA, and CUDA.

Anna Zamansky is an Associate Professor at the University of Haifa, Israel.

Her research interests include information systems and technology for animals.

Dirk van der Linden is an Assistant Professor at Northumbria University, UK.

His research interests include requirements engineering, animal-computer interaction, and cyberpsychology.