Indonesian Journal of Electrical Engineering and Computer Science
Vol. 10, No. 2, May 2018, pp. 490~497
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i2.pp490-497

Data Exfiltration of Ultrasonic Signal in Computer Security System: A Review

Farah H. A. Jabar*[1], Janatul Islah Mohammad[2], Ahmad Faizal Mohd Zain[3], Abu Bakar Hasan[4]
[1,2,4]Faculty of Engineering & Built Environment, Universiti Sains Islam Malaysia
[3]formerly at Faculty of Engineering & Built Environment, Universiti Sains Islam Malaysia

Article Info

Article history:

Received Dec 1, 2017
Revised Jan 29, 2018
Accepted Feb 22, 2018

Keywords:

Acoustic attack
Computer security
Cryptanalysis
Data exfiltration
Ultrasonic signal

ABSTRACT

It is crucial for public users and service providers to stay abreast of the progress and trends on data exfiltration in computer security system. In cryptosystem, it is unnoticeable for computer and mobile users to realize that inaudible sound used to transmit signals carrying pervasive sensitive data was in the low frequency ultrasonic range. Acoustic attacks on ultrasonic signal emanated by electronic devices have long been investigated among researchers. This paper is an exploration on the practicality of ultrasonic data exfiltration between computers in term of computer security system. It will discuss some work done by previous researchers in general, based on scientific, technological, and security perspectives. There will be inclusions of practical applications already in existence as well as future studies in related fields.

Corresponding Author:

Farah H. A. Jabar,
Faculty of Engineering & Built Environment,
Universiti Sains Islam Malaysia, Bandar Baru Nilai,
71800 Nilai, Negeri Sembilan, Malaysia.
Email: farah@hitechnics.com.my

1. INTRODUCTION

We live in the era where security is the main concern of protecting private information which is controlled via computer system. While the breach of such system has been shown to be feasible throughout the decades, the exfiltration of encrypted data for highly secured network computers [1]–[4] and mobile device [5]–[9] users are still considered a challenging task. A lot of efforts have been done in protecting this information but there are still many concerns for the security systems in which the orientation is visible and easily accessed. The focus nowadays is on the sound produced by computer peripherals such as keyboards [10], [11] and printers [12]. Technically this method of attack dates to the time of FFT-based hardware being easy enough to perform the tasks. Other conventional leakages can be power, electromagnetic radiation, optical and light emanation [13]–[15].

The development of ultrasonic data exfiltration in the context of an information security brings the possibility growth of data transmission via sound beyond the human hearing level. It is well known that sound can be used to transmit data as this can be seen in many old technologies especially for mobile system [6], [16]. This could provide the process of transmitting overhead data without the use of radio signals or physical connections or retrieving data virtually undetected for hacking, control, or other malicious activity.

2. EVOLUTION OF ULTRASONIC IN TELECOMMUNICATION

Wireless connectivity is crucial nowadays. One critical and urgent issue is the availability of wireless technology. Mobile devices like laptops, mobile phones and tablets, they communicate with echo what are known as radio waves. Useful radio waves are limited, expensive, strictly regulated and shortage of

suitable frequencies to be used. The unwanted wireless signals will significantly degrade desired signals and reduce system performance [17]. These impacts have led to the application of other alternative signals which is sound. Sound is a mechanical vibration or pressure wave that can be transmitted through a medium such as air, water or solid materials. Meanwhile ultrasound is a type of sound with a pitch or frequency above limit of human hearing (approximately more than 20kHz). It will not be able to hear without the help of a proper detector. The use of ultrasound becomes more attractive as if data signals were transmitted using audible sound the environment would be too noisy to be heard.

2.1. The History

The discoveries of ultrasonic frequency have been studied for many different reasons for hundreds of years. The first discovery started in 1794 when physiologist Lazzaro was the first to study the echolocation among bats. In 1877, Jacques and Pierre discovered the piezoelectric effect which was used in the transducers design for ultrasonic waves in air and water [18]. The successful application of piezoelectricity in the generation and detection of ultrasound waves in deep seawater was followed by further development as described in [18]–[20]. The first technological application of ultrasound dates back in 1916 which was inspired by the sinking of Titanic ship earlier before when Paul Langevin was trying to detect submarines using sound navigation and ranging technology also known as SONAR [21], [22]. Today, the development of ultrasound technology is used in many areas of life, especially in telecommunication [23], [24], heavy industry [25]–[27] and biomedical imaging [28], [29]. The frequency range of ultrasonic is very wide and depends on their use, ranging from 20 kHz in industrial devices up to 10 MHz in medical diagnostics and therapy.

2.2. Ultrasonic in Modern Computer System

The concept of transferring data over inaudible sound signal within high frequency range or simply known as ultrasonic data transmission cover a wide range of practical uses. A common way to send digital data using ultrasound is simply turning on and off the transmitter. When the receiving sensor detects the corresponding changes of sound pressure, this information can be converted back into an electrical signal and translated back to the original data. Digital data can be represented by a series of ultrasound bursts travelling as pressure waves through air. The sound signal that able to carry sensitive data imposed many opportunities and threats [30]. Transmitting anything in a low frequency range of ultrasonic can be considered exposing the data publicly but is hidden by anyone not looking for it. Nowadays most modern computers such as laptops and mobile phones have built in microphones and speakers. This means that in the absence of network cables and wireless signal, those built in devices can be utilized to control those systems maliciously.

For computer system, among the earliest technology that become great interest among computer engineers for data transmission over sound is audio watermarking. The concept of watermarking or hiding data in sound signal has started to receive interest among professionals since year 1996 [31]. The fact that the limitation of the old concept can only transmit about one character per second, more development has been done via techniques using ultrasonic signals which can transmit information at higher speeds [32]–[34]. Ultrasonic data transmission in short range also known as near-sound data transfer (NSDT) enables secure transactions by creating an electronic signature using a one-time password through inaudible audio signal of a mobile device. This technology is primarily used for mobile banking can be very delicate as range of measurement can be affected by air flow, temperature changes, humidity or environmental signal [35]. Smarter design scheme need to be developed to deliver stealthy communication utilizing ultrasonic frequency range.

For long distance tracking, multiple ultrasonic sensors are adopted to realize exactly locating motion objects with sophisticated scheme measuring their motion orientation so that their 2D coordinates should be located and positioned [36]. Latest issue has focused on the cross-device tracking which bring a serious threat to the privacy of users. A recent practice embeds ultrasonic beacons in audio device and tracks them using the microphone of mobile devices. Researchers have explored these new tracking technologies based on the capabilities, pervasiveness and technical limitations of existing commercial tracking solutions [37]–[39]. Figure 1 illustrate the development of ultrasonic technology and its application towards data exfiltration in computer security system. Some development and issues are the main concern of this paper which will be discussed further in later section.

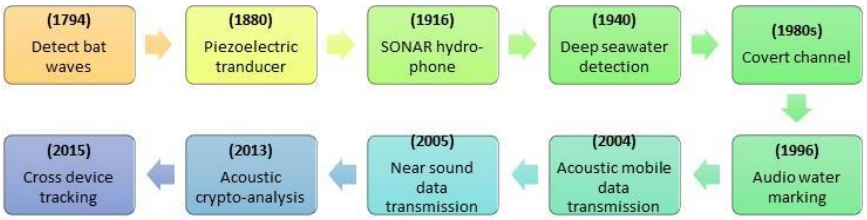

Figure 1. The Development of Ultrasonic Technology and Its Applications towards Computer Security System

3. SIGNAL LEAKAGE IN COMPUTER SYSTEM

3.1. Data Exfiltration in Covert Channel

The exfiltration of data from non-networked computers or those without physical access is still considered a challenging task. Among other type of computer security attack which exploit and exfiltrate data from air-gapped computers without requiring network connectivity is the covert channel. It started off as great debut in early year of 1980s and have been widely discussed in professional literature [40]–[42]. Different types of out-of-band covert channels have been proposed over the years, exploring the feasibility of data exfiltration through an air-gap. For example, the oldest kind of covert channel researched are likely to be the electromagnetic methods that exploit electromagnetic radiation from different components of the computer [43], [44].

Previously data exfiltration using audible and inaudible sound has been proposed and explored [45]–[47]. Looking back over a decade, researchers proposed an 'audio networking,' which allows data transmission between a pair of desktop computers, using cheap speakers and a microphone [45]. The existing method shows that data can be transmitted through the air-gap via ultrasonic signal emitted from computer speakers. For instance, recent work in [46] suggest a method of transmitting keystroke data using a malware via ultrasonic audio emitted from computer speakers. The researchers proposed a method for near-ultrasonic in covert networking among air-gapped computers with a 20bit per second speed at a distance up to 19.7m using only speakers and microphones. They were able have a keylogger transmitting recorded keystrokes across a computers' meshnet and collect the keystrokes of the primary victim computer on remote system. Another recent work has studied data leakage from a high-security of an air-gapped system to a low-security network systems using malware via high frequency signal within isolated internet environment [47]. The researchers demonstrated how the malware installed on the air-gap computer collected data, converted it into binary and then blinked LED accordingly. At the same time, the infected camera captured this pattern and the malware installed on the camera converted the Morse-code back into the binary data. These confirm the validity of the concern that ultrasonic data transmission between systems is a security threat.

Data communication over inaudible sounds has been explored and extended for different environment using laptops and smartphones [48], [49]. High security organizations do employ controls that prevent radio signals from propagating into or out of the building. An interesting concept of transmitting data across solid metal mediums via ultrasonic transducers that would otherwise block radio signals able to achieve ultrasonic data transmission via Frequency-Shift Keying (FSK) with a bit rate of up to 800 bits per second [50]. However, it does not employ stock hardware that normal consumer electronics would use.

3.2. Acoustic Cryptanalysis

Side-channel attacks are a class of physical attacks in which an attacker tries to exploit physical information leakages from those devices. Side-channel attacks target implementations of cryptographic algorithms which can leak secret information through indirect channels such as power consumption, electromagnetic emanations, timing variations and acoustic emanations [51]–[54].

Acoustic attack is a type of side-channel attacks which mainly based on the sound produced by the devices especially computer peripherals or electrical components inside computers that may not be audible to human. Acoustic emanations that generated by computers, are one such potential channel. The source of attacks on the security of computer systems produced by emanations from electronic devices have long been investigated among researchers [12], [53], [55]–[57]. This attack is inexpensive and non-invasive because the only other hardware needed to perform the attacks is a parabolic microphone. Mechanical vibrations from fans and storage devices such as hard disks during system activity induced noise may carry valuable information that is apparently of little use for cryptanalysis. Physical intrusion into the system is also not required and the sound can be recorded from a substantial distance. It is crucial for public users and service providers to stay abreast of the progress and trends on cryptanalysis of security protocol.

In another perspective, recent work shows that ultrasonic signal has emanated from computers that emit a high-pitched signal during operation, due to vibration in some of their electronic components [58]. During the CPU operation, the power consumptions fluctuate to supply the constant voltage within the chipsets components. These acoustic emanations can expose and leak valuable information regarding security-related computations. The main issue was the very low acoustic side channel bandwidth that operates under 20 kHz using common microphones, and a few hundred kHz using ultrasound microphones. Interestingly, recent studies have shown that a full 4096-bit RSA key encryption can be extracted from a laptop computer by analysing the audible sound signal during operation [58], [59]. Data encryption standard RSA among the earliest practical public-key cryptosystems that is widely used for secure data transmission. The acoustic attacks are capable to extract the public keys from various versions of computers using the sound generated during the decryption of some chosen cipher texts. Figure 2 shows the overview of equipment that have been used in the experiment [58], [59]. Three experimental setups have been considered representing various trade-offs between costs, portability and measuring capabilities. This setup aims for the best possible acoustic acquisition quality (in terms of sensitivity, signal and frequency response) and high flexibility in measurement configuration.

Figure 2. An Illustration of Acoustic Attack on Mobile Computers in [58], [59]

4. COUNTERMEASURES AND FURTHER PERSPECTIVES

An obvious idea for counter measuring acoustic attacks is silent microprocessors, which do not produce any sound or leakage signal. The latest version of CPU for example like Intel i7 with quadcore processors and above would produce faster processing time and lower sound. Smaller size device such as tablets and mobile gadgets would also prevent the acoustic signals from transmitted externally. The above-mentioned ways are useful in avoiding emanation of sound from processors or CPUs. Other method is to increase the distance between the devices and the microphone in such a way where the signal detection rate drops substantially. Although this may not be useful to all cases as microphone technology for ultrasonic has developed rapidly in term of distance detection. Introduce some obstacles between the device and microphone can also prevent the sound reaching the recording device (microphone). Avoiding contact with microphone: the absence of microphones near emanation device is also sufficient to protect privacy. For acoustic attacks emanated from other component such as keyboard or printers, also required a silent and faster technologies. Nowadays, the usage of virtual technology replacing physical hardware may also among robust and state-of-the-art solutions. For example, virtual keyboards have appeared whereby they can be projected on a flat surface [60]–[62]. Similarly with recent project on the development of virtual microphone using ultrasonic signal as sound receiver although this method may require more devices as transceivers [63]. These choices are more expensive than the standard devices, yet it can avoid valuable information from leaking.

Further work is currently being done to detect the leakage in private information caused by electronic devices' emanations. The acoustic emanations originated from the operated microprocessors inside CPU of the attacked devices has been discussed based on computer operational running with RSA encryption protocol [58], [59]. The asymmetric properties of using two different keys makes the RSA become vulnerable as the cryptosystem itself is mainly based on the mathematical problem of integer factorization. AES, for instance, uses a unique key calculated few times based on several substitutions and linear transformation of the encryption key. AES algorithm remains the preferred encryption standard for high security system around the globe. Motivated by the significant finding on the signal leakage from RSA encryption, this current work is aimed to detect and characterizes signal profiles from the emanated ultrasonic signal running on AES encryption system and determine any correlation with respect to acoustic properties. Figure 3 shows the equipment used to perform the experiment using mobile computer running on AES encryption system. Ongoing measurement and analysis of these works are being carried out and anticipate with significant results for future publications.

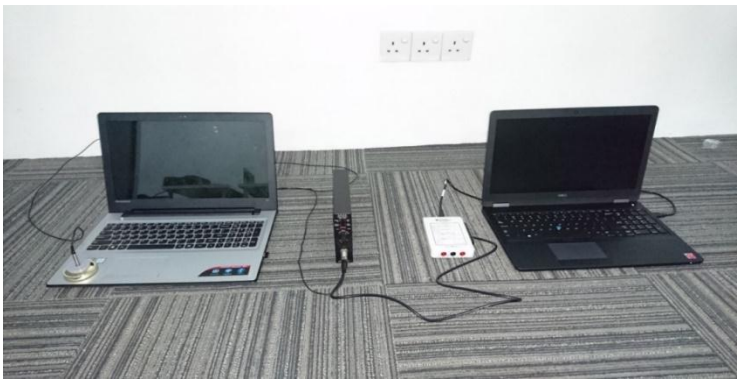

Figure 3. Photograph of Author's Portable Setup. In this Photograph (A) is a Target Computer, (B) is a ¼" GRAS 46BF Microphone Set, (C) is a GRAS 12AK Microphone Power Supply and Amplifier, (D) is a National Instruments MyDAQ Device, and (E) is a Laptop Computer Performing the Attack

5. CONCLUSIONS

Exfiltration of data over ultrasonic signal in private information caused by inaudible sound signal emanated from electronic devices has been a wide concern recently. Audio device such as microphones and speakers can measure the sound signal as it carries sensitive information in the form of frequency, wavelength and amplitude. Powerful acoustic attacks in covert channel have been identified previously which mainly for capturing login detail, passwords and other secret information recovery. In cryptosystem, the acoustic emanations would be originated from computer peripherals or the operated microprocessors inside CPU of the attacked devices. Previous work has shown that the acoustic attack can convey information about the software running on the computer, and exfiltrate sensitive data about security-related computation. Ongoing work deals with the detection and profiling of the ultrasonic signal leakage emanated from a computer that runs AES-based encryption system. Interesting results from the current research are therefore anticipated to improve related computer security issues.

ACKNOWLEDGEMENTS

This work was funded by the Ministry of Higher Education of Malaysia under research grant of Trans-Disciplinary Research Grant Scheme (TRGS). Grant No. USIM/TRGS01_PROJEK01/FKAB/59/50116.

REFERENCES

[1] R. Ramachandran, S. Neelakantan, and A. S. Bidyarthy, *"Behavior model for detecting data exfiltration in network environment,"* in 2011 IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, IMSAA 2011 - Conference Proceedings, 2011.

[2] E. Bertino and G. Ghinita, "*Towards mechanisms for detection and prevention of data exfiltration by insiders,"* in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS '11, 2011, p. 10.

[3] J. R. Michener, "Defending against user-level information exfiltration," *IT Prof.*, vol. 14, no. 6, pp. 30–36, 2012.

[4] Y. Hu, R. Hossain, P. Seye, and S. Vasireddy, "*Mining Windows Registry for data exfiltration detection,"* in Proceedings of the 9th International Workshop on Security in Information Systems, WOSIS 2012, in Conjunction with ICEIS 2012, 2012, pp. 101–108.

[5] M. Guri, A. Kachlon, O. Hasson, G. Kedma, and Y. Mirsky, "GSMem : *Data Exfiltration from Air-Gapped Computers over GSM Frequencies* This paper is included in the Proceedings of the," USENIX Secur., pp. 849–864, 2015.

[6] C. J. D'Orazio, K. K. R. Choo, and L. T. Yang, "Data Exfiltration from Internet of Things Devices: IOS Devices as Case Studies," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 524–535, 2017.

[7] A. N. I. of T. K. Chandak Surathkal, A. N. I. of T. K. Aravind Surathkal, and N. N. I. of T. K. KamathSurathkal, "WallE Surveyor Robot using Wireless Networks," *IAES International Journal of Robotics and Automation (IJRA)*, vol. 4, no. 2, 2015.

[8] Q. Do, B. Martini, and K. K. R. Choo, "Exfiltrating data from Android devices," *Comput. Secur.*, vol. 48, pp. 74–91, 2015.

[9] J. S. T. V. E. Song Suzhou, Z. S. T. V. E. Xin Suzhou, and W. S. T. V. E. Ding Suzhou, "Research On Android Intelligent Phones Controlling the Car to Run," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 11, no. 12, pp. 7438–7445, 2013.
[10] M. Kölsch and M. Turk, "Keyboards without keyboards: A survey of virtual keyboards," Work. Sens. Input Media-centric …, 2002.
[11] L. Zhuang, F. Zhou, and J. D. Tygar, *"Keyboard acoustic emanations revisited,"* Proc. 12th ACM Conf. Comput. Commun. Secur. - CCS '05, no. November, p. 373, 2005.
[12] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, *"Acoustic Side-channel Attacks on Printers,"* in Proceedings of the 19th USENIX Conference on Security, 2010, p. 20.
[13] G. Joy Persial, M. Prabhu, and R. Shanmugalakshmi, "Side Channel Attack - Survey," *Int. J. Recent Trends Electr. Electron.*, vol. 1, no. 2, pp. 49–54, 2011.
[14] E. De Mulder, P. Buysschaert, S. B. Ors, P. Delmotte, B. Preneel, G. Vandenbosch, and I. Verbauwhede, *"Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem,"* Int. Conf. Comput. as a Tool - EUROCON'05, vol. 2, pp. 1879–1882, 2005.
[15] H. Bar-El, "Whitepaper on Introduction to Side Channel Attacks," Secur. Integr. Circuits Syst., 2010.
[16] W. Chen, G. P. Hancke, K. E. Mayes, Y. Lien, and J. H. Chiu, *"NFC mobile transactions and authentication based on GSM network,"* in Proceedings - 2nd International Workshop on Near Field Communication, NFC 2010, 2010, pp. 83–89.
[17] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks: Possibilities and fundamental limitations based on available wireless network measurements," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 41–53, 2005.
[18] A. Manbachi and R. S. C. Cobbold, "Development and application of piezoelectric materials for ultrasound generation and detection," *Ultrasound*, vol. 19, no. 4, pp. 187–196, 2011.
[19] A. Toprak and O. Tigli, "Piezoelectric energy harvesting: State-of-the-art and challenges," Appl. Phys. Rev., vol. 1, no. 3, p. 31104, 2014.
[20] A. A. Vives, Piezoelectric transducers and applications. 2008.
[21] H. Peyvandi, M. Farrokhrooz, H. Roufarshbaf, and S.-J. Park, *"SONAR Systems and Underwater Signal Processing: Classic and Modern Approaches,"* in Sonar Systems, 2011, pp. 173–206.
[22] A. D. (Ashley D. Waite, Sonar for practising engineers, no. 3. 2016.
[23] R. P. Thomas, K. K. Jithin, K. S. Hareesh, C. A. Habeeburahman, and J. Abraham, "Range Detection based on Ultrasonic Principle," *Int. J. Adv. Res. Electr. Electron. Instrum. Eng*., vol. 3, no. 2, pp. 7638–7642, 2014.
[24] J.-H. Gu, H.-G. Joe, and S. C. Yu, "Development of image sonar simulator for underwater object recognition," 2013 Ocean. - San Diego, pp. 1–6, 2013.
[25] M. S. Mullakaev, V. O. Abramov, and A. V. Abramova, "Development of ultrasonic equipment and technology for well stimulation and enhanced oil recovery," *J. Pet. Sci. Eng.*, vol. 125, pp. 201–208, 2015.
[26] F. Feucht, J. Ketelaer, A. Wolff, M. Mori, and M. Fujishima, *"Latest machining technologies of hard-to-cut materials by ultrasonic machine tool,"* in Procedia CIRP, 2014, vol. 14, pp. 148–152.
[27] M. P. Matheny and K. F. Graff, "Ultrasonic welding of metals," in Power Ultrasonics: Applications of High-Intensity Ultrasound, 2014, pp. 259–293.
[28] P. N. T. Wells and H.-D. Liang, "Medical ultrasound: imaging of soft tissue strain and elasticity," J. R. Soc. Interface, vol. 8, no. 64, pp. 1521–1549, 2011.
[29] M. Postema, Fundamentals of medical ultrasonics. 2011.
[30] S. J. O'Malley and K.-K. R. Choo, *"Bridging the air gap: Inaudible data exfiltration by insiders,"* 20th Am. Conf. Inf. Syst. AMCIS 2014, no. Munro 2012, pp. 1–12, 2014.
[31] M. Arnold, *"Audio Watermarking: Features, Applications and Algorithms,"* Multimed. Expo, 2000. ICME 2000. 2000 IEEE Int. Conf. (Volume2), vol. 0, no. c, pp. 1013–1016, 2000.
[32] R. F. Olanrewaju and O. Khalifa, *"Digital audio watermarking; techniques and applications,"* 2012 Int. Conf. Comput. Commun. Eng., no. July, pp. 830–835, 2012.
[33] H. Kaur, "Blind Audio Watermarking schemes : A Literature Review," *IRACST – Eng. Sci. Technol. An Int. J.*, vol. 3, no. 2, pp. 288–295, 2013.
[34] H. Matsuoka, Y. Nakashima, and T. Yoshimura, "Acoustic Communication System Using Mobile Terminal Microphones," *NTT DoCoMo Tech. J.*, vol. 8, no. 2, pp. 4–12, 2004.
[35] M. M. Saad, C. J. Bleakley, and S. Dobson, "Robust high-accuracy ultrasonic range measurement system," in I*EEE Transactions on Instrumentation and Measurement*, 2011, vol. 60, no. 10, pp. 3334–3341.
[36] D. N. I. of I. T. Juan, Z. N. I. of I. T. Zhihong, and Y. N. I. of I. T. Minglian, "Ultrasonic Automatic Tracking System," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 12, no. 6, pp. 4664–4670, 2014.
[37] R. Diaz-Morales, *"Cross-Device Tracking: Matching Devices and Cookies,"* in Proceedings - 15th IEEE International Conference on Data Mining Workshop, ICDMW 2015, 2016, pp. 1699–1704.
[38] D. Arp, E. Quiring, C. Wressnegger, and K. Rieck, *"Privacy Threats through Ultrasonic Side Channels on Mobile Devices,"* Proc. IEEE Eur. Symp. Secur. Priv., 2017.
[39] J. Brookman, P. Rouge, A. Alva, and C. Yeung, *"Cross-Device Tracking: Measurement and Disclosures,"* Proc. Priv. Enhancing Technol., vol. 2017, no. 2, pp. 113–128, 2017.
[40] S. Cabuk, C. E. Brodley, and C. Shields, "IP Covert Channel Detection," *ACM Trans. Inf. Syst. Secur.*, vol. 12, no. 4, pp. 1–29, 2009.

[41] S. Chandra, Z. Lin, A. Kundu, and L. Khan, "Towards a systematic study of the covert channel attacks in smartphones," in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, vol. 152, 2015, pp. 427–435.
[42] S. A. Ahmadzadeh and G. Agnew, *"Turbo covert channel: An iterative framework for covert communication over data networks,"* in Proceedings - IEEE INFOCOM, 2013, pp. 2031–2039.
[43] M. Vuagnoux and S. Pasini, *"An improved technique to discover compromising electromagnetic emanations,"* in IEEE International Symposium on Electromagnetic Compatibility, 2010, pp. 121–126.
[44] M. G. Kuhn, "Compromising emanations of LCD TV sets," *IEEE Trans. Electromagn. Compat.*, vol. 55, no. 3, pp. 564–570, 2013.
[45] B. Carrara and C. Adams, "On acoustic covert channels between air-gapped systems," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8930, pp. 3–16, 2015.
[46] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *J. Commun.*, vol. 8, no. 11, pp. 758–767, 2013.
[47] A. Madhavapeddy, D. Scott, A. Tse, and R. Sharp, "Audio networking: The forgotten wireless technology," *IEEE Pervasive Computing*, vol. 4, no. 3. pp. 55–60, 2005.
[48] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These Aren't the Droids You're Looking for: Retrofitting Android to Protect Data from Imperious Applications," CCS, pp. 639–652, 2011.
[49] A. K. Sood, R. Enbody, A. K. Sood, and R. Enbody, "Chapter 5 – Data Exfiltration Mechanisms," in Targeted Cyber Attacks, 2014, pp. 77–93.
[50] T. Hosman, M. Yeary, J. K. Antonio, and B. Hobbs, *"Multi-tone FSK for ultrasonic communication,"* in 2010 IEEE International Instrumentation and Measurement Technology Conference, I2MTC 2010 - Proceedings, 2010, pp. 1424–1429.
[51] Y. Zhou and D. Feng, *"Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing,"* Inf. Secur. Semin. WS 0607, no. 60503014, pp. 1–34, 2005.
[52] N. Lawson, "Side-channel attacks on cryptographic software," *IEEE Secur. Priv.*, vol. 7, no. 6, pp. 65–68, 2009.
[53] B. Sevak, "Security against Side Channel Attack in Cloud Computing," *Int. J. Eng. Adv. Technol.*, vol. 2, no. 2, pp. 183–186, 2012.
[54] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, vol. 9610, pp. 219–235.
[55] G. M. Deepa, G. Sriteja, and S. Venkateswarlu, "An Overview of Acoustic Side-Channel Attack," vol. 3, no. 1, pp. 15–20, 2012.
[56] C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, and W. Xu, *"My Smartphone Knows What You Print : Exploring Smartphone-based Side-channel Attacks Against 3D Printers,"* in ACM CCS, 2016, pp. 895–907.
[57] D. Genkin, I. Pipman, and E. Tromer, "Get your hands off my laptop: physical side-channel key-extraction attacks on PCs: Extended version," *J. Cryptogr. Eng.*, vol. 5, no. 2, pp. 95–112, 2015.
[58] D. Genkin, A. Shamir, and E. Tromer, "Acoustic Cryptanalysis," *J. Cryptol.*, vol. 30, no. 2, pp. 392–443, 2017.
[59] D. Genkin, A. Shamir, and E. Tromer, "RSA key extraction via low-bandwidth acoustic cryptanalysis," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014, vol. 8616 LNCS, no. PART 1, pp. 444–461.
[60] S. Zhai, M. Hunter, and B. Smith, "Performance Optimization of Virtual Keyboards," *Human-Computer Interact.*, vol. 17, no. 2, pp. 229–269, 2002.
[61] N. Henze, E. Rukzio, and S. Boll, *"Observational and experimental investigation of typing behaviour using virtual keyboards for mobile devices,"* Proc. 2012 ACM Annu. Conf. Hum. Factors Comput. Syst. - CHI '12, p. 2659, 2012.
[62] T. Merkel, "Virtual Microphones : Solving the Technical Difficulties for a Practical Device," in AIA-DAGA, 2013, no. 1, pp. 894–896.

BIOGRAPHIES OF AUTHORS

Farah Hanim Abd Jabar was born in Pahang, Malaysia, in 1979. She received Bachelor degree in computer engineering from International Islamic University of Malaysia, in 2003 and Masters of Science from Universiti Sains Islam Malaysia (USIM) Nilai, Negeri Sembilan, Malaysia. Currently pursuing Ph.D. degrees in engineering at the same university. Her current research interests include acoustics, noise, sound and vibration studies. She is also a member of Society of Vibrations and Acoustics Malaysia.

Janatul Islah Mohammad obtained her Bachelor's Honours Degree in Electronic Engineering with Music Technology Systems from the University of York, United Kingdom in 1999 and a Master's degree in Sound and Vibration Studies from the University of Southampton, United Kingdom in 2002. She received her Doctoral degree in Sound and Vibration Studies from the University of Southampton in 2006. She used to work as an Acoustic Engineer in Kuala Lumpur prior to continuing her Master's degree. From March 2003 until April 2014, she was working as Lecturer and promoted to Senior Lecturer (2008) and Associate Professor (2012) at the Universiti Teknikal Malaysia Melaka (UTeM). She joins the Faculty of Engineering and Built Environment, Universiti Sains Islam Malaysia (USIM) in April 2014 and had been appointed as the Dean of Centre for Graduate Studies since May 2015 for two years. Dr. Janatul, a professional engineer certified by the Board of Engineers Malaysia, has a vast experience as administrator after her secondment at the Ministry of Higher Education, Malaysia from 2008 until 2014. She has many experiences in delivering lectures, talks and technical papers at national and international conferences. She has published tremendous articles in highly esteemed journals. Her current research interests are on acoustics and noise control.

Ahmad Faizal Mohd Zain formerly was the Director of Learning and Teaching Innovation Center at Faculty of Science & Technology, Universiti Sains Islam Malaysia (USIM). He obtained PhD from the Pennsylvania State University, USA preceded by Master and Bachelor from University of Shaffield, UK. His professional activities included membership of the Institute of Engineers Malaysia (IEM) as Fellow, Lembaga Jurutera Malaysia as Professional Engineer, Institute of Electrical and Electronics Engineers (IEEE) as Senior Member, Akademi Sains Malaysia as Chairman Engineering Discipline and Fellow & Council Member and also Institute of Materials Malaysia as Fellow. While in USIM, he became an Internal and External supervisor for more than 13 PhD students. He published more than 16 books, chapter in books, journals and proceeding since 2009. His areas of specialization and research interests include Aeronomy, Aerospace Science, Applied Sciences & Technologies, Electromagnetic Compatibility (EMC) and Wireless Communication & Technologies.

Abu Bakar bin Hasan received Bachelor degree in Physics from Universiti Kebangsaan Malaysia, in 1980 and Masters in Digital System from University of Cranfield, United Kingdom in 1984. He pursued his Ph.D. in Engineering at Universiti Tenaga Nasional (UNITEN) in 2013 after received his second Bachelor degree in Electrical Engineering from Universiti Teknologi Malaysia (UTM) in 2010. He joined the Faculty of Engineering & Built Environment, Universiti Sains Islam Malaysia (USIM) as Senior Fellow and currently appointed as Deputy Dean of Faculty of Engineering & Built Environment until present. His research interests includes Physics, digital systems, electrical and engineering.