Video Signal Recovery from the Smartphones Touchscreen LCD Display

Bogdan Trip[1(✉)], Vlad Butnariu[1], Alexandru Boitan[1], and Simona Halunga[2]

[1] The Special Telecommunications Service Bucharest, Bucharest, Romania
bogdan.tripc@gmail.com
[2] Telecommunications Department, University Politehnica of Bucharest, Bucharest, Romania

Abstract. In this paper we present several examples of video signal recovery from electromagnetic emissions generated by smartphones touchscreens as well as a number of measurements results performed in a specialized laboratory. We aimed the identification of the video signal parameters by using video images that were especially selected to facilitate this process. The measurements were performed by comparing two smartphones that have different display resolutions. In the final part we will also present a method to identify the emission frequencies for these compromising emanations.

Keywords: Smartphones · Touchscreen · Video signal · Recovery · TEMPEST · Compromising · Emanations

1 Introduction

The technological advances of recent years are reflected, among other things, in the exponential evolution of technologies used in the mobile phone industry. From the 90's, mobile communication systems evolved through several standards, from 2G - GSM to 3G - UMTS, 4G - LTE and now the 5G standard is under development. The size and complexity of the applications that can be run from a mobile terminal evolved too. While the first models of mobile phones had a 1.5 in. screen with a resolution of 84 × 48 pixels or even lower, today they have a size of 6.2 in. and a Full HD resolution of 2960 × 1440 pixels. Also, if at the beginnings the mobile phones were used only for voice and small rate data applications, today one can use such terminals for high-resolution images or high definition video (HD) transfer, but also for high security demanding applications like bank transactions or fulfilling various complex tasks imposed by the companies we work for. At this point we have come to handle a lot of information through our mobile devices and some of this information can be sensitive and important to us or to our companies. For this reason we have to discuss the issue of ensuring the confidentiality of the manipulated information that belongs to us or the employing companies.

Like any other electronic equipment, smartphones generate electromagnetic radiation. Before entering the market, they are generally tested for Electromagnetic Compatibility (EMC) compliance. In addition, they are also tested for Specific

V. Poulkov (Ed.): FABULOUS 2019, LNICST 283, pp. 89–95, 2019.
https://doi.org/10.1007/978-3-030-23976-3_9

Absorption Rate (SAR) levels for health reasons, and efforts have been made to reduce this parameter significantly during the last few years. The EMC rules and regulations [1] require that all electronic equipment should be checked so that the radiation emitted by the tested equipment should not interfere with the proper functionality of the electronic equipment in its vicinity. However, commercial electronic equipment is not tested also in terms of confidentiality of processed information and identifying the risk level of compromising information and, therefore, this task is analyzed in the TEMPEST domain. The TEMPEST regulations [2] study that part of electromagnetic emissions from which the information transmitted or processed by electronic equipment can be extracted. These electromagnetic radiations are called Compromising Emanations (CE), as they can compromise the information in question. The TEMPEST protection procedures have been presented in detail in [3, 4].

One of the most dangerous CE, is the one radiated by video display units and was first reported by van Eck [5]. Markus Kuhn has treated for a long time the risk of cathode ray tube (CRT) [6] and liquid crystal display (LCD) units [7] while in [8] the authors presented the possibility of measuring the CE from power conductors in the 100–1000 MHz range. Recent research has analyzed CE from the High Definition Multimedia Interface (HDMI) [9] by using simple display signals such as two black-and-white vertical stripes evenly spaced on the monitor screen while in [10] the CE level is analyzed by using a TEMPEST FSET22 receiver and presents the comparative results between the Video Graphics Array (VGA) interface and Digital Visual Interface (DVI). In [11] are presented for the first time examples of video signal recovery from small displays such as the 4.3 (in.) LCD display of a laser printer.

This paper is structured in six sections, as follows. Section 2 presents the measuring equipment, the test-bed as well as the devices under test (DUT). In Sect. 3, a method of detecting CE emission frequencies is exemplified while in Sect. 4 is presented the results of time domain measurements for the analyzed video signal. Section 5 illustrates some examples of video signal recovery and Sect. 6 contains the several interesting conclusions based on the results obtained.

2 Measurement Test-Bed

In our research we used a TEMPEST FSET22 receiver, an active AM524 antenna system and a Tektronix MSO5204B oscilloscope. The tested devices were two smart phones produced by two well-known companies, LG K4 (model 2016) and Samsung J5 (model 2015). All the tests were carried out in a TEMPEST specialized laboratory that is equipped with a semi-anechoic chamber.

The tested devices were placed, one by one, at a distance of 1 m from the receiving antenna, inside the testing room, according to MIL STD 461F military EMC standard. The rest of the measuring chain was placed outside the testing chamber to avoid possible influences that could interfere with the results.

3 CE Detection

In the first phase of the experimental part, we considered it useful to perform several frequency sweeps in order to be able to discover the frequency ranges in which the compromising signal is present. Thus, we chose as test message, an image consisting in three thin horizontal bars of equal size followed by a thick one.

The image was displayed on the screen of the two DUT's, resulting in two waveforms. In order to get a reference to compare them with, we choose to shut down the screens of the two phones and make a new set of sweeps, which are, further, considered as references. In the beginning of CE detection, we performed several tests in the whole frequency range, from 2 MHz to 1 GHz and we decided to focus our attention on the 30 ÷ 200 MHz subrange using a Resolution Bandwidth (RBW) of 2 MHz, respectively a Sweep Time (ST) of 35 milliseconds (ms). The receiver performs the frequency sweeps by dragging the capture filter (RBW) from the starting frequency to the end of the sweep range and the ST parameter signifies how long it stays in place at each slide. As the tested DUT has a declared refresh rate of 60 Hz, it results that the video signal has a period of 16.6 ms = 1/(60 Hz). The ST parameter was chosen to be longer than the video signal period to ensure that the CE will be detected. In Fig. 1 are shown the sweep results obtained using the LG K4 smartphone as testing device and in Fig. 2 are the ones obtained with the Samsung J5 device.

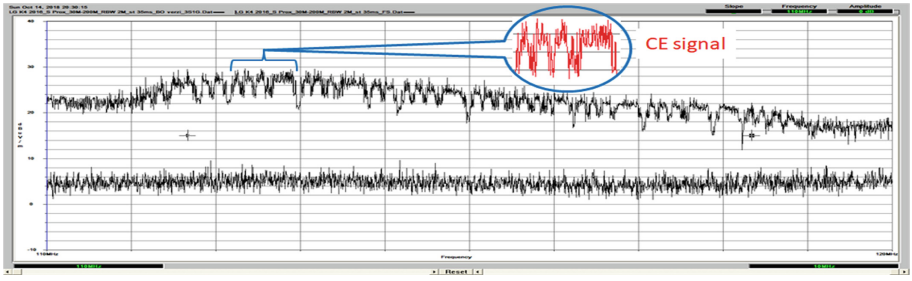

Fig. 1. CE detection for LG K4 smartphone, 110 ÷ 120 MHz

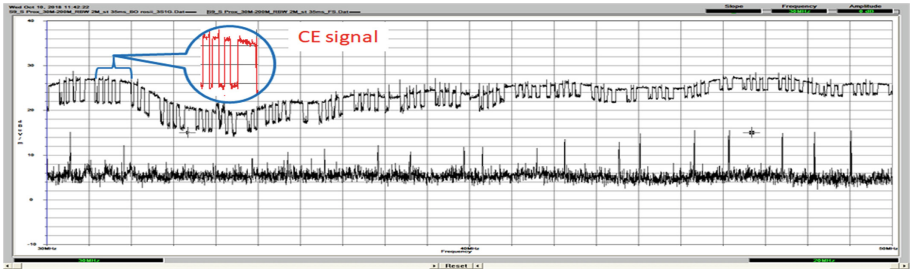

Fig. 2. CE detection for Samsung J5 smartphone, 30 ÷ 50 MHz

Thus, the upper waveform in the figures above represents the compromising signal and the lower one is the reference. For the LG K4 smartphone we chose to illustrate the 110 ÷ 120 MHz sub-range as the difference between the CE signal and the reference is the most significant, while for the Samsung J5 smartphone this is true for the 30 ÷ 50 MHz sub-range.

Also, we can notice that in Fig. 1 the CE signal is not received across the entire frequency range, such as 110–111 MHz and 119–120 MHz, and thus illustrates the result of the CE signal detection process.

4 Time Domain Measurements

The properties of video display signal were detailed in [11], as well as the difficulties encountered in detecting and visualizing the CE signal in order to assess the level classification according to the limits specified in [2], which is considered as classified information ("NATO Confidential").

Regarding this, measurements have been made to reveal the time parameters of video display signal for the smartphones that have been tested. We used the same test signal described in Sect. 3, and, as receiver, an oscilloscope that takes the analog signal after the 21.4 MHz intermediate frequency output of the FSET22 receiver. In Figs. 3 and 4 are presented the received signals for the two devices under test.

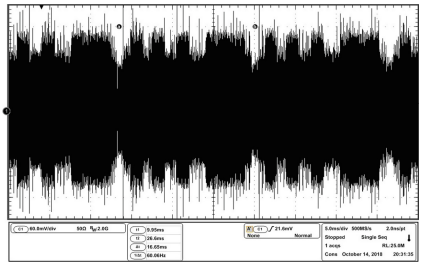

Fig. 3. Video frame period of 16.65 ms - LG K4 (3 thin bars and 1 thick bar)

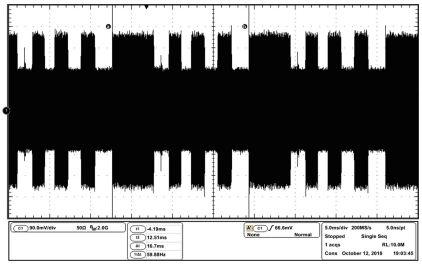

Fig. 4. Video frame period of 16.7 ms - Samsung J5 (3 thin bars and 1 thick bar)

We can see in Figs. 3 and 4 that the video signal's period of the analyzed signal, measured with two vertical markers, is 16.65 ms for LG K4 and 16.7 ms for Samsung J5. The oscilloscope is used as the receiver's time domain projection and in conclusion does not reflect the real level of the analyzed signal as the signal level depends on the receiver settings. Capturing signals via oscilloscope was done without changing the reception parameters for the FSET22 receiver. For both equipments we recorded the same noise level of approximately 360 mV. A maximum video signal level of 450 mV was received for the LG K4 smartphone and 675 mV respectively for the Samsung J5 smartphone. So we recorded a signal to noise ratio (SNR) of 20lg (450/360) = 1.9 dB for the LG K4 phone and 20lg (675/360) = 5.4 dB for Samsung J4 model.

5 Video Signal Recovery

In this section we tried to recover the image displayed on the two smartphones only based on the radiated CE. In Fig. 5 we obtained an intelligible image reconstructed from the CE radiation of the LG K4 smartphone. We observe that the image is still intelligible, even though is affected by noise. The "TEMPEST" message, written with a font size of 24, has the last letter "T" almost completely covered by noise. With further signal processing of the received signal, a much clear signal might have been obtained. In Fig. 6 we have another situation, this time a very clear image recovered from the CE radiation of Samsung J5. In this figure we can see the "TEMPEST" message, written with a font size of 48, 24, 16, 8 and also 4.

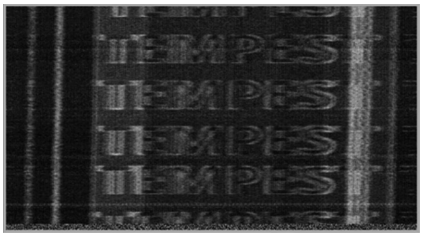

Fig. 5. Test message recovery for LG K4, on the 113 MHz reception frequency

Fig. 6. Test message recovery for Samsung J5, on the 31 MHz reception frequency

The video signal recovery examples, illustrated in Figs. 5 and 6, were performed under the same reception conditions, as described in Sect. 2. The differences in the images quality are given by the radiation differences of the CE signal existing between the two DUT's.

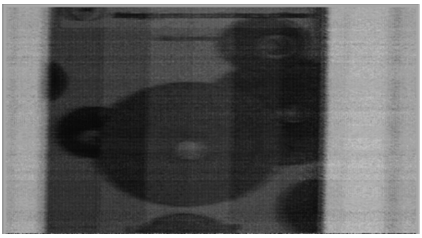

Fig. 7. LG K4 screensaver, 113 (MHz)

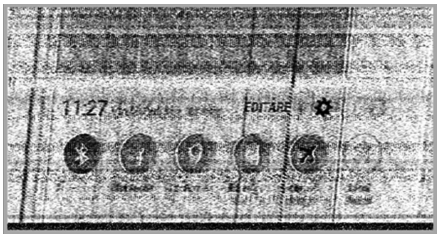

Fig. 8. Samsung J5 setting menu, 31 (MHz)

We have also performed some video signal recovery with no informational content such as the LG K4 screensaver on the 113 MHz frequency as shown in Fig. 7 and the Samsung J5 smartphone menu on 31 MHz. In Fig. 8 we can also observe that the "Bluetooth" and "airplane" modes are active during the image recovery process.

6 Conclusions

We can conclude that it is possible to recover video display signal from the reception of CE radiation generated by smartphone touchscreens that are today on the free market. From the measurements results we can see that the Samsung J5 smartphone is more vulnerable to interception than the LG K4 smartphone since, in all the cases, the signal can be recovered by an unwanted intruder easier and with better accuracy.

This unexplored vulnerability imposed by the use of modern mobile phones, often replacing personal computers, should be taken as a warning signal.

Our research should be continued to estimate the propagation distances for this CE radiation or identifying possible countermeasures. We recommend minimizing our sensitive and important information that we should handle with our smart phones in an open space area or without electromagnetic propagation obstacles.

Acknowledgment. This work was supported by contract no. 5Sol/2017 within PNCDI III, Integrated Software Platform for Mobile Malware Analysis (ToR-SIM).

References

1. The Electromagnetic Compatibility Regulations 2016. http://www.legislation.gov.uk/uksi/2016/1091/pdfs/uksi_20161091_en.pdf. Accessed 15 June 2018
2. NATO Standard, SDIP-27/1: NATO TEMPEST Requirements and Evaluation Procedures (NATO CONFIDENTIAL), NATO Military Committee Communication and Information Systems Security and Evaluation Agency (SECAN) (2009)
3. Bîndar, V., Popescu, M., Crăciunescu, R.: Aspects of electromagnetic compatibility as a support for communication security based on TEMPEST evaluation. In: 10th International Conference on Communications - COMM 2014, Politehnica University of Bucharest, Military Technical Academy, Bucharest, pp. 529–532 (2014)
4. Popescu, M., Bărtușică, R., Boitan, A., Marcu, I., Halunga, S.: Considerations on estimating the minimal level of attenuation in TEMPEST filtering for IT equipments. In: Third International Conference, FABULOUS 2017, Bucharest, Romania, pp. 9–15 (2018)
5. van Eck, W.: Electromagnetic radiation from video display units: an eavesdropping risk? Comput. Secur. **4**(4), 269–286 (1985)
6. Kuhn, M.G.: Compromising emanations: Eavesdropping risks of computer displays. https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf. Accessed 20 June 2018
7. Kuhn, M.G.: Electromagnetic eavesdropping risks of flat-panel displays. In: Martin, D., Serjantov, A. (eds.) PET 2004. LNCS, vol. 3424, pp. 88–107. Springer, Heidelberg (2005). https://doi.org/10.1007/11423409_7
8. Sekiguchi, H., Seto, S.: Measurement of computer RGB signals in conducted emission on power leads. Prog. Electromagn. Res. C **7**, 51–64 (2009)
9. Przesmycki, R.: High definition multimedia interface in the process of electromagnetic infiltration. In: PIERS Proceedings 2015/The 36th Progress in Electromagnetics Research Symposium, pp. 1173–1177 (2015)

10. Przesmycki, R., Nowosielski, L.: Compromising emanations from VGA and DVI interface. In: The 37th Progress in Electromagnetics Research Symposium (PIERS), pp. 1024–1028 (2016)
11. Boitan, A., Bărtușică, R., Halunga, S., Bîndar, V.: Video signal recovery from the laser printer LCD display. The paper had been presented at ATOM-N 2018, The 9th edition of the International Conference on Advanced Topics in Optoelectronics, Microelectronics and NanotechnologiesConstanta, Romania, 23–26 August 2018 (proceeding still under publishing)