Detection of compromising radiation from modern data transfer interfaces using the example of high definition multimedia interface

A P Durakovskiy¹, L N Kessarinskiy¹, E A Simakhin¹

¹ National Research Nuclear University MEPhI, Moscow, Kashirskoe hwy, 31, 115409, Russia

E-mail EASimakhin@mephi.ru

Abstract. Recently the technical channel of information leakage from electromagnetic emanation more and more interesting for specialists in the field of information security. At the same time, new versions of data transfer interfaces are being developed, that quickly distribute around the world. The use methods to detecting informative frequencies are based on the principles of operation of old data transfer interfaces, consider only the harmonics of the signal, excluding information about its type and interfaces that transmit information to. Accordingly, these methods to detecting informative frequencies of modern data transfer interfaces, such as high definition multimedia interface, do not reflect the completeness and may contain errors, which negatively affects the measurement stage. The article suggests a method to detecting informative signals of compromising emanation from modern data transmission interfaces, such as high definition multimedia interface, using an anechoic chamber, special test program and control program for measuring equipment. The proposed method will be useful both for educational purposes and for beginners in the field of technical information security.

Keywords: information security, compromising emanation, anechoic chamber, HDMI interface, LVDS interface

1. Introduction

In the processing of information data transfer interfaces emit informative electromagnetic waves into the surrounding space. Using special equipment and analysing the parameters of this radiation, it is possible to non-invasively intercept information and restore it [1], [2]. The emergence and widespread use of new technologies in information processing increases the risk of loss of privacy. In this regard, the information content of interfaces [3] and the complexity of information recovery [4] are analyzed, and situations of interception of informative signals of modern data transfer interfaces are modeled [5]. The characteristics of modern data transfer interfaces are analyzed in detail [6], new methods of information recovery are developed [7-8]. Extensive research in this field of information security shows the relevance of protecting information from its leakage through this technical channel. Specialists in technical data protection are particularly interested in works related to the practical detection of frequencies of modern data transfer interfaces.
2. Test signal

One of the main steps in analyzing the security of a data interface is to determine the frequencies at which it operates. To do this, specialists in the field of technical security information use specialized programs that transmit a predetermined sequence of data to the interface under study. To form such a sequence, it is necessary to accurately determine its characteristics.

2.1 Characteristics of the test signal

Due to the fact that the electromagnetic field in the conductor appears when the current or voltage changes, a periodic and time-stable test signal must be transmitted to clearly detect compromising radiation from the interface and configure the equipment. The result of the analysis is a set of security indicators that are numerically equal to the signal-to-noise ratio at each harmonic of the interface under study in a given frequency range. For the technical channel of information leakage from side electromagnetic radiation and interference, the signal-to-noise ratio for a pulse sequence in the frequency range is determined by the formula, the General form of which is given in [9]:

\[
\Delta = \frac{E_S}{E_N} = \sqrt{\frac{1}{2\pi F_c} \sum_{j=0}^{K} (E_{S+N}^2 - E_N^2)} \int_{f_h}^{f_l} E_N^2(f) df,
\]

(1)

where \(F_c\) is a clock frequency, \(\tau\) is a pulse duration, \(K\) is a number of harmonics in range, \(E_{S+N}\) is a “pure” signal and noise intensities, \(E_N\) is a noise intensities, \(f_h\) and \(f_l\) are high and low frequency range, \(E_N^2(f)\) is a “dependence” of the noise field strength on the frequency in the range.

When conducting tests related to determining the maximum distance at which it is possible to restore information, the critical operating conditions of the interface under study are evaluated. Critical conditions are determined by the minimum level of noise or interference and the maximum signal level in the surrounding space of the interface under study. The minimum noise level is achieved by choosing the time of testing or using a specialized measuring area – an anechoic chamber.

Based on the formula (1), the maximum signal level is achieved if the duty cycle of the test periodic pulse signal \(D = \tau * F_c\) is less than or equal to 1/2. Otherwise, when calculating security indicators, we will not get the maximum values. If the duty cycle of such a signal is less than 1/2, the pulse emission time will decrease, and therefore the amount of radiated energy will decrease, which contradicts the achievement of critical conditions. Accordingly, the duty cycle of the test signal should be equal to 1/2. In addition, this characteristic of the test signal shows an equally probable distribution of zeros and ones in the sequence transmitted to the interface input, and accordingly bring it closer to real operating conditions.

2.2 Generating a test signal

In accordance with the specification [10], signal transmission in the HDMI interface is based on transition-minimized differential signaling (TMDS) technology, where three channels (Ch0, Ch1, Ch2) transmit sub – pixel information, and the fourth channel is the clock channel (figure 1).

![Figure 1. Block diagram for transmitting an informative signal via HDMI](image)
To confirm the assumption in point 2.1, we used the Rohde Schwarz rtb2004 digital oscilloscope. Using an oscilloscope, the differences between the maximum and minimum voltage values of the transmitted signal were obtained in the channels of the HDMI interface of type "A", corresponding to the transmission of an informative signal with numbers: 1 and 3, 4 and 6, 7 and 9.

The signal transmitted via the HDMI interface is differential, so we can only evaluate 3 of the 6 channels corresponding to different sub-pixels, for example, channels 1, 4, and 7. If we refer to the RGB palette, the boundary colors for it are white - (255, 255, 255) and black - (0, 0, 0). When these colors alternate, we get the longest radiation time. The values of all three pixel components for white and black are the same, so we can only evaluate 1 channel, for example, the 4th (figure 2).

![Working with the oscilloscope R&S RTB2004](image)

Figure 2. Working with the oscilloscope R&S RTB2004

The results of working with the oscilloscope are shown in table 1.

| Title                      | Image on the monitor display | Oscillogram | ΔV, mV |
|----------------------------|------------------------------|-------------|--------|
| White screen               | ![White Screen Image]        | ![Oscillogram] | 791.02 |
| Black screen               | ![Black Screen Image]        | ![Oscillogram] | 561.52 |
| Point-to-point             | ![Point-to-Point Image]      | ![Oscillogram] | 859.37 |
| 2 points through 2 points  | ![2 Points Through 2 Points Image] | ![Oscillogram] | 830.47 |
| 4 points through 4 points  | ![4 Points Through 4 Points Image] | ![Oscillogram] | 805.21 |
| Half of the screen         | ![Half of the Screen Image]  | ![Oscillogram] | 66.48  |
| 3 lines                    | ![3 Lines Image]             | ![Oscillogram] | 83.64  |
| 5 lines                    | ![5 Lines Image]             | ![Oscillogram] | 80.78  |

A point-to-point test signal is a repeating sequence of one white pixel and one black pixel. A point is defined as a single pixel. Similarly for the "2 points through 2 points" and "4 points through 4 points"
tests. Table 1 shows that the point-to-point test sequence has the largest voltage difference, and as the time between the back and front edges of the two pulses increases, the signal energy decreases.

Thus, it can be established that the point-to-point test has more relevant characteristics for determining the interface frequencies. To show the difference in the energy of test sequences that differ in characteristics from sequences with a duty cycle equal to 1/2, sequences that do not meet the requirements of paragraph 2.1 were additionally considered. As can be seen from table 1, their energy is much less. To create a test sequence we was written a C++ program using the Windows API.

3. Description of the detection method

Important criteria for detecting an informative signal for the researcher are the conditionally stable electromagnetic environment and the type of measuring device that can most accurately determine the presence of the signal. In real conditions of information leakage through side electromagnetic radiation, the attacker has more sensitive and expensive equipment and searches for information with minimal noise, for example, at night. To approach such conditions, it is necessary to use a specialized measuring area - an anechoic chamber (AC) for the electromagnetic frequency range.

3.1 Measuring area

In addition to the characteristics of the measuring area, the location of the object under study is also important. The location of the interface or computer is also important for actual operating conditions. To do this, place the monitor in the center of the turntable at a height of approximately 80-90 cm from the floor. The distance from the floor is selected based on the average height of the office desk (figure 3). Also need to exclude other monitors or computers from working, which will increase the accuracy of detecting the interface's own signal.

![Figure 3. The location of the monitor](image)

In addition, there should be no devices with the analyzed interface inside the AC, even if they are turned off. This is necessary because if the wavelengths of the conductor and the data interface match, the digital signal can be modulated by various generators in the computer. Thus, the measured energy of the signal from the analyzed interface may change, which will negatively affect the accuracy of the research results. The described location measures are also used to reduce noise.

3.2 Detection

In process of analyzing the specification of HDMI and the monitor architecture, we paid attention to the adjacent informative data transfer interfaces. Next, we will call an adjacent informative interface such that it receives data from the HDMI and carries the information necessary to restore the original signal. In the case of HDMI, the following is an informative interface with low-voltage differential signaling (LVDS). Due to spread spectrum modulation (SSM), the LVDS spectrum is broadband. The spectrum of the LVDS interface for different SPAN (figures 4 and 5).
As the research has shown, the width of the LVDS spectrum increases depending on the harmonic number (figures 6, 7 and 8). Further, the LVDS harmonic will be called the central frequency of the spectrum. This does not contradict generally accepted terms, since before applying modulation transformations, the LVDS spectrum looks like the spectrum of a harmonic signal.

Also we revealed that the LVDS interface operates at the same frequencies as the HDMI interface. Thus, we observe an overlap of the spectrum of the two signals. And since the signal power from the LVDS interface is greater than the signal power from HDMI, during normal operation of the LCD monitor, we will always observe the spectrum of the LVDS interface on the measuring receiver. Thus, it will not be sufficient to simply use the receiving antenna to explicitly detect an informative signal from HDMI. To solve this problem, use a voltage probe for destructive testing or a current collector for non-invasive testing. In this case, destructive research that leads to a violation of the shell of the HDMI cable. After such an impact on the cable, it cannot be used for measurements as this is a deviation from the normal (factory) configuration of the interface and reduces the level of noise immunity. To avoid this, we can use a current collector that has a verification certificate for the search range. In this case, to measure the maximum value of the signal intensity, it is necessary to determine the wavelength. After the calculation, move the device along the cable at a distance of $\lambda/4$ from its beginning, where $\lambda$ is a wavelength in meters. Based on this, the minimum will be at a distance of $\lambda/2$ (figure 9 and 10).

Also, to solve this problem, we can turn off the monitor by pressing the button on its case. Because of this, the transmitted frames will not be displayed on the monitor screen. However, the search for the informative interface of the frequency or measuring the intensity of the receiving antenna is also incorrect. We know that an electromagnetic field propagates through space with the property of attenuation or scattering. At short distances or in the near zone from the source, the electromagnetic field is weakened in proportion to the cubic function of the distance. The distance from the cable axis to the receiving antenna is greater than to the current collector housing. The difference in distance depends on the size of the receivers and the location of the receiving antenna. From this point of view, searching for dangerous frequencies using a current collector is the right solution.
3.3 Experiment

The operating detection range from 9 kHz to 300 MHz was selected for the experiment. The Rohde Schwarz FSW 13 spectrum and signal analyzer with a frequency range from 2 Hz to 13.6 GHz was used as a measuring receiver. To search for informative frequencies of the HDMI interface, a TI2-3 current collector was used, operating in the range from 9 kHz to 300 MHz. The AI5-0 dipole antenna was used, operating in the range from 9 kHz to 2 GHz. An HDMI cable version 1.3 was used as the object of research. To control the measurement system, a program was developed in the graphical programming language "G" in the LabVIEW development environment. Using this program, we can control the measuring receiver in real time, automatically search for signals relative to noise and threshold values of intensity in a given frequency range, adjust the central frequency of the signal depending on the maximum intensity, automatically identify informative frequencies, measure the electromagnetic field strength at detected frequencies, and output a measurement report in the "*.docx" format.

The signal search is performed as follows. The first step in the search is to determine the clock frequency of the HDMI interface. Depending on the cable category, it may be different. We chose the category "A" cable, so the clock frequency is 74.25 MHz. Set the center frequency equal to the clock frequency and SPAN at least 5-10 MHz on the measuring receiver. Turn on the test signal, set the current collector to the initial position (next to the monitor connector). Then slowly move the current collector along the cable from the monitor, observing the increase in tension. To speed up the process of detecting informative frequencies, we used the reception of cyclic and sequential switching on and off of the test signal, changing the values of RBW and SPAN. After determining the expected frequency, go to the time domain (SPAN is 0 Hz) and send a test signal that is not typical for the interface, for example, 5 lines (figure 11). When the signal intensity is high, a special test for visual verification is not required, since the transmitted signal has the characteristic appearance (figure 12).

However, this method is relevant for detecting only the particular harmonic. To detect the others harmonic, we need to turn off the monitor, put the dipole antenna to the monitor connector, and select vertical polarization. Turn on the test signal and move away from the antenna at a distance of more than 1 meter to avoid interference. The accuracy and execution time of the control program search module depends on the number of samples in SPAN. A large number of samples increases the accuracy of detection, but also increases the detection process. To minimize the number of such samples, the center frequency correction mode was used. To do this, we check the small frequency region around the detected frequency equal to \(2 \times RBW\) and refine the central frequency. Then we run a selection of informative frequency, not using a typical test as a reference. The program compares the signal at each
frequency and calculates the correlation coefficient, which determines the “informative” of the frequency.

4. Conclusion
This article describes a General approach to detecting compromising radiation from modern data transmission interfaces using the example of HDMI using a dipole antenna and a current collector, and provides experimental confirmation. It is also shown that the use of an anechoic camera, a test program written in C++ using the Windows API, and a special measurement receiver control program written in the LabVIEW development environment significantly increases the detection accuracy and speeds up this process. The proposed method will be useful both for educational purposes and for beginners in the field of technical information security. Further work will be aimed at automating the process of analyzing broadband signals and working with LVDS and RSDS interfaces.

5. Acknowledgment
The authors express their gratitude to the management of the NRNU MEPhI for organizing work in the anechoic chamber, the center for the development of automated systems and rental of measuring devices "Priboroteka" for providing specialized equipment and consulting high-level specialists.

References
[1] Eck W V 1985 Electromagnetic Radiation from video display units: An eavesdropping risk? Comput. Security vol 4 no 4 (Amsterdam: North-Holland/American Elsevier) p 269
[2] Wang L and Yu B 2012 Research on the compromising electromagnetic emanation from digital signals Proc. Int. Conf. on Automatic Control and Artificial Intelligence(Xiamen) p 1761
[3] Kuhn M G 2003 Compromising emanations: Eavesdropping risks of computer displays, Technical report UCAM-CL-TR-577 (Cambridge: University of Cambridge Computer Laboratory) chapter 4 pp 77–84
[4] Kuhn M G 2013 Compromising emanations of LCD TV sets Proc. IEEE Transaction on electromagnetic compatibility vol 55 no 3 (London: IET) p 564
[5] Song T, Jeong Y and Yook J 2015 Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR Proc. IEEE Transactions on Electromagnetic Compatibility vol 57 no 2 (New York: IEEE) p 164
[6] Kubiak I and Przybysz A 2019 DVI (HDMI) and DisplayPort digital video interfaces in electromagnetic eavesdropping process Proc. Int. Symposium on Electromagnetic Compatibility – EMC EUROPE 2 (Barcelona) (New York: IEEE) p 388
[7] Meulemeester P Scheers B and Vandenbosch G A E 2019 A quantitative approach to eavesdrop video display systems exploiting multiple electromagnetic leakage channels Proc. IEEE Transactions on Electromagnetic Compatibility vol 62 no 3 (New York: IEEE) p 663
[8] Meulemeester P Scheers B and Vandenbosch G A E 2020 Differential signaling compromises video information security through AM and FM leakage emissions Proc. IEEE Transactions on Electromagnetic Compatibility (New York: IEEE) p 1
[9] Rembovskiy A A Ashihmin A V and Kozmin V A 2006 Radio monitoring: tasks, methods, tools (Moscow: Hot line - Telecom) chapter 11 pp 444–451
[10] Hitachi, Matsushita Electric Industrial Co, Philips Consumer Electronics, Silicon Image, Sony Corporation, Thomson Inc and Toshiba Corporation 2006 High-Definition Multimedia Interface Specification Version 1.3a chapter 4 pp 10–48