EasyChair Preprint

№ 13077

Self-Masking Effect of Parallel Presented Data to Ensure Protection of Information in Technical Channels of Leakage

Serhii Ivanchenko, Anatolii Holishevskyi, Oleksandr Dranovych and Oleksii Gavrylenko

March 28, 2025

Self-Masking Effect of Parallel Presented Data to Ensure Protection of Information in Technical Channels of Leakage

Serhii Ivanchenko [1], Anatolii Holishevskyi[2], Oleksandr Dranovych [3], Oleksii Gavrylenko[4]

[1] Institute of Special Communications and Information Protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Verkhnokliuchova St, 4, Kyiv, 03056, Ukraine

[2,3] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, M. Zalyznyaka St.,3, Kyiv, 03142, Ukraine

[4] The Department of Information Technology Security, National Aviation University, Lubomyr Huzar Avenue, 1, Kyiv, 03058, Ukraine

Abstract. *The influence of the bit depth of the parallel code of interfaces used in modern information and telecommunication systems on the probability of detection, interception and correct reproduction of information has been analyzed. The influence of the factor of technological difference of radio-electronic components, which are components of information and telecommunication systems with parallel code, on the security of information from leakage to technical channels has been analyzed.*

Keywords: *technical information protection, information and telecommunication systems, technical channels of information leakage, throughput, risk probability.*

One of the directions of ensuring the confidentiality of state information resources at information activity facilities and in information and telecommunication systems (ITS) is their protection from leakage through technical channels that arise as a result of unwanted parasitic effects. These are side electromagnetic radiation and guidance fields of dangerous signals (TCL), which are accompanied by the operation of technical means and information processing and transmission systems and which create a threat to its leakage beyond the boundaries of the facility. Using the specified vulnerabilities, interested parties have real opportunities to determine the parameters of a dangerous signal at a distance from its source and, analyzing them, obtain the necessary information [1].

The purpose of this work is to increase the effectiveness of countering information leakage through technical channels at facilities that use ITS with parallel code, by analyzing and improving such technical conditions that would make it impossible for attackers to implement threats to interception.

As a rule, this impossibility is reduced to ensuring the required signal/interference ratio in the environment of the dangerous signal propagation: the air, power supply and grounding circuits, branch electrical circuits and external conductors - places where the

enemy can carry out interception. The required signal/interference ratios in places of possible interception are numerical normalized indicators that, with an acceptable probability, determine the adequacy of protection of all types of information (voice, television, digital, etc.) taking into account the degrees of restriction of access to it or its value, established by the owner, and ensure the requirements for protecting information from leakage in general.

Typically, modern ITS use interfaces with binary representation of information in the form of a serial or parallel code.

As is known, parallel transmission of a digital data signal is such a transmission in which its individual elements, combined into groups, are transmitted simultaneously over separate data transmission channels or at different carrier frequencies over one channel. Parallel ports use 2N lines for simultaneous information transfer, which allows byte-by-byte data transfer. In addition to physical data lines, parallel interfaces may include such components as: parity line, receiver (transmitter) control signal line, receiver (transmitter) readiness line, zero line (GND), transmission (reception) error. For example [2], these are buses for connecting expansion cards ISA (8 or 16 bits), ATA (32 bits), PCI (32 or 64 bits), SCSI bus (8 bits) for connecting HDD drives, CD and DVD drives, for connecting printers and scanners IEEE 1284 (8 bits, also LPT), IRPR (8 bits, also BS 4421), access bus to non-volatile memory of parallel integrated circuits (Atmel, STM, AMD, Micron), etc.

Let us depict a discrete-continuous information leakage channel of the ITS system with parallel binary code. A potential adversary tries to analyze the environment of dangerous signal propagation available to him, using the optimal receiver, and to detect, intercept, and reproduce information (Figure 1).

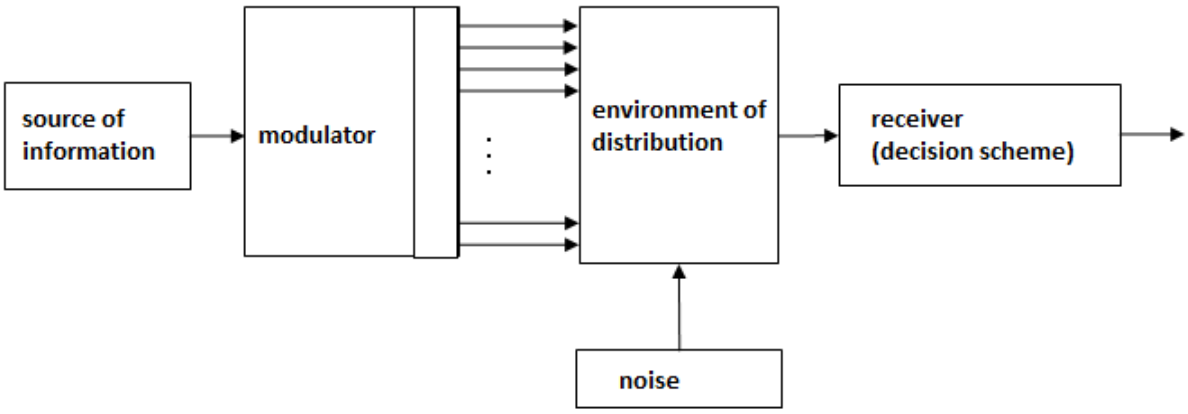

Figure 1 – Discrete-continuous information leakage channel

The energy indicator of information security in the environment of dangerous signal propagation is understood as the probability of detection and correct reproduction of informative signals in the form of TCL. This indicator is based on the theory of two-alternative solutions and characterizes the possibility of detection and correct reproduction of these signals against the background of interference as a function of their energy.

From the theoretical foundations of radar, it is known that the probability of detection of a single pulse against the background of interference is calculated as follows [3]:

$$P_{detect} = 1 - \mathrm{F}\left(\sqrt{\frac{E_{\text{imp}}}{N_0}}\right), \tag{1}$$

where $F(x)$ is the probability integral, the Laplace function, E_{imp} is the pulse energy, N_0 is the spectral power density of the interference at the receiver input.

When forming a TCL from a multi-bit pulse, there is a cumulative emission from each line of the multi-bit bus. In this regard, the total emission of several bits will be formed as an incoherent addition of the emission of each of them, and the probability of detection will be determined by the following expression:

$$P_{detect} = 1 - \mathrm{F}\left(\sqrt{\frac{kE_{\text{imp}}}{N_0}}\right), \tag{2}$$

where k is the number of bits in the signal – the source of the TCL, or the number of lines in the multi-bit bus.

Detection of a code combination differs from detection of a single pulse by an increase in the time of incoherent accumulation of pulses, which is proportional to their number in the code combination. In this case, expression (2) will take the following form:

$$P_{detect} = 1 - \mathrm{F}\left(\sqrt{\frac{\mu MkE_{\text{imp}}}{N_0}}\right) \tag{3}$$

where M is the total number of pulses in the combination, μ is the coefficient characterizing the ratio of logical units to the total number of pulses in the code combination. If the code combination is formed in accordance with the general laws of the binary computing system, then it can be assumed that.

The probability of error-free interception of a multi-bit single pulse is an information indicator based on the methods of the theory of multiple-alternative decisions. The plurality

of alternatives in this case is that for the correct reception of a multi-bit pulse it is necessary not only to detect it against the background of interference, but also to establish its correct correspondence with one of the elements of the alphabet of permissible symbols – a set of binary numbers according to a given bit depth, the number of which is defined as $K = 2^k$.

For such an alphabet, the probability of correct reception of a single multi-bit pulse is determined according to the following relation [4,5]:

$$P_{correct} = 1 - \left(2 - \frac{1}{2^{k-1}}\right) F\left(-\frac{1}{2}\sqrt{\frac{\Delta\overline{E}}{N_0}}\right), \quad (4)$$

where $\Delta\overline{E}$ - average pulse energy difference across the alphabet of permissible symbols. Value $\Delta\overline{E}$ is defined as follows:

$$\Delta\overline{E} = \frac{1}{2^k}\sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\left|E_i - E_j\right| = \frac{E_{i\text{м}n}}{2^{2k} - 2^k}\sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\left|\sum_{l=0}^{k-1}\sigma_{il} - \sum_{l=0}^{k-1}\sigma_{jl}\right|, \quad (5)$$

where E_i, E_j - cumulative (total by bits) energy of a single multi-bit pulse for the i-th and j-th symbols from the allowable alphabet, σ_{il}, σ_{jl} - pulse energy multipliers, which allow taking into account both binary encoding in the symbols of the permissible alphabet and differences in the pulse energy of individual bits.

The correct decision on the reception of a code combination of multi-bit pulses, which guarantees the interception of information due to the TCL, can be achieved only in the case of correct reception of all multi-bit pulses included in the combination. Taking this into account, to calculate the probability of correct reception of a combination of multi-bit pulses, expression (4) will have the following form:

$$P_{correct} = \left\{1 - \left(2 - \frac{1}{2^{k-1}}\right) \mathrm{F}\left(-\frac{1}{2}\sqrt{\frac{\Delta\overline{E}}{N_0}}\right)\right\}^M \quad (6)$$

For further calculations, the feasibility and value of the energy σ_{il} multiplier requires additional explanations. Expression (3) assumes that the influence of the difference in the levels of radiation from individual bits of the multi-bit bus is insignificant. In this case σ_{il} it is converted into a binary multiplier, which can have the value 0 or 1 in accordance with the binary encoding of multi-bit words. The order of

determination $E_i(E_j)$ for such cases can be shown in Table 1 using the example of a three-bit pulse.

Table 1

The difference in the total energy of a three-bit pulse

Number of the symbol (i, j)	Multiplier value σ_{il} (σ_{jl})			Resulting (total) energy of a three-bit pulse $E_i(E_j)$
0	0	0	0	0
1	0	0	1	E_{imp}
2	0	1	0	E_{imp}
3	0	1	1	2 E_{imp}
4	1	0	0	E_{imp}
5	1	0	1	2 E_{imp}
6	1	1	0	2 E_{imp}
7	1	1	1	3 E_{imp}

As can be seen from this table, unique (non-repeating) values of the total energy of a multi-bit pulse exist only for two symbols of the admissible alphabet. Namely for 000 and 111. Therefore, in the case of complete identity of the radiation of individual bits of the multi-bit bus according to the set of parameters being evaluated, the multi-alternative problem of unambiguously assigning the pulse to one of the elements of the alphabet of admissible symbols has no solution. In practice, completely identical radiation of two, and even more so several bits occurs extremely rarely. This is due to technological differences in radio electronic components, as well as different frequency characteristics of random antennas. On a research personal computer, it was practically established that when setting the test mode of transmitting a three-bit sequence via the SCSI interface to a CD-ROM drive, the difference in the radiation energy of different bits was within ±8% of the average value E_{imp}. For the LPT loop when exchanging data with a printer, this difference was 15%. As an example, Table 2 shows the calculated values σ_{il} and E_i for the above-mentioned variants of the multi-bit bus design. From the table it can be seen that even minor random deviations of the radiation levels of different bits lead to the fact that each of the symbols of the permissible alphabet receives an individual value of the total radiation energy, which makes the problem of correct reception of a multi-bit pulse solvable.

Table 2

Examples of total radiated energy of data buses

Number of the symbol (i, j)	SCSI bus to CD-ROM drive, emission difference ±8% of average value E_{imp}				LPT bus to printer, emission difference ±15% of average value E_{imp}			
	σ_{i2}	σ_{i1}	σ_{i0}	E_i	σ_{i2}	σ_{i1}	σ_{i0}	E_i
0	0	0	0	0	0	0	0	0
1	0	0	0,93	*0,93* E_{imp}	0	0	0,99	0,99 E_{imp}
2	0	1,01	0	*1,01* E_{imp}	0	1,14	0	1,14 E_{imp}
3	0	1,01	0,93	1,94 E_{imp}	0	1,14	0,99	2,13 E_{imp}
4	1,05	0	0	1,05 E_{imp}	0,87	0	0	0,87 E_{imp}
5	1,05	0	0,93	1,98 E_{imp}	0,87	0	0,99	1,88 E_{imp}
6	1,05	1,01	0	2,06 E_{imp}	0,87	1,14	0	2,01 E_{imp}
7	1,05	1,01	0,93	2,99 E_{imp}	0,87	1,14	0,99	3 E_{imp}

Conclusions. The dependencies indicated in the work show that the security of information from its detection and correct reproduction by the enemy decreases with an increase in the bit depth of the signal, at the same time, due to parallelism, in addition to the main uncertainty regarding the generated sign in the bit, there is an additional uncertainty, which significantly reduces the probability of making the correct decision regarding the generated multi-bit symbol. Also, the influence of the factor of technological difference of radio-electronic components of ITS with parallel code on the security of information from leakage through TCL channels is proven, namely, in the presence of high-performance interception means, this factor makes the task of correct reception and reproduction of a multi-bit signal solvable. As is obvious, all this requires conducting separate new scientific research, conducting a number of experimental tests to obtain the necessary statistical data, on which the appropriate conclusions and conclusions will be made.

Literature

1. Lenkov S.V. Methods and means of information protection. Volume I. Unauthorized receipt of information / S.V. Lenkov, D.A. Peregudov, V.A. Khoroshko – K.: Ariy, 2008. - 464 p.

2. Ivanchenko S., Puchkov O., Rushak O., Holishevskyi A. Leakage by technical channels for modern information and telecommunication systems / Serhii Ivanchenko, Oleksandr Puchkov, Oleh Rushak, Anatolii Holishevskyi // Materials of the articles of the

International Scientific and Practical Conference "Information Technologies and Computer Modeling", ISBN 978-617-7468-37-9, Ivano-Frankivsk, May 20-25, 2019. - Ivano-Frankivsk: Mr. Goliney O.M., 2019.– pp. 179-183.

3. Theoretical foundations of radar: a textbook for universities / edited by Ya.D. Shirman. - M.: Sov. radio, 1970. - 560 p.

4. Theoretical foundations of communication and control / A.A. Feldbaum [et al.]. - M.: Fiz-matgiz, 1963. - 932 p.

5. Burachenko D.L., Zavarin G.D., Klyuev N.I. et al. General theory of communication.– L.: VAS, 1970. - 412 p.