ELECTROMAGNETIC RADIATION AND THE COMPUTER SYSTEMS DATA SECURITY PROBLEM

Atanas NACHEV

The Problem

This problem stems from two basic facts. The first is connected with the physics of the processes taking place in digital electronic equipment. The second is due to the way of representing, processing, and transferring the information. The presence of current pulses in power buses due to the impulse character of the functioning of the digital integrated circuits, the existence of inductive and capacity parasite connections, which cause the emergence of high frequency current, and the impulse character of the currents in connecting cables and interface chains all cause the emergence of parasite electromagnetic emissions, which are transmitted as electromagnetic waves. At the same time, in the cables of the power supply alternating currents are induced in such a way that the power supply circuitry becomes a source of secondary wide band emission.

The problem of the electromagnetic emission of computer systems is mainly a problem of peripheral units, the electronic screens of monitors and printers. The modules of the videotract of the monitor are one of the main reasons for the parasite electromagnetic emissions. The field, created by them, contains the whole information about the formed images. This is specified by the principle of image formation on the monitor's screen. It is known that the video signal modulates the current of the electronic ray in accordance to the law for the received image. In that way the video signal turns to digital signal, the logical units create light dots on the luminophor of the screen. Results of studies of electromagnetic emissions of different monitors, carried out with the help of selective sensors and spectrum analyzers, show the level and the spectral characteristics of the generated electromagnetic field which depend on the type of the visualized information and the quantity of the visualized signs. The level of the narrow bands does not depend on the filling up of the screen

but the system of synchronization and the frequency of the repetition of the light dots that specify it. The video amplifier is a powerful source of wide band electromagnetic emission. Practically all interface conductors can be observed as transmission antennas of electromagnetic waves. Their structure contains the whole information of the transferred data. The spectral characteristics of the field are directly dependent on the structure of the impulse consequence, transmitted along the conductors, and the energetic parameters of the field are specified by both the size and the form of the corresponding conductors and the size and the frequency of the currents. The generated electromagnetic field when computer systems operate has wide spectrum and random character of the density of the frequency and the levels of the spectrum. The frequency spectrum is too wide; it can take a band varying from several MHz to 1000 MHz and even more.[4] We should stress that each microcomputer system has a specific electromagnetic emission (features of the spectrum and its power). Placing several computers in a room with limited proportions does not lead to interference of the electromagnetic field and thus corrupting the information because of the reasons mentioned above. In the spectrum of electromagnetic emissions frequencies equal to and multiple to the clock frequency are also present.

The definition of the frequency range of the electromagnetic field containing the information of the processed data is often quite important in terms of choosing the appropriate methods and means of protection. The means for visualizing and for providing data input should be treated as major information sources in the context of the discussed problem.

Methods for Providing Effective Security

The following methods for providing effective security of the information against remote unsanctioned access through limiting the influence of electromagnetic emissions are considered feasible:

1. Use of computer systems with appropriate design that provides low levels of electromagnetic energy emission. These are the means that normally belong to the so-called TEMPEST protection;
2. Adequately screening the premises where the computers are placed and used;
3. Use of devices for active protection [4] which generate and emit masking electromagnetic fields with corresponding characteristic.

The use of computer systems with low levels of electromagnetic emissions is perfect solution to the problem, but it involves considerable financial expenditures. Nowadays such installations can be found at the market. The major drawback of these

security systems is their higher cost compared to the cost of conventional computers. For this reason there are not many producers of such systems.

The wide usage of screened premises is inexpedient because of financial, ergonomic and other reasons.

The use of appliances for *active security* [4] is promising and economically suitable. Its application is possible if the following requirements are met:

- generating and emitting electromagnetic field which secures effective masking of electromagnetic emissions transmitted by computer systems;
- emission of masking electromagnetic field with a capacity that does not "pollute" the radio frequency spectrum, i.e. the conditions of electromagnetic compatibility with other radio electromagnetic appliances are not disturbed;
- the presence of effective means for constant control over the parameters of the masking electromagnetic field, i.e. control over the presence of the necessary protective effect;
- limiting the possibilities of using computer systems when the necessary level of security is not reached;
- clear signaling when the conditions for protection are disturbed.

To limit the influence of electromagnetic emissions when the active security approach is implemented we can choose between:

- supplying each computer system with emitters of masking electromagnetic field;
- constructing systems for protecting premises and buildings equipped with computer systems.

Experiments are under way for using compensation of the electromagnetic emissions by creating a mirror-image field of the electromagnetic field generated by computer systems.[4] It is not consider possible to use this method widely.

Furthermore, protection systems can be constructed as systems for:

- independent (autonomous) protection;
- protection of premises using devices for blocking;
- protection of premises and buildings using devices for blocking and exercising central control over the security.

The autonomous protection is realized by installing security devices in the premises, which function independently without any relation to the operation of the computer systems. Administering effective control over the masking field and the generation of signal when the conditions of effective protection are violated is a must.

When blocking devices are used, the emitters of the masking field are integrated in the computer systems. When the masking effect is disturbed or when it disturbs the functioning of the system, data processing becomes impossible. It is obvious that the blocking should be done without any loss of information or violating the systems' software. Another modification of this method is the use of reserve security means which are switched on automatically when a flaw appears in the corresponding emitters of the masking electromagnetic field. Its use is suitable for protecting premises where servers are placed and switching them off is objectionable.

Protecting premises by using locking devices and centrally controlled security devices is suitable for large buildings where top secret data is processed. The merit of the system is that it allows operative interference when there is a problem concerning the working capacity of the elements forming its structure.

Pseudo-white noise, modulated or not by noise signal impulse jamming can be used either separately or in combination with methods for protecting information through limiting the electromagnetic emissions in computer systems and their masking (active security). According to the way of generating the sequence of the impulses, both modulated and not modulated, we can have:

- impulse jamming with a constant amplitude and frequency of consequence;
- modulated and not modulated impulse jamming with a random amplitude and frequency of consequence;

It is possible also to imitate images on the screen or imitate other useful information signals.

The emission of active quasi-constant bordering jamming in the whole frequency range of the electromagnetic impulse emission from computer systems is one of the effective methods for information security. A disadvantage of this method is the need for creating a set of higher harmonics of the masking electromagnetic field over these from the electromagnetic emissions. There are some difficulties concerning the requirements of even overlapping of the frequency range from several MHz to 1GHz and more. In some cases this leads to difficulties in accomplishing the terms for effective masking of the electromagnetic emissions regarding the requirements for electromagnetic compatibility. For generating of bordering not modulated impulse jamming the use of fluctuation processes arising in semiconductors at certain conditions,[4, 5] as well as processes of excitation of constant signals in noise generators with distributed fluctuating systems, are recommended.

During the operation of computer systems high frequency electrical currents are generated in the power grid, which create conditions for remote access to the

processed data. These are the reasons why protection should be provided for securing the power supply; also electromagnetic emissions should be subsided.

In conclusion, we should say that electromagnetic emissions from computer systems are subject to unsanctioned access to the processed data and therefore represent real danger. That is why the removing of the influence of electromagnetic emissions is an important element of the data securing system.

References:

1. Dragomir Pargov, Veselin Tselkov, Rusin Petrov and Iliya Kraytchev, "Security in Computer Systems," in *Information Aspects of Security and Development of Modern Societies*, Velizar Shalamanov and Todor Tagarev, editors (Sofia: AFSEA-Sofia, 11 - 13 September 1996), 93-98.
2. Veselin Tselkov, "The challenges of 21th century for security of the information society," in *Proceedings of the 1999 AFCEA-Sofia Seminar* (Sofia: AFCEA-Sofia, November 25-26, 1999), 35-40.
3. *Systems for protecting digital equipment against remote access*, USA Patent No W090/00840.
4. *Computer security device*, European Patent No 0240328.
5. *Method and apparatus for preventing external detection of signal information*, USA Patent No W090/09067.

ATANAS NACHEV is an Associate professor at the "G.S. Rakovski" Defense Academy in Sofia, Bulgaria. Since January 2000 he is Head of "C4I systems" Section of the Institute for Advanced Defence Research. Prior to this appointment, Dr. Nachev served as Head of Communications and Information Systems Section of the Military Research Institute of the General Staff of the Bulgarian Armed Forces. He holds a M.Sc. (1979) and Ph.D. (1985) degrees in Computer Science.