International Journal of Engineering & Technology, *7 (4.36) (2018) 84-87*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

The Technology of Secure Data Processing in Production Systems Based on the Use of Special Microcontrollers

S.G. Magomedov.

MIREA - Russian Technological University,Russia

Abstract

The technology is proposed to provide secure processing of data in technological systems based on the use of special microprocessors. A variant of the architecture of such a microprocessor is presented, as well as data processing algorithms that allow efficiently solving problems of secure data processing. The basis for the protection of data processing is the use of algorithms based on the sets of residual number systems (RNS). In the operative memory of the microprocessor, not the number, but the sets of its modules, are stored and processed. Therefore, stealing an intruder of a modules set does not allow him to recover the required number. The encryption keys for each microprocessor are formed together with other ones in the framework of a subsystem controlling other microprocessors, as well as the server.

Keywords: *technology, microprocessor, server, algorithm, processed*

1. Introduction

Since the 1980s, as a result of scientific and technological progress in engineering and technology management of production processes are come essential changes in production organizations associated with the active implementation of automation tools and various information systems related to business processes, One of those technologies for introducing automation tools into a flexible production are integrated forms of production organization, which are linked to the production and marketing of products (works, services), in a single production process[1]. All partial processes are connected together based on the management of the production process using computer facilities (CF). Improvement of this technology has led to the creation of integrated computerized production systems (CIP).

Further development of works in this direction led to the emergence of CIP. One of the main disadvantages of CIP is a high degree of centralization of control processes, which often leads problems in data processing in real mode. The appearance of relatively inexpensive microcontrollers in the beginning of the century has opened up new possibilities for distributed data processing. Similar data processing technologies are now actively used in various robotic systems.

However, one of the problems that limits the active use of technologies in production systems is a security issue, since the complexity of such systems, as well as their effectiveness in controlling their operation creates opportunities for unauthorized invention in there functioning. Therefore, the problem of increasing the security of systems, their protection against unauthorized actions of any type is relevant for distributed production control systems, based on the use of microprocessor devices. It is this problem that is considered in the paper. There are several related works on this problem[2]. We also note that a qualitative leap in the introduction of various robotic systems into production processes is expected in the near future. Many of the proposed systems consist of semi-autonomous subsystems, actively using various CFs, including microcontrollers, which also points to importance of the problem under consideration.

2. Research Methods

First of all, let us cite some requirements the implementation of which in distributed production systems based on microprocessors is desirable - for short, they will be called microprocessor control systems (MCS)[3].

1) The production process consists of separately functioning subsystems. In each subsystem, the main production operations under the normal operating mode of the production system are carried out and controlled by autonomously functioning CFs.

2) In the event of a conflict between subsystems, contingencies, unforeseen or emergency situations, control is transferred to the server to which the subsystems under consideration are connected, and the solution of these management problems is performed on the basis of this server.

3) To minimize potential losses associated with the occurrence of atypical and emergency situations, as well as to prevent malicious effects on the production system, it is necessary to ensure mutual control of various CFs within each subsystem; in particular, in microprocessor control systems.

4) The server should be able to interfere with the operation of any of the subsystems at any given time, provided that in the subsystem is an abnormal situation or this decision is taken by the management of the organization.

The implementation of these requirements in the MCS is reachable with the possibility of controlling the operation of some microprocessors by others within the same subsystem. Then, in the event of failure or unauthorized operation of individual microprocessors (MPs), the very fact of their operation violation can be fixed in the MCS and transferred to the server to further solve this problem. When a problem situation arises in a certain

MP in its interaction with another MP, the first one sends control information to the second one. When the correct answer is received, the process of their interaction resumes. Otherwise, a message is sent to the server to check the situation and make the appropriate management decision.

One of the possible ways to provide the described procedure of mutual control is the use of data processing machines based on the use of residual RNS[4]. Below a possible version of the implementation of similar MCs is presented. The basis for the closed processing of data based on the use of RNS is a set of prime numbers, on the basis of which the closed processing of data in the MC is carried out. Let us briefly describe the general technology for implementing this procedure.

To implement the described scheme of mutual control MC, the following is proposed: each of the primes, included in the set forming the foundation of the RNS, provides one of the MCs or the server. Thus, the encryption keys of each MC are formed on the basis of data (prime numbers) provided by other MCs or servers. Then, when a problem situation arises, the MC can send a new prime number for a change in the encryption key of the second MC and continue the data exchange based on this new key. In this case, data exchange can be carried out only using the primes that are known to both MC; In particular, on the basis of the prime numbers that they provided to each other. If unauthorized interference with the work of the second MC is disrupted, the processing of data, which resulted either in the distortion of this data, or in the corruption of the encryption key, and this situation, probably, will be fixed by the first MC.

Practical implementation of the described general scheme assumes, first of all, the presence of MC, based on data processing for the use of RNS. A functional diagram of a possible implementation of a similar MC is proposed in the next section.

3. Results and Analysis

A key component of any modern systems of data processing and transfer are processing units (PU). The complexity of modern (PU) has increased so much that, in the absence of the original PU schemes, they are almost impossible to control even at the level of national institutions in developed countries. Thus, the number of transistors on a chip of the Pentium Nehalem processor is about 200 million. In such a huge blocks of objects you can "hide" quite effective means of theft, destruction or corruption of data, its transfer to the desired address, completion of other unauthorized actions with data. In this case, it is impossible to identify these "bookmarks" in a reasonable time.

Currently, there exists increased competition in the field of information technology and the gradual movement of the confrontation between the individual states and groups of states, large transnational corporations in the field of information warfare. As a bright example of this, the "leakage" of information about the audition of negotiations between leaders of other countries from the US intelligence services can serve. Such facts, taking into consideration that, obviously, not everything has been known, give some reason to believe that unauthorized removal tools and channels of information may appear in the software and hardware products of many of the world's leading manufacturers of IT-tools. For Russia, this problem is particularly essential in the absence of her own production of PU with sufficiently high performance. Therefore, the use of foreign PU with traditional architecture in Russian communication systems and processing of information potentially creates threats to information security (IS).

One of the possible solutions to the problem of information security when using PU is the creation of national versions of IT-products (in particular, PU), or permission to use only the types of PU controlled by the state. The aim of this work is to study the expediency of using special-difference processor (SP), in which there are mechanisms to protect data being processed against possible theft. In the basis of the data processing in SP, the use of residue number system is proposed. In the available literature, there are few works on this topic[5,6,7].

First of all, we carry out the analysis of the possibilities to ensure the protection of information for the architecture of a typical PU on which processors of the fourth and fifth generations are designed. The structural scheme of the PU is described in previous works of S. Magomedov[3]. On a functional purpose PU is classified as operating devices. In its structure, two parts are distinguished: a control unit (control device) and an operation unit (OU). The operation unit is used for data processing. The control unit performs sampling, decoding and calculation of operand addresses, as well as generating a microcommand sequence for each command. You can find detailed inventory PU-set structure and its operation in the process in the works of P. Mognonov, N. Worms et.al.[4,8] With positions IS, the use of such data processor has an after-following disadvantages:

1) The data to be placed in RAM, temporary files, swap files, is presented in an open, not a converted form. If theft or unauthorized reading it occurs, this may lead to information leakage. In particular, since the PU and the contents of RAM to hard disk after the completion of data processing used for swapping, are not usually overwritten. Therefore unauthorized reading the contents of the RAM or the hard disk after the end of the "closed" information processing procedures can lead to data theft.

2) System files used by standard PU and placed in a constant memory are potentially available to an attacker that can make unauthorized changes in them. These changes may become a source of IS violations, inadequate data processing, emergency situations.

Theoretically, to meet the challenges listed above, data encryption mechanism at the processor level and even incorporation of this mechanism directly to the processor may be used. However, existing modern encryption methods are quite complex and bulky, which when incorporated into the structure of the processor will lead to a significant complication of his work.

In addition, it is unclear how the problem of encryption keys can be solved in this case. If the encryption key is laid directly into the processor during its designing and manufacturing, that this unchanged key with repeated use can be unlocked by an attacker – then all processed information is potentially available to him. If we apply the mechanisms for periodic updating keys, the technology of use and operation of PU becomes much more complicated.

Thus, the typical PU primarily focuses on maximizing the speed program execution. Herewith, these processes ensuring information security of information processing are not allocated as a stand-alone problem at all, although, while processing confidential information of the high value, it may be important.

It should be noted that, in the Pentium processors, a special data processing mode relevant to the issues of information security is provided. It is a protected mode. However, it only solves the problems associated with inadequate data processing, that is, only after a problem has already occurred, but not in the normal course of processing.

To solve these problems, it is offered the SP structural scheme below, which allows providing a data processing mode in which data is transformed and then processed being based on a set of prime numbers included in the residue number system basis (RNS). Therefore, a potentially malicious user without the knowledge of this basis even after the data theft can not read the contents of the data. RNS basis is formed in SP for the use within any reasonable period.

Here are the basic concepts related to the calculating in RNS. The residue number system, also called "modular arithmetic"4 is a sign-value notation, in which the representation of the number is based on the deduction concept and the Chinese remainder theorem. RNS is determined by a set of mutually prime modules called basis; so that each integer x in the interval {0, M-1}, where is associated with a set of deductions. Typically, as the bases of Pi, inside the basis, primes are taken. At the same time, Chinese remainder theorem9 ensures unambiguous representation for all integers from the interval {0, M-1}. Moreover, the number of «x» itself can be found based on the relationship

$$x = x_1 \cdot e_1 + \cdots + x_n \cdot e_n (\mathrm{mod}\, M) \tag{1}$$

where

$$e_i = \frac{M}{P_i} \cdot ((\frac{M}{P_i})^{-1} \mathrm{mod}\, P_i), (1 \le i \le n) \tag{2}$$

In the formation of the scheme proposed below, PU structure peculiarities for one of the most successful architectures, namely, Intel Pentium fifth-generation microprocessor are used8,9. One of the main distinctions of the fifth generation PU from previous ones is superscalar architecture, in which the processor has multiple pipelines. It is not unique to the Pentium, but the same generation PU of other famous manufacturers: AMD K5, Cyrix M1. In the scheme of SP proposed below, it also uses superscalar architecture, but considering peculiarities of RNS. That is, the existence of scalar allows a separate calculation for different modules on different pipelines (microcores).

Thus, the proposed architecture of SP has two internal buses connected to the internal registers: one bus is designed for transfer and placement of address data, and the second one is for computer data (Fig. 1).

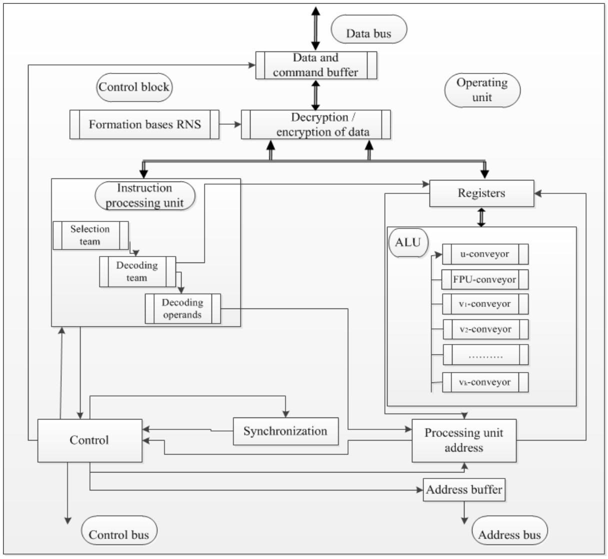

Fig. 1. Structural scheme of the SP organization on the basis of RNS

At first, when SP gets activated, database of primes is formed and stored in the "Forming RNS bases" block. Then, the SP process operation, as in the case of a typical PU on Figure 1, is divided into instruction cycles, during each of which following commands are performed:

1) the next piece of data and a command from the buffer "command and data" are selected;

2) the data is decrypted and placed in the internal registers of SP;

3) the next command is analyzed and decoded into command processing unit;

4) the decoded command, if it is associated with the use of an arithmetic logic unit (ALU), is also located in the interior registers together with the data;

5) ALU selects the performed command and data from internal registers and organizes the appropriate calculations. The process of calculation in the ALU is implemented as an extension of the scheme with two pipelines of the Pentium processor. Herewith, the u-pipeline is principal, as it works with the main flow of commands. There occurs processing the entire set of basic instructions by computing and logical commands, transition commands; assembly of all the intermediate results performed on v-pipelines, in particular, calculation base for individual modules. The calculation result preserves in internal registers of SP, and then after all calculations, data encryption by means of RNS and its placement in data buffer occur;

6) The unit of the processing addresses according to the results of the processing commands and possibly ALU (for the commands of conditional transition) involving the control unit forms the placement address of performed command results (it is placed in the address buffer) and the address of the next performed commands. This address may differ from the sequence one while performing the transition commands;

7) On the address bus, the address is set, to which the results are transferred via the data bus. Then, according to the management command at a certain moment of time, this address is transmitted through the address bus;

8) Control unit, after the formation of all the addresses and data, simultaneously forms both transfer of placement addresses of results through the address bus and data through the data bus;

9) According to the management bus, the next performed command is chosen. For clock synchronization of performing all operations, the control unit uses the synchronizer.

10) The control unit also monitors all possible managing signals from other PUs and signals associated with a particular situation in a computer system and in a processor, such as an interruption. If such signals are available, the control unit accordingly responds.

If you have multi-core SPs, command processing is carried out the same way. When loaded into RAM of the next program module, first of all, a set of n modules gets generated, where n is a number of processor cores that can be used for computations. In this case, the range of variation of prime numbers depends on the type of the use of SP. If a multi-core processor is used for parallel independent computing, in this case, the prime numbers should be compared with the data values processed by each core. If arithmetic calculations are conducted in a modular arithmetic using the Chinese remainder theorem, in this case, the measures of prime numbers should be of the order of magnitude of residuals.

4. Conclusion

The above-described scheme of SP on the basis of RNS can store in RAM and process not the number «x», but sets of its modules. Therefore, set theft by an attacker, generally speaking, does not allow him to restore the number «x» without the knowledge of basis. Basis is directly generated inside the processor, stored inside it, and is not available to the attacker. Therefore, even the presence of one or the other RAM access variant at the attacker, to temporary or swap files, does not allow him to use the information obtained. It is this property of the proposed hardware and software solutions does provide real-time data protection in the course of its processing in SP. We emphasize that the task of ensuring information security of data during its transmission through communication channels from SP to external devices goes beyond the scope of this article.

Transformation discussed above may be performed for system files that are only used by SP, with the source code of these files that can be stored in this modified form. This protects them from modification, spoofing and other malicious acts, as the amended SP file can not be adequately transformed into the code.

It is clear that the proposed hardware and software solutions do lose to conventional PUs at speed. This is the "payment" for the best quality of ensuring information security. In this regard, again, that the use of SP multi-cores can dramatically accelerate information processing. Comparison of the information processing speeds for processors with the traditional architecture and ones of the proposed SP could potentially be made using a computer simulation.

The article presents a general scheme for the formation of secure data processing technology in distributed production control systems based on the use of a microprocessor. It was proposed to use the apparatus of the theory of systems of residual classes when forming this technology. The possible architecture of such a micro-processor is given, algorithms for processing data on it are described. Specific features of algorithms are indicated in case of using multi-core microprocessors. It is substantiated that the architecture of traditional processors, focused on minimizing resource indicators (processing time, energy consumption), does not provide an opportunity to effectively solve information protection issues.

References

[1] Cherviakov N.I., Babenko M.G., Shabalina M.N. Development of a secure system for distributed data storage and processing in the clouds based on the concept of active security in rns/ PROCEEDINGS OF 2017 XX IEEE INTERNATIONAL CONFERENCE ON SOFT COMPUTING AND MEASUREMENTS (SCM) 2017. C. 558-560.

[2] Liventsov S 2007 Fundamentals of microprocessor technology (Tomsk: Publishing house of Tomsk Polytechnic University) p. 118

[3] Chervyakov N.I., Lyakhov P.A., Babenko M.G., Lavrinenko A.V., Nazarov A.S., Lavrinenko I.N. The architecture of a fault-tolerant modular neurocomputer based on modular number projections/ Neurocomputing. 2018. T. 272. C. 96-107.

[4] Worms N, Ryadnov S, Sahnyuk P, Shaposhnikov A 2003 Modular structure neuroprocessor parallel computing systems (Moscow: FIZMATLIT) p. 288

[5] Magomedov Sh. Organization of secured data transfer in computers using sign-value notation//ITM Web of Conferences. 2017. T. 10 DOI: 10.1051/itmconf/20171004004

[6] Ivanova I A, Nikonov V V, Sumkin K S 2015 Problems of improving security of data transfer in computer systems Russian Journal of Technology 4:92-8

[7] Aremu I A, Gbolagade K A 2017 Generalized Information Security and Fault Tolerant based on Redundant Residue Number System International Journal of Computer Applications 167/13:43-7

[8] Mognonov P 2003 Organization of microprocessor systems (ESSTU) p. 174

[9] Omondi A 2007 Advances in Computer Science and Engineering: Theory and Implementation (London: Imperial College Press) p. 296

[10] S. G. Magomedov, Popov G.A. Comparative analysis of various methods treatment expert assessments/International Journal of Advanced Computer Science and Applications. 2017. T. 8. № 5. C. 35-39. DOI: 10.14569/IJACSA.2017.080505