LUPINE PUBLISHERS

ISSN: 2643-6744

Current Trends in Computer Sciences & Applications

DOI: 10.32474/CTCSA.2019.01.000112

Mini Review

New Multilevel Architecture of Secured Supercomputers

AS Molyakov*

Russian State University for the Humanities, Russia

***Corresponding author:** AS Molyakov, Russian State University for the Humanities, Russia

Received: April 04, 2019 **Published:** April 10, 2019

Abstract

The author describes a new multi-tier supercomputer architecture based on non-classical operating principles and implements the MTDF architecture with support for 8 processor control modes for optimizing productivity, security and power consumption.

Keywords: Virtualization; Information Security; Supercomputers; MTDF Architecture; Power Consumption

Introduction

What tasks of information security appear in connection with the advent of supercomputers? The author noticed the following:

a) The priority task is to provide mechanisms for fast backup, "mirroring" of critical processes. Otherwise, a deliberate attack or an unintentional failure will lead to the loss of huge arrays of important data necessary for solving engineering and information and analytical tasks.

b) Significantly increased requirements for the qualifications of users and security administrators. This is due to the fact that the supercomputer is a complex distributed computing system that operates terabytes of data and has specialized software installed on it, which requires additional training. To study the guaranteed security of IC, the probing of supercomputer networks requires the involvement of hacker specialists who have knowledge of more skillful hacks of automated systems than was required earlier for ordinary industrial networks.

c) The tremendous performance of supercomputer complexes makes it very difficult to detect software bookmarks, making their work in the system invisible due to the fact that malicious processes run "on-the-fly" and do not occupy significant OS computing resources, which does not allow detecting the work of third-party software agents based on profiling system load, as in the previous generation of computers.

d) With the advent of graphics cards with a teraflops level of performance (for example, NVIDIA Tesla), embedded network adapters with support for ultrafast transfer of network packets - 10/100/1000 Gigabit / s, there is the possibility of hidden information interception, its decryption and transmission to the attacker, as well as the organization of attacks using hardware and software tabs installed in graphics cards and motherboards, host controllers. Due to the high complexity of the elemental design base (ECB), they are difficult to detect.

In classical processors with the von Neumann architecture, data and program codes are shared, which prevents the effective restriction of one object's access to the address space and data of another. They also do not implement multi-level protection against attacks when performing system calls in the multi-level context of nested guest and control operating systems [1,2]. Tagged architecture on the example of the MCST Elbrus processor provides information security on physical servers. However, the lack of support for hardware virtualization makes such architectural solutions highly specialized and not supporting the emulation of different hardware and widely used hypervisors. In addition, a number of features of hardware virtualization technology accelerates the work of virtual machines and increases the level of security. Among the advantages of virtualization, making it an integral part of any modern computing system, the following should be noted:

a) Two-level virtual memory translation tables make it easier for programmers to work with RAM and help improve application performance.

b) Tagged virtual address translation cache optimizes the process of converting a virtual memory address into a physical one.

c) The hardware protection of the DMA controller provides a high level of security when communicating with peripheral devices.

d) Combine workloads to reduce the amount of hardware and disk space requirements.

e) Increase system flexibility by managing multiple operating systems simultaneously.

f) Run applications on more reliable, energy-efficient equipment.

g) Control of the processor operating modes and reduce the energy consumption of operations at increased loads on the server equipment.

h) Isolation of operating environments for increased security and resiliency.

i) Providing redundancy to increase resiliency and reduce recovery time.

The concept of "fundamentally new architecture" is based on the following principles: the principle of redundant parallelism, the principle of non-uniformity of memory, the principle of optimal planning and asynchrony based on the multigraph request, the decomposition of information processes into an 8-level hierarchical structure, the mechanism of marker scanning and the introduction of interval time limits and energy efficiency of operations when processing requests [3]. The set for reconfiguring the execution environment to meet the requirements of mobility and ensuring the specific performance characteristics of the program includes:

SMW-TEST.CFG FILE

The fault tolerance subsystem is an autonomous functional structure, that is, it operates from a high-speed network and has its own control loop (implemented by a system operator or a service engineer). All parameters for network deployment and configuration are saved in the smw-test.cfg configuration file.

OS Param file

This file contains information about the files that must exist on your system, and their checksums, to check that the files were not damaged during the boot process, the operating system settings - the boot mode, the memory settings at different interface privilege levels, the path to executable OS image (Single Image Distributive). There are 4 sections in the file for configuring modules at IPL_ LEVEL, KERNEL_LEVEL, SUPERVISOR_LEVEL, USER_LEVEL. Levels that correspond to Dom id = 00, Dom_id = 01, Dom_id = 10, Dom_id = 11.

Boot OS image

The server OS is a Unix-like system with XEN or KVM support, VMWare ESXi or Windows Server with Hyper-V support. Under control of the specified hypervisors guest OS of virtual computers of users are started.

Catalog OS-files

This additional directory (the basic distribution with all the folders included in the boot image) contains the most recent patches, the use of which is necessary for updating the OC version. Patches are software updates modules that contain changes that need to be made to the operating system in order to function correctly and resolve previous errors in the program code.

OS-plist file

This is a list of all the files that will be uploaded. It also instructs the ports system to delete certain files during OC reconfiguration. This file is used for logging and security auditing. Vulnerability checks should be performed before installing new modules. Security checks and database updates should be performed during daily system security checks. To this end, all operations for setting up the OS are performed only by the system administrator, and the share and root directories are separated. All operations through the OS installation console are performed using private key (secret keys) using encrypted exchange protocols.

Conclusion

The author made the following series of key architectural and functional improvements in terms of the principles of the computing device, increasing its level of security, reliability and performance based on redundant parallelism, multi-level domain protection, memory heterogeneity:

a) Built-in support for globally addressable memory of 32 Pbytes.

b) Support has been introduced for eight privilege levels, which allows implementing a multi-level ("enhanced") role-based security policy. At the same time, each process can have two statuses - basic (manager) or child (slave); the total of such processes, taking into account 8 levels of the command execution hierarchy, is 16. The number of protection domains is also 16. Thus, there is an explicit link between the launched processes and hardware domains protection.

c) The tagged architecture of a massively multi-thread processor with the support of hardware virtualization technology has been developed.

d) Work is carried out with a virtual single address space of several Petabytes. The transition control is carried out with the help of token commands initialized by the verification module, and not through the use of C / C ++ software indirect references when processing lists of queries, as is done in classic OSs. With this method of operation, there are no restrictions on the size of the transmitted data (for example, in processors of the x86 family, the stack size is 256 bytes, a denial of service occurs when the reserve is exceeded).

e) Built-in support for globally addressable memory of a few dozen Pbytes (32 Pbytes).

f) Support has been introduced for eight privilege levels, which allows for a multi-level ("enhanced") role-based security policy. At the same time, each process can have two statuses - basic or child; the total of such processes, taking into account 8 levels of the command execution hierarchy is 16. The number of protection domains is also 16. Thus, there is an explicit

link between the launched processes and hardware domains protection.

g) The tagged architecture of a massively multi-thread processor with support of hardware virtualization technology has been developed.

h) Developed an innovative way of functioning of the distributed microkernel OS Microtek: it can handle huge streams of information (blocks of PBytes). Moreover, if all the fields of the generative tables are not initialized at the stage of preparing the task (as a result of an attempt to form a request as an incorrect operation, violation of addressing segments, overflow of the processed data buffer, etc.), this request is blocked and not sent for execution hardware device.

i) The processor controls the execution of operations at all levels of the command execution hierarchy: first, the entire set of variable tables is checked for each process launched. If the operation violates the requirements of the PB, then the opcode of the operation is not transferred to the hardware cores of the microprocessor device. In case of identification attempts to form an incorrect request (incorrect data format, buffer overflow, etc.). The request is blocked and not transferred for further processing to the hardware cores of the microprocessor device or peripheral equipment controllers.

j) All requests to hardware devices are presented in the form of requests with an assessment of the permissibility of performing operations in the form of allowed and prohibited values of the function Fi.

k) A mechanism has been developed for managing messages (generation of directives) by assembling commands of an immediate script for executing outgoing directives at the hierarchy level S8.

References

1. Slutskin AI and Eisymont LK (2007) The Russian supercomputer with globally addressable memory. Otkrytye Sist, pp. 42-51.
2. Mitrofanov VV, Eisymont LK (2008) The element base and architecture of high-performance multi-processor computing systems, perspective strategic and embedded supercomputers, In Sb. Dinamika radioelektroniki (Dynamics of Radio electronics), Borisov Yu I (Eds.), Moscow: Tekhnosfera, (2nd edn), p. 70-76.
3. Zhirnov V (2003) Limits to binary logic switch scaling - A Gedanken Model- Proceedings of the IEEE 91(11): 1934 -1939.

DOI: 10.32474/CTCSA.2019.01.000112