SAFETY POLICY PROBLEMS OF CLUSTER SUPERCOMPUTERS

Andrey Golovinskiy, Sergey Ryabchun, Anatoliy Yakuba

***Abstract**: The paper describes the problems of safe management and safe work of the supercomputer protected both from purposeful attacks from the outside, and from results of wrong activity of its usual users. The paper may be useful for those scientists and engineers that are practically engaged in a cluster supercomputer systems design, integration and services.*

***Keywords**: supercomputer, cluster, computer system security policy, virtualization.*

***ACM Classification Keywords**: C.1.4 Parallel Architectures. C.2.4 Distributed systems, D.4.7 Organization and Design*

Introduction

The powerful computer center is a titbit for the malefactor. The information about tens users (scientists, programmers) is usually stored into system databases, giving links to their personal computers with the valuable scientific and technical information or the developed software. The disk files of a supercomputer are stored the confidential system data, many personal programs of users. Original development of supercomputer founders also can be the object of interest.

Besides the supercomputer equipped with the broadband Internet channel, can be convenient jumping-off place for carrying out of attacks to other servers of a local network and the internet.

The basic threats to computing system (CS). We shall allocate three basic threats CS:

- Threat of disclosing, consists that the information which did not intend for a wide circulation, becomes known to a uncertain circle of persons. It is most known of threats.
- Threat of integrity, consists that as a result of some activity of users (they are not necessary malefactors) the stored information can be deformed, for example, in the environment of data transmission or in a place of its storage.
- Threat of refusal of services. This threat consists that the malefactor certain actions can cause faults in work of some system services.

The organization of supercomputer safety

The non-authorized access from which it is necessary to protect CS, it is possible to divide into two unequal parts.

- Any non-authorized access from the outside,
- Non-authorized access of the authorized supercomputer user.

The common sense prompts, that with a view of safety with an external world it is necessary to limit interaction by an entrance gateway of a supercomputer, with a minimum of the interface of interaction, for example protocols ***ssh***, ***https*** (the protocol ***http*** is possible as a variant of access to the general information only in a read-only mode). Besides external access to some technical services, to services ***DNS, NTP*** should be open. Ports of other services should be filtered.

Open services ***ssh, https, DNS*** can be exposed to external attacks, measures on reflection of such possible attacks therefore should be undertaken.

For the analysis vulnerable points inside supercomputer we shall divide into such groups:

1. The active technical equipment - managed switches, devices of an uninterrupted supply (UPS), devices of the removed management of servers (through controllers with realization of protocol IPMI) - usually is in service nets. These nets should be accessible only to system administrators.

Possible variant of the decision is as follows: allocation of such equipment in a separate virtual net in which there is an access only from a gateway, access to which, in turn, is adjusted by the net screen (Firewall)

2. Service of identification of users LDAP should have the reliable password, this password is accessible in some system scripts.

3. Scripts of administration managerial control.

4. A system of supercomputer resources handling. Its own means of protection should be involved in it.

5. Linux kernel.

6. Open ports of global file system Lustre [1].

7. Interconnect with MPI-protocol at cluster nodes.

All these create big amount of problems concerned to supercomputer safety. In everyone concrete supercomputer there is a specificity, but the common feature is potentially a plenty of gaps in protection and complexities of their overcoming.

Protection of workplaces of system administrators

Working computers of system administrators - a special class a supercomputer component, special in many senses. First, by initial development of structure of a supercomputer these computers frequently appear outside of a field of vision and have no enough the thought over protection. Second, they can keep strictly confidential data about management of the supercomputer – tuning, internal reports on safety, working notes, backup copies of software, etc. Already only this transfer demands, that to a safety of workplaces of administrators has been paid not smaller attention, than to safety of the open services.

The natural decision - to have workplaces of system administrators into physically allocated subnet with two points of interaction, one of them is an entrance supercomputer gateway, and the second - a gateway delivering the internet in the corporate local computer net. Thus in a gateway it is not necessary to create a separate operating mode of administrative computers, they should work with the rights of any external computer from the internet. Besides access from within supercomputer in the administrator subnet should be allowed only to system administrators. As if to access from the outside in this net it should be completely closed for all.

One of possible options to decide a problem of storage of working files is the organization of the X-net of terminals for work of administrators. With such an option all working materials will lay on one terminal - server on which it is easier to provide their reliable and safe storage.

Internal supercomputer nets

The organization of a net. Actually, protection of a gateway though is necessary, but rather conditional. At enough big base of users, a part from them it is necessary, even once, will begin a session of connection with supercomputer through a computer which is infected either virus, or the Trojan program which collect passwords and send them in hypothetical outside database. Therefore it is enough to malefactor to address to such database to receive the information for an input inside of a supercomputer. Therefore protection of a supercomputer is necessary for projecting in view of that a quantity of malefactors can penetrate into.

System of storage of backup copies. In the chosen model of safety the unique variant of correction of consequences of breaking is full reinstallation of operational systems on all servers of a supercomputer. It is labour-consuming procedure and it is practically equivalent to construction of a supercomputer from nothing.

To minimize consequences, it is expedient to allocate a separate server on which backup copies of all supercomputer systems will be stored. To secure this server against breaking, it is necessary to close any input to it from the net, to leave only an input from the console. Such storehouse is useful and at various failures.

Construction of protection for service of Grid-calculations. Specificity of Grid tasks is that the executed code and the data can come from any point of the world and from the unknown user. Therefore it is necessary to provide performance of such problem in the allocated container, without interaction with other components of a complex. In this case the container is set of the units allocated for the decision of one task.

As the common requirements it is possible to result the following in the container:

1. The condition of the container after performance of a task should correspond precisely to a condition up to it.
2. Breaking unit should not entail consequences for supercomputer.
3. Interaction of the user and its task with supercomputer is limited to units of the container and a gateway.

The first requirement is rather easy for resolving, if root file system to give accessible only for reading and to overload unit on the termination of a task with the subsequent deleting contents of a local disk.

The second requirement to provide much more difficultly. At the superuser on unit it is a lot of opportunities, access to base of users, wide access in the general file system, etc.

The third requirement is rather easily feasible, for example, with the help of functionality of virtual nets (VLAN) on managed switches.

The basic minus of the tendency of closing *of all* holes and passes in system is excessive complication of system, it inevitably entails occurrence of new gaps in protection. Technology which presumes to execute all these requirements with comprehensible productivity and with rather small complication of system, is ***virtualization***.

Virtual supercomputer

Supercomputer can be subjected to attack outside, but not less threats attack from within represents. Very much frequently on computing supercomputer programs are started, to check up which on safety it is not obviously possible. These programs are created literally on the move, compiled and sent in turn on performance. To make audit of a code of such programs it is unreal - the amount of these programs, their often updating and round-the-clock work supercomputer will make such attempt impossible. Therefore always there is a danger, that any of the started programs will contain a nocuous code.

Danger especially grows if to take into account, that to the author of a code "subtleties" of the environment of execution can be known. The environment of execution is here enough static, that is, as a rule, the used equipment imposes restriction on the system software that entails rare enough updating and, accordingly, means presence of some number enough for a long time found out and already corrected gaps in protection of which the malefactor can always take advantage for reception of the partial or full control over resources. Thus the purposes of attack can be anyone - access to the confidential data, infringement of integrity of the data, refusal in service, attack on external in relation to supercomputer objects and so on.

Clearly, that one of the purposes of construction of a policy of supercomputer safety should be protection of the supercomputer against such attacks, that is, from attacks from within. Complicates the decision of a task in view necessity to take into account a lot of additional conditions:

- For a parallel task the allocated resources are uniform object and toughening of protection of each separate node can lead to failure of any task;
- The supercomputer is the multiuser and multitask system.

Function chroot as a variant of the decision of a problem. Function ***chroot*** allows system to start process, using the certain catalogue as root. Thus it is possible to limit access to strictly certain data for process. And not only to limit, process can receive completely other environment of execution, for example, 32-bit ALTLinux [2] environment that root system is 64-bit CentOS [3] environment.

Very attractively, but, unfortunately, it works for a single computer. For supercomputer the application of the operator ***chroot*** only will complicate a problem to the malefactor, but full problem solving in a supercomputer cannot be reached.

The reason consists that the computing node is not an independent element - it is closely connected to other nodes which are included in a resource of a task, and also through a management system with all other supercomputer nodes. Thus. It is possible both net attack, and attempt to receive the full control over any node through a probable gap in a kernel.

Clearly, that use of functionality ***chroot*** for the decision of specific problems is allowable, and use as means of protection not only will not give necessary effect, but even harmful, as can give the manager of a supercomputer feeling of false security.

Nevertheless, the problem of creation of system of safety is, it is real also it is necessary to solve. By what means? From our point of view protection of separate elements of an infrastructure cannot be optimum, always there will be a unprotected element through which attack is possible. The most optimum is allocation for a problem of the user virtual supercomputer inside which the user is the full owner with some restrictions, namely, with the minimal administrative opportunities.

Thus, the supercomputer turns to a set from one or more virtual supercomputers with one problem and one user in everyone, and process of start of a problem of turn becomes complicated item of creation virtual supercomputer. Itself virtual supercomputer it will be submitted as a set of virtual computing nodes.

Requirements to such virtual supercomputer are simple enough - *the allocated net address space* and *the allocated file system*.

Let's try to formulate requirements to system virtualization which we shall use on computing nodes.

High efficiency. Computing supercomputer, real or virtual, has the main function - quickly to count, therefore an obligatory overhead charge on virtualization should be minimal, in an ideal case this charge should aspire to zero.

Opportunity of direct use of the allocated equipment. As the computing environment in supercomputer are frequently used the various high-efficiency communication equipment, for example, in the SCIT - 1 and the SCIT - 3 supercomputers it is InfiniBand, and in SCIT - 2 SCI [4] and if the virtual node will not have to it direct access falling of productivity of all virtual supercomputer will be rather essential enough.

Virtualization types. *Emulation of the equipment* - in host-system is created the virtual machine modelling some hardware platform (fig. 1). As each command of the processor should be simulated on a real platform productivity can fall in tens and even hundreds times.

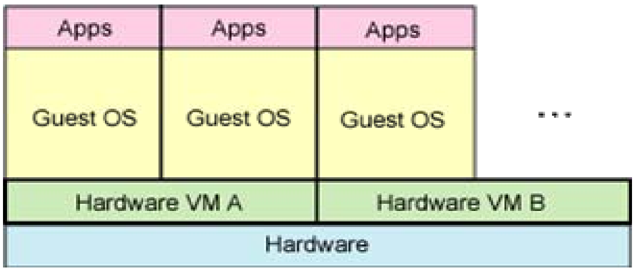

Fig. 1. Emulation of the equipment

Full virtualization - uses a program layer between guest operating systems and the equipment, *hypervisor* (fig. 2). Losses of productivity low and it can be started the unmodified guest systems, but also there is very short list of really supported equipment.

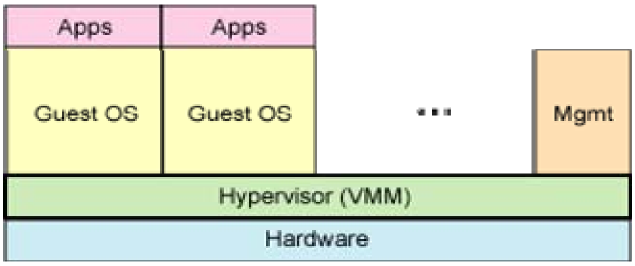

Fig. 2. Full *virtualization*

Paravirtualization - this method is similar with full *virtualization*, difference that hypervisor belongs to kernel host-systems (fig. 3). This method gives the productivity close to unvirtualized system, use of the modified guest systems however demands.

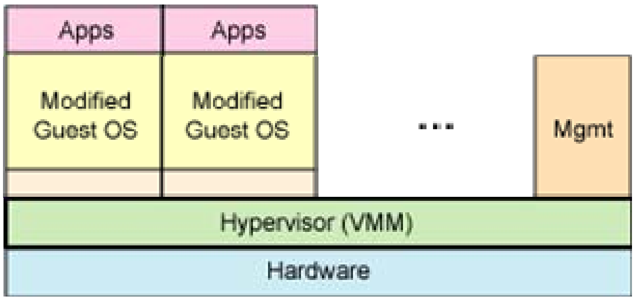

Fig. 3. Paravirtualization

A level of operating system virtualization - actually it is simple isolation of the containers, allowing to receive the productivity practically equal to initial productivity (fig. 4).

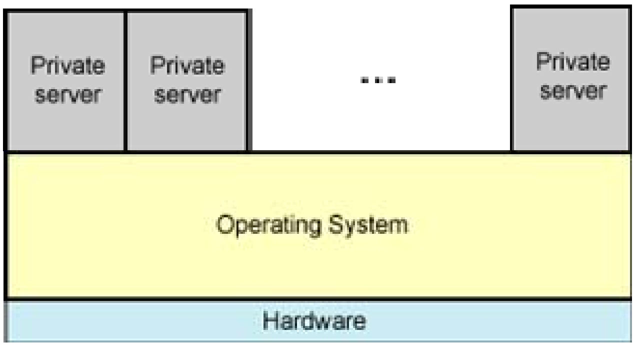

Fig. 4. A level of OS virtualization

The systems realizing p*aravirtualization* and a level of operating system *virtualization* concern to examined real candidates. However, it is necessary to refuse from paravirtualization too, as use in supercomputers enough the rare equipment generates absence of support of this equipment by the hypervisor.

Thus, only a level of operating system *virtualization is* suitable to our conditions. Though the operator ***chroot*** on the functionality to this type *virtualization* also concerns, but, unfortunately, it can *virtualize* only file system, it is required to us much more.

Examples of systems virtualization

OpenVZ - realization of technology of a virtual level of operating system on Linux kernel. OpenVZ allows to start on one physical device some the isolated environments named VPS (Virtual Private Server) or VE (Virtual Environments) [5].

OpenVZ gives excellent productivity - falling does not exceed 1-2 % on modern systems, scalability - on one physical device can be started some hundreds virtual environments, dynamic resource management is realized, administration differs simplicity. OpenVZ also supports migration of virtual environments that allows to transfer hurriedly practically the virtual environment from one physical server on another, and accordingly, allows to build various scripts of use (unfortunately, this opportunity in кластерном a supercomputer environment can be used with big enough clauses as restriction is imposed with drivers of used interconnect).

Linux-VServer - realization of technology of *virtualization* a level of operating system [6]. As well as OpenVZ, allows to start on one physical server a little isolated VPS. But as against OpenVZ, uses the concept of the expanded functionality ***chroot*** with expansion on isolation of the processor, memory and net resources. Does not support migration and has more simple net support that entails additional complexities in administration.

Clearly, that utilization of this method will not give full safety also, a gap is the opportunity of use for attack of the computer net. Nevertheless, this method gives high enough level of security.

Conclusion

In the near future we are going to carry out experiments on creation virtual supercomputers with application Linux-VServer and OpenVZ, and, in case of successful result, we shall introduce one of them in the standard circuit of use.

Further we plan to finish working versions MPI for exception of use of direct access of process to low level interfaces of the computer net. In case of the successful decision of this problem we can receive completely safe virtual supercomputer.

Bibliography

[1] http://clusterfs.com/

[2] http://altlinux.org/

[3] http://centos.org/

[4] A.Golovinskiy. S.Ryabchun, A.Yakuba. Cluster supercomputer architecture. In: Proceedings of the XII-th Int.Conf. “Knowledge-Dialogue-Solution”- Varna, 2006.

[5] Linux. An overview of virtualization methods, architectures, and implementations. http://www-128.ibm.com/developerworks/linux/library/l-linuxvirt

[6] Linux V-Server Overview. http://linux-vserver.org/Overview

Authors' Information

Andrey L. Golovinskiy - Institute of Cybernetics NAS Ukraine; Prospekt Academika Glushkova, 40, Kiev, 03680 MCP, Ukraine; email: tikus@ukr.net

Sergey G. Ryabchun - Institute of Cybernetics NAS Ukraine; Prospekt Academika Glushkova, 40, Kiev, 03680 MCP, Ukraine; email: serge.ryabchun@gmail.com

Anatoliy A. Yakuba - Institute of Cybernetics NAS Ukraine; Prospekt Academika Glushkova, 40, Kiev, 03680 MCP, Ukraine; email: ayacuba@gmail.com