УДК 004.056 DOI: 10.22184/NanoRus.2019.12.89.556.559

МОДУЛЬ ДИСТАНЦИОННОГО МОНИТОРИНГА И УПРАВЛЕНИЯ ДЛЯ СЕРВЕРОВ «ЭЛЬБРУС»

REMOTE MONITORING AND CONTROL MODULE FOR ELBRUS SERVERS

ДУДАРЕВ ДМИТРИЙ АЛЕКСАНДРОВИЧ

ПАНАСЕНКО СЕРГЕЙ ПЕТРОВИЧ
sp@ancud.ru

ООО Фирма «АНКАД»
124527, г. Москва, г. Зеленоград, Солнечная аллея, 8

DUDAREV DMITRY A.

PANASENKO SERGEY P.
sp@ancud.ru

Firm "ANCUD" Ltd.
8 Solnechnaya Alley, Zelenograd, Moscow, 124527

В докладе описана система дистанционного мониторинга и управления для серверов «Эльбрус», основанная на применении аппаратного модуля, сочетающего в себе как функции по дистанционному мониторингу и управлению средствами вычислительной техники, так и возможности по обеспечению надлежащего качества защиты от несанкционированного подключения к серверу.

Ключевые слова: удаленное управление; мониторинг; контроль доступа; аутентификация; АПМДЗ.

The paper describes a system of remote monitoring and control for Elbrus servers. The system is based on a hardware module that combines both functions of remote monitoring and management of computers, and the ability to provide high levels of protection against unauthorized connection to the servers.

Keywords: remote control, monitoring, access restriction, authentication, trusted boot modules.

Проблема дистанционного управления и мониторинга серверов распределенных компьютерных систем традиционно решается за счет использования реализаций известной спецификации IPMI (Intelligent Platform Management Interface — интеллектуальный интерфейс управления платформой). Данная спецификация была разработана в 1998 г. корпорацией Intel и используется многими ведущими производителями вычислительной техники [1].

Спецификация IPMI основана на использовании аппаратной составляющей, которой обычно является контроллер управления материнской платой BMC (Baseboard Management Controller) — размещаемый на материнской плате автономный контроллер, работающий независимо от центрального процессора, базовой системы ввода-вывода (BIOS — Basic Input/Output System) и операционной системы (ОС) компьютера. Контроллер BMC имеет собственный процессор, память и сетевой интерфейс и обеспечивает управление серверной платформой даже в тех случаях, когда сервер выключен (при наличии подключения к источнику питания).

Интерфейс IPMI, с одной стороны, дает масштабные возможности по управлению сервером, а с другой стороны, он использует слабую однофакторную аутентификацию по паролю. Поэтому можно утверждать, что данный интерфейс представляет потенциальную опасность атак на сервер (в т. ч. выключенный) через Интернет, увеличивая вероятность несанкционированного доступа к его ресурсам. Получение доступа может дать злоумышленнику практически неограниченные возможности по несанкционированному воздействию на атакуемый сервер в случае получения контроля над IPMI (см., например, [2–4]).

В работе [5] была предложена глубокая модификация аппаратно-программного модуля доверенной загрузки (АПМДЗ) семейства «КРИПТОН-ЗАМОК» [6] в целях внедрения в АПМДЗ дополнительных аппаратных компонентов и программных модулей, обеспечивающих выполнение функций удаленного управления серверами. Данная модификация позволила бы обеспечить безопасное выполнение функций по удаленному управлению, свойственных контроллеру BMC.

Как было показано в [5], возможно и перспективно создание АПМДЗ, сочетающего в себе функции, присущие аппаратно-программным модулям доверенной загрузки (защита от несанкционированного доступа, строгая аутентификация пользователей, контроль целостности программных модулей и формирование доверенной операционной среды), и функции по удаленному управлению серверами по защищенному каналу связи между управляемым сервером и автоматизированным рабочим местом (АРМ) администратора.

При этом имеет право на существование и альтернативный вариант достижения подобного функционала — путем совместного использования двух устройств:

- аппаратно-программного модуля доверенной загрузки;
- модуля дистанционного мониторинга и управления серверами (ДМУ).

В качестве АПМДЗ может быть использовано классическое серийное устройство. А доверенный модуль ДМУ не только выполняет функции, присущие контроллеру BMC, но и обеспечивает защиту данных, передаваемых в канале управления и мониторинга.

Схема системы с использованием модуля ДМУ показана на рис. 1.

Основными компонентами данной системы являются:

- сервер с установленным на него АПМДЗ и модулем ДМУ, а также программным обеспечением первоначальной настройки и инициализации модуля ДМУ;
- АРМ централизованного управления сервером с соответствующим программным обеспечением.

Использование АПМДЗ является опциональным: данный модуль требуется только в случае наличия требований по обеспечению доверенной загрузки защищаемого сервера. Тогда как

ДМУ обеспечивает выполнение следующих групп функций:

1. Функции дистанционного управления и мониторинга сервера, в т. ч.:
- чтение показаний датчиков сервера;
- дистанционное включение, выключение и перезагрузка сервера;
- обновление программы начального старта сервера;
- ведение журнала событий;
- проброс последовательного интерфейса serial-over-LAN.

2. Функции обеспечения безопасности дистанционного мониторинга и управления:
- аутентификация пользователей;
- шифрование и имитозащита данных, передаваемых в канале мониторинга и управления между управляемым сервером и АРМ администратора.

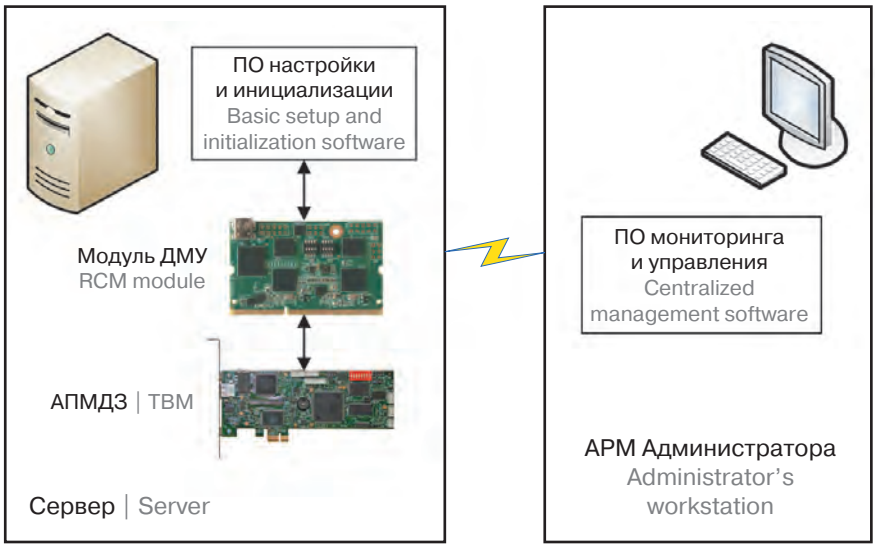

Рис. 1. Схема системы дистанционного мониторинга и управления сервером
Fig. 1. The structure of the server remote management system with the RCM module

Вторая группа функций выполняется ДМУ в тесном взаимодействии с АПМДЗ, если таковой установлен, или автономно при отсутствии АПМДЗ. В случае совместного применения АПМДЗ и ДМУ данные устройства работают согласно концепции использования АПМДЗ «КРИПТОН-ЗАМОК» в качестве основного модуля обеспечения информационной безопасности средства вычислительной техники (СВТ), в которой АПМДЗ осуществляет централизованное управление остальными модулями защиты, установленными в СВТ. Данная концепция описана, в частности, в [7].

Настройка модуля ДМУ, а также загрузка в него ключей аутентификации выполняются программой первоначальной настройки и инициализации, работающей в операционной среде управляемого сервера.

В рамках ряда работ, проводимых ООО Фирма «АНКАД» совместно с ПАО «ИНЭУМ им. И. С. Брука», разработаны компоненты описанной системы дистанционного управления и мониторинга для серверов «Эльбрус», включая следующие:
- модуль ДМУ;
- программное обеспечение первоначальной настройки и инициализации;
- программное обеспечение АРМ централизованного управления серверами.

Внешний вид разработанного модуля ДМУ представлен на рис. 2. Данный модуль выполнен в форм-факторе 204-pin SO-DIMM и имеет следующие ключевые особенности:

The problem of remote control and monitoring of servers in distributed computer systems is traditionally solved by using various implementations of the well-known IPMI (Intelligent Platform Management Interface) specification. This specification was developed in 1998 by Intel Corporation and now it is used by many leading manufacturers of computer equipment [1].

The IPMI specification is based on using a specific hardware component — baseboard management controller (BMC). It is usually a standalone controller located on the motherboard that operates independently of the CPU, the basic input/output system (BIOS) and the operating system of the computer. BMC usually has its own processor, memory and network interface and provides control of the server platform even when the server is turned off (just connected to a power source).

On the one hand, IPMI gives large-scale possibilities for server management, and on the other hand, it uses weak one-factor authentication by password. Therefore, it can be argued that this interface is a cause of a potential danger of attacks on the server (including powered off) via the Internet. This can increase the probability of unauthorized access to the server resources. Gaining access can give an attacker almost unlimited opportunities for unauthorized impact on the attacked server in case of taking control over IPMI (see, for example, [2–4]).

It was proposed to use the deep modification of the known model of Crypton-Zamok hardware trusted boot module (TBM) [5] based on implementing into TBM additional hardware components and software modules that provide servers remote management functions (see [6]). This modification would allow providing secure performance of remote control functions peculiar to the BMC controller.

As it was shown in [6], it is possible and promising to create a device that combines the functions inherent to a TBM (protection against unauthorized access, strict user authentication, integrity check of software modules and creation of a trusted operating environment), and servers remote management functions performed via a secure communication channel between the managed server and the administrator's workstation.

At the same time, the same functionality can be achieved alternatively — by simultaneous use of the following two devices:
- a trusted boot module;
- and a specific module for server remote control and monitoring (RCM module).

In such a case any known TBM can be used as a first hardware module. Herewith an RCM module not just performs the functions inherent to the BMC, but also provides protection of data transmitted in the control and monitoring channel — between the server and the administrator's workstation.

The scheme of the distributed system using the RCM module is shown on Fig. 1.

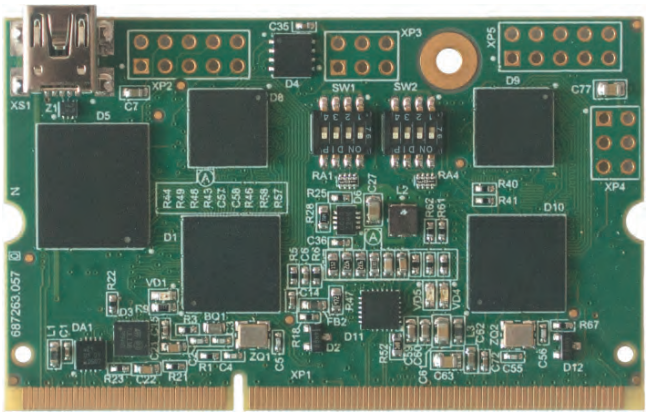

Рис. 2. Модуль ДМУ
Fig. 2. The RCM module

- модуль имеет собственную сетевую карту, работающую даже при выключенном сервере (при наличии дежурного питания);
- ДМУ оснащен двумя микроконтроллерами (один из них в основном работает с сетью, другой — с сервером), что позволяет обеспечить безопасность при взаимодействии с АПМДЗ и работе через сеть;
- для взаимодействия с АПМДЗ в данных устройствах организован выделенный канал, также способный работать при выключенном сервере;
- модуль также оснащен часами реального времени с батарейным питанием для меток времени в журнале операций.

Разработанное программное обеспечение (ПО) функционирует в ОС «Эльбрус». При этом ПО АРМ централизованного управления серверами позволяет осуществлять мониторинг и управление до 1000 серверов «Эльбрус» с одного АРМ.

Представленный модуль ДМУ позволяет обеспечить достаточный функционал по удаленному управлению серверами «Эльбрус» и их мониторингу. При этом модуль является доверенным и обеспечивает высокое качество защиты от несанкционированного использования канала дистанционного управления и мониторинга.

ЛИТЕРАТУРА

1. IPMI — Intelligent Platform Management Interface Specification Second Generation v2.0. — Document Revision 1.1, October 1, 2013. — Intel, Hewlett-Packard, NEC, Dell.
2. Schneier B. *The Eavesdropping System in Your Computer* // https://www.schneier.com — 2013.
3. Farmer D. *IPMI: Freight train to hell or Linda Wu & The night of the leeches* // http://fish2.com — Version 2.0.3 — August 22nd, 2013.
4. Farmer D. *Sold Down the River* // http://fish2.com — June 23rd, 2014.
5. Романец Ю. В., Дударев Д. А., Панасенко С. П. Модуль доверенной загрузки с возможностью удаленного управления серверами // Международный форум «Микроэлектроника-2017». 3-я Международная научная конференция «Электронная компонентная база и электронные модули». — Республика Крым, г. Алушта, 2–7 октября 2017 г.
6. АПМДЗ «КРИПТОН-ЗАМОК» // http://www.ancud.ru — ООО Фирма «АНКАД».
7. Двинских А. АПМДЗ «КРИПТОН-ЗАМОК» как системообразующий модуль // http://www.ancud.ru — ООО Фирма «АНКАД».

The main components of this system are:

- the server equipped with TBM and RCM modules with the software that performs the basic setup and initialization of the RCM module;
- the administrator's workstation equipped with the software for performing the centralized management operations.

TBM use is optional, because this module is needed only in case of requirements to provide the secure boot of the server.

The RCM module provides the support for the following groups of functions:

1. Remote control and monitoring functions, including:

- getting the current status of the server's sensors;
- remote power on, shutdown and restart of the server;
- updating the initial boot software of the server;
- event logging;
- serial-over-LAN interface forwarding.

2. Functions that provide the security for remote control and monitoring:

- user authentication;
- encryption and integrity control of data transmitted in the control and monitoring channel between the server and the administrator's workstation.

The second group of functions is performed by the RCM module in close cooperation with the TBM, if the latter is installed on the server. Otherwise, these functions are performed by the RCM module autonomously.

In the case of a joint use of TBM and RCM these devices work according to the concept of using Crypton-Zamok TBM as the main module of the complex providing the information security for the server. Such concept assumes that TBM performs the centralized management of other protection modules that are installed on the secured computer. This concept is described, in particular, in [7].

The basic setup and initialization software perform the configuration settings of the RCM module as well as the loading authentication keys into it. This software is running in the operating system of the managed server.

Components of the described remote control and monitoring system for Elbrus servers have been developed in several R&D works performed by "ANCUD" Company together with "Brook INEUM" PJSC. The developed components include the following:

- the RCM module;
- the basic setup and initialization software;
- the software for performing the centralized management operations on the administrator's workstation.

The developed RCM module is shown in Fig. 2. This module is made in accordance with the 204-pin SO-DIMM form factor. It has the following main features:

- the module has its own network adapter that works even when the server is powered off (in the presence of standby power supply);
- the module is equipped with two microcontrollers (one of them mainly works with the network connection, and the other one — with the managed server) that allows ensuring the security when interacting in distributed systems in the shown configuration;

- the dedicated channel is organized in the TBM and RCM modules to communicate between them; this channel is also able to work when the server is powered off;
- the module is also equipped with a battery-powered real-time clock for timestamps in the operation log.

The developed software runs in Elbrus operating system. The current version of the software for the administrator's workstation allows monitoring and controling up to 1000 Elbrus servers from one workstation.

The presented RCM module allows providing sufficient functionality for remote management and monitoring of Elbrus servers. The module also provides the high quality protection against unauthorized access and use of the remote control and monitoring channel.

REFERENCES

1. IPMI — Intelligent Platform Management Interface Specification Second Generation v2.0. — Document Revision 1.1, October 1, 2013. — Intel, Hewlett-Packard, NEC, Dell.
2. Schneier B. *The Eavesdropping System in Your Computer* // https://www.schneier.com — 2013.
3. Farmer D. *IPMI: Freight train to hell or Linda Wu & The night of the leeches* // http://fish2.com — Version 2.0.3 — August 22nd, 2013.
4. Farmer D. *Sold Down the River* // http://fish2.com — June 23rd, 2014.
5. Romanets Yu. V., Dudarev D. A., Panasenko S. P. *Modul' doverennoi zagruzki s vozmozhnost'yu udalennogo upravleniya serverami* // Mezhdunarodnyi forum «Mikroelektronika-2017». 3-ya Mezhdunarodnaya nauchnaya konferentsiya «Elektronnaya komponentnaya baza i elektronnye moduli». — Respublika Krym, g. Alushta, 2–7 oktyabrya 2017. (In Russian).
6. APMDZ «KRIPTON-ZAMOK» // http://www.ancud.ru — OOO Firma «ANKAD».
7. Dvinskikh A. APMDZ «KRIPTON-ZAMOK» kak sistemoobrazuyushchii modul' // http://www.ancud.ru — OOO Firma «ANKAD». (In Russian).