ISSN 2079-3316 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ №1(24), 2015, с. 61–71

УДК 004.75

В. И. Воробьев, С. Р. Рыжков, Р. Р. Фаткиева

Защита периметра облачных вычислений

Аннотация. Представлена абстрактная концепция опечатывания облачных данных с помощью определяемых политик. Описано использование криптомодулей TPM в создании доверенных серверных платформ внутри облака. Представлена обобщенная схема геотегирования.

Ключевые слова и фразы: облака, облачные вычисления, периметр безопасности, геотегирование.

Введение

В свете увеличивающегося значения геополитики в глобальной сети Интернет появляются востребованные инструменты контроля перемещения данных, которые используют в информационном пространстве понятия «геолокация», «геоограждение» и позволяют осуществлять мониторинг и контроль территориального распределения обработки данных. Технологии геолокации преобразуют физическое пространство в более доступную для различных трансформаций среду (вычислено, измерено, проверено). Это же утверждение актуально и для цифровой среды, цифрового сообщества, организованного в облачных вычислениях.

Для обеспечения основных принципов сохранения данные в облачной среде дублируются в геораспределенной структуре ЦОДов, этот подход позволяет полностью защитить их от возможных технических повреждений, но не всегда решает проблему обеспечения конфиденциальности хранимых данных. Безопасность достигается за счет разделения данных на массивы, находящиеся в географически распределенных физических хранилищах, при этом решается и проблема обеспечения целостности, поскольку кража информации из одного из «хранилищ» лишена смысла — данные естественным

образом защищены. В качестве примера можно привести распределенное облачное хранение, которое обеспечивает целостность данных в облаке благодаря технологии Distributed Storage («распределенное хранилище») [1].

Технология обеспечивает доступность данных и позволяет сократить расходы на хранение благодаря высокой степени фрагментации (в известном только провайдеру порядке) множества географически распределенных репликаций, а также благодаря использованию особого метода кодирования в момент записи, что позволяет гарантированно восстановить данные при аппаратном сбое. Логика хранения реализуется шлюзами, осуществляющими фрагментацию, распределение по удаленным серверам хранения и выполнение обратной операции сборки данных в единое целое из фрагментов с коррекцией в случае обнаружения ошибок. К сожалению, данный подход ставит клиента в полную зависимость от провайдера, т.к. не позволяет пользователю гарантированно контролировать жизненный цикл данных.

Гибкость и масштабируемость, с которой виртуальные машины могут быть перенесены из одной страны в другую, вызывает опасения и необходимость создания механизмов для отслеживания и борьбы с этими передвижениями. Проблема усугубляется и тем, что каждая страна имеет собственную законодательную базу, защищающую безопасность данных на территории государства, которая не охватывает миграцию данных и приложений при использовании облачных вычислений в географически распределенных облачных хранилищах. В связи с этим возникает необходимость разработки инструментов по контролю трансграничного взаимодействия [2].

1. Повышение безопасности облачных данных с использованием технологии геотегирования

Определение физического местоположения объекта возможно как путем описания географической информации (название страны или города), так и применением технологии GPS (Global Positioning System — система глобального позиционирования) на основе широты и долготы. Географическое положение может быть описано разными способами и с разной степенью точности, однако традиционные методы геолокации не удовлетворяют требованиям безопасности облачных вычислений как вследствие низкого уровня доверия и недостаточно точных описаний местоположения субъекта геотегирования, так и проблем доверия аппаратного уровня [3]. Поэтому

Таблица 1. Создание защищенного вычислительного пула

Этап	Задачи
1. Аттестация платформы и запуск сервера	1.1. Настройка конфигурации 1.2. Верификация гипервизора 1.3. Мониторинг гипервизора
2. Развертывание задач	2.1. Развертывание задач на доверенную платформу 2.2. Миграция данных
3. Миграция с сопоставимым уровнем	3.1. Подтверждение полномочий при изменении точки доступа доверия 3.2. Запуск мониторинга

Национальный Институт стандартов и технологий (США) в своём межведомственном отчёте NISTIR (National Institute of Standards and Technology Interagency Report) 7904 описывает геолокацию следующим образом: *«Географическое положение позволяет идентифицировать приблизительное местоположение облачного хранилища, добавляя эту информацию в корень доверия сервера. Аппаратный корень доверия создается организацией с уникальным идентификатором хоста и метаданными платформы, хранится в антивандальном оборудовании. Эта информация доступна с помощью защищенных протоколов, чтобы можно было быть уверенным в целостности платформы и подтвердить местоположение хоста»* [2].

Исходя из отчета «геотегирование» представляет собой процесс определения, создания и инициализации набора объектов геолокации вычислительного устройства. Актуальным применением гео-тега является обеспечение соблюдения пограничного контроля на основе гео-тегов в концепции, называемой «гео-заслон». Концепция геозаслона успешно применяется в мобильных компьютерах, в управлении цепочками поставок, транспортной логистике. Приложения, поддерживающие гео-заслон, позволяют администратору устанавливать правила и применять их в автоматизированном режиме при изменении границ нахождения устройств, а также в отношении задач или областей данных с выдачей соответствующих предупреждений для дальнейшего расследования [2].

1.1. Создание доверенного пула с геолокацией в облаке

Создание доверенного пула с геолокацией в облаке включает в себя три основных этапа (таблица 1). На первом этапе производится настройка оборудования, BIOS и гипервизора, проверяется достоверность серверной платформы. Выполнение постоянного контроля гипервизором обеспечивает достоверность аттестации. Аттестация платформы и запуск безопасного гипервизора являются основой надежности платформы, и благодаря постоянному мониторингу предоставляют более высокую скорость обнаружения проблем безопасности.

1.2. Развертывание задач

Производится развертывание задач с последующим переносом данных на доверенные серверные платформы внутри облака. Доверенная платформа, т.е. платформа, которой можно доверять (возможное действие гарантированно совпадает с эталонным), основана на абстракции «Корень Доверия» (Root of Trust) — определенных компонентах, чья безопасность гарантирована. Полный перечень корней доверия обладает ограниченным набором возможностей, достаточным для перечисления компонентов платформы. Существует три корня доверия:

RTM (*корень доверия для измерений*) — вычислительный механизм, производящий измерения целостности платформы.

RTS (*корень доверия для хранения*) — вычислительный механизм, способный хранить хэши значений целостности.

RTR (*корень доверия для сообщений*) — механизм, который сообщает о хранимой в RTS информации.

Данные измерений описывают свойства и характеристики измеряемых компонентов. Хэш-функции этих измерений представляют собой «снимок» состояния компьютера. Их хранение осуществляется функциональностью RTS и RTR [4]. Только при сверке хэш-функции полученных измерений с надёжно хранимыми эталонными измерениями платформы, находившейся в состояния доверия, можно говорить о целостности системы. Для перехода к третьему этапу необходимо убедиться, что потоки информации осуществляются только среди хостов с сопоставимым уровнем доверия. Миграция допускается только если оба сервера проходят проверку.

1.3. Механизмы развертывания гео-заслона

Через механизм аттестационного протокола геотегированная информация (сформированная на этапе конфигурации сервера) сохраняется в виде зашифрованного хешзначения в аппаратном криптографическом модуле BIOS (TPM – Trusted Platform Module). Для обеспечения ограничений геолокации перед развертыванием и миграцией рабочей нагрузки запускается мониторинг геолокации [2]. TPM в защите периметра выполняет следующие функции:

(1) подтверждение данных геолокации,
(2) применение ограничений геолокации,
(3) запуск мониторинга геолокации.

Он специфически служит для гарантированного доверенного хранения, мониторинга и аудита за счет использования содержащегося в аппаратной части криптопроцессора, обеспечивающего средства безопасного создания ключей шифрования (с той же степенью неповторимости, что и генератор случайных чисел), а также средства ограничения использование ключей (как для подписи, так и для шифрования/дешифрования) [5]. Модуль TPM также используется для подтверждения подлинности аппаратных средств за счет уникальности специфических устройств, что делает возможным однозначное установление подлинности доверенной платформы [6, 7].

2. Преодоление ограничений современных криптомодулей TPM

Современные криптомодули TPM плохо приспособлены к требованиям облачных сервисов по следующим основным причинам:

(1) Изначально криптомодули TPM были предназначены для защиты данных на автономном компьютере, что неудобно при использовании в многоузловых центрах обработки данных, в среде, где данные мигрируют по нескольким узлам с потенциально различными конфигурациями.
(2) Криптомодули TPM не обеспечивают высокую производительность, так как выполняют только одну команду за раз, что затрудняет масштабируемость облачных сервисов, которые используют TPM и подвержены атакам отказа в обслуживании.
(3) Идентификация TPM узлов позволяет клиентам удаленно освидетельствовать узлы, однако при этом любой посторонний может

Таблица 2. Пример атрибутов

Атрибут	Логические условия	Описание
service	"EC2"	Название сервиса
version	"1"	Версия сервиса
vmm	"Xen", "CloudVisor"	Гипервизор (Hypervisor) монитор виртуальных машин
type	"small", "large"	Ресурсы виртуальной машины
country	"KZ", "BY"	Страна развертывания
zone	"Z1", "Z2", "Z3", "Z4"	Зона доступности

узнать чувствительную информацию: количество облачных узлов, которые составляют инфраструктуру провайдера облака, распределение платформ и др. Данная информация может быть использована потенциальным нарушителем для поиска уязвимостей в инфраструктуре облака или конкурентами для получения неких бизнес-преимуществ.

(4) Текущая реализация TPM абстракций неэффективна и может привести к появлению узких мест при масштабируемости облачных сервисов.

Для преодоления этих ограничений на 21 симпозиуме по безопасности (USENIX Security 2012) была предложена новая система, Excalibur [8], позволяющая создавать доверенные облачные сервисы. Система предоставляет новую абстракцию для доверенных вычислений (Trusted Computing), называемую «данные, опечатанные политикой», данные «опечатывают», шифруют в соответствии с определенной клиентом политикой, а затем «снимают печать», т.е. расшифровывают на тех узлах, чья конфигурация соответствует политике. Для обеспечения указанной технологии используется «шифрование, основанное на атрибутах» (attribute-based encryption), что позволяет снижать издержки на управление ключами и повышает производительность используемых распределенных протоколов.

Авторы продемонстрировали систему Excalibur, внедренную в облачную платформу с открытым исходным кодом Eucalyptus [8]. Для обеспечения безопасности загрузки программного обеспечения криптоустройство TPM хранит уникальный идентификатор (ключ) и отпе-

Таблица 3. Примеры политик ограничения региона

Политика	Спецификация
P1	service = "EC2" vmm = "CloudVisor" version ⩾ "1" instance = "large"
P2	service = "EC2" vmm = "CloudVisor" zone = "Z1"
P3	service = "EC2" vmm = "CloudVisor" country = "BY"

чаток (хэш-значение) стека программного обеспечения загруженного на узел облака с возможностью запрета загрузки клиентских данных в облачные узлы, чья идентификация или отпечатки не считаются надежными.

Согласно данной технологии каждый узел облака сконфигурирован набором читаемых атрибутов. Атрибуты выражают функции программного обеспечения (vmm, version) или аппаратного (location). Политика безопасности также несет конкретные логические условия, поддерживаемые провайдером ("vmm=Xen" и "location=KZ"). В качестве примера можно привести атрибуты развертывания аналога сервиса "EC2", для двух видов виртуальных машин из четырех зон Казахстана и Белоруссии, представленных в таблице 2.

Конфигурация узла содержит набор читаемых атрибутов аппаратного и программного обеспечения конкретного узла:

Excalibur

```
service: "EC2"; version: "1"; type: "small"; country: "BY"; zone: "Z2";
vmm: "CloudVisor"
```

Приведенная реализация позволяет обеспечить надежность облачных сервисов, конфиденциальность и целостность данных, защиту от инсайдеров, а также гарантировать расположение данных в определённых географических или юрисдикционных границах. Обеспечение строгой идентификации достигается использованием ключа аттестации удостоверений Attestation Identity Key (AIK). При этом для

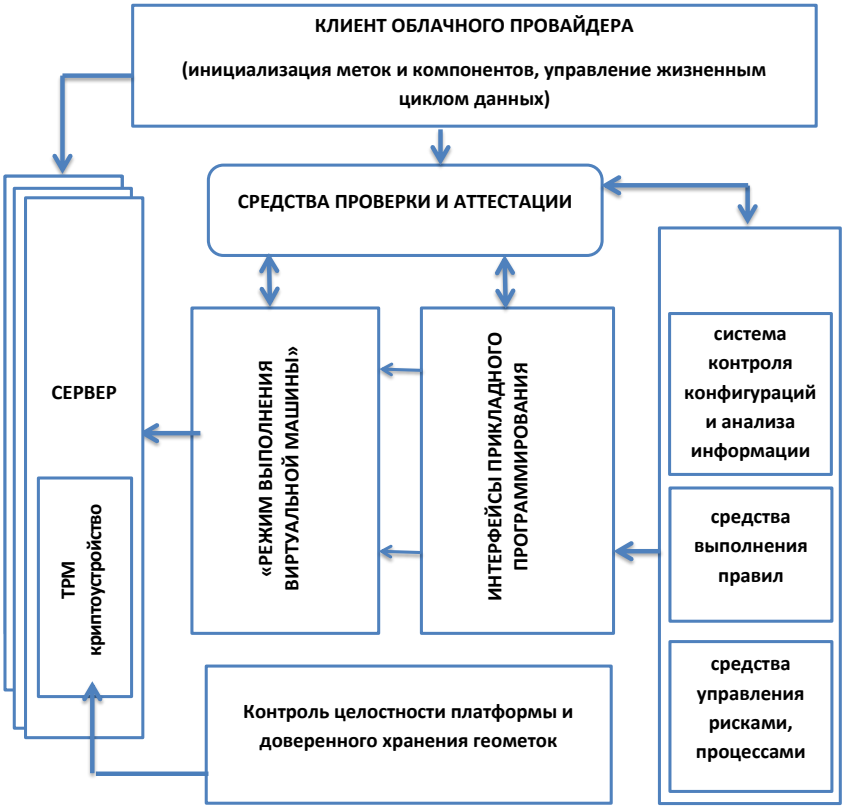

Рис. 1. Архитектура вычислительного пула

отслеживания хэш-значения TPM использует специальные регистры, называемые регистрами конфигурации платформы (РКП) — Platform Configuration Registers (PCRs). Конфигурация узла P1, представленная в таблице 3, описывает требования к версии и типу гипервизора, P2 описывает требования к зоне, а P3 ограничивает регион.

При перезагрузке значения РКП сбрасываются и обновляются новыми значениями хэш, которые связываются с текущим набором значений РКП. «Снять печать» подтверждает идентификацию и «отпечаток» программной платформы перед расшифровкой опечатанных данных.

3. Обобщенная схема геотегирования

При подключении к блоку управления представленного на рис. 1 клиент облачного провайдера осуществляет инициализацию меток и компонентов управления жизненным циклом принадлежащих ему данных, а также осуществляет доступ к конкретному физическому серверу [9] для осуществления контроля целостности платформы и доверенного хранения геометок.

На следующем этапе, используя средства проверки и аттестации (в прозрачном «сквозном» режиме [10, 11]), клиент допускается к взаимодействию с режимом выполнения виртуальной машины (через блок управления облаком и порталами, предоставленным провайдером и состоящим из системы контроля конфигураций и анализа информации, средств выполнения правил, средств управления рисками). Управление виртуальными службами осуществляется с помощью интерфейсов прикладного программирования (vCenter, OpenStack), что позволяет осуществлять необходимый контроль развертывания задач.

Заключение

Благодаря защите виртуализированных центров обработки данных на базе частного, публичного и гибридного облака от атак, направленных на компоненты, запуск которых предшествует запуску программ (BIOS, гипервизор, микропрограммы и пр.), доверенные вычислительные пулы обеспечивают соответствие требованиям к ИТ-инфраструктуре. Указанный метод измерения эталонного состояния аппаратных и предстартовых составляющих системы генерирует корень доверия. Именно доверенное выполнение кода программ является основой системы. Используя эталонные измерения как базу, администраторы систем осуществляют необходимую тонкую настройку политик размещения рабочих нагрузок и обработки конфиденциальных данных на конкретных серверах, так называемых доверенных вычислительных пулах [9]. Криптоустройство TPM обеспечивает гарантированно доверенное хранение данных с помощью шифрования [12].

Список литературы

[1] Л. Черняк. «Хранилище данных на кодах Рида–Соломона», *Открытые системы*, 2012, №2, с. 52 ↑ 62.

[2] R. Yeluri, E. Castro-Leon, *Building the Infrastructure for Cloud Security. A Solutions View*, Apress Media, 2014, pp. 93–123 ↑ 62, 63, 65.

[3] R. Santamarta. *A Wake-up Call for SATCOM Security*, IO Active, 2014, URL http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf ↑ 62.

[4] M. Ryan. *Trusted Computing: concepts*, University of Birmingham, 2008, URL http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/TrustedComputingConcepts.html ↑ 64.

[5] A. Dunn, O. Hofmann, B. Waters, E. Witchel, "Cloaking Malware with the Trusted Platform Module", *SEC'11 Proceedings of the 20th USENIX conference on Security*, USENIX Association, 2011 ↑ 65.

[6] В. Зорин. *Архитектура чипа безопасности*, PCWeek/RE (493) 31'2005 ↑ 65.

[7] A. Tomlinson, "Introduction to the TPM", *Smart Cards, Tokens, Security and Applications*, Springer, 2008, pp. 155–172 ↑ 65.

[8] N. Santos, R. Rodrigues, K. Gummadi, S. Saroiu. "Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services", 21st USENIX Security Symposium (USENIX Security 12), URL http://www.mpi-sws.org/~rodrigo/excalibur-usenix-sec12.pdf ↑ 66.

[9] W. Futral, J. Greene, *Intel® Trusted Execution Technology for Server Platforms: A Guide to More Secure Data Centers*, Apress Media, 2013, pp. 79–119 ↑ 69.

[10] V. Haldar, "Semantic Remote Attestation: a Virtual Machine Directed Approach to Trusted Computing", *3rd conference on Virtual Machine Research and Technology Symposium*. V. 3, USENIX Association, Berkeley, CA ↑ 69.

[11] E. Gallery, C. Mitchell. "Trusted Computing: Security and Applications", *Cryptologia*, **33**:3 (2008), pp. 217–245 ↑ 69.

[12] B. Berger. *Crypto chip: How the TPM bolsters enterprise security*, SC Magazine, 2008, URL http://www.scmagazine.com/crypto-chip-how-the-tpm-bolsters-enterprise-security/article/111865/ ↑ 69.

Рекомендовал к публикации *Программный комитет*
Третьего национального суперкомпьютерного форума ***НСКФ-2014***

Об авторах:

Владимир Иванович Воробьев

д.т.н., профессор, заведующий лабораторией информационно-вычислительных систем Санкт-Петербургского института информатики и автоматизации РАН

e-mail: vvi@iias.spb.su

Сергей Романович Рыжков

аспирант Санкт-Петербургского института информатики и автоматизации РАН

e-mail: ryzhkov@awax.ru

Роза Равильевна Фаткиева

К.т.н., с.н.с. Санкт-Петербургского института информатики и автоматизации РАН

e-mail: rrf@iias.spb.su

Пример ссылки на эту публикацию:

В. И. Воробьев, С. Р. Рыжков, Р. Р. Фаткиева. «Защита периметра облачных вычислений», *Программные системы: теория и приложения*, 2015, **6**:1(24), с. 61–71.

URL http://psta.psiras.ru/read/psta2015_1_61-71.pdf

Vladimir Vorobiev, Sergej Ryzhkov, Roza Fatkieva. *Cloud computing security perimeter.*

Abstract. Abstract concept of cloud data sealing by means of determinable policies is proposed. Use of TPM crypto modules for creation of trusted server platforms within the cloud is described. Generalized geo tagging scheme is presented. (*In Russian*).

Key Words and Phrases: cloud, cloud computing, security perimeter, geo tagging.

Sample citation of this publication

Vladimir Vorobiev, Sergej Ryzhkov, Roza Fatkieva “Cloud computing security perimeter”, *Program systems: theory and applications*, 2015, **6**:1(24), pp. 61–71. (*In Russian.*)

URL http://psta.psiras.ru/read/psta2015_1_61-71.pdf