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

ЗАЩИТА ПЕРИМЕТРА ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Аннотация. Представлена абстрактная концепция защиты облачных данных с помощью определяемых политик. Описано использование криптомодулей TPM в создании доверенных серверные платформы 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 концепции «геолокация», «геоограждение» и позволяют осуществлять мониторинг и контроль территориального распределения обработки данных. Технологии геолокации преобразуют физическое пространство в более доступную для различных трансформаций среду обитания (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 по географически распределенным физическим хранилищам, при этом решается и проблема нарушения целостности, поскольку, кража информации 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 DistributedStorage («распределенное хранилище»).[1] Технология сочетает доступность данных и позволяет сократить расходы на хранение благодаря высокой 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 аппаратномсбое. 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.

Показанная гибкость и масштабируемость, с которой виртуальные машины могут быть перенесены из одной страны в другую, вызывает повышенный интерес 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, но зачастую не распространяющуюся в отношении миграции 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

(GlobalPositioningSystem — система глобального позиционирования) на основе широты и долготы. Географическое положение может быть описано разными способами, с разной степенью точности, однако традиционные методы геолокации не удовлетворяют потребностям в безопасности облачных вычислений из-за низкого уровня доверия и недостаточно точных описаний местоположения как субъекта геотегирования, так и проблем доверия аппаратного уровня.[3] Поэтому Национальный Институт стандартов и технологий (США) в своём межведомственном отчёте NISTIR (NationalInstituteofStandardsandTechnologyInteragencyReport) 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 уверенно утверждать о 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 гео-заслона успешно применяется в мобильных компьютерах, в управлении цепочками поставок, транспортной логистике. Приложения, поддерживающие геозаслон позволяют администратору устанавливать правила и применять их в автоматизированном режиме при изменении границ нахождения устройств, а также задач или областей данных с выдачей соответствующих предупреждений для дальнейшего расследования.[2].

2. Создание доверенного пула с геолокацией в облаке

Создание доверенного пула с геолокацией в облаке включает в себя три основных этапа, как показано на рисунке 1.

Рисунок 1. Три этапа создания защищенного вычислительного пула с доверенноймгеолокацией.

На первом этапе производится настройка конфигурации сервера, в том числе настройка оборудования, BIOS и гипервизора, проверяется достоверность серверной платформы. Выполнение постоянного контроля гипервизора, обеспечивает достоверность аттестации. Аттестация платформы и запуск безопасного гипервизора являются основой надежности платформы и благодаря постоянному мониторингу, предоставляют более высокую скорость обнаружения проблем безопасности.

На втором этапе производится развертывание задач, с последующим переносом данных на доверенные серверные платформы внутри облака. Доверенная платформа, т.е. платформа, которой можно доверять (возможное действия гарантированно совпадает с эталонным), основана на абстракции "Корень Доверия" (RootofTrust англ.) — определенных компонентах, чья безопасность гарантирована. Полный перечень корней доверия обладает ограниченным набором возможностей, достаточным для перечисления компонентов платформы. Существует три корня доверия: корень доверия для измерений (RTM), корень доверия для хранения (RTS) и корень доверия для сообщений (RTR). RTM — вы-

числительный механизм, производящий измерения целостности платформы. RTS — вычислительный механизм, способный хранить хэши значений целостности. RTR — 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.

На третьем этапе к предыдущему подключаются механизмы развертывания гео-заслона. Через механизм аттестационного протокола, геотегированная информация (сформированная на этапе конфигурации сервера), сохраняется в виде зашифрованного хеш-значения в аппаратном криптографическом модуле BIOS (TPM TrustedPlatformModule криптоустройство). 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;

и 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 неповторяемости, что и генератор случайных чисел), а также средства способные ограничить использование ключей (как для подписи так и для шифрования/дешифрования).[5] Модуль TPM также используется для подтвердения подлинности аппаратных средств, за счет уникальности специфических устройств, что делает воз-

можным однозначное установление подлинности доверенной платформы.[6] [7]

2.1. Преодоление ограничений современныхкриптомодулей TPM

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

1. TPM абстракции были предназначены для защиты данных на автономном компьютере, что неудобно при использовании в мультиузловых 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 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, опечатанная политикой абстракция данных система Excalibur [8], позволяющая создавать доверенные облачные сервисы. Система предоставляет новую абстракцию для доверенных вычислений (TrustedComputing), называемую «данные опечатанные политикой», данные «опечатывают» шифруют в соответствии с опреде-

ленной 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-basedencryption), 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 ПО криптоустройство TPM хранит строгий идентификатор (уникальный ключ) и отпечаток (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 также несет конкретные логические условия поддерживаемые провайдером (“vmm=Xen и location=KZ”), представленным в табл. 1-3.

Таблица 1: Пример атрибутов. Представлены атрибуты из гипотетического развертывания аналога сервиса EC2, где доступны два вида виртуальных машин и четыре зоны (Центра обработки данных) в Казахстане и Белорусии.

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

Таблица 2: Пример конфигурации узла. Конфигурация содержит набор читаемых атрибутов аппаратного и программного обеспечения конкретного узла N:

УЗЕЛ	КОНФИГУРАЦИЯ
N	service : “EC2” ; version : “1” ; type : “small” ; country : “BY” ; zone : “Z2” ; vmm : “CloudVisor”

Таблица 3: Примеры политик. Приведены конфигурации узлов для развертывания, так P_1 описывает требования к версии и типу гипервизора, P_2 описывает требования к зоне, а P_3 ограничивает регион.

ПОЛИТИКА	СПЕЦИФИКАЦИЯ
P_1	service = “EC2” vmm = “CloudVisor” version ≥ “1” instance = “large”
P_2	service = “EC2” vmm = “CloudVisor” zone = “Z1”
P_3	service = “EC2” vmm = “CloudVisor” country = “BY”

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 AttestationIdentityKey (AIK). При этом для отслеживания хэш-значения, TPM использует специальные регистры называемые «регистры конфигурации платформы» (РКП) PlatformConfigurationRegisters (PCRs). При перезагрузке 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.

Рисунок 2. Доверенный вычислительный пул, архитектура решения с геотегами

3. Обобщенная схема геотегирования

При подключении к блоку управления, клиент облачного провайдера осуществляет инициализацию меток и компонентов управления жизненным циклом принадлежащих ему данных (рис. 2), 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 для взаимодействия с режимом выполнения виртуальной машины (через блок управления облаком и порталами предоставленный провайдером, который состоит 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 осуществить необходимый контроль за развертыванием 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. Указанная методика, с помощью 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]

[1] Черняк Леонид*Хранилище данных на кодах Рида – Соломона* // Открытые системы. 2012, № 2, с. 52.

[2] РагхурамЙелури (RaghuramYeluri), ЭнрикеКастро-Леон (Enrique Castro-Leon)*Building the Infrastructure for Cloud Security A Solutions View* ISBN13: 978-1-4302-6145-2.244 Pages. Publication Date: April 2, 2014

[3] Ruben Santamarta Principal Security Consultant *'A Wake-up Call for SATCOM Security.'* IOActive 2014URL:http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

[4] Mark Dermot Ryan.*Trusted Computing: concepts.* University of Birmingham (2008)URL:http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/TrustedComputingConcepts.html

[5] Alan M. Dunn, Owen S. Hofmann, Brent Waters, Emmett Witchel Cloaking Malware with the Trusted Platform Module // SEC'11 Proceedings of the 20th USENIX conference on Security. — USENIX Association, 2011.

[6] ЗоринВиталий*Архитектура чипа безопасности*PCWeek/RE (493) 31`2005

[7] Allan Tomlinson *Introduction to the TPM* // Smart Cards, Tokens, Security and Applications. — Springer, 2008. — С. 155—172. — DOI:10.1007/978-0-387-72198-9_7

[8] Nuno Santos and Rodrigo Rodrigues and Krishna P. Gummadi and Stefan Saroiu*Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services* Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)URL:http://www.mpi-sws.org/~rodrigo/excalibur-usenix-sec12.pdf

[9] William Futral and James Greene*Intel® Trusted Execution Technology for Server Platforms: A Guide to More Secure Data Centers*ISBN-13 (electronic): 978-1-4302-6149-0 2013 by Apress Media, LLC, all rights reserved

[10] VivekHaldar et al.,*Semantic Remote Attestation: a Virtual Machine Directed Approach to Trusted Computing*, VM2004 Proceedings of the 3rd conference on Virtual Machine Research and TechnologySymposium, vol. 3 (Berkeley, CA: USENIX Association)

[11] Eimear Gallery, Chris J. Mitchell *Trusted Computing: Security and Applications* // Cryptologia. — Taylor & Francis, 2008. — В. 33. — С. 217-245. — DOI:10.1080/01611190802231140

[12] Brian Berger. *Crypto chip: How the TPM bolsters enterprise security.* SC Magazine (2008)

[13] Абрамов С. М., Знаменский С. В. *Краткая инструкция для авторов журнала «Программные системы: теория и приложения»* // Программные системы: теория и приложения: электрон.научн. журн. 2013. Т. 4, № 2(16), с. 43–69. URL: http://psta.psiras.ru/read/psta2013_2_43-69.pdf

Об авторах:

Воробьев Владимир Иванович

д.т.н., профессор, раведующий лабораторией информационно-вычислительных систем, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

e-mail: *vvi@iias.spb.su*

Рыжков Сергей Романович

(основные сведения, разработки, награды,место работы — гдеделалась статья!)

*e-mail:*ryzhkov@awax.ru

Фаткиева Роза Равильевна

к.т.н., доцент, с.н.с лаборатории информационно-вычислительных систем, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

e-mail: *rikki2@yandex.ru*

Образец ссылки на публикацию:

Воробьев В.И., Рыжков С.Р, Фаткиева Р.Р..Защита периметра облачных вычислений // Программные системы: теория и приложения: электрон. научн. журн. 2014. Т. ?, № ?(??), с. ??–??. URL: http://psta.psiras.ru/read/???

Vorob`evV.I., RyzhkovS.R, FatkievaR.R. (Cloud computing security perimeter).

ABSTRACT.Presented an abstract concept of sealing cloud data with defined policies.

DescribedTPM cryptomoduleas the basicof the trusted server. Generalised geotagging presented.

*Key Words and Phrases:*cloud, cloud computing, security perimeter, geotagging.