Инфраструктура безопасности в распределенных информационно-вычислительных системах на основе технологии блокчейн

А. П. Крюков[a], А. П. Демичев

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова»,
Научно-исследовательский институт ядерной физики имени Д.В.Скобельцына,
119234, ГСП-1, Москва, Ленинские горы, 1, стр. 2

E-mail: [a] kryukov@theory.sinp.msu.ru

Уязвимым местом инфраструктур безопасности большинства существующих распределенных информационно-вычислительных систем (РИВС) является существование специального центрального сервера, от которого критически зависит безотказная и устойчивая к незаконному проникновению работа всей системы. В данной работе исследуется возможность отказа от такого специального отдельного сервера и использования для указанных целей распределенной базы данных на основе блокчейн-технологии, парадигмы умных контрактов и протокола Ethereum. Поскольку в этом случае база данных инфраструктуры безопасности распределена по всем узлам системы, такой подход приводит к повышению отказоустойчивости и безопасности РИВС.

Ключевые слова: распределенные информационно-вычислительные системы, инфраструктура безопасности, блокчейн-технология.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации, Соглашение № 14.604.21.0146 о предоставлении субсидии; уникальный идентификатор прикладных научных исследований (проекта) RFMEFI60414X0146.

Введение

Для обеспечения безопасного доступа к ресурсам распределенных информационно-вычислительных систем (РИВС) с учетом прав данного пользователя и правил обслуживания пользователей данным сервисом или ресурсом необходима инфраструктура безопасности, которая должна быть с одной стороны достаточно надежная, а с другой стороны не создавать существенных сложностей при работе пользователей. В работе [Dubenskaya, Kryukov, …, 2016] предложена методика аутентификации пользователей, которая базируется на паре логин-пароль с получением сессионного ключа с ограниченным данной сессией временем действия. Главное отличие предложенного подхода состоит в том, что вместо короткоживущего, но многократно используемого прокси-сертификата было предложено использовать постоянные уникальные сертификаты для каждого запроса. Этот подход приводит к существенному упрощению как регистрации новых пользователей в системе, так и их работы в РИВС, по сравнению с наиболее часто применяемой в РИВС инфраструктурой открытых ключей (PKI) с использованием прокси-сертификатов. Однако уязвимым местом как PKI, так и решения, предложенного в работе [Dubenskaya, Kryukov, …, 2016], является необходимость безотказной и устойчивой к незаконному проникновению работы центрального сервера инфраструктуры безопасности (сервера аутентификации и авторизации в [Dubenskaya, Kryukov, …, 2016] или сервера возобновления прокси-сертификатов в PKI).

В данной работе исследуется возможность отказа от специального отдельного сервера в инфраструктуре безопасности РИВС и использования для указанных целей распределенной базы данных на основе технологии блокчейн [BitFury Group, 2015], парадигмы умных контрактов [Szabo, 1997] и протокола Эфириум (Ethereum) [Buterin, 2016; Wood, 2015]. Поскольку в этом случае база данных инфраструктуры безопасности распределена по всем узлам системы, такой подход приведет к повышению отказоустойчивости и безопасности РИВС.

Суть блокчейн-технологии состоит в следующем. Пусть дана некоторая система, для которой определен набор дискретных состояний. Состояния системы могут изменяться в последовательные дискретные моменты времени. На каждом шаге изменение в состоянии системы происходит в результате некоторой транзакции (атомарного изменения состояния системы), что в совокупности определяет эволюцию этой системы. Протокол блокчейн предназначен для подробной и хорошо защищенной записи такой эволюции. Запись осуществляется распределенным образом — на всех или части узлов сети, образующих систему. Для данного момента времени блокчейн (цепочка блоков записей транзакций) позволяет получить информацию о любой из предшествующих транзакций. Среди прочего это позволяет убедиться, что все предшествующие транзакции были корректными, а значит и текущее состояние является корректным. Причем чем дальше по времени от текущего момента отстоит выбранная транзакция, тем труднее злоумышленнику подменить запись о ней так, чтобы это было незаметно для агентов в узлах сети (поскольку надо изменить зашифрованные записи во всех блоках — от подмененной транзакции до текущего момента времени).

Предлагаемое решение основано на идеях платформы Эфириум, которая позволяет создавать децентрализованные приложения с использованием блокчейн-технологии. Эфириум использует основные наработки, предложенные в рамках криптовалюты Bitcoin [Franco, 2015], протокола BitTorrent [BitTorrent] и идею умных контрактов [Szabo, 1997] для создания общей платформы, позволяющей разработчикам использовать эти новые технологии для различных целей.

Использование блокчейн-технологии для построения инфраструктуры безопасности РИВС

В случае РИВС система и ее состояния определяется следующим образом.

- Система определяется как набор сервисов, входящих в РИВС, идентифицируемых хешами их открытых ключей.
- Состояние РИВС определяется совокупностью состояниями запросов, обрабатываемых сервисами в данный момент.
- Транзакция определяется как изменение состояния запроса.

Аналогично Эфириуму блоки блокчейна РИВС содержат не только список транзакций, но и последнее состояние системы.

Блокчейны можно разделить на группы в соответствии с доступом к его данным. По доступу к чтению транзакций блокчейны подразделяются следующим образом: открытый блокчейн (public blockchain), в котором не существует ограничений на чтение данных блоков (при этом данные могут быть зашифрованы) и ограничений на отсылку транзакций для включения в блокчейн; закрытый блокчейн (private blockchain), в котором прямой доступ к данным и к отправке транзакций ограничен определенным списком эккаунтов. По доступу к обработке транзакций блокчейны подразделяются следующим образом: общедоступный (инклюзивный) блокчейн (permissionless blockchain), в котором не существует ограничений для обработчиков транзакций (то есть, эккаунтов, которые могут создавать блоки транзакций); эксклюзивный блокчейн (permissioned blockchain), в котором обработка транзакций осуществляется определенным списком эккаунтов.

Эксклюзивные блокчейны могут формировать более контролируемую и прогнозируемую среду, чем общедоступные блокчейны. В отличие от криптовалют и Эфириума, в эксклюзивных блокчейнах обычно не используются встроенные монеты. Встроенные монеты необходимы в криптовалютах для предоставления награды за обработку транзакций. Создание блоков в эксклюзивном блокчейне в простейшем случае не требует вычислений, связанных с алгоритмами доказательства работы. В частности, возможен следующий протокол создания блоков, похожий на делегированное подтверждение доли [BitFury Group, 2015]: существует фиксированное количество обработчиков транзакций — сервисов, входящих в состав РИВС; каждый обработчик владеет парой из секретного и открытого ключа, причем создатель каждого блока определяется по обязательной цифровой подписи блока, являющейся частью заголовка блока; обработчики (сервисы РИВС) создают блоки по очереди через фиксированные интервалы времени; порядок создания блоков может быть фиксирован или меняться случайным образом после каждого цикла обработки всеми сервисами, входящими в РИВС; если сервис по какой-либо причине не может создать блок в отведенный ему интервал времени, он пропускает этот цикл. Чтобы злонамеренно изменить транзакцию подтвержденную всеми сервисами РИВС, злоумышленник должен получить доступ ко всем секретным ключам обработчиков блоков. Таким образом, поскольку обработчики транзакций являются единственными потребителями данных блокчейна, приведенный выше протокол теоретически даже более надежен, чем протокол, основанный на доказательстве работы (в случае которого для успешной атаки необходимо получить контроль над 51% узлов сети [Franco, 2015]).

Основные моменты алгоритма аутентификации и авторизации выглядят следующим образом:

- каждый запрос оформляется как транзакция, для него (с учетом времени и идентификатора) вычисляется хеш (как обычно для транзакций в технологии блокчейн) и записывается в базу данных, распределенную по узлам РИВС;
- при получении запроса, сервис проверяет с помощью распределенной базы данных: правильность хеша запроса, а также то, что он еще не использовался (эта информация записана в транзакции, еще не включенной в блок); имеет ли данный пользова-

тель право делать полученный запрос (эта информация записана как часть состояния системы в последний сформированный блок);

- если полученная информация подтверждает корректность запроса, сервис выполняет запрос;
- когда подходит очередь данного сервиса, он формирует блок из транзакций, еще не включенных в блоки.
- Делегация прав между сервисами также реализуется с помощью информации о транзакциях (уже оформленных в блок или еще находящихся вне блоков):
- первый сервис генерирует новый запрос на основе первоначального запроса, полученного от пользователя;
- новый запрос оформляется как новая транзакция, записывается в распределенную базу данных и для него генерируется хеш;
- первый сервис передает сгенерированный им запрос второму сервису для обработки;
- второй сервис проверяет полученный хеш запроса; если проверка дает положительный результат, второй сервис продолжает его обрабатывать.

Заключение

В данной работе предложена схема работы инфраструктуры безопасности распределенных информационно-вычислительных систем на основе технологии блокчейн, адаптированной для сравнительно небольших РИВС. При этом предложено использовать эксклюзивные блокчейны, а также некоторые элементы, разработанные для платформы Эфириум. Такая инфраструктура будет свободна от важного недостатка, присущего существующим решениям, а именно, от уязвимостей, связанных с наличием специально центрального сервера, управляющего работой инфраструктуры безопасности.

Список литературы

BitFury Group, Public versus Private Blockchains. 2015. [Электронный ресурс]. URL: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf (дата обращения: 02.10.2016).

BitTorrent [Электронный ресурс]: http://www.bittorrent.com (дата обращения: 22.10.2014).

Buterin V. Ethereum White Paper. 2016. [Электронный ресурс]. URL: https://github.com/ethereum/wiki/wiki/White-Paper (дата обращения: 02.10.2016).

Dubenskaya J., Kryukov A., Demichev A., Prikhodko N. New security infrastructure model for distributed computing systems // Journal of Physics: Conference Series. — 2016. — Vol. 681. — P. 012051-1 012051-5.

Franco P. Understanding Bitcoin. Cryptography, engineering, and economics. — West Sussex: John Wiley & Sons, 2015.

Szabo N. The Idea of Smart Contracts. 1997. [Электронный ресурс]. URL: http://szabo.best.vwh.net/smart_contracts_idea.html (дата обращения: 02.10.2016).

Wood G. Ethereum: A secure decentralised generalised transaction ledger. 2015. [Электронный ресурс]. URL: http://gavwood.com/paper.pdf (дата обращения: 02.10.2016).

Security Infrastructure for Distributed Computing Systems on the Basis of Blockchain Technology

A. P. Kryukov[a], A. P. Demichev

Moscow State University, Skobeltsyn Institute of Nuclear Physics,
1, build. 2, Leninskie gory, Moscow, 119991 Russia

E-mail: [a] kryukov@theory.sinp.msu.ru

A vulnerability area of security infrastructures of the majority of existing distributed computing systems (DCS) is the need of operation of a fail-proof and tamper-resistant central server in the security infrastructure. In this work, we investigate the possibility of abandoning the special dedicated servers in the DCS security infrastructure and the use instead of them a distributed database on the basis of the blockchain technology, the paradigm of smart contracts and the Ethereum protocol. Since in this case the database of the security infrastructure is distributed across all the nodes in the system, this approach will increase the resiliency and security of DCS.

Keywords: distributed computing systems, security infrastructure, blockchain technology.

The work was supported by the Ministry of Science and Education of the Russian Federation, the Agreement No. 14.604.21.0146; unique identifier is RFMEFI60414X0146.