3. *Барсуков В. С., Романцов А. П.* Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности XXI века // Специальная техника. 2008. № 4–5 [Электронный ресурс]. Режим доступа: http://st.ess.ru/

4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М. : Изд-во ТРИУМФ, 2003.

5. *Новосельский А.* Форматы звуковых файлов // Компьютеры + Программы. 2006. № 1 [Электронный ресурс]. Режим доступа: http://www.aip.mk.ua/

АНАЛИЗ ЗАЩИЩЕННОСТИ ОБЛАЧНЫХ СИСТЕМ С ПОМОЩЬЮ ГЕНЕТИЧЕСКОГО АЛГОРИТМА

Т. И. Паюсова
(Тюмень, ТюмГУ, database_kb@mail.ru)

Научный руководитель: д-р техн. наук, профессор *А. А. Захаров*

Облачные системы являются принципиально новой концепцией предоставления сетевого доступа к вычислительным и компьютерным ресурсам, например, к хранилищу данных, серверу, приложению, виртуальной машине. Основными характеристиками облачных инфраструктур являются: объединение ресурсов в пул, широкая доступность через сеть, самообслуживание по требованию пользователя (заказчика), гибкость и масштабируемость, измеримость предоставляемых услуг.

Объединение ресурсов в пул является реализацией принципа множественной аренды (multi-tenancy): предоставляемые ресурсы объединяются в пул и динамически распределяются между большим числом пользователей в соответствии с их потребностями.

Широкая доступность облачных сервисов подразумевает, что доступ к ним можно получить с помощью стандартных средств и механизмов, используя разнородные клиентские платформы. Кроме этого, пользователь в случае необходимости может получить доступ к облачным вычислениям самостоятельно без взаимодействия с поставщиком.

Ресурсы могут оперативно резервироваться, масштабироваться и освобождаться по требованию пользователей, при этом с точки зрения потребителя доступные возможности часто выглядят ничем не ограниченными и могут быть приобретены в любом количестве, в любое время [3].

Измерение услуг, которые предоставляются облачными системами, осуществляется с помощью специальных абстрактных параметров, изменяющихся в зависимости от категории и вида услуги. Например, количественно может быть оценена вычислительная мощность, пропускная способность, размер хранилища данных.

В рамках концепции облачных систем принято выделять три модели обслуживания: облачное программное обеспечение как услуга (Cloud Software as a Service, SaaS), облачная платформа как услуга (Cloud Platform as a Service, PaaS) и облачная инфраструктура как услуга (Cloud Infrastructure as a Service, IaaS).

Модель обслуживания SaaS предполагает предоставление доступа заказчику к приложению или набору приложений, размещенных в облачной среде. Доступ осуществляется через пользовательское устройство, например, с использованием тонкого клиента. Заказчик может работать только с программным обеспечением, не имея никакой возможности влиять на работу сети, сервера, настройки операционной системы и т. д.

Модель PaaS позволяет предоставить заказчику набор программного обеспечения для разработки новых или существующих приложений. При этом платформа предлагает пользователю необходимый инструментарий, средства тестирования, системы управления базами данных. Заказчик не может контролировать остальные компоненты облачной инфраструктуры.

В случае использования облачной инфраструктуры как услуги пользователь может управлять фундаментальными вычислительными ресурсами облака, например, самостоятельно устанавливать и запускать произвольное программное обеспечение, включая операционные системы. Облачный провайдер, в свою очередь, осуществляет контроль над основной физической и виртуальной частью облака.

Выделяют четыре модели развертывания облачных систем: частное облако (private cloud), облако сообщества (community cloud), публичное облако (public cloud) и гибридное облако (hybrid cloud).

Частное облако предназначено для использования одной организацией и несколькими потребителями. Частное облако находится в собственности или самой организации, или некоторой третьей стороны и физически может существовать как внутри, так и вне юрисдикции владельца [4].

Облако сообщества используется конкретной группой заказчиков – сообществом. Участники сообщества принадлежат разным организациям, но связаны единой целью и задачей. Данный вид облака может принадлежать одной из организаций или третьей стороне. Физическое размещение community cloud определяется по аналогии с частным облаком.

Публичное облако находится в собственности некоторой организации и предназначено для свободного использования большим числом заказчиков. Физически публичное облако принадлежит поставщику услуг.

Гибридное облако является комбинацией двух или более различных облачных инфраструктур перечисленных выше. При этом предполагается, что элементы гибридного облака остаются уникальными объектами, взаимодействующими между собой при помощи стандартизованных технологий передачи данных [4].

Появление облачных систем позволило значительно повысить доступность услуг, вычислительных и компьютерных ресурсов, обеспечить масштабируемость и гибкость развернутых в облачной среде систем, понизить риски, связанные с неработоспособностью и обслуживанием элементов инфраструктуры.

Но при этом в рамках облачной концепции проявились вопросы, связанные с безопасностью предоставляемых решений. Системы облачных вычислений имеют характерные проблемы и уязвимости, среди которых можно выделить потерю клиентов, отсутствие общепринятого стандарта обеспечения безопасности облачных вычислений, ограничения модели безопасности, уязвимости программного обеспечения элементов облака и уязвимости сетевой

инфраструктуры облака, атаки на систему виртуализации, клиентов облака и, наконец, комплексные угрозы системам облачных вычислений [1].

Для облачных систем выделяют следующие специфические риски безопасности:

• Неправомерное использование облачных систем (характерно для сервисных моделей IaaS и PaaS).

Данный риск безопасности заключается в том, что злоумышленники могут использовать облачные системы в своих преступных целях, например, для создания ботнет-сетей или размещения вредоносного кода. Препятствовать данной угрозе можно с помощью исследования сетевой активности и усовершенствования процессов регистрации и верификации пользователей.

• Уязвимости в облачных системах.

В первую очередь наличие уязвимостей в облачных системах касается сервисной модели IaaS. Так, сервис модель IaaS предполагает абстрагирование аппаратных ресурсов и их представлений от вычислительных ресурсов с помощью системы виртуализации. Выделяют виртуализацию серверов, приложений, представлений и уровня операционной системы. Виртуализация повышает гибкость инфраструктуры, уровень отказоустойчивости, позволяет снизить затраты на оборудование, программное обеспечение, обслуживание и электроэнергию. Виртуальные среды в облачных вычислениях используются для координации и объединения элементов облака, поэтому атаки на систему виртуализации угрожают и всей облачной инфраструктуре в целом. Специальное программное или микропрограммное обеспечение – гипервизор – позволяет виртуализировать системные ресурсы. В гипервизорах могут присутствовать серьезные уязвимости, используя которые можно получить доступ к физическим ресурсам или повысить привилегии. Для того чтобы противостоять этой угрозе, необходимо изолировать виртуальные среды и обеспечить внедрение системы обнаружения сбоев.

• Уязвимые программные интерфейсы (API).

Угроза характерна для IaaS, Paas и SaaS сервис моделей. Безопасность облачной системы зависит от безопасности программных интерфейсов. Программные интерфейсы предоставляют пользова-

телям механизмы управления сервисами, ресурсами, виртуальными машинами. Для устранения данного риска безопасности необходимо использовать устойчивые алгоритмы шифрования и надежные методы аутентификации и авторизации.

Кроме этого, угрозы могут исходить и от сотрудников, обслуживающих облачную инфраструктуру, т. е. со стороны провайдера. Справедливыми остаются и угрозы, связанные с потерей и утечкой данных. При этом в обоих случаях угрозы касаются и IaaS, и PaaS, и SaaS сервис моделей. Использование систем мониторинга уязвимостей, запрет на передачу учетных записей, резервное копирование, шифрование данных, использование двухфакторных методов аутентификации и т. д. позволяет снизить или даже устранить риски безопасности, связанные с утечкой данных и инсайдерскими атаками [5].

Типичными атаками на облачные среды являются атаки на программное обеспечение, включая атаки с использованием уязвимостей операционных систем, сетевых протоколов, модульных компонентов системы. Установка систем обнаружения вторжений, межсетевых экранов, антивирусов позволяет противостоять атакам на уровне программного обеспечения.

Атаки на клиента системы, например, межсайтинговый скриптинг (Cross Site Scripting, XSS), кража паролей, перехват веб-сессий, также актуальны для облачной инфраструктуры, поскольку пользователи часто подключаются к облаку именно с помощью браузера. Ярким примером атаки на клиента облака является атака «человек посередине» (man in the middle). Данный вид атаки реализуется с помощью перехвата атакующих сообщений, которыми обмениваются корреспонденты, при этом ни один из корреспондентов не догадывается о присутствии злоумышленника в канале связи. Атакующий может читать и видоизменять сообщения, тем самым реализовывая атаки на нарушение конфиденциальности и целостности информации [6].

Поскольку облачная инфраструктура представляет собой многослойную систему, для нее также остаются справедливыми и функциональные атаки на элементы облака, и защита системы становится равной защите самого слабого звена. При этом каждый «слой»

системы требует определенного подхода с точки зрения безопасности, например, веб-сервер требует контроль целостности страниц, уровень систем управления базами данных – защиту от sql-инъекций, системы хранения данных нуждаются в резервном копировании и т. д.

Анализ защиты облачных систем требует комплексного подхода. Несмотря на большое количество и высокое качество продуктов защиты, представленных на рынке, трудно найти универсальное и масштабируемое решение для анализа защищенности облачной среды. Дело в том, что существует множество сценариев реализации атак, и предусмотреть все варианты, детали и тонкости бывает достаточно нелегко [2].

Одним из решений данного вопроса может стать построение и анализ графа атак. Граф атак отражает, во-первых, структуру облачной системы, а, во-вторых, все возможные последовательности действий злоумышленника.

Вершинам графа соответствуют источники, цели и результаты атаки. Также вершины могут обозначать атаки, выполненные с использованием уязвимостей. Структурные связи и переходы системы из состояния в состояние обозначаются в виде дуг.

Анализ графа атак является многокритериальной задачей, поскольку на практике обычно требуется оценить и проанализировать защищенность достаточно крупных систем, представленных большим количеством хостов, внутренних и внешних связей. И вопрос автоматизации процесса синтеза и анализа графа атак становится особенно актуальным.

Решать подобные задачи позволяют эвристические алгоритмы, которые дают приближенное решение без строгого обоснования и, в отличие, например, от списочных методов, обеспечивают меньшую погрешность. В частности, эволюционно-генетические алгоритмы позволяют решать многокритериальные задачи за полиномиальное время с помощью действий, напоминающих основные механизмы биологической эволюции, например, кроссинговера, естественного отбора, мутаций, смены поколений, формирования популяций и представления данных в виде хромосом. Генетические алгоритмы являются одними из наиболее эффективных алго-

ритмов, позволяющих в начале построить оптимальное решение, а затем внести в него необходимые корректировки вручную.

Генетический алгоритм позволяет определить множество мер наименьшей стоимости, максимально повышающих защищенность облачной системы. Стоимость каждой меры защиты определяется политикой безопасности.

Основная структура данных в алгоритме – хромосома – представляется в виде битовых векторов, например, первый вектор отвечает за устранение уязвимости с помощью обновления программного обеспечения, и длина вектора равна количеству уязвимостей; второй вектор соответствует дуге в графе атак, и наличие единичного бита говорит о присутствии фильтрации трафика в системе или IDS-сенсора и т. д. Каждый компонент хромосомы называется геном.

Целевая функция алгоритма определяется как отношение количества входящих в вершину дуг, удаляемых после реализации мер защиты, к стоимости всех реализованных мер защиты в хромосоме [2].

В начале работы алгоритма формируется случайная популяция – несколько индивидуумов (особей) со случайным набором хромосом. Далее в ходе работы алгоритма осуществляется имитация эволюции этой популяции с помощью механизмов кроссинговера и мутаций: в результате кроссинговера особи обмениваются генами, а в ходе мутаций особь «получает» другой набор генов. Новая популяция формируется в соответствии с целевой функцией, которая определяет приспособленность особи. Чем приспособленнее особь, тем больше вероятность ее участия в кроссинговере.

Целевая функция определяет наиболее приспособленные особи для осуществления процесса кроссинговера. Например, в кроссинговере участвует только половина наиболее приспособленных особей, вторая половина «погибает». Также целевая функция определяет момент остановки алгоритма: алгоритм завершает свою работу, когда наступает вырожденность популяции (у каждой особи одно и то же значение целевой функции). Кроме этого, алгоритм предусматривает использование переменной вероятности мутации с целью снижения вероятности попадания алгоритма в область

локального оптимума. Вероятность мутации меняется в зависимости от количества поколений. В начале алгоритма вероятность мутаций выше, при схождении – ниже.

Применение генетического алгоритма для анализа графа атак, описывающего облачную инфраструктуру, позволяет значительно повысить защищенность системы при минимальном использовании ресурсов.

Библиографические ссылки

1. *Емельянова Ю. Г., Фраленко В. П.* Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления // Программные системы: теория и приложения : электрон. науч. журн. 2011. № 4(8). С. 17–31 [Электронный ресурс]. URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf

2. *Паюсова Т. И.* Анализ графа атак с помощью генетического алгоритма с переменной, вероятность мутации для предотвращения сетевых атак на облачные вычисления // Безопасность информационного пространства : сб. ст. Тюмень : Изд-во ТюмГУ, 2012. С. 112–116.

3. http://www.moysklad.ru/chto_takoe_oblachnye_servisy/

4. http://clouds-microsoft.blogspot.ru/p/blog-page_10.html

5. http://www.anti-malware.ru/node/2333

6. http://www.securitylab.ru/news/363719.php

СИСТЕМА ЭМУЛЯЦИИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Е. Ф. Попов
(Тюмень, ТюмГУ)

Динамичное развитие технологий передачи данных приводит к изменению угроз информационной безопасности. Появление новых методов атаки на сети передачи данных требует постоянного усовершенствования средств защиты информации.

При разработке программного обеспечения или проектировке систем, предназначенных для обеспечения информационной безопасности, важным этапом является тестирование выбранного или