МОДЕЛИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Мукашева Г.Е., докторант I курса специальности 6D060200 «Информатика»
Научный руководитель: Сагындыков К.М., к.т.н., доцент
Казахский гуманитарно-юридический инновационный университет г.Семей Республики Казахстан

Люди, которые используют форму заявки, должны будут устанавливать шлюзы и интеллектуальные счетчики различной степени в своих домах. Основная проблема безопасности возникает при аутентификации этих шлюзов и интеллектуальных счетчиков. Каждое интеллектуальное устройство обнаружит IP-адрес. Атака может произойти на устройстве, сообщая о ложных показаниях на интеллектуальных счетчиках, подделывая IP. Есть несколько решений для проблемы аутентификации. В таких случаях можно использовать инфраструктуру открытого ключа. Обмен ключами Dieffie-Hellman предполагает, что интеллектуальные счетчики могут зашифровать данные до того, как они передадут их на устройства тумана. Затем ваше устройство настроено на дешифрование данных. Вторжения в интеллектуальную сетку могут быть распознаны с помощью метода, основанного на сигнатурах, где можно обнаружить любое несоответствие в дизайне и поднять флаг о возможном неправильном поведении.

Биометрическая аутентификация является наиболее выгодным методом аутентификации, который может использоваться для обеспечения легкого доступа. Биометрическая аутентификация, такая как аутентификация по отпечаткам пальцев, косметическое распознавание, репутация сетчатки глаза и т. д. Может использоваться в аутентификации на основе туманов. Могут быть расхождения в аутентификации через человека в середине забастовки, смягчении кражи данных и т. Д. Для решения проблемы могут быть использованы методы, основанные на инфраструктуре, такой как инфраструктура открытого ключа (PKI), может быть использована доверенная исполняемая среда (TEE). рассматривается в облачных вычислениях тумана. Метод, основанный на измерении, может использоваться для фильтрации поддельного или неквалифицированного туманного облака, которое не находится в непосредственной близости от конечных пользователей, что, безусловно, уменьшит стоимость аутентификации.

Индивидуальный доступ к данным и обнаружение вторжений

Обеспечение контроля доступа к интеллектуальным устройствам и облаку всегда было надежным инструментом, обеспечивающим безопасность компьютера. Управление доступом в облаке достигается за счет использования методов нескольких схем шифрования для создания расширенного доступа к управлению в облачной обработке. Методы диагностики вторжений применялись для смягчения нарушений на цифровом аппарате или гипервизоре. Эти системы распознавания вторжений могут использоваться на координирующей машине для обнаружения вторжений.

Конфиденциальность. Поскольку область хранения и вычисления достаточны для обоих краев в туманном облаке, могут быть предложены методы сохранения конфиденциальности. Алгоритмы сохранения уровня конфиденциальности могут выполняться между туманом и облаком, поскольку для обоих атрибутов достаточно вычислений и хранения. Нам нужны методы сохранения конфиденциальности, потому что в настоящее время пользователи больше обеспокоены риском утечки личной конфиденциальности. Туманный узел обычно собирает данные, генерируемые датчиком и конечными устройствами. Такие методы, как гомоморфное шифрование, могут использоваться для обеспечения агрегирования с сохранением конфиденциальности на соседних шлюзах без расшифровки. Для статистических целей может применяться дифференциальный метод личной конфиденциальности для обеспечения личной конфиденциальности любой произвольной отдельной записи в наборе данных.

Доверенная модель. В таких сервисах, как электронная коммерция, одноранговая связь (P2P), обзоры пользователей и модели доверия, основанные на репутации онлайн-сетей, могут быть успешно реализованы. Модель доверия, основанная в основном на доверии, - это простой метод, при котором люди создаются для оценки другого человека после того, как функции присваивают его рейтингам доверие или репутацию, полученную в результате оценок. Для выбора эталона в сетях P2P была предложена надежная система репутации с использованием выделенного алгоритма опроса для оценки надежности вашего ресурса. Нам придется заняться такими вопросами, как, как добиться постоянной, уникальной и специфической идентичности, как лечить преднамеренное и случайное плохое поведение. Помимо моделей, упомянутых выше, существуют также модели доверия, основанные на специальном оборудовании, таком как Secure Aspect (SE), уважаемая среда выполнения (TEE) или Trusted Platform Component (TPM), которые могут обеспечить доверие к приложениям туманных вычислений.

Обеспечение безопасности. Сотрудничество в области политики является важным компонентом на центральном уровне модели вычислений тумана. Внедрение политики взаимодействия для поддержки безопасного письма и связи в распределенной среде. Поскольку туманные вычисления также включают в себя взаимодействие с взаимодействием с физическим элементом, эта необходимость дает возможность перейти к новой группе проблем безопасности, которые включают управление идентификацией, источник управления доступом к информации, надежную балансировку заполнения, качество обслуживания и т. Д. Структура, основанная на страховом полисе, состоит, если следующие модули.

Модуль механизма принятия решений: этот модуль запрограммирован для принятия агрегированных решений по данным, предоставленным всеми компонентами. Предназначенный для обслуживания, запрошенного пользователем знака, этот двигатель двигателя анализирует правила,

определенные в репозитории покрытия, и вырабатывает решение, которое впоследствии вступает в силу.

Администратор приложения: мультитенантный характер парадигмы обработки тумана повышает требование к администратору указывать политики и руководящие принципы, которые привязывают потребителя к приложениям и обеспечивают безопасную совместную работу и миграцию клиентских данных между несколькими функциями, которые поддерживаются приложением.

Репозиторий полисов: Безопасный репозиторий, содержащий правила и руководящие принципы, на которые ссылается двигатель механизма принятия решений о плане страхования во время принятия решения о страховом полисе, называется репозиторием покрытия.

Принудительный страховой полис: страховой полис является наиболее динамичным компонентом построения управления покрытием. Он находится в виртуальном корпусе или центре обработки данных облачных вычислений или в физическом устройстве, таком как мобильное устройство, система глобального позиционирования и подключенные транспортные средства.

Человек в среднем атаке: Это самая типичная атака в туманных вычислениях. В этом типе атак шлюзы, служащие в качестве противотуманных устройств, могут подвергаться опасности или заменяться имитационными.

Настройки окружения теста скрытности: человек в середине атаки может быть довольно скрытным в парадигме обработки тумана. Этот тип атаки потребляет очень мало ресурсов в таких противотуманных устройствах, как незначительное использование процессора и незначительное потребление памяти. Поэтому традиционные методы не могут выставить человека в центре атаки.

Человек в центре атаки легко запустить, но трудно справиться. Многие приложения, работающие в туманной вычислительной среде, восприимчивы к нападению человека в центре. В дальнейшем требуется работа по устранению вреда человеку в середине в туманных вычислениях.

Снижение край данных: Облачные вычисления сталкиваются с новыми проблемами безопасности данных. Существующие механизмы покрытия, такие как шифрование, не нашли своего символа во избежание атак кражи. Чтобы одержать победу над этим, была предложена новая методика мониторинга доступа к данным в облаке и поиска ненормального доступа к данным для получения привычек. Когда подозревается несанкционированный доступ, а затем подтверждается с помощью контрольного вопроса, возникает эпизод дезинформации, когда злоумышленнику возвращаются большие объемы жесткой информации. Это защищает от неправильного использования реальных данных пользователя.

Профилирование пользовательских привычек: владельцы или одобренные пользователи ваших персональных компьютеров обычно знакомы с данными в системе. Так что любое исследование файлов ограничено и может иметь стиль. Когда информация получена незаконно, в статьях системы

документов может быть знакомая структура. Это чрезмерное поведение поиска, которые показывают изменения отслеживаются.

Технология приманки: файлы ловушек размещаются в системе записи. Документы с сеткой, загружаемые клиентом, расположены в очень заметных местах, которые не мешают нормальной работе машины. Пользователь, который не знаком с системой записей, скорее всего, получит доступ к поддельным документам, если для конфиденциальных документов установлено отдельное лицо. Чтобы позволить им быть пойманными с помощью данных приманки.

В некоторых случаях оба эти метода могут быть объединены для защиты данных от кражи.

Список литературы:

1. Turner, M., Budgen, D. and Brereton, P. (2003) Turning Software into a Service. Computer, 36, 38-44.
2. Gartner IT Glossary (2017) Software as a Service (SaaS) from the Gartner IT Glossary.
3. Buxmann, P., Hess, T. and Lehmann, S. (2008) Software as a Service. Business Informatics, 50, 500-503.
4. Godse, M. and Mulik, S. (2009) An Approach for Selecting Software-as-a-Service (SaaS) Product. 2009 IEEE International Conference on Cloud Computing, Bangalore, 21-25 September 2009, 155-158.