технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service);

Таким образом можно подытожить, что обеспечение информационной безопасности при использовании облачных вычислениях зависит и от клиента, и от провайдера. Следует подойти серьезно к составлению договора с поставщиком облачных услуг и учесть все факторы, которые могут повлиять на обеспечение конфиденцианости данных. Со стороны клиента - это использование современных программных и аппаратных средств, работа профессионально подготовленного персонала, обеспечение безопасности сетевого оборудования, хранилища данных, сервера и гипервизора. Дополнительно возможно размещать в выделенном ядре антивирус для предотвращения заражения гипервизора через виртуальную машину, систему шифрования данных для хранения пользовательской информации в зашифрованном виде и средства для реализации зашифрованного тунелирования между виртуальным сервером и клиентской машиной. Также проводить своевременный аудита всех систем на выявление уязвимостей и контроль уровней доступа пользователей.

Список использованных источников:

1. Котяшичев И. А., Бырылова Е. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. — 2015. — №6.4. — С. 30-34. — URL https://moluch.ru/archive/86/16357/ (дата обращения: 24.03.2019).
2. Удо Шнайдер Использование облачных сервисов [Текст] / У. Шнайдер //
3. Информационная безопасность в облачных вычислениях: уязвимости, методы и средства защиты, инструменты для проведения аудита и расследования инцидентов URL: https://www.bibliofond.ru/view.aspx?id=783809 (дата обращения: 24.03.2019)
4. Арзамасов Е.В., Чурикова А.А. Угрозы облачных вычислений и методы их защиты // Технические и математические науки. Студенческий научный форум: электр. сб. ст. по мат. V междунар. студ. науч.-практ. конф. № 5(5). URL: https://nauchforum.ru/archive/SNF_tech/5(5).pdf

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ МЕТОДОМ АНАЛИЗА ДИНАМИКИ ВВОДА ТЕКСТА

Супринович И.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Искра Н.А. – старший преподаватель

В данной работе рассматриваются алгоритмы идентификации пользователя методом анализа динамики ввода текста. Помимо этого рассматривается возможность и сценарии применения этого метода идентификации, а также изучаются способы классификации, которые позволят сделать идентификацию пользователя более точной.

Потребность в распознавании людей по каким-либо уникальным, присущим только им признакам, возникла достаточно давно. Эту проблему призвана решить аутентификация — процесс идентификации и подтверждения личности пользователя. Обычно он сопровождается авторизацией, которая является механизмом определения того, какими правами наделяется пользователь после идентификации.

Аутентификация классифицируется следующим образом:

1) аутентификация на основе уникальной информации — для успешной идентификации пользователю необходимо ввести пароль;

2) аутентификация на основе уникального предмета — для успешной идентификации пользователю необходимо предъявить уникальный предмет, например пластиковую карту;

3) аутентификация на основе какой-либо уникальной характеристики пользователя, физиологической или поведенческой (биометрия).

Одним из представителей поведенческой биометрии является аутентификация методом анализа динамики ввода текста (АМАДВТ) — распознавание пользователя с помощью анализа динамики ввода текстовых последовательностей. Данный метод считается достаточно надёжным, так как очень сложно изучить темп и стиль ввода другого человека. Также он не требует какого-либо специального оборудования в отличие от методов физиологической биометрии.

В основе АМАДВТ лежат алгоритмы выявления аномалий — алгоритмы, позволяющие выделить необычные значения в выборке данных. От выбора алгоритма зависит точность распознавания пользователя. Наиболее часто используемыми метриками для выявления аномалий являются стандартное расстояние Махалонобиса, а также его разновидности — фильтрованное и масштабированное.

Большинство алгоритмов АМАДВТ состоят из следующих этапов:

1) сбор данных — собираются данные о времени нажатия и отпускания клавиш во время ввода пользователем пароля;

2) создание модели пользователя — преобразование данных, полученных на первом этапе, в модель с параметрами HoldTime (время удержания клавиши), DownDownTime (время между последовательными нажатиями двух клавиш) и UpDownTime (время между отпусканием клавиши N и нажатием клавиши N + 1). В течение некоторого времени эти данные накапливаются, после чего их можно использовать;

3) расчёт схожести полученной выборки и идеальной — расчёт расстояния между моделью пользователя и полученной на этапе ввода выборкой. Чем меньшее значение получено, тем более похожими являются выборки;

4) анализ полученных результатов — расчёт вероятности того, что данные были введены истинным пользователем.

Для улучшения распознавания пользователя можно использовать несколько моделей пользователя, которые отличаются временем сбора данных (темп набора пользователя может изменяться в зависимости от времени суток).

У АМАДВТ есть серьёзный недостаток: его точность напрямую зависит от удобства клавиатуры (эргономика, ход клавиш, размеры), то есть при смене пользователем устройства ввода необходимо обучить систему аутентификации заново. Также стоит отметить тот факт, что модель пользователя может быть применена только для того устройства, на котором она создавалась, поэтому АМАДВТ желательно использовать в качестве дополнительного уровня идентификации.

Таким образом, аутентификация методом анализа динамики ввода текста является достаточно хорошим способом аутентификации, хоть и не лишённым недостатков.

Список использованных источников:

1.А.Г. Дьяконов, А.М. Головина — Выявление аномалий в работе механизмов методами машинного обучения — 2017. — С.389-396.

2.Dr.Abdulameer Khalaf Hussain, Mustafa Nouman Al-Hassan — Multifactor Strong Authentication Method Using Keystroke Dynamics — 2013. — Vol.2, No.2, — C.31-34.

TMOF УЯЗВИМОСТЬ

Трафимук М.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Селезнев И.Л. – к.т.н.,доцент

В современном мире все большее количество услуг и сервисов предоставляется посредством сети Интернет, поскольку Интернет и, соответственно, все его ресурсы доступны повсеместно. Помимо описанных положительных сторон, есть и отрицательные: доступность, стабильность и надежность зависят не от пользователя, а от владельца ресурса. Обеспечить максимальную стабильность – это первостепенная задача администратора ресурса, для выполнения которой необходимо знать возможные уязвимости и способы их устранения. Не менее важно помнить и про известные проблемы, которые не считаются уязвимостями, вроде TMOF – too many open files.

С течением времени все большее количество услуг и сервисов предоставляется посредством сети Интернет. Повсеместное распространение доступа к сети и ее ресурсам является основной причиной этого явления. Помимо положительных сторон, у этого явления есть и отрицательные моменты: доступность, стабильность и надежность зависят не от пользователя, а от владельца ресурса. Обеспечить максимальную стабильность – это первостепенная задача администратора ресурса, для выполнения которой необходимо знать возможные уязвимости и способы их устранения.

На сегодняшний день ключевые ресурсы сети Интернет являются достаточно устойчивыми к различного вида атакам, использующим уязвимости протоколов UDP и TCP, а также DNS-серверов и других широко используемых сущностей. Ранее использование недоработок в этих компонентах для реализации атак приводило к неприятным последствиям для владельцев и администраторов ресурсов сети Интернет. Ключевой идеей этих, устаревших на данный момент, атак является генерация и отправка больших потоков данных атакуемому ресурсу. Некоторые современные атаки используют схожие механизмы, но избегают условий, в которых воздействие считается атакой и нейтрализуется существующими методами противодействия вроде «blackholing».

Современные атаки используют узкопрофильные уязвимости, которые, тем не менее, могут покрывать достаточно большой процент ресурсов сети Интернет. Например, уязвимостям, направленным на подсистемы серверов на базе Unix, подвержены свыше 40% всех серверов сети