УДК XXX.XXX

ЗАЩИЩЁННЫЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ

В.В. Ващило, М.И. Кошевник

В работе исследуется вопрос безопасного использования способов идентификации и аутентификации пользователей. Для рассматриваемых различных способов выделяются их ключевые особенности. Исходя из механизма атаки, предлагается способ защиты привычного клавиатурного метода аутентификации пользователя (на примере ввода пароля). В заключении приводится сравнительная таблица рассмотренных методов.

Введение

С началом использования многопользовательских систем возникла необходимость разделения доступа между различными пользователями. Для того, чтобы представить пользователя некоторой системе, была разработана модель «Идентификация – аутентификация – авторизация». В её концепцию заложен следующий принцип: на этапе идентификации пользователь представляет данные о себе некоторой системе – называет своё имя и заранее согласованный пароль (секрет); на этапе аутентификации система производит проверку – сравнивает данные, указанные пользователем, с уже имеющимися в базе; в случае успеха происходит заключительная операция – авторизация – пропуск пользователя в систему, выдача прав на проведение операция и передача ему управления, в противном – возврат к этапу идентификации либо полный отказ в доступе.

Первыми идентифицирующими пользователя признаками в информационных системах являлись логин – зарегистрированное в системе имя, и пароль – комбинация алфавитно-цифровых символов, вводимых с клавиатуры. И хотя при грамотном и правильном использовании данного метода он предоставлял достаточную защиту, с ходом развития и усложнения информационных технологий выявлялись определённые угрозы безопасности идентифицирующих и аутентифицирующих систем, что ставило перед системными администраторами и специалистами по информационной безопасности новые задачи.

Постановка задачи

Система идентификации и аутентификации – основа программно-технических средств безопасности. Именно она является первой линией защиты информационной системы.

Процесс идентификации позволяет представиться системе, сообщив данные о себе – назвав своё имя. Аутентификацией вторая сторона убеждается, что идентифицирующий пользователь – действительно тот, за кого себя выдаёт.

В современном мире ввиду активного развития и использования многопользовательских систем возникают риски получения доступа к системе лицами, которым к системе изначально не предусмотрен и/или запрещён.

Злоумышленник, в зависимости от вида защищённой системы, может поступать различными способами – либо кражей секрета, либо его подбором.

На сегодняшний день широко распространены средства захвата данных, поступающих с клавиатуры, как аппаратной, так и виртуальной, во время прохождения процедур идентификации и аутентификации. Данная проблема вызывает необходимость её изучения и анализа для повышения безопасности механизмов идентификации и аутентификации.

Задача защищённой системы идентификации – обеспечить выполнение всех операций в идеале без риска компроментации пользовательских данных.

Существующие решения

Защита на основе многоразовых паролей

Классический принцип: пользователю выдаётся постоянный пароль, используемый для каждого входа в систему.

На идентификационные признаки в виде многоразового пароля должны быть наложены технические ограничения:

- минимальная длина, необходимость содержать символы обоих регистров, цифровые знаки и т.п.;
- сроки действия паролей, их периодическая смена;
- число неудачных попыток входа в систему;
- доступ к файлу паролей.

Допустимо использование программных генераторов паролей (программ, основанных на правилах, которые генерируют благозвучные и запоминающиеся пароли).

Защита на основе одноразовых паролей

Более устойчивым средством защиты является одноразовые пароли, выдаваемые пользователю на время сеанса работы. Общая идея их реализации сводится к односторонней функции (функция, вычислить обратное значение которой за приемлемое время не представляется возможным), известной пользователю и серверу аутентификации. Пользователь на этапе начального согласования протокола обмена, обладая секретным ключом, известным только ему, применяет функцию к нему определенное количество раз, и сохраняет результат на сервере. Процедура аутентификации после этого происходит в виде общения сторон клиент-сервер, передавая друг другу вычисляемые значения этой функции по собственному алгоритму. Если сервер получает от пользователя корректные значения, которые без обратимой функции можно вычислить только обладая секретным ключом, то аутентифицирующая сторона убеждается в подлинности пользователя и выдаёт разрешение на вход в систему.

Защита такой системы обуславливается надёжностью алгоритма, согласовывающего, генерируемого и производящего общение между сторонами клиент-сервер.

Защита от кейлоггеров

Одним из способов кражи учётных данных является использование злоумышленником кейлоггерама – программного либо аппаратного устройства,

регистрирующего действия, совершаемые пользователями. Внедрив такое устройство в целевую систему, злоумышленник получает информацию о нажатии клавиш на клавиатуре, движении и нажатиях мыши, а также дате и времени этих нажатий. Таким образом, он получает полную последовательность действий, совершенную пользователем и может воспроизводить её самостоятельно для извлечения необходимых данных. Примером программного кейлоггера служит утилита, работающая в операционной системе скрытым для пользователя образом, регистрирующая события устройств ввода и отправляющая данные злоумышленнику. Примером аппаратной реализации является физическая накладка на клавиатуру, которую могут устанавливать на цифровые клавиши ввода банкоматов и платёжных терминалов.

В целях ликвидации возможности перехвата учётных данных кейлоггерами можно использовать сторонние решения – программные комплексы сертифицируемых антивирусных систем. Такие системы в режиме реального времени следят за активностью всех исполняемых процессов, что уменьшает вероятность регистрации действий устройств ввода сторонними программами при их наличии в системе.

Так как данные, полученные кейлоггерами, по своему принципу должны быть доставлены злоумышленнику, в целях дополнительной безопасности можно проводить контроль сетевого траффика. В интерактивном режиме администратором формируются правила, согласно которым разрешается определённый сетевой траффик в зависимости от направления. Все остальные попытки установить соединение – запрещаются. В таком случае, даже если перехват в пользовательской системе произведён, данные злоумышленнику доставлены не будут.

Механизм keyhook

Кейхук (keyhook) – системный механизм из API операционной системы, выполняющий захват сообщений и мониторинга событий. Отличие от кейлоггера заключается в том, что последнее является целевым зловредом для внедрения в операционную систему. Сам же механизм легально используется даже утилитой управления видеоадаптером для поворота изображения.

От клавиатуры при работе в операционной системе Windows может поступать четыре сообщения: WM_KEYDOWN, WM_KEYUP, WM_SYSKEYDOWN, WM_SYSKEYUP. Когда происходит нажатие клавиши, генерируется сообщение WM_KEYDOWN или WM_SYSKEYDOWN, в зависимости от того, какая была нажата клавиша и была ли эта клавиша нажата в комбинации с клавишей <Alt>. При отпуске клавиши генерируется сообщение WM_KEYUP или WM_SYSKEYUP.

Используя механизм keyhook, можно получать данные, передаваемые другим приложениям. Этим методом пользуются клавиатурные шпионы. При работе операционной системы могут работать одновременно несколько экземпляров кейхука. Различить их назначение – зловредное либо необходимое пользователю – достаточно сложно.

Защита от полного перебора

Защита от автоматического подбора паролей – брутфорса – может произведена методом ограничения попыток идентификации и аутентификации. Так как операция брутфорса происходит в автоматическом режиме практически без участия человека, системным администратором может быть установлено правило на допустимое количество либо интервал между неудачными попытками авторизации. В этом случае на стороне идентифицирующей системы будет временно отключена атакующая учётная запись, что не позволит выполнить в неё вход стороннему лицу. Соответствующие события могут быть залогированы для последующего анализа администратором системы.

Также дополнительным средством защиты, ликвидирующим автоматические системы взлома, является капча (captcha)– слово либо фраза, представленная в искажённом графическом либо аудиальном виде.

Двухфакторная аутентификация

Ввиду того, что полной гарантии защиты от несанкционированного получения доступа нет, учётные записи могут защищаться дополнительными методами проверки. Данные методы производятся уже после предоставления логина и пароля, но всё ещё до и авторизации и входа в систему.

Такие системы называются системами двухфакторной аутентификации. В качестве дополнительной защиты – второго фактора – согласовывается метод, используемый по иному принципу и, возможно, другому каналу связи, а также с помощью иного устройства. Это может быть канал SMS-сообщений, телефонный звонок либо смартфон. Секретом в данном случае может выступать разовый ключ, полученный в SMS сообщении на мобильный номер пользователя.

Бесклавиатурные методы

Бесклавиатурные методы предполагают, исходя из своего названия, такие способы идентификации и аутентификации, которые не используют клавиатуру в привычном для неё исполнении. Сделано это в первую очередь для того, чтобы избежать перехвата паролей кейлоггерами – устройствами, регистрирующими нажатия клавиш, движения манипуляторами курсора и иные действия, совершаемые пользователем.

По идентификационным признакам бесклавиатурные методы бывают:

1. Электронными;
2. Биометрическими;
3. Комбинированными.

Электронные бесклавиатурные методы идентификации

В электронных системах идентифицирующий пользователя признак хранится в памяти стороннего носителя. Образцами такой системы являются:

- Контактные смарт-карты;
- Бесконтактные смарт-карты;
- USB-ключи.

В любом типе смарт-карт имеется защищённая область в памяти, которая отвечает за хранение секретной идентифицирующей информации. Информационным носителем в контактной смарт-карте, как правило, является

магнитная полоса либо встроенный чип. Для проведения аутентификации необходим физический контакт такой карты с устройством-считывателем. Процедура обмена в бесконтактном варианте происходит с помощью радиосигнала на предельно малом расстоянии (до десяти сантиметров) по технологии NFC – Near Field Communication.

USB-ключи представляют собой внешний USB-накопитель с записанной в памяти устройства цифровой подписью владельца. Работает такой ключ в паре с соответствующим установленным программным обеспечением на необходимом компьютере. Процедура подключения USB-ключа в USB-порт является в данном случае идентификацией пользователя. При извлечении ключа происходит блокировка либо завершение сеанса работы.

Биометрические бесклавиатурные методы идентификации

В системах данного вида идентификационным признаком является индивидуальная особенность человека. Во время идентификации происходит получение биометрических характеристик от авторизуемого пользователя и сравнение этих данных с имеющимися в базе шаблонами.

В свою очередь, биометрические методы подразделяются на две категории:

- Статические;
- Динамические.

Примером статических данных являются неизменные признаки человека, такие как отпечаток пальца, узор радужной оболочки глаза, форма ушной раковины и иные.

К динамическим данным относятся действия, совершаемые человеком – демонстрация его голоса или почерка.

Комбинированные бесклавиатурные методы идентификации

Данные методы подразумевают использование сразу нескольких признаков. Они могут относиться как к одной группе – например, комбинация только статических, так и обоих – отпечаток пальца и демонстрация голоса.

Электронный вариант бесклавиатурной идентификации имеет свои положительные стороны в практичности использования. Недостаток – в потенциальной возможности кражи либо утери.

Биометрические методы являются сегодня самым дорогостоящим вариантом. Их использование может быть оправдано в организациях с соответствующим уровнем риска – политических либо финансовых. Достоинства: уникальность, крайне высокая сложность подделки. Недостатки: высокая стоимость, невозможность замены в случае кражи/утечки.

Бесклавиатурный метод может использоваться в качестве второго этапа двухфакторной аутентификации. Это позволяет серьёзным образом повысить уровень защиты.

Примером использования одноразовых паролей является аутентифицирующая утилита «Google Authenticator». Данная система представлена в виде приложения для мобильных операционных систем. На начальном этапе настройки генерируется секретный ключ и кодируется в base32, который далее используется для генерации разовых ключей.

Необходимая согласовывающая информация передаётся на серверную сторону. Теперь, при попытке входа в систему после ввода логина и пароля сервер аутентификации ожидает ввод ключа, который каждые 30 секунд генерируется в том числе в мобильном приложении. Для работы системы больше не требуется передача данных от приложения к серверу. Отображённый на экране мобильного устройства временный ключ пользователь вводит в web-форму.

Уязвимость данного метода заключается в потенциальной возможности кого-либо знать или подсмотреть исходный секретный ключ, используемый на этапе согласования. Обладая такой информацией, можно вычислять код для входа в аккаунт по тому же алгоритму, что использует аутентифицирующая система.

Аналогичный, но обратный по сторонам аутентификации принцип работы использует приложение двухфакторной аутентификации от Microsoft. После представления системе на этапе ввода пары логин-пароль запрос на вход в систему поступает в пользовательское приложение. Web-форма, в которой пользователь представлял свои данные, указывает сгенерированную комбинацию из пяти алфавитных символов, например, «ABCDE». Пользователь видит поступивший в приложение запрос и при совпадении сгенерированной фразы разрешает его.

В основу двух этих мобильных приложений для двухфакторной аутентификации заложен разный принцип работы. В версии от Google заранее согласован алгоритм, на клиентской стороне сгенерирован ключ и для его работы не требуется интернет-соединение – единственным критерием правильной работы является точное время на обоих сторонах. В варианте от Microsoft заранее согласованного секрета нет – сервер сам генерирует временный ключ, и отправляет запрос на его одобрение в пользовательское приложение. В последнем случае обязательно наличие интернет-соединения.

Метод виртуальных клавиатур

С ходом развития web-технологий широкое распространение получили виртуальные клавиатуры, работающие по принципу экранного ввода. Отрисовка таких компонентов, как правило, выполняется с помощью JavaScript, положение этой формы можно самостоятельно менять на экране. В некоторых случаях возможно изменение стандартного расположения клавиш. Сделано это, в первую очередь, для ликвидации возможности захвата событий keyhook и кейлоггером. Но остаётся доступной возможность захвата инструментом mousehook – регистрирующим события, поступающие с мыши.

В данном случае восстановить последовательность действий, совершённую пользователем возможно только с одновременными снимками экрана и захватом координат.

Предлагаемые варианты решения

Самым распространённым вариантом аутентификации по-прежнему является клавиатурный метод, основная уязвимость которого состоит в возможности прослушивания событий нажатий клавиш через механизм keyhook.

При помощи аппаратного шифрования самой клавиатурой обеспечивается защита ввода данных через EPP-клавиатуру в банковских устройствах.

Разработкой методов, обеспечивающих защиту от клавиатурных шпионов, занимаются различные производители антивирусных средств. Однако, публикации в последнее время статистик об используемых пользователями паролях свидетельствуют, что эти же программные средства непосредственно выполняют сбор паролей с последующей их отправкой на свои сервера для анализа, зачастую даже не предупреждая и не спрашивая на это разрешения пользователя.

Разработка собственных программных средств, обеспечивающих защиту от клавиатурных шпионов, является обоснованным в условиях невозможности по разным причинам использования других средств. Закрытые готовые разработки просто вынуждают пользователей поверить в их благонадёжность и доверить им свои данные.

Для защиты обычных компьютерных клавиатур – аппаратных и виртуальных – предлагается вариант маскировки реальных событий, наполняя приложением, принимающим пользовательский ввод, очередь поступающих с устройства реальных скан-кодов клавиш виртуальными.

Таким образом, каждое приложение, в которое осуществляется ввод данных пользователем, получает данные как из клавиатуры, так и из приложения генерации нажатий клавиш. Приложение, которое осуществляет генерацию, является и получателем и может легко отделить из всего потока только данные, введённые пользователем, например, пароль. Все другие приложения этого сделать не могут из-за отсутствия различия между реальными событиями и генерируемыми.

Например, паролем является строка «1234». В процессе его ввода приложение дополнительно сгенерировало события нажатий клавиш «A», «4», «9», «8», «7». Таким образом, из потока ввода может получить, например, строку «1A4239847». Легальное приложение-получатель (оно же и генератор) анализирует и вычитает из полученной строки символы «A4987», получая в итоге искомый пароль «1234». Все другие приложения через механизм keyhook получат значение «1A4239847».

Заключение

Имея модель потенциальных угроз, специалист по защите информации обязан грамотным образом выбрать подходящие способы идентификации пользователя.

Необходимо отметить, что надежность средства защиты прямо пропорциональна его стоимости, а кража бесплатных био-идентификаторов может угрожать жизни его владельца.

Таким образом, при выборе средств идентификации и аутентификации специалисту необходимо пользоваться принципом разумной достаточности: найти компромисс между надежностью, доступностью по стоимости и удобством использования и администрирования.

Таблица 1

Сравнительная характеристика средств идентификации и аутентификации по основным критериям

	Идентифицирующий признак	Сложность воспроизведения	Стоимость использования	Сложность замены в случае утери/кражи
Классический пароль	Многоразовый ключ	Предельно простая	Минимальная	Минимальная
Двухфакторная аутентификация	Одноразовый генерируемый ключ	Не используется	Минимальная	Достаточно просто (генерация нового ключа и согласование с сервером)
Стороннее устройство	Секрет, хранящийся в смарт-карте	Практически невозможно	Обусловлено стоимостью смарт-карты	Обусловлено стоимостью смарт-карты
Уникальная биометрическая информация	Динамический: Голос либо почерк	Достаточно высокая	Очень высокая стоимость оборудования, бесплатный био-идентификатор	Практически невозможно
	Статический: Отпечаток пальца, скан сетчатки глаза либо радужной оболочки глаза	Очень высокая		

Использование дополнительных программных средств позволяет обеспечить защищённость от кражи данных даже подверженную уязвимости «прослушивания» процедуру идентификации пользователя через ввод пароля с использованием обычной клавиатуры.

Список литературы

1. Brian Donohue – Двухфакторная аутентификация: что это и зачем оно нужно? [Электронный ресурс] / – Официальный русский блог Лаборатории Касперского. – Режим доступа: https://blog.kaspersky.ru/ what_is_two_factor_authenticatio/4272/. – Дата доступа: 30.11.2015.

2. Клавиатурные сообщения [Электронный ресурс] / Электронная библиотека книг Александра Фролова и Григория Фролова. – Режим доступа: http://frolov-lib.ru/books/bsp/v11/ch5_1.htm. – Дата доступа: 05.12.2015.

Ващило Владимир Витольдович, старший преподаватель кафедры Системного программирования и компьютерной безопасности Гродненского государственного университета имени Янки Купалы, v.vaschilo@grsu.by

Кошевник Максим Игоревич, студент кафедры Системного программирования и компьютерной безопасности Гродненского государственного университета имени Янки Купалы, maxim.koshevnik@gmail.com