СОВРЕМЕННЫЕ МЕТОДЫ АУТЕНТИФИКАЦИИ

РЕКВИЕМ ПО ПАРОЛЯМ

Вы все еще используете пароли?
Тогда мы идем к вам!

«АУТЕНТИКАЦИЯ»…

Слово, вынесенное в название раздела является, по идее, правильным переводом английского слова **authentication**, - термина из сферы информационной безопасности. Слово обозначает процедуру проверки на основании некой уникальной информации личности человека, который пытается получить доступ к данным (идентификация), а также выяснение, является ли этот субъект тем, за кого себя выдает.

В русском языке, однако, прижился модифицированный вариант этого термина – **аутентификация**. Видимо, аналогом для подобной метаморфозы послужила идентификация (**identification**), которая определяется как процедура распознавания субъекта по его идентификатору (какой-либо информации – числу, строке символов и т.д.).

Причина этого лингвистического казуса представляется вполне ясной – понятия «аутентификация» и «идентификация» столь близки, что порой их путают даже квалифицированные специалисты. Вот и сейчас – определения даны, а ясности пока нет. Попробуем разобраться более детально.

Для простоты представим себе проходную предприятия и охранника, который обязан контролировать проход на территорию и задерживать всех посторонних. Всех сотрудников внесли в списки, и для того, чтобы пройти мимо бдительного сотрудника охраны, нужно назвать себя. Дальше происходит то, что как раз и называется идентификацией: в имеющейся «базе учетных данных» происходит поиск идентификатора. Если сотрудник начал работать недавно и еще не попал в списки, охранник его не пропустит – в базе нет такого идентификатора. В этом примере подлинность субъекта не проверяется – зная ФИО любого сотрудника можно незаконно проникнуть на охраняемую территорию. Таким образом, идентификация не обеспечивает высокой степени безопасности, так как идентификатор легко отделим от субъекта и может быть использован посторонним.

Описанный недостаток присущ всем системам идентификации вне зависимости от принципа, лежащего в их основе. Всем знакомые турникеты-«вертушки», открывающиеся от приложенной карточки с беспроводной радиометкой RFID, тоже никак не проверяют личность субъекта. Понятно, что такой способ приемлем, например, для контроля прохода в метро, но для обеспечения действительно надежной защиты он не годится.

Отличный пример аутентификации подарили нам отечественные мультипликаторы. В 15-м выпуске «Ну, погоди!» Бегемот-охранник на входе в Дом Культуры не только спрашивает у Волка идентификатор («Кто?»), но и проверяет, соответствует ли Волк тому, за кого он пытается себя выдать («заяц», «зебра», «черепаха»). Другими словами, Бегемот проводит аутентификацию субъекта.

> *Итак, идентификация – это распознавание субъекта по идентификатору (есть в базе или нет), а аутентификация – это проверка соответствия между субъектом и предъявляемым им идентификатором*

…И ЕЕ ФАКТОРЫ

Каким же способом можно проводить аутентификацию? Прежде чем ответить на этот вопрос, введем еще одно понятие. **Фактор аутентификации** – это определенный вид уникальной информации, предоставляемый субъектом системе при его аутентификации.

Вернемся к аналогиям. На этот раз воспользуемся образами из шпионских романов. Агенту Смиту необходимо встретиться со связным и передать ему секретную информацию. Друг друга они не знают и никогда раньше не встречались. Как Смит сможет удостовериться, что перед ним действительно связной, а не вражеский агент? Различают всего четыре фактора аутентификации. Рассмотрим их все.

«У Вас продается славянский шкаф?» - это пример первого фактора, когда субъект что-то знает. На практике это может быть пароль, логин, кодовая фраза – словом, любой секрет, известный обеим сторонам.

Связной может предъявить, например, половину разорванной фотографии или что-то еще, что есть только у него – это пример второго фактора аутентификации, основанного на том, что у субъекта есть что-то. В современных системах информационной безопасности для этих целей используются **токены** – персональные аппаратные средства аутентификации.

Для обеспечения безопасности встречи можно условиться, что она должна состояться на третьей скамейке справа от входа в Центральный парк. Третий фактор – субъект находится в определенном месте. В

информационных системах могут определяться, например, IP-адрес компьютера субъекта или считываться данные радио-метки.

Ну и наконец, Смиту могли показать фотографию связного, чтобы он смог его узнать.Четвертый фактор (субъект обладает некой биологической особенностью) применяется только в случае, когда субъект аутентификации – человек, а не, например, сервер или процесс, не имеющие отпечатков пальцев, структур ДНК или радужной оболочки глаза.

Рассмотрим представленные факторы подробнее.

СТРАСТИ ПО ПАРОЛЯМ

Широко распространено мнение, что парольная аутентификация – самая простая и дешевая из всех возможных. Действительно, для ее внедрения в информационную систему организации не нужно приобретать дополнительного программного или аппаратного обеспечения и нанимать квалифицированных специалистов.

Однако как показывает практика, а также исследования авторитетных компаний, пароли обходятся компаниям достаточно дорого. Дело в том, что для того, чтобы пароли были действительно надежными, они должны быть длинными, сложными и случайными. Например, широко известно, что на сегодняшний день для обеспечения приемлемого уровня защиты криптографические алгоритмы должны использовать ключи длиной 256 бит. Считается, что на современном уровне развития техники перебор всех вариантов этого ключа (2^{256} или около 10^{77}) потребует значительно больше времени, чем то, за которое информация устареет (15 лет).

Если попробовать подсчитать «стойкость пароля», состоящего из строчных и прописных латинских букв и цифр, то для достижения такой же 256-битной надежности (2^{256} вариантов перебора) нужен случайный пароль длиной 43 символа. Например, такой: 09fqt9PJ0nsRNBkBqGGnFpHp7BsgnliKTR25vQLlXe8. Естественно, ни один пользователь не в состоянии запомнить подобный пароль, поэтому администраторы безопасности, зажмурив глаза, все-таки позволяют использовать более короткие пароли, требуя, однако, их регулярной смены.

В компаниях же, где требования к парольной политике сформулированы хотя бы в минимальном соответствии с реальными угрозами, основной проблемой становятся пользователи, записывающие свои пароли на бумажках, и пользователи, регулярно забывающие свои пароли. Если опасность первого способа запоминания пароля очевидна (обычно пользователи оставляют бумажку с паролем вблизи компьютера, поэтому любой может воспользоваться информацией и проникнуть в систему), то «забывчивость» сотрудников может показаться спорным «камнем в огород» парольной защиты.

Дело в том, что в случае такой «амнезии» на пароли, пользователю приходится просить администратора безопасности сбросить защиту паролем (чтоб была возможность, во-первых, зайти в систему, а во-вторых, поставить новый пароль для защиты). Вот эта самая процедура сброса пароля пользователя и является потенциально слабым местом в системе информационной безопасности компании. Ведь чаще всего администраторы выполняют такие просьбы просто по телефонному звонку. Стоит ли говорить, что звонящий может оказаться кем угодно? В компании даже из 100 человек далеко не всех можно узнать по голосу.

Для повышения безопасности приходится значительно усложнять эту процедуру, что автоматически влечет за собой рост стоимости поддержки системы парольной аутентификации: простои в работе сотрудника, рабочее время администратора – все это по оценкам Gartner Group выливается в сумму от $30 до $140 в год на одного пользователя.

КЛАВИАТУРНЫЕ «ШПИОНЫ»

Помимо атаки, основанной на подборе пароля пользователя, серьезную опасность для этого метода аутентификации представляют клавиатурные «шпионы». «**Шпион**» (от англ.spyware) – это вредоносное ПО, которое, при наличии физического доступа, может быть установлено злоумышленником на целевой компьютер за несколько минут, пока сотрудник отлучился, забыв заблокировать рабочую станцию. Трех-пяти минут, которые обычно устанавливают как тайм-аут для автоматической блокировки при бездействии пользователя, вполне достаточно, чтобы хозяин ушел достаточно далеко, а злоумышленник успел подключить флешку, запустить с нее «шпиона» и заблокировать рабочую станцию, с тем, чтобы вернувшийся с чашкой кофе хозяин компьютера ничего не заподозрил.

Установленный «шпион» в дальнейшем никак себя не проявляет, максимально маскируя свое присутствие на компьютере «жертвы». Он практически не определяется штатными средствами и может «жить» на чужом ПК сколь угодно долго. Даже если «хозяин» регулярно обновляет антивирусную базу (что на практике случается довольно редко), из-за большого количеством модификаций такого класса программ лишь очень малая их часть обнаруживаются локально установленными антивирусами.

Другой возможный путь заражения компьютера «шпионом» – это электронная почта и интернет. Имеющиеся в практически любом современном программном обеспечении уязвимости позволяют

«заразить» компьютер даже при простом посещении сайта без скачивания и установки чего-либо. Эффективно борются с такими угрозами буквально считанные единицы шлюзовых решений для фильтрации и очистки трафика. Все остальные пользователи, а особенно домашние, если их провайдер не предлагает услугу «чистый интернет», подвергаются риску при посещении даже самых привычных сайтов. Современные хакеры нередко взламывают благонадежные сайта (новостные или спортивные) и «заряжают» их, успешно обманывая те «наивные» средства обеспечения интернет-безопасности, которые основаны на простой URL-фильтрации. Сегодня сайт «чист» с точки зрения наличия активного вредоносного контента, а завтра - уже кишит spyware.

На сайтах многих банков можно встретить так называемые виртуальные клавиатуры, которые позволяют без нажатий клавиш, щелкая мышкой по нарисованной на экране клавиатуре, ввести пароль. Действительно, классические шпионы и трояны-перехватчики становятся бессильны против такого механизма ввода пароля, однако современные продукты злодейской мысли уже давно научились распознавать текущий открытый сайт и при необходимости делать скриншоты части экрана вокруг курсора мыши при нажатии на ее левую кнопку.

Всю собранную за время своей работы на зараженном компьютере информацию шпион может пересылать по протоколам электронной почты или через сеть Интернет своему хозяину. Это позволяет в удаленном режиме собирать всю пользовательскую информацию, просто заманив человека на специально подготовленный сайт. И никакого физического доступа! После сбора нужных паролей можно опять же в удаленном режиме аккуратно удалить все следы присутствия злонамеренного кода на ПК для уменьшения риска своего раскрытия. Вот и все.

Среди пользователей, озабоченных проблемами безопасности собственных паролей, широкую популярность получили приложения, позволяющие хранить логины и пароли на внешних носителях - USB-флеш накопителях или, что более безопасно, смарт-картах и USB-ключах с чипом смарт-карты. Такой подход не требует от пользователя ввода пароля ни с реальной, ни с виртуальной клавиатуры, позволяя автоматически подставлять их в нужные поля браузера или Windows-приложения. Хранение пароля на внешнем носителе позволяет использовать длинные и сложные пароли, которые даже не нужно запоминать.

К большому сожалению пользователей и радости злоумышленников, самые продвинутые современные кейлоггеры могут подключаться, например, к процессу Internet Explorer и получать пароли непосредственно из поля ввода. В этом случае пароль будет украден даже несмотря на то, что он не был введен с клавиатуры. Другие браузеры и приложения также подвержены такому типу атак.

ЕСТЬ ЕЩЕ НАДЕЖДА НА СПАСЕНЬЕ

Прочитав все вышеперечисленное, могло сложиться впечатление, что ситуация с компьютерной безопасностью просто ужасающая, однако на самом деле не все так

страшно, и выход есть. Для преодоления всех ухищрений компьютерных мошенников и повышения безопасности своих данных на сегодняшний день уже существуют надежные средства, о которых мы расскажем во второй части нашего повествования.

ОТКРОЙТЕ, ЭТО СВОИ!

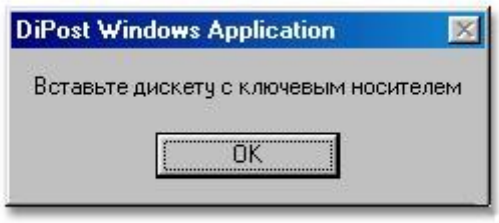
Токены

В настоящее время в западных компаниях, а в последнее время и в российских организациях широкое распространение получили персональные аппаратные средства аутентификации. Это небольшие по размеру устройства, которые позволяют пользователю получать доступ к информационным системам с локального рабочего места или удаленно с использованием подключения к сети интернет. Такие устройства принято называть **токенами** (от английского token – метка, жетон, ярлык).

Принципы, лежащие в основе процедуры аутентификации с использованием токенов, могут быть самыми различными: одноразовые пароли, цифровые сертификаты, хранение в памяти устройства паролей и ключей шифрования и т.п. Кроме того, и сами токены различаются по внешнему виду и могут использоваться по-разному в зависимости от конкретных бизнес-потребностей. Например, для контроля доступа в помещение и к компьютерным ресурсам используется токен в формате смарт-карты с имплантированной RFID-меткой. На поверхность смарт-карты могут быть нанесены идентификационные данные – ФИО, место работы, должность. На рабочем месте для такой карты понадобится специальный считыватель – ридер для смарт-карт.

Не требуют считывателя USB-устройства – они подключаются напрямую к USB-порту, затем пользователь вводит свой PIN-код и происходит аутентификация. Мы еще вернемся к вопросу самой технологии чуть позже, в разделе «**Двухфакторная аутентификация**», а здесь отметим лишь, что с использованием токена можно обеспечить безопасный доступ в удаленном режиме, даже тогда, когда возможности подключить устройство попросту нет.

Не останавливаясь в рамках статьи на описание самих механизмов работы, сформулирую основное требование к этим устройствам: невозможность создания за разумные деньги и время дубликата.



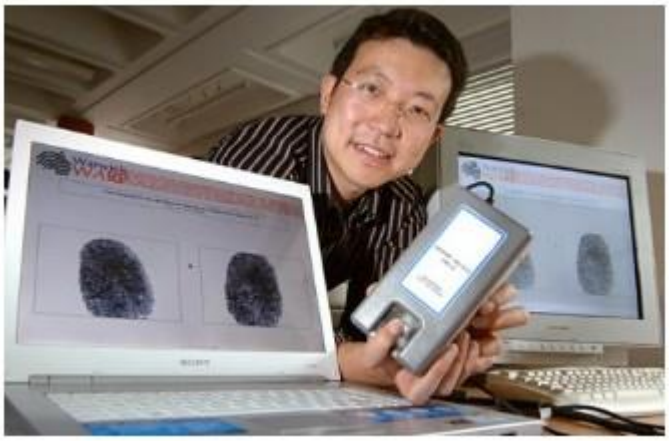
Действительно, использование для доступа к клиент-банку «ключевой дискеты» архаично не только из-за практически полного выхода из обихода 3,5” дисководов, но и по причине простоты изготовления копии такого «токена». USB-флешки в этом смысле от дискет тоже ушли не далеко. Пожалуй, наиболее безопасным на сегодняшний день является использование смарт-карт и USB-ключей с чипом смарт-

карты. Именно эти аппаратные средства аутентификации и стали стандартом де-факто для многих зарубежных и российских компаний.

Кстати, в разделе «**Реквием по паролям**», посвященном паролям, не был отмечен еще один их важный недостаток: кражу пароля нельзя заметить. Это позволяет злоумышленнику безнаказанно читать, например, всю электронную почту жертвы или отслеживать финансовые транзакции при работе в системе интернет-банкинга, оставаясь не пойманным длительное время. Кражу или потерю токена заметить легко, а значит легко и заблокировать доступ к системе по факту утраты устройства.

ВСЯ ПРАВДА О БИОМЕТРИИ

Режиссеры современных фильмов очень любят для создания атмосферы полной секретности какой-нибудь очередной военной базы или исследовательской лаборатории снабдить их биометрическими системами контроля доступа. Хотя такие системы в тех же фильмах периодически обманываются имитаторами голоса, «силиконовыми» пальцами и отрубленными головами, широко распространено мнение, что биометрия – это очень надежно и безопасно.



Созданный имидж, к сожалению, ничего общего с реальностью пока не имеет. Один из немногих плюсов биометрии – это удобство использования. То, что аутентифицирует пользователя в биометрической системе, всегда находится вместе с ним (действительно, сложно забыть свой палец дома или потерять сетчатку глаза). Этот плюс одновременно является и минусом – биометрическую характеристику нельзя запереть в сейф в конце рабочего дня, как это можно сделать, например, со смарт-картой. Постоянное нахождение аутентификатора в недоверенной среде (кафе, бары, дискотеки – в зависимости от пристрастий носителя) является серьезным риском.

Важно также понимать, что биометрия не является строгим методом аутентификации. Два отпечатка одного и того же пальца будут немного, но отличатся из-за влияний внешней среды (жарко или холодно), состояния человека и т.д. Для успешного прохождения аутентификации достаточно частичного совпадения полученного отпечатка с эталонным, например, на 90%. Таким образом, биометрия является вероятностным методом аутентификации, так как всегда есть некая вероятность как ложного срабатывания (постороннего приняли за легального сотрудника), так и ложного несрабатывания (лицо загоревшего и поправившегося в отпуске пользователя не совпадает с его двухнедельной «фотографией»).

При доступе к конфиденциальным данным вряд ли стоит руководствоваться вероятностным подходом: ведь никто не

будет разрешать вход в систему, если пароль будет верен, например, только на 90%.

Если же говорить про удаленный доступ, то биометрическая аутентификация становится совершенно бесполезной. Современные технологии не позволяют (и вряд ли когда либо смогут) передать по сети интернет сетчатку глаза или отпечаток пальца. На сервер отправляется оцифрованная информация, полученная с соответствующего биометрического сканера. Понятно, что злоумышленнику без разницы, что перехватывать - пароль или цифровую последовательность. И то и другое можно будет впоследствии легко использовать для повторного входа в удаленную систему.

«ГДЕ ЖЕ ТЫ, ГДЕ?...»

Многие современные сайты крупных производителей автоматически определяют по IP-адресу страну своего очередного посетителя и предлагают ему интерфейс на родном языке, а пользователям поисковых систем удобно, когда им автоматически предлагается поиск по сайтам их родного государства.

К сожалению, использовать эту информацию для аутентификации пользователя при доступе к конфиденциальной информации вряд ли стоит. IP-адрес можно легко поменять – в интернете за несколько минут можно найти сотни «анонимайзеров» - анонимных прокси-серверов, позволяющих скрыть реальный IP-адрес, а MAC-адрес сетевой карты (который по идее должен быть уникальным) можно поменять даже без перезагрузки компьютера.

Более-менее достоверно узнать местонахождения человека на сегодня позволяют спутниковые системы навигации и (с гораздо большей погрешностью) метод определения координат по ближайшим базовым станциям сотового оператора. Это удобно пользователям, которые могут узнать расположение ближайших заведений и предприятий той или иной категории, но мало помогает компаниям, обеспечивающим аутентификацию при удаленном доступе.

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Для повышения общей безопасности в современных системах используется многофакторная аутентификация, то есть пользователь предъявляет системе два разных аутентификатора. Важно, чтобы при этом они были основаны на разных методах. К примеру, ввод двух паролей не является двухфакторной аутентификаций, по сути это один пароль, только разбитый на две части.

Среди всех возможных комбинаций факторов аутентификации наибольшую популярность получила комбинация аппаратного устройства (токена) и пароля (PIN-кода). Второй фактор позволяет не переживать при утрате самого устройства – воспользоваться им злоумышленник не сможет. Конечно, нельзя исключать возможность

компрометации сразу двух факторов, но вероятность такого исхода, конечно, существенно меньше, чем при использовании только одного из них.

Токены в форм-факторе смарт-карты, требующие для доступа к содержимому их памяти ввода секретного пароля, широко распространены за рубежом. Их используют крупные и средние компании, учебные заведения, государственные организации для проверки пользователей обращающихся к информационным ресурсам.

Появившиеся на рынке чуть позже и запатентованные компанией **Aladdin Knowledge Systems** USB-ключи, совмещающие в себе чип смарт-карты и миниатюрный карт-ридер, на практике оказались удобнее в повседневном использовании, ведь для их подключения не требуется приобретать считывателей смарт-карт (карт-ридеры). Рынок аппаратных токенов формировался в то время, когда USB-ключи уже были широко известны и доступны, именно поэтому в нашей стране смарт-карты менее популярны, хотя для нанесения на них изображения (например, фотографии сотрудника) они, конечно, удобнее.

Токены для аутентификации (в частности, реализованные на основе смарт-карт) позволяют генерировать и хранить ключи шифрования, обеспечивая тем самым строгую аутентификацию при доступе к компьютерам, данным и информационным системам. Чаще всего, создание инфраструктуры токенов в информационной системе какой-либо компании является платформой для дополнительных защитных мер, таких как безопасный доступ к базам данных, порталам, обеспечение контроля физического доступа и контроля доступа к приложениям. Благодаря своим функциям защиты электронные ключи могут использоваться для развертывания самых различных систем безопасности (в том числе и на основе PKI – инфраструктуры открытых ключей) и обеспечивают максимальную масштабируемость, а, следовательно, гибкость внедрения таких решений.

Широкому распространению, в том числе на российском рынке, токены обязаны своей много функциональности. Один токен можно использовать для решения целого ряда различных задач, связанных с шифрованием пользовательских данных, электронной цифровой подписью документов и аутентификацией самого пользователя. С одной и той же смарт-картой сотрудник может входить в Windows, участвовать в защищенном информационном обмене с удаленным офисом (например, с помощью VPN), работать с web-сервисами (технология SSL), подписывать документы (ЭЦП), а также надежно сохранять закрытые ключи и сертификаты в памяти своего токена.

эпилог

Рассмотренные вопросы лишь частично освещают все многообразие средств и методов аутентификации, так или иначе применяемых в наши дни. Поэтому в ближайшее время ждите продолжений, в которых постепенно будут раскрыты все детали и нюансы конкретных технологий и аппаратных устройств.