ОСОБЕННОСТИ ПРОЦЕССОВ АУТЕНТИФИКАЦИИ В КОРПОРАТИВНОЙ СРЕДЕ

ПАРОЛЬНЫЕ ВОЙНЫ

Специалисты по информационной безопасности уже давно твердят о том, что парольная аутентификация - это самый ненадежный и уязвимый способ проверки подлинности пользователя. Любопытное исследование было проведено в школе усовершенствования командного состава ВМС США. Среди слушателей и профессорско-преподавательского состава наиболее распространенным для использования оказался 6-символьный пароль. Исследователи провели программный эксперимент по подбору пароля путем простого перебора и выяснили, что 6-символьные пароли подбираются примерно за 6 дней непрерывной работы компьютера, 8-символьные - примерно за 80 дней для английского языка и до 110 дней для русского. Интересный момент: при использовании заглавных букв приведенные цифры можно умножить еще на 2. Добавим к этим данным год исследования -2003, ресурс для исследования -процессор Pentium 166 и скорость подбора паролей 6000-15 000 в минуту. Проецируя ситуацию на сегодняшний день, можно сделать весьма неутешительные выводы. Технологии ушли далеко вперед, скорости возросли в несколько раз, а люди в большинстве своем по-прежнему в качестве паролей используют имена своих собак.

Компания Symantec и он-лайн-сервис сравнения цен moneysupermarket.com провели акцию-опрос в лондонском районе Covent Garden в сентябре 2008 г. Из 207 человек, заинтересовавшихся акцией, 60% были готовы обменять данные о своем пароле на подарочный купон moneysuper-market.com стоимостью 5 фунтов. Когда участники опроса сообщили свои пароли, оказалось, что 45% из них использовали для доступа к электронной почте, социальным сетям и даже финансовым сайтам пароли, состоящие из даты рождения, девичьей фамилии матери и клички своего домашнего животного.

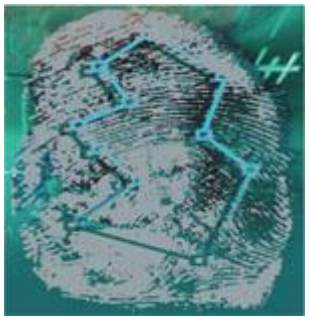
Однако справедливости ради заметим, что пароли тоже могут быть надежными. Скажем, подбор пароля из 47 случайных цифр, символов, строчных и прописных латинских букв по сложности сопоставим со взломом 256-битного ключа современного алгоритма шифрования. Вот только вряд ли найдется много людей, способных запомнить хотя бы два-три таких пароля, а ведь пользователи зачастую работают с еще большим количеством информационных систем и приложении, и при этом в каждом случае требуется свой пароль.

Естественное желание офицеров безопасности ужесточить парольную политику на практике приводит к тому, что пользователи записывают свои пароли и нередко хранят их, например, приклеенными на стикере к обратной стороне клавиатуры. Как показало исследование Aberdeen Group, в 52% компаний для доступа к информации требуется простое сочетание "логин-пароль", при этом пользователи не относятся к паролям должным образом. "...Именно "человеческий фактор" при работе с паролями делает данную методику морально устаревшей и недопустимой в качестве основной при аутентификации пользователей" - делается вывод в исследовании.

Политика информационной безопасности требует менять пароль не реже раза в месяц, кроме того, длина пароля должна быть минимум 8 символов. Каждый месяц запоминать новый 8-символьный случайный пароль не так просто. Очередной раз забыв нужную комбинацию, пользователи звонят администратору с просьбами "сбросить" пароль. Для минимизации уязвимостей этого процесса с точки зрения безопасности приходится усложнять данную процедуру. Во многих компаниях простого звонка пользователя недостаточно: требуются подписанные служебные записки и/или личный визит администратора сети на рабочее место сотрудника. Такие усложнения неизбежно ведут к дополнительным расходам ресурсов.

Аргумент в пользу бесплатности паролей на деле не выдерживает критики. Согласно исследованию Burton Group, любое обращение в службу технической поддержки обходится компании в $25-50, причем 35-50% из этих обращений связаны с утерей паролей1. Если учесть еще и задержку в рабочем процессе, связанную с утратой пароля, то ущерб становится очевидным.

КРИМИНАЛИСТИКА В БЫТУ



В современные ноутбуки все чаще встраивают сканеры отпечатков пальцев. Биометрия -относительно новая технология в области ИБ. На практике крупных серьезных внедрений биометрии в корпоративной среде единицы. Биометрические системы довольно дороги, кроме того, не стоит сбрасывать со счетов и морально-нравственные аспекты: сотрудник, меняющий место работы, не обязательно будет безучастен к своему оставляемому прежнему начальству "цифровому клону".

Однако главным недостатком биометрии является вероятностный подход к определению личности. Отпечаток пальца сравнивается с эталонным на "похожесть", и всегда есть вероятность того, что один человек окажется "похожим" на второго, или же подлинник окажется "не похож" сам на себя (например, вследствие химического ожога пальца).

Не так прост вопрос и с централизованным хранением биометрических характеристик сотрудников - в свете Федерального закона "О персональных данных" стоимость работ по обеспечению безопасности такой базы данных вполне может оказаться не намного меньше стоимости внедрения самой системы биометрической аутентификации.

Наиболее удобным в биометрии является невозможность забыть свой фактор аутентификации дома. С другой стороны, постоянное нахождение важного элемента безопасности в недоверенной среде является серьезной уязвимостью: оставляемые человеком отпечатки пальцев могут быть доступны злоумышленникам.

АППАРАТНАЯ АУТЕНТИФИКАЦИЯ

Неудобство биометрии и уязвимость паролей стали одной из предпосылок появления альтернативного метода аутентификации с помощью электронных ключей - USB-токенов или смарт-карт, которые используются сегодня во многих крупных организациях коммерческого и государственного секторов во всем мире. В основе их применения лежит использование криптографии с открытым ключом, а сам подход называется строгой двухфактор-ной аутентификацией. Строгость аутентификации достигается с помощью шифрования: в математических преобразованиях вероятности не используются, результат аутентификации может быть только однозначным: либо да, либо нет. Двухфакторность же обеспечивается тем, что для доступа в сеть или к какому-либо информационному ресурсу от сотрудника требуется подключить само устройство к компьютеру и ввести PIN-код от него.

Для управления жизненным циклом аппаратных средств аутентификации, в крупных организациях насчитывающих десятки тысяч, используются специальные системы класса Token Management System, что упрощает процесс управления токенами в масштабах предприятия путем автоматизации ряда администраторских функций и типовых операций для средств аутентификации.

Кроме того, средства аутентификации нередко интегрируются в информационных системах с системами контроля и управления физическим доступом (СКУД). Достигается это имплантацией внутрь устройств RFID-меток.

УДАЛЕННЫЙ ДОСТУП

Каждая компания выбирает свой подход к обеспечению безопасности. Есть примеры решения проблемы удаленного доступа радикальным методом: он просто-напросто запрещен. Конечно, это самый эффективный способ защиты, однако на рынке, полном конкурентов, позволить себе такой подход могут немногие. Сотрудники должны иметь возможность работать в любое время в любом месте, и проблема аутентификации при обеспечении безопасности удаленной работы занимает сегодня одно из центральных мест.

По мнению автора, наиболее надежным способом аутентификации при мобильном доступе, в том числе из недоверенной среды, является использование токенов. Передаваемые по сети в открытом виде пароли могут быть перехвачены злоумышленником и повторно использованы без ведома самого пользователя. Биометрические характеристики, считанные локально установленным сканером и отправленные на сервер аутентификации, с точки зрения перехвата ничем не отличаются от паролей. И пароль, и биометрия при удаленном доступе могут выступать лишь как часть системы обеспечения безопасности аутентификации пользователей.

Реализованные в современных токенах аппаратные криптографические алгоритмы позволяют бороться с потенциальными злоумышленниками, прослушивающими трафик между рабочим местом пользователя и удаленным сервером (так называемая атака "человек посередине"), и обеспечивают достаточно высокий уровень безопасности и когда есть возможность подключения USB-устройства, и когда его нет. В последнем случае используются автономные генераторы одноразовых паролей (OTP - One Time Password).