УДК 004.056.53

студентка К.В. Григорьева
ГВУЗ «Национальный горный университет»

ТОКЕН – АЛЬТЕРНАТИВА ПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ

В работе рассмотрены проблемы использования паролей на предприятиях и преимущества внедрения токенов как альтернативного метода аутентификации.

Как это ни парадоксально звучит, парольная защита является одним из самых дорогих в эксплуатации способов аутентификации. Казалось бы, наоборот, система защиты встроена в ОС, никаких дополнительных затрат не нужно. Но обслуживание и сопровождение парольной защиты отнимает много времени у сотрудников компании, ответственных за работоспособность информационной системы. Им необходимо регулярно проводить аудит паролей пользователей, консультировать по правилам выбора и хранения паролей, производить замену паролей для профилактики, а также в случае их утери или забывчивости пользователей. Все это требует времени и ресурсов, причем немалых. Исследования Gartner показывают, что от 10 до 30 % звонков в службу технической поддержки компании – просьбы сотрудников восстановить забытые ими пароли.[1]

Обычные статические пароли не являются надежным средством безопасности, даже при соблюдении строгих правил их использования. Ведь "строгая" аутентификация означает необходимость обеспечения невозможности симуляции личности и действий от ее имени, т.е. входа в информационную систему и работу в этой системе. Главное преимущество паролей в простоте их использования. Однако, такие вопросы как забывчивость, передача по незащищенным каналам, набор пароля на клавиатуре, перехват по сети, программы вычисления зашифрованных паролей, их подбора, предсказуемость и т.д. ставят под сомнение некоторые важные с точки зрения безопасности операции.

Если сравнивать пароль с криптографическим ключом, то выводы напрашиваются весьма неутешительные. В ГОСТ 28147-89 длина ключа составляет 256 бит (32 байта). При использовании генератора псевдослучайных

чисел, ключ обладает хорошими статистическими свойствами. Пароль же, который является, например, словом из словаря, можно свести к псевдослучайному числу длиной 16 бит, что короче ГОСТ-ового ключа в 16 раз.

Логичное решение этой проблемы – использование одноразовых паролей, выдаваемых без использования компьютеров, входящих в информационную систему. Такой пароль весьма надежен – устройство, выдавшее его (токен), должно быть зарегистрировано в этой системе, для его использования требуется ввод пин-кода, а сам пароль зависит от нескольких факторов – как правило, от времени создания и происходивших в системе событий (ранее выданных паролей). Токен имеет постоянную виртуальную связь с защищаемой информационной системой; можно сказать, что они постоянно синхронизированы при помощи нескольких внутренних и внешних процессов. Внутри устройства находится шифровальная машина DES или 3DES (TripleDES), отвечающая за генерацию паролей и сигнатур (например, цифровых подписей). Подделка пароля и неавторизованный вход в систему становятся крайне трудновыполнимыми задачами, защита транзакций от перехвата также существенно повышается.

Первоначальная функция токенов – это не извлекаемое хранение ключевой информации. Ключ из токена никогда не попадает никуда извне, например, в оперативную память компьютера. Данную строгую политику можно ослабить до того, что разрешается экспорт ключа из токена в оперативную память только в зашифрованном виде. Также существует опция экспорта ключа в открытом виде. Но даже при выборе владельца токена использовать только эту опцию, уровень безопасности все равно выше, чем хранение ключа на обычной флэшке. Выше он потому, что для экспорта ключа требуется знание PIN-кода, а для копирования ключа с флэшки PIN-код не требуется. Можно хранить ключ на флэшке и шифровать его паролем при помощи, например, RAR. Но, чтобы перебрать все пароли к архиву у нарушителя будет сколь угодно большое

количество попыток, а токен после трех последовательных попыток ввода неверного PIN-а блокируется. Вывод: даже при самых скромных настройках безопасности хранить ключ на токене безопаснее, чем на флэшке. [2]

У USB-токенов есть и другие достоинства. Во-первых, они позволяют следить за активностью пользователя на протяжении всего сеанса работы, а не только на этапе аутентификации. Это позволяет получать более детальные данные о действиях пользователя и ограничить доступ к запрещенным ресурсам. Во-вторых, возможность использования различных кодов позволяет администраторам более гибко управлять доступом к файлам и приложениям.

Несмотря на то, что токены содержат полный арсенал криптографических операций, достаточно сложных для понимания большинством пользователей, само применение токена не представляет особого труда и интуитивно понятно. Токен действительно не требует от пользователя специальных профильных знаний и глубокого понимания заложенных в него механизмов. И он потенциально способен прийти на смену паролей и всего, что с ними связано.

Перечень литературы:

1. http://www.aladdin-rd.ru/press/publications/detail.php?ID=20823
2. http://habrahabr.ru/blogs/infosecurity/126828/