М. А. Стюгин, *канд. техн. наук, ФГАОУ ВО «Сибирский федеральный университет», г. Красноярск, styugin@gmail.com*

Метод аутентификации с использованием динамических ключей[1]

Многоразовые пароли — самый популярный способ аутентификации на сегодняшний день, однако при этом — самый небезопасный. В данной работе представлен метод аутентификации с использованием многоразовых паролей, существенно усложняющий реализацию атак, следствием которых является получение информации, достаточной для подбора паролей. Суть метода — «размывание» пароля пользователя на множестве узлов в сети.

Ключевые слова: аутентификация, многоразовые пароли, хеш-функция, хранение пароля, разделение секрета.

Введение

Данное исследование посвящено одной из наиболее насущных тем в области информационной безопасности — сохранности паролей пользователей от утечки с удаленных сервисов. С компрометацией паролей сталкивался практически каждый пользователь Интернета. Для защиты паролей от кражи непосредственно с базы данных ресурсов используют однонаправленные криптографические хеш-функции. Используя полученный хеш, мы не можем получить исходный пароль путем вычислений. Однако, используя хеш, возможно подобрать пароль, и это создает потенциальную уязвимость. Для того чтобы максимально усложнить процесс подбора, используются различные методы, которые можно обозначить тремя основными направлениями.

1. Использование хеш-функций, требующих большего вычислительного ресурса и большего объема памяти. Это требует от злоумышленника больших временных затрат на перебор паролей.

2. Использование «соли», добавляемой к тексту пароля до вычисления хеша. Применение «соли» затрудняет массовый подбор паролей с использованием одной хеш-функции и вынуждает подбирать каждый пароль в отдельности.

3. Использование паролей с высокой энтропией. Пароли с низкой энтропией быстро подбираются «по словарю» в соответствии с многочисленными правилами компоновки и преобразования. Высокоэнтропийные пароли, состоящие из случайной комбинации символов и знаков, не дают какой-либо информации, определяющей пространство перебора, и вынуждают злоумышленника проводить тотальный перебор всех комбинаций.

Применение всех перечисленных методов не обеспечивает приемлемой защиты, кроме того, создает дополнительные неудобства для пользователей и дополнительную нагрузку на вычислительные ресурсы.

В данной работе мы представим метод аутентификации с использованием многоразового пароля, позволяющий не опираться на стойкость хеш-функций или шифрования паролей. Реализация предложенной технологии — алгоритм DKAuth. Сам проект является открытым и выложен на сайте

[1] Работа поддержана грантом Президента Российской Федерации МК-5025.2016.9.