УДК 004.056.5(076.5)

А.В. КОЗИКОВ, ст. викладач, Д.І. ДВИГУН, студент,
Криворізький національний університет

СТАНДАРТ БЕСПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ WEBAUTHN КАК РЕШЕНИЕ ПРОБЛЕМЫ ЗАЩИТЫ ДАННЫХ В СЕТИ

В связи с растущим развитием IT-технологий в мире, увеличивается количество аккаунтов у пользователей, а это влечет за собой увеличение личной информации пользователей в сети. Общение между людьми практически полностью перешло в интернет. В связи с этим одной из важнейших задач в информационных технологиях на данный момент, является защита персональных данных, которые пользователи оставляют в своих аккаунтах разных сервисов, в личных переписках и т.д.

Традиционная аутентификация пользователя через логин и пароль используется уже долгое время и все еще остается наиболее популярным методом, несмотря на то, что появляются новые современные подходы, например, сканеры отпечатков пальцев или системы распознавания лиц. Однако пароли не в состоянии обеспечить должную защищенность конфиденциальной информации. Около 80% взломов учетных записей связаны со слабыми паролями или их кражей. Пользователи не в состоянии запоминать большое количество комбинаций паролей, которые для каждого сервиса в сети, могут иметь свои правила. Это влечет за собой то, что пользователи используют один и тот же пароль для разных сервисов или делают их слишком простыми для лучшего запоминания.

Одним из решений данной проблемы может быть недавно принятый стандарт беспарольной аутентификации. Идея состоит в том, чтобы не хранить конфиденциальные данные пользователей (например, пароли), а просто подтверждать их, используя смартфоны или ключи обеспечения безопасности. Это позволит отказаться от уязвимостей аутентификации с помощью паролей и повысить безопасность пользователей при работе в интернете.

Web Authentication является веб-стандартом, разработанным Консорциумом Всемирной паутины (W3C) и Альянсом FIDO. Этот стандарт призван решить все проблемы с традиционной аутентификацией.

Криптографические учетные данные FIDO уникальны для каждого веб – сайта, личные данные пользователя, такие как пароль или логин, не покидают устройства пользователя и не сохраняются на сервере. Это устраняет риск любых видов краж паролей.

Вход в систему осуществляется с помощью удобных пользователю методов, сканер отпечатков пальцев, камеры, ключ безопасности FIDO или смартфон.

Ключи FIDO являются уникальными для каждого интернет-сайта, благодаря этому нет возможности отслеживать пользователя на разных сайтах.

WebAuthn состоит из 3 основных компонентов: веб-сайт, веб-браузер, аутентификатор. Аутентификатор представляет из себя совокупность средств и методов, с помощью которых можно идентифицировать аккаунт без ввода персональных данных.

Во время аутентификации WebAuthn показывает верификатору, на то, что у пользователя имеются все данные, которые позволяют подтвердить его личность согласно протоколу FIDO.

Ключ безопасности FIDO в настоящее время обычно представляет из себя USB-накопитель, который можно подключить к устройству. При входе на web-страницу, браузер должен проверить вставлен ли ключ в устройство. Если ключ обнаружен, пользователь войдет в учетную запись точно так же как делал бы это с помощью пароля.

Таким образом этот стандарт может обеспечить простую и надёжную аутентификацию в сервисах. Эта аутентификация унифицированная, она не зависит от платформы, сервиса или браузера. Технология WebAuthn уже получила поддержку в операционных системах Windows 10 и Android, а также в браузерах Google Chrome. Отныне она объявлена официальным стандартом для всемирной паутины, что должно обеспечить её использование вместо паролей.

Список літератури

Web Authentication Working Group [електронний ресурс] Режим доступу : www/ URL: https://www.w3.org/blog/webauthn/ – 28.03.2019 г. – Загол. з екрану.