Представлен новый релиз OpenSSH

Разработчики программного пакета OpenSSH представили релиз OpenSSH 8.2. Главным нововведением в последнем выпуске стала возможность использования двухфакторной аутентификации при помощи устройств, поддерживающих U2F-протокол.

U2F представляет собой открытый, бездрайверный протокол для двухфакторной аутентификации, основанный на вызов-ответной аутентификации, позволяющий пользователям использовать устройство с поддержкой U2F как второй фактор для аутентификации на большом количестве online-сервисов.

Для взаимодействия с подобными устройствами в OpenSSH добавлены новые типы ключей «ecdsa-sk» и «ed25519-sk», использующих алгоритмы цифровой подписи ECDSA и Ed25519, в сочетании с хэшем SHA-256. Процедуры взаимодействия с токенами вынесены в промежуточную библиотеку, которая загружается по аналогии с библиотекой для поддержки PKCS#11 и является обвязкой над библиотекой libfido2, предоставляющей средства для коммуникации с токенами поверх USB.

Также при генерации и аутентификации ключей необходимо локальное подтверждение физического присутствия пользователя. Например, от пользователя потребуется коснуться сенсора на токене, усложняя осуществление атак на системы с подключенным токеном для удаленных злоумышленников. На этапе запуска ssh-keygen есть возможность задать пароль для доступа к файлу с ключом.

В числе прочих изменений были добавлены новые директивы «Include» и «PubkeyAuthOptions» в файл настроек sshd_config, новые опции «-O write-attestation=/path» и «no-touch-required» в ssh-keygen, добавлен новый исполняемый файл ssh-sk-helper и пр.

Источник: https://www.securitylab.ru/news/505092.php