УДК 004.6

ПРОТОТИП ПРИЛОЖЕНИЯ, ЗАЩИЩАЮЩЕГО ДАННЫЕ С ПОМОЩЬЮ ПРОТОКОЛОВ ШИФРОВАНИЯ

А.С. Тимофеев

Аннотация. *Рассмотрен прототип настольного приложения, задачей которого является защита данных посредством протоколов шифрования. Затронуты вопросы безопасного хранения и управления паролями пользователей с помощью менеджера паролей. Указаны подходы к реализации двойной аутентификации на основе аппаратных криптопровайдеров для повышения защиты ключей шифрования.*

Ключевые слова: *менеджер паролей, безопасность данных, шифрование, двухфакторная аутентификация, генерация паролей, хранение паролей, аппаратная аутентификация, криптопровайдеры, протоколы шифрования.*

Окружающий нас мир содержит массу цифровых инструментов и требует от нас постоянного взаимодействия с различными онлайн-сервисами, в том числе социальными сетями, электронной почтой. В силу этого возникает огромная потребность в безопасном хранении и управлении множеством паролей, которые мы используем для доступа к различным ресурсам.

Большинство людей, согласно статистике, применяют простые, короткие пароли, так как они легко запоминаются. Такие пароли таят в себе большую опасность, поскольку злоумышленники прибегают к различным видам атак (например, к brute-force – атаке полным перебором), которые дают доступ к личным данным и наиболее успешны в случае легких, небольших паролей.

Для предотвращения утечки данных и взлома аккаунтов нужно придумывать уникальные и длинные пароли (их сложно запомнить). Здесь на помощь приходят менеджеры паролей. Они обеспечивают высокий уровень безопасности, так как предотвращают несанкционированный доступ.

Однако вышеназванные менеджеры не только гарантируют надежное хранение паролей, но и выполняют ряд других полезных функций. Например, они позволяют генерировать сложные пароли, удовлетворяющие заданным критериям безопасности; осуществляют автозаполнение, избавляя пользователей от необходимости вводить пароли вручную при каждом входе в аккаунт или на интернет-ресурс. Некоторые

менеджеры паролей предоставляют возможность синхронизации данных с серверным облаком, благодаря чему на разных устройствах, применяемых индивидом, обеспечивается доступ к паролям, т. е. не нужно передавать базы данных вручную.

Разработка менеджера паролей с двойной аутентификацией, использующей аппаратную аутентификацию и мастер-ключ на криптопровайдере, решит многие проблемы безопасности хранения и управления паролями. Указанный менеджер станет надежным и удобным инструментом обеспечения безопасности паролей и управления ими [1].

Менеджер паролей является программным приложением, разработанным для защиты паролей от похищения их посторонними лицами [9]. Он позволяет генерировать сложные коды, сохранять их в зашифрованной форме и автоматически вводить в нужные места при необходимости. Как следует из всего вышесказанного, цель менеджера паролей – обеспечение высокого уровня безопасности и удобства использования.

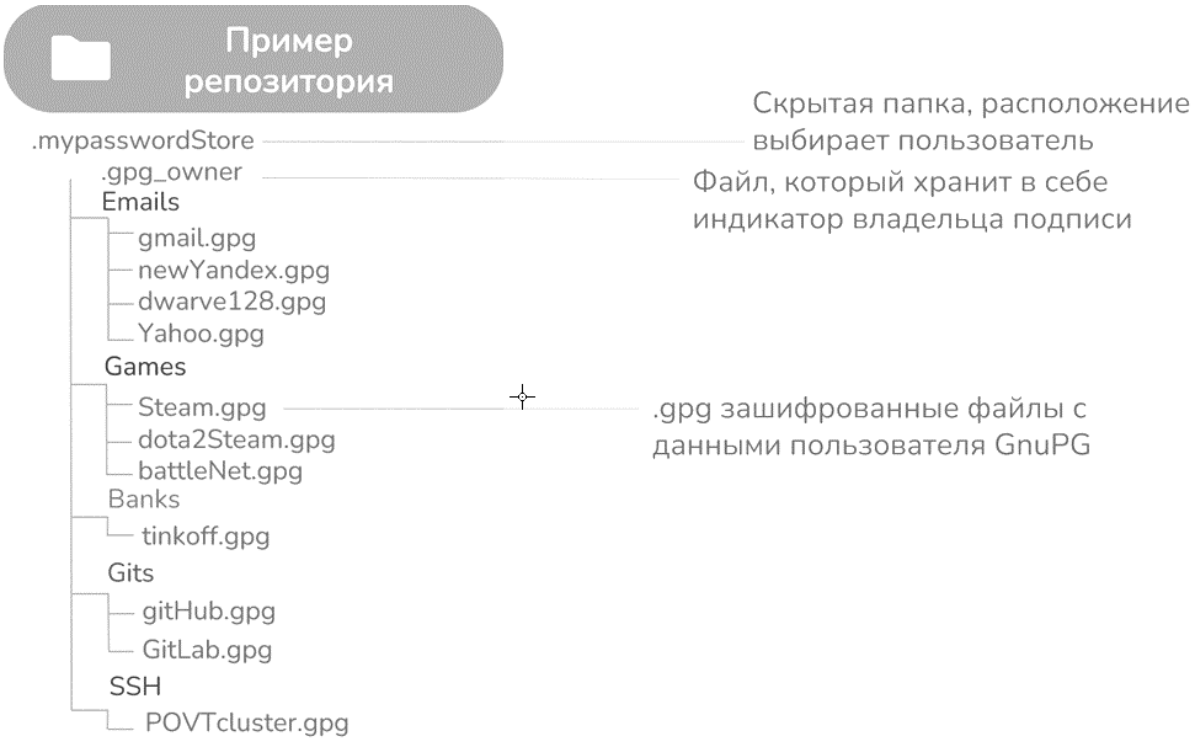
Таким образом, генерация надежных паролей – важный аспект управления ими, т. е. менеджер паролей предоставляет пользователям возможность генерации случайных и «сильных» паролей. Генератор паролей все чаще основан на криптографических алгоритмах, способствующих созданию уникальных и надежных кодов, которые сложно подобрать или угадать [6].

Должны быть учтены аспекты проектирования, обеспечивающие совместимость менеджера паролей с операционной системой Windows:

1. Платформа разработки (она должна поддерживать указанную операционную систему).

2. Интеграция с криптопровайдерами (такими как YubiKey, «Рутокен») для поддержки аппаратной аутентификации, что подразумевает разработку соответствующих модулей для регистрации, опознания и управления аппаратными ключами.

В разработанном прототипе входной информаций для проекта является указание идентификатора подписи владельца. Этот идентификатор необходим при поиске связки ключей в системе (к примеру, в рамках открытого стандарта для криптографических операций OpenPGP). В качестве такого указания может выступать как электронный адрес, введенный при создании подписи, так и уникальный номер, сгенерированный при формировании подписи. Файл с подписью хранится в репозитории пользователя (рисунок), локацию которого можно (при желании) менять.



Пример репозитория для менеджера паролей

Для добавления пароля к репозиторию человек вводит на входе имя файла, логин и пароль. Они вначале обрабатываются в модуле менеджера паролей, затем передаются в модуль криптопровайдера, шифруются, в результате чего в репозитории образуется зашифрованный файл.

Промежуточной информацией является или логин, или пароль, который пользователь запрашивает у менеджера паролей. Порядок операций при этом таков: сначала главный модуль обрабатывает поступившие к нему данные, потом расшифровывает в модуле криптопровайдера и далее предоставляет пользователю расшифрованный контекст в буфере обмена (контекст хранится ровно 30 с, а потом удаляется).

Протокол OpenPGP (сокращение от Open Pretty Good Privacy) обеспечивает шифрование, цифровую подпись и аутентификацию данных. Он поддерживает как симметричное, так и асимметричное шифрование, а также алгоритмы хеширования для генерации цифровых подписей. В менеджере паролей протокол OpenPGP используется для кодирования файлов, защиты логинов и паролей пользователей [1].

«КриптоПРО» является криптографической библиотекой и одновременно набором протоколов для разработки безопасных приложений; обеспечивает шифрование данных, генерацию и проверку цифровых подписей, аутентификацию и другие криптографические операции. «КриптоПРО» применяется для взаимодействия с аппаратным

криптопровайдером и выполнения криптографических операций, связанных со связкой ключей и паролями [3].

Для повышения безопасности менеджера паролей предлагается использовать двойную аутентификацию на основе аппаратной аутентификации связки ключей, которая записана на криптопровайдер. В данном случае криптопровайдер может быть представлен, например, названными выше YubiKey или «Рутокен» [4]. Они обеспечивают дополнительную защиту приватного ключа и реализуют протоколы OpenPGP и «КриптоПРО» для взаимодействия с программным обеспечением [5].

Двойная аутентификация происходит следующим образом:

1. Пользователь генерирует связку ключей, после этого записывает ее на криптопровайдер (например, YubiKey). На криптопровайдере будет находиться как приватный, так и публичный ключ. На персональном компьютере остается только сертификат, который выступает в роли буфера обмена между указанным компьютером и криптопровайдером, дающим возможность получать ключи.

2. Шифруя контекст, программа забирает публичный ключ с криптопровайдера.

3. Расшифровывая контекст, программа забирает приватный ключ с криптопровайдера, при этом она расшифровывается дополнительно ключом аутентификации.

Получается, что оба ключа не хранятся на персональном компьютере, но участвуют в шифровании и расшифровке. Приватный ключ дополнительно защищен ключом аутентификации. Таким образом, двойная аутентификация позволяет защитить связку ключей от несанкционированного взлома сертификата.

Библиографический список

1. OpenPGP [Электронный ресурс]. – Режим доступа: https://securityguide.github.io/personal/level-three/openpgp.html (дата обращения: 20.04.2024).

2. КриптоПРО: официальный сайт [Электронный ресурс]. – Режим доступа: https://www.cryptopro.ru (дата обращения: 20.04.2024).

3. Что такое КриптоПРО и зачем это нужно [Электронный ресурс]. – Режим доступа: https://astral.ru/info/kriptopro/ (дата обращения: 20.04.2024).

4. Рутокен [Электронный ресурс]. – Режим доступа: https://sbis.ru/help/ep/key/rutoken (дата обращения: 22.04.2024).

5. YubiKey: официальный сайт [Электронный ресурс]. – Режим доступа: https://www.yubico.com/products/how-the-yubikey-works/ (дата обращения: 23.04.2024).

6. Random password generator [Электронный ресурс]. – Режим доступа: https://cryptography.fandom.com/wiki/Random_password_generator (дата обращения: 28.04.2024).

7. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001. 190 с.

8. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходный код на С. М.: Диалектика, 2022. 1040 с.

9. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010. 390 p. URL: https://moodlearchive.epfl.ch/2020-2021/pluginfile.php/2319743/mod_resource/content/1/Understanding-Cryptography.pdf (дата обращения: 28.04.2024).

A PROTOTYPE OF AN APPLICATION THAT PROTECTS DATA USING ENCRYPTION PROTOCOLS

A.S. Timofeev

Abstract. *The article is dedicated to the prototype of a desktop application whose task is to protect data using encryption protocols. The issues of secure storage and management of user passwords using a password manager are considered. Approaches to implementing two-factor authentication based on hardware crypto providers to enhance encryption key protection are discussed.*

Keywords: *password manager, data security, encryption, two-factor authentication, password generation, password storage, hardware authentication, crypto providers, encryption protocols.*

Об авторе:

ТИМОФЕЕВ Александр Сергеевич – бакалавр, ФГБОУ ВО «Тверской государственный технический университет», Тверь. E-mail: bluhhar@gmail.com

Научный руководитель – ПРОХНЫЧ Алексей Николаевич, кандидат технических наук, доцент кафедры программного обеспечения, ФГБОУ ВО «Тверской государственный технический университет», Тверь. E-mail: prohnych@yandex.ru

About the author:

TIMOFEEV Aleksander Sergeevich – Bachelor's Degree, Tver State Technical University, Tver. E-mail: bluhhar@gmail.com

Research Manager – PROKHNYCH Alexey Nikolaevich, Candidate of Technical Sciences, Associate Professor of the Department of Software, Tver State Technical University, Tver. E-mail: prohnych@yandex.ru