устройства отключен. В это время операционное система выключает NFC контроллер и HCE сервисы не работают. Однако это можно исправить, прописав необходимые свойства в приложение. После этого при поднесении устройства к NFC считывателю, Android предложит пользователю разблокировать устройства. После разблокировки, появится диалоговое окно для завершения транзакции. Эта мера защиты необходима, т.к. пользователь может подносить мобильное устройство к NFC считывателю случайно, не подозревая об этом, т.к. NFC является бесконтактной технологией [2].

Работа с NFC на персональном компьютере отличается от таковой на операционной системе Android. Если Android эмулирует NFC карты, то программному обеспечению на ПК необходимо производить различные запросы к приложению на мобильном устройстве. Эти запросы должны соответствовать APDU, а данные можно передавать и получать с помощью формата NDEF. Также для организации работы с NFC на компьютере необходимы специальный драйвер и библиотека. Самой популярной библиотекой для работы с NFC на языке Java является nfctools, которая упрощает организацию пиринговой сети с мобильным устройством через NFC.

Технология Near Field Communication (NFC) в настоящее время много где используется и продолжает набирать популярность. Организация взаимодействия мобильного устройства на базе операционной системы Android и персонального компьютера посредством NFC открывает некоторые возможности для упрощения работы устройств между собой, хранения и доступа к данным. Однако существуют некоторые ограничения по организации пиринговой сети с мобильным устройством, например, устройство должно находиться в разблокированном состоянии. Данное ограничение обусловлено в непредумышленном контакте посредством NFC и защите пользовательских данных. В ходе работы были проведены исследования, а также разработано ПО по обеспечению пиринговой сети с помощью технологии NFC между персональным компьютером и мобильным устройством.

ЛИТЕРАТУРА

1. Near Field Communication [Электронный ресурс] – Режим доступа: https://en.wikipedia.org/wiki/Near_field_communication. – Дата доступа: 30.03.2015.
2. Host-based Card Emulation [Электронный ресурс] – Режим доступа: https://developer.android.com/intl/ru/guide/topics/connectivity/nfc/hce.html. – Дата доступа: 28.03.2015.

УДК 004.49

МЕНЕДЖЕР ПАРОЛЕЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ NFC

А.И. СТАТУТ
(Представлено: канд. физ.-мат. наук, доц. О.В. ГОЛУБЕВА)

Для безопасного использования веб-сайтов, где требуется аутентификация, необходимо использовать сложные и длинные пароли, которые трудно запомнить. Исследуются проблемы хранения паролей существующими способами, а также предлагается несколько иной способ хранения и доступа к паролям.

Сейчас глобальная сеть Интернет используется повсеместно. Огромное количество людей посещают миллионы сайтов каждый день. Некоторые сайты для работы с ними требуют пройти аутентификацию пользователей с помощью учетных записи, обычно имя пользователя и его пароля. Однако существует несколько проблем связанных с этим процессом.

В среднем каждый пользователь имеет десятки учетных записей [4]. Запомнить даже несколько различных сложных паролей практически невозможно. Помимо этого, большинство людей используют очень легкие пароли. Также одна из самых серьезных проблем является многократное использование одного пароля, т.к. происходят утечки паролей каждый год на огромном количестве сайтов. Чтобы предотвратить утечку паролей, пользователь должен использовать сложный уникальный пароль на каждом веб-сайте. Однако запомнить все пароли практически невозможно. Для этих целей используются так называемые менеджеры паролей.

Менеджер паролей – программное обеспечение, которое помогает пользователю хранить и организовывать пароли. Менеджеры паролей обычно хранят пароли в зашифрованном виде и требуют у пользователя создать мастер пароль. Мастер-пароль – единый, довольно сложный пароль, который предоставляет пользователю доступ к базе его паролей. Некоторые менеджеры паролей хранят пароли на устройстве пользователя, другие – на своих серверах. Также большинство менеджеров предоставляют дополнительные возможности, например, автозаполнение форм и создание сложных, случайных паролей [3].

Основные ошибки использования и хранения паролей пользователями:

Простые пароли – короткие, которые используют слова из словарей, не используют различные типы символов (цифры, пунктуацию, специальные символы, верхний и нижний регистры) или попросту говоря, являются легко отгадываемыми.

Пароли можно обнаружить – на стикерах на мониторах, в блокноте компьютера, в документе на компьютера, хранящиеся на устройствах в открытом виде и так далее.

Использование одного пароля – использование одного пароля на множестве веб сайтах, никогда не меняя его.

Использование общего пароля – передача пароля другим лицам, пересылка незашифрованных писем с парольной информацией, использование наемными рабочими одного пароля для всех учетных записей.

Обычно пользователи совершают хотя бы одну из этих ошибок. Это предоставляет легкий путь для злоумышленников получить доступ к индивидуальным учетным записям или даже к ресурсам компании. Поэтому использование менеджеров паролей крайне важно.

Менеджеры паролей также могут быть использованы для защиты против фишинга. Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям [5]. В отличие от человека, менеджер паролей содержит автоматизированный скрипт входа, который сравнивает Uniform Resource Locator (URL) текущего сайта с URL сайта, хранимого в базе менеджера. Если они не совпадают, то менеджер паролей автоматически не заполняет веб-форму. Это используется в качестве защиты от визуальных подражаний и похожих друг на друга веб-сайтов [2].

Использование менеджера паролей на переносимом устройстве, в данном случае на смартфоне с технологией Near Field Communication (NFC), дает дополнительные преимущества, такие как: пароли хранятся в зашифрованном виде только в одном месте, к ним не имеют доступа посторонние лица, использовать менеджер паролей можно также для аутентификации не только на веб сайтах, но и для доступа к физическим устройствам (при написании соответствующего программного обеспечения (ПО) для них).

NFC – это технология, позволяющая смартфонам и другим устройствам обмениваться данными по беспроводной высокочастотной связи друг с другом при близком контакте, обычно около десяти сантиметров [1]. Технология NFC используется во многих областях.

Рассмотрим некоторые аналоги. Существует несколько популярных менеджеров паролей, например, LastPass, Dashlane, KeePass, 1Password и RoboForm. 4 из 5 из этих менеджеров являются платными и поставляются с закрытым исходным кодом. Также большинство из них используют свои сервера для хранения паролей, что можно считать существенным минусом. На мой взгляд, лучшим из представленных выше менеджеров паролей является KeePass. Преимуществом разработанного менеджера пароля является то, что его можно использовать не только с браузером и вообще с компьютером, но и с другими устройствами, поддерживающими технологию NFC для аутентификации на них.

В ходе реализации работы были выбраны алгоритмы для защиты данных. Для шифрования данных в менеджере паролей используется симметричный алгоритм блочного шифрования AES (Advanced Encryption Standard). Алгоритм обладает очень высокой защищенностью. Единственный работающий способ взлома шифра AES – это атаки по побочным каналам. Такие атаки не связаны с математическими особенностями AES, а используют определенные особенности реализации систем, использующих шифр, с целью раскрыть частично или полностью секретные данные, в том числе ключ. Также алгоритму присуще очень высокая скорость шифрования. Программная реализация на машине с частотой 2 ГГц позволяет шифровать данные со скоростью 700 Мбит/с.

Для обмена ключами для AES между мобильным устройством и расширением для браузера, используется ассиметричный алгоритм шифрования RSA. RSA – один из наиболее успешных асимметричных алгоритмов шифрования на сегодняшний день. Безопасность RSA основана на математической проблеме факторизации целых чисел. Шифруемое сообщение рассматривается как одно большое число. Во время шифрования оно возводится в степень ключа и делится с остатком на произведение первых двух. Повторяя процесс с другим ключом, можно получить исходный текст.

Для хранения мастер-пароля на мобильном приложении используется алгоритм SHA-2 (Secure Hash Algorithm 2). Хэш-алгоритмы SHA-2 называются безопасными, потому что по заданному алгоритму невозможно вычислить следующее: 1) восстановить сообщение по конкретному дайджесту сообщения, или 2) найти два различных сообщения, у которых один и тот же дайджест сообщения (найти коллизию). Любые изменения в сообщении, с очень высокой вероятностью, приводят к различным хэш-значениям. Это свойство полезно при создании и проверке цифровых подписей, при аутентификации сообщений, при создании случайных чисел.

В ходе работы была исследована проблема надежного хранения паролей от веб-ресурсов. Запомнить все пароли невозможно, а использовать одинаковые небезопасно, наилучшее решение этой проблемы – использование менеджеров паролей. Были проанализированы существующие менеджеры паролей, среди которых выявлены недостатки, например, хранение пользовательских данных на серверах компаний. Разработанный менеджер паролей хранит данные на устройстве пользователя, которое поддерживает технологию NFC, а по запросу, предоставляет эти данные. Аналогов среди менеджеров паролей, использующих данный принцип работы, не существует.

В ходе выполнения работы было проделано следующее:

– исследованы проблемы хранения паролей.

– ознакомление с разработкой для операционной системы Android.

– разработан менеджер паролей на базе операционной системы Android.

– разработан протокол обмена учетными данными между менеджером паролей и другими устройствами.

– разработано программное обеспечение для ПК, поддерживающее протокол обмена данных.

– ознакомление с разработкой расширений для браузера Google Chrome и разработаны расширения, для взаимодействия с приложением на базе ОС Android.

– разработано расширение для браузера Google Chrome, с поддержкой автоматического заполнения веб-форм, а также автоматического извлечения из них учетных данных для последующей передачи их в менеджер паролей.

Таким образом, разработанное ПО можно расширять для использования в других расширениях, а также в других приложениях для ПК. Также менеджер паролей можно использовать с другими устройствами, поддерживающие технологию NFC и протокол обмена данных менеджера паролей. Главным недостатком разработанных приложений является обязательная поддержка на мобильном устройстве и ПК технологии NFC.

ЛИТЕРАТУРА

1. Near Field Communication [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Near_field_communication. – Дата доступа: 30.03.2015.
2. Password manager [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Password_manager. – Дата доступа: 28.03.2015.
3. Should You Use a Password Manager? [Электронный ресурс]. – Режим доступа: http://www.tomsguide.com/us/password-manager-pros-cons,news-19018.html. – Дата доступа: 28.03.2015.
4. Three quarters of Britons risking online safety [Электронный ресурс]. – Режим доступа: https://www.cyberstreetwise.com/blog/three-quarters-britons-risking-online-safety
5. Фишинг [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/фишинг. – Дата доступа: 03.04.2015.

УДК 512.643

О ПРЕДСТАВЛЕНИИ (2 × 2)-МАТРИЦЫ С ПОЛОЖИТЕЛЬНЫМ ОПРЕДЕЛИТЕЛЕМ В ВИДЕ ПРОИЗВЕДЕНИЯ ТРЕУГОЛЬНЫХ МАТРИЦ С ПОЛОЖИТЕЛЬНЫМИ ДИАГОНАЛЬНЫМИ ЭЛЕМЕНТАМИ

В.А. ЗАЙЦЕВ, Д.А. ГОЛУБЕВ
(Представлено: канд. физ.-мат. наук, доц. А.А. КОЗЛОВ)

Одним из основных вопросов теории матриц является задача о факторизации матриц, т.е. о разложении матрицы из некоторого класса матриц в произведение матриц, принадлежащих некоторым (возможно, иным) подмножествам матриц. Рассматривается задача представления квадратной (2 × 2)-матрицы с положительным определителем в виде произведения семи треугольных матриц. Отличительной особенностью найденного разложения от иных и, прежде всего, от LU –разложения, является то, что все матрицы-сомножители в нем имеют положительную диагональ.

Имеет место
Лемма *Для матриц*

$$\alpha := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \beta := \alpha^{\mathrm{T}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma := \alpha^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \tag{1}$$