Все сообщения об ошибках корректно отображаются в диалоговых окнах (рис. 14).

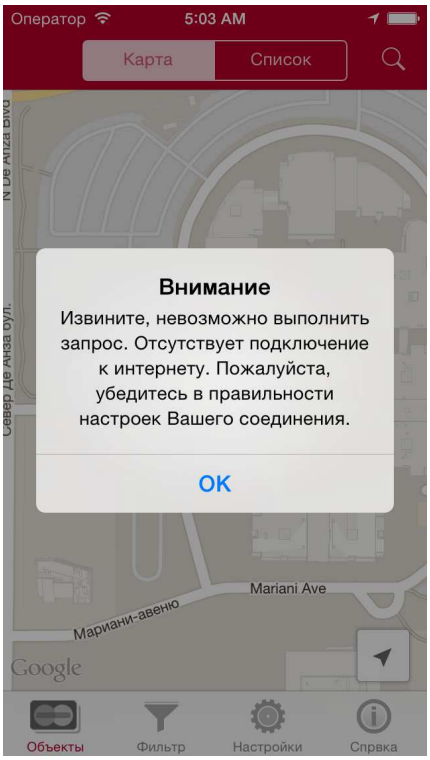

Рис. 14. Отображение сообщений

В статье подробно рассмотрен пользовательский интерфейс мобильного приложения под ОС Apple iOS для отображения объектов Московского кредитного банка, а так же сценарий действий пользователя. Приведены подробные иллюстрации игрового интерфейса.

УДК 004.42

ВЗАИМОДЕЙСТВИЕ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА И МОБИЛЬНОГО УСТРОЙСТВА НА БАЗЕ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID ПОСРЕДСТВОМ ТЕХНОЛОГИИ NFC

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

Произведены исследования организации взаимодействия персонального компьютера и мобильного устройства на базе операционной системы Android с современной технологии близкого контакта NFC. Исследованы протоколы взаимодействия и формат передаваемых данных, а также организация пиринговой сети между ПК и мобильным устройством через NFC.

NFC (Near Field Communication) – 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:

1. Коммерция.
2. Устройства NFC могут применяться в бесконтактных платежных системах, в электронных билетных смарткартах, а также для осуществления платежей с мобильных устройств.
3. Обмен информацией с другими людьми.
4. NFC может быть использована для обмена контактами, фотографиями, видео или другими файлами, а также для входа в мультиплеерные игры.
5. Подтверждение личности и коды доступа.
6. NFC-устройства используются как электронные удостоверения личности.
7. Другие возможности [1].

Смартфоны с NFC могут работать вместе с NFC-тегами, которые могут быть запрограммированы NFC-приложениями для автоматизации некоторых задач. Эти приложения могут позволить изменить настройки телефона, создать и отправить текст, запустить другое приложение или выполнить любое другое действие, которое позволяет смартфон.

Также смартфоны с NFC можно использовать для работы с персональными компьютерами. Для этого необходимо иметь специальное NFC устройство для персонального компьютера, позволяющее считывать и записывать информацию на NFC-теги, например, ACR 122 USB NFC Reader.

Рассмотрим, как можно обмениваться данными между персональным компьютером не только с NFC-тегами, но и мобильными устройствами и организовать пиринговую сеть посредством технологии NFC.

В качестве формата обмена данных между NFC устройствами используется NDEF. NDEF (NFC Data Exchange Format) – это стандартизированный формат данных, который можно использовать для обмена информацией между любым NFC совместимым устройством и другим NFC устройством или NFC-тегом.

NDEF формат используется для хранения и обмена информацией, например ссылок, контактов, текста и т.д., используя общий понимаемый формат. NFC-теги, такие как карты Mifare Classic, могут быть настроены как NDEF-теги и данные, записанные на них одним NFC устройством, могут быть прочитаны другим. Также NDEF сообщения могут использоваться для обмена данными между двумя активными NFC устройствами в пиринговом режиме. Придерживаясь NDEF формата обмена данными, NFC устройства, не зная информации друг о друге, способны обмениваться данными в организованной и взаимно понятной форме.

Необходимо исследовать, как происходит взаимодействие с NFC на базе операционной системы Android. С помощью операционной системы Android 4.4 и выше можно использовать режим host-based card emulation (HCE), который позволяет любым Android приложениям эмулировать NFC карту и общаться им напрямую с NFC считывателем (рис. 1).

Рис. 1. Схема работы Host Card Emulation

HCE использует Application Protocol Data Units (APDU). Этот протокол используется для взаимодействия Android приложений и NFC считывателя. APDU – это командные и ответные пакеты для обеспечения связи между смарт-картами. Команда APDU содержит код инструкции и ассоциированные с ним данные. APDU ответ содержит данные и код состояния ответа на запрос предыдущей команды APDU. Архитектура Host-based Card Emulation в Android основана на сервисных компонентах операционной системы, называемые HCE сервисы. Одно из ключевых преимуществ сервисов заключается в том, что они могут быть запущены в фоновом режиме без пользовательского интерфейса. Это является естественным для многих HCE приложений, в которых пользователь не должен запускать само приложение, чтобы использовать функции NFC. Работает всю следующим образом: когда пользователь подносит мобильное устройство к NFC считывателю, системе Android необходимо знать, какой HCE сервис необходим для NFC считывателя. Здесь приходит на помощь спецификация ISO/IEC 7816-4, которая описывает способ выбора приложений на основе AID (Application ID), который содержит не больше 16 байт информации. Также существует особенность работы Android с NFC контроллером, когда экран мобильного

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].