УДК 004.056

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА УСТРОЙСТВАХ ПОД УПРАВЛЕНИЕМ ANDROID

Поелуева Екатерина Сергеевна
студент
Козюкова Екатерина Сергеевна
студент
Мордовский государственный университет им. Н.П. Огарёва, Саранск
author@apriori-journal.ru

Аннотация. В статье рассматриваются вопросы проектирования программного обеспечения, предназначенного для мобильных устройств, на которых установлена операционная система Android, для хранения текстовой информации в зашифрованном виде с использованием облачных хранилищ. В качестве облачного хранилища предлагается использовать DropBox и Яндекс.Диск. В качестве алгоритма шифрования конфиденциальной информации используется ГОСТ 28147-98.

Ключевые слова и фразы: мобильное устройство; операционная система Android; облачное хранилище; программное обеспечение.

SOFTWARE DEVELOPMENT SAFE STORAGE OF CONFIDENTIAL INFORMATION ON THE ANDROID DEVICE

Poelueva Ekaterina Sergeevna
student
Kozyukova Ekaterina Sergeevna
student
Ogarev Mordovia State University, Saransk

Abstact. This article discusses the design of software designed for mobile devices that are running the operating system Android, for storing text information in encrypted form using cloud storage. As the cloud storage is proposed to use DropBox and Yandex.Disk. As the encryption algorithm used confidential information to GOST 28147-98.

Key words: mobile device; OS Android; cloud storage; software.

Устройства под управлением операционной системы (ОС) Android получили большое распространение в последнее время. Подавляющее число пользователей хранит на своих устройствах конфиденциальную информацию как личную, так и служебную. Но она никак не защищена и при утере устройства, что является основной угрозой конфиденциальной информации на мобильных устройствах, возможен беспрепятственный доступ злоумышленника к защищаемой информации.

Отсюда возникает проблема безопасного хранения такой информации. Для решения данной задачи была разработана программа для хранения конфиденциальной информации в памяти устройства в виде, затрудняющем извлечение информации [4; 5].

Основные особенности программы [2]:

- возможность ввода информации различного вида (графическая, текстовая, бинарные данные);
- журнал событий. Предназначен для фиксации действий пользователя и выявления несанкционированных действий с хранилищем;
- контроль целостности БД с внесением результатов проверки в журнал событий;
- резервное копирование и восстановление. Возможно два способа: сохранение копии БД в локальной памяти устройства, либо синхронизация с облачным хранилищем;
- хранение информации в виде, затрудняющем извлечение полезной информации;
- простой и эффективный способ аутентификации, основанный на мастер-пароле. Имеется контроль сложности создаваемого мастер-пароля;
- исполняемый файл программы обфусцирован для противодействия анализу и модификации программы при декомпиляции.

Рассмотрим процесс входа в систему и внесения информации для хранения. Данный процесс изображен на рисунке 1.

Прежде всего, осуществляется проверка целостности базы данных. В случае отрицательного результата выдаётся соответствующее сообщение пользователю и информация о проверке заносится в журнал событий. В случае успешной проверки у пользователя запрашивается мастер-пароль, после чего происходит его проверка. Если введённый пароль неверный, то пользователю дается еще несколько попыток на ввод. В случае правильности пароля, на его основе вырабатывается ключ преобразования информации в читаемый вид и происходит преобразование информации, хранимой в базе данных [1; 2; 4].

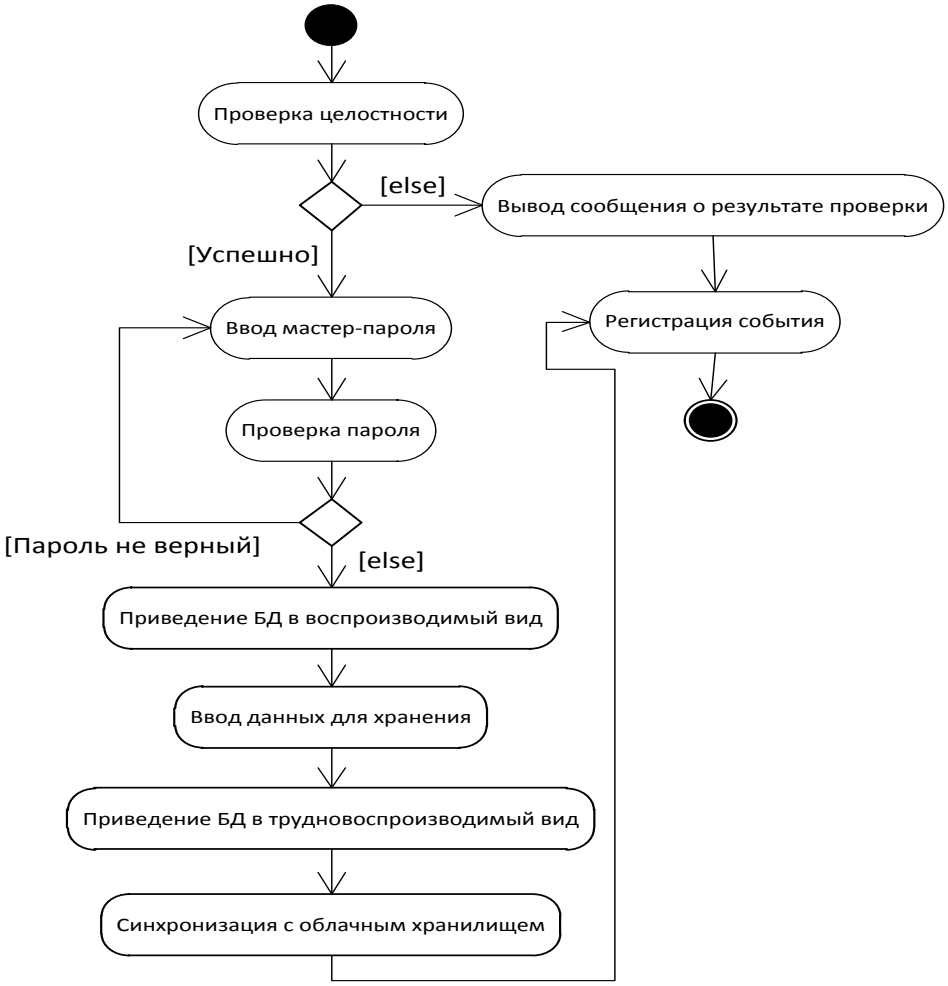

Рис. 1. Диаграмма деятельности операции входа внесения конфиденциальной информации

После этого пользователь осуществляет ввод новой информации, которая преобразуется в трудно воспроизводимый вид и сохраняется в базе данных. Далее происходит отправка базы данных с преобразованной информацией в облачное хранилище.

При разработке данного программного продукта использовался язык программирования Java, среда разработки Eclipse IDE for Java Developers, версия Indigo Service Release 2, плагин Android Development Tools, версия 18.0.0.v201203301601-306762, средство для отладки виртуальной машины Dalvik Android Dalvik Debug Monitor Service, версия 18.0.0.v201203301601-306762, средство для анализа трассировочной информации Android Traceview, версия 18.0.0.v201203301601-306762, эмулятор Android устройства Android Emulator, средство обфускации ProGuard [4].

Программа предназначена для решения задачи защиты конфиденциальной информации, хранимой на мобильных устройствах под управлением ОС Android. Приложение представляет собой защищенное хранилище, доступ к которому имеет лишь пользователь мобильного устройства.

При работе с программой пользователь имеет возможность инициализировать хранилище, заменить мастер-пароль, вносить информацию для хранения, просматривать внесенную информацию, осуществить синхронизацию с облачным хранилищем, экспортировать хранилище в виде БД на SD-карту, импортировать хранилище с SD-карты, просматривать журнал событий.

Программа предназначена для мобильных устройств только на ОС Android, начиная с версии 2.2 [2; 4].

В состав программы входит:

- модуль разметки пользовательского интерфейса;
- модуль работы с хранилищем;
- криптографический модуль.

Модуль работы с хранилищем является основным модулем. В состав его функций входит: ввод, проверка, замена мастер пароля, ведение БД с записями пользователя, синхронизация с облачным хранилищем, импорт/экспорт БД на SD-карту, проверка целостности БД, ведение журнала событий. Данный модуль связан с криптографическим модулем и модулем разметки пользовательского интерфейса. В состав модуля входят классы: EnterMainPassActivity, ReplacementActivity, SaveMainPassActivity, CriptoActivity, JournalActivity, MainListActivity.

Криптографический модуль отвечает за процессы зашифрования и расшифрования информации, выработки хеш-суммы. Предоставляет свои функции модулю работы с хранилищем. В состав модуля входят классы: CipherUtil, GOST28147, GOSTR3411. Спецификации этих классов представлены в приложении А, причем класс CipherUtil не имеет атрибутов.

Модуль разметки пользовательского интерфейса отвечает за построение интерфейса пользователя, начальную инициализацию элементов интерфейса. Предоставляет данные о пользовательском интерфейсе модулю работы с хранилищем. В состав модуля входят файлы XML разметки: data_add.xml, entermpass.xml, journal.xml, mainpass.xml, replacement.xml, row_list.xml.

Модуль работы с хранилищем связан с программой типа «Файловый менеджер». Указать точное название такой программы не представляется возможным, так как разработанное приложение автоматически находит программу типа «Файловый менеджер», исходя из предъявленных требований к ней [3].

Программа не предъявляет особых требований к центральному процессору, поэтому приложение будет работать нормально с любым ARM процессором, который удовлетворяет системным требованиям Android 2.2.

В процессе исследования в средстве Dalvik Debug Monitor Service было выявлено, что программа занимает не более 7,445 Мб ОЗУ.

После удачной установки приложения, его запуск можно осуществить путем выбора соответствующего ярлыка в списке всех приложений, установленных на мобильном устройстве [4].

Таблица 1

Результаты функционального тестирования

Название метода	Назначение	Статус	Время выполнения (сек.)
testCreatePass	Тестирование процедуры создания мастер пароля	Успех	7,109
testLogin	Тестирование процедуры входа в систему	Успех	10,716
testAddEntry	Тестирование процедуры добавления записи	Успех	8,829
testDisplayEntry	Тестирование процедуры просмотра записи	Успех	8,978
testImport	Тестирование процедуры импорта БД	Успех	11,868
testExport	Тестирование процедуры экспорта БД	Успех	5,322
testDisplayJournal	Тестирование возможности просмотра журнала	Успех	6,469

Выходными данными являются: выводимая на экран текстовая информация, файл базы данных формата SQLite с записями пользователя, журнала событий.

Функциональное тестирование включает проверку работоспособности основных процессов приложения: создание мастер-пароля, вход в систему, добавление записи, просмотр записи, импорт/экспорт базы данных, ведение журнала событий [1; 2].

Тестирование проводилось при помощи создания приложения по технологии JUnit, включающего соответствующий набор тестовых методов. Все тестовые прогоны завершились без ошибок. Результаты функционального тестирования представлены в таблице 1.

Таким образом, примененные алгоритмы «запутывания» кода не позволяют эффективно анализировать код программы, полученным в результате обратной разработки.

Тестирование информационной безопасности также включает анализ содержимого базы данных. Для этого была использована программа SQLite Database Browser версия 2.0b1. Перед анализом в базу данных были введены две тестовых записи. Содержимое таблицы secret_data представлено в таблице 2.

Тестирование информационной безопасности также включает анализ содержимого базы данных. Для этого была использована программа SQLite Database Browser версия 2.0b1. Перед анализом в базу данных были введены две тестовых записи. Содержимое таблицы secret_data представлено в таблице 2 [4].

Таблица 2

Содержимое таблицы secret_data

name	login	pass	comment	file	filename
1649d0df 82940663	97f483569 880d973	3ce4984c c163905b		<данные в бинар-ном виде>	8462a3edcf 96fe3e1...
b0afa051 6aec21c6	d5d2d1c7 0872f836	545d281b 4268dd81	9f794c676 5bf7f8c		

Значение столбца filename отображено не полностью, так как оно имеет слишком большое количество символов. Из таблицы видно, что все данные хранятся в зашифрованном виде. Даже если база данных попадет к злоумышленнику, то он не сможет воспользоваться, полученной информацией.

Для тестирования проверки целостности, при помощи программы Database Browser версия 2.0b1, было изменено содержимое таблицы secret_data в соответствии с таблицой 3 [4].

Таблица 3

Обновленное содержимое таблицы secret_data

name	login	pass	comment	file	filename
1649d0df 82940663	97f483569 880d973	4ce4984cc 163905b		<данные в бинарном виде>	8462a3edcf 96fe3e1...
b0afa051 6aec21c6	d5d2d1c7 0872f836	545d281b 4268dd81	9f794c676 5bf7f8c		

В результате тестирования, было выявлено, что программный продукт выполняет все заявленные возможности правильно, в соответствии с функциональными требованиями. Тестирование информационной безопасности проводилось при помощи дополнительного программного обеспечения и с допущением, что у потенциального злоумышленника был доступ к БД (на практике взломщику сначала нужно попытаться получить доступ к БД). В результате тестирования осуществить НСД к защищаемым данным не удалось.

Для нормальной работы программного продукта необходимо: любой ARM процессор, удовлетворяющий минимальным системным требованиям Android 2.2, 8 Мб свободной памяти ОЗУ, 690 369 байт на SD-карте, 2,36 Мб во внутренней памяти, диагональ экрана от 2,8 дюймов.

Таким образом, использование данной программы позволяет предотвратить утечку конфиденциальной информации, хранимой на мобильных устройствах под управлением ОС Android. И если злоумышленник получит доступ к защищаемой информации, то приведение ее в человеко-читаемый вид займет достаточное время для потери актуальности атакуемой информации.

Список использованных источников

1. Александров Э.Э. Программирование на языке С в Microsoft Visual Studio 2010 / Э.Э. Александров, В.В. Афонин. Саранск: Изд-во Мордов. ун-та, 2010. 428 с.
2. Афонин В.В., Федосин С.А. О структурировании лабораторно-практических занятий при изучении дисциплин программирования // Образовательные технологии и общество. 2014. Т. 17. № 4 С. 497-506.
3. Афонин В. В. Анализ управляемости нелинейных аффинных систем управления в системе Matlab // Вестник мордовского университета. 2012. № 2. С. 177-181.
4. Воронкин Р.А. Бабкин В.Ю. Программа для безопасного хранения конфиденциальной информации на устройствах под управлением ОС Android // Инфокоммуникационные технологии в науке, производстве и образовании: V междунар. науч.-тех. конф. Ставрополь: Северо-Кавказский гуманитарно-технический институт, 2012. 250 с.
5. Александров Э.Э., Афонин В.В., Программирование на языке С в Microsoft Visual Studio 2010. [Электронный ресурс]. Режим доступа: http://www.intuit.ru/department/pl/prcmsvs2010 (дата обращения: 31.10.2015).