РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ УПРАВЛЕНИЯ ПАРОЛЯМИ

Анастасия КИРИЛЕНКО (ЦУРКАНУ), студентка
CZU: 004.415.2
anastasia.kiriliuk@outlook.com

The security of personal data is a very actual problem for people of 21st century. Leaking of sensitive data may cause into stealing people's money, applying them for unwanted credit cards or loans under victim's name. Developed centralized application for storing and managing passwords is dedicated to keep secret data in a safe place, protected by the strongest encrypting algorithms. Applying the latest technologies like Cloud Solutions and Java guarantee the effectiveness of created system.

Приводится созданная система управления паролями, используемая для упрощения работы пользователя при входе в различные системы посредством упорядочивания паролей для учетных записей. Актуальность разработанной системы заключается в использовании самых передовых технологий Android и Cloud Storage от Firebase, а также в использовании техник flat design от Google для создания лаконичного дизайна. Требования для разработки заключались в создании комплексной информационной системы в качестве репозитория и генератора паролей, которая привнесла бы новые функции в сравнении с уже существующими на рынке решениями. В сущности, данная разработка подчеркивает вклад мобильных технологий в повседневную жизнь и спрос на простые решения с широким спектром возможностей.

Программа обеспечивает управление паролями и доступ к ним с помощью Single Sign-On к веб-приложениям и хост-приложениям. Пользователи входят в систему только один раз, и диспетчер паролей затем выполняет все необходимые действия: производит автоматический вход в защищенные системы, реализует политики паролей и автоматизирует задачи конечных пользователей. Приложение расчитано на пользователей мобильных устройств под управлением Android OS.

Среди использованных сервисов можно выделить Google Cloud Messaging. Эта служба имеет четко определенный механизм для передачи данных с безопасным приемом сообщений. Принципы можно резюмировать в несколько шагов, описанных в Рисунке 1.

1. Приложение с устройства посылает запрос на сервер Google для идентификации.
2. Сервер Google отправляет в ответ уникальный токен.
3. Приложение с устройства отправляет этот уникальный токен на сервер приложений;

Рис. 1. Схема генерации токенов на устройстве Android

Затем сервер отправляет сообщения на устройства Android через облачный сервис.

1. Сервер приложения сохраняет токен, привязывая его к мобильному устройству.
2. Сервер, используя этот уникальный для каждого устройства токен, сохраняет сообщение в локальной базе данных.
3. Сервер Google отправляет сообщение устройтву, когда установлено стабильное соединение с Интернетом.
4. Устройство Android афиширует сообщение.

В качестве основного шаблона реализации был выбран MVVM [1]. Его главной задачей стало разделить приложение на 3 уровня: пользовательский интерфейс, представление данных и бизнеслогика, что позволяет изолированно работать во всех трех слоях.

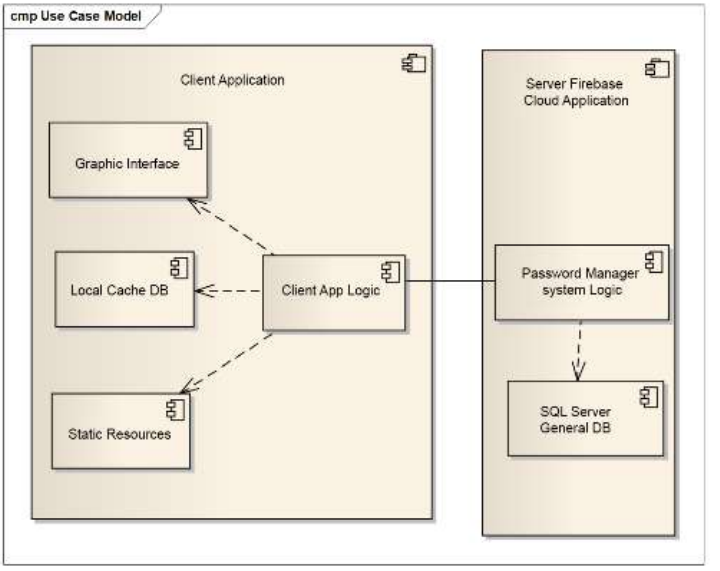

Рис. 2. Диаграмма составляющих системы

Правильное функционирование информационной системы обеспечивается несколькими модулями (Рис. 2)

Ядром системы является логический модуль приложения, который выполняющий роль принятия решений в зависимости от взаимодействия пользователя с графическим интерфейсом, или администратора, управляющего серверной частью системы. Графический интерфейс пользователя – это реагирующая часть, связывающая прямое взаимодействие пользователя с системой Password Shelf. На уровне реализации этот модуль можно найти в Activity и фрагментах приложения Android или в веб-интерфейсе серверного приложения. Локальные ресурсы приложения предс-

тавляют собой стили, изображения и ресурсы, присутствующие в каталоге Res проекта Android Studio. Эти ресурсы используются для создания графики и хранения статистических данных. Модуль базы данных Sqlite представляет собой пакет служебных классов, управляющий хранением данных на локальном уровне, на стороне клиента информационной системы Password Shelf. Модуль взаимодействия с сервером описывается библиотеками, используемыми для создания связи REST API [2], а именно библиотекой Retrofit для HTTP-запросов, json для сериализации и десериализации данных и HttpClient для обработки сложных запросов.

Клиентское приложение можно установить на любое устройство, работающее на операционной системе Android с подключением к Интернету. Серверная часть приложения находится на сервере, имеющем базу данных типа NoSQL – Firebase Realtime database. Благодаря режиму реального времени, данные синхронизируются между всеми клиентами и девайсами моментально. Обмен данными является двунаправленным: от клиента поток данных проходит через Интернет, отправляя HTTP-запросы на сервер, а также передача происходит через защищенное соединение SSL [3]. Из использованных технологий и программных продуктов можно выделить Java, JavaScript, CSS, JSON, Firebase, Crashlytics, Google Services, Android Studio, Genymotion.

В заключение отметим, что проблема потери личных данных сейчас очень остра. Умение правильно защищать информацию высоко ценится и трудно достигается. Менеджер паролей поможет решить вопрос хранения и управления конфиденциальными данными.

Литература:

1. BEVIS, Tony. *Java Design Pattern Essentials, Second Edition Paperback*, 2012, p. 126.
2. BOILEAU, Thierry. *Restlet in Action: Developing RESTful Web APIs in Java*, 2012.
3. KIM, Gene, LOVE, Paul and SPAFFORD, George. *Visible Ops Security: Achieving Common Security And IT Operations Objectives*, p. 67.

Рекомендовано
Олга Чербу, докт., конф.

ИССЛЕДОВАНИЕ И ПРИМЕНЕНИЕ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Константин ВИГУЛЯР, студент
***CZU:* 004.056** kostavigulear@outlook.com

На сегодняшний день вопрос информационной безопасности (ИБ) – одна из приоритетных задач не только в сфере информационных технологий, но и в повседневной жизни современного общества. Возрастающая роль информационной сферы оказывает колоссальное влияние на безопасность в политических, корпоративных, экономических, личных и многих других аспектах жизни. Постепенно информация приобрела статус наиценнейшего ресурса наряду с ископаемыми дорогими металлами и энергетическими источниками. Информация стала определяющим фактором успешности любого бизнеса. Вместе со столь возросшей значимостью и ценностью информации, появился целый ряд проблем и рисков, связанных с ней. Данный вопрос стал причиной появления явления информационной безопасности как отдельной науки и профессии.

Вопрос защиты информации особенно важен в век информационных и цифровых технологий, когда почти любое электронное устройство позволяет установить соединение с собой напрямую или удаленно. Для обеспечения надлежащей безопасности требуется комплексный и ресурсоемкий подход.

Зачастую проблема ИБ воспринимается в рамках информационных технологий, но на самом деле это проблема бизнеса в целом. Очень важно следить за выполнением правил ИБ с точки зрения требований бизнеса и закона. ИБ невозможно представить в качестве конечного продукта, который необходимо установить, выполнив определенные требования. Каждый день на информационном рынке появляются десятки новых лазеек, инструментов для взлома и проникновения, и то, что сегодня кажется защищенным, завтра может оказаться взломанным за считанные секунды. Поэтому ИБ следует воспринимать в качестве продолжительного прикладного процесса, требующего постоянного