Проблемы защиты информации в приложениях для мобильных систем

Зубков К. Н., Диасамидзе С. В.
Петербургский государственный университет путей сообщения Императора Александра I
Санкт-Петербург, Россия
kirillzubkoff@gmail.com, sv.diass99@yandex.ru

Аннотация. **Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные, несанкционированный доступ к которым может привести к непредсказуемым результатам. В настоящий момент современные средства защиты не позволяют в полной мере решить вопросы безопасности мобильных систем и оценить возможные риски потенциальных злоумышленных действий. В связи с этим возникает задача систематизировать основные угрозы и уязвимости мобильных приложений для последующего формирования методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем.**

Ключевые слова: **мобильная операционная система, приложение, уязвимость, анализ защищенности, мобильная платформа, мобильное устройство.**

Введение

В соответствии с последними данными исследовательской компании eMarketer [1], специализирующейся на анализе рынка высоких технологий, смартфонами уже пользуется четверть мирового населения. Это около 2 млрд человек. И тенденция роста пользователей мобильных устройств продолжается. На рис. 1 представлена динамика роста числа пользователей смартфонов в период с 2013 по 2016 г. с прогнозом на 2017–2018 г.

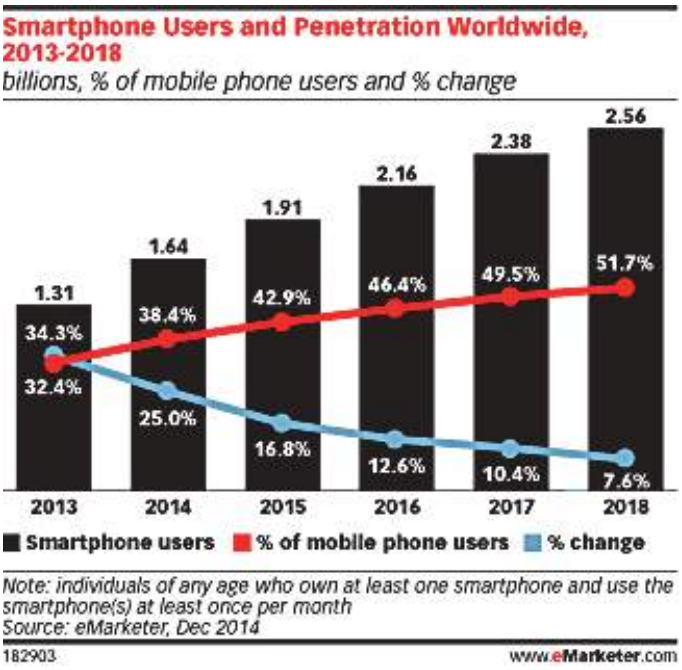

Рис. 1. Прогноз роста числа пользователей смартфонов

В настоящий момент Россия занимает пятое место в списке из 25 стран по числу пользователей мобильных устройств (рис. 2).

Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные: номера кредитных карт, электронную почту, геолокационные сведения [2], профили в социальных сетях, средства удалённого доступа и управления предприятием, фотографии, видео и т. д. Несанкционированный доступ к таким чувствительным данным может привести к критической ситуации. Между тем, рынок мобильных

Top 25 Countries, Ranked by Smartphone Users, 2013-2018
millions

	2013	2014	2015	2016	2017	2018
1. China*	436.1	519.7	574.2	624.7	672.1	704.1
2. US**	143.9	165.3	184.2	198.5	211.5	220.0
3. India	76.0	123.3	167.9	204.1	243.8	279.2
4. Japan	40.5	50.8	57.4	61.2	63.9	65.5
5. Russia	35.8	49.0	58.2	65.1	71.9	76.4
6. Brazil	27.1	38.8	48.6	58.5	66.6	71.9
7. Indonesia	27.4	38.3	52.2	69.4	86.6	103.0
8. Germany	29.6	36.4	44.5	50.8	56.1	59.2
9. UK**	33.2	36.4	39.4	42.4	44.9	46.4
10. South Korea	29.3	32.8	33.9	34.5	35.1	35.6
11. Mexico	22.9	28.7	34.2	39.4	44.7	49.9
12. France	21.0	26.7	32.9	37.8	41.5	43.7
13. Italy	19.5	24.1	28.6	32.2	33.7	37.0
14. Turkey	15.3	22.6	27.8	32.4	37.2	40.7
15. Spain	18.9	22.0	25.0	26.9	28.4	29.5
16. Philippines	14.8	20.0	24.8	29.7	34.8	39.4
17. Nigeria	15.9	19.5	23.1	26.8	30.5	34.0
18. Canada	15.2	17.8	20.0	21.7	23.0	23.9
19. Thailand	14.4	17.5	20.4	22.8	25.0	26.8
20. Vietnam	12.4	16.6	20.7	24.6	28.6	32.0
21. Egypt	12.6	15.5	18.2	21.0	23.6	25.8
22. Colombia	11.7	14.4	16.3	18.2	19.7	20.9
23. Australia	11.4	13.2	13.8	14.3	14.7	15.1
24. Poland	9.4	12.7	15.4	17.4	19.4	20.8
25. Argentina	8.8	10.8	12.6	14.1	15.6	17.0
Worldwide* **	**1,311.2**	**1,639.0**	**1,914.6**	**2,155.0**	**2,380.2**	**2,561.8**

*Note: individuals of any age who own at least one smartphone and use the smartphone(s) at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed*
Source: eMarketer, Dec 2014
182905 www.eMarketer.com

Рис. 2. Топ 25 стран по количеству пользователей мобильных устройств

приложений растёт с большой скоростью, а пользователи особенно не задумываются о том, какие разрешения они предоставляют приложениям, устанавливая их на свой смартфон, а также о последствиях, которые могут наступить.

Последний отчёт компании Digital Secuirty об исследовании российских приложений мобильного банкинга показал, что все они содержат, по крайней мере, одну уязвимость, позволяющую либо перехватить данные, передающиеся между клиентом и сервером, либо напрямую эксплуатировать уязвимости устройства и самого мобильного приложения [3].

Проблемы безопасности касаются не только банковского сектора. Игры на мобильных устройствах, множество других популярных приложений могут быть потенциально опасными. Например, популярное приложение «Музыка ВКонтакте», размещённое на площадке Google Play и имеющее довольно высокий рейтинг (4,5 из 5), а также более 500 тысяч скачиваний, вовсе похищало идентификационные данные пользователей, что приводило к потере доступа к профилю в социальной сети.

Всё это говорит о том, что существует реальная необходимость оценить текущее состояние информационной безопасности наиболее распространённых мобильных операционных систем, систематизировать основные угрозы и уязвимости мобильных приложений и составить детальный подход к разработке методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем.

Популярные мобильные операционные системы

Сегодня наиболее распространёнными мобильными операционными системами являются ОС Android, iOS и ОС Windows Phone.

По последним данным, 8 из 10 современных мобильных устройств работают на базе операционной системы с открытым кодом Android. На рис. 3 приведена статистика с сайта https://www.statista.com. На графиках продемонстрированы доли рынка мобильных операционных систем в соответствии с продажами устройств конечным пользователям в период с 2009 по 2016 г. В третьем квартале 2015 г. 84,7 % от количества всех проданных смартфонов базировались на операционной системе Android.

По последним статистическим сведениям, ОС Android получила статус самой уязвимой. В 2016 г. на ОС Android специалисты по информационной безопасности нашли 523 уязвимости. На рис. 4 приведена статистика 2016 г., демонстрирующая количество уязвимостей на различных мобильных операционных системах.

Классификация приложений для мобильных устройств

Существует множество классификаций приложений для мобильных устройств, но в контексте информационной безопасности приложений следует выделить две большие группы:

• web-приложения, представляющие собой специальную версию web-сайта;

• мобильные приложения, разработанные под определённую мобильную операционную систему с использованием специализированного API.

Перед тем как рассматривать методологии анализа защищенности мобильных приложений, следует определить типовые уязвимости приложений и потенциальные угрозы несанкционированных действий для пользователя.

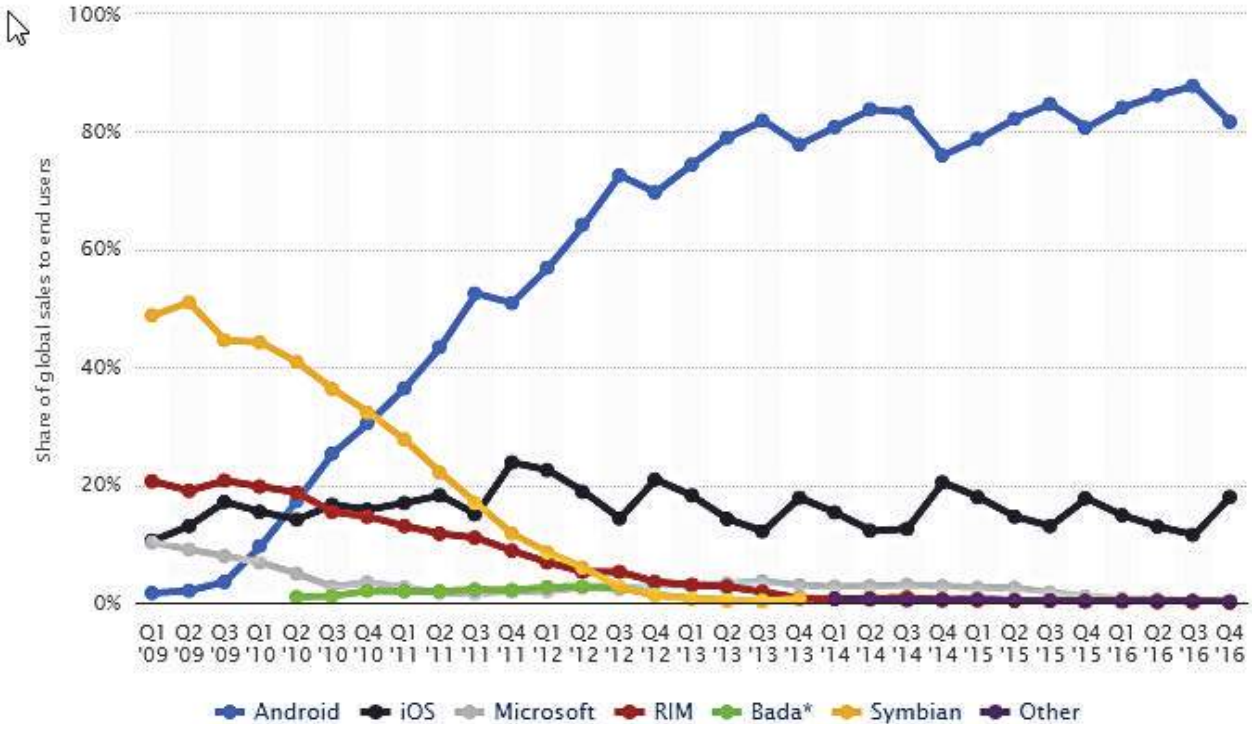

Рис. 3. Доли рынка мобильных операционных систем в соответствии с продажами мобильных устройств конечным пользователям в 2009–2016 гг.

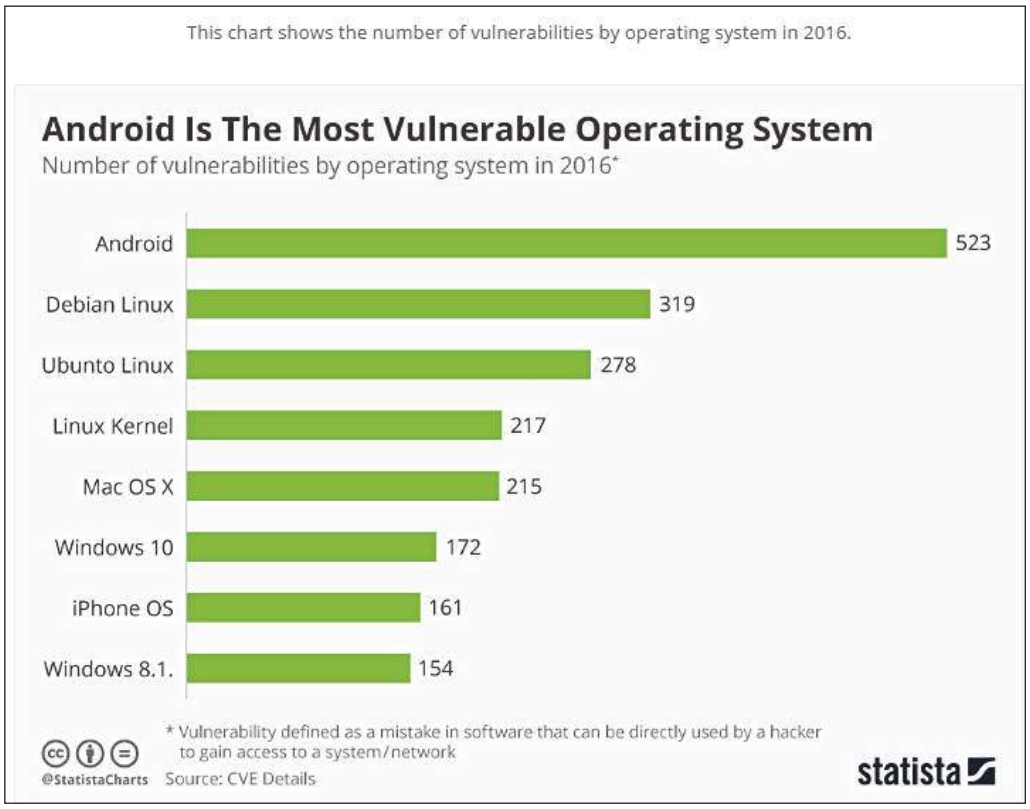

Рис. 4. Количество уязвимостей, найденных в мобильных операционных системах, 2016 г.

Типовые уязвимости

В соответствии с классификацией открытого проекта обеспечения безопасности web-приложений OWASP [4] (Open Web Application Security Project), к основным уязвимостям, которым подвержены мобильные устройства, относятся:

1) системные уязвимости (архитектурных решений мобильной платформы);

2) небезопасное хранение данных;

3) недостаточная защищенность протоколов передачи данных;

4) уязвимости системы авторизации и аутентификации;

5) слабая криптостойкость;

6) уязвимости кода приложения;

7) скрытый функционал приложений;

8) ненадлежащий контроль за клиентскими приложениями.

Остановимся на каждом из пунктов более подробно, акцентируя внимание на особенностях наиболее популярных мобильных операционных систем.

1. Уязвимости архитектурных решений мобильной платформы

Основная причина, по которой операционная система Android является наиболее слабо защищенной, – это отсутствие технологии подписывания ядра на уровне архитектуры платформы [5]. Суть подписи кода заключается в том, что она не позволяет выполняться в системе стороннему коду, не подписанному компанией, выпустившей мобильную операционную систему. Благодаря тесной взаимосвязи программного и аппаратного обеспечения в устройствах, например, под управлением iOS или Windows Phone, каждый шаг, начиная с нагрузки системы и заканчивая установкой приложений, анализируется с точки зрения безопасности и эффективности использования ресурсов. Целостность системы безопасности напрямую зависит от целостности и надежности ядра iOS. На рис. 5 схематично показана архитектура системы безопасности iOS, на рис. 6 – структурная схема операционной системы Android.

2. Небезопасное хранение данных

Этот раздел включает в себя следующие проблемы информационной безопасности:

• уязвимость «Hardcoded and Forgotten».

Это уязвимости, случайно созданные разработчиками при проектировании программного продукта.

Android-приложение представляет собой apk-файл (англ. Android Package – формат архивных исполняемых файлов-приложений для Android), т. е. архив, в котором хранятся исполняемые файлы, конфигурационные файлы, ресурсы приложения и т. д. Если распаковать архив apk и проанализировать конфигурационные файлы, то часто можно обнаружить строки кода, которые разработчики забыли убрать из финальной версии продукта. Эти строки кода чаще всего используются для отладки в течение периода разработки приложения, и они могут значительно облегчить злоумышленнику задачу получения данных конфиденциального характера или реализацию других несанкционированных действий;

• некорректное назначение прав доступа для файлов, которое создаёт приложение.

На этапе тестирования разработчики часто некорректно назначают права доступа и забывают редактировать их при финальном выпуске программного продукта, в связи с чем у злоумышленников появляется ещё больше возможностей для несанкционированного доступа;

• хранение важных данных на SD-карте.

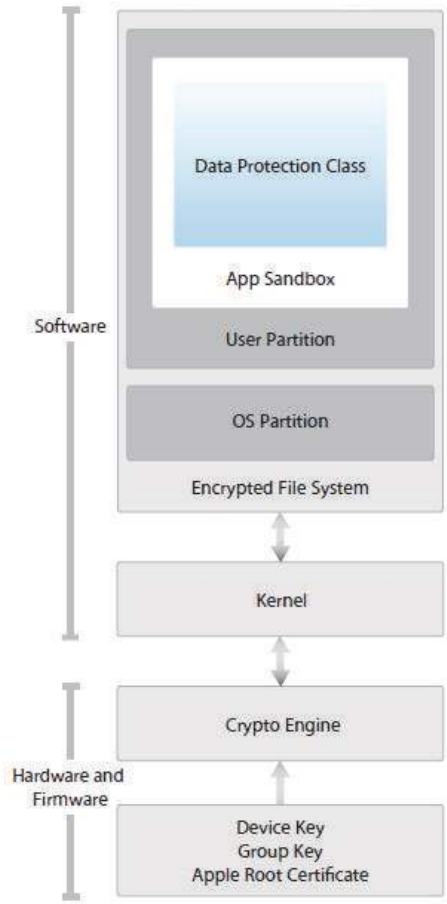

Рис. 5. Архитектура безопасности операционной системы iOS

Часто пользователи хранят важные данные на SD-карте, забывая, что эти данные доступны для всех приложений по умолчанию. Некоторые приложения могут хранить даже cookie-файлы (небольшой фрагмент данных, отправленный сервером для хранения браузером пользователя) и ISDN-токены на SD-картах;

• логирование [6].

Логи представляют собой файлы регистрации, содержащие записи обо всех событиях, происходящих в мобильной операционной системе, с высокой степенью детализации. В Android любое приложение при установке может запросить права доступа на чтение логов. Многие пользователи не обращают внимания на этот запрос, но опасность заключается в том, что любое устанавливаемое приложение, которое запросило доступ к чтению логов, и при этом получило одобрение со стороны пользователя, получит право чтения всей информации, которое приложение заносит в логи, если логирование не выключено пользователем. Зачастую в логи попадает вся отладочная информация и персональные данные без шифрования;

• получение прав суперпользователя.

Часто пользователи смартфонов стремятся к получению полного доступа к файловой системе устройства, чтобы обеспечить возможность установки сторонних приложений (не из официальных магазинов AppStore или Google Play Market). На мобильных устройствах компании Apple эта процедура называется Jail Break, а на Android-смартфонах – получение Root-прав (или прав суперпользователя). Стоит отметить, что jail-break или root – это компрометация всей системы безопасности устройства, а не просто опция, расширяющая возможности смартфона.

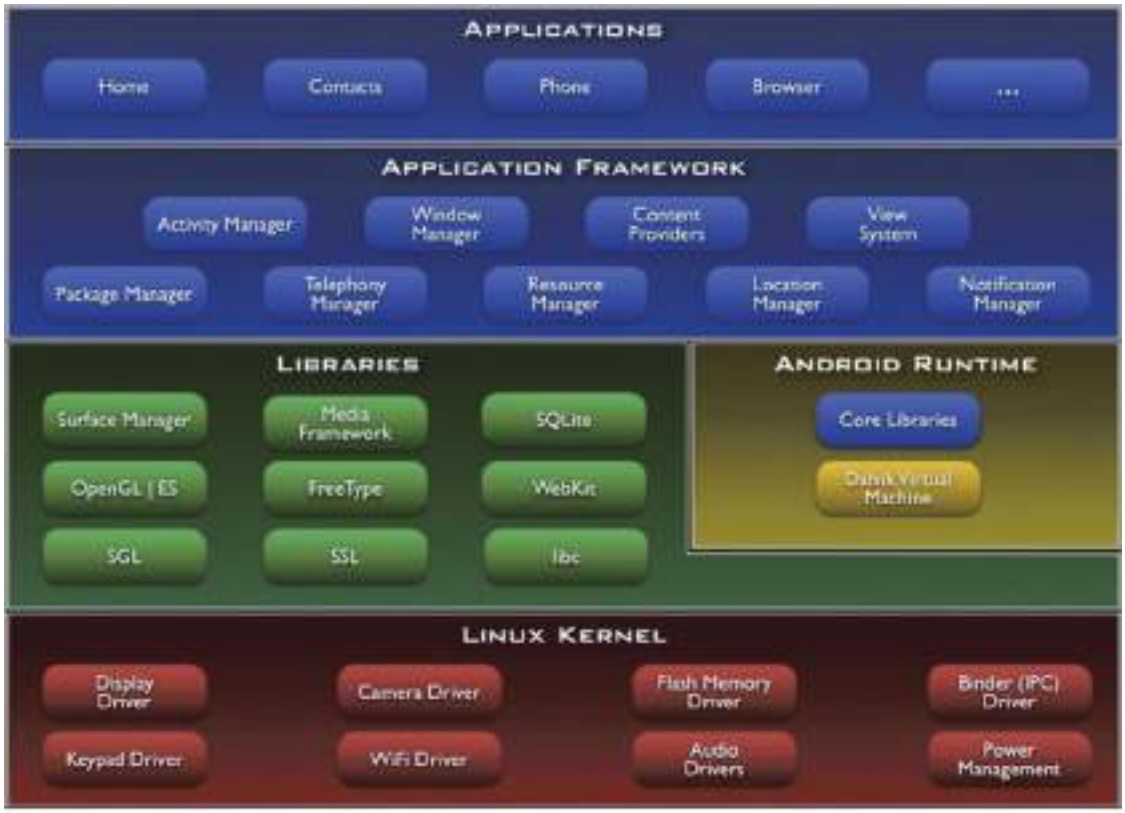

Рис. 6. Архитектура операционной системы Android

Меры, которые следует предпринимать для защиты персональных данных мобильного устройства от несанкционированного доступа:

• не допускать хранения важных данных на SD-карте;

• отключить логирование перед установкой приложений;

• при разработке приложений необходимо настроить права доступа с учетом того, что мобильное устройство пользователя может быть скомпрометировано root-правами;

• периодически просматривать конфигурационные файлы на предмет забытых отладочных строк кода, позволяющих получить несанкционированный доступ к персональным данным.

3. Недостаточная защищенность протоколов передачи данных

Основные проблемы:

• не используется шифрование при передаче данных (например, использование протокола http вместо https);

• при передаче данных используются самоподписанные сертификаты;

Меры по обеспечению информационной безопасности:

• проверка трафика мобильного приложения;

• использование web-сниффера, который будет анализировать трафик мобильных приложений и проверять, чтобы важные данные уходили в зашифрованном виде по протоколу https;

• использование сертификатов, подписанных доверенными центрами;

• при использовании контент-провайдеров (предоставляющих доступ к файлам или базам данных для других приложений) проверка и прописывание прав доступа.

4. Слабая авторизация [7]:

• анонимная работа с приложением.

Требования к защищенности мобильных приложений не такие, как к web-приложениям. Предполагается, что пользователь может работать оффлайн, поэтому часто используется онлайн-авторизация с последующим хранением данных в сессионных cookie-файлах.

После того как были введены идентификационные данные (логин и пароль) и приложение авторизовало пользователя, оно сохраняет специальный идентификатор, который в дальнейшем предъявляется серверу при каждом запросе, поступающем от приложения.

Если злоумышленник получил идентификатор пользователя и при этом в системе не были реализованы процедуры проверки IP-адреса сессии или наличия более одного соединения в пределах сессии, злоумышленник сможет получить доступ в систему с правами аккаунта пользователя. Если это приложения, связанные с интернет-банкингом или с личным кабинетом платежной системы, то о последствиях несанкционированного доступа в таком случае догадаться нетрудно;

• слабые пароли.

Считается, что в мобильных приложениях пароли не должны быть длинными, и большинство приложений разрешает создавать пароли от четырех символов. При этом пароли в большинстве случаев не шифруются и помещаются в базу в хешированном виде. Если злоумышленник получил доступ к базе данных, то с помощью готовых хэш-таблиц расшифровать пароли из четырех символов для него – тривиальная задача, требующая незначительных временны́х затрат.

Меры защиты при данном типе уязвимости:

• аутентификация в мобильном приложении должна соответствовать таковой в web-версии;

• локальная аутентификация должна работать через cookie-файлы только после авторизации на сервере;

• создание сложных паролей длиной более 6 символов.

5. Ненадлежащий контроль за клиентскими приложениями

Это процесс верификации загружаемого в магазины Appstore программного обеспечения. Перед тем как попасть на площадку App Store, iOS-приложения детально проверяются на наличие уязвимостей и на соответствие стандартам разработки Apple. Каждое приложение, устанавливаемое на iOS, должно быть подписано специальным сертификатом «iOS Developer Program», выдаваемым компанией Apple только после целого ряда необходимых проверок. Такие меры безопасности обеспечивают отсутствие вредоносного программного обеспечения в магазине приложений App Store.

К тому же в операционной системе iOS реализована политика «песочницы» (sandbox) для всех сторонних приложений. У каждого приложения есть строго определённая директория, создаваемая во время его установки на мобильное устройство, в которую помещаются файлы приложения. При необходимости доступ к системной информации приложение может получить посредством API или системных служб.

Если говорить об операционной системе Android, то перед загрузкой приложений на площадку Google Play приложения не проверяются на наличие вредоносного кода. Вместо процедуры предварительной проверки компанией Google реализован механизм регулярного автоматического сканирования магазина приложений на предмет потенциально вредоносного программного обеспечения. Как показывает практика, этот метод анализа информационной безопасности повышает процент проникновения вредоносных приложений и их дальнейшего распространения на конечные устройства пользователей.

При установке нового приложения на мобильное устройство на операционной системе Android пользователю предоставляется полный перечень прав доступа, запрашиваемых приложением. Внимательно изучив этот перечень, пользователь может самостоятельно определить потенциально вредоносное программное обеспечение и отменить его установку. Например, если приложение, базовое функциональное предназначение которого – фонарь, запрашивает доступ к контактным данным либо подключение к Интернету, то данное приложение с высокой долей вероятности можно отнести к вредоносному программному обеспечению.

В iOS раздача прав доступа приложениям реализована более гибко. Каждая категория доступа, будь то доступ к камере или к GPS, должна быть либо подтверждена, либо отклонена пользователем.

Таким образом, обязательная подпись кода приложений и корректное исполнение политики безопасности расширяет рамки действия принципа доверия с уровня операционной системы на уровень приложений и препятствует выполнению вредоносного или самомодифицирующегося кода.

Методы анализа защищённости мобильных приложений

Существуют различные методы оценивания угроз информационной безопасности в приложениях для мобильных систем, которые применяются как в отдельности, так и в совокупности. Разделить их можно на две большие категории: статистические и динамические.

В качестве методов динамического анализа используются:

- стресс-тестирование;
- анализ сетевого трафика мобильного приложения;
- анализ памяти приложения;
- анализ взаимодействия приложения с файловой системой.

К методам статистического анализа относятся [9]:

- аудит безопасности кода приложения;
- Reverse Engineering;
- дизассемблирование;
- декомпиляция.

Для комплексной оценки состояния защищенности мобильной системы необходимо исследовать три составляющих: клиентскую часть, серверную часть и непосредственно канал связи. Для этого применяют такие методы:

- комплексный анализ архитектуры клиентской и серверной части приложения;
- моделирование угроз в соответствии с логикой приложения;
- проектирование модели нарушителя.

Заключение

Несмотря на большое количество методов обеспечения безопасности информации, хранящейся на мобильных устройствах, уровень распространения вредоносных приложений в мобильном сегменте растёт высокими темпами. Угрозы безопасности создают риски персональным данным пользователя, риски компрометации критичных данных вплоть до хищения денежных средств. К тому же разработчики мобильных приложений не всегда уделяют достаточного внимания проблемам безопасности или просто не следуют руководствам по безопасной разработке.

На настоящий момент ни высокие рейтинги приложения, ни большое количество скачиваний, ни список ресурсов, доступ к которым пользователь предоставляет приложению перед его установкой, не позволяют оценить возможные риски персональным данным и последствия потенциальных злоумышленных действий. Современные средства защиты (антивирусы, снифферы) могут помочь предотвратить определенный спектр угроз, но их применение не позволит решить проблему безопасности комплексно. В связи с этим возникает задача разработки комплексной методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем, а также методики анализа приложений на предмет их соответствия требованиям информационной безопасности.

Литература

1. Аналитический центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2016. URL: https://www.infowatch.ru/report2016 (дата обращения 01.05.2017).

2. Михайлов Д. М. Исследование уязвимости мобильных устройств систем Apple и Google / Д. М. Михайлов, А. В. Зуйков, И. Ю. Жуков и др. // Спецтехника и связь, 2011, № 6. С. 38-40. URL: http://cyberleninka.ru/article/n/issledovanie-uyazvimosti-mobilnyh-ustroystv-sistem-apple-i-google#ixzz4hjVQGz9w.

3. Корниенко А. А. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте / А. А. Корниенко, С. Е. Ададуров, А. П. Глухов. М.: УМЦ ЖДТ, 2014. 440 с.

4. Anton K. OWASP Top-10 Proactive Controls 2016 / K. Anton, J. Bird, J. Manico // The OWASP Foundation. 2016 February. URL: https://www.owasp.org/images/5/57/OWASP_Proactive_Controls_2.pdf.

5. Rovelli P. Developing a Next-generation Mobile Security Solution for Android. April 2014 School of Computer Science Reykjavík University / P. Rovelli. URL: http://skemman.is/stream/get/1946/19500/43671/1/Developing_a_next-generation_Mobile_Security_solution_for_Android_-_Paolo_Rovelli.pdf.

6. Сафин Л. К. Исследование информационной защищенности мобильных приложений / Л. К. Сафин, А. В. Чернов, Я. А. Александров, К. Н. Трошина // Вопр. кибербезопасности, 2015, № 4 (12). С. 28-37. URL: http://cyberleninka.ru/article/n/issledovanie-informatsionnoy-zaschischennosti-mobilnyh-prilozheniy.

7. Diasamidze S. V. Implementation of the Role Based Access Control in Application for Mobile Device on the Android OS Platform / S. V. Diasamidze, E. Yu. Kuzmenkova, D. A. Kuznetsov, A. R. Sarkisyan // Интеллектуальные технологии на транспорте, 2016, № 1. С. 21-26.

8. Толюпа Е. А. Метод обеспечения безопасности пользователей интернет-магазинов мобильных приложений / Е. А. Толюпа // Прикладная дискретная математика. Приложение, 2014, № 7. С. 101-103. URL: http://cyberleninka.ru/article/n/metod-obespecheniya-bezopasnosti-polzovateley-internet-magazinov-mobilnyh-prilozheniy.

9. Цыганенко Н. П. Статический анализ кода мобильных приложений как средство выявления его уязвимостей / Н. П. Цыганенко // Тр. БГТУ. Сер. 6: Физико-математические науки и информатика, 2015, № 6. С. 200-203. URL: http://cyberleninka.ru/article/n/staticheskiy-analiz-koda-mobilnyh-prilozheniy-kak-sredstvo-vyyavleniya-ego-uyazvimostey.

Formation Security Problems in Applications for Mobile Systems

Zubkov K. N.,
Diasamidze S. V.
Emperor Alexander I Petersburg State Transport University
St. Petersburg, Russia
e-mail: kirillzubkoff@gmail.com,
sv.diass99@yandex.ru

Abstract. **Mobile phones are not just communications facilities nowadays, but the devices which are the storage of sensitive personal data and unauthorized access to them can lead to unpredictable results. Nowadays modern information security solutions don't allow to resolve the security issues of mobile systems and to assess the possible risks of potential malicious acts. So the problem of systematization of the main mobile applications threats and vulnerabilities becomes important for the following developing of methodology connected with evaluation of information security threats in applications for mobile systems.**

Keywords: **mobile operation system, application, vulnerability, security analysis, mobile platform, mobile device.**

References

1. InfoWatch Analytical Centre. Global research of corporate information leaks and confidential data, 2016 [Analiticheskii Tsentr InfoWatch. Global'noe issledovanie utechek korporativnoi informatsii i konfidentsial'nykh dannykh, 2016]. Available at: https://www.infowatch.ru/report2016 (accessed 1 May 2017).

2. Mikhailov D. M., Zuikov A. V., Zhukov I.Iu., Bel'tov A. G., Starikovskii A. V., Froimson M. I., Tolstaia A. M. Study of the Vulnerability of Mobile Devices of Apple and Google Systems [Issledovanie uiazvimosti mobil'nykh ustroistv sistem Apple i Google], *Special Technics and Communication [Spetstekhnika i sviaz']*, 2011, no. 6, pp. 38-40.

3. Kornienko A. A., Adadurov S. E., Glukhov A. P. Information Security and Information Protection in Rrailway Transport [Informatsionnaia bezopasnost' i zashchita informatsii na zheleznodorozhnom transporte]: in 2 is. – Is. 1: Methodology and system for ensuring information security in railway transport [Metodologiia i sistema obespecheniia informatsionnoi bezopasnosti na zheleznodorozhnom transporte]. Moscow, UM ZhDT, 2014. 440 p.

4. Anton K., Bird J., Manico J. OWASP Top-10 Proactive Controls 2016. *The OWASP Foundation*, February, 2016. Available at: https://www.owasp.org/images/5/57/OWASP_Proactive_Controls_2.pdf.

5. Rovelli P. Developing a Next-generation Mobile Security Solution for Android. April 2014 School of Computer Science Reykjavík University. Available at: http://skemman.is/stream/get/1946/19500/43671/1/Developing_a_next-generation_Mobile_Security_solution_for_Android_-_Paolo_Rovelli.pdf.

6. Safin L. K., Chernov A. V., Aleksandrov Ia. A., Troshina K. N. A Study of Mobile Application Security. [Issledovanie informatsionnoi zashchishchennosti mobil'nykh prilozhenii]. *Cybersecurity issues* [*Voprosy kiberbezopasnosti*], 2015, № 4 (12), pp. 28-37. Availble at: http://cyberleninka.ru/article/n/issledovanie-informatsionnoy-zaschischennosti-mobilnyh-prilozheniy.

7. Diasamidze S. V., Kuzmenkova E. Yu., Kuznetsov D. A., Sarkisyan A. R. Implementation of the Role Based Access Control in Application for Mobile Device on the Android OS Platform // Intelligent technologies in transport [Intellektual'nye tehnologii na transporte], 2016, no. 1, pp. 21-26.

8. Toliupa E. A. Method to Provide Safety for Customer of Application's Store [Metod obespecheniia bezopasnosti pol'zovatelei internet-magazinov mobil'nykh prilozhenii], *Applied Discrete Mathematics. Application [Prikladnaia diskretnaia matematika. Prilozhenie]*, 2014, no. 7, pp. 101-103. Available at: http://cyberleninka.ru/article/n/metod-obespecheniya-bezopasnosti-polzovateley-internet-magazinov-mobilnyh-prilozheniy.

9. Tsyganenko N. P. The Static Analysis of Mobile Applications Code as Vulnerabilities Detection Method [Staticheskii analiz koda mobil'nykh prilozhenii kak sredstvo vyiavleniia ego uiazvimostei], *Proceedings of BGTU. Series 6: Physics and Mathematics and Computer Science [Trudy BGTU. Seriia 6: Fiziko-matematicheskie nauki i informatika]*, 2015, no. 6, pp. 200-203. Available at: http://cyberleninka.ru/article/n/staticheskiy-analiz-koda-mobilnyh-prilozheniy-kak-sredstvo-vyyavleniya-ego-uyazvimostey.