Министерство образования оренбургской области государственное автономное профессиональное образовательное учреждение

«Оренбургский Колледж Экономики Информатики» (ГАПОУ ОКЭИ)

Исследовательская работа на тему: "Безопасность в мобильных приложениях"

Выполнил: Барагузин К.В.
Группа: 1ис1
Руководитель: Бухарова Э.Э.
Консультант: Кирьянова Д.А.

Цель и задачи:

Цели: Понять как работает приложение и каким образом происходит утечка данных.

Задачи:
Исследовать работу приложения.
Найти уязвимости при его работе.
Найти способ устранения этих уязвимостей.

Методы исследования

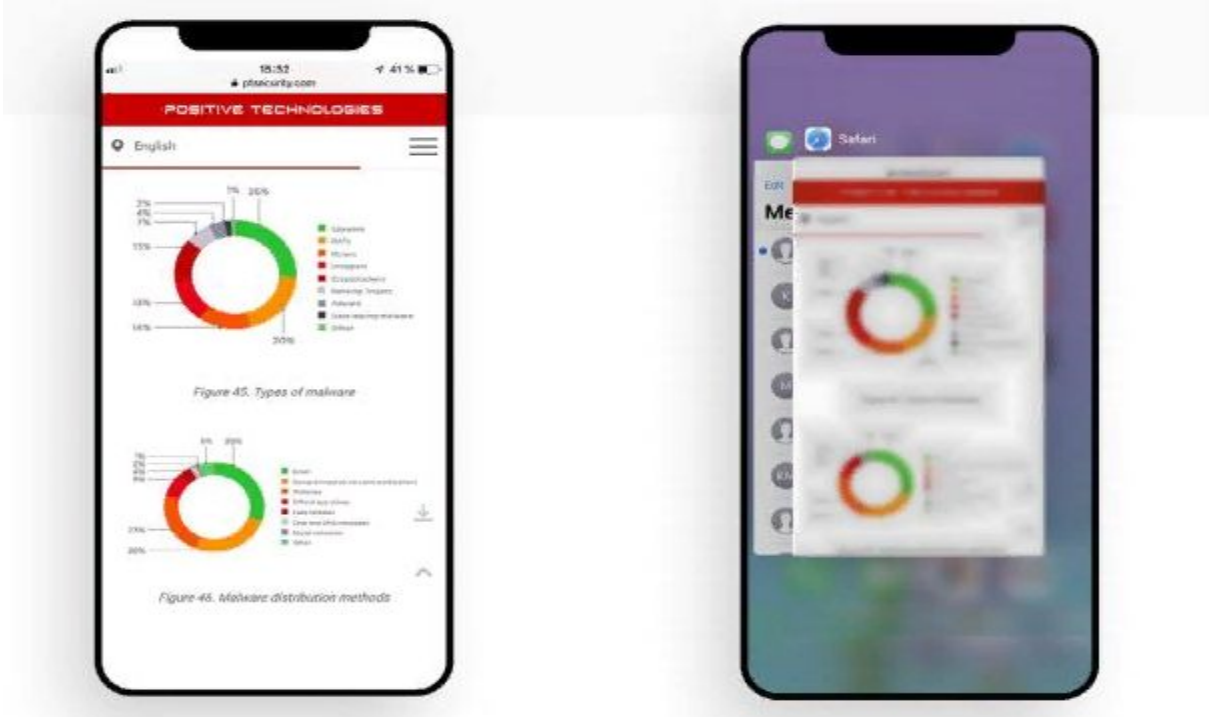
Сбор и анализ данных по этой теме, вывод заключений.

Поиск нужной информации в интернете.

С точки зрения обычного пользователя, установленная на смартфон программа — это и есть мобильное приложение, ведь именно с ней он взаимодействует напрямую: совершает покупки, оплачивает счета, просматривает почту. Но в действительности есть еще один компонент, который принято называть сервером.
Серверная часть находится на стороне разработчика. Зачастую ее роль выполняет то же программное обеспечение, которое отвечает за генерацию и обработку контента на сайте. Другими словами, чаще всего серверная часть — это веб-приложение, которое взаимодействует с мобильным клиентом через интернет посредством специального интерфейса (API). Сервер по праву можно считать главной частью: здесь обрабатывается и хранится информация; помимо этого, он отвечает за синхронизацию пользовательских данных между устройствами.

В мобильных устройствах есть возможность просмотра недавно использованных программ и быстрого переключения между ними. Для этого, когда пользователь сворачивает приложение, операционная система делает снимок состояния экрана. Прямой доступ к снимкам есть только на устройствах с административными привилегиями. Важно предусмотреть вариант, при котором на скриншотах экрана окажутся чувствительные данные; например, в случае с мобильным банком на изображение могут попасть данные платежной карты. Эти изображения могут быть похищены, например если устройство заражено вредоносным ПО.

Способ решения: Используйте специальное фоновое изображение, которое будет перекрывать экран приложения, содержащий чувствительную информацию.

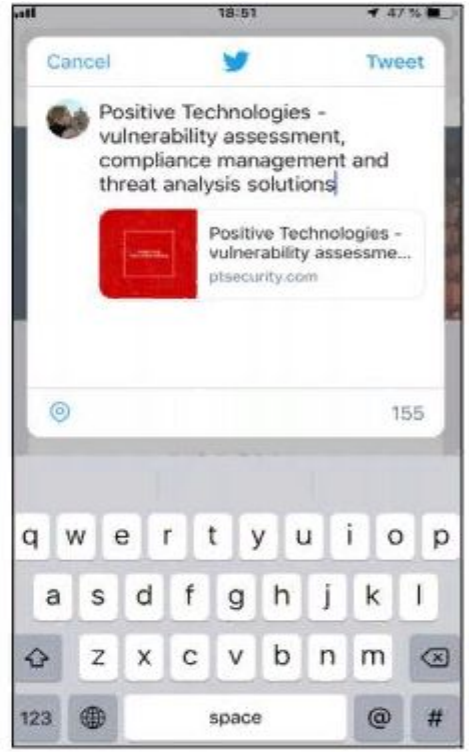


Межпроцессное взаимодействие в iOS-приложениях, как правило, запрещено, однако существуют случаи, когда оно необходимо. В iOS версии 8 компания Apple представила новую технологию под названием App Extensions, с помощью которой приложения могут делиться своими функциональными возможностями с другими установленными на устройстве приложениями (например, мобильные приложения для социальных сетей позволяют быстро делиться контентом из браузера).

Способ решения: IOS: При необходимости использовать ссылки для взаимодействия между компонентами приложения используйте защищенный механизм Universal Links

Вызывающее приложение (Host App)
В данном случае браузер Safari

Основное приложение (Containing App)
В данном случае Twitter



Расширение (App Extension)
В данном случае расширение для Twitter

В 2018 году, анализируя мобильные приложения для iOS, мы могли столкнутся с ошибкой в механизмах их защиты, как отсутствие ограничений на использование установленных пользователем клавиатурных расширений. Компания Apple позволила использовать клавиатуры сторонних производителей начиная с iOS версии 8, в это время такая возможность уже существовала в Android. Стоит отметить, что iOS накладывает более строгие ограничения на использование клавиатуры, чем Android; однако Apple не может контролировать, что делают разработчики клавиатур с данными нажатия клавиш, если пользователь разрешает этим приложениям сетевое взаимодействие.

Способ решения: IOS: Реализуйте метод shouldAllowExtensionPointIdentifier класса UIApplicationDelegate, запрещающий использовать клавиатурные расширения в приложении

Android: Если в приложении предполагается ввод чувствительных данных (например, финансовой информации), реализуйте собственную клавиатуру. Это защитит от атак с подменой системной клавиатуры

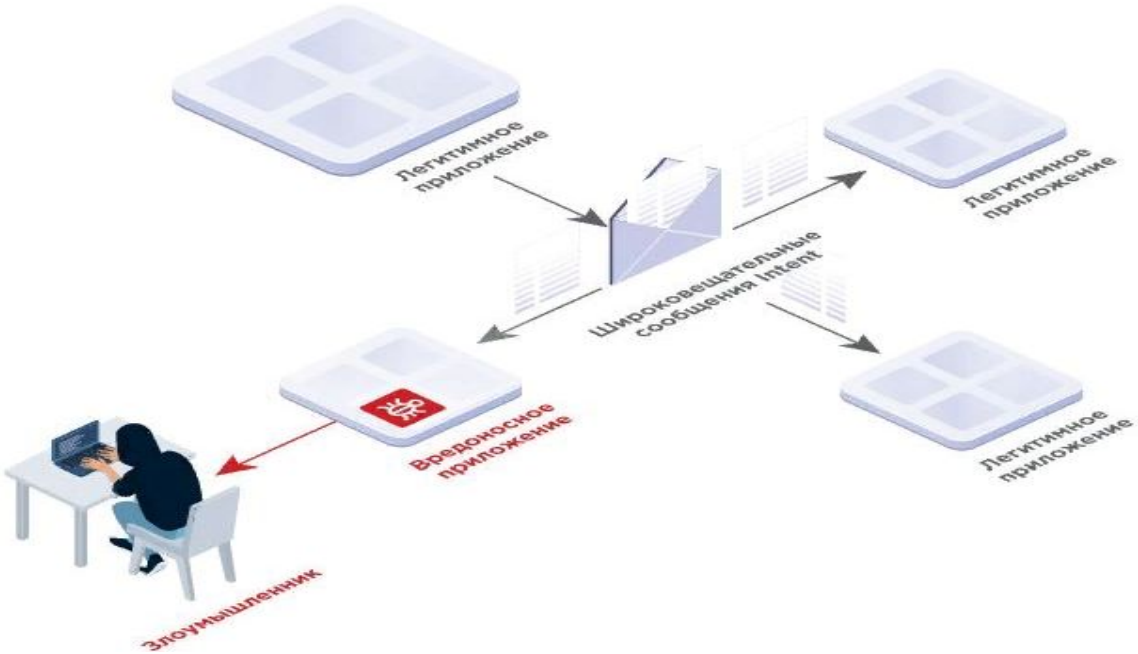
25% приложений для платформ Android позволяют создавать резервную копию при подключении мобильного устройства к комьютеру. Каждая третья уязвимость мобильных приложений для Android связана с недостатками конфигурации. Например, при анализе файла AndroidManifest.xml наши специалисты нередко обнаруживают директиву android:allowBackup в значении true. Это позволяет создавать резервную копию данных приложения при подключении к компьютеру. Недостатком может воспользоваться злоумышленник и получить данные приложения даже без прав пользователя root.

Способ решения: Android: Запретите создание резервной копии данных приложения при подключении мобильного устройства к компьютеру, установив директиву android:allowBackup в значение false.

```
<manifest  >
    ...
    <application android:allowBackup="false"  >
        ...
    </application>
</manifest>
```

Небезопасное использование межпроцессного взаимодействия — распространенная критически опасная уязвимость, которая позволяет злоумышленнику удаленно получить доступ к данным, обрабатываемым в уязвимом мобильном приложении. Остановимся на ней более подробно.
Операционная система Android предоставляет механизм взаимодействия компонентов приложения посредством сообщений (объектов класса Intent). Если для обмена сообщениями используются широковещательные рассылки, то чувствительные данные, содержащиеся в этих сообщениях, могут быть скомпрометированы вредоносным ПО, зарегистрировавшим свой обработчик широковещательных сообщений (компонент BroadcastReceiver).

Способ решения: Android: Используйте компонент LocalBroadcastManager для отправки и получения широковещательных сообщений, не предназначенных для сторонних приложений.



Заключение

Мобильные приложения развиваются с каждым днём, но в них так же присутствуют уязвимости, различные недоработки и лазейки, которыми могут воспользоваться злоумышленники. Некоторые из можно решить самому, другие же, исправляются на программном уровне.
Пользователи могут сами способствовать компрометации своих устройств: расширять стандартные возможности смартфона, лишая его защиты, переходить по подозрительным ссылкам в SMScообщениях, загружать программы из неофициальных источников, поэтому безопасность пользовательских данных — ответственность не только разработчиков приложений, но и самих владельцев мобильных устройств.

Именно поэтому советуем Вам быть более внимательным в установке приложений из неизвестных источников, следить за тем какие разрешения Вы даёте приложению и использовать максимально возможные уровни защиты.

Если мы в угоду безопасности отдаём свободу — мы лишаемся и того и другого.

(C) Вячеслав Вячеславович Мальцев.