Лекция №11
Тема: Механизмы обеспечения безопасности Android

7.11.2020 (ИСИП-19-1,2,3)

Введение

При разработке любого мобильного приложения, обрабатывающего пользовательские данные, важно уделить внимание безопасности. Каждый год появляются новые технологии и возможности, а вместе с ними — новые особенности поведения и уязвимости.

Предпосылки к появлению угроз Android

1. Открытость

2. Фрагментация платформы

3. Человеческий фактор: халатность, социальная инженерия и глупость

Открытость

Во-первых, *это доступность кода*, который может быть использован, модифицирован и улучшен разработчиками в зависимости от их потребностей и идей. С одной стороны, для производителей устройств и разработчиков это несомненный плюс, с другой стороны, это дает возможность не только исследователям, но и злоумышленникам более продуктивно находить уязвимости и ошибки.

Во-вторых**,** существует возможность *установить приложения как из официального каталога приложений* Google Play (ранее назывался Android Market), так и из любого другого доступного источника.

***В-третьих*,** создание приложений является практически общедоступным, так как необходимо заплатить деньги в случае, если разработчик желает размещать свои продукты в официальном каталоге, а для распространения программ вне его материальные затраты не нужны.

***В-четвертых*,** размещаемые в Google Play программы *до недавнего времени не подвергались предварительной проверке* или тестированию со стороны Google.

Фрагментация платформы

По мере выхода очередного обновления системы в нее добавляются не только новые функции, но и закрываются обнаруженные ранее уязвимости. Производители на свое усмотрение выпускают соответствующие версии обновлений. Иногда случается так, что аппарат, еще недавно бывший флагманом, не получает новую версию ОС или программного обеспечения и, соответственно, остается незащищенным от потенциальных угроз.

Человеческий фактор: халатность, социальная инженерия и глупость

Каким бы ни был уровень защищенности системы, далеко не последнюю роль в обеспечении безопасности играет человеческий фактор.

Приложения также могут подделываться, и невнимательный пользователь с большой долей вероятности поделится со злоумышленниками своими персональными данными (логин и пароль от социальной сети, данные кредитной карты и т. п.).

Теория механизмов безопасности Android

Система *Android* базируется на ядре *Linux*, тем не менее ее разработчики сильно модифицировали некоторые базовые механизмы, что в конечном итоге *привело и к усилению защиты*. В частности, рабочая среда *Android* включает в себя драйверы оборудования, поддержку сетевого стека, файловую систему, а также механизмы управления памятью, процессорным временем и расходом электроэнергии.

Все эти механизмы реализуются с помощью библиотек, написанных на языке Си/Си++, но все приложения для *Android* исполняются в виртуальной машине *Dalvik VM*, которая, по своей сути, является подмножеством *Java 5 Standard Edition*.

В отличии от *Java, в* ***Android*** используются свои библиотеки классов и более компактный метод сохранения исполняемых файлов *(выполняемые программы для Android имеют расширение .dex).* Приложения для *Android* формируются в специальные пакеты, которые имеют расширение *.apk* и очень похожи на jar-файлы Java.

Каждое приложение **Android** имеет собственный идентификатор и запускается в собственной виртуальной машине.В Android вместо одного пользователя с высокими привилегиями предусмотрено целых три: ***root, system u rild. ОС Android*** во время загрузки в память запускает мастер-процесс zygote, который порождает новые экземпляры ***Dalvik VM*** — по одному для каждого приложения. Кроме того, во время старта ОС запускается несколько системных процессов **system_server**, которые реализуют все необходимые сервисы операционной системы: процесс **init**, инициализирующий операционную систему; mountd, отвечающий за работу со съемными дисками; **rild**, управляющий взаимодействием с телефонной сетью и другими коммуникационными интерфейсами.

В ***Android*** используется отличный от принятого в *Linux* механизм распределения прав, называемый привилегиями.Так, есть привилегии для работы с мобильной сетью (например, CALL_PHONE), работы с изображениями (CAMERA) или доступа к Интернет (INTERNET), и, чтобы получить определенные привилегии, приложение должно их декларировать в своем описании. При установке приложения набор этих привилегий проверяется, и пользователю предлагается их подтвердить.

Основные угрозы и атаки на Android

1. Вирусы и другое вредоносное ПО

2. Уязвимости Android и ПО

Архитектура Android построена таким образом, что все приложения работают с ограниченными правами и не имеют доступа к защищенным данным других приложений. Начиная с первой версии ***Android*** в системе по умолчанию включен режим ***SELinux (Security Enhanced Linux).*** Он предусматривает принудительный контроль прав доступа на уровне ядра ОС.

1. Одна из главных проблем, с которыми могут столкнуться пользователи, — уязвимости системы, позволяющие ***получить права root.***
2. Одним из ключевых элементов безопасности Android является ***система разрешений (Permission System).*** При установке приложений пользователю демонстрируется список всех функций, которые будут доступны той или иной программе. После установки приложения получают возможность выполнять заложенные в них функции без участия пользователя.

3. Угрозу также может представлять *использование неофициальных или сторонних прошивок*.

Во-первых, в такие прошивки изначально могут быть встроены вредоносные программы. ***Во-вторых,*** когда цифровой подписью образа системы подписывается какое-либо приложение, оно получает те же права, что и сама система, в которой оно работает. В рамках Android Open Source Project (AOSP) подписи для образов являются приватными, поэтому такой сценарий возможен, например, в случае кражи соответствующей подписи.

4. Системные приложения, как стандартные, так и приложения от поставщиков Android-устройств, тоже подвержены уязвимостям.

Методы защиты платформы Android

Безопасность физического доступа.

1.1 Экран блокировки. Чтобы никто не считал личную информацию пока наш смартфон находится вне поля зрения, нужно обязательно ставить защиту на *разблокировку экрана*.

- Пароль
- Графический ключ
- Сканер отпечатков пальцев

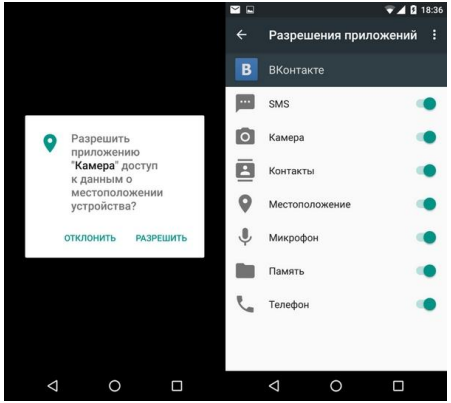
1.2 Шифрование данных.

Впервые появилось в Android 4.3, где пользователь мог ее по желанию активировать. В Android 5.0 Lollipop она же ***задействована по умолчанию*****.** Шифрование данных привязывается к паролю или ПИН-коду на снятие блокировки экрана смартфона – как только вы его ввели происходит дешифровка данных.

1.3 Удаленное управление.

Функция безопасности Android, позволяющая найти потерянный или украденный смартфон (должна быть включена геолокация), а если это сделать невозможно, то — удаленно стереть все свои данные.

Правильная настройка политик безопасности



Особенностью системы безопасности **Android** является то, что любое приложение должно задекларировать все права доступа к функциям системы, на которые она претендует. Это может быть разрешение на использование ***интернета, СМС, голосовых вызовов, камеры и т.д***. Если же такие привилегии не прописаны в инсталляторе приложение, то и доступ к ним будет запрещен. И перед установкой программы пользователь в обязательном порядке должен ознакомится и согласиться со списком этих прав.