УДК 004.056

ОРГАНИЗАЦИЯ ЗАЩИТЫ ДАННЫХ В МОБИЛЬНЫХ УСТРОЙСТВАХ

Шнитко А.В., студент,
Мелихов В.А., студент
Белорусский национальный технический университет
Минск, Республика Беларусь
Научный руководитель: канд.техн.наук, доцент Дробыш А.А.

Аннотация:
Рассматриваются проблемы организации защиты данных в мобильных устройствах. Продемонстрированы виды угроз на мобильных устройствах и пути защиты от них.

Мобильные устройства прочно вошли в жизни людей. Сейчас каждый из нас обладает как минимум одним из таких устройств. Почему же мобильные устройства стали частью жизни людей? Во-первых, самое очевидное – это средство коммуникации, во-вторых, это один из основных рабочих инструментов, который заметно облегчает множество процессов и не привязывает сотрудника к рабочему месту, ведь теперь смартфоны могут иметь в наличии доступных программ такие, как MS Word, MS Excel, MS PowerPoint. Функционал современных смартфонов не уступает функционалу компьютеров. Удаленное администрирование, поддержка VPN, браузеры с flash и java-script, синхронизация почты, заметок, обмен файлами и многое другое доступно на мобильных устройствах.

С таким обилием функционала мобильные устройства содержат десятки гигабайт данных. Все это очень удобно, однако рынок средств защиты для подобных устройств развит еще слабо. Злоумышленники используют любую лазейку, чтобы воспользоваться нужными им данными, например, очень распространенный случай атак – это взлом электронной почты. Обычно люди привязывают к своему электронному адресу множество аккаунтов в социальных сетях, приложениях, интернет-магазинах, и злоумышленники благополучно могут пользоваться этими данными после взлома.

Самыми популярными операционные системы для смартфонов – это Android iOS. В целом, телефоны с Android покупают и используют

гораздо чаще во всем мире - по последним данным эта операционная система установлена на 74% представленных на рынке устройств. Однако по мнению антивирусной компании Trend Micro, операционная система Google Android более уязвима перед лицом хакерских атак, нежели Apple iOS, работающей на iPhone, iPod и iPad [4].

Международное исследовательское агентство Gartner давно обратило внимание на проблему мобильных угроз для коммерческих организаций и в 2019 году выпустило собственное исследование, в котором разделяет угрозы на три основных вида [3]:

- Угрозы уровня устройства.
- Угрозы уровня сети.
- Угрозы уровня приложений.

Угрозы уровня устройства, как правило, связаны с программно-аппаратной начинкой устройства. Злоумышленники ищут способы, чтобы обойти заводскую защиту. Для атак в этом случае хакеры чаще всего используют эксплоиты – программы, фрагменты программного кода или последовательность команд, которые применяются для осуществления атаки на вычислительную систему, их делают вручную либо используют находящиеся в открытом доступе на специализированных форумах [3].

В ситуации угроз уровня сети, злоумышленники используют уязвимые точки каналов связи. Мобильные устройства используют ряд способов и протоколов для коммуникации, например, 3G, LTE, 5G, Bluetooth, Wi-Fi, SMS и тому подобное. Контролируя любой из этих каналов, злоумышленник может вести прослушку за пользователем, манипулировать его действиями.

В этом случае хакеры используют атаку типа «Man-in-the-Middle» (MITM) или «человек посередине», вставая между устройством пользователя и сервером. Особенно опасны атаки, при которых злоумышленнику удается просматривать зашифрованные при помощи TLS/SSL данные сайтов (то есть передающихся по HTTPS), включая логины и пароли. Это достигается либо снятием шифрования, либо подменой сертификата, что позволяет устройству злоумышленника подменять оригинальный сервер и далее обращаться к нему от лица пользователя [3].

В случае с угрозами уровня приложений ситуация, в принцип, понятна. Приложения с вредоносным ПО может попасться пользо-

вателю не только на сомнительных сайтах, но и магазинах приложений—Play Market и App Store. Магазины приложений ежедневно блокируют сотни приложений, которые не проходят проверку на вредоносное ПО. Хакеры используют приложения для внедрения различного рода угроз, которые могут просто кликать по рекламе, а могут зашифровать информацию на устройстве и вымогать деньги у владельца.

Также существует термин «серое ПО» — его еще называют нежелательным. Это такие приложения, которые необязательно являются вредоносными, но могут конфликтовать с корпоративными политиками и подвергать риску корпоративные данные. Серое ПО включает в себя приложения, которые могут привести к утечке данных. Пример серого ПО — это приложения, у которых есть разрешения на доступ к списку контактов устройства, и они собирают эту информацию для отправки рекламодателю [3].

Отдельно от всего можно рассмотреть атаки на серверную часть мобильных приложений, поскольку в этом случае доступ к устройству злоумышленнику не требуется [1].

Видов и сценариев атак очень много, но что же насчет защиты данных мобильных устройств? На рынке кибербезопасности существует отдельная группа решений, которые называются MTD (Mobile Threat Defence) и их основная задача — это защита мобильных устройств от угроз [2].

Эти решения защищают от всех трех типов угроз.

На уровне устройства MTD отслеживают такие показатели, как:

- версии ОС;
- версии обновлений безопасности;
- системные параметры;
- конфигурация устройства;
- микропрограммное обеспечение;
- системные библиотеки.

В этом случае решения выявляют уязвимые места устройства, настроек безопасности. MTD-инструменты проверяют изменения в системных библиотеках и конфигурациях, а также наличие на устройстве Jailbreak или Root-доступа [2].

На уровне угроз сети решения отслеживают трафик на предмет подозрительного или несанкционированного поведения. Здесь про-

веряется наличие недействительных или поддельных сертификатов, а также выявляются уязвимости в протоколах.

На уровне приложений MTD определяют нежелательные и вредоносные программы. Для этого используются статические методы анализа, включая сигнатуры и репутацию известных угроз, оценку запрашиваемых приложением разрешений, используемые библиотеки. Некоторые производители MTD выполняют также разбор мобильных приложений до уровня исходного кода, чтобы гарантированно обнаружить угрозу [2].

Список использованных источников

1. Безопасность мобильных устройств и приложений [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/pt/blog/509814/ – Дата доступа: 10.03.2021.

2. Мобильные угрозы: защита смартфонов и планшетов [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/new-renewal-center/home – Дата доступа: 13.03.2021.

3. Разновидности актуальных мобильных угроз [Электронный ресурс] – Режим доступа: https://update.megafon.ru/post/mobile-threats – Дата доступа: 10.03.2021.

4. Что безопаснее Android или iOS? [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/resource-center/preemptive-safety/android-vs-ios – Дата доступа: 10.03.2021.