Демидов А.А., Кондрушин И.Е., Демидова У.А.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
email: aademidov@list.ru

Анализ атак и моделей нарушителей мобильных устройств

Многие предприятия стали задаваться актуальностью вопроса связанных с безопасностью передачи данных, которые могут выдать персональные данные и местоположения людей на территории различных предприятий.

В настоящее время мобильные устройства становятся незаменимым помощником в жизни каждого человека. Затруднительно найти человека, который не пользуется мобильным телефоном.

Для удобства навигации и позиционирования в закрытом пространстве стали актуальны исследования в пользу инерциальной навигации и позиционированию в сенсорной сети на основе Bluetooth Low Energy маяков.

Параллельно этому вырос спрос на информационную безопасность данных позиции человека используемого мобильного устройства.

Атаки на мобильные устройства возможны при следующих ситуациях:

— Физический доступ к мобильному устройству;

При физическом доступе злоумышленник получает доступ к файловой системе, даже наличие аутентификационной защиты на устройстве злоумышленнику несложно получить персональные данные.

С использованием криптографических средств защиты имеется возможность шифрования основных данных и острой необходимости удаление их с мобильного устройства, а также появляется возможность выявления канала утечки данных в ходе использования шифрования.

— Вредоносное приложение, установленное на мобильное устройство;

После установки вируса или вредоносного программного обеспечение на устройство, злоумышленник вправе поднять свои привилегии в операционной системе и пользуясь обычной передачей данных, может получить удаленный доступ к устройству, что приведет к полному захвату устройства, а так же полной утечки личной информации хранящейся на нем.

Регулярное обновление программного обеспечения на мобильном устройстве, а также использование программных средств защиты и повышения осведомленности пользователей предприятия об информационной безопасности мобильного устройства, поможет от утечек конфиденциальных данных пользователя.

— Использование контролируемого канала передачи данных;

В ходе атаки типа “Человек посередине” перехватываются данные между устройством и клиент-сервером. Для реализации данного способа атаки необходимо находиться в одной сети с клиентом и эмитировать поддельные точки доступа. В итоге злоумышленник может прослушать и подменять передаваемые данные, что приведет к краже личных данных.

При использование верной реализации работы с SSL в мобильном приложение при передаче пакетов данных на сервер доверять исключительно SSL-сертификату банка, данное действие может уберечь от компрометации корневого центра сертификации.

Из вышеописанных угроз можно точно выделить несколько модель угроз, которые являются актуальными на данный момент, а именно:

— Злоумышленник, имеющий физический доступ к устройству клиента. При этом на устройстве не включена блокировка экрана и не используется шифрование.

— Злоумышленник, не имеющий доступ к устройству, находящийся рядом с жертвой и способный провести атаку типа «человек посередине».

— Злоумышленник, который загрузил на устройство клиента свое вредоносное приложение, используя официальные магазины приложений или иные способы.

Литература

1. Стефаров, А. П. Формирование типовой модели нарушителя правил разграничения доступа в автоматизированных системах / А. П. Стефаров, В. Г. Жуков // Известия ЮФУ. Технические науки. — 2012. — № 12 (137), Т. 137. — С. 45–54.

2. Чекалин, А. А. Защита информации в системах мобильной связи / А. А. Чекалин, А. В. Заряев, С. В. Скрыль, В. А. Вохминцев. — Москва : Горячая линия — Телеком, 2005. — 171 с.