Эссе №6
Курс: Защита информации

Воробьев Олег

8 июня 2015 г.

В данной статье автор рассматривает вопросы безопасности данных в мобильных приложениях. Автор рассматривает систему Android как наиболее удачный объект исследований. Она привлекательна как очень популярная система для мобильных устройств следовательно, содержащая большой объем информации о данных пользователя. Так же дольшое количество приложений под эту систему делает оюъем данных, контактирующих с ней еще более внушительным.

Например режим ECB. Главная его уязвимость заключается в том, что одинаковые фрагменты данных с помошью этого алгоритма шифруются одинаковым шифром. Дананя система может быть усилена добавлением случауного числа "соли"в функцию, что создаст больше сложности с подбором.

Анализ безопасности проволится на основе собственноручно разработанного инструмента на базе androguard-framework. Основная идея состоит в поиске по исходному коду значений инициализирующих векторов, ключей и т.д. а так же криптоалгоритмов. При помощи этого приложения исследовано 11 748 приложений среди которых 10 327 используют криптографию неправильно, а это больше 85

Далее приводится три алгоритма шифрования с различными типами блочного шифрования. Анализируя алгоритмы автор предлагает нам в качестве резюме 6 правил для правильного использования защита информации в Android системах.

- Не использовать ECB режим при криптографии
- Не использовать non-randon IV для CBC шифрования
- Не использовать константные ключи шифрования
- Не использовать константную соль для шифрования на основе пароля
- Не использовать менее 1000 итераций для шифрования на основе пароля
- Не использовать постоянные seed для получения псевдослучайных последовательностей SecureRandom()

Правило 1 запрещает использоавть ECB так как эта схема шифрования не предоставляет должных параметров безопасности. Правило 2 весьма очевидно. Использование динамических колчей шифрования значительно повысит криптоустойчивость системы. Правило 3 аналогичо правилу 2. Правило 4 и 5 выведено чисто опытным путем для PBE схем.

Инструмент автора проверяет соблюдение этих правил. Приложения на android не схожи с обычными java приложениями. За их выполнение отвечает виртуальная машина Dalvik, которая имеет мало схожего со стандартной BM Java. Такие приложения получают доступ к графическому интерфейсу и подсистемам. При помощи JCA регистрируются cryptographic service

providers (CSP), которые отвечают за большинство алгоритмов. Для использования этих алгоритмов необходимо вызвать метод Cipher.getInstance.

Следует отметить, что по умолчанию выбирается режим шифрования ECB. В статье разобрано подробно, как строились графы потока управления приложения. И показывалось, как в них находились нарушения. Так же проволится анализ нескольких популярных приложений.

В заключении автор еще раз говорит, что 88 процентов протестированных приложений оказались несоответствующими хотя бы одному правилу. Основываясь на выводах с огромного анализа реальных приложений, автор надеется что в дальнейшем безопасность Android систем.