Эссе №6

Анастасия Тарасова

10 июня 2015 г.

В этой статье рассматривается безопасность данных в мобильных приложениях. Автор считает систему Android удачным объектом исследований. Система Android - очень популярная система для мобильных устройств ,а значит, содержит много информации о пользователе. Множество приложений под эту систему также увеличивает объем данных.

Режим ECB. Его главная уязвимость - одинаковые фрагменты данных с помошью алгоритма ECB алгоритма шифруются одинаковым шифром. Эта система может быть усилена добавлением случайного числа в функцию, что создаст больше сложности с подбором.

Анализ безопасности проводится на основе собственного разработанного инструмента на базе androguard-framework. Идея заключается в поиске по исходному коду значений инициализирующих ключей, векторов и криптоалгоритмов. С помощью этого приложения было исследовано 11 748 приложений среди которых более 85% шифруют данные неверно.

Затем 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 пользоваться ECB так как эта схема шифрования не имеет должных параметров безопасности. Правило 2 - использование динамических колчей шифрования повысит криптостойкость системы. Правило 3 аналогично правилу 2. Правило 4 и 5 выведено чисто опытным

путем для PBE схем. Инструмент автора проверяет соблюдаются эти правила или нет. За выполнение андроид-приложений отвечает виртуальная машина Dalvik, которая не похожа на ВМ Java. При помощи JCA регистрируются cryptographic service providers (CSP), которые отвечают за большинство алгоритмов. Для использования этих алгоритмов необходимо вызвать метод Cipher.getInstance. 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 проводился 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 улучшится.