Исследование неправильного шифрования в Android-приложениях

Агафонова Оксана

11 июня 2015 г.

В Android-приложениях разработчиками используется шифрование API-интерфейсов, с целью защиты данных на мобильных устройствах, таких как пароли и личная информация. Для шифрования они используют общие знания о безопасности, например, IND-CPA безопасность. Ими используются примитивы шифрования, как блочные шифры и код аутентификации сообщений (MACs) для защиты данных и информации.

При алгоритме шифрования ECB идентичные фрагменты данных шифруются одинаковыми блоками шифров, таким образом, не обеспечивается IND-CPA-безопасность.

Для статического анализа проверки безопасности используется инструмент CryptoLint, основанный на анализе программы Androguard Android. Основная ее идея заключается в поиске по исходному коду значений инициализирующих ключей, векторов и криптоалгоритмов. С использованием CryptoLint было проведено исследование по реализации шифрования на 11748 Android-приложениях. В результате 10 327 программ (88%) использовали шифрование неверно.

Был предложен процесс исправления. Во-первых, во время проверки инструментами разработчика можно проверить несколько свойств безопасности, на корректность шифра. При добавлении в CryptoLint легкой проверки, улучшается безопасность. Во-вторых, реализуется предположение о правильном использовании шифрования. Например, документация о шифровании CBC утверждает, что вектор инициализации не должен быть постоянным. В-третьих, не рекомендуется поведение по умолчанию в библиотеках шифрования. Например, в Android-приложениях по умолчанию выполняется режим блочного шифрования (ECB) для AES. Чтобы исправить эту проблему, предлагается изменить поведение по умолчанию на более безопасный вариант. А именно:

1. Предлагаются легкие методы статического анализа и инструменты, которые могут поймать неправильное использование шифрования.
2. Провести крупномасштабный эксперимент для измерения неправильного использования шифрования в Android.
3. Предлагаются меры по восстановлению.

CryptoLint проверяет реальные Android-приложения на нарушение шести правил безопасности, изложенных ниже:

1. Не использовать ECB режим при криптографии
2. Не использовать non-randon IV для CBC шифрования
3. Не использовать константные ключи шифрования
4. Не использовать константную соль для шифрования на основе пароля

5. Не использовать менее 1000 итераций для шифрования на основе пароля

6. Не использовать постоянные seed для получения псевдослучайных последовательностей SecureRandom()

В результате 10327 Android-приложений (88 % от вышеуказанного набора), которые нарушили хотя бы одно из правил.