An Empirical Study of Cryptographic Misuse in Android Applications

Дедков Сергей

2015

1 An Empirical Study of Cryptographic Misuse in Android Applications

Авторы данной статьи опросили разработчиков, используют ли они криптографические API которые обеспечивают криптографическую безопасность. Разработали методы анализа и проанализировали Google Play рынок, обнаружив, что 10327 из 11748 приложений - используют криптографические интерфейсы. 88% допустили хотя бы одну ошибку.

Разработчики используют криптографические примитивы, такие как блочные шифры и код аутентфикации сообщения(MAC) для защиты данных и связи. Криптографы знают, что есть правильный способ и неправильный способ использовать эти примитивы, где правильный способ обеспечивает надежные гарантии безопасности, а неправильный способ неизменно приводит к беде.

Так например используя режим ECB, разарботчики подвергают свое ПО уязвимостям. Такой режим уязвим, т.к. в нем одинаковые фрагменты шифруются в одинаковую последовательность. Для предотвращения к блокам добавляют соль, для более сложного взлома.

Авторы предлжили 6 правил. Любое приложение, которое нарушает одно из них не может быть безопасным:

- Не используйте режим ECB для шифрования.
- Не используйте неслучайный IV для шифрования CBC.
- Не использовать постоянные ключи шифрования.
- Не используйте постоянные соли для PBE.
- Не используйте меньше 1000 итераций для PBE.
- Не используйте статические семена посеять SecureRandom (·)

Авторами был разработан инвтрумент CryptoLint для анализа для оценки соблюдения этих правил в реальных Android-приложениях.

В отличие от обычных java-приложений Android-приложение запускается на виртуальной машине Dalvik. С этим байкодом и работает инструмент авторов - CryptoLint. Приложения, которые запускаются на виртуальной машине Dalvik получают доступ к интерфейсу и подсистемам. Для получения доступа к алгоритмам шифрования вызывается метод Cipher.getInstance, которые зарегистрированы в cryptographic service providers (CSP), в подсистеме Java Cryptography Architecture (JCA).

В такой реализации по-умолчанию выбирается ECB шифрование. Авторами проводились исселдования графа потока управления приложения и то, как находились нарушения. В качестве примера было рассмотрено 3 популярных приложения с уязвимостями, при этом эти приложения имели миллионы скачиваний.