ПОДДЕРЖКА DIGITAL RIGHTS MANAGEMENT В МОБИЛЬНЫХ УСТРОЙСТВАХ НА БАЗЕ ANDROID

П.В. САВЧЕНКО, Е.Р. ПЕЛЬКИН

Возросшая популярность мобильных устройств под управлением системы Андроид, ставит перед пользователем компьютерной техники новые проблемы. Одна из них, для многих достаточно важная, это защита информации на мобильных устройствах под управлением Андроид.

Большинство DRM решений построены по единой архитектуре. Защищаемый контент предварительно шифруется DRM модулем шифрации (как правило, применяется AES-128), а модуль управления лицензиями выдает ключи пользователям на просмотр контента (как правило создается на базе Java сервера приложений). Такая реализация позволяет эффективно разделить этапы обработки контента, доставки контента и управления разрешениями на использование.

В случае Android системы защиты контента приложение берет на себя лишь дешифрацию данных получаемых по HTTP Live Streaming протоколу при помощи заранее указанного ключа дешифрации. В качестве алгоритма используется стандартный AES-128. в этом случае разработчику приложения нужно реализовать на серверной части механизм сохранения ключей шифрации и очень аккуратной их выдачи, а на клиентской части обеспечить качественный прием этих ключей с минимальным риском для перехвата (например, обеспечить jailbreak detection в приложении).

При доставке ключей в приложение для защиты ключей предлагается использовать HTTPS. При этом остается риск перехвата ключа, в тех случаях если произвели взлом устройства (Jailbreak) или каким-то образом сэмулировали на PC данное устройство. Существенно снизить этот риск, можно лишь при написании своего приложения, реализовав дополнительные проверки.

НЕРАВНАЯ ЗАЩИТА ДАННЫХ ПРИ ПОМОЩИ НЕРАВНОМЕРНОГО ДВУМЕРНОГО КОДИРОВАНИИ ИНФОРМАЦИИ

НЕСТОР АЛЬФРЕДО САЛАС ВАЛОР

Известны многие алгоритмы декодирования двумерного неравномерного кодирования информации. Одним из них является алгоритм на основе нахождения на предварительном этапе обработки кодеком данных всевозможных комбинаций размещения ошибок определенной кратности ti в сжатой форме. Все эти образы ошибок формируют общую библиотеку образов ошибок и для каждого образа формируются правила идентификации ошибок соответствующей кратности. Известна библиотека образов ошибок для неравномерного совместного способа кодирования информации. Однако, данный способ кодирования и декодирования информации неэффективен и сложен в реализации при коррекции многократных ошибок.

Для устранения данных недостатков предложен метод формирования библиотеки образов ошибок на основе двумерного равномерного кодирования информации. Установлено, что при данном способе кодирования и декодирования общее число образов трехкратных и четырехкратных ошибок уменьшается примерно на 32% и 18% соответственно по сравнению с использованием библиотеки образов ошибок при неравномерном совместном кодировании и декодировании информации. Уменьшение общего числа образов обеспечиваются за счет исключения из