Технология защиты от копирования

Писарев А.А.,Орёл ГТУ

Технология AACS (Advanced Access Content System) специально разработана для защиты аудио- видеоданных, находящихся на оптических носителях стандарта BD. С помощью неё определяются правила обращения к защищенному содержимому. Она построена на основе алгоритма шифрования со 128-битным ключом и средств блокировки медиаданных. Более того, технология не только пресекает попытки несанкционированного копирования, но и определяет допустимый порядок перемещения аудио- и видеосигнала в рамках домашней сетевой среды.

Одной из функций упомянутой технологии является «Image Constrain Token», которая производит преобразование сигнала высокой четкости в менее качественный вариант (960x540) при его трансляции посредством аналогового соединения или интерфейса HDMI, не поддерживающего технологию HDCP. Включение данной возможности в систему защиты оптического диска будет производиться непосредственно самим обладателем авторских прав. Однако в текущий момент она еще не используется. Еще одной функцией технологии AACS является «Digital Only Token», которая вовсе запрещает вывод видеосигнала через аналоговый коннектор. Применяться она будет исключительно в деловой среде (например, предварительный вариант киноленты, представленный в формате высокой четкости).

Функция «Audio Watermark». Подразумевает возможность включения в звуковую дорожку уникальных эффектов, не воспринимаемых человеком, однако также препятствующих попыткам незаконного копирования содержимого носителя. В текущий момент еще не используется. Ожидается, что ее поддержка будет интегрироваться в оптические приводы после выхода

Ёе ограничения оказались настолько честными, что не смогли стать сколько-нибудь серьезной преградой. Любую музыку, купленную через iTunes, можно записать на незащищенный аудиодиск. Несмотря на это, хакеры пошли дальше, убрав DRM-защиту вообше, что дало пользователям возможность избежать связанного с потерями качества перекодирования. Норвежец Jon Lech Johanssen взломал защиту FairPlay в ноябре 2003 года. Его программа QTFairUse сохраняет лишь медиаданные полученного от iTunes музыкального произведения, удаляя при этом DRM-защиту. Конечно, программисты Apple нарастили броню и усовершенствовали защиту FairPlay, однако снаряд под названием QTFairUse, выпущенный летом 2006 года, пробил и ее. Пока неприступной остаётся лишь версия iTunes 7.0.2.

В августе 2006 года хакер под псевдонимом Viodentia выложил в Сети программу под названием Fair-Use4WM. с помощью которой любой пользователь мог удалить средство DRM-защиты Plays ForSure. При этом хакер хотел лишь из простого честолюбия помериться силами с ведущим игроком музыкального рынка. Таким образом, Viodentia выяснил, что Microsoft использует «простую процедуру обеспечения безопасности». У плееров Media Player 10 и 11 (b) 56-битный ключ свободно располагается в оперативной памяти и может быть легко извлечен оттуда.

Особенно сильно успех Viodentia затрагивает службы типа Napster. Этот портал разрешает неограниченное скачивание музыки всего за $10 в месяц. Ее DRM ограничивает срок пользования записью 30 днями. Клиенту достаточно один раз заплатить $10, подключиться к Napster, скачать и раскодировать все, что нужно.

После двух обновлений DRM-защиты Microsoft выпустила финальную версию плеера Media Player 11, с которой FairUse4WM больше не сотрудничает. Microsoft пытается привлечь к суду хакера.Viodentia украл у Microsoft коды, чтобы написать свою программу. Хакер возражает, что ему совсем не требовалось пользоваться исходными кодами. Применяемые программистами Microsoft библиотеки с алгоритмами шифрования открыты

для общего пользования, и любой желающий может с ними работать. Против утилиты бессильны любые «заплатки». Они лить затруднили бы и на некоторое время замедлили поиск в RAM нужных данных.

Еше никогда затраты на создание средств защиты от копирования не были так велики: файлы видеофильмов Blu-ray и HD-DVD зашифрованы постоянно, причем неважно, находятся ли они на дисках, передаются в компьютере от одного компонента к другому или направляются от видеоплаты к монитору. Сам фильм защищен средствами AACS, пути передачи закрывают аппаратные средства зашиты HDCP.

У обычного пользователя все это вызывает отрицательные эмоции, так как привели к дополнительным расходам. Теперь ему нужно менять свою видеоплату на новую, с поддержкой функции HDCP, и покупать такой же монитор. Системный блок тоже приходится апгрейдить. прибавляя ему быстродействия. И все эти расходы на HDCP не имеют никакого смысла, если исходная система AACS уже взломана.Шифрование контента также не имеет никакого смысла, хотя это звучит странно, хотя AACS использует 128-битное кодирование AES — алгоритм, который пока не удалось взломать.Для защиты содержимого диска AACS использует данный алгоритм с целым набором ключей. Часть ключей имеется в плеере, другая часть — на диске. Из обоих половинок вычисляется Volume Unique Key (VUK), который и позволяет раскодировать содержание фильма. Именно этот ключ и нужен хакеру. Никаких ухищрений для этого не требуется,только вставил HD-диск в дисковод и запустил программный .

Конечно, параллельно с этим нужно открыть hex-редактор и прочитать содержимое операционной памяти компьютера, в которой знающий человек без труда отыщет тот самый ключ VUK. 27 декабря 2006 года хакер по имени Muslix64 предал огласке свое открытие. Заодно была выложена и Java-программа под названием BackupHDDVD, способная копировать диски HD-DVD.

В зависимости от уровня подготовки пользователя может пройти несколько недель, пока в hex-коде удастся вычислить нужную последовательность символов ключа Volume Unique Key и понять, какие плееры можно использовать для успешного поиска. Пока же известно, что OEM-версии плееров WinDVD 8, а также PowerDVD 6.5 и 6.6 годятся для начинающих хакеров. Muslix64 быстро вычислил, что аналогичная дыра существует и у Blu-ray-плееров, для которых написана утилита BackupBluray. Опытному хакеру для взлома достаточно было взглянуть на спецификацию BD и состояние памяти, записанное в hex-редакторе и присланное ему кем-то из друзей (у Muslix64 на тот момент не было железа, которое поддерживало бы технологию Blu-ray).

Сегодня ключи VUK свободно циркулируют в Сети, программы копирования получили привычный графический интерфейс, а утилит для последующей обработки видеофайлов более чем предостаточно. Оригиналы фильмов и их обработанные копии можно получить в файло-обменных сетях. Cyberlink уже в середине февраля выпустила апдейт для PowerDVD Ultra, который затрудняет просмотр состояния оперативной памяти. Еше до того как данные попадут в редактор, плеер обновляет их. Конечно, AACS LA могла бы аннулировать на новых дисках ключи OEM-плееров, однако она сделала вполне разумное заявление: сама-то технология зашиты AACS не взломана.

5 февраля 2007 года хакер по имени Amezami рассказал о втором способе обхода защиты AACS — и небрежно написанные плееры уже не нужны. Потребуются привод определенной модели и знание принципов работы AACS.

Для перехвата потока данных, идущего от HD-DVD-Привода производства Microsoft, Amezami воспользовался USB-сниффером, так как USB-канал не шифруется. Цель ясна: определить значения, из которых генерируется VUK.

В первую очередь Amezami отыскал значение Volume Identifier, или Volume ID. Как он сам говорит, ему было трудно в это поверить. Согласно требованиям спецификации AACS, ID-номер должен быть случайно сгенерированным значением, но на деле оказалось, что Volume ID у HD-DVD с фильмом «Кинг-конг» состоит из даты (18.09.2006) и времени (08:41) изготовления диска. Другие пользователи подтвердили, что подобная схема применяется на многих дисках. Значение Volume ID позволяет, таким образом, предсказать или ограничиться сравнительно небольшим перечнем данных. Также был опубликован Private Host Key от PowerDVD, с помощью которого плеер запрашивает Volume ID. Благодаря этому можно получить Volume ID любого DVD.

Сначала у Amezami не было ключа Processing Key, чтобы суметь вычислить значение VUK. Он нашел его с помощью самостоятельно написанной программы, изучив данные, передаваемые модифицированным плеером в оперативную память. Найденный Processing Key действителен для любого диска, имеющегося на рынке, неважно какого — Blu-ray или HD-DVD. Всегда один и тот же ключ — звучит легкомысленно, однако вполне обоснованно: изменение значения ключа Processing Key компания AACS LA хотела использовать для «отсечения» взломанных плееров. Она могла бы выбирать новый Processing Key таким образом, чтобы ключи Device Key взломанных плееров не смогли бы его больше считывать. Однако AACS работает со всеми имеющимися плеерами так как будто они себя ничем не скомпрометировали, то есть используют для всех дисков один и тот же Processing Key.

Компания Verance Corporation, создатель инновационной технологии звуковых «водяных знаков», намерена предоставлять лицензию на использование собственной разработки производителям медиа-проигрывателей, которые поддерживают форматы Blu-ray и HD DVD. Обладатели такой лицензии смогут встраивать в производимое оборудование специальные механизмы, отвечающие за распознавание «водяных знаков» в

просматриваемых видеоматериалах. Метки, разработанные Verance, позволяют идентифицировать незаконно изготовленный видео-контент и запрещать его воспроизведение. К примеру, на видеотехнике нового поколения невозможно будет просмотреть видеофильм, снятый на камеру в зале кинотеатра и оцифрованный в домашних условиях.

Список приверженцев технологии уже включает в себя крупнейшие корпорации, включая Universal Studios, Sony Pictures Entertainment и Microsoft Corporation

Идет ли речь об онлайновой музыке, DVD или HD-дисках, тенденция однозначна: системы защиты от копирования взламываются с момента появления все быстрее.

Microsoft DRM 1 (аудио)

Появилась s 1999 году, взломана в октябре 2001 года

CSS (видео)

Появилась в июне 1996 года, взломана в октябре 1999 года

Apple FairPlay (аудио)

Появилась в апреле 2003 годэ, взломана в ноябре 2003 года

Microsoft PlaysForSure (аудио)

Появилась в октябре 2004 года, взломана в августе 2006 года

Sony ARccOS (видео)

Появилась в марте 2004 года, взломана в сентябре 2004 года

Macrovislon RipGuard (видео)

Появилась в феврале 2005 года взломана в ноябре 2005 года

AACS (видео)

Появилась в апреле 2006 года, взломана в декабре 2006 года

Settee Alpha DVD (видео)

Появилась в январе 2006 года, взломана в феврале 2006 года

HD-DVD-носители используют защиту стандарта AACS, а их конкуренты в этих же целях используют еще и два дополнительных слоя, «BD-ROM Mark» и «BD+».

BD-ROM Mark

Дополнительный физический слой, содержащий некоторую информацию, препятствующую неавторизированному тиражированию содержимого оптического носителя «пиратами». Для переноса данных, находящихся в пределах специального слоя, необходимо особое оборудование, иначе осуществить задуманное не удастся. Отсутствие слоя на матрице делает информацию на ней нечитаемой.

BD+

Каждый проигрыватель BD-дисков обладает виртуальным модулем (Virtual Machine), обеспечивающим базовую обработку кода B+ и позволяющим тиражирующим записи студиям размещать его уникальную версию на оптическом носителе. В процессе воспроизведения происходит постоянное обращение к нему (благодаря дешифратору, степень нагрузки на проигрыватель минимальна), что позволяет мгновенно блокировать сигнал в том случае, если его считывание происходит при помощи «пиратского» устройства.

Вся технология BD+ базируется на трех основных элементах:

• Преобразующий код (может быть интегрирован в контент носителя вне зависимости от типа записи на нем).

Часть данных, находящихся на компакт диске, «поглощается» или «повреждается» кодом, впоследствии она может быть прочитана лишь при помощи виртуального модуля, интегрированного в привод. Использовать его можно и в судебных целях для идентификации источника незаконно копируемой продукции.

• Основные средства противодействия незаконному тиражированию (применяются в случае подтверждения взлома системы защиты).

При возникновении малейшего намека на обход системы безопасности злоумышленником, студия записи может начать расследование. После получения подтверждения произошедшего от производителя учувствовавшего в этом проигрывателя, первая из сторон приступает к

разработке новой модификации кода BD+, которая способна не только распознать единожды использованный способ атаки, но и противостоять ему.
• Расширенные средства противодействия незаконному тиражированию.

Таким образом, для обхода системы безопасности оптического носителя, «пиратам» придется взломать преобразующий код и преодолеть еще один его вариант, использованный записывающей студией в индивидуальном порядке.

Вывод

Представители музыкальной индустрии ставят под вопрос перспективу самой концепции цифрового управления правами (DRM). Например, компания EMI заявила о своем намерении в будущем распространять через Интернет незащищенные музыкальные произведения. Руководитель службы Yahoo! Music Dave Goldberg полагает, что DRM уже до конца нынешнего года перестанет существовать. И даже шеф Apple Стив Джобе вслух размышляет о необходимости прекратить использование средств DRM. Он считает,что нет смысла защищать онлайновые музыкальные файлы, если 90% продаж музыки приходится на аудио CD, зашита от копирования которых уже давно признана неэффективной.

Между тем ситуация ясна: не производимые с мая текушего года диски HD-DVD получат новые ключи. Однако поможет ли это, если и их можно будет перехватить? Дело в том, что тот же Amezami представил для этой цели утилиту под названием aacskeys.exe, которая переписывает все ключи с HD-диска. Можно ли еше спасти технологию AACS? Маловероятно: с февраля в сети имеется Device Key для WinDVD 8.0, а утилита AnyDVD, распространяемая с недосягаемых Карибских островов Антигуа, обновлена до версии, способной справляться как с BD, так и HD-DVD. С ее помощью любой пользователь в состоянии создать копию лицензионного диска.

Список литературы

1)Пронин И.В.,«Конец защите от копирования?»/Журнал «CHIP»-Москва №6.М.: «Бурда»,-2007 г.,с.54-57

2)Калиниченко М.А., «Microsoft предлагает новую технологию защиты от копирования»,http://stra.teg.ru/lenta/security/1754/,24 апреля 2003 г.

3)Ураков Ю.П.,«Protection Technology представила новую технологию защиты»,http://www.relcom.ru,27 апреля 2005 г.

4)Антонов М.О.,«Sony выпускает диски с новой технологией защиты от копирования»,http://www.comdes.ru,21 декабря 2004 г.