Московский физико-технический институт (ГУ МФТИ)

Факультет радиотехники и кибернетики

Эссе по курсу ''Защита Информации''
кафедра радиотехники, http://www.re.mipt.ru/infsec

Уязвимости CSS и AACS
Vulnerability of CSS and AACS

Рыжиков М.А., 311 группа

Долгопрудный, 2007

1. CSS

Из-за потенциальной возможности делать точные цифровые копии, параноидальные киностудии потребовали включения в стандарт DVD требований к более глубокого механизма защиты. "Система кодирования содержимого" - это схема кодирования данных и авторизации, которая была призвана предотвратить копирование видео-файлов непосредственно с диска.

Система шифрования CSS (Content Scrambling System)

Любой плейер (программный или аппаратный) имеет свой собственный уникальный ключ доступа к DVD-диску, именуемый ключом плейера. Всего существует 409 таких ключей.

На каждом DVD-диске, в свою очередь, содержится 5-байтный (40 бит) ключ диска, зашифрованный каждым из 409 ключей плейера. Другими словами, имеется 409 ячеек, в каждой из которых лежит ключ диска, который соответствующий программный или аппаратный плейер может расшифровать. Каждому владельцу лицензии (производителю плейера) известен номер ячейки, соответствующий его ключу плейера.

Собственно механизм системы CSS состоит из двух частей - аутентификации и шифрования. Всего же на DVD-диске находится три различных ключа: **ключ аутентификации**, **ключ диска**, а также **ключ названия**, расположенный в заголовке сектора данных. Каждый ключ должен обрабатываться и проверяться - начиная с самого первого (ключа аутентификации) - перед тем, как переходить к следующему.

Ключ аутентификации, по сути своей, - это хеш-функция от ключа диска. Каждый DVD-декодер, будь он аппаратный или программный, с помощью своего уникального 40-битного ключа плейера расшифровывает ключ диска, лежащий в соответствующей ему ячейке. Для того чтобы убедиться в правильности расшифровки, вычисляется хеш-функция полученного результата и сравнивается с ключом аутентификации. Если они равны, ключ диска комбинируется с ключом названия, чтобы "отпереть" кинофильм для воспроизведения. Хотя вся эта конструкция может на первый взгляд показаться весьма изощренной, в действительности механизм защиты CSS оказался значительно слабее, чем предполагали его разработчики.

В мае 1997 года началось первое распространение лицензии CSS для программного декодирования. Эта лицензия очень сильно ограничена для предотвращения утечки информации о ключах и алгоритме шифрования CSS. Конечно, ничего что используется в миллионах плееров и приводах по всему миру не может оставаться в секрете достаточно долго. И в октябре 1999 года алгоритм CSS был взломан и опубликован в Internet, вызвав много шума и судебных разбирательств. Вспомним события того времени.

История взлома CSS

Это известие прошло в начале ноября 1999 практически через все агентства новостей. Вскрыли CSS - систему, используемую для шифрования кинофильмов на дисках формата (DVD) и призванную защитить фильм от несанкционированного копирования. По Сети начала свободно распространяться программная утилита под названием DeCSS, которая считывала зашифрованный кинофильм с DVD-диска, расшифровывла содержимое и клала получившийся файл на жесткий диск компьютера пользователя. DVD-движение привлекло внимание группы программистов, именующей себя MoRE, то есть "Мастера обратной разработки" (Masters of Reverse Engineering). Норвежцы занимались анализом и восстановлением кода всевозможных DVD-плейеров в надежде добраться до "ключа плейера". Все владельцы лицензии на технологию DVD обязаны хранить свой ключ плейера в зашифрованном виде, так, чтобы при обратной разработке

(reverse engineering) программы нельзя было добраться до ключа в явном виде. Увы, одна из фирм-владельцев лицензии по недосмотру не зашифровала свой ключ.

Как сообщили члены группы MoRE, они добыли первый такой ключ, когда восстановили код программы XingDVD компании Xing Technologies. Наличие одного расшифрованного ключа и общие слабости криптосхемы позволили Йону Леху Йохансену (Jon Lech Johansen) и его партнерам по группе MoRE восстановить еще более 170 ключей плейера, принадлежащих другим фирмам, а также создать программу DeCSS. Историю написания программы от авторов можно найти по адресу http://web.lemuria.org/DeCSS/dvdtruth.txt.

. Как показали дальнейшие исследования системы CSS, крайне слабый алгоритм шифрования позволяет очень быстро (с затратами порядка 2^{25} вариантов ключа – несколько десятков секунд) аналитически отыскивать ключ диска, вообще не зная никакого ключа плейера. Анализ криптографической системы на стойкость провёл парень по имени Франк Эндрю Стивенсон (*Frank A. Stevenson*)

Поскольку вся защита CSS создавалась так, чтобы удовлетворять экспортным ограничениям США и Японии на криптографию, она изначально была крайне слабой (уязвимой к брут-форсу). По сути дела, вся ее "стойкость" сводилась к секретности алгоритмов шифрования, а это принцип защиты, бесперспективный по самой своей сути. Публикация CSS продемонстрировала то, что специалисты именуют "фатально порочным" подходом к криптографии. По общему мнению, самые серьезные слабости CSS – это

1) закрытый "фирменный" алгоритм, не исследованный независимыми экспертами;
2) использование ключа плейера длиной всего 40 бит;
3) то, что он вообще был реализован программно.

2. AACS

Летом 2006г двум конкурирующим лагерям — консорциуму DVD Forum (ведающему HD DVD) и альянсу BDA (Blu-ray) — удалось-таки, наконец, договориться с Голливудом и между собой. Единая спецификация защиты, носящяя название «Продвинутая система доступа к контенту» или кратко AACS (Advanced Access Content System) была доведена до финальной версии 1.0. AACS первоначально была предложена как замена CSS (content scrambling system), системы защиты DVD.

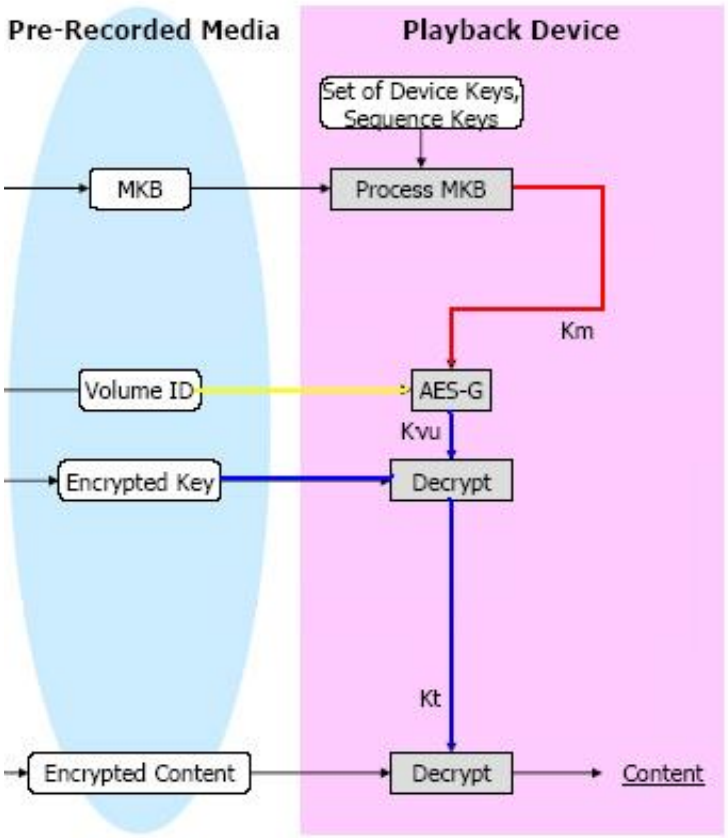
Финальная версия AACS

В отличие от CSS, в основу стандарта AACS заложен очень сильный криптоалгоритм AES для шифрования файлов на диске, что полностью исключает возможности доступа к контенту без знания ключа (как, скажем, это делают сейчас с DVD популярные в народе программы-декрипторы). Если же какой-то из ключей пиратам все же удастся тем или иным образом раздобыть, то кардинально усиленная система управления ключевыми параметрами позволяет без проблем аннулировать любой скомпрометированный ключ, так что он не будет подходить для расшифровки дисков, выпускаемых впоследствии.

В предельно упрощенном виде AACS аналогична печально известной системе CSS, Как и там, в AACS каждое устройство воспроизведения получает свой секретный **ключ устройства** (**device key**). Каждое устройство использует эти строго индивидуальные ключи для вычисления гораздо более многочисленной группы **ключей обработки (processing key)**. В свою очередь для каждого фильма, защищённый AACS, генерируется свой уникальный **"ключ названия" (title key)**, и множество копий title key, зашифрованных разными ключами обработки, хранится в специальном разделе на оптическом диске (в поле заголовка). Чтобы воспроизвести такой диск, плеер определяет, какую из копий title key он может расшифровать, и использует свой ключ устройства для вычисления необходимого ключа обработки, а тот, в свою очередь, позволяет расшифровать ключ названия и получить доступ к контенту для воспроизведения.

Эти три типа ключей имеют разную ценность с точки зрения безопасности и противостояния вскрытию. Разумеется, атакующему наиболее интересны и полезны ключи устройства. Если вы их знаете, то можете расшифровать любой диск, воспроизводимый плеером. Поэтому для защиты device keys предприняты максимальные меры безопасности и разработан хитрый механизм определения и блокирования скомпрометированных ключей такого рода. Ключи названий наименее полезны, поскольку каждый из них годится для расшифровки лишь единственного фильма. Ключи обработки занимают по ценности промежуточное положение, однако они нигде не хранятся - ни в плеере, ни на диске, - а вычисляются на одном из этапов подготовки фильма к воспроизведению. Поэтому их добыча атакующей стороной представлялась наиболее проблематичной, по крайней мере теоретически. На практике, однако, все оказалось иначе.

Технические детали (от arnezami)



MKB = Media Key Block
Process MKB = Subset-Difference Tree system
Km = Media Key
Kvu = Volume Unique Key
Encrypted Key = Encrypted Title Key
Kt = Title Key

Этот рисунок показывает все ключи, необходимые для расшифрования содержимого. И каждый играет свою роль.

Subset-Difference Tree system: по существу, это огромная и секретная коллекция никогда неизменяющихся **Processing** и **Device Keys,** полученный из одного **Master Device Key**. Device Keys могут быть использованы для получения желаемого **Processing Key**, и так как в плейере есть всего несколько **Device Keys**, он может использовать только небольшую часть всех **Processing Keys**. Вследствие этого, некоторые плейеры неспособны получить правильный **Processing Key**, который необходим для получения **Media Key**. Т.е., если устройство себя скомпрометировало, то можно сделать так (с помощью изменения MKB), что диски, выпущенные позднее уже не будут воспроизводиться данным устройством (что и будет сделано в ближайшее время).

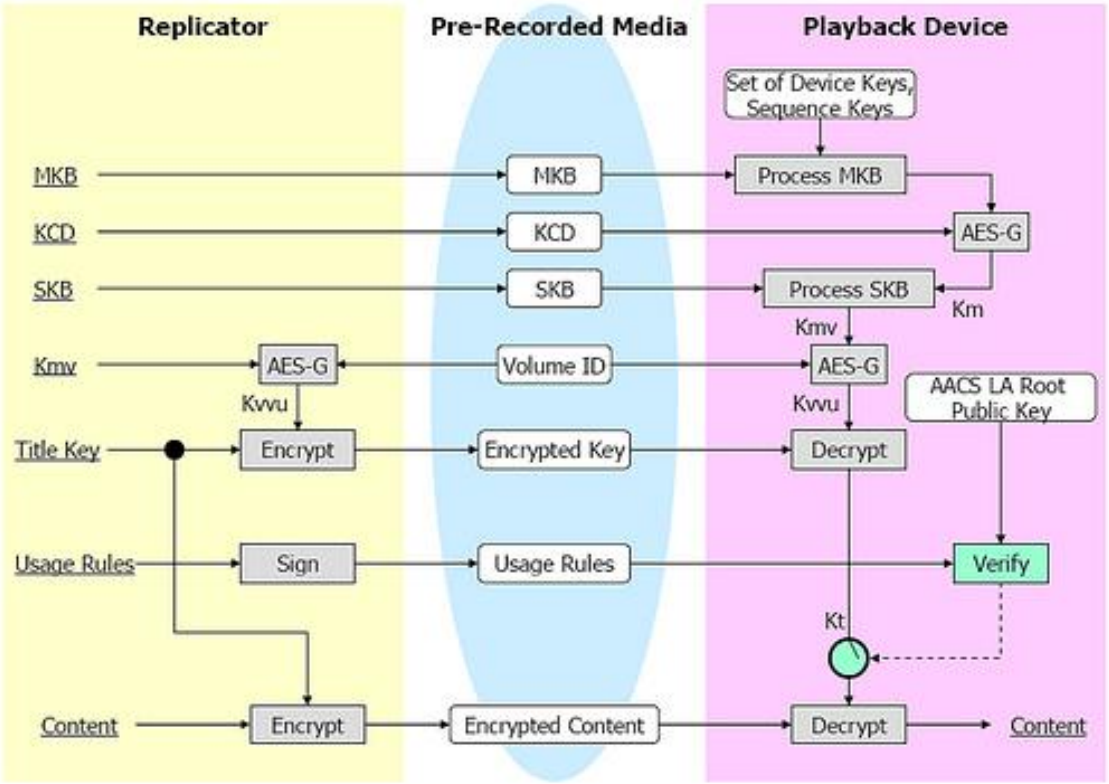
Volume ID: он используется для предотвращения побитового копирования, так как может быть получен только специальным запросом с диска (он не хранится в файле). При копировании зашифрованного диска этот кусок информации не будет скопирован, делая тем самым невозможность декодирования/проигрывания содержимого: копия не будет работать. **Volume ID** комбинируется с **Media Key** для получения Volume Unique Key, который в свою очередь декодирует Title Keys.

Media Key: он получается из **Processing** and a **C-value** (которое берётся из файла с MKB) в результате работы **Subset-Difference Tree system.** Для каждого фильма он уникален. Поэтому, если вы найдёте один такой ключ, то сможете декодировать только один фильм (при условии, что вы сможете получить Volume ID)

Multiple Title Keys: даже если вы смогли получить один Title key, вы сможете декодировать только часть содержимого диска, делая тем самым полного декодирования сложнее, так как вы должны получить все такие ключи. Разница между ними состоит в количестве раз, которыми они зашифрованы.

Это основы AACS.

Общая схема декодирования фильма



История вскрытия AACS

27 декабря, 2006

В сети появилась программа под названием BackupHDDVD, которая для обхода ограничений использует метод подставления специального ключа, наподобие того, как это делают обычные бытовые проигрыватели таких дисков. В архив включено уже скомпилированное приложение на языке Java (необходим интерпретатор версии 1.5), исходные коды, а также инструкция для «употребления».

Подробнее можно прочесть на форуме сайта Doom9, в топике под названием ‘’BackupHDDVD, a tool to decrypt AACS protected movies’’ by muslix64 по адресу http://forum.doom9.org/showthread.php?t=119871.

В том же топике сам автор делится подробностями своей работы.

При взломе схемы CSS хакерам удалось найти и выделить незашифрованный "ключ устройства" внутри кода программного плеера Xing. В случае с AACS этот опыт был разработчиками явно учтен, так что поиски ключа в коде программ воспроизведения успехом не увенчались. Тогда Muslix64 не стал взламывать плейер, а решил поискать иной ключ - Title Key совсем в ином месте - в оперативной памяти компьютера. Сначала Muslix64 выделил для анализа соответствующий дамп памяти плейера, где находилось начало зашифрованого фильма и, вероятно, собственно ключ. А затем, зная общую структуру хранения блоков на диске и принятые в спецификациях стандарты их оформления, он предположил, как должны выглядеть первые байты расшифрованных

блоков (plain text). Теперь задача приобрела почти классический вид отыскания ключа по известному фрагменту открытого текста. Проверка подтвердила, что это действительно Title Key.

Все эти подробности стали известны гораздо позже. Поначалу же Muslix64 опубликовал в Сети лишь свою программу BackupHDDVD, которая реализует общедоступные спецификации алгоритма AACS и по известному Title Key расшифровывает файлы с HD-DVD для архивации на жестком диске. Однако ни одного из найденных Title Key сам Muslix64 не опубликовал, отметив лишь, что владельцы HD-дисков могут найти их сами в оперативной памяти компьютера.

20 января, 2007г

Что касается Blu-ray, то привода под диск этого стандарта у Muslix64 не было. Зато он был у другого человека с ником Janvitos, который применил аналогичную технику анализа структуры файлов и выделения дампа памяти. Затем к делу снова подключился Muslix64 - и в итоге в Сети появились Title Keys к фильмам на Blu-ray

(http://forum.doom9.org/showthread.php?t=120869)

11 февраля, 2007

Новая глава в преодолении защиты AACS. Как показал анализ участников doom9.org, внешне грозная защита имеет не просто слабости, а вопиющие прорехи. Участник форума, скрывающийся под псевдонимом Arnezami, обнаружил, что в сложной и многоуровневой системе защиты дисков HD DVD имеется один ключ, processing key, который позволяет получать индивидуальные ключи названий (title keys), а значит, и доступ к зашифрованному содержимому, для всех выпущенных на тот день дисков. Более того, вскоре выяснилось, что этот же самый ключ обработки подходит и для расшифровки всех фильмов на дисках Blu-ray.

Ни одного ключа устройства на сегодняшний день публично не скомпрометировано. До появления работы Arnezami все успешные случаи обхода защиты AACS так или иначе были связаны с отысканием ключа названия в оперативной памяти компьютера при воспроизведении фильма программным плеером (WinDVD). Понятно, что подобные атаки весьма замысловаты с технической точки зрения. А для человека, далекого от анализа дампов памяти, единственная возможность сделать резервную копию HD-диска сводилась к поиску в Сети уже вскрытого и опубликованного кем-то title key для данного фильма.

Но затем появился Arnezami, который придумал иной ход - анализировать не память, а канал обмена информацией между hd-dvd usb дисководом xbox360 и компьютером. Он применил общедоступную программу-сниффер для анализа передач по USB-каналу (SniffUSB.exe) и действительно сумел выделить сгенерированный плеером processing key для имевшегося у него фильма (King Kong). Тут же посетители форума выяснили, что этот же ключ обработки подходит и для всех остальных фильмов, выпущенных на дисках HD DVD. А также и для всех проверенных фильмов на дисках Blu-ray. (http://forum.doom9.org/showthread.php?t=121866&page=6)

Согласно спецификациям AACS, каждый плеер имеет свой уникальный набор из нескольких сотен device keys, на основе которых может быть вычислено несколько миллиардов ключей обработки. В принципе, processing keys вполне могут совпадать для разных плееров, но при столь внушительном их числе каждый конкретный ключ обработки по законам теории вероятностей должен совпадать лишь у небольшой доли плееров по всему миру. А каждый конкретный фильм, в свою очередь, имеет на диске список идентификаторов тех ключей обработки, которые могут расшифровать содержимое диска, - то есть любого из перечисленных processing key достаточно для расшифровки title key и доступа к контенту.

По непонятным причинам все выпущенные на рынок диски имели один и тот же набор идентификаторов для 512 ключей обработки. Это и означает, что установленный Arnezami ключ подходит для расшифровки всех дисков.

3.Литература

DVD copy control association
http://www.dvdcca.org/

DeCSS Central Main Page
http://web.lemuria.org/DeCSS

Cryptanalysis of Contents Scrambling System(о уязвимости защиты)
http://web.lemuria.org/DeCSS/crypto.gq.nu/

Frank Stevenson's CSS Cracks
http://www.cs.cmu.edu/~dst/DeCSS/FrankStevenson/index.html

Advanced Access Content System Licensing Administrator
http://www.aacsla.com/home

Продолжение истории со взломом HD дисков
http://ilya-314.livejournal.com/38283.html

THE in-place to be for everyone interested in DVD conversion
http://forum.doom9.org

BackupHDDVD, a tool to decrypt AACS protected movies
http://forum.doom9.org/showthread.php?t=119871

Processing Key, Media Key and Volume ID found!!!
http://forum.doom9.org/showthread.php?t=121866&page=6

Clarification on the state of AACS
http://forum.doom9.org/showthread.php?t=124505

Understanding AACS (including Subset-Difference)
http://forum.doom9.org/showthread.php?t=122363

Blu-ray and AACS
http://forum.doom9.org/showthread.php?t=120869

http://www.securitylab.ru/

http://www.computerra.ru/

Единый ключ, что правит всем
http://offline.computerra.ru/2007/676/309087/