Эссе по курсу «Защита Информации»

студента 913 группы

Липина Дмитрия

по теме:

Методы защиты DVD дисков.

В уже далеком 1995 году было официально объявлено о создании формата DVD. Этот формат не является детищем какой-то одной компании – в его разработке принимали участие 10 гигантов мировой индустрии - Toshiba, Hitachi, Matsushita, JVC, Mitsubishi, Philips, Thomson, Pioneer, Time Warner и Sony. Позднее, в 1997 году, на замену консорциуму их этих 10 компаний, пришел DVD Forum, который является открытым для всех, и в настоящее время в нем начитывается более 200 членов. Изначально аббревиатура DVD означала Digital Video Disk, однако позднее, в связи с расширением функций DVD, стала чаще всего расшифровываться как Digital Versatile Disk, однако официальной расшифровки того, что скрывается за буквами DVD, не существует. Благодаря одному из своих главных достоинств – возможности хранить большие объемы данных на одном носителе – DVD используется для записи и воспроизведения высококачественного видео и аудио.

Региональная защита.

Главная задача компаний аудиовидео индустрии - получение максимальной прибыли от производства собственной продукции, что достигается чаще всего двумя путями – прокатом продукции и ей продажей. Для получения максимальной выгоды от проката, компании, производители DVD дисков, могут устанавливать на них региональные коды защиты (region lock). Чтобы потребитель мог просмотреть такой диск на своем устройстве воспроизведения DVD, тот должен иметь тот же региональный код защиты, что и сам DVD-диск. В настоящее время существует 8 зон:

1. Канада, США
2. Япония, Европа, Южная Африка и страны ближнего востока (включая Египет)
3. Юго-Восточная и Восточная Азия (включая Гонк-Конг)
4. Австралия, Новая Зеландия, Центральная и Южная Америка, Мексика, Тихоокеанские и Карибские острова.
5. Восточная Европа (бывший СССР), Индийский полуостров, Африка, Северная Корея и Монголия
6. Китай
7. Зарезервировано
8. Международная зона (самолеты, пароходы и т.д.).

Компании-производители DVD устройств понимают, что введение регионального кода в их устройства сильно мешает развитию этого стандарта и является преградой для получения максимальной прибыли. Поэтому в последнее время все чаще DVD аппаратура выпускается мультизонной. У аппаратуры, являющейся однозонной, можно сменить прошивку, для того, чтобы она не проверяла этот код. (однако стандартных методов для этого не существует). В корневой директории каждого диска содержится файл video.ifo, в котором содержится ключевая информация о диске, среди которой и региональный код. Этот файл считывается при раскрутке диска. В спецификациях DVD указано, что в этом файле может содержаться кусок программы, который позволяет автоматически перейти к определенной части диска, в зависимости от некоторых параметров. Идея этого состоит в том, чтобы можно было

автоматически выбирать некоторые параметры просмотра (язык, субтитры , формат видео). Однако попытка проиграть DVD диск в мультизонном проигрывателе не всегда завершиться успехом. В последнее время все чаще и чаще появляются диски, которые содержат так называемую «защиту от нулевого кода региона» (считается, хотя технически это никак не отображено, что код региона 0 означает мультизонность), и таким образом не могут быть проиграны на плеерах с «нулевым кодом». Все диски, выпущенные компанией Digital Video Compression Center (производит диски для таких крупных корпораций как Fox, Universal, MGM/UA), содержат такую защиту. Название этой защиты – «region code enhancement» (RCE, также известна как RAE). Такие диски не могут быть проиграны на плеерах, которые являются мультизонными, однако они могут быть проиграны на плеерах, на которых возможно вручную включить нужную зону. Также могут быть проблемы с проигрыванием таких дисков на плеерах, автоматически переключающих свою зону. Однако это зависит от зоны, установленной по умолчанию в таком плеере. На диске, защищенном RCE, флаги всех регионов установлены таким образом, что плеер не может определить, на какую из зон переключиться. Если при проверке соответствия зоны плеера и диска была обнаружено расхождение – диск играться не будет. Если зона плеера по умолчанию равна 1 и зона RCE диска тоже 1, то после проигрыша в течение нескольких секунд такого диска большинство самопереключающихся плееров установят свою зону равной 1 и таким образом можно будет проиграть RCE диск. Обратная сторона медали – некоторые однозонные плеера с кодом региона, соответствующим коду диски, не проходят проверку и, таким образом, диск невозможно проиграть на них. Стоит отметить, что региональные коды не применяются для DVD-Audio дисков и, как правило, не применяются для записываемых дисков.

Защита от нелегального копирования.

Набор средств для защиты и ограничения доступа к информации на DVD, который имеет общее название CPSA (content protection system architecture), был разработан сообществом “4”, в которое входят компании IBM, Intel, Matsushita. Существует множество видов защиты информации на DVD:

1. Analog CPS (Analog Copy Protection System).
   Разработана компанией Macrovision. Предназначена для защиты от копирования сигнала с аналогового (видео) выхода DVD устройства (например, на обычную VHS кассету). При выводе изображения в сигнал подмешиваются слабые быстро модулирующиеся цветовые полосы и импульсы вертикальной синхронизации, что сбивает систему автоматической подстройки уровня сигнала у 95% моделей видеомагнитофонов. Естественно, эти помехи будут воспроизведены, если проигрывать DVD-видео диски на аппаратуре, которая не поддерживает Macrovision, но в настоящее время такая уже давно не производится. Аппаратура, которая поддерживает Macrovision, способна фильтровать помехи, и показывать нормальную картинку. Сигнал защиты состоит из двух элементов: автоматического регулирования усиления (AGC) и цветовых полос (colorstripe). AGC в телевизоре медленно реагирует на изменения, в то время как в видеомагнитофоне AGC реагирует достаточно быстро. Технология Macrovision пытается использовать эту особенность, особым образом изменяя сигнал (помещая всплески в интервалы гашения обратного хода развертки). Таким образом, телевизор все еще будет правильно показывать картинку, а видеомагнитофон уже не сможет корректно ее записать, копии будут слишком тусклыми и/или будут содержать различные помехи. Цветовые полосы изменяют сигнал цветовой синхронизации, причем изменение не заметно на оригинале, а на копии оно приведет к появлению раздражающих линий на картинке.
   Эта защита часто может быть отключена сменой прошивки плеера или использованием RGB выхода.

2. CGSM (copy generation management system)
   В отличии от Macrovision, которая должна полностью устранить создание новых копий,

данная защита применяется для ограничения их количества. Есть два разновидности этой защиты.
А) CGMS-A - аналоговая защита, рассчитанная на компьютерные платы видеозахвата и цифровые видеокамеры. В 20-й или 21-й строке стандарта NTSC передаётся код защиты от записи.
Б) CGMS-D. Эта система основана на стандарте IEEE 1394 и предназначена для ограничения ("copy once) и запрещение ("copy never) создания цифровых копий. Цифровые приборы, такие, например как DVD плеер и цифровой TV, будут обмениваться ключами и идентификационными подтверждениями перед установлением канала. DVD плеер шифрует видео сигнал при отправке, а получающий прибор расшифровывает его. Пишущие цифровые приборы не смогут получать сигнал при внутренней маркировке "copy never", а при маркировке "copy once"- сделают копию и изменят маркер на "copy never". CGMS/D спроектирован для следующего поколения цифровых ТВ и видео рекордеров. Для этой системы нужны DVD проигрыватели нового поколения с цифровыми соединениями.

3. CSS (content scrambling system)
Используется для предотвращения копирования содержимого DVD диска на жесткий диск компьютера. Включает в себя шифрование данных и идентификацию. Каждому обладателю лицензии CSS выдается один из ~400 главных ключей, которые хранятся на каждом диске, защищенном CSS. Это позволяет отменить лицензию, удалив свой ключ из дальнейших дисков. Для предотвращения копирования из "цифры" в "цифру" на компьютере используется идентификация по шине и кодирование. Как известно, DVD ROM проигрыватель и карта-декодер соединены друг с другом шиной компьютера. Так как данные на шине компьютера можно легко перехватить, DVD-ROM должен проверить подлинность получателя перед отправкой данных. Верно и обратное: для предотвращения потенциального проигрывания пиратских материалов карта-декодер должна проверить подлинность отправителя данных. Соответственно требуется взаимная аутентификация. А для предотвращения перехвата и замещения данных после аутентификации, привод использует шифрование данных с помощью зависящего от времени ключа. Слабость этой системы состоит в том, что блок дешифрования должен быть встроен в каждый софтверный декодер, которые может проигрывать такие диски, и любой может легально скачать такую программу, и препарировать её. В итоге произошло то, что должно было произойти. 16 летний норвежский программист Jon Johansen сумел разобраться в работе дешифровального блока, и выпустил программку называемую DeCSS, которая расшифровывает данные и позволяет записывать содержимое защищённых DVD-видео дисков в чистом виде на винт. Основные сведения о взломе CSS представлены после краткого обзора всех методов зашиты.

4. CPPM (Content Protection for Prerecorded Media)
Используется исключительно для защиты DVD-Audio. Был разработан для совершенствования CSS. Каждая запись на DVD-Audio также имеет так называемые "цифровые водяные знаки", которые расположены в неслышимой области спектра и распознаются DVD-Audio оборудованием при проигрывании через цифровые и аналоговые интерфейсы, и препятствуют копированию. Бытовое DVD-Audio оборудование также обычно не воспроизводит звук через цифровой выход или делает это с намеренным даунсемплингом в пониженное разрешение. Ключи хранятся в начальной области диска, но, в отличие от CSS, в заголовках секторов нет заглавных ключей. Каждый носитель содержит 56-битный идентификатор альбома (поле дескриптора тома файловой структуры, определяющее набор дисков, к которому принадлежит том), который схож с CSS ключом и который содержится в контрольной области. Каждый диск содержит область цифрового ключа, которая содержится в файле на диске. Данные этой области логически упорядочены в строки и столбцы, которые

используются при идентификации для создания из определенного набора ключей DVD – устройства одного ключа для расшифрования. Если ключ устройства аннулирован, обработка данных из области цифрового ключа закончиться тем, что будет выдан неверный ключ. Как и в случае с CSS, область цифрового ключа может быть обновлена для того, чтобы помешать использованию несанкционированных ключей устройства. Механизм идентификации используется такой же, как и в CSS, поэтому вносить изменения в уже существующие устройства не требуется.
В данное время способов обойти защиту CPPM не существует.

5. CPRM (content protection for Recorded Media)
   Используется для записываемых DVD дисков (DVD-RAM, DVD-RW, DVD-R). Каждый чистый записываемый DVD диск содержит уникальный 64-битный идентификационный номер, нанесенный в BCA (burst cutting area) – зоны около вокруг центра диска. Этот самый номер выжигается YAG лазером и содержится в штрих-коде. Когда защищенное содержимое записывается на диск, оно может быть зашифровано 56-битным шифром C2 (Cryptomeria). При воспроизведении идентификационный номер (ID) читается из BCA и используется для генерации ключа для расшифрования содержимого диска. Если содержимое диска копируется на другой носитель, ID будет отсутствовать или же оказаться неправильным, и все данные не смогут быть расшифрованы.

6. DCPS (Digital Copy Protection System)
   С целью обеспечить цифровое соединение между компонентами и исключить точное цифровое копирование, ассоциации CEA (Consumer Electronic Association) было предложено 5 систем защиты от цифрового копирования. Лидером является протокол DTCP (digital transmission content protocol), который базируется на стандарте IEEE1394/FireWire, но также может быть распространен и на другие. Проект был представлен пятью компаниями – Sony, Intel, Toshiba, Hitachi и Matsushita в феврале 1998, а уже в середине 1999 корпорация Sony представила чип, поддерживающий DTCP. При использовании этого протокола цифровые устройства обмениваются ключами и сертификатами для установления защищенного соединения. Далее при передаче информации между этими устройствами происходит шифрование данных, что мешает другим подключенным, но неавторизированным устройствам получать несанкционированный доступ.

7. HDCP (High-Bandwidth Digital Content Protection)
   HDCP схож с DTCP, но создан был для работы с интерфейсами цифровых мониторов, например, DVI. В 1998 году была создана ассоциация DDWG (Digital Display Working Group) для разработки стандарта, который должен был заменить стандартный VGA. В апреле 1999 были выпущены спецификации DVI (Digital Video Interface), которые были основаны на технологии PanelLink компании Silicon Image, которая отличалась пропускной способностью около 5Gbps при разрешении 1600x1200. Intel предложила технологию HDCP для защиты интерфейса DVI. В настоящее время используется новый стандарт соединения HDMI, который объединяет в себе DVI и HDCP. HDCP включает в себя идентификацию, шифрование и аннулирование. Рассмотрим схему шифрования данных в устройстве воспроизведения и мониторе перед их передачей по линии связи. Когда выход HDMI замечает, что подключенный монитор не поддерживает HDCP, он снижает качество картинки защищенного содержимого. Процесс обмена ключей устанавливает, может ли принимающее устройство отображать или записывать видео. Для этого используется массив сорока 56-битных ключей устройства и вектор выбора 40-битного ключа. Если надежность дисплея не подтверждена, его вектор выбора ключа помещается в лист для аннулирования. Главное устройство обязано придерживаться листа аннулирования, который обновляется при помощи системных сообщений, которые вносят новые устройства и видео содержимое. После установления разрешений принимающего устройства, видео содержимое шифруется с помощью исключающего

ИЛИ с потоковым шифром, созданным из ключей, полученных в процессе идентификации. Если дисплей пытается показать зашифрованное содержимое без попыток расшифровки, то на экране появляется лишь шум.

Взлом CSS.

В прошивке каждого DVD проигрывателя зашит маленький набор ключей. При попытке проиграть новый диск, плеер попробует расшифровать содержимое с помощью набора ключей, которым он обладает. Каждый диск содержит область данных о ключах диска, которая можно описать следующим образом:

– 5-байтовый хеш расшифрованного дискового ключа (hash)
– дисковый ключ, зашифрованный с помощью ключа 1 плеера (dk_1)
– дисковый ключ, зашифрованный с помощью ключа 2 плеера (dk_2)
….
– дисковый ключ, зашифрованный с помощью ключа 409 плеера (dk_{409})

В предположении, что плеер обладает действительным ключом для 213 слота, он вычислит $K_d=D_A(dk_{213},K_{p213})$

Для проверки правильности ключа K_d, происходит следующая проверка:
$K_d=D_A(hash, K_d)$

Если равенство не достигается, то берется следующий ключ плеера.
Очевидная слабость такой системы вытекает из того, что путем перебора 2^{40} различных K_d ключ диска может быть получен без знания настоящих ключей DVD-плеера. Как будет показано, количество проверок можно свести к 2^{25}, что вполне реально осуществить. Другую очевидную атаку на защиту можно провести, зная всего один действующий ключ плеера – другие ключи плеера могут быть получены с помощью схожий поисков. Эта атака может быть проведена автономно, и ключи, полученные из предыдущих атак, могут быть использованы в качестве начальной точки отсчета.
Чтобы расшифровать содержимое, дополнительный (заголовочный) ключ tk расшифровывается уже найденным действующим дисковым ключем $K_t=D_B(tk,K_d)$.

Каждый сектор информационных файлов по выбору шифруется ключом, который получается из K_t исключающим ИЛИ выбранных байтов из нешифрованных первых 128 байт из 2048 байтного сектора. Расшифрование производится с помощью элементарного потокового CSS кодирования, которое описано ниже.

Потоковый шифр CSS базируется на 2х регистрах линейного сдвига, связанных вместе. Каждый регистр проходит 8 тактов на каждый выходной байт, и существует 4 способа комбинировать выходы двух регистров для получения выходного байта. Эти 4 состояния являются установками на 2х инверторах, и работа, приписываемая этим состояниям, выполняется следующая:

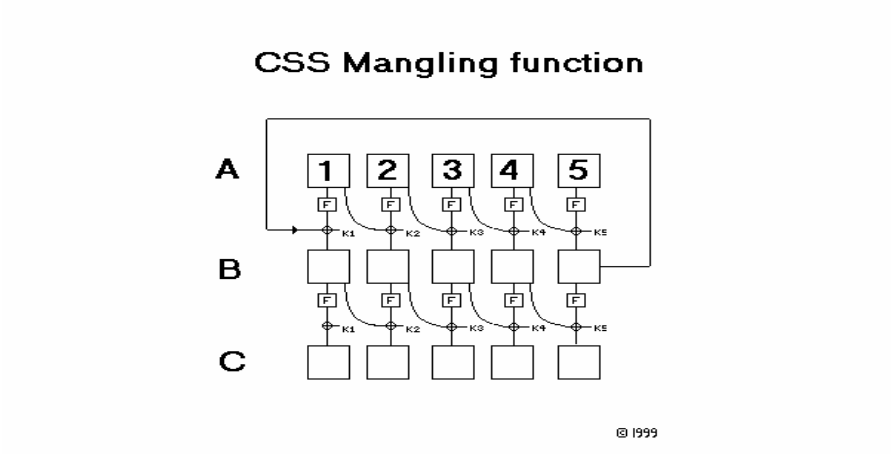
1. Аутентификация DVD привода
2. Расшифровка дискового ключа D_A
3. Расшифровка заголовочного ключа D_B
4. Расшифровка блоков данных

1й регистр: 17 бит инициализируется первыми 2мя байтами ключа, и установка главного значащего бита в 1 для предотвращения холостого цикла.
2й регистр: 25 бит в 4х ответвлениях, инициализируется байтами 3,4,5 сдвига ключа всеми кроме 3х наименее значащих бит вверх на 1 позицию, и установка 4го бита для предотвращения

холостого хода. При работе регистров новые биты устанавливаются в них, и те же самые биты устанавливаются в выводы регистров инвертировано. (С опциональной инверсией битов):
Выход первого регистра: O1(1), O1(2), O1(3) ...
Аналогично, на втором регистре: O2(1), O2(2), O2(3) ...
Эти два потока объединяются путем добавления 8 бит с переносом на следующих выход. Бит переноса устанавливается в 0 при старте потока:
O(i) = O1(i) + O2(i) + c где c – бит переноса их O(i-1)
Потоковый шифр очень непрочный, возможен тривиальный перебор 2^{16} с выходными данными известными для i = {1,2,3,4,5,6}. Представим начальное состояние первого регистра, и отсчитаем 3 байта. O2(1), O2(2), O2(3) могут быть однозначно установлены, и благодаря этому состояние с i=3 полностью известно. Можно также рассмотреть другие три байта шифра и сравнить результаты.

Когда потоковый шифр CSS используется для шифрования ключей D_A(data, key) и D_B(data, key), используется дополнительное действие над данными. Рассмотрим следующую схему.

A(1,2,3,4,5) – входные байты (данные)
C(1,2,3,4,5) – выходные байты (данные)
Ki= O(i) – вывод шифра
B(1,2,3,4,5) – временные стадии
Шифр вычисляется сверху вниз (исключения обозначены стрелками)



Пример вычисления шифра:

B(j) = xor(F(A(j)) , A(j-1) , kj) при j = {2,3,4,5}
B(1) = xor (F(A(1)) , B(5), k1)
C(j) = xor(F(B(j)) , B(j-1) , kj) при j = {2,3,4,5}
C(1) = xor (F(B(1)) , k1)
F – это функция, определенная таблицей перестановок байтов. Если известен шифр и открытый текст, полный шифр находится с минимальными затратами:

- Рассмотрим какое-нибудь k5
- B(5) = xor(F(A(5)) , A(4) , k5)
- B(4) = xor(F(B(5)) , C(5), k5)
- k4 = xor(F(A(4)) , A(3) , B(4))
- B(3) = xor(F(B(4)) , C(4), k4)
- k3 = xor(F(A(3)) , A(2) , B(3))
- B(2) = xor(F(B(3)) , C(3), k3)
- k2 = xor(F(A(2)) , A(1) , B(2))
- B(1) = xor(F(B(2)) , C(2), k2)

- k1 = xor(F(A(1)) , B(5) , B(1))
- проверка условия C(1) = xor (F(B(1) , k1)

Таким образом, рассмотрев 256 комбинаций, мы сможем восстановить 5 выходных байт из потового CSS шифра, и тем самым восстановиться ключ. Эта атака может быть непосредственно использована для восстановления других ключей плеера. Даже если ключ плеера не восстановлен при реверсировании потокового шифра, выход шифра известен, что также окажется полезным для расшифровки дисков, которые работают с другими ключами плеера.

Также возможна атака на хеш ключа диска. Её смысл в том, что, зная хеш, нам надо отыскать такой дисковый ключ, что расшифрованный хеш равен самому этому ключу. Эта атака требует около 2^{25} действий и на современных машинах занимает порядка несколько секунд (10-20 в зависимости от мощности процессора).

Используемые источники:

1. Digital Transmission Content Protection
   http://www.dtcp.com/data/dtcp_public.pdf
2. Content Protection System Architecture: A Comprehensive Framework for Content Protection.
   http://www.4centity.com/data/tech/cpsa/cpsa081.pdf
3. HDCP Specification revision 1.0
   http://www.digital-cp.com/data/HDCP10.pdf
4. Region Coding in DVD
   http://regionhacks.datatestlab.com/region_coding_in_dvd.htm
5. Robert Lundemo. DVD Info.
   http://www.unik.no/~robert/hifi/dvd/
6. Jim Taylor. DVD FAQ
   http://www.dvddemystified.com/dvdfaq.html
7. Дмитрий Чеканов. Методы защиты DVD дисков
   http://www.3dnews.ru/reviews/storage/dvd-protection/
8. Lehmen. PC-DVD FAQ
   http://www.3dnews.ru/reviews/storage/dvd
9. Алексей Шашков. DVD-Rip
   http://www.3dnews.ru/reviews/multimedia/dvd-rip/
10. Максим Лядов. Часто задаваемые вопросы по DVD
    http://www.ixbt.com/dvd/ixbt-dvd2003-faq.shtml
11. Денис Яковлев. Действия, запрещённые для пользователя DVD-диска
    http://www.ixbt.com/dvd/prohibited-operations.shtml
12. DVD Multi Specifications
    http://www.dvdfllc.co.jp/multi101.pdf
13. DVD Copy Protection
    http://www.asus.com.tw/support/english/techref/dvdcopy/index.aspx
14. Дмитрий Петрусенко. Защита копирования DVD
    http://www.hardvision.ru/?dir=storage&doc=dvd_copy_protection
15. Frank A. Stevenson. Cryptanalysis of Contents Scrambling System
    http://www.lemuria.org/DeCSS/crypto.gq.nu/