Защита авторских прав в DVD.

Загороднов Кирилл Валерьевич

Эссе по курсу "Защита информации", кафедра радиотехники,
Московский Физико-Технический Институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

Введение.

Формат DVD был разработан ещё в 1995 году, а уже в 1997 году на выставке в Лас-Вегасе, США общественности были представлены готовые устройства и диски. Тем не менее, кинокомпании начали массовый выпуск видео дисков сравнительно недавно. Причиной этого служила довольно низкая надёжность защиты авторских прав. Производителям аппаратуры были представлены серьёзные требования для организации такой защиты даже на аппаратном уровне. В основном, они были неудобными как для производителя, так и для конечного пользователя и потому приводили к сильному торможению в распространении формата DVD. Не так давно этот формат получил широкое распространение и в этом эссе я хотел изложить некоторые основные методы защиты авторских прав DVD, которые и предоставили возможность такого прорыва.

Региональный код.

Один из первых методов защиты дисков – региональный код. В то время как в одной стране мира показы фильмов в кинотеатрах были уже закончены и начинались продажи DVD, в другой – показы только начинались. Распространение DVD в этих регионах означало бы срыв маркетинговой политики компании. Чтобы этого избежать, было решено на каждом диске один байт тратить на специальную информацию о регионе, где этому диску разрешено распространяться. Законы США обязали производителей считывать этот код на каждом диске, и, если он не соответствует региональному коду устройства, не позволить считывание информации с этого диска. Мир был поделен на шесть регионов. Код региона, в котором находится Россия – "5". Код "0" означает, что диск можно считывать везде. Описанный метод защиты устарел и в Европе уже сейчас продаются DVD - проигрыватели с региональным кодом 0 (можно читать любые диски). В США продажа таких устройств пока запрещена. Уже существуют программы, устанавливающие код проигрывателя в "0". В ответ на такие действия, появились диски, которые не позволяют считывать с себя информацию, если проигрыватель международный (с кодом 0). Вот список регионов мира с кодами.

1. США, Канада
2. Европа, Япония, Южная Африка, Средний Восток (включая Египет)
3. Южная и Восточная Азия (включая Гонконг)
4. Австралия, Новая Зеландия, Острова Тихого Океана, Центральная и Южная Америка, Мексика
5. Восточная Европа (страны бывшего СССР: Россия, Украина и др.), Индийский полуостров, Африка, Северная Корея, Монголия.
6. Китай

7. Зарезервировано
8. Для специального международного использования (самолеты, круизные лайнеры и т.п.)

Существуют и такие проигрыватели, у которых код можно менять, но конечное число раз. Для дисков DVD-ROM, содержащих программное обеспечение, система региональных кодов не применяется.

Macrovision

Macrovision – аналоговая система защиты от копирования на VHS. До появления DVD она использовалась для запрета копирования с кассеты на кассету. Сейчас все производители DVD проигрывателей обязаны встраивать в устройство плату Macrovision. При воспроизведении на изображение накладываются шумовые эффекты, которые не видны при воспроизведении на телевизоре или мониторе, но сильно портят изображении при копировании на VHS, приводя к частому изменению яркости и появлению раздражающих полос. Macrovision используется для полного устранения пиратских копий. Тем не менее, эту защиту можно избежать, аккуратно устранив плату Macrovision из устройства. Кроме того, сейчас уже продаются проигрыватели без Macrovision.

CGMS

Защита CGMS применяется для ограничения количества копий лицензионной продукции. Существует два формата: CGMS-A (аналоговый) и CGMS-D (цифровой). В обоих форматах в потоке видеоинформации содержится также флаг, состоящий из двух бит и в случае аналогового формата передающийся на 21-й линии NTSC. Он передает так называемую CCI (Copy Control Information) – информацию о том, можно или нельзя копировать этот диск, а если можно, то сколько раз. Не все устройства поддерживают этот формат, и он служит, скорее, как знак того, является ли эта продукция лицензионной, или нет. Многие проигрыватели сознательно игнорируют CGMS-A. Система CGMS-D – включает в поток MPEG информации биты, означающие, как и в случае с CGMS-A, информацию о числе возможных копий. Формат CGMS-D относится к классу DTCP (см. ниже) и пока ещё официально не утверждён.

CSS (Content Scrambling System)

Этот формат отличается от вышерассмотренных тем, что он предусматривает шифрование содержимого диска и его последующее расшифрование проигрывателем. Был разработан фирмами Matsushita и Toshiba. Каждому лицензированному проигрывателю присваивается “ключ проигрывателя” (player key) – один из 409. Каждому диску присваивается “дисковой ключ” (disk key). Процесс начинается с взаимной аутентификации проигрывателя и программы, которая проигрывает DVD. При этом используется секретная хэш-функция. В процессе аутентификации обговаривается и сессионный ключ, используемый затем для шифрования данных в процессе передачи от устройства к программе. Затем происходит процесс аутентификации диска и устройства. Проигрыватель просматривает ключи в скрытой области диска. Находит тот, который верно расшифровывается дисковым ключом. Именно он и будет

использоваться далее при шифровании как начальные данные для регистра сдвига. Именно с помощью них формируется псевдослучайная последовательность, уже непосредственно используемая для блочного шифрования содержимого диска. Защита CSS довольно слабая. Есть много относительно несложных вариантов её взлома:

Атака полным перебором. Дело в том, что длина ключа шифрования данных CSS равна всего 40 битам, что делает возможным просто угадать его перебором 2^{40} вариантов.

Обращение к линейным регистрам сдвига. Зная 5 байтов его выхода, можно перебором 2^{16} вариантов установить начальное значение регистров, а значит и все случайные ключи. 5 байтов выхода линейных регистров сдвига можно узнать анализом зашифрованного и незашифрованного текстов.

Можно доказать, что ключ можно установить перебором 2^{25} вариантов без использования информации из линейных регистров сдвига.

Система CSS была взломана в 1999 году. В Интернете была опубликована программа DeCSS. Взломщики установили принципы аутентификации программы и устройства – одно из самых слабых мест CSS. Кроме того, в ней была использована неаккуратность производителей Xing Player, которые не зашифровали должным образом ключи своего проигрывателя.

CPPM (Content Protection for Prerecorded Media)

Создана для защиты DVD-Audio, но в скором времени, видимо, будет использована и для формата DVD-Video. Так же, как и CSS, шифрует данные на диске. Каждому DVD-проигрывателю даётся набор из n ключей. Процесс шифрования CPPM состоит из следующих частей.

Генерируется 56-битный идентификатор альбома.

Генерируется media key, и ему в соответствие ставится целый Media Key Block (MKB). MKB выбирается из соображений, чтобы любой лицензированный DVD-проигрыватель с помощью набора своих ключей может восстановить media key K_m = Process_MKB(MKB, ключи устройства).

Ключ шифрования получается из K_m (media key) и идентификатора альбома, а также из информации о возможность копирования CCI (Copy Control Information).

Идентификатор альбома и MKB записываются на диск. Считывающее устройство с помощью своего набора ключей считывает media key. А по нему восстанавливает ключ шифрования. Сложность этого алгоритма именно в том, что, не зная ключей проигрывателя, сложно определить media key, используя MKB. Видимо, поэтому до сих пор попытки взломать CPPM не привели к успеху. Хотя, теоретически, длины всех

ключей CPPM ограничены 56 битами и эта система, как и CSS, уязвима к атаке полным перебором.

CPRM (Copy Protection for Recorded Media)

Эта система создана для защиты записываемых дисков (DVD-R, DVD-RW и т.д.). Для этого необходимо иметь устройство, поддерживающее CPRM. Принцип работы этой системы защиты таков: на каждый диск в области недалеко от центра лазером выжигается специальный 64-битный код – для каждого диска – разный. Этот код затем используется затем как для шифрования данных диска, так и для расшифрования. До копирования происходит процесс идентификации: проверка устройства на наличие лицензии. Этот процесс аналогичен описанному выше процессу для CPPM. В нем также используется МКВ. При побитовом копировании данные копируются полностью, но код диска, разумеется, становится другим. Поэтому, расшифровать содержимое диска уже не удается.

Водяные знаки для DVD

Концепция водяных знаков на DVD – это присутствие некоторых регулярных намеренных искажений в видео и в аудио файлах. Эти искажения незаметны глазу (в случае видео файлов) и уху (в случае аудио файлов). Они могут нести различную информацию – в том числе и о количестве возможных копий. Причем, при нелицензированном копировании диска, эти водяные знаки исчезают. При лицензированном копировании изменяются вместе с изменением числа возможных копий диска. Это позволяет потребителям рассмотреть, продают ли им лицензионный продукт, или всего лишь копию. При помощи водяных знаков можно также осуществить контроль проигрывания (Playback Ctl.) – запрет воспроизведения дисков без водяных знаков и контроль записи (Record Ctl.) – запрет копирования дисков без водяных знаков. (см. рисунки 1 и 2).

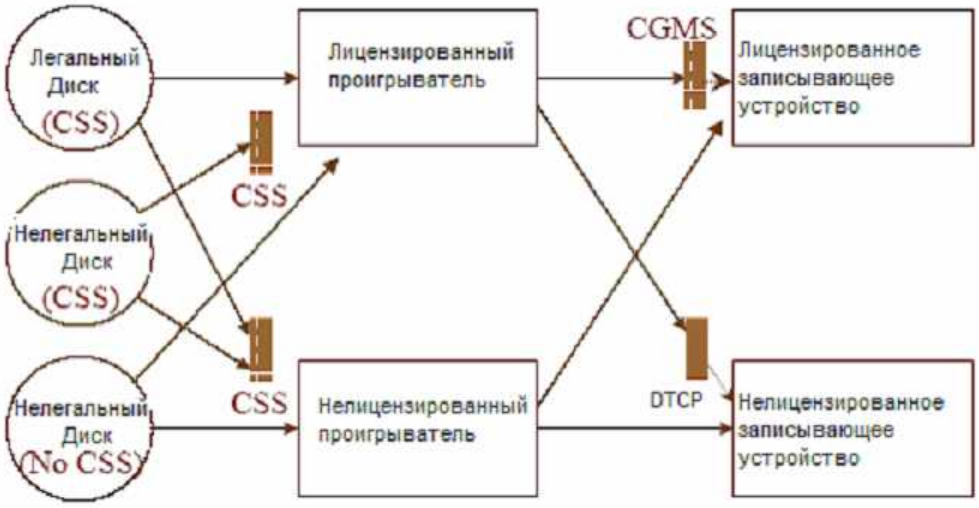

рис.1. Работа систем защиты авторских прав без водяных знаков

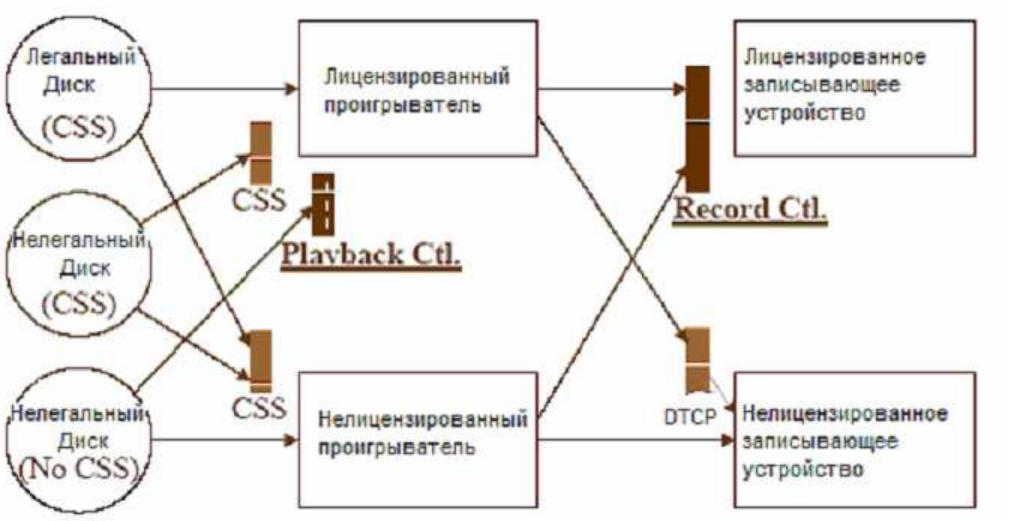

рис. 2. Работа систем защиты авторских прав с водяными знаками

DTCP (Digital Transmission Content Protection)

Эта система была создана в 1998 году пятью компаниями: Intel, Sony, Matsushita, Hitachi и Toshiba. Она предусматривает обмен шифрованной информацией между двумя цифровыми устройствами, соединенными шиной стандарта IEEE 1394. Хотя, на самом деле, использовать можно соединение не только этой шиной. Устройствами могут быть: DVD-player и цифровой телевизор или DVD-player и другой DVD-player: одно из устройств получает, другое – передает. Принцип работы DTCP можно описать следующими шагами:
(будем называть эти устройства: передающее – source device, получающее – sink device).

> Source Device передает зашифрованный поток информации, которая содержит встроенный EMI (Encryption Mode Indicator). EMI – защищённая версия флагов CGMS
>
> В зависимости от полученной EMI, sink device решает, аутентифицироваться полностью – в случае, когда копирование разрешено (Full Authentication) или частично – когда запрещено или ограничено(Restricted Authentication)
>
> Совершается обмен ключами, служащими для шифрования информации во время передачи по шине. (AKE – Authentication and Key Exchange)
>
> Начинается передача шифрованной информации по секретному каналу.

Иллюстрация к этому алгоритму – на рисунке 3.
Если EMI флаг соответствует “копировать один раз” или “больше не копировать”, то возможна только полная авторизация. Шифрование информации предотвращает её кражу при передаче. При этом, содержимое диска остаётся незашифрованным, а шифрование производится всегда новыми сессионными ключами и только при передаче.

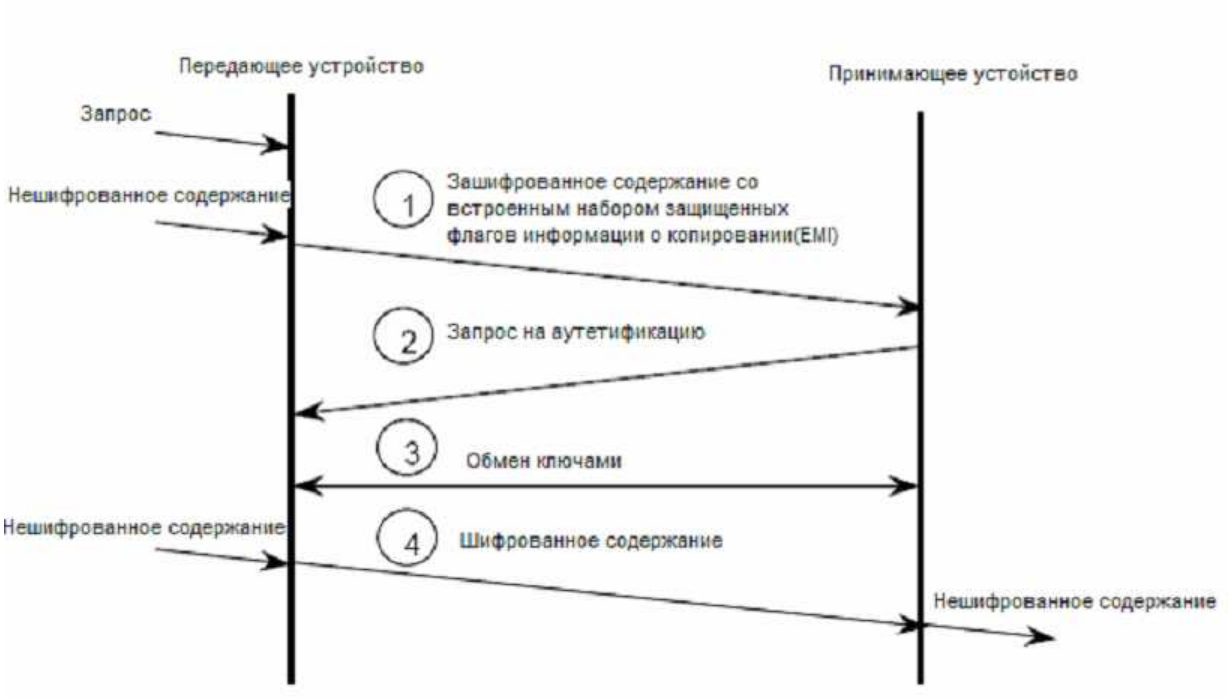

рис.3 Принцип работы DTCP

HDCP (High-Bandwidth Digital Content Protection)

HDCP вполне аналогична DTCP, но работает между проигрывателем DVD и цифровым монитором. В процессе обмена ключами, выясняют, является ли этот монитор авторизованным. Разные условия авторизации накладываются на воспроизводящие устройство и на записывающее. В 1998 году Digital Display Working Group создала новый цифровой интерфейс связи DVI, который мог работать при скорости 5Gbps на разрешении 1600x1200. В этот интерфейс встроена рассматриваемая нами защита HDCP. Предполагается, что эта цифровая разработка вытеснит в будущем используемый сейчас интерфейс SVGA.

Заключение

Из этого обзора всего многообразия средств защиты, мы видим как устаревшие технологии, так и новые, не вполне доведённые ещё до реализации. Но мы видим, что перспективными методами в будущем, видимо, будут те, которые основаны на шифровании данных не на самом диске, а только во время передачи их по конкретному соединению. Такие методы, фактически, включают все самое полезное от предшественников. В нашем обзоре эти методы были представлены DTCP и HDCP. Кроме этого, сильным методом является CPPM, который будет использован в будущем и для шифрования DVD-Video.

Ссылки на источники информации:

Jeffry A. Bloom, Ingemar J. Cox, Ton Kalker, Jean-Paul Linnartz, Matt L. Miller, Brendan Traww “Copyright protection for DVD video”
www.ee.ucl.ac.uk/~icox/papers/1999/ProcIEEE1999b.pdf

Bo Zhou, Peixian Yan, Gang Liu, Zongpeng Liu, Metthew Black “Content Scramble System (CSS)
www.cs.bham.ac.uk/~mdr/teaching/modules/security/students/SS7/CSS_report.doc

Gregory Kesden “Content Scrambling System(CSS): Introduction”
www-2.cs.cmu.edu/~dst/DeCSS/Kesden/

AsusCom (перевод Д.Чеканов) “Методы зашиты DVD дисков”
www.3dnews.ru/storage/dvd-protection/

Andre Adelsbach, Jorg Schwenk “Key Assignment Strategies for CPPM”
http://www.nds.ruhr-uni-bochum.de/adelsbach/papers/AdeSch2004.pdf

DEG Report. Content Protection & DGM
http://www.dvdinformation.com/TechResources/images/DEG%20DRM%20Glossary.pdf

Preserving an Effective DVD Copy Protection System
www.macrovision.com/pdfs/Preserving-an-effective-DVD-Copying-System_0303.pdf

В работе использованы рисунки из Jeffry A. Bloom, Ingemar J. Cox, Ton Kalker, Jean-Paul Linnartz, Matt L. Miller, Brendan Traww “Copyright protection for DVD video”
www.ee.ucl.ac.uk/~icox/papers/1999/ProcIEEE1999b.pdf