Московский физико-технический институт
(ГУ МФТИ)
Кафедра радиотехники
http://www.re.mipt.ru/infsec

Эссе по курсу "Защита информации"

«Способы защиты CD от нелегального копирования»

Выполнил: студент гр.116
Нилов М.В.

Долгопрудный
2005 г.

Введение.

В настоящее время на компакт дисках распространяется огромное количество информации: музыка, фильмы, программное обеспечение и т.д. Поэтому защита CD от нелегального копирования является актуальным вопросом. Широкое распространение компакт диски получили в начале девяностых годов. В то время не было возможности записать диск в домашних условиях, поэтому разработчики старались предотвратить несанкционированное копирование информации с CD на жесткий диск компьютера. Но в начале XXI века пишущие приводы стали доступны, практически, для любого пользователя, и сейчас каждый третий владелец PC может записать CD (а иногда и DVD) диск на своем компьютере.

Проблемы защиты информации на предшествующих носителях не существовало (или она не была настолько серьезной), так как, например, сделать копию с виниловой пластинки не было никакой возможности. Магнитофонную или видео кассету скопировать было не трудно, но при этом резко ухудшалось качество содержащейся на ней информации. А вот с компакт дисками дело обстоит совсем по-другому: чтобы сделать копию, нужно всего лишь пару десятков минут, причем качество копии будет точно таким же, как и у оригинала. Поэтому разработчики всячески стараются создать новые надежные способы защиты информации распространяемой на CD, а пользователи стараются сделать все возможное, чтобы их взломать.

Структура компакт диска.

Чтобы лучше понять механизмы защиты, сначала следует изучить физическую структуру носителя и способ записи информации на диск.

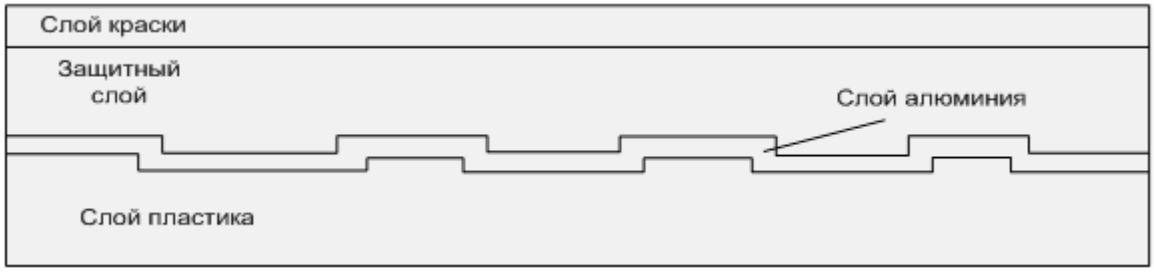

Рис. 1. Структура лазерного диска.

Информация на диске хранится в виде последовательности питов (углублений) и лендов (возвышений), которая образует спираль, идущую от центра диска к его периферии. Если в определенном участке этой последовательности есть переход от пита к ленду (или от ленда к питу), то на соответствующем месте в потоке данных стоит единица, а если такого перехода нет, то ноль. 36 байт образуют кадр (F1 frame); 98 кадров, в свою очередь, образуют сектор. Внутри сектора кадры перемешаны, что позволяет уменьшить отрицательное влияние физических дефектов на качество записи информации. Сектор является принципиально важной порцией информации, так как это наименьшая часть данных, которую может считать CD привод. Адресация секторов возникла в то время, когда они использовались для записи музыки, и поэтому имеет вид мин:сек:доли (доля равна 1/75 секунды). В стандарте для записи AudioCD (IEC 908) сектор представляет собой блок из 2352 байтов, содержащий в себе только поток цифровой музыки. Но этот способ оказался непригодным для записи данных, так как на треке длинной в минуту

могло содержаться около тысячи ошибок. В связи с этим пришлось ввести некоторые вспомогательные поля. У разных режимов записи эти поля отличаются.

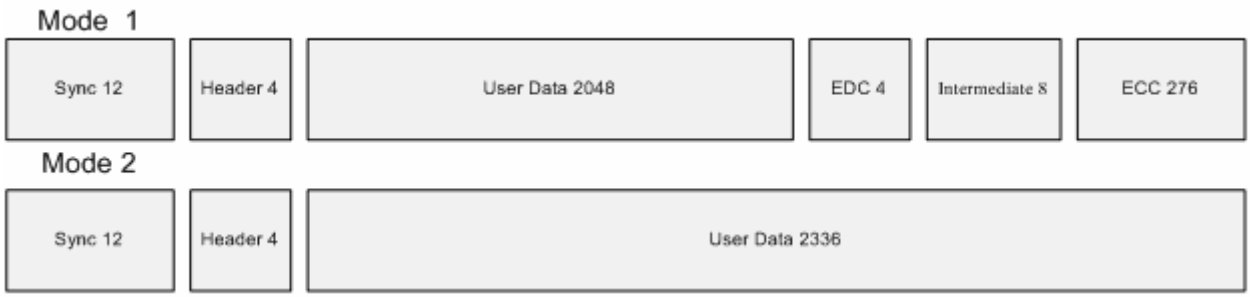

Рис. 2. Сектора для разных режимов записи.

- Поле Sync – является признаком начала сектора и имеет вид: 00 FF FF FF FF FF FF FF FF FF FF 00.
- Поле Header содержит адрес сектора (мин:сек:доли) и режим записи (Mode 1, Mode 2,…).
- Поле User Data – информация.
- Поле EDC (Error Detection and Correction) - область данных, представляющая собой контрольную сумму сектора.
- Поле Intermediate – вспомогательное (в нем записаны нули).
- Поле ECC (Error Correcting Code) – корректирующие коды Рида-Соломона.

Сектора, записанные в одном формате, образуют Track. Минимальная длина трека равна 300 секторов, а максимальная ограничивается размером диска. Первый трек диска называется Lead-In area, а последний – Lead-Out area. Размер области Lead-In составляет 9 Мбайт, 60 секунд или 4500 секторов. Поле ECC содержит TOC (Table of Content) – таблицу содержимого. TOC включает в себя информацию об адресах областей Lead-In и Lead-Out, а также типы всех треков данной сессии (Audio или Data) и режим записи (Mode 1, Mode 2,…).

Любая закрытая сессия заканчивается областью Lead-Out. Ее размер для первой сессии равен 13,5 Мбайт, 90 секунд или 6750 секторов, а для последующих 4 Мбайта, 30 секунд или 2250 секторов. Закрытой называется сессия, у которой есть области Lead-In и Lead-Out. Если за областью Lead-Out следует область Lead-In, то такой диск является мультисессионным.

Переходим непосредственно к защите информации, содержащейся на компакт диске. Можно провести следующую классификацию:

По типу защиты:

- Механизмы предотвращающие нелегальное копирование;
- Механизмы предотвращающие нелегальное цифровое воспроизведение информации (в частности аудио).

По Методу защиты:

- Отклонение от стандарта;
- Обращение к физическим характеристикам диска.

В стандарте записи компакт дисков (еще 20 лет назад) в Red Book был описан бит DIGITAL COPY PROHIBITED/PERMITTED, который либо запрещал, либо позволял цифровое воспроизведение информации, записанной на диске. Этот бит находится в Q-канале, но в настоящее время он просто игнорируется. Поэтому для защиты авторских прав нужно применять другие методы.

Защита AudioCD.

Как известно, компакт диски часто используются для записи музыки в формате AudioCD, которые в основном предназначены для воспроизведения в обычных музыкальных проигрывателях (не на компьютере). Как правило, музыкальные проигрыватели не поддерживают диски, содержащие более одной сессии, и игнорируют содержание TOC (Table of Content). Поэтому очевидным способом защиты является искажение информации, содержащейся в TOC, таким образом, музыкальный проигрыватель беспрепятственно воспроизведет аудио данные, записанные в первой сессии, а CD-ROM возвратит ошибку, вызванную некорректным форматом TOC.

Например, реализацией этого метода может быть неправильный указатель на область Lead-Out: т.е. нужно сделать так, чтобы в TOC указатель на область Lead-Out указывал на место близкое к началу диска. Второй способ: прописать в TOC адрес первого трека как указатель в область, предшествующую области Lead-In, т.е. присвоить отрицательный адрес.

Защита диска от копирования.

Защита диска от копирования делится на две основные категории: защита, препятствующая пофайловому копированию, и защита, препятствующая посекторному копированию. Далее будет показано, как реализовать первую из них.

В файловой системе лазерных дисков каждый файл имеет две важные величины:

- Номер сектора с которого начинается файл. Он задан в формате LBA (Logical Block Address), который можно вычислить, зная адрес в формате MSF, следующим образом: (min*60+sec)*75+frame-150;
- Длина файла в байтах.

Следовательно, чтобы не дать копирующей программе скопировать файл, нужно просто увеличить его размер. Но при этом нужно учесть следующее обстоятельство. Если сектор, которому принадлежит конец файла, не находится за пределами последнего сектора диска, то копирование завершится без проблем, при этом будут скопированы все файлы, которые полностью лежат в промежутке от указанного начала до указанного конца. Поэтому, чтобы механизм защиты сработал, нужно чтобы указатель на конец файла оказался за пределами диска. В этом случае появится ошибка, и считывание прекратится. Но этот метод защиты легко взломать. Для этого достаточно всего лишь задать размер файла, чтобы он влезал на диск, затем скопировать на жесткий диск и отбросить ненужную информацию, находящуюся в конце файла.

Можно повысить защиту, изменив начальный адрес файла. То есть сделать его меньше чем на самом деле. Следовательно, считанный файл (нелегальным образом) будет иметь ненужную информацию в начале, и, кроме того, он будет урезан в конце. Для правильного считывания файла, необходимо, чтобы защитный механизм корректно исправил адрес начала файла.

Еще более надежной защитой является комбинация двух вышеизложенных, т.е. когда изменяется и адрес начала файла, и его длина.

Замечание: защитный механизм должен знать размер копируемого файла, т.е. это число должно храниться в программе. Обычно это большое число, и с помощью несложного анализа злоумышленник может его легко выделить из множества других констант, содержащихся в программе. Поэтому для увеличения степени защиты следует хранить не это число, а остаток от деления на другое небольшое число, например, на число, равное размеру обрабатываемого блока.

Можно пойти другим путем: разрешить копирование файла, предварительно зашифровав его. И, если это мультимедийная информация, то расшифровывать ее сразу при воспроизведении. Самой простой реализацией этого подхода является XOR с некоторой ключевой последовательностью. Такой метод защиты подвержен атаке по открытому тексту, так как аудио и видео файлы почти всегда содержат большое число идущих подряд нулей или F. Кроме того, например, mp3 файл всегда начинается с последовательности FF FB 04. Действия взломщика защиты тривиальные: он ищет повторяющуюся последовательность (скорее всего ею зашифрована более длинная последовательность 0 или F), и проделывает операцию e_data XOR 00..0 (либо FF..F), где e_data – это зашифрованные данные. Таким образом, получается ключевая последовательность, так как:

((data XOR key) XOR data) = key.

Отсюда видно, что для усиления защиты необходимо выбирать длину ключа соизмеримую или заведомо большую длины характерной для данного формата последовательности.

Проверка местоположения физических дефектов диска.

Этот способ защиты основан на том, что на диске делают специальные повреждения (дефекты). При считывании этого места с диска привод делает несколько попыток (в большинстве случаев безуспешных), после чего программа, которая производит копирование, выдает сообщение об ошибке и завершает свою работу. Если же программе удастся считать “испорченную” информацию, то на получившемся диске (образе диска) на соответствующем месте будет находиться физически считываемый сектор, но он будет содержать абсолютно бесполезные данные.

Создать дефекты на диске можно различными способами: самый простой – сделать царапину (т.е. механическое повреждение), также можно выжечь пятно при помощи лазера. Но в большинстве случаев ничего этого делать не надо, так как изготовить идеальный диск практически невозможно, т.е. на нем изначально есть некоторые дефекты, которые можно использовать в качестве ключевых меток для определения того, является диск оригинальным, или это всего лишь дешевая копия.

Принцип действия этой защиты очень прост: в зависимости от положения дефекта с помощью некого алгоритма вырабатывается ключ, а потом из этого ключа получают

регистрационный номер. Пользователь, купивший лицензионный продукт, вводит регистрационный код, и защитный механизм при помощи обратных вычислений получает местоположение дефекта и проверяет, есть ли соответствующий дефект на диске. Если есть - все в порядке, если нет, то это поддельная копия…

Что можно сделать на месте производителя пиратских копий? Можно, конечно, попытаться сделать такой же дефект и на копии, но вероятность того, что защитный механизм не обнаружит подделку, очень мала, так как сектора на диске не связаны с физическим расположением. Кроме того, расположение будет зависеть от таких параметров как плотность спирали и области Lead-In. То есть, воспроизвести физическую структуру cd не удастся, следовательно, придется бороться с защитой программными средствами. Например, сделать программу, которая при проверке секторов на наличие дефекта возвращала бы ошибку чтения, а защитный механизм при этом бы думал, что наткнулся на физический дефект. (Программы CloneCD и Alcohol 120% имитируют физические дефекты на логическом уровне).

Кроме того, можно использовать защиту, основанную на временных диаграммах чтения информации с диска или на измерении угла между секторами. Но это довольно трудоемкая процедура, так как она носит вероятностный характер, и к тому же данные характеристики зависят не только от конкретного носителя, но и от привода, с помощью которого производится чтение.

Система защиты StarForce.

Существует система защиты данных от нелегального копирования "StarForce CD-R, которая включает в себя не только программные средства зашиты, но и сами носители. Существенное отличие дисков StarForce от обычных CD-R заключается в том, что их емкость не 700 Mb или 650 Mb, а 615 Mb.

Рис. 3. Схема создания защищенного диска с помощью StarForce

Защита состоит и следующих этапов:

- Пользователь, который хочет защитить свое программное обеспечение, подготавливает необходимые файлы;
- С помощью удаленного сервера StarForce производится шифрование этих файлов;
- Пользователь записывает эти файлы на диск StarForce;
- С помощью удаленного сервера StarForce генерируется ключ;
- Записываются диски, содержащие защищенные дистрибутивные файлы и ключ.

Литература:

- *Крис Касперски*, Техника защиты компакт-дисков от копирования.- СПб.: БХВ-Петербург, 2004.

- Способы защиты CD от копирования
  http://rusdoc.kulichki.ru/public/multimedia/sposoby_zasity_cd.shtml

- Система защиты данных от нелегального копирования "Starforce CD-R"
  http://www.ixbt.com/optical/starforce-cdr.shtml