УДК 07.09.2004

ЗАЩИТА CD ДИСКОВ И СПОСОБЫ ЕЁ ОБХОДА

Аспирант кафедры ИУ-8 Ковынёв Н. В.
Московский государственный технический университет
им. Н. Э. Баумана

На примере нескольких коммерчески используемых защит посмотрим, как применяется на практике многообразие возможностей нарушения стандартов формирования CD.

Большинство защит используют особые методы размещения информации на диске для создания ключей. В областях, которые сложно скопировать, находится определенная последовательность байтов, позволяющая «открыть» основной исполняемый модуль. Поэтому защита как бы встраивается в защищаемую программу.

Это позволяет авторам защиты совмещать аппаратную защиту (то есть особое устройство диска, не позволяющее его копировать стандартными средствами) с программной, которая может, например, отслеживать обращение программ-эмуляторов, использование записываемых носителей и т. п. Это, в свою очередь, ведет только к усложнению программ-эмуляторов и обратному же усложнению программ-защит. Ниже представлены некоторые типы защит. В целом они довольно похожи, отличаются лишь в нюансах, которые зачастую не разглашаются: защита SecuROM; защита SafeDisc; защита LaserLock; защита Starforce; защита Safecast; защита Tages; защита Alcatraz; изменение логической структуры

Эти методы просты в реализации и вместе с тем могут поставить в тупик большинство пользователей. Нам думается, что они являются самыми оптимальными, потому что профессиональные пользователи все равно скопируют то, что захотят, тем или иным способом.

Аудиодиски защищать сложнее, потому что они не содержат программ, которые могли бы проверять, оригинальный это диск или нет. Поэтому многие системы защиты стараются исключить возможность использования таких дисков на компьютерах.

Первый способ реализовать это заключается в том, что компьютерный диск сложнее устроен, чем аудиодиск. Иными словами, у аудиоплееров требований к структуре диска меньше – они играют что могут: видят аудиодорожку – играют, видят компьютерную дорожку – пропускают.

Компьютер, увидев дорожку, предназначенную для него, во что бы то ни стало старается ее прочесть. И если не выходит, то отказывается читать весь диск. Поэтому производители просто помещают в конец диска нечитаемую компьютерную дорожку. Подобная защита используется, например, в дисках, защищенных Key-Audio и Cactus Data Shield [1].

Но есть более изящное решение. Нечитаемая дорожка по какой-то причине видна на диске невооруженным взглядом. Она находится на внешней стороне диска и отделена от аудиотреков двухмиллиметровым ободком. Достаточно прочертить прямую линию, которая бы проходила через всю компьютерную дорожку и не затрагивала бы аудиотреки. Таким образом, компьютер будет обманут вторично и воспримет диск как аудио.

Есть защиты другого типа. В таких дисках присутствует компьютерный трек. На нем содержатся специальные драйвера, которые устанавливаются при первом использовании диска. Эти драйвера впоследствии предотвращают копирование диска. Данная защита более эффективна, чем предыдущая. Ведь вы можете прослушивать аудиодиск на компьютере. Однако и она не безупречна с моральной точки зрения. Зачем на компьютер устанавливается то, что не нужно? Соответственно, и способ борьбы с ней тривиален. Его открыл некто Джон Холдерман. Для предотвращения работы этой защиты достаточно отключить автозапуск программ с компакт-дисков при первом и всех последующих использованиях диска.

В принципе защита ненадежна, потому что операционная система Windows способна на отключение автозапускающихся программ.

Еще один способ защиты от копирования аудиотреков заключается опять же в том, что аудиотреки менее требовательны к стандартам, чем компьютерные. В них можно неправильно прописать информацию EFM, например. Программа, проигрывающая треки, просто проигнорирует это. А программа, копирующая диски, скопирует мусор. Так действуют защиты типа Safeaudio, MusicGuard [2].

Выход и здесь прост: для копирования нужно использовать специализированное программное обеспечение, например Alcohol. Ну и опять же, некоторые программы для записи MP3 и wav с аудио-дисков прекрасно работают и здесь.

Во всех рассмотренных защитах исполняемый файл защищаемой программы шифруется. Ключи к шифр могут быть спрятаны в RAW-данных, в субканалах и даже в специально устроенных сбойных секторах. Трудности возникают при попытке точно скопировать содержащуюся на диске информацию (многие приводы не передают в компьютер служебную информацию, самостоятельно применяя алгоритм коррекции ошибок и игнорируя ненужную служебную ин формацию). Но даже если ваш привод умеет работать с RAW информацией, воспроизвести артефакты вроде метола LaserLock физически невозможно.

Большинство защит можно обойти копированием при помощи программ, умеющих хорошо работать с RAW-данными (наличие привода, умеющего такие данные читать, обязательно): на пример, таких как BlindWrite или CloneCD. Другой путь – попытаться скопировать структуру диска, а «подправить» программу на жестком диске, чтобы она «позабы-

ла» проверить подлинность CD – хакерский метод. Можно дать программе фиктивные данные – простор для креативной энергии любителей дизассемблеров открывается довольно широкий. Для многих защит существуют универсальные патчи, не дающие защите определить «родной» диск. Например, так можно избавиться от LaserLock. Впрочем, диски с этой защитой за просто может копировать программа CloneCD, несмотря даже на тот факт, что с CD-R невозможно скопировать метку проштампованную на заводе. Оказалось, что нужды в абсолютно точном ее повторении просто нет [3].

Запуск и, конечно же, изготовление хакерских патчей вызывает много вопросов у правоохранительных органов. Но есть возможность найти компромисс, заключающийся в следующем: скопировать диск настолько точно, насколько это позволяют технологии записи компакт-дисков, а то, что не удалось скопировать, сымитировать.

Этот метод хорош, во-первых, тем, что он относительно универсален – не обязательно знать точный метод работы защиты, а разработчикам эмуляторов вовсе необязательно дизассемблировать код защиты (что в большинстве случаев прямо запрещено лицензионным соглашением). Очевидно, что данные, которые программа запрашивает у CD-привода, это не какая-то загадочная и непостижимая информация. А значит, ее можно повторить.

Пусть не всегда удается записать то, что потом программа может прочитать. Но можно заставить ее поверить в то, что все в порядке. Одна из самых распространенных программ, которая не только копирует диски с максимальной точностью, но и эмулирует недостающие данные, – Alcohol.

Для успешного создания резервной копии диска желательно знать тип защиты, который используется в том или ином программном обеспечении. Узнав тип защиты, мы сможем подумать, как ее обойти. Повторимся, что «обходить» защиты допускается только тогда, когда вы хотите создать копию оригинального диска, опасаясь, к примеру, физически повредить дорогой лицензионный диск. Но если вы хотите сделать копию для друга или на продажу, то вы должны четко отдавать себе отчет в том, что это незаконно. Кроме того, это не допускается лицензионным соглашением программ, которые используются для копирования дисков. Так что вы дважды нарушите лицензию. Наша книга предназначена лишь для тех, кто не нарушает закон. Надеемся, что вы понимаете это.

Итак, самая распространенная программа, используемая для определения типа защиты – ClonyXXL. Несмотря на то, что программа уже больше года не обновляется, она прекрасно справляется с определением самых новых защит. Ведь важно узнать не название защиты, а параметры, которые затем могут быть использованы, например, в программе Alcohol.

Список защит, которые она может распознать, довольно внушителен: SafeDisc версий 2.x, 2.51.x, 2.9x; SecuRom, в том числе версий больше четвертой; LaserLok; CD-Cops; DiscGuard; ProtectCD версий VOB и V5; Tages; Ring Protect; StarForce до третьей версии включительно; PhenoProtect;CopyKiller; Dummy Files; Bad Sectors; Key2Audio для AudioCD; Cactus Data Shield версий 100 и 200 для AudioCD;Illegal TOC для AudioCD; Psx-Lybcrypt для PlayStation-дисков.

При этом сканирование не ограничивается только областью CD, проверке могут быть подвергнуты и файлы установленной с диска программы на жестком диске. Это позволяет определить тип защиты с большой точностью.

Литература

1. Ричард Лайонс Цифровая обработка сигналов. – 2-е. – М: Бином-Пресс, 2006. – 656 с.

2. Куприянов, М. С., Матюшкин, Б. Д. Цифровая обработка сигналов. – 2-е. – СПб: Политехника, 2000. – 592 с.

3. Сергиенко, А. Б. Цифровая обработка сигналов. – 2-е. – СПб: Питер, 2006. – 751 с.

УДК 621

ТЕХНИЧЕСКОЕ ДИАГНОСТИРОВАНИЕ РЕЗЕРВУАРОВ ДЛЯ ХРАНЕНИЯ НЕФТИ И НЕФТЕПРОДУКТОВ

Студенты гр. 11312113 Корнюшко С. П., Бедик А. О.
Ст. преподаватель Куклицкая А. Г.
Белорусский национальный технический университет

Целью данной работы является выбор технического средства и разработка методики технического диагностирования резервуаров для хранения нефти и нефтепродуктов.

Под техническим диагностированием понимается комплекс работ, включающих подготовку, натурное обследование элементов конструкции, оценку технического состояния и составление технического заключения о возможности дальнейшей эксплуатации резервуара. Целью диагностирования является своевременное выявление дефектов, снижающих эксплуатационную надежность резервуара.

При проведении технического диагностирования резервуаров для хранения нефти и нефтепродуктов используются следующие методы неразрушающего контроля: ультразвуковой, радиографический, визуально-измерительный.

В качестве технического средства реализации технического диагностирования выбраны: для проведения ультразвукового контроля – ультразву-