применение которого позволяет ускорить вычисления. Значения времени зашифрования и расшифрования на компьютере с процессором К6-233 приведены в табл. 1.

Таблица 1 – Время выполнения процедур зашифрования для данных разной длины и для модулей преобразования разной длины.

M		191	409	191	409
L_k		190	408	190	408
$L_д$		100кБайт	100кБайт	100Байт	100Байт
t,c	Обычная схема	0,5	2,98	0,44	2,91
	Усиленная схема	0,5	3,57	0,44	3,51

При рассмотрении данных таблицы необходимо учесть, что большинство времени выполнения процедур уходит на генерацию общего секрета и ключа. Конечно, время, затрачиваемое на выполнение зашифрования при модуле преобразования 409 бит, достаточно высоко, но при этом необходимо учитывать, что увеличение размера шифруемого текста не приведет к значительному увеличению суммарного времени шифрования (время, затрачиваемое на зашифрование 100 байт на 0,06 секунды меньше, чем время, затрачиваемое на зашифрование 100 кБайт). Кроме того, модуль преобразования 409 бит является слишком большим. При нынешнем развитии средств вычислительной техники и математическом аппарате криптоанализа при шифровании не требуется использования модулей такой длины. Заметим, что операции вычисления ключевой пары d_e и Q_e, а также вычисления общего секрета Z можно производить либо предварительно и затем хранить их соответствующим образом, либо возлагать на специальный сопроцессор. В этом случае скорость шифрования может быть увеличена на несколько порядков.

Заключение

Следует ожидать, что в ближайшее время в качестве направленного шифра будут использоваться алгоритмы (схемы), реализованные в группах точек на эллиптической кривой. Их использование позволяет с одной стороны обеспечить необходимый уровень стойкости, с другой – уменьшить сложность, т. е. повысить скорость преобразований.

Литература: 1. X9.62-1998 Public Key Cryptography For The Financial Services Industry:The Elliptic Curve Digital Signature Algorithm (ECDSA). 2. Стандарт ISO 11166 3. И. Д. Горбенко, П. В. Колесников Оценка стойкости RSA систем, в которых открытые ключи или параметры являются личными.: Радиотехника № 119. 2001 г. 4. X9.42 – 1998, Public Key Cryptography for The Financial Service Industry : Agreement of Symmetric Keys on Using Diffie-Hellman and MQV Algorithms. 5. X9.63-199x Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. 6. И. Д. Горбенко, С. И. Збитнев, А. А. Поляков Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда.: Радиотехника № 119. 2001 г.

УДК 638.235.231

ИСПОЛЬЗОВАНИЕ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ НА КОМПАКТ-ДИСКЕ ОТ НЕЛЕГАЛЬНОГО КОПИРОВАНИЯ И ТИРАЖИРОВАНИЯ

Павел Ткачев, Александр Синицкий, Павел Хлызов, Владимир Горчаков, Сергей Карловский

Научно-информационное предприятие "Виа 4С"

Аннотация: **Приводятся методы защиты информации, которая находится на компакт-диске, от нелегального копирования и тиражирования.**

Summary: **Compact disk unauthorized cloning protection methods are observed. Experemental results are taken and discussed.**

Ключевые слова: **Защита информации, компакт-диск, субканалы, тиражирование, TAO, SAO, RAW, несанкционированное копирование.**

В статье рассмотрены некоторые вопросы защиты информации, записанной на носители данных большего объема, вошедшие во всеобщее употребление полтора десятка лет назад, в частности, с защиты от нелегального копирования и тиражирования данных, записанных на компакт-диски.

Эта проблема очень актуальна, так как известно, какой вред наносит пиратство как медиа-, так и компьютерной индустрии.

Однако, прежде чем описывать практические методы защиты информации, записанной на компакт-диск, от копирования, следует в общих чертах обрисовать особенности постановки подобной задачи.

В настоящее время существует большое количество специальных форматов данных, используемых для записи информации на компакт-диск. К ним относятся не только формат для аудиоданных (CD Digital Audio – CD-DA) и формат, применяемый для хранения произвольной информации в общепринятом для современных компьютерных систем виде (DATA CD), но также специфические форматы, позволяющие создавать фотоколлекции (Kodak CD, CD-G), хранить видеоинформацию в доступном к воспроизведению виде (CD-I), сохранять специфическую текстовую информацию наряду с аудиоданными (CD-TEXT) и другие. Предтечей всех этих форматов является обычный аудиодиск. Развитие других форматов было связано исключительно с грандиозным скачком технологий, произошедших вскоре после внедрения аудиодисков в серийное производство. Фирма Philips, как разработчик базового стандарта записи аудиодисков, была вынуждена признать необходимость разработок принципиально нового подхода к проблеме записи структурированных данных на компакт диск. Более того, в связи с существованием на мировом рынке целого ряда аппаратных платформ, работающих на существенно отличающихся операционных системах, была произведена попытка унификации формата записи данных на компакт-диск. Так возникли весьма экзотические форматы записи, в некоторых случаях необходимые для написания игр и мультимедиа на базе игровых консолей (Amiga CD32, Atari Jaguar, Sony Playstation), в других – для расширения возможностей мультимедийного подхода в компьютерных и бытовых технологиях (Video-CD, CD-I, CD-XA, CD-TEXT, CD-G). Следует отметить одну немаловажную деталь – все эти форматы являются адаптацией базового формата для записи аудиодисков.

Таким образом, на рынке за рекордно малый промежуток времени возникло гигантское количество компакт-дисков, несущих разнообразную информацию как по содержанию, так и по фактической стоимости. Одновременно появилась проблема, связанная с нелегальным распространением подобного рода данных.

За 15 лет развития медиа- и компьютерной индустрии были попытки защитить такого рода интеллектуальную собственность и эти попытки были весьма успешные. Однако говорить о тех методах, которые были применены в то время для реализации защиты, как о методах, которые можно предположительно использовать не в заводских условиях, просто не имеет смысла. Защита дисков тех лет базировалась исключительно на манипуляциях с покрытием дисков, что было в принципе невозможно сделать, не имея пресс-станка для тиражирования дисков заводским способом.

Но теперь ситуация изменилась. Не так давно на рынке появились устройства записи дисков, позволяющие производить достаточно сложные манипуляции как с данными, так и с физикой процесса записи. И, что особенно важно, эти устройства стали вполне доступными в ценовом плане и не требуют специального оборудования.

Рассмотрим предлагаемые нами и принципиально отличные от других методы защиты информации.

Метод 1. Защита информации путем нарушения некоторых управляющих служебных сигналов, записанных на диск синхронно с данными.

Метод 2. Защита информации путем записи на заранее подготовленный носитель, поверхность которого содержит ряд неустранимых дефектов, не мешающих чтению, однако кардинально мешающих перезаписи диска.

Метод 3. Защита информации, базирующаяся на изменении файловой системы, используемой при записи.

Рассмотрим подробнее каждый из перечисленных методов.

Метод 1.

При записи абсолютно всех типов данных на компакт-диск синхронно с блоками данных формируется и записывается ряд управляющих цифровых сигналов. Подобная запись в подавляющем большинстве случаев делается аппаратно и означает, что при этом устройство при помощи внутреннего генератора формирует управляющие последовательности без непосредственного участия программы-копировщика и помещает их в конце каждого блока данных. Такие последовательности принято называть субканалами. Субканалов всего восемь и их принято нумеровать строчными английскими буквами P, Q, R, S, T, U, V, W.

Компакт-диски, записанные в стандарте CD-DA, используют лишь два субканала – P-субканал, который является по сути дела стробирующим при передаче данных от инициатора к устройству, и Q-субканал, в котором записывалась информация о тайм-коде, статусе устройства, кодах аппаратного

корректора ошибок, работающего по схеме Соломона-Рида, а также некоторая другая. Для дальнейшего использования было зарезервировано еще 6 субканалов – R – W, которые на компакт-диск записываются, но фактически не используются. За период развития формата CD-DA в прочие форматы было сделано лишь несколько удачных попыток использования R–W субканалов. Например, в R-субканале при записи диска в форматах CD-G и CD-TEXT записывается некоторая пользовательская информация о копирайтах и авторстве для каждого трека. В редких случаях информацию из R–W субканалов используют тестовые программы для оценки производительности того или иного устройства чтения/записи дисков. Практически, на сегодняшний день ординарный компакт-диск, содержащий информацию произвольного типа, несет в себе 75% незадействованных субканалов.

Подобная ситуация позволяет особым образом защитить компакт-диск. В процессе записи субканалов отдельно от данных формируются полностью заполненные блоки, причем такая запись отнюдь не нарушает никаких договоренностей и стандартов записи данных на компакт-диск, но дополняет. В области неиспользованных субканалов записывается дополнительная управляющая информация, которая неявно связана с данными субканалов P и Q. Программа для записи защищенных подобным образом дисков использует данные Q-субканала для формирования W-субканала. Данные, которые будут записаны в W-субканал, есть по сути закодированные симметричным алгоритмом соответствующие управляющие данные. Первичный ключ для кодирования формируется на основе данных, записанных в служебных областях на компакт-диске. Параллельно вводится дополнительный псевдостробирующий R-субканал. Суть введения последнего заключается в том, что часть записанных на диск данных помещаются в область с верным Q-субканалом, но с ошибочным основным стробом. При чтении записанного таким образом компакт-диска эти данные будут просто проигнорированы, не вызвав сообщения об ошибке. Однако, при использовании программы, способной корректно читать подобные диски, перед принятием решения о том, насколько эффективна читаемая информация, будет произведена дизъюнкция реального и псевдостробирующих каналов, что обеспечит корректное и полное чтение данных во всем объеме.

Смысл введения кодированного W-субканала заключается в следующем. Большинство программ при копировании диск-диск не читают область субканалов непосредственно, но используют встроенные генераторы либо полагаются на возможности самого устройства. При попытке перезаписи диска с использованием подобных алгоритмов W и R субканалы потеряются. Программа, которую нелегально скопировали, перед запуском или в процессе своей инсталляции проверит ультраструктуру субканалов носителя, с которого произведен запуск, и в том случае, если декодирование субканала с программно полученным ключом не даст контрольного результата, просто не запустится.

Данный вариант защиты еще более эффективен при совместном использовании с методом 2.

Метод 2.

Данные должны быть записаны на диск, содержащий «плохие» для чтения области. Подобные области не должны мешать чтению данных ни одним из принятых для данного формата методов. Попытки чтения этих областей при копировании компакт-диска должны закончиться негативно и прервать процесс копирования.

Существует целый ряд устройств для записи компакт-дисков, поддерживающих команды управления мощностью лазера и скоростью вращения вала привода. К ним относятся Plextor, Matsashita, Plasmon и некоторые модели Teac. Создание сбойной области на диске сводится к процедуре хаотичного варьирования этих параметров в процессе записи при помощи SCSI-команд Optical Power Calibration и Set Shaft Spd [1, 2]. Необходимым и достаточным условием последующего успешного чтения данных, записанных подобным образом, есть точный мониторинг сбойных зон в момент записи. Это означает, что записывающая программа варьирует параметры лазера до записи, после чего, при достижении нормальных условий записи на поверхность диска в данном месте, записывает эффективные данные. Причем данные Q-субканала, отвечающие за позиционирование следующего не сбойного сектора, формируются внутри пишущей программы, а не самим устройством и записываются отдельно.

Таким образом, используя этот алгоритм, можно получить защищенный диск с практически любыми данными.

Недостаток этого метода состоит в ощутимом уменьшении общего объема данных, которые возможно записать при повышении степени защиты диска. Однако преимущество метода в том, что ни одно устройство копирования не сможет сделать копию такого диска в режимах TAO (Track-at-Once), SAO (Session-at-Once) и RAW. Конечно пользователь может нелегально скопировать данные без дублирования структуры диска, но легко реализуемая программная проверка носителя, откуда запущена программа, не даст возможности для запуска программы не с оригинального компакт-диска.

Метод 3.

Запись данных на любой носитель всегда делается структурировано. Метод построения базовых структур для упорядочения информации на носителях принято называть файловой системой. Этот метод определяет

такие параметры, как размер апертуры чтения/записи (что иногда ошибочно называют длинной сектора), способ формирования директориальных записей и таблицы размещения, синхронизационные данные и коды контрольных сумм.

Запись данных на компакт-диск производится с использованием файловой системы CDFS (Compact Disc File System). При этом в служебной области формируется таблица размещения данных, содержащая векторы начала данных (дорожек или файлов) и длины.

Суть данного метода защиты сводится к использованию нестандартной файловой системы при абсолютно стандартной записи таблицы размещения. При записи совокупности данных на диск пишущая программа формирует таблицу и записывает ее в соответствующую часть служебной области. При этом запись о размере данных остается равной нулю, а первый вектор данных указывает на область, в которой в стандартном CDFS-формате записан блок данных, соответствующих специфической программе-загрузчику. Собственно данные пишутся после этого блока уже в формате защищенной файловой системы.

При попытке копирования такого диска стандартная программа чтения определит, что диск заполнен, но суммарная длина всех файлов близка к нулю и не сможет выполнить копирование ни в одном режиме, кроме режима RAW. С другой стороны, при запуске с такого диска программа-загрузчик, которая начнет работать автоматически, корректно прочитает данные из областей с нестандартной файловой системой, после чего приложение, записанное на диске, запустится. Использование этого метода возможно вместе с методами 1 и 2, что еще в большей степени повышает надежность защиты.

Недостатком данного метода является его несколько меньшая универсальность.

Описанные методы позволяют осуществить защиту от попыток копирования с использованием режимов TAO, SAO и RAW. Однако следует помнить, что существует еще и метод снятия копии с матрицы-оригинала компакт-диска в заводских условиях, когда делается полная и точная физическая копия на пресс-станке, а потом тиражируется в нужных пиратам объемах. Но это уже скорее общая проблема обеспечения безопасности на фирме-производителе. Поэтому мы считаем, что разработанные нами методы должны существенно снизить возможность нелегального копирования и тиражирования данных с компакт-диска.

ООО “Виа-4С” предлагает ряд комплексных решений по защите от несанкционированного копирования информации, записанной на носители типа “компакт-диск” в форматах CD-DA (Digital Audio), ISO/IEC 10149 (Data Mode 1), ISO/IEC 10149 (Data Mode 2), CD-ROM XA (Data Mode 2 form 1),Mixed Mode CD, CD-I, а так-же vendor-specific форматов при наличии соответствующего технического описания.

Возможна реализация защиты как на аппаратном, так и на программном уровнях.

Аппаратный уровень защиты подразумевает внедрение специфических зон в служебные и PMA (Program Memory Area) [1, 2, 3] зоны физического носителя. Эффект проявляется в невозможности корректного копирования защищенного носителя в режимах TAO, SAO и RAW.

Программный уровень защиты подразумевает контроль специфично записанных зон носителя при запуске и работе защищенного программного продукта. Подобные зоны формируются как элементы защиты аппаратного уровня, что также обеспечивает дополнительный уровень защиты.

В таблице приводятся результаты тестов по копированию дисков разных типов.

Таблица

Программа-копировщик	CD(RW) Привод	Тип носителя, режим копирования	Результат	Комментарии
CloneCD 3.0.9.1, © Elaborate Bytes	TEAC CD-W54E, PLEXTOR CDR PX-W1210A	CD-DATA SAO, RAW NO Read Subchannels NO Fast Error Skip NO Intelligent Bad Sector Scanner	Unable to Read Sectors	Копирование останавливается в результате большего количества ошибок чтения
CloneCD 3.0.9.1, © Elaborate Bytes	TEAC CD-W54E , PLEXTOR CDR PX-W1210A	CD-DATA SAO+SUB, RAW Read Subchannels Audio NO Fast Error Skip NO Intelligent Bad Sector Scanner	Unable to Read Sectors	Копирование останавливается в результате большего количества ошибок чтения

Продолжение таблицы

CloneCD 3.0.9.1, © Elaborate Bytes	TEAC CD-W54E , PLEXTOR CDR PX-W1210A	CD-DATA SAO, SAO+SUB, RAW Read Subchannels Audio Fast Error Skip NO Intelligent Bad Sector Scanner	Unable to Read Sectors	Копирование происходит неприемлемо медленно, ориентировочное время создания имиджа диска превышает 150 часов. При прерывании процесса чтения и попытке записи незавершенного имиджа на диск копия не работает.
CloneCD 3.0.9.1, © Elaborate Bytes	TEAC CD-W54E, PLEXTOR CDR PX-W1210A	CD-DATA SAO, SAO+SUB, RAW Read Subchannels Audio Fast Error Skip Intelligent Bad Sector Scanner		Копирование происходит неприемлемо медленно. Данные из защищенных зон переписываются некорректно. Копия не соответствует оригиналу.
CDRWIN 4.0A © Golden Hawk Technology	TEAC CD-W54E, PLEXTOR CDR PX-W1210A	CD-DATA Disc Image/Cue Sheet ALL reading options	Error: Unable to analyze disc layout. Illegal track type encountered.	Копирование невозможно.
Nero-Burning 5.0.2.2 © Ahead Software	TEAC CD-W54E, PLEXTOR CDR PX-W1210A	CD- DATA CD-Copy ALL reading options	Illegal track mode	Копирование невозможно.
WinOnCD 3.70.572 © CeQuadrat	TEAC CD-W54E, PLEXTOR CDR PX-W1210A	CD- DATA CD-Copy ALL reading options	There's not enough room on drive D: to hold the image files. Requires approx. 18850 GB, available 1.5 GB	Копирование невозможно. Определяемый размер имидж файла не соответствует истинному. Копирование зависает.
PlexTools 1.0.8 © Plextor	TEAC CD-W54E, PLEXTOR CDR PX-W1210A	CD-DATA	No messages	Копирование невозможно. Копирование зависает.

Литература: 1. International standard. Audio recording – compact disk digital audio system. CEI/ IEC 60908. February 1999. 2. National Standard of Accredited Standards Committee X3. Working draft. Project X3T9.2-375D. Revision 10L. September 1993. 3. American National Standards Institute, National Committee on Interface Technology Standards T10. Working draft. Project T10/1363-D. Revision 01. March 2000. 4. American National Standards Institute, National Committee on Interface Technology Standards T10. Project 333-2000. May 2000.