Продукция компании Protection Technology

Сегодня, когда информационные технологии развиваются невероятными темпами, проблема защиты информации встает особо остро. В частности, в связи с тем, что широкое распространение получают диски форматов CD-R/RW, а также специализированные программы-дупликаторы, которые делают процесс копирования доступным практически каждому пользователю.

По некоторым оценкам сегодня в России объемы нелегального копирования, производимого в домашних условиях, стали соизмеримы с объемом нелегального копирования, производимого заводским способом. То есть, примерно половина всего нелегального копирования производится в домашних условиях. И если противодействовать заводскому пиратству еще удается, то бороться с домашним копированием практически не возможно.

В дополнение ко всему вышесказанному, многие средства защиты от нелегального копирования, используемые западноевропейскими и американскими издателями программной продукции, имеют невысокую стойкость и требуют заводского оборудования для производства лицензионных дисков.

В период, когда создавалась компания Protection Technology, наиболее популярными средствами защиты от копирования компакт-дисков являлись те, которые наносили физические метки на определенные области дисков. При попытке копирования содержимого компакт-диска стандартные программы не могли прочитать соответствующие области и выдавали сведения об ошибки чтения, соответственно, процесс копирования заканчивался. Однако, подобные системы защиты требовали использование специального заводского оборудования, имевшееся в ряде европейских стран, а также в США, Японии и Австралии.

Разработки Protection Technology были нацелены на создание системы защиты, не требующей использования специального оборудования — так, что любой завод мог осуществлять тиражирование защищенных дисков. В основу технологии был положен следующий принцип определения легальности копии: проводилась проверка соответствия физических параметров установленного пользователем диска аналогичным параметрам лицензионного CD. Так как эти параметры определяются исключительно геометрией исходной матрицы, с которой была отпечатана партия заводских дисков, то эти диски нельзя ни скопировать, ни эмулировать. При этом диски, произведенные с разных матриц, но содержащие

один и тот же программный продукт, различались по своим физическим параметрам.
Чтобы извлечь 16-байтный ключ, содержащий информацию об оригинальных физических параметрах всей заводской партии дисков, достаточно использовать один лицензионный CD и обыкновенный привод CD-ROM. Извлекаемый ключ используется модулем защиты, который встраивается в качестве эталона для идентификации лицензионных дисков в выполняемый файл программного приложения.

Для того, чтобы исключить слабые стороны, присущие многим современным системам защиты (такие, как недостаточная антиотладочная база и низкая устойчивость к профессиональному взлому), была разработана технология шифрования выполняемых файлов и реализован ряд решений, эффективных против современных методов реверсинга (reverse engineering), например восстановление дампа оперативной памяти и трассировка выполняемого кода с помощью отладчиков. Программный код шифруется при помощи псевдослучайного закона. Это позволяет при неоднократной защите всем защищенным версиям одного и того же выполняемого файла отличаться друг от друга, что значительно затрудняет работу взломщиков. Теперь будет невозможно разработать универсальный алгоритм нейтрализации защиты (так называемого generic crack), и, следовательно, придется взламывать по-новому каждый из защищенных StarForce программных продуктов и обновлений для них.

Помимо собственной системы шифрования, была внедрена клиент-серверная система ее установки. Операции по шифрованию исполняемых файлов и извлечению ключа выполняются на удаленном сервере StarForce с помощью алгоритмов, недоступных злоумышленнику. Таким образом, вся процедура установки защиты производится непосредственно с рабочего компьютера – необходим только доступ в Интернет.

StarForce Professional является основным продуктом компании Protection Technology, который позволяет производить защиту программных продуктов, издаваемых на компакт-дисках большими тиражами, то есть в заводских условиях.

В основе защиты лежит принцип привязывания программного обеспечения к параметрам заводской партии дисков с помощью 24-байтного ключа. Кроме того, разработчикам поставляется комплект, позволяющий значительно повысить стойкость защиты ко взлому еще на этапе создания программного кода путем внедрения callback- и loopback-функций.

Для установки StarForce Professional применяется уже упомянутая клиент-серверная технология. Программа Professional Wizard в автоматическом режиме производит шифрование на удаленном сервере исполняемых файлов и программных библиотек, а также извлекает (экстрагирует) открытый ключ, который в последствии будет использован для изготовления заводской партии компакт-дисков.

В процессе запуска приложения встроенный в него модуль защиты генерирует запрос на введение открытого ключа, который печатается на упаковке лицензионного компакт-диска. Пользователю достаточно ввести пароль один раз: если он верен, то программа запишет его в реестр компьютера и будет использовать для дальнейших запусков. Если ключ не соответствует параметрам CD, вставленного в дисковод, то программный код не будет выполнен.

В отличие от многих других систем защиты, StarForce Professional способна защитить программный продукт от копирования с помощью специальных утилит клонирования, а также препятствует запуску программ с носителя путем эмуляции привода CD-ROM.

StarForce CD-R отличается от предыдущей системы зашиты тем, что предназначена в первую очередь для защиты предварительных и тестовых версий программного обеспечения. Также система может использоваться для защиты единичных экземпляров программ, которые тиражируются при помощи привода CD-R или CD-дупликатора.

Для системы StarForce CD-R были разработаны специальные носители CD-R, которые, фактически, являются одним из компонентов защиты (для их производства используют матрицы, разработанные в компании Protection Technology). Это было сделано потому, что привязка программного обеспечения к обычным CD-R дискам оказалось неэффективной. Дело в том, что диски из одной заводской партии могли быть свободно приобретены как разработчиками, так и пиратами. Физические параметры дисков StarForce CD-R, используемые для идентификации лицензионного программного обеспечения, отличаются от параметров, применяемых другими производителями. В результате максимальный объем информации, который можно вместить на один спецноситель, ограничен 615 мегабайтами (против 650-700 мегабайт для обычных носителей). При этом рекомендуется записывать диски на скоростях, не превышающих 16х.

Система защиты StarForce достаточно функциональна, чтобы копии дисков StarForce CD-R с защищенным приложением, клонирование с помощью таких программ как CloneCD, CDRWin, BlindWrite и других были неработоспособными. Защищенный диск также нельзя запустить с помощью эмуляторов CD-ROM (таких как Virtual CD-ROM и подобных). Немаловажным фактом является и то, что диски StarForce CD-R совместимы с разнообразными моделями существующих устройств CD/DVD-ROM. Это обусловлено тем, что поверхность дисков не содержит искусственных повреждений или специальных нечитаемых меток.

Как и случае с StarForce Professional, для установки защиты система StarForce CD-R используется клиент-серверная технология. При помощи программы CD-R Wizard пользователь производит операции шифрования исполняемых файлов и программных библиотек, а также извлекает (экстрагирует) ключ. Отличие заключается в том, что тиражирование производиться с помощью привода CD-R/RW, а ключ записывается непосредственно на носитель. В процессе запуска приложения ключ автоматически считывается с компакт-диска. В случае, если программа защиты установит несоответствие ключа физическим параметрам носителя, диск идентифицируется как нелегальная копия, и приложение запущено не будет.

(Picture)

StarForce File Protection – инструмент, предназначенный для защиты от несанкционированного просмотра, изменения и копирования данных (в том числе представленных в файлах стандартных форматов). Объектами защиты могут стать электронные энциклопедии, базы данных, мультимедийные библиотеки, компьютерные игры, обучающие программы и т.п. StarForce File Protection является приложением к системам StarForce Professional и StarForce CD-R.

В процессе защиты пользователь указывает, какие файлы данных в приложении необходимо защитить, а затем все они переводятся в единый файл-контейнер, где хранятся в формате, закрытом для обычного использования. В процессе работы приложения доступ к файлам происходит только через модуль защиты. Файлы извлекаются из контейнера по запросам защищенного приложения, для которого работа с этими файлами не отличается от работы с ними в обычном формате. При попытке нейтрализовать установленную защиту с целью получить копию программного продукта, работающего без лицензионного компакт-диска, происходит блокировка доступа к файлам данных, а копия приложения начинает работать некорректно. Чтобы этого избежать, злоумышленнику придется

проверить работу приложения от начала до конца, что приведет к увеличению материальных затрат, что уменьшит экономическую целесообразность взлома.

Antireversing C/C++ Compiler – суть полнофункциональный компилятор C/C++, который в процессе компиляции добавляет в программный код дополнительные инструкции и операторы так, что вернуть его в начальное состояние практически невозможно. При этом функциональность программного модуля не нарушается, а затраты времени, необходимого для исследования скрытых алгоритмов приложения с помощью отладчиков и дизассемблеров, многократно увеличиваются. С помощью Antireversing C/C++ Compiler разработчики могут самостоятельно защищать выполняемые файлы приложения, написанные на C/C++.

Электронный ключ, который был разработан в компании Protection Technology, достаточно своеобразен. В нем представлены все стандартные функции подобных систем: шифрование данных, генерация случайных чисел, вычисление хэш-функций, хранение данных в энергонезависимой памяти. Но есть и отличия. Часть процедур защищенного приложения хранятся и выполняются внутри ключа, а приложение получает лишь результаты их выполнения. Это стало возможно благодаря виртуальной машине с собственным языком программирования, используемой внутри ключа. В процессе подготовки программного кода разработчику достаточно указать наиболее важные функции приложения. Затем, на удаленном сервере StarForce, в процессе шифрования всего программного кода и библиотек приложения, эти функции будут транслированы на язык виртуальной машины и перенесены в ключ. Таким образом, чтобы создать эмулятор ключа и нейтрализовать защиту, злоумышленнику помимо расшифрования плавающего протокола обмена информацией между ключом и ядром защиты необходимо полностью восстановить фрагменты скрытого в ключе кода.

StarForce PDF – эта разработка Protection Technology предназначена для защиты от несанкционированного использования электронных документов, представленных в формате PDF и распространяемых на дисках CD-ROM и CD-R. В основу работы StarForce PDF положена привязка PDF-документов к лицензионному CD. Пользователь, используя стандартную версию программы Acrobat Reader, может открыть защищенные документы только при наличии в приводе CD-ROM лицензионного компакт-диска.

По материалам:

1) Игорь Павлюк, «Protection Technology: защита по-русски», КомпьютерПресс 7'2002.
2) Александр Воробьев, «Система защиты данных от нелегального копирования "Starforce CD-R"», 28 августа 2002 года.