УДК 004.056.5

Подсистема защиты авторского права в программном обеспечении

А.В. Чернышова, Д.В. Кубашевский
Донецкий национальный технический университет
alla@pmi.dgtu.donetsk.ua, dehax12@gmail.com

Чернышова А.В., Кубашевский Д.В. Подсистема защиты авторского права в программном обеспечении. *В данной работе выполнен анализ существующих механизмов защиты авторского права на программное обеспечение и предложено описание работы программной подсистемы защиты ПО с использованием криптографических алгоритмов шифрования.*

Введение

Ежедневно продаётся огромное количество копий программного обеспечения. Каждая такая копия обычно включает в себя систему защиты от копирования и проверки лицензии на приобретённое ПО. Однако зачастую подобные системы защиты ненадёжны, так как их разработке уделяется значительно меньше времени и внимания, чем оригинальному продукту — объекту защиты. Поэтому программное обеспечение, которое имеет такую слабую защиту, обычно подвергается "взлому" "крэкерами". Далее взломанные копии попадают в открытый доступ, где обычные пользователи бесплатно скачивают полностью работоспособное ПО. Таким образом, разработчики ПО несут огромные финансовые потери.

Лицензия на программное обеспечение — это правовой инструмент, определяющий использование и распространение программного обеспечения, защищённого авторским правом. Обычно лицензия на программное обеспечение разрешает получателю использовать одну или несколько копий программы, причём без лицензии такое использование рассматривалось бы в рамках закона как нарушение авторских прав издателя.[1]

На рынке программного обеспечения в настоящий момент активно используется программное обеспечения с открытым кодом, но также большое количество коммерческих программных продуктов.

Сегодня используются такие виды лицензий на программное обеспечение: открытая лицензия (Open Source), бесплатная лицензия (Freeware, GPL, Adware, Postcardware, Donationware, Nagware, begware) условно-бесплатное программное обеспечение (ShareWare, Trial, trialware, Demo, demoware), коммерческое программное обеспечение (Commercial). [1]

Цель работы — описать подсистему защиты авторского права в программном обеспечении с использованием криптографических алгоритмов шифрования для возможного использования при лицензировании условно-бесплатного или коммерческого программного обеспечения.

Обзор существующих механизмов защиты авторского права на программное обеспечение

Для защиты ПО используется ряд методов, таких как:

- алгоритмы запутывания - используются хаотические переходы в разные части кода, внедрение ложных процедур - "пустышек", холостые циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и т.п.;
- алгоритмы мутации - создаются таблицы соответствия операндов - синонимов и замена их друг на друга при каждом запуске программы по определённой схеме или случайным образом, случайные изменения структуры программы;
- алгоритмы компрессии данных - программа упаковывается, а затем распаковывается по мере выполнения;
- алгоритмы шифрования данных - программа шифруется, а затем расшифровывается по мере выполнения;
- вычисление сложных математических выражений в процессе отработки механизма защиты - элементы логики защиты зависят от результата вычисления значения какой-либо формулы или группы формул;
- методы затруднения дизассемблирования - используются различные приёмы, направленные на предотвращение дизассемблирования в

пакетном режиме;

- методы затруднения отладки - используются различные приёмы, направленные на усложнение отладки программы;

- эмуляция процессоров и операционных систем - создаётся виртуальный процессор и/или операционная система;

- нестандартные методы работы с аппаратным обеспечением - модули системы защиты обращаются к аппаратуре. [2]

Практически для каждого популярного ПО можно найти в интернете взломанную рабочую копию. В основном, защитные механизмы делятся на две основные категории: основанные на знании пароля, серийного номера и основанные на владении носителя информации с ключом, файлов программы.

Защита, основанная на знании, является наиболее уязвимой, так как легальные пользователи могут сообщить всем серийный номер, с помощью которого другие пользователи могут запустить программу нелегально. В случае если серийный номер уникально генерируется для каждого пользователя и является функцией его имени, активировать программу одинаковым серийным номером не получится. В этом случае придётся проанализировать алгоритм генерации серийного номера в зависимости от имени пользователя либо избавиться от алгоритма защиты, "пропатчив" исполнимый код программы, то есть, изменив в бинарном коде программы условие, при котором система защиты посчитает ПО активированным.

Более стойкими являются системы защиты второй категории, основанные на владении некоторым носителем, который практически невозможно воссоздать самостоятельно. Но огромным минусом такой защиты является тот факт, что ключевой носитель может быть потерян или испорчен. Тогда пользователю придётся пройти процедуру восстановления такого носителя при условии, если разработчик её вообще поддерживает. [3]

Алгоритм работы подсистемы защиты авторского права программного обеспечения

Предположим, имеется разработанное программное обеспечение, которое нужно защитить от незаконного копирования и дальнейшего использования.

При выборе алгоритма работы подсистемы защиты авторского права программного обеспечения будем считать, что программное обеспечение условно-бесплатное или коммерческое.

Основная идея подсистемы защиты авторского права ПО состоит в том, что существует некоторый файл, без которого программа не способна выполнить какие-либо важные для пользователя функции (набор функций программы ограничен). Для доступа ко всему набору функций ПО, необходимо получить доступ к дополнительному файлу. Получить расширенные возможности по работе с программной пользователь может лишь предварительно подтвердив свои лицензионные данные — права на использование данного ПО. Таким образом, невозможно будет использовать программу без покупки лицензии на неё. [4]

Пусть защищаемое ПО состоит из запускаемого исполнимого модуля *.exe и вспомогательного модуля *.dll [5], благодаря которому будет возможно работать с полной версией программы, доступной в платной версии. Покупая программу, пользователь получает установочный дистрибутив, который содержит только лишь запускаемый модуль *.exe.

После установки программы, система защиты запрашивает данные о лицензии, например, персональные данные пользователя и соответствующий ключ, которые данный пользователь получил при покупке ПО.

На рисунке 1 изображён процесс получения вспомогательного модуля программы.

Алгоритм получения пользователем вспомогательного модуля программы будет следующим. При установке программного обеспечения и вводе пользователем данных (ФИО, электронный адрес, номер телефона), персональные данные пользователя и некоторая информация об используемом аппаратном обеспечении компьютера (серийный номер процессора, жёсткого диска, MAC-адрес сетевого адаптера), а также ключ, который пользователь получил при покупке, передаётся на сервер фирмы-разработчика устанавливаемого программного обеспечения с использованием защищённого канала связи (использование защищённого протокола передачи данных) [6]. Полученная информация на сервере записывается в базу данных фирмы-разработчика ПО. Таким образом, на сервере хранится вся информация, идентифицирующая пользователя, установившего программный продукт.

Следующим этапом является использование криптографических алгоритмов [7] для шифрования вспомогательного модуля программы *.dll.

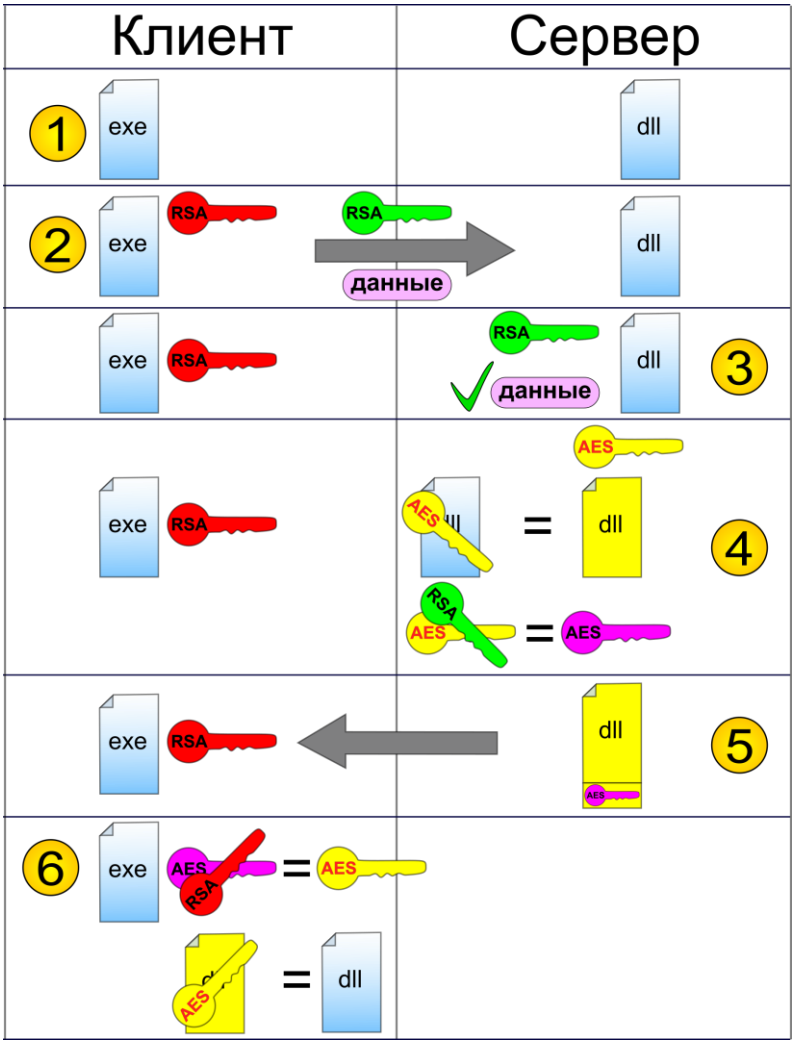

Рисунок 1 — Получение вспомогательного модуля программы с использованием криптографических алгоритмов шифрования

Файлы *.dll можно защитить, используя симметричный алгоритм шифрования (например, AES) [8]. Для генерации уникального ключа симметричного алгоритма, которым будет зашифрован вспомогательный модуль, можно использовать полученную информацию из регистрационной формы пользователя.

Таким образом, вспомогательный модуль программы будет зашифрованным передаваться по сети, храниться на машине пользователя.

При использовании симметричных алгоритмов шифрования для защиты файлов, хранящихся на диске или передаваемых по сети, рекомендуется ключи, которыми шифруются файлы, также защищать. Для защиты ключей симметричных криптографических алгоритмов используют криптографические алгоритмы с открытым ключом, например алгоритм RSA.[7]

Предположим, что на сервере фирмы-разработчика ПО уже сгенерирован ключ симметричного алгоритма шифрования для пользователя, подтверждающего свою лицензию и ожидающего вспомогательного модуля программы.

Для шифрования самого ключа симметричного алгоритма используем схему шифрования с открытым ключом [7].

При регистрации пользователя в программе должна сгенерироваться пара ключей (открытый и закрытый).[8] В дальнейшем закрытый ключ будет храниться на машине пользователя, открытый ключ вместе с персональными данными пользователя передаётся на сервер фирмы разработчика и также хранится в базе данных. С помощью открытого ключа сервер зашифрует ключ симметричного алгоритма, которым был зашифрован вспомогательный модуль программы, допишет его в зашифрованный вспомогательный модуль (например, в конец файла) и передаст программе пользователя.

При необходимости использования вспомогательного модуля программой сначала будет извлечён зашифрованный открытым ключом ключ симметричного алгоритма, с

помощью закрытого ключа ассиметричного алгоритма будет расшифрован ключ симметричного алгоритма, затем с помощью ключа симметричного алгоритма будет расшифрован сам файл вспомогательного модуля. Программа сообщает об успешной активации лицензии. Теперь, при необходимости обращения к вспомогательному модулю, программа расшифровывает его "на лету", а при завершении работы удаляет расшифрованный файл из памяти.

Достоинства и недостатки подсистемы защиты авторского права программного обеспечения

Описанная подсистема защиты ПО обладает рядом достоинств и недостатков.

Достоинства:

– обычный опытный пользователь не сможет обойти защиту;

– система защиты способна справиться с крэкерами-новичками, а также запутать крэкеров среднего уровня;

– в случае использования эффективного средства обфускации для сокрытия алгоритма подсистемы защиты, а также использования методов виртуализации функций системы защиты, даже опытным крэкерам понадобится немало времени, чтобы исследовать и взломать алгоритм проверки лицензии;

– для получения вспомогательного модуля, для защиты которого используются криптографические алгоритмы, нужно знать ключи и используемые криптографические алгоритмы;

– взлом базы данных сервера фирмы-разработчика ПО, на котором хранится персональная информация о пользователях и их серийных номерах программы, не даст информации обо всех используемых ключах криптосистемы, а значит, не позволит расшифровать вспомогательный модуль программы и использовать незаконно программный продукт;

– для предотвращения использования метода перебора ключей, рекомендуется использовать значительную длину ключей в симметричных и ассиметричных алгоритмах шифрования.

Недостатки:

– без обфускации подсистема защиты не защищена от декомпиляции и дизассемблирования с целью внесения изменений в алгоритм работы функций защиты (патчинг);

– при активации программы необходимо подключение к интернету;

– в случае использования информации об аппаратном обеспечении конечного пользователя для генерации уникального ключа, которым будет зашифрован вспомогательный модуль, при замене какой-либо аппаратной части необходимо будет сообщать разработчику об этом и проходить снова процедуру активации программы.

Выводы

В ходе выполнения данной работы были рассмотрены и проанализированы существующие механизмы защиты авторского права на программное обеспечение, предложен общий алгоритм работы подсистемы защиты авторского права программного обеспечения, рассмотрена возможность использования криптографических алгоритмов шифрования для защиты вспомогательного модуля программного обеспечения, представлены достоинства и недостатки предлагаемой подсистемы защиты. На данный момент не существует абсолютной программной защиты ПО, которое невозможно было бы взломать, если не учитывать время, затраченное на исследование этой защиты. Однако наиболее эффективными средствами при создании подобного рода систем проверки лицензии являются использование криптографических алгоритмов и обфускация функций подсистемы защиты.

Литература

1. Виды лицензий на программное обеспечение // Information Technology Engineering Projects. [Электронный ресурс]. – Режим доступа: http://www.it-ep.ru/knowledge_base/software_licensing/type_of_software_license/

2. Серада С.А. Оценка эффективности систем защиты программного обеспечения // CITForum. [Электронный ресурс]. – Режим доступа: http://citforum.ru/security/software/sereda1/

3. Касперски К., Рокко Е. Искусство дизассемблирования. – СПб.: БХВ-Петербург, 2008. – 896 с.

4. Скляров Д. Искусство защиты и взлома информации. – СПб.: БХВ-Петербург, 2004. – 288 с.

5. Работа с библиотеками динамической компоновки (DLL) // Visual C++. [Электронный ресурс]. - Режим доступа: http://www.softzenware.com/visual/visual12.html

6. Каналы защищенной передачи данных //Энциклопедия теоретической и прикладной криптографии. [Электронный ресурс] - Режим доступа: http://cryptowiki.net/

7. Столлингс В. Криптография и защита сетей. - М.: Издательский дом "Вильямс", 2001 г., - 669 стр.

8. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. - М.: ДМК Пресс, 2002 г. – 655 стр.

Alla Chernyshova,Denis Kubashevskiy.The Copyright Protection Subsystem in the Software.
In this article, the authors analyzed the existing mechanisms for the copyright protection of software and suggested the description of software protection subsystem which uses cryptographic encryption algorithms.

Keywords:software license, additional module, software protection, symmetric encryption algorithms, asymmetric encryption algorithms

А.В. Чернишова, Д.В. Кубашевський.Підсистема захисту авторського права у програмному забезпеченні.*У даній роботі були проаналізовані наявні механізми захисту авторського права на програмне забезпечення та запропонований опис роботи програмної підсистеми захисту ПЗ із використанням криптографічних алгоритмів шифрування.*

Ключові слова: ліцензія на програмне забезпечення, додатковий модуль, захист ПО, симетричні алгоритми шифрування, асиметричні алгоритми шифрування

Статья поступила в редакцию 20.05.2016
Рекомендована к публикации д-ром техн. наук В.Н. Павлышом