Косинов Николай Николаевич

Магистрант НАЧОУ ВПО СГА

Направление: Информатика и вычислительная техника

Магистерская программа:

Распределенные автоматизированные системы

Использование сетей Петри для защиты программного обеспечения

Аннотация. В статье описана проблема использования нелицензированного программного обеспечения и способы решения данной проблемы в современных условиях компаниями – разработчиками программного обеспечения.

Кроме того приводится описание механизма сетей Петри в качестве одного из современных способов защиты программного обеспечения для защиты от незаконного копирования, распространения и использования.

Ключевые слова: нелицензионное программное обеспечение; Защита программного обеспечения; Способы защиты программного обеспечения; Компьютерное пиратство; Сети Петри.

Согласно исследованиям различных изданий, уровень пиратского программного обеспечения в России в 2013 г. составил 62%. Несмотря на то, что эта цифра каждый год снижается (в 2012 году она была 63%, а в 2004 – 87 %), для производителей коммерческого программного обеспечения это означает огромную недополученную прибыль.

Л.Н. Чевтаева выделяет 5 наиболее распространенных видов компьютерного пиратства:

1) незаконное копирование конечными пользователями;

2) незаконная установка программ на жесткие диски компьютеров;

3) изготовление подделок;

4) нарушение ограничений лицензии;

5) Интернет-пиратство [5, с. 284].

Многие крупные компании производители программного обеспечения предпочитают бороться с компьютерным пиратством организационными и юридическими мерами. Например, компания сделала заявление, что скорость закрытия нелегальных раздач ее программных продуктов на «торрент-трекерах» составила рекордные 26 секунд. Однако мониторинг торрент-трекеров и показательные судебные процессы – лишь часть большого комплекса мер по защите интеллектуальной собственности.

По мнению А.А. Салтан повсеместное развитие информационных технологий привело к тому, что уже сейчас рынок программных продуктов (ПП) вышел на одно из первых мест по приоритетности развития, прибыльности и скорости роста. В связи с этим необходимость принятия различного рода мер по сдерживанию теневого рынка ПП становится все более актуальной. Существуют весьма серьезные факторы, стимулирующие развитие компьютерного пиратства. Наряду с все еще отсутствующим общественным осуждением пиратства и низкой вероятностью оказаться выявленным нарушителем за использование и распространение нелицензионного программного обеспечения (ПО), весомой причиной является высокая стоимость легального ПО [3, с. 146].

При этом отличительной особенностью компьютерного пиратства тот же автор называет возможность легко копирования цифровых товаров без потери информации и качества [2, с. 9].

В большинстве случаев наиболее надежными и эффективными остаются технические способы защиты, но для успешного противостояния всем угрозам разработчики коммерческого программного обеспечения должны озаботиться вопросами информационной безопасности еще на старте разработки нового продукта. А вопросов здесь по большому счету два: как защитить свои ноу-хау и как противостоять нелегальному копированию?

На основании исследования Трегубовой М.В. по данным на октябрь 2013 г., число пользователей, покупающих легальный контент в Рунете составляет

всего 8 млн чел. Однако по данным Международной ассоциации правообладателей, в России уровень использования нелицензионного программного обеспечения прекратил снижаться. Основной причиной данного факта называют желание пользователей сэкономить и недооценка рисков, связанных с использованием нелегального программного обеспечения [4, с. 101 – 102].

В плане организации защиты программного обеспечения следует отметить также и то обстоятельство, что работа большинства программных продуктов не может быть проверена на практике во всех режимах их эксплуатации. Отсюда следует, что при тестировании и испытании программного обеспечения всегда остается незадействованной часть операторов, которая «соответствует непроверенным режимам функционирования ПО». Она может содержать не выявленные закладки в программном обеспечении.

К их числу относятся механизмы верификации, тестирования, анализа корректности результатов вычислений и контроля эффективности реализации защитных функций. Вопросы верификации, контроля безопасности кодов программ рассматривались в ряде теоретических и прикладных работ как отечественных научных коллективов, возглавляемых В.Б. Бетелиным, В.А. Васениным, П.Д. Зегждой, В.Н. Козловым, Б.П. Пальчуном, И.Б. Шубинским, Л.М. Ухлиновым, Р.М. Юсуповым, так и зарубежных ученых: А. Авизьениса, Г. Брандла, Дж.С. Лапри, Г.Д. Майерса, Э. Нельсона, Т. Тейера. В этих работах аспекты защиты программ от деструктивных воздействий рассматривались на стадиях их тестирования, автономных и комплексных испытаний. Вместе с тем, подходы, изложенные в этих работах, не позволяют в полной мере устранить угрозу поражения программного обеспечения средствами скрытого информационного воздействия на этапе его проектирования. Современные методы защиты программного обеспечения не дают высокой вероятности отсутствия возможности взлома ПО. Хакеры придумывают все новые и новые

способы взлома, распространяя взломанные версии по заниженным ценам, либо вообще бесплатно, нанося неоценимый ущерб компаниям-разработчикам.

Сети Петри – один из уникальных и современных методов построения системы защиты программного обеспечения от нелицензионного копирования и использования. Механизм их функционирования позволяет реализовать такую структуру переходов, что при использовании злоумышленников единственного способа взлома подобного механизма – полного перебора всех возможных вариантов переходов – он просто будет ходить по кругу, постоянно уходя от главного перехода к второстепенным. Помимо этого выделяют возможность гибкой реализации самомодифицирующейся системы защиты, которая сможет стать фактически несокрушимым препятствием на пути злоумышленников. Это, несомненно, будет существенным шагом в развитии защиты программных продуктов. На текущий момент времени подобных механизмов защиты не существует на практике, поэтому изучены они в основном в теории.

По мнению А.Н. Ивутина и И.А. Страхова сети Петри – это собирательный термин, который включает в себя большое количество системных моделей, методов анализа, графического представления и условных обозначений, основанных на конкретных предположениях о миру обработки информации [1, с. 135].

Сети Петри в своей основе содержат теорию мульти ориентированных графов. Каждая сеть содержит множество позиций, множество переходов, входной и выходной позиций. Каждый переход может быть осуществлен из одной вершины в другую в случае наличия между ними соединяющей дуги. Дуги указывают направление перехода из одной вершины в другие.

Сеть Петри определяется пятеркой, включающей в свой состав множество позиций; множество переходов; функцию следования; функцию предшествования; начальное маркирование (состояние) сети; множество положительных целых чисел.

Практическая значимость использования сетей Петри в компьютерном моделировании давно известна на примере реализации UML-моделей, используя их как гибкий инструмент моделирования переходов состояний системы.

Задача достижимости – основная задача, решаемая при анализе сетей Петри, к которой сводится множество других задач (в частности – задача активности). Задача достижимости формулируется следующим образом: для данной сети Петри с маркировкой m и маркировки m’ определить: m’ÎR(C,m). Задача активности и достижимости в общем случае не решены. Решение задачи достижимости в случае сетей Петри сводится только к методу полного перебора всех возможных переходов. В данном случае решение подобной задачи теоретически возможно, при применении мощных средств вычислительной техники и наличии некоторых временных запасов. Однако существуют методы повышения уровня сложности сетей Петри, начиная от увеличении количества вершин в сети и заканчивая построение «ложных» переходов, которые «уводят» злоумышленников от верного перехода. Практическая значимость данной задачи состоит в возможности создания структуры переходов в сети Петри, вызывающей зацикливание программ взлома и обеспечивающих надежную защиту программного обеспечения.

Для организации распределения возможных переходов каждая вершина маркируется некоторым количеством фишек. В зависимости от количества фишек на позициях переход может быть разрешен или запрещен. Таким образом, для прохождения сети необходимо знать порядок, по которому необходимо переходить на следующую позицию по переходу, чтобы не зайти в тупик. Поэтому при задании определенной начальной последовательности размещения фишек можно получить ключ для защиты программного обеспечения, сложность которого будет зависеть от сложности построенной сети.

В зависимости от сложности построения подобных сетей и реализации схемы переходов по ней и снижается вероятность взлома подобных механизмов

защиты. Единственным способом взлома системы защиты, основанной сети Петри является полный перебор всех переходов, который при большом количестве последних может быть просто невыполнимым.

Литература

1. Ивутин А.Н., Страхов И.А. Фреймворк для построения и исследования сетей Петри и их модификаций // Известия Тульского государственного университета. Технические науки. 2013. № 9-2.
2. Салтан А.А. Моделирование рынка программного обеспечения при наличии внешнего сетевого эффекта и компьютерного пиратства // Прикладная информатика. 2012. №2 (38).
3. Салтан А.А. Продуктовая стратегия компании-производителя программного обеспечения при наличии внешнего сетевого эффекта и компьютерного пиратства // Вестник СПбГУ. Серия 5. 2013. № 2.
4. Трегубова В.М., Оводкова Т.А., Мялкина А.Ф. Глобальная сеть в России: проблемы и перспективы // Социально-экономические явления и процессы. 2014. № 4 (062).
5. Чевтаева Л.Н. Интернет-пиратство: вчера и сегодня // Вестник СГТУ. 2013. № 4 (73).