Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Защита программного обеспечения от нелегального использования с помощью сетей Петри

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Кочаровского Ивана Александровича

Научный руководитель

доцент, к.ф.-м.н. _____ А.Н. Гамова

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

В связи с бурным развитием информационных технологий и выделением разработки коммерческого программного обеспечения в отдельную отрасль экономики на передний план вышла задача борьбы с нелегальным использованием программных продуктов. В рамках этой проблемы нарушители авторских прав в одних случаях продают и используют нелегальные копии программного обеспечения целиком, а в других – вырезают и нелегально используют отдельные части программного продукта, представляющие особую ценность.

По результатам исследований международной ассоциации BSA (Business Software Alliance), в среднем доля нелицензионного программного обеспечения на Российском рынке составляет 64% [1]. Другими словами, каждые шесть из десяти копий программы оказываются в каком-то смысле украденными у производителя и лишают его прибыли. Коммерческая стоимость нелицензионного программного обеспечения, установленного на российские компьютеры, составила в прошлом году $3,2 млрд. В России соотношение пользователей лицензионного программного обеспечения к тем, кто использует нелицензионные программные продукты постоянно или очень часто, составляет один к одному. Опрос BSA выявил, что 19% российских пользователей компьютеров стараются не пользоваться нелицензионным программным обеспечением из-за риска быть пойманными, тогда как 23% осознают незаконность использования нелегальных программных продуктов и поэтому приобретают легальные продукты.

С использованием нелегального программного обеспечения можно бороться различными способами. Основным, безусловно, является юридический. То есть, взлом и незаконное распространение программного обеспечения должны быть правильно описаны в соответствующих законах, и государство должно осуществлять преследование лиц, занимающихся созданием и распространением нелегального программного обеспечения, и

привлекать их к ответственности. Тем не менее, в России этот подход пока не принес ощутимых результатов.

Ещё одним эффективным методом борьбы с использованием нелегального программного обеспечения является экономический. Например, когда цена продукта настолько низка, что может сравниться с ценой взломанного продукта. В большинстве случаев, если цены будут приблизительно одинаковыми, покупатель предпочтёт лицензионный продукт. Однако экономическая конкуренция с нелицензионным программным обеспечением дело очень тяжелое и подходит далеко не всем производителям программного обеспечения. Такие производители обращаются к третьему методу – защите программного обеспечения от взлома и нелегального копирования, что выдвигает на первый план задачу создания эффективной системы защиты программного продукта.

Целью данной работы является разработка системы для защиты программного обеспечения от нелегального использования с помощью сетей Петри. Применение сетей Петри позволяет использовать многопоточное управление, что повышает надежность такой системы в несколько раз.

Исходя из поставленной цели, основными задачами являются:

1. изучить кодирование данных в сетях Петри;
2. разработать программу, позволяющую строить сеть Петри;
3. разработать программу, использующую сеть Петри для последующей защиты других программ;
4. разработать клиент-серверное приложение, с поддержкой криптографических алгоритмов, позволяющее безопасно обмениваться данными двум сторонам.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 6 приложений. Общий объем работы – 93 страницы, из них 45 страниц – основное содержание, включая 47 рисунков и список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе «Теория сетей Петри» приводятся основные понятия теории сетей Петри, описывается кодирование в сетях Петри и рассматривается наращивание сложности сетей Петри в соответствии с [2-5].

Во 2 разделе «Необходимые алгоритмы» описывается гибридная криптосистема согласно [6] и [7], шифр RSA в соответствии с [8] и [9], а также описывается шифр AES, основываясь на [10]. Данные шифры и описанная криптосистема используются в клиент-серверном приложении, которое позволяет безопасно обмениваться данными двум сторонам.

В 3 разделе дипломной работы «Программная реализация» описывается система, представляющая собой клиент-серверное приложение с поддержкой криптографических алгоритмов, позволяющее строить сеть Петри и использовать ее для защиты других приложений. Данная система состоит из пяти программ: программы создания сетей Петри, программы, устанавливающей защиту на выбранное приложение, программы, реализующей защиту с помощью сетей Петри, клиентской и серверной части клиент-серверного приложения. Программы написаны на языке C#, скомпилированы и протестированы в среде Visual Studio 2017. Для написания программ были использованы материалы из источников [11-20].

Программа построения сетей Петри позволяет создавать новые и редактировать уже созданные сети Петри. Программа, устанавливающая защиту на выбранное приложение, позволяет защитить выбранное приложение путем добавления в него защиты, на основе сетей Петри. Основной задачей программы, реализующей защиту на основе сетей Петри, является проверка указанной сети Петри. Клиентская и серверная части клиент-серверного приложения служат для безопасного обмена данными между клиентом и сервером соответственно.

В 4 разделе «Пример защиты программного продукта при помощи разработанной системы» рассматривается полный процесс защиты какого-либо программного продукта с использованием разработанной системы.

ЗАКЛЮЧЕНИЕ

Данная работа была посвящена разработке системы для защиты программного обеспечения от нелегального использования с помощью сетей Петри.

В качестве графа, управляющего логикой системы, используется сеть Петри. Следовательно, система защиты на основе сетей Петри имеет значительно более высокий уровень стойкости к атаке удаления или изменения данных из программного продукта, так как это приводит к повреждению графа, управляющего логикой системы и, как следствие, некорректной работе сети Петри.

Использование сетей Петри с приоритетами, повышает надежность защиты тем, что можно построить сеть таким образом, чтобы решающий переход имел наименьший приоритет у окружающих его переходов. А это значит, что один из окружающих переходов сработает раньше, не давая возможности, выполниться решающему переходу. Также очень сложно определить какой из переходов в сети Петри является решающим, так как при неправильной начальной маркировке решающий переход недостижим.

Не стоит забывать и о том, что каждый переход в сети Петри – это отдельный поток, а сама сеть Петри в процессе своего выполнения является динамическим графом. Следовательно, анализ кода программы, использующей несколько потоков, каждый из которых работает с динамическими данными, требует постоянного переключения потока и анализа, как исполняемого кода, так и области данных. На практике значительно проще анализировать программу, имеющую один поток и использующую только статичные данные.

В ходе работы было изучено кодирование данных в сетях Петри, и в итоге на языке программирования C# разработана и реализована система, представляющая собой клиент-серверное приложение с поддержкой криптографических алгоритмов, позволяющее строить сеть Петри и использовать её для защиты других приложений.

Таким образом, все поставленные задачи были полностью выполнены, а цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Исследование BSA: уровень использования нелицензионного ПО в России составляет 64%. [Электронный ресурс] // Business Software Alliance [Электронный ресурс] : [сайт]. URL: http://www.bsa.org/country/News%20and%20Events/News%20Archives/global/05252017-GSS.aspx (дата обращения: 10.12.2017). Загл. с экрана. Яз. рус.

2 Котов, В. Е. Сети Петри / В. Е. Котов. Москва : Наука, 1984. 160 с.

3 Питерсон, Дж. Теория сетей Петри и моделирование систем [Электронный ресурс] / Дж. Питерсон. // М. : Мир, 1984. 264 с. Загл. с экрана. Яз. рус.

4 Бабичев, С. Л. Применение сетей Петри для диагностирования проблем синхронизации в вычислительных системах с общей памятью [Электронный ресурс] / С. Л. Бабичев, К. А. Коньков, А. К. Коньков. М. : МФТИ, 2012. С. 81 – 88. Загл. с экрана. Яз. рус.

5 Шнайер, Б. Практическая криптография [Электронный ресурс] / Б. Шнайер, Н. Фергюсон. М. : Издательский дом «Вильямс», 2004. 432 с. Загл. с экрана. Яз. рус.

6 Молдовян, Н. А. Введение в криптосистемы с открытым ключом / Н. А. Молдовян, А. А. Молдовян. СПб. : БХВ-Петербург, 2005. 288 с.

7 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. М. : Триумф, 2003. 816 с.

8 Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс] : учеб. пособие / В. Н. Салий // Саратовский государственный университет имени Н. Г. Чернышевского [Электронный ресурс]. Саратов, 2017. 43 с. URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2017/10/18/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 09.11.2017). Загл. с экрана. Яз. рус.

9 Rivest, R. L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / R. L. Rivest, A. Shamir, L. Adleman [Электронный ресурс] // MIT CSAIL [Электронный ресурс] : MIT Computer Science and Artificial Intelligence Laboratory. 1977. URL: http://people.csail.mit.edu/rivest/Rsapaper.pdf (дата обращения: 12.11.2017). Загл. с экрана. Яз. англ.

10 Advanced Encryption Standart. [Электронный ресурс] // Computer Security Resource Center [Электронный ресурс] : Federal Information Processing Standards: Security standards. URL: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf (дата обращения: 13.11.2017). Загл. с экрана. Яз. англ.

11 Троелсен, Э. Язык программирования C# и платформа .NET 4.6 [Электронный ресурс] / Э. Троелсен, Ф. Джепикс. М. : Издательский дом «Вильямс», 2016. 1440 с. Загл. с экрана. Яз. рус.

12 Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире. [Электронный ресурс] / Б. Шнайер. СПб. : Питер, 2003. 368 с. Загл. с экрана. Яз. рус.

13 Федотов, И. Е. Модели параллельного программирования [Электронный ресурс] / И. Е. Федотов. М. : СОЛОН-ПРЕСС, 2012. 384 с. Загл. с экрана. Яз. рус.

14 Сетевое программирование в .NET Framework. [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/4as0wz7t(v=vs.110).aspx (дата обращения: 20.11.2017). Загл. с экрана. Яз. рус.

15 .NET Framework Cryptography Model. [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/0ss79b2x(v=vs.110).aspx (дата обращения: 20.11.2017). Загл. с экрана. Яз. рус.

16 Класс RSA. [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-

ru/library/system.security.cryptography.rsa(v=vs.110).aspx (дата обращения: 20.11.2017). Загл. с экрана. Яз. рус.

17 Класс AES. [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/system.security.cryptography.rsa(v=vs.110).aspx (дата обращения: 20.11.2017). Загл. с экрана. Яз. рус.

18 Класс Thread. [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/system.threading.thread(v=vs.110).aspx (дата обращения: 15.11.2017). Загл. с экрана. Яз. рус.

19 Класс Tcp Client. [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/system.net.sockets.tcpclient(v=vs.110).aspx (дата обращения: 20.11.2017). Загл. с экрана. Яз. рус.

20 Класс Socket. [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/system.net.sockets.socket(v=vs.110).aspx (дата обращения: 20.11.2017). Загл. с экрана. Яз. рус.