УДК 004.056.53

К.В. Сергієня[1]

[1]*Східноукраїнський національний університет імені Володимира Даля, Луганськ*

МЕТОДИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕСПЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ

В статті розглянуто проблему захисту програмного забезпечення від несанкціонованого копіювання. Узагальнено та сформовані основні методи та алгоритми захисту програмного забезпечення.
Ключові слова: захист, програмне забезпечення, методи, алгоритм, електронний ключ, криптографія

Вступ

На сьогоднішній час, активний розвиток інформаційних технологій і використання їх у різних областях людської діяльності привело до того, що крім задач передачі, збереження й обробки інформації виникла не менш, а в ряді випадків і більш важлива задача захисту інформації. Постали такі проблеми, як незаконне використання алгоритмів, що є інтелектуальною власністю автора, несанкціоноване використання, модифікація, поширення і збут програмних продуктів. Це обумовило необхідність використання відповідних систем захисту.

Захист комерційних версій програм звичайно зводиться до вбудовування фрагмента, що містить перевірку ключа, а для злому сучасних програм найчастіше використовують їхній динамічний аналіз і за допомогою різних наладчиків визначають місця перевірки ключа. Як правило, досить легко виявити місце звірення уведеного ключа з «правильним» значенням і, модифікувавши код захищеної програми, домогтися її працездатності. Найбільш відомі методи захисту змінюють або блокують роботу налагоджувальних засобів.

У відповідь на різні створювані засоби захисту хакери розробляють способи їхнього злому, тому необхідно постійно придумувати нові підходи для вдосконалення захисту.

Тому питання захисту від несанкціонованого копіювання є найважливішим напрямком у забезпеченні інформаційної безпеки.

Основна частина

Системи захисту програмного забезпечення (ПЗ) широко поширені і знаходяться в постійному розвитку, завдяки розширенню ринку ПЗ і телекомунікаційних технологій. Необхідність використання систем захисту ПЗ обумовлена списком проблем, серед яких слід виділити:

1. незаконне використання алгоритмів, що є інтелектуальною власністю автора, при написанні аналогів продукту (промислове шпигунство);
2. несанкціоноване використання ПЗ (крадіжка і копіювання);
3. несанкціонована модифікація ПЗ з метою впровадження програмних зловживань;

4. незаконне розповсюдження та збут ПЗ (піратство);
5. втрата прибутку від реалізації продукту.

Для більш наглядного представлення на рис. 1 показані графіки отримання прибутку від продажів незахищеного і захищеного продуктів.

Як видно з графіків, якщо продукт погано захищений, то його досить швидко «розкривають», і на ринку з'являється дешева піратська версія, яка не дозволяє ліцензійної версії завоювати свою частку ринку, і продажу легального продукту швидко падають. Якщо ж продукт добре захищений, то в піратів йде досить багато часу на розтин захисту і продукт встигає досягти необхідного рівня продажів і досить довго утримуватися на ринку.

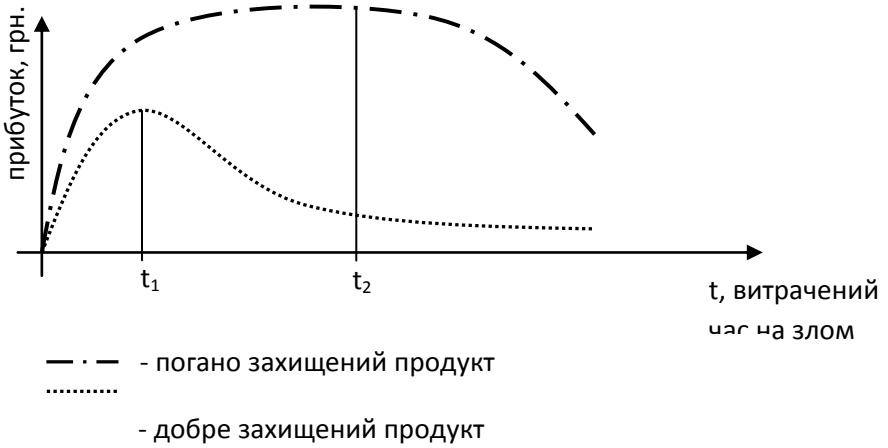

Рис.1. Приведена динамічна залежність прибутку від ступеня захищеності продукту

Для захисту ПЗ використовується ряд методів та алгоритмів. Всі методи захисту можна розділити на апаратні та програмні. До програмних відносяться методи, у яких не зачіпаються фізичні характеристики носіїв інформації, спеціальне обладнання і т.п. До апаратних відносяться методи, що використовують спеціальне обладнання (наприклад, електронні ключі, які підключаються до портів комп'ютера) або фізичні особливості носіїв інформації (компакт-дисків), щоб ідентифікувати оригінальну версію програми і захистити продукт від нелегального використання.

Розроблена значна кількість апаратних засобів різного призначення, проте найбільшого поширення отримують наступні:

1. спеціальні регістри для зберігання реквізитів захисту: паролів, ідентифікаційних кодів, або рівнів грифів секретності;
2. пристрої вимірювання індивідуальних характеристик людини (голосу, відбитків) з метою його ідентифікації;
3. схеми переривання передачі інформації в лінії зв'язку з метою періодичної перевірки адреси видачі даних;
4. пристрої для шифрування інформації (криптографічні методи).

Найбільше поширення одержали системи, засновані на використанні так званих апаратних (електронних) ключів. Дані ключі мають свої переваги та недоліки.

До переваг відносяться: значне утруднення нелегального розповсюдження і використання; звільнення виробника від розробки власної системи захисту; висока автоматизація процесу захисту; можливість легкого створення демо-версій та досить великий вибір таких систем на ринку.

А недоліками є утруднення розробки і налагодження з-за обмежень з боку систем захисту; додаткові витрати на придбання системи захисту та навчання персоналу; уповільнення продажів з-за необхідності фізичної передачі апаратної частини; підвищення системних вимог за захисту (сумісність, драйвери); зниження відмовостійкості; можливість несумісності систем захисту і системного або прикладного користувача; можливість несумісності захисту та апаратури користувача; загроза крадіжки апаратного ключа

Апаратні ключі захисту складаються з ключа (підключається до LPT або COM-порту) та програмного забезпечення.

Такі ключі виконані на мікросхемах FLASH-пам'яті, на PIC-котроллерах або на замовних ASIC-чіпах. Інформаційний обмін між ключем і комп'ютером відбувається, зазвичай, у послідовному вигляді, з використанням стробуючого сигналу, формованого драйвером.

Деякі ключі мають додаткові можливості: енергонезалежні таймери, енергонезалежність, можливість використання одного і того ж ключа для захисту декількох пакетів прикладного програмного забезпечення.

На даний час електронні ключі дуже легко зламувати, для цього достатньо зняти інформацію безпосередньо з роз'єму і роблять апаратні емулятори ключів, або визначити алгоритм обміну шляхом перехоплення звернень до регістрів управління COM і LPT-портами.

Основними методами захисту ПЗ, які спрямовані на протидію статичним способам зняття захисту від копіювання, є [1]:

- криптографічні;
- методи прив'язки до ідентифікатора;
- методи, засновані на роботі з переходами і стеком;
- маніпуляція з кодом програми.

По виду впливу на вихідну інформацію криптографічні методи поділяють на чотири групи: кодування (заміна смислових конструкцій вихідної інформації кодами); стенографія (дозволяють приховати не тільки сенс зберігається або переданої інформації, але й сам факт її зберігання або передачі); стиснення/розширення (зменшує обсяг вихідної інформації і не дозволяє її прочитати без спеціальних програм розширення) та шифрування/дешифрування.

Методи протидії динамічним способам зняття захисту ПЗ від копіювання включають [1]:

- незаконне використання алгоритмів, що є інтелектуальною власністю автора, при написанні аналогів продукту (промислове шпигунство);
- періодичний підрахунок контрольної суми, займаної чином завдання області оперативної пам'яті, у процесі виконання;
- перевірка кількості вільної пам'яті і порівняння з тим обсягом, до якого завдання звикла або привчена;
- перевірка вмісту векторів переривання на наявність тих значень, до яких завдання звикла;
- повторне встановлення векторів переривання (при цьому стеження за відомими векторами не дає бажаного результату);
- постійне чергування команд дозволу і заборони переривання, що ускладнює встановлення контрольних відладчиком точок;
- контроль часу виконання окремих частин програми, що дозволяє виявити «зупинки» в тілі виконуваного модуля.

В табл. 1 наведенні деякі алгоритми захисту ПЗ.

Таблиця 1

Найменування алгоритму	Характеристика
Алгоритми мутації	створюються таблиці відповідності операндів - синонімів і заміна їх один на одного при кожному запуску програми за певною схемою або випадковим чином, випадкові зміни структури програми.
Алгоритми заплутування	використовуються хаотичні переходи в різні частини коду, впровадження помилкових процедур - «пустушок», неодружені цикли, спотворення кількості реальних параметрів процедур ПЗ, розкид ділянок коду по різних областях ОЗП і т.п.
Алгоритми компресії даних	програма упаковується, а потім розпаковується по мірі виконання.
Алгоритми шифрування даних	програма шифрується, а потім розшифровується по мірі виконання.

Якщо система захисту розпізнає спробу злому, працездатність прикладної програми навмисно порушується. Це може проявлятися в неможливість запуску прикладної програми, так в її неправильне функціонування. В останньому випадку злом захищається програми стає ще важче, тому не зрозуміло, на якомусь етапі спрацював захист.

За час планування захисту ПЗ від несанкціонованого копіювання необхідно враховувати наступне обмеження: не втратить програма за час зняття її захисту своєї актуальності.

Висновки

Проведено аналіз існуючих рішень (методів та алгоритмів) в області захисту програмного забезпечення. Зроблено висновок, що існуючі методи захисту ПЗ мають потребу в удосконаленнях для ускладнення пошуку ключа, а також налагодження й дизасемблювання. Виявлено необхідність розробки універсального методу для захисту ПЗ від несанкціонованого копіювання.

Застосування тільки програмних засобів захисту не дозволяє забезпечити захищеність ПЗ на достатньому рівні, але в комплексі з апаратними методами дає можливість домогтися більш досконалого результату.

Література

1. Казарин О.В. Теория и практика защиты программ. – Москва, 2004. – 450 с.
2. Ховард М., Лебланк Д. Защищенный код/Пер. с англ. — 2_е изд., испр. — М.: Издательство «Русская Редакция», 2005. — 704 стр.: ил.
3. Герасименко В. А., Малюк А. А. Основы защиты информации.- М.: Инкомбук, 1997.
4. Michael Horward, David LeBlank. Writing secure code. 2nd ed. // Library of Congress Catalog-ing-in-Publication Data, pp. 92–104 (2003).
5. Tillman, Hope N.; Williams, Wilda W. Protecting Software. // Library Journal; 2/1/1991, Vol. 116 Issue 2, p. 110.

Надійшла до редколегії 05.05.2013 р.

Рецензент: д.т.н., проф. Петров А.С.

Сергиеня Е.В.

МЕТОДЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

В статье рассмотрены методы защиты программного обеспечения от несанкционированного копирования. Обобщены и сформированы основные методы и алгоритмы защиты программного обеспечения.

Ключевые слова: защита, программное обеспечение, методы, алгоритм, электронный ключ, криптография.

Sergienya E.V.

METHODS TO PROTECT THE SOFTWARE FROM UNAUTHORIZED COPYING

The article discusses methods to protect the software from unauthorized copying. Compiled and formed the main methods and algorithms for software protection.

Keywords: protect, software, methods, algorithm, electronic key, cryptography.