УДК 004.056

О. Р. Паламарчук

АЛГОРИТМ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ

Вінницький національний технічний університет;

Анотація

Розглянуто та проаналізовано поширені методи захисту вихідного коду від несанкціонованого копіювання, модифікації та дослідження. Запропоновано власний метод для підвищення рівня захищеності програмних продуктів від подібних атак. Виявлено переваги та недоліки запропонованого методу.

Ключові слова: кібербезпека, несанкціоноване копіювання, обфускація, шифрування.

Abstract

Common methods of protecting source code from unauthorized copying, modification and research are considered and analyzed. An own method has been proposed to increase the level of software protection from such attacks. The advantages and disadvantages of the proposed method are revealed.

Keywords: cybersecurity, unauthorized copying, obfuscation, encryption.

Вступ

Сьогодні значною проблемою у сфері кібербезпеки є несанкціоноване копіювання програми та її подальша модифікація, реверсивне дослідження алгоритмів роботи програми, пошуку вразливостей, тощо. Особливо важливим даний захист є в сфері комп'ютерних ігор, оскільки при достатньо високих затратах для повного циклу розробки і ризику низьких продаж готового продукту, несанкціоноване розповсюдження копій може призвести до значних фінансових втрат, а для невеликих студій, навіть банкрутства.

Метою роботи є покращення існуючих методів захисту вихідного коду програм від несанкціонованого копіювання, модифікації та дослідження.

Для досягення мети необхідно розв'язати такі задачі:

- проаналізувати існуючі методи для захисту програм від несанкціонованого копіювання, модифікації та дослідження;
- проаналізувати відомі засоби захисту програм від несанкціонованого копіювання, модифікації та дослідження;
- розробити власний комплексний метод захисту.

Результати дослідження

Для захисту вихідного коду чиста обфускація мало придатна, оскільки сучасні деобфускатори дозволяють усунути більшість модифікацій, що спричиняють обфускатори і привести код до читабельного вигляду [1].

Запропоновано метод покращення захисту вихідного коду від несанкціонованого копіювання, модифікації та дослідження за допомогою розбиття файлу з кодом на два різні файли. Перший файл буде містити зашифрований оригінальний код програми за допомогою унікальних параметрів системи [2], а другий файл буде скриптом, який буде здійснювати розшифрування. До скрипта потрібно буде застосувати методи обфускації для приховування алгоритму його роботи. Оскільки скрипт буде містити однаковий код для всіх випадків можна вручну обфускувати його команди для уникнення вразливостей автоматичних обфускаторів.

Алгоритм роботи методу:

1)програма інсталятор отримує унікальні парамаетри системи і відправляє їх на сервер;

2)сервер отримавши унікальні параметри перетворює їх певним чином в секретний ключ, шифрує на ньому фали програми і передає їх інсталятору;

3) інсталятор встановлює отримані файли, а при запуску програми розшифровує программу використовуючи як секретний ключ параметри програми.

Даний метод має такі переваги над відомими:

- вищий рівень захищеності від несанкціонованої модифікації та дослідження порівняно із стандартними методами обфускації, за рахунок використання унікального ідентифікатора в алгоритмі шифрування;

Серед недоліків можна виділити:

- збільшення часу виконання програми;
- обмеження кількості використання копій програми легітимним користувачем;
- небезпека розкриття вихідного коду програми за допомогою дампу пам'яті [3].

В підсумку можна сказати, що даний метод попри недоліки варто використовувати замість стандартних методів обфускації, оскільки при схожих недоліках він забезпечує більший рівень захищеності від модифікації та дослідження. У той же час використання прив'язки до пристрою робить метод також стійким до несанкціонованого копіювання.

Висновки

Встановлено, що запропонований підхід дозволяє підвищити загальний рівень захищеності програми від несанкціонованого копіювання, модифікації та дослідження порівняно з стандартними методами обфускації. Наведені результати аналізу переваг та недоліків запропонованого методу дозволили виділити множину задач, для яких його використання є доцільним.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Обзор существующих обфускаторов и их алгоритмов. Компьютерная и программная инженерия – 2015 год: – Донецк: ДонНТУ, 2015. с. 117-119.

2. Каплун В.А., Дудатьєв А.В., Семеренко В.П. Захист програмного забезпечення. Частина 1 : навчальний посібник / В.А. Каплун, А.В. Дудатьєв, В.П. Семеренко – Вінниця : ВНТУ, 2005. – 139 с.

3. Каплун В.А., Дмитришин О.В., Баришев Ю.В. Захист програмного забезпечення. Частина 2 : навчальний посібник / В.А Каплун, О.В. Дмитришин, Ю.В. Баришев – Вінниця : ВНТУ, 2014. – 105 с.

Паламарчук Олександр Русланович — студент групи 1БС-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Баришев Юрій Володимирович*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Palamarchuk Oleksandr R. — student of 1БС-18б group, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia,

Supervisor: ***Baryshev Yurii V.*** — PhD (Eng.), Associated professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia