УДК 004.832

Христофор Я. О.
Лужецький В. А.

МЕТОД ОБФУСКАЦІЇ КОДУ З ШИФРУВАННЯМ АДРЕС

Вінницький національний технічний університет

Анотація
Розроблено метод, що забезпечує обфускацію програмного коду застосунку типу .exe. Описано алгоритм його роботи.
Ключові слова: обфускація; зворотна інженерія; покажчик; вихідний код.

Abstract
A method for obfuscating the program code of a software application of .exe type are developed. The working algorithm if described.
Keywords: obfuscation; reverse engineering; pointer; source code.

Вступ

Забезпечення захисту програмного забезпечення після його розробки є постійною проблемою. В наш час переважна більшість комерційного програмного забезпечення поширюється у вигляді виконуваних файлів, а оскільки існує не лише програмне забезпечення з відкритим кодом (вільне), а й пропрієтарне (об’єкт інтелектуальної власності), то виникає необхідність в забезпеченні відповідного рівня захисту вихідного коду програми[1].

Після виконання обфускуючих процедур над вихідним кодом програмного застосунку його функціональність не зміниться, але будуть попереджені спроби зловмисника отримати несанкціонований доступ до вихідного коду програми.

Процедура обфускації не гарантує абсолютної безпеки вихідного коду застосунку, проте значно ускладнює процес зворотньої інженерії зловмиснику, велика частина таких зловмисників припинять дослідження коду програми після виявлення системи значних заплутувань коду.

Розробка методу

Запропонований метод захисту передбачає посилення обфускації за рахунок виконання [2]:

- представлення даних у вигляді покажчиків;
- використання шифрування покажчиків[3];
- заплутування коду програми шляхом об'єднання всіх явних покажчиків в один масив невизначених[4];
- зворотного перетворення невизначених покажчиків до явних.

Таким чином реалізується підхід, що полягає в застосуванні великої кількості простих прийомів заплутування, кожен з яких окремо легко розплутується, але в сукупності вони роблять завдання аналізу коду (особливо статичного аналізу) досить складним.

Реалізація запропонованого методу здійснюється в послідовному виконанні п'яти етапів:

- приведення всіх змінних критичного коду програми до покажчиків на дані (завдання не є складним, оскільки в мові високого рівня C/C++ існує операція взяття адреси змінної, яка може бути поміщена до відповідного збірного покажчика);
- опис всіх алгебраїчних або логічних виразів у вигляді функцій (в загальному випадку можна створити покажчик на ці функції, використовувати його також як і покажчики на дані, але без його шифрування);
- перетворення всіх явних покажчиків в невизначені покажчики і об'єднання їх в один масив (створюється масив невизначених покажчиків, розмір якого дорівнює кількості раніше створених раніше покажчиків на змінні);

– шифрування елементів масиву невизначених покажчиків за допомогою заздалегідь визначених глобальних констант (шифрування полягає в зміні значень адрес, які вказують на дійсне розташування значень змінної в пам'яті, за допомогою додавання їх з глобальними константами програми);
– використання шифрованих елементів масиву невизначених покажчиків і заздалегідь визначених статичних змінних глобальних констант для опису всіх алгебраїчних або логічних виразів критичного коду (процес розшифрування покажчиків проводиться безпосередньо при використанні цих покажчиків в якості параметрів функцій, коли оператор функції звертається до обфускованої ділянки критичного коду програми).

На рисунку 1 показана загальна схема описаного методу обфускації стосовно до одного оператора критичного коду програми.

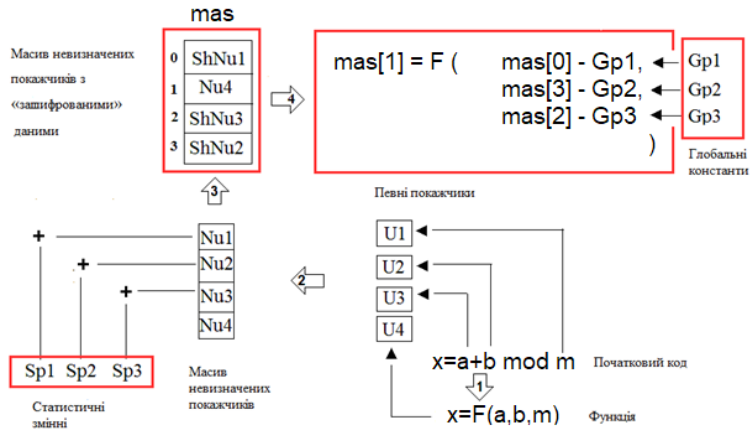

Рисунок 1 – Схема обфускації для ділянки коду

Таким чином цей метод посилює ефект заплутування за рахунок спільного застосування описаних і окремо використовуваних способів: шифрування покажчиків, об'єднання їх в один масив та їх розшифрування в момент виклику функції, що визначає значення виразів коду програми, які необхідно обфускувати.

Висновки

Аналіз відомих методів та засобів обфускації програмного коду показав, що найбільш перспективним є метод модифікації графу потоку керування застосунку з додатковим шифруванням строк коду.

Була досліджена структура розміщення виконуваного файлу в оперативній пам’яті, визначено її сторінкове розміщення, що використано для розробки методу обфускації.

Розроблений метод підвищує рівень захищеності комерційного програмного забезпечення, а його використання не вимагає значного рівня знань та є простим у використанні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. C. Thomborson Manufacturing opaque predicates in distributed systems for code obfuscation / C. Thomborson, D. Majumdar. – M. : Volume 48. Australian Computer Society, Inc., 2006, с. 187–196.
3. Касперски К. Образ мышления – дизассемблер IDA Pro / Касперски К. – Д. : — М.СОЛОН_Р,2010.
4. Чернов А. В. Анализ запутывающих преобразований программ / Чернов А. В. – Д. : Института Системного программирования РАН-2009 , – Труды Института Современного Программирования РАН-2009

Христофор Ярослав Олегович — студент групи 1БС-19м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yaroslav833@gmail.com

Лужецький Володимир Андрійович — доктор технічних наук, професор, завідувач кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: luzhetskyi@conferences.vntu.edu.ua

Khrystofor Yaroslav O.— Student of 1BS-19m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: yaroslav833@gmail.com

Luzhetsky Volodymyr A. — Doctor of Technical Sciences, Professor, Head of the Information Security department, Vinnytsia National Technical University, Vinnytsia, e-mail: luzhetskyi@conferences.vntu.edu.ua