УДК 004.056.53

ГУРІН Сергій
КАПЛУН Валентина

ЗАХИСТ ПРОГРАМНОГО КОДУ З ВИКОРИСТАННЯМ АЛЬТЕРНАТИВНИХ ПОТОКІВ NTFS

Вінницький національний технічний університет

Анотація. *В даній статті досліджено можливість використання альтернативних потоків файлової системи NTFS для захисту програмного забезпечення. Дані, записані в альтернативний потік прихованого файлу використовуються захищеною програмою для проходження авторизації і подальшого запуску програми у випадку співпадіння критичної інформації, доступ до якої і вміст якої доступний тільки легальному користувачу.*

Ключові слова: *захист програмного застосунку, альтернативні потоки NTFS.*

Abstract. *This article examines the possibility of using alternative streams of the NTFS file system for software protection. The data recorded in the alternative stream of the hidden file is used by the protected program to pass authorization and subsequently launch the program in case of coincidence of critical information, access to which and the content of which is available only to a legal user.*

Keywords: *application protection, alternative NTFS threads.*

Вступ

Захист програмного забезпечення є однією зі складових загальної системи захисту ресурсів комп'ютера, оскільки програмний засіб може бути комерційним і містити в собі деяку критичну інформацію: специфічні алгоритми, конфіденційну інформацію тощо.

В даній роботі для захисту програмного забезпечення він несанкціонованого копіювання і використання застосовано альтернативні потоки. Використання альтернативних потоків NTFS для захисту додатків означає можливість зберігати деякі дані, необхідні для повноцінної роботи програми, у додатковому потоці захищуваного файлу, але так, щоб наявність їх була не очевидною. Така можливість може бути використана для підвищення безпеки додатків шляхом приховування конфіденційної інформації у файлі, що робить його менш вразливим до несанкціонованого доступу або підробки.

Метою даної роботи є покращення захищеності програмних засобів шляхом розробки застосунку для прив'язки до даних, що знаходяться в альтернативному потоці, та реалізації механізму перевірки.

Результати дослідження

Існує кілька способів захисту програм, які можна реалізувати за допомогою альтернативних потоків даних NTFS (ADS). Деякі з них включають:

- приховування конфіденційних даних: зберігаючи конфіденційні дані в альтернативному потоці, зловмиснику стає набагато складніше знайти їх і отримати доступ до них. Це може допомогти захистити від несанкціонованого доступу, неправильного використання або зміни конфіденційних даних;
- впровадження додаткового рівня безпеки до існуючих додатків: додавши альтернативний потік даних до файлу, компанії можуть додати додатковий рівень захисту без необхідності модифікувати саму програму. Це може допомогти підвищити безпеку існуючих додатків без значних змін в основному коді;
- захист від шкідливих програм і програм-вимагачів. Багато шкідливих програм і програм-вимагачів не призначені для виявлення або обробки альтернативних потоків даних, що робить їх використання ефективним методом захисту від цих типів загроз;
- захист даних без шифрування. Використовуючи ADS, компанії можуть захистити конфіденційну інформацію без необхідності шифрувати весь файл, що зменшує обчислювальну

потужність, необхідну для шифрування та розшифрування даних, і забезпечує швидший доступ до інформації;

- нанесення водяних знаків на файли. Додавши до файлу унікальний альтернативний потік даних, компанії можуть створити водяний знак, який надалі використовувати для ідентифікації файлу як оригіналу, а не копії.

Ідея запропонованого захисту базується саме на тому, що альтернативні потоки не можуть бути виявлені штатними засобами для роботи з системою, такими як, наприклад, вбудований файловий провідник в операційній системі Windows. Кожен потік закріплюється за будь-яким файлом, та може містити в собі певні дані, а отже, мати деякий розмір. Однак, при перегляді властивостей файлу за допомогою стандартного провідника, система ніяким чином не відображає їх наявності, що робить використання альтернативних потоків чудовим способом зберігання важливої інформації.

Даний захист від несанкціонованого доступу до програмного забезпечення (ПЗ) реалізовано в програмному засобі мовою програмування C++, яка надає більш низькорівневі можливості при розробці. Алгоритм передбачає використання «ліцензійного ключа» або буд-якого іншого набору даних.

Сутність розробленого захисту полягає в наступному: після введення користувачем даних, за певним визначеним шляхом буде створено файл з альтернативним потоком, всередину якого буде записано введену інформацію, яку в подальшому буде використано для авторизації програмного застосунку. Для посилення захисту в потік записується не символьне значення ліцензійного ключа, а байтові значення кожного з його символів. Це зроблено для того, щоб навіть при знаходженні шляху (а це можна виявити за допомогою файлових моніторів), за яким збережено файл та спробі читання даних з альтернативного потоку, справжнє значення ключа не буде розкрито, а при спробі внесення інформації з потоку в поле діалогового вікна верифікації, перевірку не буде пройдено і програму не буде запущено. Сам файл залишається пустим і не містить ніякої інформації.

Алгоритм роботи застосунку такий (рис. 1). При запуску захищуваної програми користувач повинен ввести шлях та ім’я файлу, в якому буде збережено файл з альтернативним потоком, а також інформацію, що буде записано в даний NTFS потік і яку надалі буде використано для авторизації в програмі (рис. 2). Далі введену інформацію буде зчитано та здійснено перетворення символів у їх байтові значення. Після цього завантажується створений файл, розташований за шляхом, вказаним користувачем та зчитуються байтові значення з альтернативного потоку. В результаті отримано два рядка даних, відносно яких здійснюється перевірка. Якщо їх значення співпадають, буде виведено повідомлення про успішне проходження перевірки та виконання основі частини програми (рис. 3,а). У випадку,

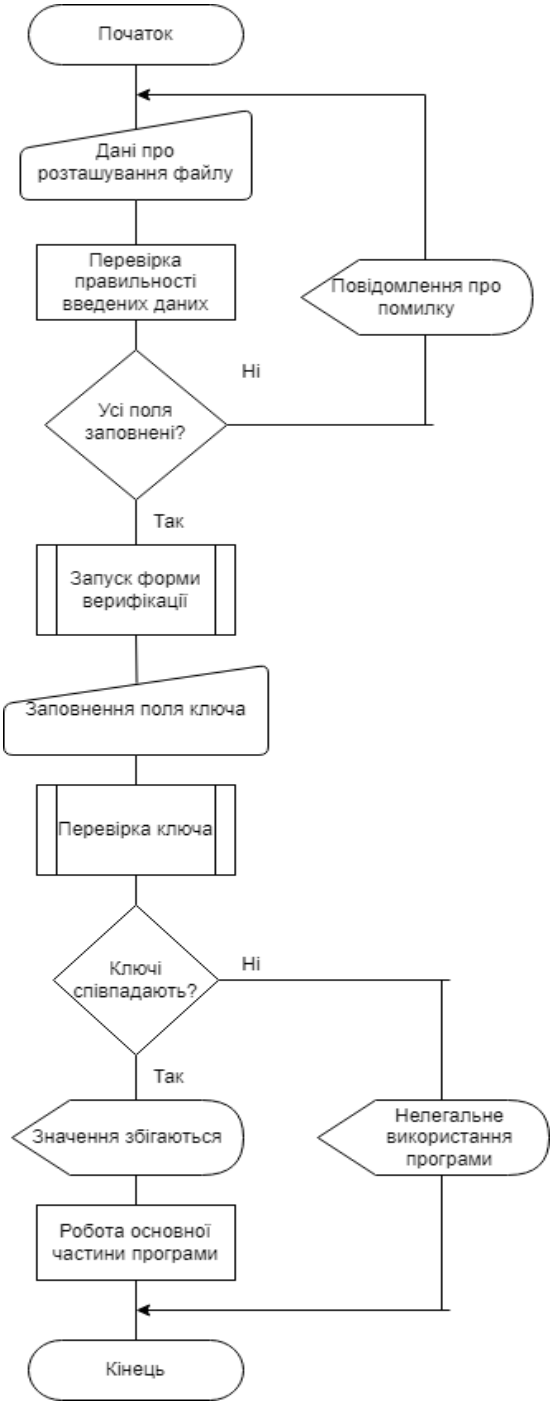

Рисунок 1 – Алгоритм захисту ПЗ

якщо перевірку не пройдено, з’явиться повідомлення про невдале проходження перевірки і виконня програми не відбудеться (рис. 3,б).

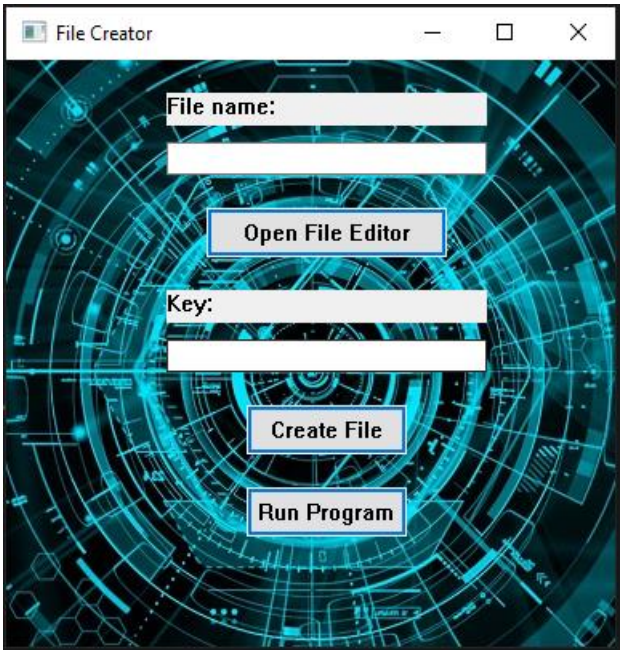

Рисунок 2 – Вигляд головного вікна програми

а)

б)

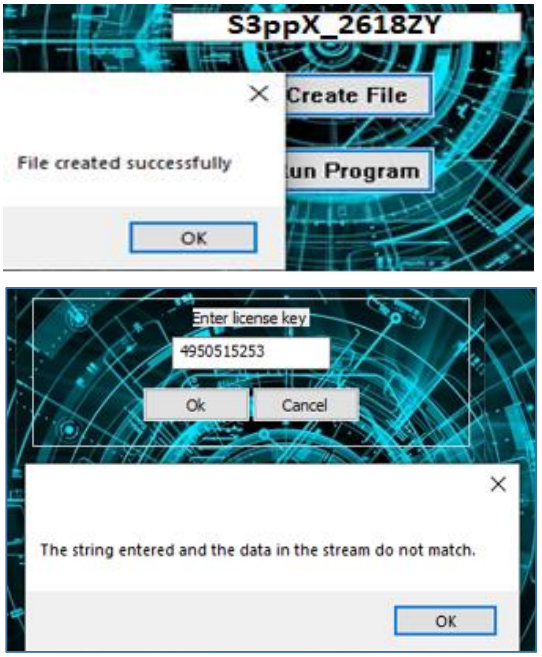

Рисунок 3 – Вигляд повідомлень при правильному (а) і неправильному (б) проходженні процесу веріфікації

Тестування розробки довело коректність роботи програмного застосунку і правильність роботи захисту програмного застосунку за допомогою приховування інформації в альтернативному потоці NTFS.

Висновки

Даний підхід дозволяє зберігати ліцензійний ключ у прихованому місці серед інших файлів комп'ютера, але при цьому дозволяє програмі отримати доступ до ключа і, за необхідності, перевірити його. Даний метод захисту ПЗ шляхом запису ліцензійного ключа в байтовому представленні в альтернативний потік є ефективним і безпечним засобом захисту програмного застосунку. Розроблений метод захисту може бути ефективним для запобігання несанкціонованому використанню програмного інструменту, оскільки він ускладнює доступ третьої сторони до ліцензійного ключа та використання програмного забезпечення без дозволу. Крім того, використання байтового представлення ліцензійного ключа надає додатковий рівень безпеки, ускладнюючи зламникам підробку даних ліцензійного ключа.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Келлі Девід А. Захист програмного забезпечення: чому це важливо та як це зробити: IEEE Software, том. 34, вип. 5, С. 78-81, 2017.
2. Руссинович М., Соломон Д. Р89 Внутреннее устройство Microsoft Windows. 6-е изд. СПб.: Питер, 2013. 800 с.
3. Alternate Data Stream. [Електронний ресурс] : URL : https://www.sciencedirect.com/topics/computer-science/alternate-data-stream.

ГУРІН Сергій – студент групи 1БС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: misterhurin@gmail.com.
КАПЛУН Валентина, ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, valuka8379@gmail.com.

HURIN S. - student of group 1BS-20b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.
KAPLUN V. – Lecturer of the Chair of Safety of Infomation and Communication Systems, NTU, Vinnytsia.