АПАРАТНІ МЕТОДИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО ВИКОРИСТАННЯ

Дюжаєв Л. П., к.т.н, доц., Максимець Д. В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ, Україна

Захист програмного забезпечення (ПЗ) від несанкціонованого використання є важливим кроком для регулювання використання та розповсюдження програмного продукту. Головним методом захисту ПЗ є його ліцензування, яке використовується з метою врегулювання використання комерційного ПЗ. Ліцензування відноситься до інструментів захисту ПЗ з програмною реалізацією. Поряд з програмними методами захисту (ліцензуванням) можуть використовуватись апаратні ключі (донгли). Метою даної статті є наведення особливостей використання апаратних ключів для захисту ПЗ.

Апаратний ключ (електронний ключ, іноді донгл) — апаратний засіб, призначений для захисту програмного забезпечення і даних від копіювання, нелегального використання та несанкціонованого розповсюдження. Як правило, апаратний ключ будується на спеціалізованій мікросхемі, або на захищеному від зчитування мікроконтролері. Сучасні апаратні ключі виконують у вигляді малогабаритного змінного USB носія, що має пластиковий або металевий корпус. Як правило, донгл виконується на двошаровій платі, яка заливається компаундом [1]. Поряд з електронним ключем користувачу поставляється інсталяційний пакет. Він виконує роль посередника з метою активації програмного продукту.

Принцип роботи електронного ключа. Технологія захисту від несанкціонованого використання базується на взаємодії виконуючого файлу програми з електронним ключем. Взаємодія може включати в себе наступні етапи [2]:

– перевірка підключення ключа;

– зчитування необхідних програмних даних з ключа в якості параметрів запуску програми;

– запит на розшифрування даних чи виконуючого коду, необхідних для роботи програми, які були зашифровані при захисті програми;

– запит на розшифрування даних, зашифрованих самою програмою (дозволяє відправляти кожного разу різні запити до ключа, і тим самим, захиститися від емуляції самого ключа);

– перевірка цілісності програмного коду шляхом порівняння його поточної контрольної суми з оригінальною контрольною сумою, що зчитується з ключа (це також допомагає захиститися від емуляції ключа);

– запит до вбудованого годинника реального часу (при його наявності

може здійснюватися автоматично при обмеженні часу роботи апаратних алгоритмів ключа по його внутрішньому таймера).

Потрібно відмітити, що електронний ключ може також використовуватися з метою захисту алгоритму, що використовується в програмі, від копіювання та несанкціонованого використання. Це здійснюється шляхом зберігання алгоритму або частини програмного коду на електронному ключі.

Алгоритм перетворення (криптографічний чи інший) є основою роботи апаратного ключа. У більшості сучасних ключів алгоритм реалізується апаратно. Це майже повністю виключає створення повного емулятора ключа, оскільки ключ шифрування ніколи не передається на вихід донгла, що унеможливлює перехоплення ключа шифрування.

Іншим способом реалізації алгоритму шифрування є програмна реалізація та генерація електронного ключа, що буде використовуватися виконуючою програмою. Останній спосіб можливо реалізувати з використанням звичайного USB накопичувача [3,4].

На даний час представлено велику кількість апаратних ключів, серед який можна відзначити «Кристал-1», «Алмаз-1К» та «Кристал-1Д» [5]. Наведені донгли різняться між собою призначенням, конструкцією та технічними характеристики. Розглянемо більш детально апаратний ключ «Кристал-1», який показано на рис. 1.

Рис. 1. Апаратний ключ «Кристал-1»

Одним з найбільш поширених застосувань апаратного ключа «Кристал-1» є генерація відкритого та закритого ключів для алгоритмів програми чи протоколу розподілу ключів. «Кристал-1» виконано у вигляді малогабаритного змінного USB-пристрою, який може мати програмний CCID інтерфейс та електронний flash-диск [5]. Електронний ключ «Кристал-1» реалізує ряд криптографічний стандартів та протоколів [5]:

– шифрування за ДСТУ ГОСТ 28127:2009 (режим простої заміни та режим вироблення імітовставки);

– протоколи довжини електронних ключів за ДСТУ 4145-2002;

– протоколи розподілу ключових даних Діффі-Геллмана.

Слід зазначити, що в даному випадку протокол Діффі-Геллмана використовується як спосіб обміну ключів шифрування та дешифрування. Цей протокол дозволяє отримати загальний секретний ключ, який в подальшому використовується для шифрування даних, якими обмінюються, за допомогою симетричних алгоритмів шифрування.

Злом апаратного ключа. Злом апаратного ключа може здійснюватися шляхом повної або часткової емуляції ключа. Емулятор аналізує взаємодію

програмного модуля з апаратним ключем. Злом програмного модуля здійснюється з метою виділити блок захисту і деактивувати його. Програмний модуль може бути дизасемблений, тобто перетворений в лістинг програмного коду на мові Асемблеру. В результаті можна отримати алгоритм роботи програми. Іншим методом злому програмного модулю є його декомпіляція — отримання коду програми на мові високого рівня.

Області застосування. Електронний ключ зазвичай застосовується з ПЗ високої вартості. До такого ПЗ можна віднести CAD/CAM системи, системи туризму та торгівлі, системи для редагування відео та аудіо промислових масштабів, аудіо консолі та інше.

Перелік посилань

1. Електронний ключ [Електронний ресурс] — Режим доступу до статті: https://uk.wikipedia.org/wiki/Електронний_ключ — Назва з екрану.

2. Электронный ключ [Електронний ресурс] — Режим доступу до статті: https://ru.wikipedia.org/wiki/Электронный_ключ — Назва з екрану.

3. AntiDuplicate drive [Електронний ресурс] — Режим доступу до статті: https://www.atdisk.com/antiduplicate/index.html — Назва з екрану.

4. Create USB dongle from any regular USB Flash Drive [Електронний ресурс] — Режим доступу до статті: http://usbsoftprotect.com/create-usb-dongle-from-usb-flash-drive — Назва з екрану.

5. Комплекси та засоби захисту інформації [Електронний ресурс] — Режим доступу до статті: https://iit.com.ua//index.php?page=getcontent&p=3 — Назва з екрану.

Анотація

Розглянуто особливості роботи та реалізації апаратного ключа як методу захисту програмного забезпечення від несанкціонованого використання. Наведено приклад одного з існуючих апаратних ключів та його характеристики.

Ключові слова: апаратний ключ, електронний ключ, донгл, ліцензування програмного забезпечення.

Аннотация

Рассмотрено особенности работы и реализации аппаратного ключа как метода защиты программного обеспечения от несанкционированного использования. Приведен пример существующего аппаратного ключа и его характеристики.

Ключевые слова: аппаратный ключ, электронный ключ, донгл, лицензирование программного обеспечения.

Abstract

Features of inner implementation and usage of software licensing dongle are described in the article. Software licensing dongle example with its characteristics are presented.

Keywords: dongle, software protection dongle, software licensing protection.