**Практична робота №2**

**ЗАХИСТ ПРОГРАМ ВІД КОПІЮВАННЯ ШЛЯХОМ ПРИВ’ЯЗКИ ДО ФІЗИЧНИХ ПАРАМЕТРІВ**

**Мета і задачі**

* Ознайомитись з основними поняттями ОС, необхідними для створення захисту програмного забезпечення від несанкціонованого копіювання.
* Ознайомитись з методами отримання параметрів комп’ютерної системи.
* Ознайомитись з основними методами захисту програмного за безпе-чення за допомогою прив’язки до носіїв для запобігання копіюванню.
* Дослідити існуючі програми захисту від копіювання.

**КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ**

**Способи захисту від несанкціонованого копіювання**

Захист програмного продукту від несанкціонованого копіювання – актуальна задача у зв'язку зі збереженням комерційних і авторських прав фірм і розробників. Термін "захист від копіювання" досить умовний, оскільки практично завжди можна переписати інформацію, що знахо-диться на дискеті або диску. Інша справа, що після цього програма може не виконуватися. Таким чином, без санкції розробника чи фірми-розповсюджувача неможливо одержати працездатний програмний продукт. Тобто, "захист від копіювання" – це створення засобів, що здійснюють можливість "захисту від несанкціонованого виконання".

Системи захисту від несанкціонованого копіювання можна розділити на такі групи:

* прив’язка до дистрибутивного носія (диску, CD або DVD-диску);
* прив’язка до комп’ютера (до архітектури, технічних характеристик або штатного програмного забезпечення);
* прив’язка до ключа (ЕК або SecretKey);
* обмеження на використання ПЗ.

Перші три групи методів захисту від копіювання пов’язані з роботою з дисками на фізичному рівні, а для цього необхідно добре знати будову дисків та можливості керування ними.

Однією з розповсюджених технологій захисту від НСК є створення особливо обумовлених носіїв. Їх особливість полягає в тому, що на носії створюється спеціально організована мітка, яка використовується як ознака її дистрибутивності. Функцію контролю мітки виконує спеціальна частина програми, що захищається. Після копіювання засобами OС диска, що захищається, буде скопійована вся інформація, за винятком мітки. Під час виконання програми її контролююча частина (КЧП) встановить, що диск не дистрибутивний, і припинить виконання програми. Тим самим програма ніби "прив'язується" до свого носія.

**Методи отримання повної інформації про комп’ютерну систему**

Існує декілька методів для отримання необхідної інформації про апаратну частину системи, яка нас цікавить.

По-перше, це опосередковане звертнення до BIOS, через переривання BIOS та DOS.

По-друге – можна звернутись безпосередньо до розділу пам’яті BIOS (копія таблиці параметрів в пам’яті) за його абсолютною адресою.

Можна використати бібліотеки функцій мови програмування високого рівня або самої операційної системи Windows (табл. 1).

Таблиця 1 – Способи отримання інформації про комп’ютер

|  |  |  |
| --- | --- | --- |
| Опис метода | Переваги | Недоліки |
| Опосередковане звертання до BIOS, через переривання | Можливість отримання пов-ного спектру необхідної інформації  Висока швидкодія  Зручність у використанні | Необхідність створення коду програми на мові низького рівня  Існуючі недоліки переривань |
| Отримання інформації з пам’яті BIOS, за його абсолютною адресою | Найбільша швидкодія | В пам’яті BIOS знаходяться лише деякі основні дані.  Незручність у використанні |
| Використання бібліотеки функцій мови програмування високого рівня | Дуже зручне у використанні. | Найменша швидкодія  Функції високого рівня мають ряд власних дефектів |
| Використання бібліотеки функцій операційної системи Windows | Дуже зручне у використанні. Висока швидкодія. Висока точність. | Необхідна наявність документації для цих функцій |

Оскільки для захисного програмного забезпечення одним з критичних ресурсів є час, то оптимальним буде використання комбінації двох перших найшвидших методів.

Серед програмних бібліотек є бібліотеа, яка містить заголовочний файл *wmi.hpp,* у якому описано структури для роботи з запитами *wmi,* що містить величезну кількість полів. За допомогою цих функцій можна отримати багато різноманітної інформації про комп’ютерну систему, щод надалі здійснити прив’язку до них, як до унікальних параметрів (табл. 2).

Таблиця 2 – Інформація, використовувана для "прив’язок"

|  |  |  |
| --- | --- | --- |
| Розділ | Інформація | |
| Тип комп'ютера | 1. Ідентифікатор машини. | 2. Додатковий код моделі |
| Процесор | Тип і модель процесора  Тактова частота процесора  Сімейство процесора | Тип співпроцесора  Фірма-виготовлювач процесора  Сигнатура процесора і т.д. |
| BIOS | Модель BIOS. Дата BIOS | BIOS |
| Відеоадаптер | Тип, назва моделі відеоадаптера. | Обсяг відеопам'яті |
| Диски | Кількість FDD HDD дисків  Виготовлювач HDD  Модель HDD  Серійний номер HDD | Контрольний номер HDD  Кількість голівок циліндрів HDD  Розмітка HDD |
| Пам'ять | Розмір основної пам'яті  Розмір вільної основної пам'яті  Адреса керуючої програми драйвера XMS | Розмір пам'яті XMS  Розмір вільної пам'яті XMS  Розмір пам'яті EMS  Розмір вільної пам'яті EMS |
| CD ROM | Кількість пристроїв. Номера пристроїв CD-ROM (букви дисків)  Версія драйвера MSCDEX | |
| Інше | Кількість портів Наявність ігрового порту і підключеного пристрою  Тип звукової карти | Тип клавіатури / кількість клавіш  Тип миші / кількість клавіш  Версія драйвера миші  Тип операційної системи |

**Контрольні питання**

1. Навести характеристику сучасних технологій захисту програмного за безпечення від копіювання.

2. Охарактеризувати рівні роботи з дисковою системою комп’ютерів.

3. Навести перелік методів захисту від НСК шляхом прив’язки до дистрибутивного носія.

4. Що означає поняття нестандартного форматування і яким чином воно використовується для захисту від НСК? Навести приклади.

5. Що означає метод, що базується на опитуванні довідника? Що таке електронні ключі, які типи елекронних ключів?

6. Що таке ключі ідентифікації, який принцип захисту вон використовують і чим відрізняються від електронних ключів?

7. Знайти в інтернеті програмні продукти, використовувані для захисту від копіювання. Навести їх можливості, способи захисту, використовувані методи.

**Порядок виконання роботи**

1. Запустити програму test\_wmi.ехе. Проаналізувати основні параметри вашого комп’ютера. Ознайомитись з кодом програми з папки wmi. Дослідити можливості використання namespace Wmi. У звіт: характеристики Вашого комп’ютера; програмні засобі для отримання інформації; висновки і пропозиції щодо можливості використання отриманої інформації при захисті.

2. В проекті wmi модифікувати програму таким чином щоб отримати інформацію про характеристики жорсткого диску, flesh-носіїв, CD-дисководу (за наявності).

У звіт: характеристики переглянутих дисків і їх порівняння (таблиця); програмні засоби для отримання інформації про дискову систему.

3. Дослідити роботу і код програм Crack05 i Crack09. Дослідити їх можливості, спосіб захисту. У звіт: охарактеризувати спосіб захисту, програмні засоби для роботи з реєстром.

У звіт: охарактеризувати спосіб захисту, програмні засоби для роботи з реєстром.

4. Звіт з виконання цієї частини лабораторної роботи можна оформити, звівши всю досліджену інформацію у таблицю за такою формою.

|  |  |  |
| --- | --- | --- |
| Функція | Параметри і їх значення | Призначення функції |
|  |  |  |

5. Встановити на комп’ютері програму Orien. Дослідити її інтерфейс та можливості захисту за її допомогою. Взяти будь-яку виконувану програму (можна використати програму, розроблену під час курсового проектування) і захистити її різними способами за допомогою програми Orien. Впевнитись в тому, що програму справді захищено від копіювання, запустивши її на іншому комп’ютері. У звіт: призначення, можливості і варіанти захисту; назва програми об’єкту, призначення, результати виконання без захисту; вид захисту (використати 4 різних захисти), розмір після захисту, результати виконання на "рідному" комп’ютері, результати виконання на "чужому комп’ютері.

6. Навести відомості про програми, використовувані для захисту від несанкціонованого використання. У звіт: назва програми, виробник, вартість, призначення, режими роботи, методи захисту.