

МЕТОДИ АНТИВІДЛАДЖУВАЛЬНОГО ПРОГРАМУВАННЯ

Для створення і розповсюдження конкурентоздатного програмного продукту потрібні чималі фінансові витрати: на розробку, його підтримку і, якщо передбачено, на подальший розвиток. Для окупності витрат зазвичай користувачу надається тимчасово безкоштовна версія продукту, після закінчення якої користувач зобов'язан внести плату за подальше користування. Деякі несвідомі користувачі замість придбання продукту намагаються його несанкціоновано запустити, що ставить під загрозу окупність програмного продукту.

При розробці програмного забезпечення впроваджуються засоби протидії несанкціонованому запуску, такі як: перевірка ключа активації, серійного номеру та інші. Однак ці засоби можуть бути деактивовані через модифікацію програмного коду, який, попередньо, досліджено відладжувачем.

Відповідно, метою впровадження антивідлагоджувальних методів в програмний код є унеможливлення або підвищення складності проведення відлагоджувачем аналізу виконуваного коду і ускладнення відтворення вихідного коду програмного продукту.

Існує дві популярні стратегії протидії відлагоджуванню: впровадження заборони запуску відлагоджувача або виявлення роботи відлагоджувача і подальше переривання нормальної роботи програми.

Заборона запуску базується на блокуванні "відлагоджувальних" переривань процесора (int 1, int 3), що унеможливорює взагалі запуск відлагоджувача. В програму слід впровадити власні обробники відлагоджувальних переривань, адреси яких при запуску повинні бути записані в таблицю векторів переривань процесора. Такі «самописні» обробники переривань можуть складатися з однієї команди – власне ігнорувати команди переривання. Слід врахувати, що можлива ситуація коли зломщик виявить частину коду, що відповідає за запис адреси оброблювачів в таблицю переривань, видалить її, та, відповідно, захист буде деактивовано. Отже, таку частину коду слід уважно шифрувати.

Виявлення роботи відлагоджувача має більш розвинені варіанти розвитку. Одним з таких варіантів є відстежування клавіатури. В процесі трасування програми (при її покроковому виконанні) зломщику необхідно натискати на клавіші для переходу до чергової команди, відповідно, якщо

прибрати реакцію комп'ютера на натискання клавіш - налагодження програми буде зірвано. На початку роботи програми виконується спеціальна команда «CLI», що встановлює прапор ігнорування всіх переривань від зовнішніх пристроїв. У процесі роботи програми відстежується стан цього прапора. Якщо буде використано режим покрокового виконання програми - відладчик дозволить клавіатурні переривання, змінивши при цьому прапор, а, отже, відстежувач зможе зафіксувати відлагоджування. Після виявлення такого режиму можна закрити програму або перейти на хибну гілку виконуваного коду. Слід зауважити, що метод працює тільки в ситуаціях, коли для роботи програми не потрібне введення даних від користувача (оператора).

Іншим методом, схожим до відстежування клавіатури, є слідкування за прапором переривань таймера. Відладчик під час своєї роботи зупиняє програму, а, відповідно, за викликом відповідного переривання, зупиняється таймер виконання програми. Відповідно, досліджуючи стан переривання таймеру, можна виявити роботу роботи відлагоджувача. Ще один варіант з застосуванням таймеру полягає у контролі часу виконання програми. На етапі розробки слід виконати пошук коду програми, який виконується доволі часто з приблизно однаковим часом. Після виявлення таких ділянок коду слід поставити перевірку часу, витраченого на їх виконання. Якщо при виконанні програми на таких ділянках буде виявлено суттєві розбіжності часу – це є свідченням роботи під відлагоджувачем. Методи, які базуються на роботі з таймером, не накладають обмежень на дії користувачів, а, отже, кращі ніж клавіатурний метод.

Проаналізувавши антивідлагоджувальні методи отримано розуміння, що прийоми захисту від відлагоджувачів не є універсальними: їх дієздатність забезпечена лише особливостями архітектури поточних процесорів і наявними підходами відлагоджування програм. Такі особливості обмежені, а їх принципи роботи – загальновідомі.

Однак, незважаючи на це, антивідлагоджувальні методи слід застосовувати при розробці програмного продукту, бо вони здатні забезпечити захист від зломщика-початківця і здатні забрати певний час в професійного зломщика.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Касперські К. Техніка відлагоджування програм без вихідних текстів [Текст] / К. Касперські; – СПб.: БХВ-Петербург, 2005. – 832 с.