УДК 004.056.53

ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ШЛЯХОМ ПРОТИДІЇ ПРИХОВАНОМУ СКАНУВАННЮ ПРОГРАМНОГО КОДУ

Поповський Р.А.
Тернопільський національний економічний університет, магістрант

Необхідність використання систем захисту програмного забезпечення (ПЗ) обумовлена рядом чинників, серед яких слід виділити: незаконне використання алгоритмів, що є інтелектуальною власністю автора, несанкціонований доступ, використання і модифікація ПЗ, незаконне розповсюдження і продаж ПЗ. Тенденція до зростання рівня піратства, яка зберігається і в даний час, збільшує фінансові втрати виробників ПЗ. У зв'язку з цим задача розробки надійних програмних систем захисту інформації (ПСЗІ) є актуальною.

Стійкість до злому ПСЗІ багато в чому визначається стійкістю до злому програмної підсистеми захисту логіки роботи (ППЗЛР), яка є складовою частиною будь-якої ПСЗІ. На сьогоднішній день, можна говорити про брак нових способів протидії засобам вивчення програм для операційних систем (ОС) Windows, які можуть бути використані при розробці ППЗЛР, що тягне за собою зниження стійкості до злому ПСЗІ, які функціонують в користувацькому режимі ОС Windows [1].

Проведений аналіз способів протидії прихованому скануванню програмного коду, які використовуються в ПСЗІ дозволяє зробити висновки про серйозні недоліки існуючих способів, які розроблені для користувацького режиму ОС Windows. Більше того, частина існуючих способів протидії не може бути реалізована для ОС Windows.

З структурної схеми ПСЗІ від несанкціонованого доступу видно, що будь-яка ПСЗІ містить ППЗЛР. Метою даної підсистеми є протидія можливим спробам нейтралізації системи захисту і/або її дискредитації. Будь-яка ППЗЛР повинна містити [2, 3]:

- способи протидії засобам динамічного сканування;
- способи протидії засобам статичного сканування;
- способи протидії програмам отримання дампу пам'яті.

Обов'язковою умовою при практичній реалізації ППЗЛР є:

- концептуальна цілісність ППЗЛР;
- всі способи протидії повинні бути розосереджені по всій ППЗЛР;
- способи протидії повинні взаємно захищати один одного;
- способи протидії не повинні бути реалізовані послідовно по групах протидії класам засобів сканування.

Останній пункт підтверджується тим, що успішна протидія одному класу засобів сканування не означає успішна протидія іншому класу засобів сканування. Дотримання даного твердження максимально утруднить аналіз механізмів захисту.

Разом з розробленими новими способами протидії засобам сканування, в ППЗЛР необхідно використовувати способи протидії, розглянуті в [4]. Необхідність такого підходу полягає в тому, що запропоновані тільки ті способи протидії, які направлені на нейтралізацію засобів сканування, що не мають протидії з боку ПСЗІ, які розроблялися до цього часу. Розроблені способи протидії призначені для обов'язкового комплексного використання з вже існуючими способами, що дозволяє значно збільшувати ефективність протидії ПСЗІ засобам сканування.

Запропоновані способи протидії засобам сканування можуть бути реалізовані у вигляді електронного ключа, який запобігає незаконному використанню і прихованому скануванню програми.

Список використаних джерел

1. Шадхин В. Е. Анализ средств взлома программных систем защиты информации / В.Е. Шадхин // Матеріали науково-технічного семінару «Проблеми інформатизації». – Черкаси: ЧДТУ, 2008. – Випуск 2 (2). – С.15 – 16.
2. Бабенко Л. К., Ищуков С. С., Макаревич О. Б. Защита информации с использованием смарт-карт и электронных брелоков / С. С Ищуков, О. Б. Макаревич // М.: Издательство: Гелиос.– 2003 г. – 352 с.
3. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров // М.: Издательство: ДМК; Серия: Компьютерная безопасность. – 2006. – 448 с.
4. Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин // - СПб.: БХВ-Петербург, 2006. - 384 с.