УДК 004.4
О.П. Ясній., докт. техн. наук, проф., В.І. Карплюк
(Тернопільський національний технічний університет імені Івана Пулюя)

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА АПАРАТНОМУ ТА ПРОГРАМНОМУ РІВНЯХ

UDC 004.4
O.P. Yasniy, Dr. Sc., Prof., V.I. Karplyuk

SOFTWARE PROTECTION AT HARDWARE AND SOFTWARE LEVELS

Перевагами захисту на програмному рівні є: гнучкість, порівняно низька вартість, сумісність із уже готовими системами. Однак великий недолік такого підходу – обмежена міцність. Із вдосконаленням існуючих та розвитком нових потужних методів, котрі дозволяють обійти безпеку додатків, фахівцям доводиться винаходити нові методики захисту своїх програмних продуктів. Враховуючи збільшення об'ємів віртуальної та накопичувальної пам'яті, а також беззаперечного приросту потужності процесорів, розробки методів захисту зі сторони програмістів та атак зі сторони реверс інженерів значно пришвидшилися.

Локальні конфіденційні дані, а також програмне забезпечення можна захистити за допомогою зашифрованої аутентифікації. При кожному запуску додатку здійснюватиметься захищена ідентифікація користувача, а усі необхідні для поточної робочої сесії блоки коду розшифровуватимуться у режимі реального часу обчислювальними ресурсами кінцевого користувача. Однак така методика захисту зможе гарантувати абсолютну безпеку лише в тому випадку, коли процеси шифрування та дешифрування виконуватимуться на окремому криптографічному співпроцесорі або спеціальному зовнішньому обладнанні. У такому випадку зловмисник не зможе отримати унікальний алгоритм шифрування та витягнути необхідний йому ключ дешифрування, оскільки доступними будуть тільки передбачені функції вводу та результати виводу (в якості реакції програмного продукту). Очевидно, що далеко не всі кінцеві клієнти зможуть забезпечити своє середовище такими апаратними модулями, тому ефективність такої методики низька. Аутентифікація стикається з подібними проблемами захисту.

Апаратними засобами, котрі дозволяють розв'язати таких задачі, можуть бути смарт-картки, які відіграють роль носія ключа доступу до продукту, а також виконуватимуть процеси шифрування/дешифрування. Проте такий підхід також не є популярним, оскільки такі апаратні додатки часто зазнають фізичних пошкоджень і потребують заміни зі сторони виробника. Також трапляються зловживання, пов'язані із вигаданим пошкодженням/втратою таких засобів, а для їх заміни виробнику потрібно виготовити та передати новий.

Отже, недоліками апаратних методів захисту є: неминуче підвищення вартості, несумісність із певними видами уже готових систем, модернізація, складність передачі, технічне обслуговування. Якщо хоча б один з апаратних засобів зламають зловмисники, заміні підлягатимуть усі, а саме тому гнучкість апаратних пристроїв низька у порівнянні з програмними підходами. Тому програмні механізми захисту можна доповнити апаратно та платформо незалежними методами обфускації, що забезпечить їх гнучкість та результативність.