УДК 004.422.8; 004.056
Н. Шингера
(Тернопільський національний технічний університет імені Івана Пулюя)

ПРОГРАМА TRUECRYPT ЯК АЛЬТЕРНАТИВА ІНСТРУМЕНТУ WINDOWS BITLOCKER

Як відомо, BitLocker Drive Encryption є потужною технологією, що дозволяє захищати дані шляхом повного шифрування дисків (логічних, карток, usb-накопичувачів, томів). Коли потрібне шифрування? У випадку зберігання користувачами на власних комп'ютерах конфіденційних даних (наприклад, особистих фінансових документів). Шифрування посилить захист таких відомостей від зловмисників. Особливо це стосується власників ноутбуків (є загроза їх втрати або крадіжки).

Використання BitLocker є не єдиним можливим вирішенням. Прекрасною альтернативою може стати TrueCrypt – потужний і надійний засіб для електронного захисту секретних даних, який до того ж є безкоштовною утилітою із відкритим кодом. Цей продукт ні в чому не уступає комерційним і навіть має багато переваг в порівнянні з ними. Працює в ОС сімейства Microsoft Windows XP/2000/2003/Vista і Linux. Програма підтримує роботу через командний рядок і має детальну документацію, яка містить навіть опис алгоритмів шифрування.

TrueCrypt створює на диску комп'ютера захищений том. Усе, що збережене у цьому томі, повністю шифрується, включно із іменами файлів і папок. Фізично том – це файл, який може мати будь-яку назву (на вибір користувача). Операційна система «бачить» цей файл як окремий диск. Під час запису на цей «диск» дані автоматично зашифровуються, при зчитуванні – розшифровуються. Усе відбувається миттєво. Користувач працює так само, як працював би із звичайним диском.

Файли на віртуальних дисках можна копіювати, переміщувати, знищувати, тобто виконувати з ними усі операції, які є доступними для будь-якого іншого файлу. Для отримання доступу до вмісту файлу, зашифрованого за допомогою TrueCrypt, необхідно змонтувати том (файловий контейнер) як окремий диск. Заздалегідь потрібно задати пароль для шифрування. В середовищі Windows файловий контейнер представляється у вигляді окремого накопичувача (такого ж, як диски C: и D:) Після цього можна отримувати доступ до зашифрованого файлового контейнера, додавати туди файли і папки, а також видаляти їх чи змінювати.

У список алгоритмів шифрування, які підтримуються у TrueCrypt входять AES, Serpent і Twofish. Усі три алгоритми дуже надійні, і на сьогодні не існує навіть теоретичного способу злому, окрім методу повного перебирання. При виборі одного із запропонованих алгоритмів слід керуватися швидкістю його роботи на конкретній машині. Протестувати алгоритми на швидкість роботи можна за допомогою відповідної вбудованої в програму функції. Також можливе використання каскадного шифрування різними шифрами, наприклад: AES+Twofish+Serpent і т.п. Усі алгоритми шифрування використовують режим LRW, який є безпечнішим, ніж режим CBC.

Зашифрованим сховищем («диском») може бути як частина вільного місця на диску, так і цілий розділ жорсткого диску, а також flash-карти або інші знімні пристрої зберігання даних.

Маючи такі потужні переваги, TrueCrypt все ж дуже проста у використанні програма. Те ж саме стосується її встановлення і налаштування.

Отже, справедливим буде зауваження, що TrueCrypt – це той випадок, коли на тлі розрекламованих криптографічних систем, насправді якісні і потужні розробки нерідко залишаються непоміченими.