УДК 621.396:004.056.5 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.178

КОНЦЕПТУАЛЬНІ ЗАСАДИ МЕТОДУ ЗМІШУВАННЯ БІТ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ШИФРУВАННЯ PE-ФАЙЛІВ НА БАЗІ БЛОКОВИХ АЛГОРИТМІВ

Шавлак А.В., Чалий Д.В., Бондаренко Г.Р.
Науковий керівник – к.т.н., с.н.с. Калюжний М.М.
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна
e-mail: artem.shavlak@nure.ua,e-mail:dmytro.chalyi.@nure.ua,
e-mail: hryhorii.bondarenko@nure.ua

Block encryption algorithms provide high encryption speed and are relatively simple to implement. However, under certain conditions, a decrease in stability may be observed. For example, for DES in ECB mode, in the case of encryption of EXE files and files of other types, the first block of which is the header of this file, since knowing its content, it is possible to significantly reduce the time of breaking the cipher itself. To avoid such situations, it is suggested to perform a bit-mixing operation on the original message to be encrypted. Such an operation destroys semantic features in the file being encrypted, thereby creating conditions for increasing the cryptographic stability of the cipher.

Криптосистема DES, завдяки архітектурним особливостям, забезпечує високу швидкість обробки та рівень стійкості, достатній для шифрування конфіденційних даних, що не належать категорії секретних. При цьому, найвища швидкодія забезпечується у режимі ECB (Electronic Codebook).

Разом з тим, у випадку шифрування файлів деяких типів (dll, exe, drv, sys, mui тощо), що наслідують формат PE, застосування DES-ECB може вести до швидкого розкриття шифру зловмисником. Це зумовлено тим, що, шифрування DES здійснюється на рівні блоків 64 біта. При цьому, у режимі ECB усі блоки, виокремлені у межах файлу, шифруються незалежно один від одного з єдиним ключем, тоді як заголовок PE-файлу має також довжину 64 біта. Ураховуючи те, що зміст заголовку є, по-перше, стандартним, а, по-друге, чітко виокремлюється з довільного потоку даних завдяки характерним сигнатурам (зокрема, 0x5A4D та 0x3C), завдання реконструкції вихідного файлу стає тривіальним.

Для усунення зазначеного недоліку пропонується застосувати метод попереднього змішування біт PE-файлу, тим самим руйнуючи семантичні ознаки заголовку. При цьому, така процедура має відповідати наступним вимогам:

- проста алгоритмічна та математична реалізація, що дозволяє виконувати шифрування у режимі реального часу, не вносячи помітну затримку;
- порядок змішування біт повинен бути динамічним;

- процедуру має бути побудовано у вигляді окремого модулю, що передує шифруванню, тим самим не вносячи змін у базовий алгоритм.

Щоб виконати умову щодо динамічного порядку змішування, для файлу пропонується попередньо обчислити ряд інформативних ознак $q_1 \dots q_n$, які далі буде використано у ролі опцій для побудови процесу. При цьому, якщо такі інформативні ознаки обчислено на базі змісту файлу, їх подальше використання, по-перше, створює умови для можливості побудови унікального сценарію змішування, а по-друге – користувач буде позбавлений необхідності самостійно встановлювати параметри процедури.

Розглянемо сценарій реалізації процедури змішування, побудований на базі двох технологічних етапів, а саме:

- циклічного бітового зсуву даних заголовку та службових полів на рівні байт позиції заголовків та службових полів;
- виконання байтового зсуву на рівні усього файлу для зміни позиції службових компонент та заголовку.

У ході першого технологічного етапу кожен байт b заголовку та службових полів, загальною кількістю n, спочатку конкатенують між собою на рівні біт, тим самим утворюючи суцільний масив біт B. Після зазначеної процедури у межах масиву B виконується операція sh циклічного зсуву на ξ позицій, за результатами чого утворюється змінений масив B':

$$B' = sh(d; \xi; B; n), \quad (1)$$

$$n > 8,$$

де n - кількість байт, включених у множину B, що визначається на базі раніше розрахованої інформативної ознаки у загальному вигляді, як $n = \phi(q_1)$; вимога щодо величини масиву B зумовлюється необхідністю внесення невизначеності у структуру файлу ще до етапу шифрування;

d - напрямок зсуву, що визначається також на базі однієї з попередньо обчислених інформативних ознак як $d = f(q_2)$.

Для обчислення кроку ξ циклічного бітового зсуву, так само, як і для визначення напрямку d, тут використовується будь-яка інша з виявлених інформативних ознак у загальному вигляді $\xi = \varphi(q_3)$.

У свою чергу, зсув змісту файлу та службових даних на рівні байт для зміни стартової позиції Φ першого біту PE-заголовку може виконуватися аналогічно принципу, зазначеному виразом (1), а саме:

$$\Phi' = sh(\bar{d}; \bar{\xi}; \Phi), \quad (2)$$

де Φ' - позиція першого біту PE-заголовку після виконання зсуву;

$\bar{\xi}$ - крок байтового зсуву, що обчислюється аналогічно ξ, проте для його розрахунку може використовуватися інша інформативна ознака та функціональне перетворення;

$\bar{d}$ - напрямок байтового зсуву, який знаходиться за тим же принципом, як і напрямок d, але, у загальному випадку, на базі іншої інформаційної ознаки і функціонального перетворення.

Отже, побітовий зсув на рівні PE-заголовку спочатку порушує його структуру, а також структуру деякої кількості службових полів, тим самим маскуючи характерні семантичні ознаки. У свою чергу, циклічний байтовий зсув на другому етапі процесу змішування змінює позицію вже модифікованої ділянки файлу, де міститься у т.ч. заголовок.

Таким чином, сформовано концептуальні засади методу попереднього змішування біт файлів PE-архітектури, що забезпечує подальше ефективне його шифрування на базі криптографічної системи DES у режимі ECB.

У рамках методу передбачається використання системи інформаційних ознак, що розраховується для кожного файлу, який підлягає шифруванню, окремо, виходячи з особливостей його змісту. Такі інформаційні ознаки виступають у ролі параметрів реалізації процесу змішування. Це, у свою чергу, дозволяє забезпечити унікальний перебіг процесу, а також повністю його автоматизувати.

Реалізація методу змішування біт відповідно до запропонованої концепції дозволяє протидіяти криптоаналітичним атакам - таким, як атака за відомим відкритим повідомленням, та подібним їй. Це є актуальним не лише для DES-ECB, але і для інших симетричних шифросистем з розміром блоку, рівним 64 біта.

У рамках подальшого розвитку концепції передбачається:

- формування математичного апарату для розрахунку системи інформативних ознак файлу;
- проведення експериментального дослідження для виявлення ефективного діапазону розмірів файлів, відносно якого може бути використано створюваний метод.

Список використаних джерел:

1. Portable Executable // Iana URL https://www.iana.org/assignments/media-types/application/vnd.microsoft.portable-executable (дата звернення: 05.03.2024)

2. Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard // Computer URL https://www.computer.org/csdl/magazine/co/1977/06/01646525/13rRUwInvDu (дата звернення: 05.03.2024)

3. Block Ciphers // Uwaterloo URL https://cacr.uwaterloo.ca/hac/about/chap7.pdf (дата звернення: 05.03.2024)