Секція 1

ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ АЛГОРИТМІВ ГЕШУВАННЯ

Бутенко С. І.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В.Я.

Актуальність. З розвитком інформаційних технологій широкого розповсюдження набули задачі, які вирішуються з використанням геш-функцій. Серед задач можна виділити процес створення електронний цифровий підпис (ЕЦП) та системи зберігання паролів. ЕЦП використовується для контролю цілісності документа та ідентифікації особи, що його підписує [1]. При підписанні деякого набору даних вони обробляються за допомогою алгоритму гешування. У загальному випадку геш-функція - це математичний алгоритм, який перетворює дані довільного розміру в бітовий масив фіксованого розміру [2]. Це одна з вимог до геш-функції.

При організації систем зберігання паролів алгоритми гешування використовуються для того щоб не зберігати паролі у відкритому вигляді. Після обробки отримується бітова послідовність заданої довжини яка не може бути напряму конвертована у сам пароль. У разі викрадення паролів з системи даний метод захистить від миттєвої компрометації. В обох випадках швидкодія алгоритмів гешування корелюється з ефективністю використання ресурсів пристроїв на яких вони виконуються.

Для збільшення швидкості роботи алгоритмів потрібно підвищувати ефективність використання ресурсів. Висока швидкодія та пов'язана з нею висока ефективність дозволяє реалізовувати системи з їх застосуванням на пристроях з невеликими або сильно обмеженими обчислювальними можливостями.

Метою даної роботи є порівняння алгоритмів гешування за критерієм швидкодії.

Основні положення. У доповіді надано результаті порівняльного аналізу алгоритмів SHA-2(256) – зараз самий розповсюджений алгоритм гешування, Kupyna – національний стандарт гешування в України, Стрібог – міждержавний стандарт, с - останній з алгоритмів серії Message Digest (приймав участь в конкурсі на новий стандарт SHA-3) [3]. Задля досягнення повноти та коректності при проведенні

досліджень було враховувано фактори, які вплинути на отримані результати. Тестування швидкодії алгоритмів проводилось в рамках однієї системи з чітко визначеними параметрами, був мінімізоване вплив інших програмних засобів на ресурси системи, тестування алгоритмів проводилось на процесорах з різною архітектурою (x86 та ARM). Також слід брати до уваги те, що різні реалізації одного і того самого алгоритму можуть мати різний показник швидкодії. Під час проведення тестування було виявлено, що виконання сучасних алгоритмів гешування може бути розділено на декілька потоків. На результати тестування значно впливав доступний об'єм кеш-пам'яті процесора. Також було виявлено, що для виключення впливу інших програмних засобів потрібно за допомогою засобів операційної системи задати процесу, що виконує алгоритм, максимальний з доступних пріоритетів.

Висновки. При виборі алгоритмів для сучасних комп'ютерних систем слід звертати основну увагу на можливість виконання алгоритму у багато потоковому режимі, а також те, наскільки ефективно він може використовувати доступні ресурси системи.

Список літератури

1. Пєвнєв В. Я. Моделі загроз і забезпечення цілісності інформації. *Системи та технології*. 2018. №2 (56/1). С. 79–94.
2. Хеш-функция, что это такое? *Habr*. URL: https://habr.com/ru/post/534596/ (дата звернення 11.11.2021).
3. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. Вид. офіц. Київ : Мінекономрозвитку України, 2015. 5 с.

Відомості про авторів

Бутенко Сергій Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 068-395-71-04, s.butenko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu