УДК 004.056:004.424.47

Ю. В. Баришев
Т. А. Лавренюк

МЕТОД ЗАВ'ЯЗУВАННЯ БЛОКІВ ДАНИХ ДЛЯ ПСЕВДОНЕДЕТЕРМІНОВАНОГО ГЕШУВАННЯ

Вінницький національний технічний університет, м. Вінниця.

Анотація

Запропоновано метод збільшення стійкості конструкцій гешування до загальних атак без збільшення довжини проміжного геш-значення за рахунок використання псевдонедетермінованого гешування з рівномірним розподілом псевдовипадкового відхилення для обрання наступного блоку повідомлення для обробки.

Ключові слова: гешування, геш-значення, загальні атаки, генератор псевдовипадкових чисел (ГПВЧ).

Abstract

The method for infeasibility increasing against generic attacks avoiding intermediate hash value expanding by usage of the pseudonondeterministic hashing approach with arbitrary distributed pseudorandom divergence of the next data block is proposed.

Keywords: hashing, hash, generic attacks, pseudorandom generator.

Вступ

Наразі одним з найефективніших методів забезпечення цілісності, автентичності та конфіденційності інформації є гешування. Серед загальних атак пошуку мультиколізій, які здійснюються на конструкції гешування, істотну загрозу становить атака Келсі-Коно [1-4]. Вона дає можливість попередньої підготовки наборів блоків даних, що при послідовній обробці, дозволяють отримати певне геш-значення [1]. Актуальною проблемою є розробка нових методів протидії даній атаці, оскільки більшість відомих вимагають додаткових апаратних ресурсів і часу обробки, що є недоліком у практичному застосуванні, особливо для мобільних пристроїв невеликих розмірів та реалізації криптографічних протоколів у мікропроцесорних системах.

За мету дослідження обрано – збільшення стійкості до загальних атак без збільшення довжини проміжного геш-значення. Виходячи з мети були поставлені такі задачі:

- аналіз псевдонедетермінованого гешування;
- вибір методу генерування псевдовипадкового відхилення;
- аналіз особливостей використання методу.

Конструкції гешування

Для протидії атакам попередньої підготовки відомий метод псевдонедетермінованого гешування, у якому блоки повідомлення, яке гешується, обробляються не послідовно, а залежно від деякого псевдовипадкового відхилення [2-4]. Приклад такої конструкції [2]:

$$\begin{cases} r_i^{(1)}=rand\left(m_i^{(1)}\right), \\ r_i^{(2)}=rand\left(m_i^{(2)}\right), \\ \ldots \\ r_i^{(q)}=rand\left(m_i^{(q)}\right); \\ h_i^{(1)}=f_i^{1}\left(h_{i-1}^{(1)}, m_i^{(1)} * m_{i-r_i^{(1)}}^{(1)}\right), \\ h_i^{(2)}=f_i^{2}\left(h_{i-1}^{(2)}, m_i^{(2)} * m_{i-r_i^{(2)}}^{(2)}\right), \\ \ldots \\ h_i^{(q)}=f_i^{q}\left(h_{i-1}^{(q)}, m_i^{(q)} * m_{i-r_i^{(q)}}^{(q)}\right), \end{cases}$$

де $r_i^{(j)}$ – псевдовипадкове відхилення від номера поточного блока даних, яке отримують у j-тому каналі; *rand*(·) – деяка функція генерування псевдовипадкових чисел; «*» – операція об'єднання двох операндів в один.

Для вибору даного відхилення необхідний генератор псевдовипадкових чисел, що утворює рівномірну числову послідовність у змінних діапазонах при сталих внутрішніх параметрах.

Генератор псевдовипадкових чисел

Пропонується використовувати принцип подвійного модуля, де перший модуль ГПВЧ підібраний з урахуванням усіх вимог для повного періоду послідовності, а другий модуль регулюється в залежності від кількості блоків повідомлення. Далі наведено застосування даного принципу для лінійного конгруентного ГПВЧ [5]:

$$\begin{cases} x_{i+1} = (ax_i + c) \bmod N; \\ r_{i+1} = x_{i+1} \bmod M, \text{якщо } x_{i+1} < (N - N \bmod M), \end{cases}$$

де $M<N$.

Для підвищення стійкості пропонується також попереднє визначення внутрішніх параметрів ГПВЧ в залежності від певного блоку повідомлення.

Особливістю псевдонедетермінованого гешування є необхідність зберігати в пам'яті повний набір блоків вхідних даних. Оскільки довжина повідомлення на практиці може бути занадто великою щодо виділених ресурсів, пропонується застосовувати принцип «ковзного вікна», виділивши буфер для фіксованої кількості блоків і обробляючи дані у його межах.

Висновки

Запропонований метод вибору псевдовипадкового відхилення утворює рівномірну послідовність чисел, період якої перевищує кінцевий модуль. При такому порядку обробки блоків повідомлення при гешуванні реалізація атаки попередньої підготовки значно ускладнюється.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kelsey J. Second preimages on n-bit hash functions for much less than 2n work / J. Kelsey, B. Schneier // EUROCRYPT. – 2005. – P. 474 – 490.

2. Лужецький В. А. Конструкції хешування стійкі до мультиколізій / Лужецький В. А., Баришев Ю.В. // Наукові праці ВНТУ. – №1. – 2010. – 8 с.

3. Luzhetsky V. Methods of Generic Attacks Infeasibility Increasing for Hash Functions / Volodymyr Luzhetsky, Yurii Baryshev // The 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013), September 12-14, 2013 Berlin, Germany. – Режим доступу до статті: idaacs.net/2013/wp-content/uploads/abstracts/i13-071_8d0bb875.rtf

4. Luzhetsky V. The Generalized Construction of pseudonondeterministic hashing / Volodymyr Luzhetsky, Yurii Baryshev // Computing. – Vol. 11 (Issue 3). – 2012. – p. 302-308.

5. Баришев Ю. В. Методи формування псевдовипадкових чисел для псевдонедетермінованих геш-функцій / Ю. В. Баришев, Т. А. Кравчук // Тези доповідей Третьої міжнародної науково-практичної конференції "Інформаційні технології та взаємодії", м. Київ, 8-10 листопада 2016 року. – К. : Видавничо-поліграфічний центр "Київський університет", 2016 – С. 207-208.

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна e-mail: yuriy.baryshev@gmail.com.

Лавренюк Тетяна Андріївна — студентка групи 1БС-13б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: kravchuktetiana95@gmail.com.

Yurii Baryshev — Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine**.**

Tetiana Lavreniuk — Student, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.