

УДК 621.396

<sup>1</sup>Мареk Александер, <sup>2</sup>Уляна Яциковська

<sup>1</sup>Державна вища технічна школа у Новому Сончі, Польща

<sup>2</sup>Тернопільський національний технічний університет імені Івана Пулюя, Україна

## ЗБІЛЬШЕННЯ ПРОДУКТИВНОСТІ ВИКОРИСТАННЯ ОБЧИСЛЮВАЛЬНОГО РЕСУРСУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

**Marek Aleksander, Ulyana Yatsykovska**

### INCREASE PRODUCTIVITY USING THE COMPUTING RESOURCES OF COMPUTER NETWORK

При створенні сучасних комп'ютерних мереж необхідно враховувати обчислювальні ресурси мережі для досягнення їх надійності і доступності [1].

Нехай  $b$  - кількість бітів в IP-заголовку, яку можна використовувати для маркування повідомлення маршрутизатором. Наприклад,  $b = 25$  [2-4].

Алгоритм для надання повідомлення  $M_x$  до користувача  $V$  від кожного маршрутизатора  $X$  в мережі атаки заснований на методі випадкового посилення. Основна ідея цього методу полягає у виконанні наступних перетворень для  $M_x$ :

- значення  $M_x$  має бути таким, щоб  $|M_x|$  було кратним до  $l$ ;
- обчислити досить велику (і статистично випадкову) контрольну суму  $C = C(M_x)$  в послідовності  $M_x$ . Доцільно, щоб контрольна сума  $C(M_x)$  була випадковою або статистично випадковою (наприклад, випадкова хеш-функція) і непередбачувана для ініціатора атак;
- розбити  $M_x$  в послідовність  $W$  непересічних фрагментів слів  $M_0, M_1, M_2, \dots, M_{l-1}$ ;
- створити набір блоків, які використовуються для перезапису  $b$  біт, так щоб  $b_i = [i, C, M_i]$ .

Таким чином, блок складається з індексу, контрольної суми, і фрагменту повідомлення.

Блоки  $b_i$  використовуються для передачі повідомлень  $M_x$  користувачеві  $V$ , проте вони не передаються в довільному порядку. Нехай,  $C = C(M_x)$  для повідомлення  $M_x$  буде використовуватися і як асоціативний адрес  $M_x$ , і як контрольна сума для "посилання" всіх частин  $M_x$ . Значення  $C$  є статистично випадковим і непередбачуваним для ініціатора атак, а тому, це доцільно використати для алгоритму відновлення повідомлення. Алгоритм відновлення повідомлення є достатньо простим, оскільки для набору блоків  $b_i$  з таким самим значенням  $C$ , користувач складає разом блоки  $b_i$  в правильному порядку, використовуючи контрольні суми  $C$ , щоб була правильна послідовність блоків повідомлення. Коли користувач  $V$  має дійсну послідовність  $b_i$  побудовану в правильному порядку, тоді він відновлює повідомлення  $M_x$ .

Якщо можна повторно використати деякі біти із IP-заголовком для інформації маркування маршрутизаторів, то доцільно розбити  $b$  багаторазові біти в IP заголовку таким чином:

- $\lceil \log l \rceil$  бітів для фрагмента індекса  $i$ ;
- $c$  бітів для контрольної суми, які є як асоціативна адреса і як контрольна сума;
- $h = b - c - \lceil \log l \rceil$  біт для даних слова  $M_i$ .

Нехай функція  $C(M_X)$  або  $M_X$  є випадкова, так що значення контрольної суми  $C(M_X)$  статистично випадкове і непередбачуване для ініціатора атак. Проте, це мало ймовірно, тому що хеш-функція є випадковою для  $C(M_X) = C(M_Y)$  з аналогічним вихідним розміром і для двох різних повідомлень маршрутизатора  $M_X$  і  $M_Y$ . Зокрема, щоб  $C(M_X)$  було непередбачуваним для ініціатора, який знає тільки значення  $X$ , але не знає всього повідомлення  $M_X$ . Значення  $M_X$  має бути кратним до  $l$  і тоді можна обчислити с-біт контрольної суми  $C = C(M_X)$  для  $M_X$ , і розбити значення  $M_X$  в послідовність  $W$  з  $l$  слів  $M_0, M_1, M_2, \dots, M_{l-1}$  довжиною  $h$  біт кожна. Визначимо набір з  $l$  блоків  $b_0, b_1, \dots, b_{l-1}$  такі, що  $b_i = [i, C, M_i]$ , де контрольна сума  $C$  входить в кожен блок  $b_i$ . Значення  $C$  зв'язує блоки  $b_i$  разом і є асоціативною адресою для блоків.

Отже, підхід випадкового посилення використовує великі за розміром ланцюжки контрольної суми повідомлення. В цьому методі фрагменти повідомлення  $M_X$  складаються таким чином, що ланцюжки контрольної суми  $C$  виступають в якості асоціативної адреси і цілісності даних даного повідомлення. Такий підхід є швидким та ефективним для відновлення повідомлення користувачем при кількості 500 маршрутизаторів у мережі атаки. Тому, використання методу випадкового посилення дає можливість відновити повідомлення за короткий проміжок часу і визначити джерело атаки при великому розмірі мережі атаки. Таким чином, запропонований підхід збільшує продуктивність використання обчислюваного ресурсу комп'ютерної мережі при великих розподілених атаках на відмову в обслуговуванні.

### **Література**

1. Халиль Х. А. Алгоритмы маршрутизации в мобильных сетях / Х. А. Халиль, А. Шкерат // Гірнична електромеханіка та автоматика: наук.-техн. зб. – 2002. – Вип. 69. – С. 94–100.
2. Dean D. An algebraic approach to IP traceback / D. Dean, M. Franklin, A. Stubblefield // In Network and Distributed System Security Symposium (NDSS). – 2001. – P. 3–12.
3. Goodrich M. T. Efficient packet marking for large-scale IP traceback / M. T. Goodrich // In 9th ACM Conf. on Computer and Communications Security (CCS). – 2002. – P. 117–126.
4. Goodrich M. T. Implementation of an authenticated dictionary with skip lists and commutative hashing / M. T. Goodrich, R. Tamassia, A. Schwerin // In Proc. 2001 DARPA Information Survivability Conference and Exposition. – 2001. – Vol. 2. – P. 68–82.