УДК 621.396

[1]Марек Александер, [2]Уляна Яциковська
[1]Державна вища технічна школа у Новому Сончі, Польща
[2]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-заголовоку, 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 посилання. 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 $M_0, M_1, M_2, \ldots, M_{l-1}$;

- 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 заголовоку 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 малоймовірно, 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 $M_0, M_1, M_2, \ldots, M_{l-1}$ довжиною *h* біт кожна. Визначимо набір з *l* блоків $b_0, b_1, \ldots, b_{l-1}$ 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 посилання використовує великі за розміром ланцюжки контрольної суми повідомлення. В цьому методі фрагменти повідомлення M_X складаються таким чином, що ланцюжки контрольної суми С 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 посилання 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 // Гірнича 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.