УДК 681.51:519.876
У. Яциковська, М. Карпінський, Я. Кінах
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕХАНІЗМ ЗАХИСТУ ВІД АТАК НА ВІДМОВУ

Серед найважливіших на сьогодні задач безпеки в мережі Інтернет є загроза відмови в обслуговуванні. Розподілені відмови в обслуговуванні типу DDoS вичерпують комутаційні та обчислювальні ресурси протягом короткого проміжку часу.

Виділяють три етапи захисту від атак на відмову: попередження атаки, виявлення атаки та протидія атаці. Попередженням атаці є здійснення заходів протидії до її початку реалізації. Виявлення атаки на відмову є важливим етапом, оскільки потрібно її відслідкувати в разі її появи в системі. Протидія атаці включає відбиття атакуючих пакетів та забезпечення нормальної роботи системи. Основною задачею протидії атаці є відфільтрування трафіку атаки та забезпечення нормального трафіку для законних користувачів.

У схемі виявлення атаки на відмову показником ефективності є відсоток виявлення атак. Деякі типи атак на відмову використовують експлойти та вразливості програмного забезпечення, фальсифікацію і специфічну форму пакетів, імітацію звичайного трафіку для перевантаження каналів зв'язку. В такому разі, схема виявлення атаки на відмову може помилково прийняти звичайний інтенсивний трафік за атакуючий. Ознакою здійснення атаки на відмову є перевантаження каналів мережі. Тому, щоб виявити атаку потрібно оцінити завантаженість мережі та шукати причину перевантаження у мережевих потоках чи з'єднаннях. Виявлення перевантажень системи є ефективним, коли воно спричинене атакуючим трафіком та можна аналізувати пакети перевантаженої ланки. В разі, коли перевантаження спричинено звичайним трафіком, при великому напливі законних користувачів, виявлення перевантажень може бути хибним, оскільки алгоритм не зможе відрізнити легітимний трафік від атакуючого.

Механізми захисту на проміжних мережах ефективні, оскільки атака може бути відстежена та знешкоджена. Прикладом таких механізмів є трасування, буксирування [1]. Механізм джерело – мережа може зупинити потоки атаки перш ніж вони увійдуть до Інтернет ядра і перш ніж вони агрегуються та з'єднаються з іншими потоками атак.

Фергесоном та Сені [2] запропоновано рівень фільтрації, який обмежує спад трафіку з IP-адресами, які не відповідають префіксу домену підключеного на вхід маршрутизатора. Вихідна фільтрація забезпечує тільки визначеного чи виділеного IP-адресного простору, що залишає мережу. Парк та Лі [3] використовують інформацію про маршрути, щоб відфільтрувати підроблені IP-адреси.

Безсумнівно, що DDoS атаки є важливою задачею для механізмів захисту. Розглянуті механізми захисту дозволяють на практиці організувати ефективну комп'ютерну мережу, ресурс якої в повній мірі використовується виключно для користувачів мережі.

1. S. M. Bellavin, "ICMP traceback messages", Internet Draft, 2001

2. P. Ferguson and D. Senie, "RFC 2827: Network Ingress Filtering: Defeating Denial of Service attacks which employ IP source Address .

3. K. Park and H. Lee, "On the effectiveness of probabilistic packet making for IP traceback under Denial of Service attack", hoc. IEEE WOCOMM Anchorage, AK, USA, pp. 338-347, Apr. 2WI.