УДК 004

О.К. Савеленко[1]
Кіровоградський національний технічний університет

Способи ослаблення IP-спуфінг атаки

Вступ. DoS-атаки, що недавно спостерігалися, з використанням підміни адреси відправника показали наявність серйозної небезпеки для провайдерів Internet (ISP) і співтовариства Internet в цілому. Розглянемо простий і ефективний метод боротьби з такими атаками шляхом використання фільтрації вхідного трафіку з метою блокування DoS-атак, в яких використовуються IP-адреси, що не відносяться до точок агрегації ISP.

Основна частина. Проаналізувавши IP-пакет, а зокрема - адресу хоста, можна визначити IP-адресу джерела даних. IP-спуфінг приховує IP-адресу, створюючи пакети, що містять помилкові адреси, щоб приховати дані при з'єднанні та відправці інформації. IP-спуфінг – це загальновизнаний метод, використовуваний спамерами і хакерами для маскування своєї реальної IP-адреси. Визначити IP-спуфінг можна наступним чином: перевірити IP-адресу яка була знайдена в даних і відповісти на неї, перевірити значення TTL (Time to Live) оригінального пакету перед відправкою на сумнівний хост, перевірити ідентифікаційний номер пакету.

Загрозу IP-спуфінга можна трохи ослабити (але не усунути) за допомогою наступних кроків:

1. *Контроль доступу.* Найпростіший спосіб запобігання IP-спуфінга полягає в правильному налаштуванні управління доступом. Щоб понизити ефективність IP-спуфінга, необхідно побудувати контроль доступу на відсікання будь-якого трафіку, що поступає із зовнішньої мережі з початковою адресою, розташованою усередині мережі. Це допомагає боротися з IP-спуфінгом, коли санкціонованими є тільки внутрішні адреси. Якщо санкціонованими є і деякі адреси зовнішньої мережі, даний метод стає неефективним.

2. *Фільтрація RFC 2827*. Можна припинити спроби IP-спуфінга чужих мереж користувачами своєї мережі. Для такої реалізації потрібна фільтрація будь-якого витікаючого трафіку, початкова адреса якого не є однією з IP-адрес організації. Цей тип фільтрації, відомий під назвою "RFC 2827", може виконувати і провайдер. Зрештою відфільтрується весь трафік, який не має початкової адреси, яка очікується на певному інтерфейсі. Наприклад, якщо провайдер надає з'єднання з IP-адресом 192.1.1.0/24, він може побудувати фільтр так, щоб з даного інтерфейсу на маршрутизатор провайдера допускався тільки трафік, що надходить тільки з адреси 192.1.1.0/24. Проте значне віддалення від фільтрованих пристроїв значно ускладнює проведення точної фільтрації.

Висновок. Виходячи з вище сказаного, найбільш ефективним методом є використання контролю доступу, в якому після впровадження певних мір атака втрачає сенс.

---

[1] викладач кафедри програмного забезпечення