- забезпечення справедливості обслуговування пакетів одного потоку;
- підтримка розподілених рішень з управління інформаційними чергами;
- простота алгоритмічно-програмної та апаратної реалізації мережі;
- віртуалізація мережевих засобів та пристроїв;
- класифікація та маркування мережевих інформаційних пакетів;
- визначення черговості передавання пакетів з черг в канал передачі.

Дослідження показує, що актуалізується проблематика адаптивного структурно - функціонального синтезу логічної інфраструктури інформаційної мережі приймаючи до уваги цільове призначення процесів, флуктуаційний характер та пікові значення інтенсивності потокового навантаження різних типів, що в процесі динамічного програмного конфігурування ресурсів забезпечило б виконання вимог до продуктивності інформаційної мережі, оперативності доставки даних та якості обслуговування користувачів.

Таким чином, на відміну від ідеалізованої моделі побудови у реальних інформаційних мережах проблеми та перспективи побудови систем управління ресурсами інформаційних комунікаційних мереж мають важливе значення для створення нових мереж. Це необхідно та спостерігається не тільки на рівні інформаційної мережі в цілому, але і на рівні окремих комунікаційних пристроїв.

Перелік посилань

1. Лунтовський А. О. Етапи розвитку сучасних інфокомунікаційних сервісів та енергетична ефективність мережевих технологій / А.О. Лунтовський, П. О. Гуськов, А. Р. Масюк // Вісник Національного університету «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації. — Львів: Видавництво Львівської політехніки, 2014. - № 796. - С. 131-139.

2. Стеклов В.К. Інформаційна система: підручник для студентів вищих навчальних закладів за напрямком «Телекомунікації» / В.К. Стєклов, Л.Н. Беркман. – К.: Тех-ніка, 2014. – 792 с.

Процес визначення початку атаки типу HTTP GET flood

Соколюк Я.В.
Науковий керівник – к.т.н.,доц. Муляр І.В.
Хмельницький національний університет

Для виявлення початку атаки та подальшого виявлення шкідливого трафіку оптимальним буде підхід, який базується на аналізі аномалій, що призводить до порівняння поточного стану системи з її нормальним станом.

При цьому порівнюються різні властивості мережної активності. Ці властивості контексті DDoS-атак можуть включати: тип та кількість запитів, кількість запитів певного протоколу, IP-адресу джерела, час та швидкість запитів, тощо [1].

Атака типу HTTP GET flood використовується нападниками для атаки веб-серверів та серверів веб-додатків. Атака - це сукупність на перший погляд законних запитів GET або POST до сервера [2]. Це спеціально розроблені запити на споживання значної кількості серверних ресурсів. В результаті вони можуть призвести до стану відмови в обслуговуванні, без необхідності переповнювати канал великим обсягом трафіку. Такі запити у випадку розподіленої атаки DoS надсилаються з десятків тисяч заражених вузлів. На рис. 1 схематично показує послідовність пакетів у запиті HTTP GET після з'єднання TCP.

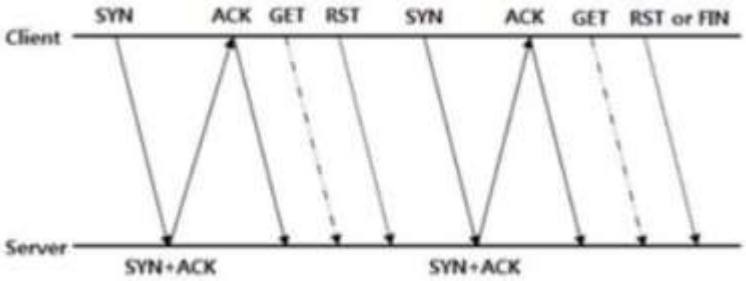

Рисунок 1- Послідовність пакетів при атаці типу HTTP GET

В процесі атаки зловмисник постійно відправляє запити, створюючи при цьому нові TCP з'єднання. Останнім часом [3] також стали розповсюдженими HTTP GET flood атаки в рамках одного TCP з'єднання (див. рис. 2). Цей тип атаки не можливо виявити методом оцінки кількості SYN запитів.

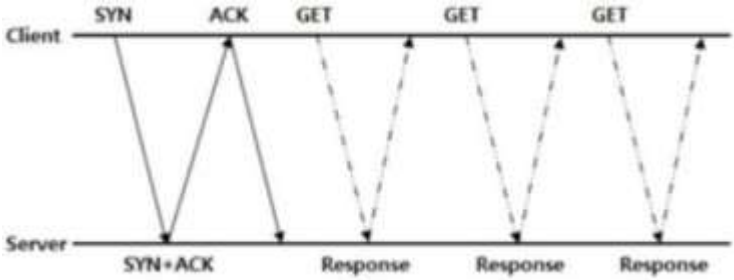

Рисунок 2 - Послідовність пакетів при атаці типу HTTP GET в рамках одного TCP з'єднання

Нині атака HTTP-потоків є однією з найдосконаліших загроз інформаційній безпеці, яка безпосередньо не пов'язана з уразливістю програмного забезпечення. Для обладнання безпеки відрізнити зловмисні HTTP-запити від законних надзвичайно складно, а неправильні методи або налаштування призводять до великої кількості помилкових спрацьовувань. Використання метрик, заснованих лише на оцінці інтенсивності запиту, не є оптимальним методом виявлення DDoS-атак, таких як повеня HTTP, оскільки обсяг трафіку може бути нижче порогового. Тому доцільно використовувати багатокритеріальний метод виявлення DDoS-атак з показниками, які залежать від інтенсивності запитів, і тими, які не залежать від цього показника.

MapReduce - модель проведення розподіленої паралельної обробки великих масивів даних з використанням кластерів (великої кількості обчислюваних блоків). Робота MapReduce складається із двох етапів: Map і Reduce [4].

На етапі Map виконується попередня обробка вхідних даних. Для цього один із обчислювальних елементів кластеру (головний вузол, master node) отримає вхідні дані для розрахунку і розподіляє дані серед робочих вузлів.

На етапі Reduce попередньо оброблені дані обертаються. Основний вузол отримує відповіді від робочих вузлів і на їх основі формує результат - рішення проблеми.

Перевага моделі MapReduce полягає в тому, що вона дозволяє виконувати операції попередньої обробки та згортки паралельно і незалежно, а також горизонтально масштабувати обчислювальну потужність кластера. Операції попередньої обробки діють незалежно одна від одної і можуть виконуватися паралельно (хоча на практиці це обмежується джерелом вхідного сигналу та / або кількістю використовуваних обчислювальних блоків). Аналогічно, група робочих вузлів може конвертувати - для цього потрібно лише те, щоб усі результати попередньої обробки з одним конкретним значенням ключа оброблялися одним робочим вузлом одночасно.

Для роботи багатокритеріального методу виявлення DDoS-атак необхідно провести попередній аналіз та розрахунки: визначити показники (критерії), за якими буде ідентифіковано наявність або відсутність атаки; побудувати модель для звичайного мережевого трафіку; встановити пороги для вибраних показників.

В якості критеріїв оцінки були обрані наступні показники:

- рівень завантаження процесора сервера;
- обсяг зайнятої оперативної пам'яті сервера;
- розмір упаковки;
- поточний рівень трафіку (Мбіт / с);

- розподіл значення адреси джерела запитів (source ip);

- користувач-агент у запиті;

- URI (ієрархічна частина та фрагменти URL-адреси запиту);

Наявність атаки потоку HTTP GET flood може характеризуватися кількістю запитів від джерела за секунду [4]. Зрозуміло, що законний користувач не постійно робить велику кількість запитів на один і той же ресурс, як це може вузол, керований зловмисником (зомбі). Тому деякий час *A*t надходить з IP-адреси джерела x надходить s. запитів.

Для цього необхідно правильно визначити початкову точку атаки. Це дозволить класифікувати весь попередній трафік як законний та відкриє додаткові можливості для розподілу змішаного трафіку, що надходить після атаки, на законний та шкідливий [5]. У цьому випадку метод виявлення шкідливого трафіку, у першому наближенні, буде зведений до наступних етапів:

1. Визначте поточні сезонні періоди.

2. Беручи до уваги сезонність, визначте початкову точку нападу.

3. Ми відносимо весь попередній трафік до початку атаки до законного.

4. Класифікуємо змішаний трафік на законний та шкідливий.

5. Порівняйте законний трафік, вибраний із змішаного, з трафіком, отриманим до атаки.

6. На основі результатів, отриманих на попередньому кроці, та розроблених критеріїв успіху, скоригуємо вибірки.

7. Весь вхідний трафік аналізується на основі отриманих даних.

Серед основних методів можна виділити методи, що базуються на статистичному аналізі. Це допомагає оцінювати різні параметри мережної активності і діагностувати початок атаки або визначати шкідливий трафік.

Основними параметрами, за якими проводиться аналіз, можуть бути:

• Кількість запитів за певний період.

• Швидкість надходження запитів.

• Кількість запитів з певного джерела або з певною мережі.

• Кількість запитів до певного пункту призначення (для вебсервера це конкретний скрипт).

• Час між запитами.

• Інші різні параметри мережевої активності.

За допомогою середньоквадратичного відхилення можна розрахувати допустиму межу для одного з параметрів мережевої активності, наприклад, для кількості запитів за якийсь період часу. У разі якщо межа буде порушена, це стане свідченням початку атаки. Так як в різний час навантаження на мережевий ресурс, так само може бути різною, то для раннього виявлення атаки необхідний постійний моніторинг і перерахунок кордонів для кожного тимчасового кроку. Постійний моніторинг дозволить

визначити атаку, якщо вона почнеться в період невеликої мережевої активності, або, якщо зловмисник шукає потенційно вразливі місця на сервері, проводячи міні- DDOS-атаки і вивчаючи поведінки сервера. У разі якщо верхня межа задана строго і зловмисник проводить міні-атаки в період найменшої мережевої активності, він може не порушувати задану кордон, і його дії будуть не виявлені. Атака буде виявлена тоді, коли зловмисник знайде потенційно вразливе місце, і зробить на нього атаку. Постійний моніторинг активності і перерахунок допустимих меж дозволяє цього уникнути. У період меншою мережевий активності верхня межа знизиться.

Перелік посилань

1. Долішний В.С. Аналіз і моніторинг сучасних DDoS - атак / В.С. Долішний, В.М. Чешун. - Тези доповідей Всеукраїнської науково-практичної конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів "Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка" [Текст] / за заг. редакцією І.В. Толока. – К. : ВІКНУ, 2018. – С. 147 - 148.

2. DDoS Definitions - DdoSPedia, [Електронний ресурс]. http://security.radware.com/knowledge- center/DDoSPedia/http-flood

3. Zinchenko, V. V, Zinchenko, M. V (2017), Viyavlennya ddos-atak prikladnogo rivnya [Detection of application layer DDoS attacks], Mizhnarodna naukovo-tehnichna konferentsiya «RadIotehnichni polya, signali, aparati ta sistemi», Kyiv, pp. 262-264.

4. Системи і методи виявлення вторгнень: сучасний стан і напрями вдосконалення [Електронний ресурс]. URL:http://citfomm.ni/security/ intemet/ids_overview/#3

5. Холявка Є. П.; Метод виявлення мережевих атак в комп'ютеризованих системах управління: наукова робота, Хмельницький національний університет. - Хмельницький, 2019, [Електронний ресурс]. URL: http://konkurs.khnu.km.ua/wp-content/uploads/sites/25/2019/04/ DP3Eugen.pdf

Прогнозування ризиків завадостійкості в телекомунікаційних системах

Хмельницький Ю.В.
Хмельницький національний університет

Більшість сучасних телекомунікаційних систем визначаються значною кількістю параметрів, функціональними можливостями, вимогами до забезпечення захисту інформації, високою надійністю, розгалуженою інфраструктурою. Для якісної та надійної передачі інформаційних даних у телекомунікаційних системах задача забезпечення завадостійкості та захисту