Мета даного дослідження полягала у тому, щоб забезпечити нове джерело випадковості, яким можна доповнити існуючі джерела. Для цього було запропоновано використовувати дані датчиків Android пристрою для отримання високоентропійних даних. Результати показали, що зразки даних містять велику кількість непередбачуваності і мають рівномірний розподіл значень. 256-бітне випадкове число для отримання випадкового ряду отримується близько раз у 50 мілісекунд.

Поєднання отримання даних з високою ентропією з давачів з існуючим апаратом ентропії на основі апаратного забезпечення допоможе захистити користувачів пристроїв Android від вразливостей щодо безпеки.

Література

1. Boaz Barak and Shai Halevi. A model and architecture for pseudo-random generation with applications to /dev/random. In Proceedings of the 12th ACM conference on Computer and communications security, p. 203-212. ACM, 2005.

2. Daniel J Bernstein. The Salsa20 family of stream ciphers. In New stream cipher designs, pages 84-97. Springer, 2008.

3. Jonathan Voris, Nitesh Saxena, and Tzipora Halevi. Accelerometers and randomness: perfect together. In Proceedings of the fourth ACM conference on Wireless network security, pages 115-126. ACM, 2011.

Аналіз аномалій результатів порівняння DDoS-атак поточного стану системи з її нормальним станом

Долішний В.С.
Науковий керівник – к.т.н.,доц. Чешун В.М.
Хмельницький національний університет

Оптимальним рішенням для виявлення початку атаки і подальшого виявлення шкідливого трафіку буде рішення, засноване на проведення аналізу аномалій, в результаті якого відбувається порівняння поточного стану системи з її нормальним станом. Порівняння станів системи в контексті DDoS-атак можна проводити шляхом порівняння різних властивостей мережевої активності. До цих властивостей можуть бути віднесені: кількість запитів, тип запитів, кількість запитів певного типу або протоколу, IP адреса джерела, швидкість надходження запитів, їх час і т.д.

Нехай множина $A\left(a_1, a_2, a_3, ..., a_n\right)$ - набір всіх можливих властивостей для всіх мережевих клієнтів. Множина $B\left(b_1, b_2, b_3, ..., b_m\right)$ - множина легітивних клієнтів конкретного мережевого ресурсу. Кожен мережевий клієнт має набір індивідуальних властивостей. Наприклад, клієнт b_1 має властивості $A1\left(a_4, a_8, a_{10}, a_{14}\right)$, клієнт b_2 має властивості

$A2\left(a_3, a_8, a_{11}, a_{14}\right)$ і т.д. Дані властивості представляють набір підмножин множини *A*. Перетин всіх цих підмножин характеризує клієнтів мережевого ресурсу, за якими вони можуть бути класифіковані. Точно так нелегітивні клієнти матимуть свій набір властивостей, за якими вони також можуть бути класифіковані.

У минулому був популярний засіб протидії DDoS-атакам типу HTTP-flood, що працює на стороні сервера, що атакується і виявляє шкідливий трафік за допомогою аналізу таких властивостей мережевої активності, як тип даних при завантаженні. Справа в тому, що браузер легітивного клієнта при завантаженні вмісту web-сторінки автоматично завантажує додаткові файли, необхідні для нормальної побудови і відображення сторінки. До цих файлів можуть відноситися: зображення, що знаходяться на сторінці, іконки, каскадні сторінки стилів, фрагменти скриптів JavaScript, винесені в окремі файли. Для зловмисника ці файли є непотрібними, його головне завдання - змусити відпрацювати скрипт, що генерує сторінку, і, тим самим, викликати додаткове навантаження на ресурси сервера. Таким чином, комп'ютери зомбі-мережі могли бути ідентифіковані з високою часткою ймовірності з аналізу тільки однієї цієї властивості. Природно, що зловмисники у відповідь на створення даного методу ускладнили алгоритм атаки, і на сьогоднішній день зомбі-комп'ютери намагаються завантажувати і всі супутні дані. На сьогоднішній день DDoS-атаки ускладнюються, і зловмисники намагаються повністю імітувати поведінку легітивних клієнтів. У цій ситуації перевагу при аналізі властивостей мережевої активності необхідно віддати тим властивостям, які не можуть бути підроблені зловмисниками. При нестачі таких властивостей необхідно вводити штучні властивості, наприклад, проходження модифікації тест Тьюринга - введення даних з картинки.

Таким чином, завдання по визначенню і виявлення шкідливих запитів в контексті даної роботи зводиться до їх класифікації на підставі властивостей мережевої активності. Оптимальним рішенням для виявлення шкідливого трафіку є використання різних класифікаторів і нейронних мереж. Складністю в реалізації даного рішення є той факт, що для нормального функціонування класифікатора потрібно мати дві актуальні навчальні вибірки, відповідно шкідливому і легітивному трафіку. Однак до моменту початку атаки отримати ці вибірки не представляється можливим. Це цілком очевидно для вибірки, що відповідає шкідливому трафіку, так як до початку атаки шкідливі запити відсутні. Але це також справедливо і для вибірки, що характеризує легітивний трафік. Так як мережева картина постійно змінюється, буде змінюватися і вміст вибірки відповідного легітивного трафіка. Таким чином, вибірка по легітивності трафіка, наприклад, місячної давності, може бути не актуальна для поточної мережевої ситуації. Крім того, є ризик, що в цій вибірці можуть виявитися дані, відповідні шкідливим запитам, що в подальшому викличе помилки в

роботі класифікатора. Дана проблема дуже актуальна, тому що зловмисник може спеціально почати підмішувати до легітивного трафіку незначне число шкідливих запитів, які не зможуть бути ідентифіковані як початок атаки, але зможуть негативно «навчити» вибірку, що характеризує легітивний трафік.

Для подолання цієї проблеми необхідно точно визначити точку початку атаки. Це дасть можливість весь попередній трафік віднести до легітивного і відкриє додаткові можливості по розділенню змішаного трафіку, який приходить після початку атаки, на легітивний і шкідливий. В цьому випадку методика виявлення шкідливого трафіку, в першому наближенні, буде зводитися до наступних кроків:

1. Визначаємо актуальні сезонні періоди.
2. З урахуванням сезонності визначаємо точку початку атаки.
3. Відносимо попередній перед початком атаки трафік до легітивного.
4. Класифікуємо змішаний трафік на легітивний і шкідливий.
5. Порівнюємо легітивний трафік виділений зі змішаного з трафіком що надійшов до початку атаки.
6. На підставі результатів, отриманих в попередньому кроці і вироблених критеріїв успішності, коригуємо вибірки.
7. Весь трафік, що надходить аналізуємо з урахуванням отриманих даних.

В рамках розробки методики виявлення DDoSатак і шкідливого трафіку розроблений оригінальний алгоритм виявлення на ранніх стадіях точки початку розподіленої атаки, спрямованої на відмову в обслуговуванні. Алгоритм враховує сезонні відхилення в навантаженні, що дає можливість виявляти точку початку атаки на ранніх стадіях і з більшою точністю. Додатково проведено дослідження, спрямоване на підтвердження існування сезонності і виявлення типових сезонних періодів. В результаті дослідження виявлені тижнева, добова і невизначена сезонність і причини її виникнення.

Розроблено методику отримання навчальних вибірок та класифікації трафіку, що надходить, на групи шкідливих і надійних запитів. Для поділу змішаного трафіку використовується алгоритм кластеризації k-means. Вибір даного алгоритму обгрунтований, проведено доказ його ефективності. Для алгоритму підібрані оптимальні характеристики і розмірність даних, вироблені критерії успішності. Розроблені алгоритми складають основу узагальненої методики виявлення DDoS-атак і шкідливого трафіку, яка в загальному вигляді може бути записана так:

1. За допомогою накопичених статистичних даних, визначаємо існуючі сезонні періоди.
2. Для кожного сезонного періоду визначаємо допустиму верхню межу кількості запитів.
3. У разі порушення границі, фіксуємо точку початку атаки.
4. Відносимо весь, що передує початку атаки, трафік до кластеру, відповідному надійному трафіку.

5. За допомогою алгоритму k-means класифікуємо змішаний трафік на надійний і шкідливий.

6. Порівнюємо трафік, що передує початку атаки, з кластером, надійного трафіку, виділеного зі змішаного трафіку.

7. На підставі результатів, отриманих на попередньому кроці, і з урахуванням вироблених критеріїв успішності, коригуємо кластери.

8. Весь трафік, що надходить, аналізуємо з урахуванням отриманих в попередньому пункті результатів.

Література

1. Алферов, А.П. Основы криптографии /А.П.Алферов, А.Ю. Зубов, А.В. Черемушкин. – М.: Гелиос АРБ, 2002. – 480 с.

2. Анин, Б.А. Защита компьютерной информации / Б.А. Анин – Спб.: БХВ-Петербург. 2000. – 384с.

3. Бабаш, А.В. Информационная безопасность. Лабораторный практикум : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - 2-е изд., стер. - М. : КНОРУС, 2016. - 132 с.

4. Бабаш, А.В. Криптографические методы защиты информации : учебник для студ. вузов / А. В. Бабаш, Е. К. Баранова. - М. : КНОРУС, 2016. - 190 с.

Модель формування множини альтернативних структур енергосистеми з альтернативними джерелами енергії

Єлісєєва А.Р. , Бойко О.В.
Науковий керівник - доц. Шендрик В.В.
Сумський державний університет

У роботі розглядається типова енергосистема, у якій джерелами електроенергії є сонячні батареї (СБ) та вітрові турбіни (ВТ). Для підтримки безперервного живлення енергосистема також містить акумуляторні батареї (АБ). У даному дослідженні розглядаються саме ці елементи, так як від них, у першу чергу, залежить рівень електрозабезпечення та ціна системи. Інші елементи енергосистеми при плануванні її структури не розглядаються.

На сучасному ринку існує велика кількість установок сонячної та вітрової генерації електроенергії, що відрізняються потужністю, ціною, габаритами. Це збільшує час на прийняття правильного рішення відносно визначення можливих конфігурацій енергетичної системи з використанням альтернативних джерел енергії (АДЕ).

Важливим питанням є ефективне використання АДЕ, а саме їх комбінація для максимізації отримання генеруючої енергії при мінімізації витрат на їх установку та підтримку. Проблема планування структури таких систем на даний час все більше привертає увагу дослідників.

Мета даної роботи – створення моделі розрахунку робочих