МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет
імені Тараса Шевченка

І МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

"ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ" (PCSITS)

05-06 квітня 2018 року

Київ – 2018

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431
П 78

П78 Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 05-06 квітня 2018 року р.; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова) та ін. – К.: ВПЦ «Київський університет», 2018. – 510с.

Тексти виступів і тез опубліковано в авторській редакції однією з робочих мов конференції: українською, російською, англійською.

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431

Література:

1. Гулак Г.М. Формування вимог щодо забезпечення гарантоздатності автоматизованих систем переробки інформації й управління критично-важливими об'єктами інфраструктури. / Гулак Г.М., Складанний П.М. // II Всеукраїнська науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання» (Одесса, 17 листопада 2017р.). – Одесса: ОДУВС, 2017 – С.12-14.

2. Гулак Г. М. Швидкий алгоритм генерації підстановок багатоалфавітної заміни / Г. М. Гулак, В. Л. Бурячок, П. М. Складанний // Захист інформації. – 2017. – №2. – С. 173–177.

3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие. – М.: Гелиос АРВ, 2005, - 160 с.

4. Духин А.А. Теория информации: Учебное пособие. – М.; Гелиос АРВ, 2007. -248с., ил. ISBN 978-5-85438-168-0

УДК 004.056.5:004.75

Т.А.Радівілова[1], М.Х. Тавалбех[1]

[1]Харківський національний університет радіоелектроніки

tamara.radivilova@gmail.com

tavalbeh@icloud.com

СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ПРИ НАЯВНОСТІ САМОПОДІБНИХ ВЛАСТИВОСТЕЙ ВХІДНОГО ТРАФІКУ

Виявлення вторгнень (атак) - це процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі з метою пошуку ознак можливих інцидентів. Мережеві системи виявлення та запобігання вторгнень (NIDS/NIPS, Network Intrusion detection system/Network Intrusion prevention system) це необхідний елемент захисту від мережевих атак. Найбільш часто використовується розподілена архітектура, в якій кожен датчик NIDS аналізує отриманий трафік на наявність незаконних мережевих дій і, при необхідності, генерує попередження. Вузьким місцем, що впливає на продуктивність мережі, є швидкість обробки вхідних даних мережевим пристроєм безпеки.

Система виявлення вторгнень в мережі фіксує кожен пакет даних в мережі і вимагає багато часу і системних ресурсів для аналізу і зіставлення пакета даних функції будь-якого типу атаки. Мережеві IDPS можуть не виконувати повний аналіз при високих навантаженнях, однак це може привести до того, що деякі атаки не будуть виявлені. Тобто, якщо швидкість виявлення не відповідає швидкості передачі мережевих даних, то система виявлення вторгнень мережі не буде враховувати частину пакетів даних, що вплине на коректність і ефективність системи [1,2].

Однією з важливих проблем є наявність у трафіку самоподібних характеристик і великих викидів, що викликає серйозний дисбаланс навантаження при статичних правилах балансування між розподіленими датчиками, що може привести до втрати пакетів. Отже, розподілена архітектура NIDS повинна поєднуватися з адекватними динамічними механізмами перерозподілу навантаження. Таким чином, критичною проблемою є розробка методу балансування самоподібного навантаження для підвищення пропускної здатності мережевої системи виявлення вторгнень.

У даній роботі пропонується використовувати аналіз вхідного трафіку на наявність фрактальних властивостей і динамічний перерозподіл навантаження між датчиками. Для цього пропонується використовувати балансувальник, який отримує періодичну інформацію про стан датчиків, і на основі політики управління потоками він може здійснювати механізм балансування навантаження для переміщення частини мережевого трафіку з перевантажених датчиків на менш навантажені. В роботі [3] запропоновано модифікований метод балансування навантаження, заснований на обліку часу обслуговування, який враховує ступінь мультифрактальності трафіку. На вхід NIDS надходить трафік (безліч пакетів даних) від клієнтів, які розподіляються між датчиками відповідно до політики поділу трафіку в чергах [1,2].

Запропонований в даній роботі метод може забезпечити рівномірне балансування навантаження в дискретні моменти часу, щоб повною мірою використовувати багатоядерні/багатопотічну

сність, що призводить до більш ефективного використання системних ресурсів при обробці даних для виявлення вторгнень.

Даний метод складається з наступних операцій.

1. Від клієнтів приймається безліч пакетів даних. Пакети даних обов'язково містять тип протоколу і властивість протоколу. Типи протоколів даних включають в себе протоколи TCP, UDP, STCP, ARP, ICMP, IGMP та інші. Властивості протоколу пакетів даних містять IP-адресу джерела, порт джерела, IP-адресу призначення і порт призначення.

2. Пакети, що прибули, балансуються на датчики відповідно до швидкості їх прибуття протягом заданого періоду часу T. Може застосовуватися балансування за будь-яким обраним алгоритмом. Далі пакети даних обробляються процедурою поділу, яка класифікує їх в потоки пакетів даних за типом обслуговування шляхом ідентифікації заголовків пакетів, що прибули, відповідно до типу і властивості протоколу.

3. Для кожного потоку обчислюються мультифрактальні параметри і відношення кількості сигнатур для кожного типу потоку до загальної кількості сигнатур.

4. Балансувальник аналізує пакети, що прибули, в заздалегідь визначені періоди часу. Обчислює відношення кількості пакетів для кожного типу обслуговування до загальної кількості пакетів, що прибули, за заданий період часу. Далі балансувальник оцінює час порівняння пакетів з сигнатурою і час обробки для конкретної послуги, на основі параметрів мультифрактальності і відношення кількості сигнатур для кожного типу потоку до загальної кількості сигнатур.

5. Виконується процедура виявлення вторгнень відповідно до набору сигнатур. Оцінюється середній час глибокої перевірки пакетів DPI, відповідних конкретній послузі і сортується в порядку убування. Генерація першого списку послуги, які мають середній час DPI, яка дорівнює або перевищує заданий рівень. Генерація другого списку послуги, які мають середній час DPI менше заданого рівня відповідно.

6. Ініціація включення зміни правила балансування. Відбувається, коли виконується задана умова, що впливає на загальний час DPI NIDS. Зняття статистики часу роботи, яка

необхідна для порівняння сигнатур з пакетом для кожного типу послуги.

7. Створення нового правила балансування навантаження. Воно може періодично змінюватися в залежності від результату аналізу трафіку. Правило створюється на основі оцінки середнього значення DPI. Згідно з новим правилом балансування навантаження пакети для кожного типу послуги, що включені в перший список послуги, призначаються на певні компоненти NIDS, а пакети для типів послуги, що включені у другий тип послуги, призначаються для обробки інших компонентів NIDS.

8. Після аналізу підпису правило балансування навантаження оновлюється. Балансування навантаження виконується відповідно до оновленого правила балансування навантаження.

9. Проведення балансування пакетів, що прибули, в наступний заданий період часу 2T на декількох ядрах і компонентах NIDS з використанням сформованого нового правила балансування на основі результату аналізу пакетів прибули в заданий період часу T.

10. Моніторинг подій перевищення заданого рівня трафіком, що надходить, або закінчення заданого часу балансування навантаження до аналізу пакетів, які прибули в період часу 2T. Обробка та аналіз пакетів NIDS з використанням оновленого правила балансування навантаження.

11. Здійснення наступного балансування відповідно до операцій 2-10.

Запропонований в роботі метод враховує ступінь мультифрактальності трафіку для розрахунку часу DPI, на основі якого обчислюється час, необхідний для порівняння пакета з сигнатурами, збирає статистику часу роботи, здійснює генерацію і оновлення правил балансування пакетів, що прибувають. Таким чином, пропонований метод покликаний забезпечити високу швидкість і точність визначення вторгнень при якісному балансуванні входного навантаження.

Література:

1. Xiao-Qian Li. Load balancing method for Network Intrusion Detection /Xiao-Qian Li, Tom Chen// United States Patent Application Publication. - №US 2010/0246592 A1. – 2010.

2. Yoon-ho Choi. Load balancing method and apparatus in Intrusion Detection Sysytem /Yoon-ho Choi, Seung-Woo Seo, Bon-Hyun Koo and Hye-Jung Cho// United States Patent Application Publication. - №US 2017/0295191 A1. – 2017.

3. L. Kirichenko. Analyzes of the distributed system load with multifractal input data flows /L. Kirichenko, T. Radivilova// CADSM, Lviv. – 2017. – Pp. 260-264.