УДК 004.72
Морозов Б. – ст. гр. СКмз-61
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ МЕТОДІВ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Науковий керівник: ст. викладач Маєвський О.В.

Morozov B.
Ternopil Ivan Pul`uy National Technical University

RESEARCH METHODS OF ANALYZING NETWORK TRAFFIC

Supervisor: Majevskiy A.

Ключові слова: мережевий трафік, аномалія, виявлення, метод, аналіз
Keywords: network traffic, anomaly, detection, method, analysis

Швидкий розвиток мереж і їх об'єднання в мережу Інтернет призвів до зростання числа порушень принципів інформаційної безпеки.

Аналіз останніх досліджень показав, що основним недоліком переважної кількості сучасних комерційних систем виявлення атак є низька, близька до нуля, ефективність виявлення невідомих атак.

Розуміння природи аномалій трафіку у мережі є актуальним питанням. Незалежно від того, шкідливими чи ні є аномалії, важливо проаналізувати їх з двох причин:

– аномалії можуть створювати перевантаження в мережі і підвищити використання ресурсів маршрутизаторів, що робить виявлення цих аномалій вкрай важливим;

– деякі аномалії не обов'язково впливають на мережу, але вони можуть мати серйозний вплив на клієнта або кінцевого користувача.

Проведемо класифікацію методів виявлення аномалій мережевого трафіку.

Кластерний аналіз. Суть даної групи методів полягає в розбитті множини спостережуваних векторів-властивостей системи на кластери, серед яких виділяють кластери нормальної поведінки.

Статистичний аналіз. Дана група методів використовує побудову статистичного профілю поведінки системи протягом деякого періоду «навчання», при якому поведінка системи вважається нормальною.

Нейронні мережі. Нейронні мережі для виявлення аномалій навчаються протягом деякого періоду часу, коли вся спостережувана поведінка вважається нормальною.

Експертні системи. Інформація про нормальну поведінку представляється в подібних системах у вигляді правил, а спостережувана поведінка у вигляді фактів.

Імунні мережі. Виявлення аномалій є одним з можливих додатків імунних методів. Так як кількість прикладів нормальної поведінки звичайно на порядок перевищує число прикладів атак, використання імунних мереж для виявлення аномалій має велику обчислювальну складність.

Розглянемо методи виявлення аномалій мережевого трафіку, що використовують нейронні мережі та математичний апарат вейвлет-аналізу більш детально.

Штучна нейронна мережа (ШНМ) є математичною (а також програмною або апаратною) моделлю, побудованою за принципом організації та функціонування біологічних нейронних мереж. Сьогодні існує кілька архітектур штучних нейронних мереж, які з успіхом застосовуються для вирішення складних технічних і економічних завдань. Деякими з особливостей ШНМ є здатність в процесі навчання виявляти складні залежності між вхідною і вихідною інформацією. Нейронні мережі мають ряд переваг, які вигідно відрізняють їх від традиційних рішень, а саме високу ступінь паралелізму обробки інформації; здатність до узагальнення; адаптацію до змін навколишнього середовища; розпізнавання зашумлених образів; низький рівень ресурсоємності.

Для виявлення аномалій мережевого трафіку можна використати метод на основі кореляційного аналізу IP-адрес призначення вихідного трафіку на виході маршрутизатора. Для ефективного виявлення аномалій за допомогою статистичного аналізу кореляція адресних даних здійснюється за допомогою дискретного вейвлет-перетворення.

Спочатку обчислюється кількість рівнів вейвлет-розкладу сигналу як двійковий логарифм від кількості розбиттів сигналу. Потім обчислюються початкові значення апроксимуючих коефіцієнтів, використовуючи значення трафіку, що були записані в масиві і викликається підпрограма вейвлет-перетворення Хаара, яка обчислює апроксимуючі та деталізуючи коефіцієнти різних рівнів розкладу мережевого трафіку.

Далі здійснюється зворотне вейвлет-перетворення, за допомогою якого відбувається реконструкція сигналу, а також визначення аномальної і трендової складової сигналу. Значення аномальної складової дозволяє встановити наявність атаки на комп'ютерну мережу.

З проведеного дослідження можна зробити висновок, що використання вейвлет-аналізу для виявлення атак на комп'ютерну мережу вимагає меншого часу, ніж нейронних мереж, проте останні, за рахунок можливості навчання, дозволяють виявити всі відомі атаки.

Література

Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / Соколов А.В., Шаньгин В.Ф. – М. : ДМК Пресс, 2002 – 656 с.

Куссуль Н.Н. Нейросетевая модель пользователей компьютерных систем / Куссуль Н.Н., Сидоренко А.В., Скакун С.В. // Кибернетика и вычислительная техника. – 2004.

Петухов А.П. Введение в теорию базисов всплесков / А.П. Петухов. – СПб.: Изд-во СПбГТУ, – 1999. – 132 с.

УДК 004.73; 004.77

Острожинський С. – ст. гр. СНмз-61
Тернопільський національний технічний університет імені Івана Пулюя

ПРО ПОНЯТТЯ «СОЦІАЛЬНІ МЕРЕЖІ»

Науковий керівник: ст. викладач Маєвський О.В.

Ostrozyns'kyy S.
Ternopil Ivan Pul`uy National Technical University

CONCEPT OF "SOCIAL NETWORK"

Supervisor: Majevskiy A.