УДК 004.42

**РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ АНОМАЛІЙ**

**ДЛЯ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ**

*Півторайко І. В., науковий керівник д. т. н., професор Лахно В. А.*

Швидкий розвиток і широке використання систем стільникового зв'язку супроводжується розвитком загроз для їх безпеки. Застосування поширених сигнатурних методів, для попередження загроз, не дає бажаних результатів. У статті запропоновано структурну схему системи виявлення аномалій в мережах операторів стільникового зв'язку (СОСС). На основі аналізу типів даних і існуючих методів виявлення вторгнень була запропонована модель гібридної системи виявлення аномалій в СОСС. Наведено загальну структуру і логіка гібридної системи. Обґрунтовано і обраний метод виявлення аномалій в СОСС. Представлений покроковий алгоритм виявлення аномалій в СОСС.

Однією з галузей, де виявлення аномалій є дійсно актуальною проблемою, є телекомунікаційна сфера, а саме - мережі операторів стільникового зв'язку. Сигнатурні методи виявлення загроз не дозволяють вчасно виявити витік трафіку, оскільки це не є прямою атакою на мережу оператора. Факти такої кражі трафіку можна виявити вже постфактум, що приносить значні збитки компаніям [1].

Виявлення аномалій в залежності від типів даних класифікується як:

1. Host-based (моніторинг вузла мережі).

2. Network-based (власне моніторинг мережі). Network-based моніторинг зазвичай виконується з даними типу мережевого трафіку, пакетів даних і т.д.

У зв'язку з дослідженнями в області стільникового зв'язку, в мережах найбільших операторів досі перебуває істотна частка мобільних апаратів, які або зовсім не мають операційних систем нового покоління (Android, iOS, Windows Phone), або ці системи вже є застарілими і не мають перспектив розвитку (Symbian, Bada OS). Проблема таких пристроїв полягає в тому, що їх обчислювальної потужності не вистачить для участі в Host-based системі. Тому логічним рішенням є розробка системи з використанням Network-based підходу. Загальна структура системи зображена на рис. 1.



Рис. 1. Загальна структура гібридної системи

На вхід системи подається трафік, який паралельно аналізується двома модулями - Misuse Detection (виявлення сигнатури) і Anomaly Detection (виявлення аномалій). У разі, якщо загроза виявляється тільки модулем сигнатурного виявлення - на вихід системи подається сам факт наявності загрози і її опис відповідно до баз даних. Якщо загроза виявляється тільки модулем виявлення аномалій - на виході буде лише сам факт загрози. Якщо загрози не виявлені дані відзначається як нормальні.

В якості модуля Misuse Detection доцільно використовувати open-source утиліту Snort, яка працює на операційних системах Windows, так і Linux [2].

Snort - це система виявлення вторгнень (СВВ), яка є надзвичайно потужним інструментом, навіть в порівнянні з комерційними СВВ. Багато користувачів в активному співтоваристві Snort діляться їхніми правилами безпеки, що може стати в нагоді, якщо потрібно мати найсучасніші правила.

Snort може бути запущений в 4 режимах:

* Sniffer mode (режим перехоплювача) - зчитування мережевого трафіку і виведення його на екран.
* Packet logger mode (режим збору логів) - запис мережевого трафіку в файл.
* IDS mode (режим СВВ) - мережевий трафік, який відповідає правилам безпеки записується.
* IPS mode (режим системи запобігання вторгнень) - модифікований варіант попереднього режиму. Він приймає пакети від фаєрвола, порівнює їх з сигнатурними правилами і ставить мітку «відкинути» в разі якщо пакети відповідають правилу.

В якості модуля Anomaly Detection можна використати метод Decision Tree. Decision Tree - широко використовуваний в аналізі даних метод. Він є потужним інструментом для класифікації і передбачення. Метою є створення моделі, яка передбачає значення цільової характеристики, базуючись на декількох вхідних характеристиках. На рис. 2 зображено загальну схема Decision Tree.

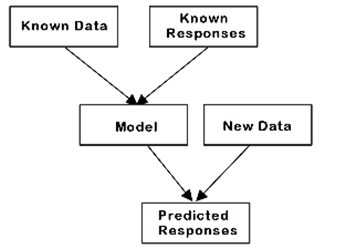


Рис. 2. Загальна схема Decision Tree

Схема відображає багатокроковий процес, на кожному етапі якого виконується бінарне рішення. Дерево складається з вузлів, які діляться на внутрішні і термінальні гілки. Внутрішні вузли поділяються на два дочірніх. Кожному внутрішньому вузлу відповідає одна з вхідних характеристик, а дочірні вузли містять кожне можливе значення для цієї характеристики. Термінальні вузли містять мітку класу, з яким вони асоціюються, наприклад, спостереження, які відповідають конкретному термінальному вузлу. Для використання Decision Tree, в якості вхідних даних потрібно надати вектор характеристик. Якщо значення характеристики погано визначено, тоді рішення переходить на лівий дочірній вузол. Якщо добре визначено переходить до правого. Процес триває, поки не буде досягнутий один з термінальних вузлів і мітка часу, яка відповідає термінальному вузлу, буде призначена шаблоном.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Мюрей A. Виявлення новизни з використанням продуктів простих експертів - потенційна архітектура для вбудованих систем / A. Мюрей. – New York: Neural Networks, 2001. – P. 1257-1264.
2. Чен Х. Бізнес-аналітика та аналітика: від великих даних до великого впливу / Х. Чен // MIS Quarterly. – 2012. – No.36(4). – P 1165-1188.