**Тема:** Концептуальная модель СОВ на основе принципов самозащиты.

**Актуальность:** Ну здесь что нибудь можно написать. Например, обзор Secuirity Lab на проблему защиты сети (и так понятно, что проблема актуальна).

Обзор (по СОВ): И вот здесь у меня встает вопрос: «Что же рассматривать?». У меня есть обзор СОВ. Есть обзор правил СОВ. И обзор методов построения правил СОВ.

Тут у меня есть идея с объединением классифиаций (далее представлены сами классифкации).

Классификация СОВ (сделана по литературе):



Классификация правил:



Классификация методов построения правил:



Вообще говоря было бы правильней сказать, что мы делаем именно классификацию СОВ. Ведь с математической точки зрения такое понятие, как правило определяется именно подходом к построению правил (обнаружению атак). То есть, СОВ можно классифицировать по принципу действия, по расположению сенсоров, а так **же по способу обнаружения атак**. То есть СОВ на базе сигнатурных методов анализа и СОВ на базе методов выявления аномалий (в дополнение можно еще и смешанные методы).

Ну а отсюда и вывод, что понятие правила с математической точки зрения зависят от типа СОВ. Так, например, в методе сравнения с эталонным значением, правило – это де факто определенные сигнатуры и инструкция, которую следует исполнить при совпадении информационного потока с сигнатурами. Отталкиваясь от этого можно определить правило для данного типа СОВ так:

|  |  |
| --- | --- |
| , где | (1) |

– очередное правило;

– действие, определяющее правило;

– множество сигнатур, определяющих правило.

**Цель**: Повышение эффективности или защищенности?

Вот здесь все-таки хотелось бы акцентировать свое и ваше внимание на вопросе того, что мы планируем сделать.

**На консультации вы предложили идею сделать СОВ, которая определяла бы атаку на саму себя. В аспекте атак на отказ в обслуживании.**

**Изначально же мы планировали сделать механизм самообучения для СОВ, то есть СОВ сама бы правила себе строила в случае новой атаки.**

Вы предложили идею анализировать состояние сети, и, отталкиваясь от изменения состояния (анализ уязвимостей и анализ состояния сети), создавать новое правило некоторым генератором.

Таким образом, получается, что мы как бы смешиваем два метода обнаружения вторжений. То есть берём за основу СОВ с сигнатурными методами анализа и дописываем (добавляем) к ней некоторый модуль, который при выявлении аномалий в работе сети отталкиваясь от какого-то метода распознавания «новых» образов генерирует правила (действие + сигнатура) для новой атаки (то есть метод выявления аномалий). Далее приведена схема и ее описание (в том числе математической).



Рисунок 11 – Схема работы СОВ с элементами самообучения

На рисунке мы видим несколько информационных потоков. Это информационные входные и выходные потоки x и x’. Поток, показывающий состояние сети Y. И поток Z предпринимаемых СОВ действий. На рисунке блоками схематично изображены составляющие сети. F – это FireWall, LAN – это локальная сеть, АУ – анализатор уязвимостей, IDS – система обнаружения вторжений, ADMIN – администратор сети.

На входе сетевой IDS есть множество X, которое описывается всеми множествами трафика, поступающими на вход IDS в соответсвии с выбранным расположением. Например:

X = {Xin, X’in, Xdrop-in, Xout, X’out, Xdrop-out}, где (2)

Xin – подмножество входящего трафика, принимаемого фильтрами IDS до файрвола;

X’in – подмножество входящего трафика, поступающего на фильтры IDS после прохождения через фильтры файрфола;

Xdrop-in – подмножество входящего трафика, отсеянного фильтрами Firewall;

Xout – подмножество исходящего трафика, принимаемого фильтрами IDS до файрвола;

X’out – подмножество исходящего трафика, поступающего на фильтры IDS после прохождения через фильтры файрфола;

Xdrop-out – подмножество исходящего трафика, отсеянного фильтрами Firewall.

То есть у нас есть входной поток X и X’(или множество потоков X). От этого потока зависит выходной поток Z. Известно, что для исполнения инструкции необходимо что бы поток соответствовал некоторой сигнатуре. Таким образом, выходной поток зависит так же от правил работы.

|  |  |
| --- | --- |
| , где | (3) |

– то – есть множество заданных правил проверки потока

При этом мы знаем, что правило по формуле 2 определено как множество сигнатур и выполняемое при совпадении действие. Но что если правило для данного потока не задано.

Пусть в некоторый момент времени t на вход поступил неизвестный информационный поток X. Для этого потока pi – это неизвестная величина. Следовательно, после проверки потока по правилам, которые настроены в СОВ, Z так же будет неизвестным.

Так как уже предусмотрено, что состояние сети можно проанализировать, то можно ввести некоторую функцию, которую назовем функцией создания правила.

|  |  |
| --- | --- |
| , где | (4) |

Y – состояние сети после воздействия на него некоторого потока.

Тогда в момент времени t+1 к множеству правил p в момент времени t, будет добавлено новое правило, которое можно вычислить по формуле 4.

Следовательно, в момент времени t+1 множество правил p определяется следующей зависимостью.

|  |  |
| --- | --- |
|  | (5) |

При этом в момент времени t система так же будет зависеть от функции определения правила.

|  |  |
| --- | --- |
|  | (6) |

Ну это собственно и есть правила и система генерации правил (то – есть вот вам модель и математика самообучения). Здесь мы уже говорим, что f1 нам известная функция. А вот f2 – это как раз функция, описывающая метод создания правил для СОВ.

Теперь вернемся к вопросу самозащиты от DOS. Везде в литературе говорится, что DoS и DDoS атака – это одна из главных проблем СОВ. Суть в самой работе СОВ. СОВ анализирует весь сетевой трафик, а, следовательно, любая DoS атака на сеть (а точнее, на любой из ее компонентов) будет по умолчанию направлена и на саму СОВ (так как сенсоры СОВ собирают весь сетевой трафик).

Поэтому да, ваше предложение по поводу анализа состояния самой СОВ тоже вполне логично. Даже если DoS будет направлен на Firewall, то из-за особенностей самих СОВ, DoS так же направлен и на СОВ.

Вывод: нужно контролировать загруженность СОВ. Если СОВ доходит до порога загруженности, значит ее атакуют.

Но мне кажется, что стоит так же рассматривать ситуацию просто большой нагрузки на сеть (ну например, резко возросла популярность товара, который продается на сайте). Не будет ли в этом случае правомерная нагрузка на сеть воспринята как DoS атака. Поэтому, стоит все-таки не считать резко возросшую нагрузку DoS-атакой априори, а провести анализ. Математику я уже предложил. Хотя я не уверен на все 100, что она правильная, но там все вполне логично и закономерно.

Ну а контроль доступного для СОВ ресурса из общего с целью не допустить перегрузки системы – идея хорошая, а если это будет делать сама СОВ (то есть фильтры с ограничением), то вообще хорошо.

Правда тут может возникнуть еще одна заковырка, как мне кажется… Не будет ли в таком случае сама СОВ отставать от реального сетевого трафика?

**Что касаемо обзора методов повышения эффективности, пока рассмотрел 2 статьи, сей час еще одну нашел.**