Модель обнаружения вторжений

курс: "Обнаружение нарушений в сети"

Нестеренко В.А.

Модель предложена **Дороти Деннинг**

D. E. Denning. An intrusion detection model. *IEEE Transactions on Software Engineering, SE-13, 1987, 222-232.*
URL: http://www.cs.colostate.edu/~cs656/reading/ieee-se-13-2.pdf

- Модель является отправным пунктом при построении практически любой системы обнаружения вторжений.
- Модель независима от любой специфической системы, прикладной среды окружения, уязвимости системы или типа вторжения.
- Модель описывает структуру экспертной системы обнаружения вторжения общего назначения.

В основе модели лежит гипотеза:

Использование уязвимостей системы проявляется в аномальном (нетипичном) поведении системы.

Примеры:

- *Отказ в обслуживании (Denial-of-Service)* – поведение, проявляющееся в монополизации ресурса (например, сети), может иметь аномально высокую активность в отношении этого ресурса.
- *Попытка взлома (Attempted break-in)* –попытка взлома системы может сопровождаться большим количеством отказов в принятии пароля для отдельной учетной записи.
- *Троянский конь (Trojan horse)* - поведение программы с установленным троянским конём может отличиться от обычной программы по загруженности CPU или интенсивности операций ввода/вывода.
- *Вирус (Virus)* - вирус, установленный в системе, мог бы привести к увеличению частоты перезаписи исполнимых файлов используемых как вирусные распространители.

Компоненты модели:

Субъекты – источники активности в системе: процессы, сама система, пользователи или процессы, инициализированные пользователями.

Объекты – точка приложения активности субъектов: программы, файлы, устройства, отчёты, ...

Записи аудита системы (логи) – записи генерируемые системой при воздействии субъекта на объект: вход в систему, доступ к файлу, выполнение команды, ...

Профиль активности описывает поведение данного субъекта по отношению к объекту.

Записи об аномалиях – создаются при обнаружении аномального поведения системы.

Правила активности – реакция системы обнаружения нарушений.

Записи аудита **-** фиксирует воздействие субъекта на объект.

Структура записи:
<Subject, Action, Object, Exception-Condition, Resource-Usage, Time-stamp>

- Subject – субъект;
- Action – воздействие субъекта на объект;
- Object – объект;
- Exception-Condition – передаваемый системе код завершения (должен соответствовать предусмотренным в системе случаям обработки исключений).
- Resource-Usage – список, каждый элемент списка характеризует использование некоторого ресурса: время использования процессора, количество чтений из файла, количество записей в файл и т.п. ;
- Time-stamp – время события;

Пример: копирование пользователем **User** файла **file1** в **file2:**

(User, execute, COPY.EXE, O, CPU=00002, 11058521678) - системный вызов функции копирования;

(User, read, file1, O, RECORDS=0, 011058521679) - чтение файла **file1;**

(User, write, file2, write_viol, RECORDS=O, 11058521680) - запись в файл **file2** (операция привела к нарушению защиты).

Профиль активности - поведение данного субъекта по отношению к объекту. Поведение описывается в терминах метрики и модели активности.Конкретные значения, полученные в рамках введённой метрики, используются совместно с моделью активности для нахождения аномальных событий.

Структура профиля:

<Variable-Name, Action-Pattern, Exception-Pattern, Resource-Usage-Pattern, Period, Variable-Type, Threshold, Subject-Pattern, Object-Pattern, Value>

- Variable-Name – имя переменной, соответствующей наблюдаемой величине;
- Action-Pattern – операция (‘login’, ‘read’, ‘execute’, …);
- Exception-Pattern – код завершения;
- Resource-Usage-Pattern – используемый ресурс;
- Period – интервал измерения;
- Variable-Type – абстрактный тип данных, определяет тип используемой метрики и модели активности;
- Threshold – параметр модели активности, задаёт критерий аномалии;
- Subject-Pattern – субъект;
- Object-Pattern – объект;
- Value – текущие значения наблюдаемой величины;

Профиль активности должен однозначно идентифицироваться именем переменной, субъектом и объектом.

Пример записи профиля:

Variable-Name:	SessionOutput
Action-Pattern:	‘logout‘
Exception-Pattern:	0
Resource-Usage-Pattern:	amount
Period:	
Variable-Type:	ResourceByActivity
Threshold:	4
Subject-Pattern:	User
Object-Pattern:	*
Value:	

Структура профиля может быть создана администратором системы безопасности или автоматически создаваться при первом использовании объекта субъектом.

Записи об аномалиях - фиксируют аномальное поведение системы.

В соответствии с правилами активности система обнаружения вторжений создаёт запись профиля активности и производит проверку относительно аномального поведения.

Запись об аномальном событии:

<Event, Time-stamp, Profile>

- Event – событие, предшествовавшее выявлению аномалии;
- Time-stamp – время выявления аномалии;
- Profile – профиль активности, соответствующий выявленной аномалии.

При необходимости система обнаружения вторжений может добавить дополнительные поля к профилю активности.

Правила активности **-** реакция системы обнаружения нарушений.

Специфицируют действие, выполняемое при удовлетворении некоторых условий (запись аудита, генерации записи об аномальном событии, завершение временного интервала).

Правила активности состоят из двух частей: условия и тела (действия).

Условия проверяются посредством следующих правил:

- Правило записи аудита.
- Правило периодической проверки активности.
- Правило аномальных записей.
- Правило периодической проверки аномалий.

Метрика и модель активности.

Центральным пунктом системы обнаружения вторжений являются используемые метрика и модель активности.

Метрика позволяет получить количественную меру состояния системы в соответствии с теми её характеристиками, которые имеют отношение к задаче выявления вторжений.

Модель активности системы предназначена для получения значений метрики соответствующих нормальному (легитимному, типичному) состоянию системы.

Типы метрик:

- Счётчик событий – число записей аудита удовлетворяющих некоторым условиям в течение заданного интервала времени. Например, количество пакетов поступивших в течение одной секунды.
- Временной интервал – промежуток времени между двумя событиями. Например, время между двумя входами пользователя в систему.
- Мера (величина) ресурса – “количество ресурса” измеренное в соответствующих единицах. Например: объём используемой оперативной памяти, количество одновременно открытых файлов, объём отправленной информации.
- ...

Модели активности

1. Операционная модель.

Модель базируется на допущении о том, что аномалия может быть выявлена при сравнении нового наблюдения величины с фиксированным пределом.

Модель применима в тех случаях, когда эксперименты показывают, что некоторые значения метрики обычно соответствуют вторжениям. Например, пароль неверно был неверно введён более трёх раз подряд.

Модели активности

2. Модель среднего значения и стандартного отклонения.

Новое наблюдение X_n будет аномальным, если выходит за пределы доверительного интервала $\bar{X} \pm d \cdot \sigma_x$.

Например. В соответствии с неравенством Чебышева: $P\left\{\left|X_{n+1} - \bar{X}\right| \geq d * \sigma_X\right\} \leq 1/d^2$ Это означает, что для любого вида распределения и при значении параметра $d = 3$ вероятность выйти за пределы доверительного интервала не превышает 0.111.

Модели активности

3. Многовариантная модель. Модель базируется на корреляциях между несколькими метриками. Например, загрузка процессора и частота обращения к устройствам ввода/вывода, количество входов в систему и длительность сеанса и т.д.

4. Модель Марковского процесса. *В* модели вводится матрица переходов, описывающая частоту переходов между состояниями. Событие определяется как аномальное, если вероятность его появления (в соответствии с предыдущим состоянием и матрицей переходов) мала. Эта модель может быть полезна при анализе событий в том случае, когда важна их последовательность.

5. Модель временных рядов (серий). Модель использует временной интервал совместно с мерой ресурса или счётчиком событий, учитывая величину и время появления событий. Событие считается аномальным, если вероятность его появления в данный момент времени мала.