Оценка защищенности архитектур распределенных информационных систем

Писковский Виктор Олегович

План

1. История вопроса
2. Пуассоновский процесс
3. Пример архитектуры

История вопроса

Пример:

- 100 узлов (АРМ и серверы)
- Full mesh (каждый с каждым)
- Вероятность соединения - Пуассоновский процесс (λ=0,1)

ОЦЕНКА ЗАЩИЩЕННОСТИ В БЕЗОПАСНЫХ АРХИТЕКТУРАХ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ,
А. А. Грушо и другие
Системы и средства информатики, 2016. т.26. № 4, стр. 31-37

История вопроса

Пример:

За 10 единиц времени в среднем реализуется одно соединение каждого узла с каждым, или около 10 тысяч в сети (9900 или 4950, в зависимости от модели)

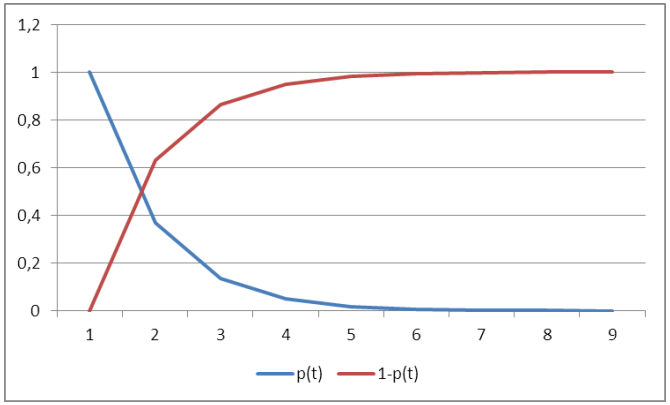
$$\begin{bmatrix} h_1 & \cdots & h_{100} \\ \vdots & \ddots & \vdots \\ h_{100} & \cdots & 1 \end{bmatrix}$$

Пуассоновский процесс

Свойства:

- Независимость: $p(0,t_1)\cdot p(0,t_2)=p(0,t_1+t_2)$
- Простота: $p(0,t)=e^{-\lambda t}$ - вероятность того, что следующее событие наступает позже, чем за время *t,* то есть время до следующего события *1-p(0,t)*

t	p(t)	1-p(t)
0	1	0
1	0,367879	0,632121
2	0,135335	0,864665
3	0,049787	0,950213
4	0,018316	0,981684
5	0,006738	0,993262
6	0,002479	0,997521
7	0,000912	0,999088
8	0,000335	0,999665



https://intuit.ru/studies/courses/966/522/lecture/11779
https://ru.wikipedia.org/wiki/Процесс_Пуассона

Предположения

Для утечки информации необходимо иметь:

- ✓ Сетевую связность от системы обработки или хранения информации к внешним узлам
- ✓ Маршрут, допускающий такую передачу

Предположим:

- ✓ невозможность использования неконтролируемых гипервизоров, руткитов, уязвимостей
- ✓ Имеются только разрешенные взаимодействия

Определения

Оценка защищенности - это оценка возможностей противника в реализации угроз.

Реализация угроз связана с взаимодействием компонентов.

Анализ защищенности = анализ взаимодействий компонентов.

Метод решения - политики безопасности MLS (multilevel security)

Политика безопасности - набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение информации

Определения

Оценка защищенности - это оценка возможностей противника в реализации угроз.

Реализация угроз связана с взаимодействием компонентов.

Анализ защищенности = анализ взаимодействий компонентов.

Метод решения - политики безопасности MLS (multilevel security)

Политика безопасности - набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение информации

Определение

- Конфликт:
  - неразрешенный поток
  - запрет на разрешенный поток
  - пропуск сбоя

Примечание: Сбой для ПКС коммутатора – нет соответствующего правила в таблицах коммутации, инициируется запрос *Packet-In* контроллеру

Требования к системе

- Перечисление информационных потоков и анализ их содержания

Пример

Дано:

- Множество атрибутов безопасности $\{A_1, \ldots, A_m\}$
- Задача B -> D(B) – приложение верификации атрибутов безопасности
- Корневое дерево R:
  - корень B_0 – компонент управления ОВС, включая мониторинг и регистрацию сбоев
  - Ветви – информационные потоки

Утверждение 1

- Дерево R – полурешётка
- Информационный обмен – только по ребрам R в соответствии с $D(B_i)$

Утверждение 1

В рамках современной ОВС с D(B) и корневым дерево R не может быть конфликтов.

Доказательство:

1) неразрешенный поток невозможен оп определению

2) запрет на разрешенный поток вызывает нарушения протокола взаимодействия между B_i и B_j, как следствие ошибочную диагностику, передаваемую в B_0

3) Регистрация сбоев в B_0 – функционал по определению B_0

Утверждение 2

Утверждение 2

Если справедливо Утверждение 1, то топология R - полурешётка (древовидный граф).

Доказательство:

От обратного. Если не полурешётка, то возможен альтернативный путь между B_i и B_j, а следовательно - рассинхронизация данных, нарушение целостности данных, то есть сбой, при отсутствии регистрации сбоя.

Структуры в защите информации. Модель решетки ценностей

SC – частично упорядоченное множество относительно бинарного отношения ≥:

∀ A, B, C:

1) рефлексивность: $A \leq A$
2) транзитивность: $A \leq B, B \leq C \Rightarrow A \leq C$
3) Асимметричность: $A \leq B, B \leq A \Rightarrow A=B$

Грушо А.А., Э.А. Применко, Е.Е. Тимонина, Теоретические основы компьютерной безопасности, Издательский центр «Академия», 2009, 270 стр.

Структуры в защите информации. Модель решетки ценностей

Определение

Для ∀ A, B ∈ SC: C=A + B – наименьшая верхняя граница, если

1) A ≤ C, B ≤ C
2) A ≤ B, B ≤ D ⇒ C≤D ∀D ∈ SC

Определение

Для ∀ A, B ∈ SC: C=A x B – наибольшая нижняя граница, если

1) E ≤ A, E ≤ B
2) D ≤ A, D ≤ B ⇒ D≤E ∀D ∈ SC

Структуры в защите информации. Модель решетки ценностей

Определение

(SC, ≤) – решетка,

если ∀ A, B ∈ SC ∃ $A + B$ ∈ SC и ∃AxB ∈ SC

Лемма

∀ $S = \{A_1, \dots, A_n\}$, A_i ∈ SC

∃$(+)S = A_1 + \cdots + A_n$ – наименьшая верхняя границы S

∃$(x)S = A_1$x … xAn – наибольшая нижняя границы S

Полурешётки

Теорема (Верхняя полурешетка)

Любое упорядоченное множество, в котором всякое двухэлементное подмножество имеет точную верхнюю грань, является полурешеткой, естественный порядок которой совпадает с отношением $\leq$

Теорема (Нижняя полурешетка)

Любое упорядоченное множество, в котором всякое двухэлементное подмножество имеет точную нижнюю грань, является полурешеткой, причем естественный порядок этой полурешетки является порядком, двойственным к исходному порядку $\leq$

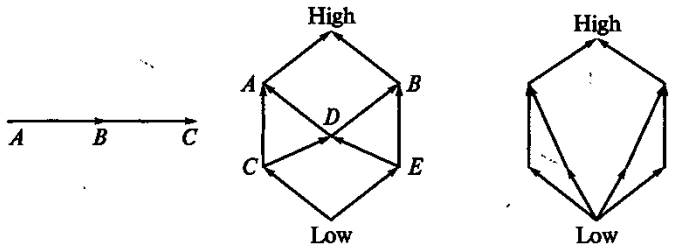
https://mathhelpplanet.com/static.php

MLS решётки

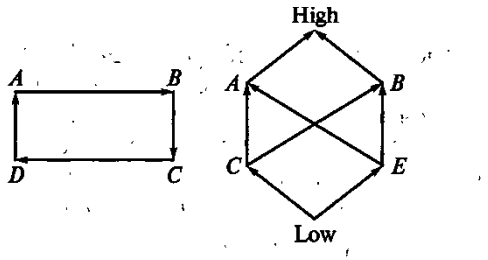
<u>Определение</u>

Линейная решётка – линейно упорядоченное множество: {0, 1, …, n} = SC

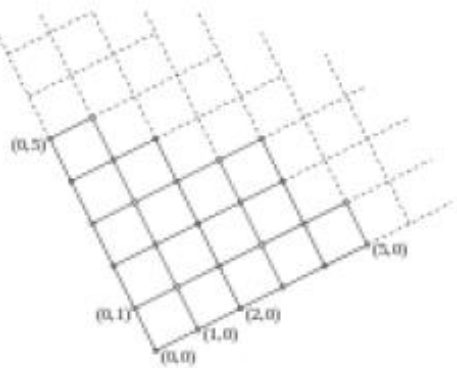
Решётки

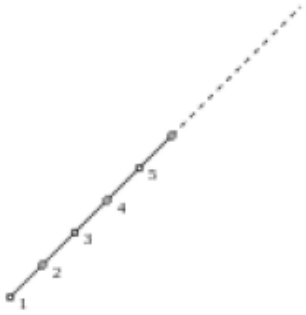


Нерешётки



Решетки





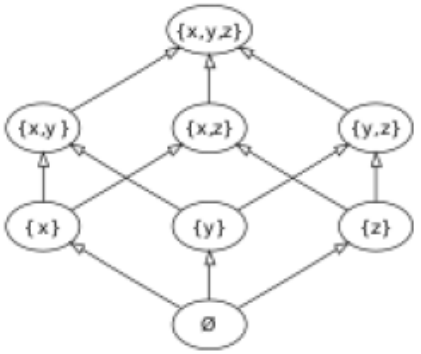


Рис. 1: Решетка подмножеств

Нерешетки

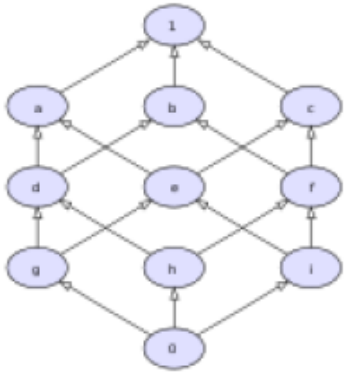


Рис. 8: ЧУМ без решетки: a и b имеют общие нижние границы 0, d, g, h и i, но ни одна из них не является точной нижней границей

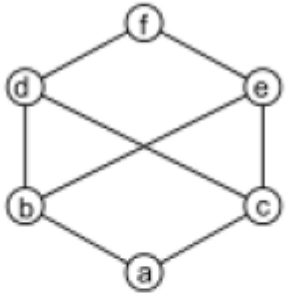


Рис. 7: Нерешетчатое множество: b и c имеют общие верхние границы d, e и f, но ни одна из них не является наименьшей верхней границей .

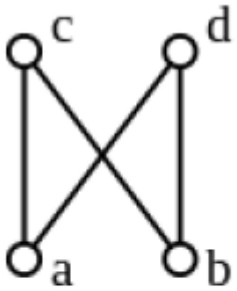


Рис. 6: Нерешетчатый poset: c и d не имеют общей верхней границы.