И.Ю. БОГОМАЗОВА, студентка гр. КЗИ-108;
М.Ю. МОНАХОВ, д.т.н., профессор;
М.М. МОНАХОВА, аспирант;
Д.В. МИШИН, ст. преподаватель.

ГРАФОВАЯ МОДЕЛЬ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Выбран уровневый поход к представлению СПД на основе модели ISO OSI. Разработан и формализован подход к построению графовых моделей СПД на различных уровнях.

Ключевые слова: СЕТЬ ПЕРЕДАЧИ ДАННЫХ, МОДЕЛЬ ISO OSI, УРОВЕНЬ, МОДЕЛИРОВАНИЕ, ГРАФОВАЯ МОДЕЛЬ, ГРАФ, ВЕРШИНА, РЕБРО, ВЕС, СЕТЕВАЯ АТАКА.

0 рис., 0 табл., 1 источник.

Цель работы - разработать графовое представление сети передачи данных (СПД), позволяющее моделировать сетевые атаки.

Поставленная цель определила необходимость решения следующего ряда задач:

1. Исследовать и адаптировать к поставленным задачам понятийный аппарат данной предметной области.

2. Выбрать детализацию представления СПД.

3. Разработать и формализовать подход к построению графовых моделей СПД.

4. Проиллюстрировать данный подход на примере СПД.

Что касается выбора уровней для представления сети, за основу иерархии была взята модель взаимодействия открытых систем ISO OSI. Из-за ее излишней детализированности, было принято решение рассматривать лишь те уровни модели, на которых проводятся самые распространенные атаки. Таким образом, будем рассматривать физический, канальный, сетевой и прикладной уровни эталонной модели.

Как было решено ранее [1], в связи с многообразием и сложностью структур СПД современных предприятий, будем использовать классические графовые модели, которые переработаем под наши задачи.

Предварительно были выделены основные элементы СПД и представлены в терминах теории множеств, как то:

1. Оконечные устройства: множество $P = \{p_1, p_2, .., p_f \mid f \in N\}$ оконечных устройств в рассматриваемой сети, где |P| - мощность множества, то есть количество устройств данного типа в СПД.

2. Концентраторы: множество $H = \{h_1, h_2, .., h_g \mid g \in N\}$ концентраторов в рассматриваемой сети, где |H| - мощность множества, то есть количество устройств данного типа в СПД.

3. Мосты: множество $B = \{b_1, b_2, .., b_i \mid i \in N\}$ мостов в рассматриваемой сети, где |B| - мощность множества, то есть количество устройств данного типа в СПД.

4. Коммутаторы: множество $S = \{s_1, s_2, .., s_j \mid j \in N\}$ коммутаторов в рассматриваемой сети, где |S| - мощность множества, то есть количество устройств данного типа в СПД.

5. Маршрутизаторы: множество $R = \{r_1, r_2, .., r_k \mid k \in N\}$ маршрутизаторов в рассматриваемой сети, где |R| - мощность множества, то есть количество устройств данного типа в СПД.

6. Другие устройства: множество $O = \{o_1, o_2, .., o_m \mid m \in N\}$ других устройств, не перечисленных выше, в рассматриваемой сети, где |O| - мощность множества, то есть количество таких устройств в СПД.

Количество элементов СПД без коммуникационных линий связи $n = |P| + |H| + |B| + |S| + |R| + |O|$.

На каждом уровне отображаются только устройства, работающие на данном уровне сети.

Представим сеть на физическом уровне в виде неориентированного мультиграфа без петель: упорядоченной пары

$G' = (V', E')$, где

$V' = V = \{v_1, v_2, .., v_n\}$ – множество вершин графа, такое, что:

$V = P \cup R \cup S \cup H \cup B \cup O;\ n' = n = |P| + |R| + |S| + |H| + |B| + |O|$.

E' – мультимножество неупорядоченных пар вершин – ребер, соответствующих непосредственным физическим соединениям между устройствами с помощью линий связи.

Представление в виде мультиграфа обусловлено возможностью наличия избыточности в сети на физическом уровне.

На канальном уровне будем изображать сеть в виде неориентированного графа без петель: упорядоченной пары

$G'' = (V'', E'')$, где

V'' – множество вершин графа, такое, что:

$V'' \subset V'$ и $V'' \subset V$, $V'' = P \cup R \cup S' \cup B' \cup O'$; $S' \subset S$ – множество коммутаторов, работающих на канальном уровне в рассматриваемой сети (участвующих во взаимодействии), $B' \subset B$ – множество мостов, работающих на канальном уровне в рассматриваемой сети и участвующих во взаимодействии, также учитываются множества других устройств, имеющихся в рассматриваемой сети передачи данных и работающих на канальном уровне; $n'' = |P| + |R| + |S'| + |B'| + |O'|$

E'' – множество ребер, соответствующих непосредственным физическим соединениям между устройствами с помощью линий связи, по которым осуществляется передача информации (незаблокированным), или соединениям через концентраторы.

На третьем уровне (сетевом) представим сеть в виде неориентированного взвешенного графа без петель: упорядоченной пары

$G''' = (V''', E''')$, где

V''' – множество вершин графа, такое, что:

$V''' \subset V''$ (и, соответственно, $V''' \subset V'$, $V''' \subset V$), $V''' = P \cup R \cup S'' \cup O''$; $S'' \subset S$ – множество коммутаторов третьего уровня в рассматриваемой сети, также могут быть включены другие множества устройств, имеющихся в рассматриваемой сети передачи данных и работающих на сетевом уровне; $n''' = |P| + |R| + |S''| + |O''|$

E''' – множество ребер, соответствующих непосредственным или через устройства более низкого уровня (канального) связям между устройствами (логическим связям).

Каждое ребро $e''' \in E'''$ снабжено весом $l_{E'''}(e''') > 0$, причем ребрам, соединяющим оконечные устройства между собой в пределах каждого широковещательного домена, присваивается минимальный вес a (где $a \in N$ – некоторое натуральное число), ребра, соединяющие оконечные устройства с маршрутизатором в пределах каждого широковещательного домена, должны иметь вес b (где $b \in N$ – некоторое натуральное число, $b > 1/2a$), а ребра, связывающие маршрутизаторы, получают динамически меняющийся вес $l_{E'''}(e''')$, исходя из совокупной оценки некоторых параметров - метрик. Выполнение данного условия позволяет оценить «стоимость» того или иного маршрута.

$\Sigma_{E'''} \subset N$ – полное множество (алфавит) возможных весов ребер графа G'''.

$l_{E'''} : E''' \to \Sigma_{E'''}$ – отображение, описывающее задание весов ребрам графа G'''.

Сеть передачи данных на прикладном уровне представим в виде неориентированного графа без петель: упорядоченной пары

$G'''' = (V'''', E'''')$, где

V'''' – множество вершин графа, такое, что:

$V'''' \subset V''$ (и, соответственно, $V'''' \subset V'$, $V'''' \subset V$, $V'''' \subset V$); $V'''' = P$; $n'''' = |P|$.

E'''' – множество ребер, соответствующих взаимодействиям по передаче информации по сети между приложениями на устройствах.

Информационные процессы (ИП) в СПД могут быть показаны на графе G''''.

Графы верхних уровней могут быть спроецированы на графы нижних уровней, отображение происходит сверху вниз. То есть атака уровня n должна быть представлена на графах СПД уровня n и уровней меньше n.

Определены также правила отражения взаимодействия между элементами сети на моделях всех выделенных уровней. Взаимодействие между двумя устройствами показывается на графе маршрутом (путем), соединяющим вершины графа, соответствующие данным устройствам. Под путем (маршрутом) по графу, соединяющим две вершины u и v, будем понимать простую цепь, то есть все вершины, а следовательно, и все ребра в данном маршруте различны. Это обуславливает следующее ограничение : все вершины и все ребра в маршруте между двумя вершинами различны.

Данное ограничение является достаточным для адекватного моделирования и достоверного отражения взаимодействия элементов сети на физическом, канальном и прикладном уровнях.

Для сетевого уровня вводятся дополнительные ограничения, учитывающие веса ребер и помогающие в создании, приемлемых моделей для сложных связей.

Дополнительные правила взаимодействия между узлами сети на сетевом уровне:

1. Взаимодействие между двумя элементами сети отражается маршрутом с наименьшим весом («стоимостью»).

2. В маршруте не могут одновременно присутствовать ребра с весом a и ребра с другими весами. Иначе говоря, оконечные устройства не могут взаимодействовать с другими устройствами в сети через иные оконечные устройства.

В докладе на семинаре были представлены результаты моделирования СПД на основе разработанного подхода.

Таким образом, на данном этапе работы:

1. Исследован и адаптирован понятийный аппарат данной предметной области.

2. Выбран уровневый поход к представлению СПД на основе модели ISO OSI.

3. Разработан и формализован подход к построению графовых моделей СПД на различных уровнях.

4. Промоделирована исходная СПД.

В дальнейшем планируется выделить основные характеристики узлов, постоянные и изменяющиеся в ходе атаки, предложить способ проецирования векторов атак на разработанные графы сети.

Литература

1. И.Ю. Богомазова, Д.В. Мишин, М.Ю. Монахов Графовые модели представления сетей передачи данных // Материалы НТС кафедры "Информатика и защита информации", - 2012. [Электронный ресурс]. URL:http://izi.vlsu.ru/HTC/17.pdf