О подходе к расчету числа сценариев реализации последовательной композиции совокупности векторов атак

И.А. Трещев, А.А. Обласов, А.И. Малаховец

Комсомольский-на-Амуре государственный университет

Аннотация: В работе рассмотрен подход к описанию поведения злоумышленников в случае, когда используется несколько векторов атак и в результате может быть достигнута одна из множества целей. В качестве формальной модели используется слабо связное ориентированное дерево, удовлетворяющее ряду условий. Приведен пример описания поверхности и совокупности векторов атак, описывающий атаку на информационную систему через уязвимость, связанную с возможностью полного перебора паролей пользователя от сайта и неосведомленностью относительно фишинговых писем, целями которой являются получение базы данных организации или отказ в обслуживании сервера. Проведено исследование множества сценариев атаки, задаваемых на формальной модели. Введена последовательная композиция, как объединение, совокупностей векторов атаки. Для случая произвольного числа совокупностей сформулировано правило позволяющее оценить количество сценариев.
Ключевые слова: моделирование атак, информационная безопасность, траектория атаки, сценарий атаки, вектор атаки, кибербезопасность.

Введение

С развитием информатизации, внедрением систем интернета вещей на предприятиях, повсеместным использованием мобильных технологий и цифровой трансформаций общества все более актуальной становится задача защиты от угроз информационной безопасности. Одним из основных направлений при этом является анализ потенциальных точек для проникновения в защищенный периметр организаций [1] злоумышленниками и возможных действий, которые могут быть ими совершены, используя графы атак [2], другие графоаналитические модели [3,4], элементы теории игр [5], сети Петри и другие [6]. Под поверхностью атаки будем понимать совокупность всех возможных уязвимостей информационной системы, которые могут быть использованы для проникновения в ее инфраструктуру. Под вектором атаки будем понимать способ получения несанкционированного доступа, с использованием некоторой уязвимости [7].

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Под сценарием [8] будем понимать осуществление конкретного вектора атаки.

Атаки зачастую проводит группа злоумышленников, используя всю поверхность, поэтому необходимо анализировать как можно большее количество векторов, которые, вообще говоря, могут быть направлены на достижение разных целей.

Совокупность сценариев атак

Под совокупностью векторов атак будем понимать обобщение слабо связанного ориентированного дерева [9], которое в отличие от традиционных деревьев атак и их модификаций [10], задается кортежем, для которого выполняются условия 1-8:

$$G = (A, V, dom, cod), \quad (1)$$

где $V = \{v_1, v_2, \ldots, v_m\}$ - множество вершин (которые, например, соответствуют результату очередного этапа в рамках реализации вектора атаки), при этом оно представляет из себя объединение трех непересекающихся множеств $V = V_{in} \cup V_{op} \cup V_{out}$, $V_{in} \cap V_{op} = \varnothing$, $V_{in} \cap V_{out} = \varnothing$, $V_{out} \cap V_{op} = \varnothing$ (именуемых входными, соответствующие компонентам поверхности атаки, промежуточными и выходными, соответствующие целям реализации векторов, вершинами), $A = \{a_1, a_2, \ldots, a_n\}$ - множество стрелок (описывающих действия злоумышленников, связывающих вершины), и заданы две тотальные функции $A \xrightarrow{dom} V, A \xrightarrow{cod} V$ определяющие для каждой стрелки начало и конец. В отличие от транспортных сетей не требуется задание весов для стрелок, исток и сток не единственны. Ордерево назовем слабо связным, если при игнорировании направлений стрелок оно становится связным, в том смысле что существует маршрут между любыми двумя вершинами. Ориентированным маршрутом (далее маршрутом) $l(v_1, v_n)$, связывающим две

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

вершины назовем чередующуюся последовательность вершин и стрелок $l(v_1, v_n) = v_1 a_1 v_2 a_2 \ldots v_{n-1} a_{n-1} v_n$, удовлетворяющую следующим условиям

1. $\forall i = 1..n-1, a_i \in A, \forall j = 1..n, v_j \in V$ (вершины и стрелки входят в дерево).

2. $\forall i = 1..n-1, dom(a_i) = v_i, cod(a_i) = v_{i+1}$ (начало и конец каждой стрелки в маршруте – соседние элементы в маршруте).

Отметим, что в силу однозначности сопоставления для каждой стрелки начала и конца, маршрут можно задавать последовательностью стрелок, а под длиной маршрута понимается их количество.

Простой ориентированной цепью (далее цепью) назовем маршрут для которого выполняются:

1. $\forall i = 1..n-1, \forall j = 1..n-1, i \neq j \Rightarrow a_i \neq a_j$ (все стрелки попарно различны)

2. $\forall i = 1..n, \forall j = 1..n, i \neq j \Rightarrow v_i \neq v_j$ (все вершины попарно различны)

Ориентированным циклом (далее циклом) назовем простую ориентированную цепь для которой первая и последняя вершины совпадают.

Для (1) должны выполняться следующие условия:

1. $\forall a \in A, dom(a) \neq cod(a)$ (отсутствуют петли).

2. $\forall a_1, a_2 \in A, \begin{cases} dom(a_1) = dom(a_2), \\ cod(a_1) = cod(a_2) \end{cases} \Rightarrow a_1 = a_2$ (отсутствуют кратные ребра).

3. $\forall v \in V, \left[\begin{array}{l} \exists a \in A, dom(a) = v. \\ \exists a \in A, cod(a) = v. \end{array}\right.$ (отсутствуют изолированные вершины).

4. $\forall v \in V_{in}, \forall a \in A, cod(a) \neq v$ (для вершин из множества входных нет стрелок, концом которых они являются и они формируют поверхность атаки).

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

5. $\forall v \in V_{out}, \forall a \in A, dom(a) \neq v$ (для вершин из множества выходных нет стрелок, началом которых они являются и они формируют цели).

6. $\forall v \in V_{op}, \exists a_1, a_2 \in A, dom(a_1) = v, cod(a_2) = v$ (для каждой вершины из множества промежуточных обязательно есть по крайней мере одна стрелка концом и одна началом которых она является).

7. $\forall a \in A, cod(a) \in V, dom(a) \in V$ (ребро обязательно связывает две вершины).

8. Граф задаваемый кортежем (1) слабо связен и в нем отсутствуют циклы.

Простую цепь, начинающуюся в одной из входных вершин и заканчивающуюся в одной из выходных назовем сценарием. При этом гарантируется наличие по крайней мере одного сценария для каждой входной вершины. Множество всевозможных сценариев обозначим через $Trace_G$ и в силу возможности задания маршрута как последовательности стрелок и отсутствия циклов имеем $Trace_G \subseteq \bigcup_{i=1}^{n} \prod_{j=1}^{i} A, | A | = n$. Обозначим количество сценариев между двумя вершинами $u \in V_{in}, v \in V_{out}, d(u,v)$, тогда $| Trace_G | = \sum_{\substack{u \in V_{in} \\ v \in V_{out}}} d(u,v)$, учитывая, что если сценарии между вершинами отсутствуют то их количество принимаем равным нулю.

Пример описания совокупности сценариев

Пусть имеет место атака на информационную систему, описываемая совокупностью сценариев в форме (1), для которой верны условия 1-8:

v_1 - сформировано фишинговое письмо;

v_2 - сформирован словарь логинов и паролей (для пользователя);

v_3 - получен доступ к сайту организации от имени пользователя;

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

v_4 - получена пара логин, пароль администратора СУБД;

v_5 - получена пара логин, пароль администратора домена организации;

v_6 - злоумышленником получена база данных клиентов и доступ к счетам;

v_7 - злоумышленник вывел из строя сервер организации;

$V_{in} = \{v_1, v_2\}, V_{out} = \{v_6, v_7\}, V_{op} = \{v_3, v_4, v_5\}, V = V_{in} \cup V_{out} \cup V_{op}$,

a_1 - посылка фишингового письма для получения логина и пароля пользователя для доступа к сайту организации;

a_2 - перебор по словарю логинов и паролей пользователя для доступа к сайту организации;

a_3 - внедрение межсайтового скриптинга (Cross-Site Scripting, XSS) для получения логина и пароля администратора СУБД;

a_4 - внедрение межсайтовой подделки запроса (Cross-Site Request Forgery, CSRF) для получения логина и пароля администратора домена;

a_5 - выгрузка базы данных на удаленный хост злоумышленника;

a_6 - уничтожение всех данных в базе данных;

a_7 - скачивание файла базы данных из домена организации на хост злоумышленника;

a_7 - удаление системных файлов на сервере и его перезагрузка;

$A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$,

$dom = \{(a_1, v_1), (a_2, v_2), (a_3, v_3), (a_4, v_3), (a_5, v_4), (a_6, v_4), (a_7, v_5), (a_8, v_5)\}$,

$cod = \{(a_1, v_3), (a_2, v_3), (a_3, v_4), (a_4, v_5), (a_5, v_6), (a_6, v_7), (a_7, v_6), (a_8, v_7)\}$.

Визуально ордерево может быть отображено в форме графа см. рис. 1

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

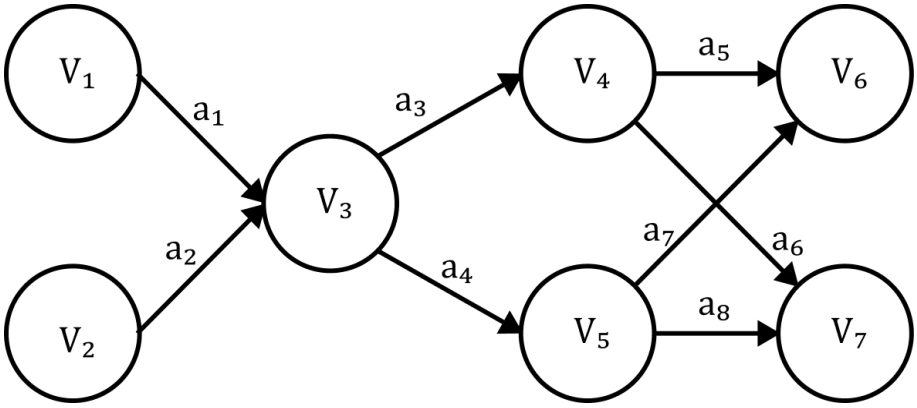

Рис. 1. – Визуальное представление ордерева соответствующего совокупности атак

При этом

$$Trace_G = \{(a_1,a_3,a_5),(a_1,a_3,a_6),(a_1,a_4,a_7),(a_1,a_4,a_8),(a_2,a_3,a_5),(a_2,a_3,a_6),(a_2,a_4,a_7),(a_2,a_4,a_8)\}$$

Операция последовательной композиции

Введем операцию последовательной композиции, которая позволит комбинировать атаки, предполагая их последовательную или параллельную реализацию. Пусть заданы две совокупности векторов атак

$$G_1 = (A^1, V^1, dom^1, cod^1), V^1 = V_{in}^1 \cup V_{op}^1 \cup V_{out}^1,$$

$$G_2 = (A^2, V^2, dom^2, cod^2), V^2 = V_{in}^2 \cup V_{op}^2 \cup V_{out}^2,$$

Такие что

$$V_{op}^1 \cap V_{op}^2 = \varnothing, V_{op}^1 \cap V_{in}^2 = \varnothing, V_{op}^1 \cap V_{out}^2 = \varnothing, V_{op}^2 \cap V_{in}^1 = \varnothing, V_{op}^2 \cap V_{out}^1 = \varnothing, V_{out}^2 \cap V_{in}^1 = \varnothing,$$

другими словами, могут пересекаться только входные вершины, выходные, выходные первой совокупности со входными второй. Обозначим $V_{out}^1 \cap V_{in}^2 = V^*$.

Дополнительно пусть задано число элементов множеств сценариев для каждой совокупности:

$$|Trace_{G_1}| = \sum_{\substack{u \in V_{in}^1 \\ v \in V_{out}^1}} d(u,v), \; |Trace_{G_2}| = \sum_{\substack{u \in V_{in}^2 \\ v \in V_{out}^2}} d(u,v)$$

Под композицией двух совокупностей будем понимать $G_2 \circ G_1 = (A^1 \cup A^2, V^1 \cup V^2, dom^1 \cup dom^2, cod^1 \cup cod^2)$. Ясно, что введенная таким

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

образом композиция не нарушает условий 1-8 для совокупности векторов атак. Рассмотрим восемь возможных случаев пересечения множеств входных, выходных и промежуточных вершин и оценку числа сценариев для каждого случая (остальные случаи исключаются по определению совокупностей векторов атак и по построению композиции), при этом разобьем их на две укрупненные группы ($V^* = \varnothing$ и $V^* \neq \varnothing$):

Случай, когда $V^* = \varnothing$:

1. $V_{in}^1 \cap V_{in}^2 = \varnothing, V_{out}^1 \cap V_{in}^2 = \varnothing, V_{out}^1 \cap V_{out}^2 = \varnothing$.
2. $V_{in}^1 \cap V_{in}^2 \neq \varnothing, V_{out}^1 \cap V_{in}^2 = \varnothing, V_{out}^1 \cap V_{out}^2 \neq \varnothing$.
3. $V_{in}^1 \cap V_{in}^2 = \varnothing, V_{out}^1 \cap V_{in}^2 = \varnothing, V_{out}^1 \cap V_{out}^2 \neq \varnothing$.
4. $V_{in}^1 \cap V_{in}^2 \neq \varnothing, V_{out}^1 \cap V_{in}^2 = \varnothing, V_{out}^1 \cap V_{out}^2 = \varnothing$.

В этом случае

$$|Trace_{G_2 \circ G_1}| = |Trace_{G_1}| + |Trace_{G_2}| = \sum_{\substack{u \in V_{in}^1 \\ v \in V_{out}^1}} d(u,v) + \sum_{\substack{u \in V_{in}^2 \\ v \in V_{out}^2}} d(u,v) \quad (3)$$

Случай, когда $V^* \neq \varnothing$:

1. $V_{in}^1 \cap V_{in}^2 \neq \varnothing, V_{out}^1 \cap V_{in}^2 \neq \varnothing, V_{out}^1 \cap V_{out}^2 = \varnothing$
2. $V_{in}^1 \cap V_{in}^2 = \varnothing, V_{out}^1 \cap V_{in}^2 \neq \varnothing, V_{out}^1 \cap V_{out}^2 = \varnothing$
3. $V_{in}^1 \cap V_{in}^2 \neq \varnothing, V_{out}^1 \cap V_{in}^2 \neq \varnothing, V_{out}^1 \cap V_{out}^2 \neq \varnothing$
4. $V_{in}^1 \cap V_{in}^2 = \varnothing, V_{out}^1 \cap V_{in}^2 \neq \varnothing, V_{out}^1 \cap V_{out}^2 \neq \varnothing$

В этом случае:

$$|Trace_{G_2 \circ G_1}| = \sum_{\substack{u \in V_{in}^1 \\ v \in V_{out}^1 \\ v \notin V^*}} d(u,v) + \sum_{\substack{u \in V_{in}^1 \\ z \in V_{out}^2 \\ v \in V^*}} d(u,v) * d(v,z) + \sum_{\substack{u \in V_{in}^2 \\ v \in V_{out}^2 \\ u \notin V^*}} d(u,v) \quad (4)$$

Отметим, что, если $V^* = \varnothing$ выражение (4) обращается в (3), поскольку при отсутствии путей их количество принято равным нулю.

Выражение (4) допускает обобщение для случая произвольного количества совокупностей. Пусть заданы *n* совокупностей векторов атак, для которых справедливы условия 1-8:

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

$G_1=(A^1,V^1,dom^1,cod^1),V^1=V_{in}^1\cup V_{op}^1\cup V_{out}^1,$

$G_2=(A^2,V^2,dom^2,cod^2),V^2=V_{in}^2\cup V_{op}^2\cup V_{out}^2,$

…

$G_n=(A^n,V^n,dom^n,cod^n),V^n=V_{in}^n\cup V_{op}^n\cup V_{out}^n$, сверх того

$\forall i=1..n-1,V_{op}^i\cap V_{op}^{i+1}=\varnothing,V_{op}^i\cap V_{in}^{i+1}=\varnothing,V_{op}^i\cap V_{out}^{i+1}=\varnothing,$
$V_{op}^{i+1}\cap V_{in}^i=\varnothing,V_{op}^{i+1}\cap V_{out}^i=\varnothing,V_{out}^{i+1}\cap V_{in}^i=\varnothing$

другими словами, могут пересекаться только входные вершины, выходные, выходные одной совокупности со входными последующей. Обозначим $\forall i=1..n-1,V_{out}^i\cap V_{in}^{i+1}=V_i^*$.

Дополнительно пусть задано число элементов множеств сценариев для каждой совокупности:

$$\forall i=1..n,|Trace_{G_i}|=\sum_{\substack{u\in V_{in}^i\\ v\in V_{out}^i}}d(u,v),$$

Под композицией семейства совокупностей будем понимать $G_n\circ G_{n-1}\circ\ldots\circ G_1=(\bigcup_{i=1}^n A^i,\bigcup_{i=1}^n V^i,\bigcup_{i=1}^n dom^i,\bigcup_{i=1}^n cod^i)$ и для нее верно выражение (5), которое может быть получено индукцией по числу совокупностей векторов атак.

$$|Trace_{G_n\circ G_{n-1}\circ\ldots\circ G_1}|=\sum_{i=1}^{n-1}\sum_{\substack{u\in V_{in}^i\\ v\in V_{out}^i\\ v\notin V_i^*}}[d(u,v)]+\sum_{\substack{u\in V_{in}^1\\ z\in V_{out}^n\\ v\in V_1^*\\ l\in V_{n-1}^*}}[d(u,v)*d(l,z)*\prod_{\substack{i=1\\ a_i\in V_i^*\\ a_{i+1}\in V_{i+1}^*}}^{n-2}d(a_i,a_{i+1})]+\sum_{\substack{u\in V_{in}^n\\ v\in V_{out}^n\\ u\notin V_{n-1}^*}}[d(u,v)] \qquad (5)$$

Множество всевозможных совокупностей векторов атак совместно с введенной операцией композиции образуют некоммутативный моноид относительно единицы – пустой совокупности векторов $G_\varnothing=(\varnothing,\varnothing,\varnothing,\varnothing)$, что следует из определения объединения и способа задания композиции.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

Заключение

Предлагаемый подход, при описании поверхности атаки и совокупности векторов, позволяет провести предварительный анализ возможных сценариев реализации действий по проникновению в информационные системы. Введенная операция последовательной композиции для совокупностей векторов атак позволяет анализировать комбинированные атаки, если известны характеристики соответствующих компонент, а также исследовать как атаки, не связанные по входным и выходным вершинам, так и случаи, когда одна является продолжением другой, или же они проводятся одновременно. Оценка выполнения и числа сценариев позволяет специалистам по защите информации принимать взвешенные решения относительно необходимости внедрения дополнительных механизмов защиты на различных этапах исполнения атаки.

Литература

1. Лазарева, Н. Б. Анализ сетевой устойчивости и оптимизация обмена данными в банковских системах // Инженерный вестник Дона, 2025, № 2. URL: ivdon.ru/magazine/archive/n2y2025/9839.

2. Kazeminajafabadi A., Imani M. Optimal monitoring and attack detection of networks modeled by Bayesian attack graphs // Cybersecurity. 2023. Vol. 6, № 1. URL: doi.org/10.1186/s42400-023-00155-y.

3. Крюков Д.М. Графоаналитическая модель процесса ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты // Инженерный вестник Дона, 2022, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2022/7613.

4. Palma A., Cicimurri C., Angelini M. Progressive attack graph: a technique for scalable and adaptive attack graph generation // International Journal of Information Security. 2025. Vol. 24. pp. 212–225. URL: doi.org/10.1007/s10207-025-01125-w.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

5. Catta, D., Di Stasio, A., Leneutre, J., Malvone, V. and Murano, A. (2023). A Game Theoretic Approach to Attack Graphs. In Proceedings of the 15th International Conference on Agents and Artificial Intelligence - Volume 1: ICAART; ISBN 978-989-758-623-1; ISSN 2184-433X, SciTePress, pages 347-354. DOI: 10.5220/0011776900003393.

6. Котенко Д.И., Котенко И.В., Саенко И.Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. 2012. № 3(22). С. 5–30. EDN PCCYJH.

7. Ветров И.А. Формирование вектора сетевых атак с учетом специфики связей техник и тактик // Вестник СибГУТИ. 2023. № 4. С. 49–61. DOI: 10.55648/1998-6920-2023-17-4-49-61. EDN JNTENM.

8. Kumar R. et al. Effective Analysis of Attack Trees: A Model-Driven Approach // Fundamental Approaches to Software Engineering (FASE 2018). Lecture Notes in Computer Science. 2018. Vol. 10802. P. 56–73. URL: doi.org/10.1007/978-3-319-89363-1_4.

9. Волкова Е.С. Метрики на деревьях атак, согласованные с модульной композицией // Вопросы кибербезопасности. 2024. № 3(61). С. 14–22. DOI 10.21681/2311-3456-2024-3-14-22. EDN FFCCGK.

10. Цициашвили Г.Ш. Зонирование районов региона по близости к внешней границе // Ученые записки Комсомольского-на-Амуре государственного технического университета. 2024. № 7(79). С. 46–49. EDN FDRJXS.

References

1. Lazareva N.B. Inzhenernyj vestnik Dona. 2025. № 2. URL: ivdon.ru/magazine/archive/n2y2025/9839.

2. Kazeminajafabadi A., Imani M. Cybersecurity. 2023. Vol. 6, № 1. 22 p. URL: doi.org/10.1186/s42400-023-00155-y.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026

3. Kryukov D.M. Inzhenernyj vestnik Dona. 2022. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2022/7613.

4. Palma A., Cicimurri C., Angelini M. International Journal of Information Security. 2025. Vol. 24. pp. 212-225. URL: doi.org/10.1007/s10207-025-01125-w.

5. Catta D., Di Stasio A., Leneutre J., Malvone V., Murano A. A Game Theoretic Approach to Attack Graphs, Proceedings of the 15th International Conference on Agents and Artificial Intelligence, Volume 1: ICAART. 2023. pp. 347-354.

6. Kotenko D.I., Kotenko I.V., Saenko I.B. Trudy SPIIRAN. 2012. № 3(22). pp. 5-30.

7. Vetrov I.A. Vestnik SibGUTI. 2023. Vol. 17, № 4. pp. 49-61.

8. Kumar R., Gaikwad S., Kadam A., Katti J., Kulkarni P. Effective Analysis of Attack Trees: A Model-Driven Approach, Fundamental Approaches to Software Engineering (FASE 2018). Lecture Notes in Computer Science. 2018. Vol. 10802. pp. 56-73. URL: doi.org/10.1007/978-3-319-89363-1_4.

9. Volkova E.S. Voprosy kiberbezopasnosti. 2024. № 3(61). pp. 14-22.

10. Tsitsiashvili G.Sh. Uchenye zapiski Komsomol'skogo-na-Amure gosudarstvennogo tekhnicheskogo universiteta. 2024. № 7(79). pp. 46-49.

Дата поступления: 9.12.2025

Дата публикации: 24.01.2026

© Электронный научный журнал «Инженерный вестник Дона», 2007–2026