Трещев И. А., Монастырная Е. И.
I. A. Treschev, E. I. Monastyrnaya

СОБЫТИЙНАЯ ФОРМАЛЬНАЯ МОДЕЛЬ ПОВЕДЕНИЯ ЗЛОУМЫШЛЕННИКА

EVENT-BASED FORMAL MODEL OF MALICIOUS BEHAVIOR

Трещев Иван Андреевич – кандидат технических наук, доцент, декан факультета компьютерных технологий Комсомольского-на-Амуре государственного университета (Россия, Комсомольск-на-Амуре); тел. 8(914)175-91-62. E-mail: kalkt@yandex.ru.
Ivan A. Treschev – PhD in Engineering, Associate Professor, Dean of Computer Technologies Faculty, Komsomolsk-na-Amure State University (Russia, Komsomolsk-on-Amur); tel. 8(914)175-91-62. E-mail: kalkt@yandex.ru.

Монастырная Елизавета Игоревна – студент Комсомольского-на-Амуре государственного университета (Россия, Комсомольск-на-Амуре); тел. 8(914)429-71-20. E-mail: liza.monastyrnaya@mail.ru.
Elizaveta I. Monastyrnaya – Student, Komsomolsk-na-Amure State University (Russia, Komsomolsk-on-Amur); tel. 8(914)429-71-20. E-mail: liza.monastyrnaya@mail.ru.

Аннотация. Данная работа сосредоточена на модели поведения злоумышленника и его действиях при организации атак на информационную систему. Модель нарушителя служит для анализа различных угроз и позволяет определить время, затрачиваемое на реализацию определённой стратегии. Рассмотрен сценарий, в котором злоумышленник начинает свои действия с внешнего периметра корпоративной сети. В работе такой сценарий представлен в виде ориентированного графа с чётко определёнными выделенными начальными и конечными состояниями, что позволяет проанализировать этапы атаки и исключить обратные переходы.

Summary. This paper focuses on the intruder behavior model and its actions when organizing attacks on an information system. The intruder model is used to analyze various threats and allows us to determine the time it takes to implement a certain strategy. We consider a scenario in which an intruder starts his actions from the outer perimeter of the corporate network. In this paper, such a scenario is represented as a directed graph with clearly defined initial and final states, which allows us to analyze the stages of the attack and exclude reverse transitions.

Ключевые слова: модель нарушителя, орграф, действия злоумышленника, система переходов, ордерево, угрозы, вектор атаки, корпоративная сеть.

Key words: intruder model, orgraph, intruder actions, transition system, tree, threats, attack vector, corporate network.

УДК 004.942

Введение. В последнее время информационные системы всё больше подвергаются постоянным препятствиям, мешающим их нормальной работе. Это связано с тем, что технологии, используемые злоумышленниками, постоянно совершенствуются. Поэтому решение вопросов по сохранению защищённости становится первостепенной задачей, требующей постоянного контроля и модернизации. Основным способом решения этих вопросов является применение математических моделей, которые используются для анализа кибератак и прогнозирования действий злоумышленников.

Продолжая анализировать тему, рассмотренную в [1], сфокусируемся на последовательности действий нарушителя и возможности её представления в виде ордерева.

Такой подход позволяет исследовать процесс атаки, начиная с этапа сбора информации о системе до завершения получения доступа к цели. Действия нарушителя представим в виде орграфа, вершинами которого являются действия злоумышленника, а рёбрами – переходы между

этими действиями. Ограничения, накладываемые на направления перехода, а также отсутствие циклов помогут рассмотреть ордерово и позволят упростить анализ.

Цель исследования – создать модель поведения нарушителя, которая в дальнейшем может использоваться для того, чтобы улучшить существующие инструменты для обнаружения и предотвращения атак в будущем.

Методы и материалы. Исходные данные, рассматриваемые в работе, содержат информацию об общей форме системы переходов, рассмотренной в [1], где некоторое количество стратегий злоумышленника обозначается как p_n, в которых e_i^j – это события нарушителя (j – номер события, i – номер процесса). При этом события, имеющие одинаковые номера процессов, могут происходить параллельно и взаимодействовать со следующими процессами согласно их порядковому номеру. Помимо этого, время взаимодействия между двумя произвольными событиями есть константа $\tau \geq 0$.

Временной системой переходов называется четвёрка: LTS (E, t, Q, τ), где $E = \{e_1^1,\ e_1^2, .., e_1^{n_1}, e_2^1,\ e_2^2, .., e_2^{n_2}, .., e_l^1,\ e_l^2, .. e_l^{n_m}\}$ – множество событий, с помощью которых злоумышленник будет добиваться цели, при этом рассматривается система, состоящая из l процессов, совершаемых нарушителем, а вектор $\{n_1,\ n_2, .. n_m\}$ задаёт количество событий в каждом процессе.

При моделировании стратегии атаки злоумышленника с помощью ордерева используется структура орграфа, в которой действия злоумышленника заданы как вершины графа, а переходы между ними – как рёбра.

При описании формул и утверждений используются следующие элементы:

V – множество вершин графа;

A – множество рёбер графа.

Ранее [1] была рассмотрена общая модель поведения злоумышленника, основанная на системе переходов [4], разберём конкретную модель поведения внешнего злоумышленника.

Модель нарушителя представляет собой реализацию той или иной угрозы, которые в свою очередь определены экспертным методом – показателем затрачиваемого времени на действия злоумышленника.

Рассмотрим возможный сценарий, где нарушитель начинается действовать с внешнего периметра. Он преследует несколько целей: кража идентификационных данных с их последующим использованием, кража интеллектуальной собственности, нарушение работы корпоративной сети. Систему взаимодействующих последовательных действий можно описать при помощи соответствующей модели (см. рис. 1).

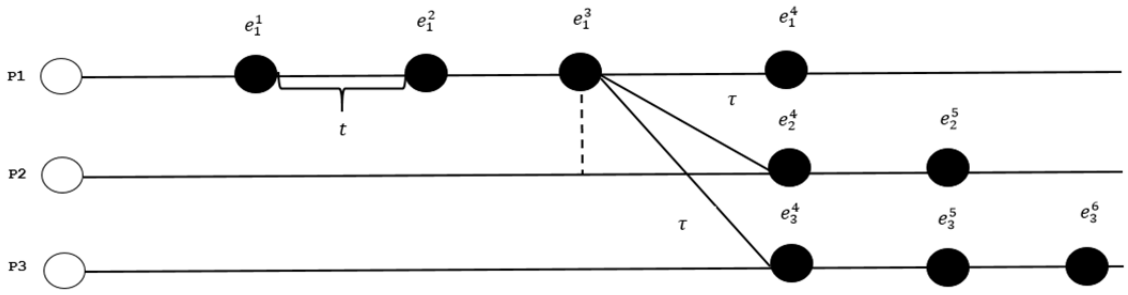

Рис. 1. Математическая модель внешнего нарушителя

Предположим, что есть некоторое количество параллельных сценариев p_n, e_i^j – это событие нарушителя (j – номер события, i – номер процесса). Далее пусть:

e_1^1 = фишинг (злоумышленник создаёт фишинговую компанию, отправляя поддельные электронные письма с вредоносными вложениями или ссылками на сотрудников организации; цель – получить доступ к компьютерам сотрудников);

e_1^2 = установка вредоносного ПО (сотрудник организации случайно открывает вредоносное вложение в фишинговом письме, что приводит к инфицированию его компьютера вредоносным программным обеспечением);

e_1^3 = установка Backdoor (после открытия сотрудником письма с вредоносным ПО устанавливается «задняя дверь» на компьютере сотрудника, предоставляя злоумышленнику удалённый доступ к системе);

e_1^4 = получение данных пользователя (доступ к корпоративным данным и последующая кража конфиденциальных данных, таких как бизнес-планы, патенты, технологические разработки или исследования);

e_2^4 = DDoS-атака (сервер);

e_2^5 = эксплуатация уязвимости (сбой работы сервера и приостановление работы корпоративной сети);

e_3^4 = сканирование портов и устройств (злоумышленник ищет другие устройства и службы внутри сети, сканируя открытые порты и службы);

e_3^5 = перехват сеансов (злоумышленник использует полученные учётные данные для перехвата активных сеансов другими устройствами и службами внутри сети);

e_3^6 = перехват административного доступа (целью может быть кража идентификационных данных сотрудников или клиентов, таких как логины и пароли, для дальнейшего мошенничества).

Пусть происходит событие e_1^3, взаимодействующее с e_1^4, e_2^4 и e_3^4. А события e_2^5 и e_3^5 происходят параллельно. Пусть время взаимодействия между произвольными событиями есть константа $\tau \geq 0$. Такой подход позволяет описать взаимодействующие последовательные сценарии с рядом ограничений, накладываемых на модели.

Предположим, что описана временная система переходов, изображённая на рис. 1, и экспертным методом задано время реализации событий $t(e_1^1) = 5$, $t(e_1^2) = 15$, $t(e_1^3) = 30$, $t(e_3^4) = 50$, $t(e_3^5) = 25$, $t(e_3^6) = 15$.

Тогда найдём время функционирования сценария злоумышленника:

$\text{Max}(t(e_1^1) + \tau, t(e_1^2) + \tau, t(e_1^3) + \tau, t(e_3^4) + \tau, t(e_3^5) + \tau, t(e_3^6) + \tau) = \text{Max}[5 + \tau, 15 + \tau, 30 + \tau, 50 + \tau, 25 + \tau, 15 + \tau] = 50 + \tau$. Из этого следует, что для реализации атаки потребуется не менее 50 единиц времени.

Итак, на основе заданных временных показателей для событий мы определили, что сценарий атаки будет функционировать не менее 50 единиц времени. Это означает, что в течение этого периода злоумышленник будет продолжать свои действия, представленные в модели, включая фишинг, установку вредоносного ПО, установку Backdoor, получение данных пользователя, DDoS-атаку, эксплуатацию уязвимости, сканирование портов и устройств, перехват сеансов и перехват административного доступа.

Такой подход позволяет оценить продолжительность атаки и, следовательно, разработать эффективные методы обнаружения и предотвращения атак. Понимание, что атаки могут продолжаться не менее определённого времени, позволит специалистам по защите информации разработать политику реагирования на инциденты.

Далее рассмотрим, как вышеуказанную модель можно представить в виде орграфа. Для этого введём два события, которые будем именовать как начальный этап атаки злоумышленника (сбор информации о системе) и конечный (конкретная цель, достигаемая злоумышленником). Действия злоумышленника на орграфе будут представлять собой вершины, а переходы между ними – рёбра.

Пусть v^* – начальный этап атаки, v^{**} – конечная цель злоумышленника. Тогда v_1^1, v_2^1, v_1^2, v_2^2, v_2^3 – последовательные действия злоумышленника. При этом зададим рёбра так, что откат назад, к предыдущему действию, невозможен (см. рис. 2).

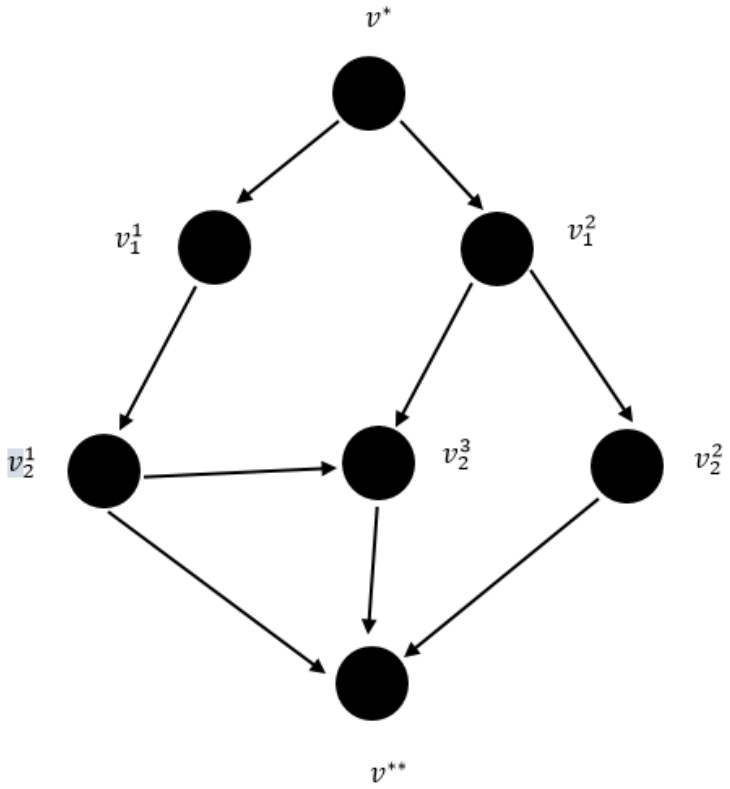

Рис. 2. Ордерево событий атаки злоумышленника

В случае, когда орграф можно интерпретировать как ордерево с выделенными вершинами v^*, v^{**}, справедливы следующие утверждения:

$$\{\exists!\, v^* \in V | \nexists a \in A \mathrm{cod}(a) = v^*\}, \tag{1}$$

$$\begin{cases} u \in V | \nexists a \in A \mathrm{cod}(a) = u \\ v \in V | \nexists a \in A \mathrm{cod}(a) = v \end{cases} => u = v. \tag{2}$$

Для v^{**} аналогично справедливы утверждения

$$\{\exists!\, v^{**} \in V | \nexists a \in A \mathrm{dom}(a) = v^* *\}, \tag{3}$$

$$\begin{cases} u \in V | \nexists a \in A \mathrm{dom}(a) = u \\ v \in \mathrm{V} | \nexists a \in A \mathrm{dom}(a) = v \end{cases} => u = v. \tag{4}$$

Выражение (1) означает, что для вершины v^* из множества вершин V не существует такого ребра a из множества рёбер A, которое бы входило в эту вершину. Аналогичные условия заданы в (3) для конечной цели.

Выражение (2) описывает, что если существуют две вершины u, v из множества вершин V, для которых гарантировано отсутствие входящих в них рёбер, то эти две вершины являются одной и той же вершиной дерева.

Дополнительно (4) означает, что если существуют две вершины u, v из множества вершин V, для которых гарантировано отсутствие выходящих из них рёбер, то эти две вершины являются одной и той же вершиной дерева.

Анализ ордерева позволяет нам более глубоко понять структуру последовательных действий в рамках модели атаки, а также определить ключевые этапы. Заданные ограничения являются определяющими для анализа сценариев.

Заключение. Результаты, полученные в ходе исследования, могут быть применены для разработки методов по обнаружению и устранению неблагоприятных воздействий кибератак, а

также для проведения анализа различных видов уязвимостей в распределённых информационных системах и создания системы по реагированию на инциденты информационной безопасности.

Имея полное представление о структурах атаки и времени их выполнения, специалисты по защите информации получат возможность улучшить стратегию по защите информационных ресурсов.

Дальнейшие исследования следует связать с переходом в категорию сетей Петри, анализа достижимости и других характеристик моделей.

ЛИТЕРАТУРА

1. Трещев, И. А. Математическая модель распределённых вычислений на основе последовательных событий / И. А. Трещев, А. С. Ватолина // Наука, инновации и технологии: от идей к внедрению: материалы II Междунар. науч.-практ. конф. молодых учёных. Т. 1 / Редкол.: А. В. Космынин (отв. ред.) [и др.]. – Комсомольск-на-Амуре: ФГБОУ ВО «КнАГУ», 2022. – С. 416-418.
2. Аверченков, В. И. Аудит информационной безопасности органов исполнительной власти: учеб. пособие / В. И. Аверченков. – М.: Флинта, 2020. – 297 с.
3. Аверченков, В. И. Аудит информационной безопасности: учеб. пособие / В. И. Аверченков. – М.: Флинта, 2021. – 679 с.
4. Козлов, А. А. Моделирование угроз безопасности информации на основе систем переходов состояний / А. А. Козлов, Ю. Ю. Ходяков // Научно-технический вестник информационных технологий, механики и оптики. – 2019. – Т. 19. – Вып. 4. – С. 682-687.
5. Афанасьев, А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учеб. пособие для вузов / А. А. Афанасьев. – М.: Горячая линия – Телеком, 2020. – 438 с.
6. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем: учеб. пособие / Е. В. Глинская, Н. В. Чичварин. – М.: ИНФРА-М, 2020. – 118 с.
7. Гордеев, А. В. Моделирование атак на информационную систему с использованием матрицы связей уязвимостей / А. В. Гордеев, Н. В. Жукова // Вестник Пермского национального исследовательского политехнического университета. Информатика и вычислительная техника. – 2018. – № 2. – С. 107-116.
8. Грачев, М. В. Моделирование кибератак на информационные системы на основе теории графов / М. В. Грачев, А. В. Переверзев // Системы и средства информатики. – 2019. – Т. 29. – Вып. 2. – С. 43-59.
9. Девянин, П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П. Н. Девянин. – М.: Радио и связь, 2018. – 176 с.
10. Долгов, А. С. Моделирование угроз кибербезопасности информационных систем на основе теории системных динамических переходов / А. С. Долгов, Н. А. Соколова, С. А. Кабанов // Системы управления и информационные технологии. – 2018. – № 5. – С. 54-59.
11. Дударев, А. В. Использование теории систем переходов при моделировании кибератак / А. В. Дударев, А. В. Герус // Проблемы безопасности информационных технологий. – 2019. – Т. 1. – Вып. 1. – С. 43-49.