Математические структуры и моделирование
2024. № 2 (70). С. 80–86

УДК 519.83:004.056
DOI 10.24147/2222-8772.2024.2.80-86

СОЗДАНИЕ СЕРВИСА ДЛЯ АНАЛИЗА ЗАЩИЩЁННОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ ТЕОРЕТИКО-ИГРОВОГО ПОДХОДА И БАЗЫ ЗНАНИЙ MITRE ATT&CK

Т.В. Вахний
канд. физ.-мат. наук, доцент, e-mail: vahniytv@mail.ru
П.В. Константинов
студент, e-mail: konstantinov.pavel.va@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В статье описано создание сервиса для оптимизации подбора средств защиты и анализа защищённости компьютерных систем на основе теоретико-игрового подхода. Стратегии администратора безопасности и злоумышленника строятся на данных базы знаний MITRE ATT&CK, вычисление лучших стратегий проводится на основе критериев Вальда, Лапласа и Сэвиджа методом Монте-Карло с применением алгоритма UpperConfidenceBound.

Ключевые слова: компьютерная система, цифровизация, кибербезопасность, матричная игра, оптимальная стратегия.

Введение

В современном мире цифровые технологии играют ключевую роль в развитии бизнеса и повышении его конкурентоспособности. Они помогают автоматизировать процессы, улучшить качество продукции и услуг, эффективно коммуницировать с клиентами, а также стимулируют развитие инноваций. Однако внедрение цифровых технологий сопряжено с угрозой безопасности данных. Успешная кибератака может повлечь не только к невообразимые убытки и серьёзно подорвать доверие клиентов, но даже нарушить функционирование компании или привести к банкротству. При этом киберпреступники постоянно совершенствуют свои тактики и методы атак, используя новые технологии, чтобы обойти защитные меры. Непрекращающийся рост числа атак, их усложнение и изощрённость побуждают к созданию большого количества средств защиты, и построение надёжной системы безопасности становится всё более сложной задачей.

Стохастической природе проблем защиты компьютерных систем соответствуют математические методы принятия решений в условиях неопределённости, в частности методы теории игр [1–4]. В данной статье описано создание сервиса, позволяющего на основе теоретико-игрового подхода рассчитывать лучшие стратегии защиты при минимизации финансовых затрат и оценивать эффективность уже используемого набора мер по предотвращению угроз безопасности системы компании. Источником данных для сервиса послужила «MITRE ATT&CK™» – открытая

база знаний о техниках, используемых киберпреступниками в ходе атак на корпоративные сети, и о мерах по устранению рисков, связанных с соответствующими атаками [5].

1. Постановка задачи и игровой подход

Для поиска наилучшего набора программных средств защиты компьютерной системы можно провести математическую игру двух сторон, одной из которых является система защиты, а другой – возможные атаки на неё. Нанесение злоумышленником ущерба обычно является следствием его действий, а не самой целью. В действительности при атаке он может преследовать какие-то свои цели, порой известные лишь ему. Поскольку данная работа направлена на нахождение администратором такой стратегии защиты, при которой возможные потери от атак будут минимальны, а цели атакующих злоумышленников не представляют интереса, то было сделано предположение о том, что злоумышленник увлечён желанием нанести как можно больший ущерб атакуемой компьютерной системе. В таком случае его выигрыш равен проигрышу администратора безопасности и можно получить матрицу для игры двух лиц с нулевой суммой.

В платёжной матрице строки соответствуют стратегиям одного игрока (программное средство или набор из программных средств), а столбцы – стратегиям другого игрока, на их пересечении стоит цена игры. Если администратор для обеспечения безопасности компьютерной системы компании может выбирать из S программных средств защиты и при этом их можно устанавливать одновременно, то у него будет $N = 2^S - 1$ вариантов стратегий. Аналогично, если злоумышленник имеет L способов атаки, то у него будет $M = 2^L - 1$ вариантов стратегий. Проведение матричной игры позволяет определить наиболее выигрышные стратегии игроков.

Ходом администратора безопасности является использование одной из N стратегий защиты x_i ($i = 1, 2, ..., N$), а ходом злоумышленника – применение одной из M стратегий атаки y_j ($i = 1, 2, ..., M$) на компьютерную систему компании. Последовательно перебирая все стратегии игроков, можно заполнить таблицу, указывая соответствующий ущерб a_{ij} для администратора при выборе стратегии защиты x_i и способа атаки y_j.

Таблица 1. Таблица матричной игры

	y_1	y_2	...	y_M
x_1	a_{11}	a_{12}	...	a_{1M}
x_2	a_{21}	a_{22}	...	a_{2M}
...	...	...	...	...
x_N	a_{N1}	a_{N2}	...	a_{NM}

Из таблицы можно выписать платёжную матрицу A с элементами a_{ij}, содержащую N строк и M столбцов:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1M} \\ a_{21} & a_{22} & \dots & a_{2M} \\ \dots & \dots & \dots & \dots \\ a_{N1} & a_{N2} & \dots & a_{NM} \end{pmatrix}.$$

Здесь элементы a_{ij} платёжной матрицы вычисляются следующим образом:

$$a_{ij} = R(x_i, y_j) + G_i,$$

где $R(x_i, y_j)$ – величина ущерба от атаки y_j при использовании стратегии защиты x_i; G_i – затраты администратора на приобретение и использование программных средств защиты, необходимых для реализации стратегии x_i.

Матричная игра состоит в том, что администратор выбирает стратегию защиты x_i, злоумышленник выбирает стратегию атаки y_j, после чего вычисляется исход игры, заключающийся в том, что администратор терпит ущерб, равный a_{ij}, а злоумышленник получает прибыль a_{ij}. Цель администратора безопасности – выбор такой стратегии, т. е. набора программных средств защиты, который сводит потери от атак и затраты на покупку средств защиты к минимуму, а цель атакующего – выбор такой стратегии, которая даст ему наибольший выигрыш. Решение матричной игры сводится к отысканию равновесных (оптимальных) стратегий игроков x_{i_0} и y_{j_0}. Выбор одним из игроков любой другой стратегии, вероятнее всего, приведёт к ухудшению его результатов игры и улучшению их у противника.

2. Стратегии игроков и критерии оптимальности

В настоящее время для описания и структурирования различных инцидентов специалисты по компьютерной безопасности всего мира используют открытую базу знаний MITRE ATT&CK [5]. Она содержит информацию о техниках, используемых киберпреступниками в ходе атак на корпоративные сети, и способах устранения рисков, связанных с соответствующими атаками. По мере появления новых уязвимостей и способов атак они добавляются в структуру ATT&CK, которая таким образом постоянно развивается. Для проведения матричной игры были определены стратегии злоумышленника и администратора безопасности на основе информации из этой базы.

База знаний MITRE ATT&CK представлена объектом bundle в STIX-формате и в полном объёме доступна для скачивания в официальном репозитории MITRE в Github [5]. STIX-формат (Structured Threat Infromation eXpression) позволяет получать данные в виде читаемых JSON-файлов и быстро определять связи между объектами. Так, например, можно быстро получать техники, устраняемые конкретной мерой противодействия.

В матричной игре администратор безопасности стремится выбрать такую стратегию, которая позволит ему свести к минимуму наносимый компьютерной системе ущерб от реализации тех или иных угроз. Поставим в соответствие каждой i-ой стратегии администратора x_i число $W_i(A)$, вычисляемое с помощью платёжной матрицы A. Критерий выбора оптимальной стратегии x_{i_0} для администратора

состоит в том, чтобы взять $W_{i_0} = \min\limits_i W_i(A)$. Злоумышленник, наоборот, стремится выбрать такую стратегию, которая позволит ему нанести компьютерной системе наибольший ущерб от реализации тех или иных угроз. Поставим в соответствие каждой j-ой стратегии злоумышленника y_j число $W_j(A)$, вычисляемое с помощью платёжной матрицы A. Критерий выбора оптимальной стратегии y_{j_0} для злоумышленника состоит в том, чтобы взять $W_{j_0} = \max\limits_j W_j(A)$. Для нахождения в платёжной матрице чисел $W_i(A)$ и $W_j(A)$ можно использовать различные критерии к выбору оптимальной стратегии [3]. Если оба игрока осторожны, то для поиска их лучших стратегий наиболее подходят критерии Вальда, Лапласа и Сэвиджа.

3. Создание сервиса для анализа защищённости компьютерных систем и работа с ним

На основе описанного подхода на языке программирования Python был создан сервис, который позволяет рассчитывать наилучший по выбранному критерию набор средств защиты для компьютерной системы. При написании программного кода были использованы следующие Python-библиотеки:

1) streamlit.io – фреймворк для языка программирования Python, содержит инструменты, которые помогают перенести модель машинного обучения в веб, позволяет запускать программный код в браузере без наличия сервера, быстро отображать различные данные, графики, матрицы, таблицы, формулы и т. д.;

2) numpy – библиотека для быстрой работы с многомерными массивами и матрицами больших объёмов данных;

3) pyinterval – библиотека для интервальной арифметики, позволяет оперировать над вещественными интервалами;

4) pandas – библиотека для анализа структурированных данных, размещённых в таблицах, позволяет сохранять данные в DataFrame объекты (рис. 1).

Данные тактик Mitre ATT&CK

		external_references	modified	name	description	x_mitre_version	x_mitre_attack_spec_version	x_mitre_modified_by_ref
4	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Privilege Escalation	The adversary is trying to gain higher-level permissions. Privilege Escalation consists	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
5	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Lateral Movement	The adversary is trying to move through your environment. Lateral Movement consis	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
6	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Defense Evasion	The adversary is trying to avoid being detected. Defense Evasion consists of techniq	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
7	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Exfiltration	The adversary is trying to steal data. Exfiltration consists of techniques that adversar	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
8	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Discovery	The adversary is trying to figure out your environment. Discovery consists of techniq	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
9	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Collection	The adversary is trying to gather data of interest to their goal. Collection consists of t	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
10	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Resource Developme	The adversary is trying to establish resources they can use to support operations. Re	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
11	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
12	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Command and Contr	The adversary is trying to communicate with compromised systems to control them.	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
13	>-4611-8297-d1b8b55e40b5	[object Object]	2022-04-25T14:00:00.188Z	Initial Access	The adversary is trying to get into your network. Initial Access consists of techniques	1.0	2.1.0	identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5

Рис. 1. Просматриваемый DataFrame с данными тактик MITRE ATT&CK

Поскольку в созданном сервисе была реализована возможность выбирать лучшую стратегию из огромного количества техник, указанных в базе знаний MITRE ATT&CK, то размер платёжной матрицы может получиться очень большим, достигнув величины $2^{425} - 1$. В результате решение матричной игры потребует больших затрат на вычислительные ресурсы и оптимальная стратегия администратора безопасности будет вычисляться очень продолжительное время. Для сокращения времени

на нахождение решения расчёты на сервисе проводятся методом статистических испытаний Монте-Карло с применением алгоритма UpperConfidenceBound [4].

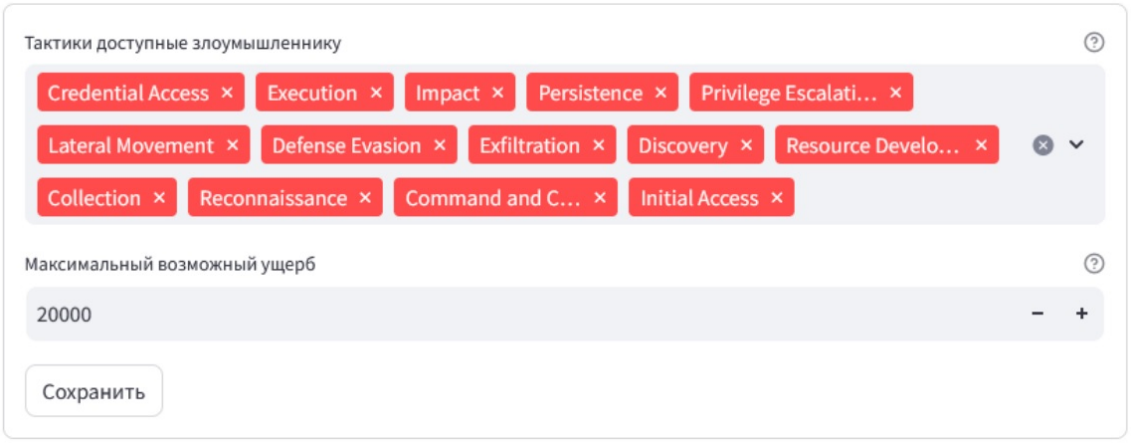

Рис. 2. Меню с выбранными тактиками злоумышленника

Результаты выполненных на сервисе расчётов зависят от введённых пользователем данных. Например, пользователь может выбирать тактики, доступные злоумышленнику (рис. 2), добавлять новые стратегии, отсутствующие в сервисе, указывать их стоимость, возможный ущерб от реализации определённой атаки, сопоставлять способность средства защиты противостоять каждой возможной атаке (рис. 3).

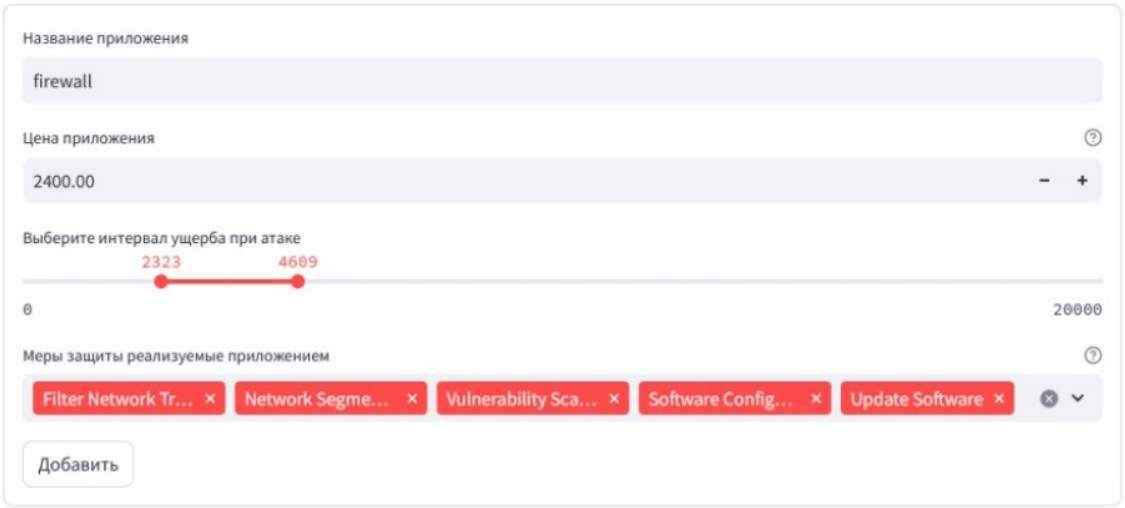

Рис. 3. Меню добавления ресурса

Пользователь может указать критерии оптимальности стратегий администратора безопасности и злоумышленника, выбирая из реализованных на сервисе критериев Вальда, Лапласа и Сэвиджа (рис. 4), а также количество лучших стратегий защиты (с наименьшими значениями цены игры), которые требуется вывести.

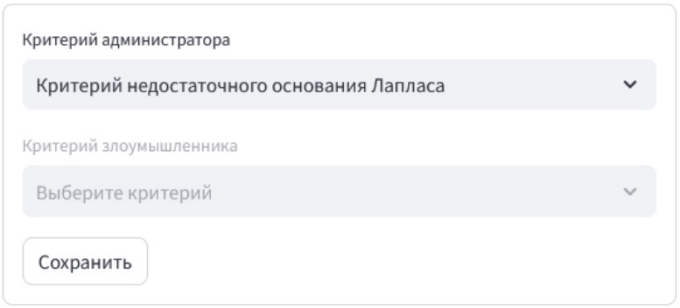

Рис. 4. Меню выбора критериев оптимальности стратегий игроков

В результате проведения расчётов данный сервис находит решение матричной игры и пользователь получает комбинацию из интересующего его количества наилучших стратегий защиты с указанием цены игры при их использовании. В дальнейшем найденные наилучшие стратегии могут быть реализованы в компьютерной системе для повышения её защищённости или просто оказаться полезными для дополнительного анализа используемой в компании на данный момент системы безопасности.

Заключение

В статье описано создание сервиса, который на основе теоретико-игрового подхода позволяет администратору анализировать и оптимизировать подбор программных средств для построения системы безопасности компании. Преимуществом сервиса является то, что участвующие в матричной игре стратегии злоумышленника и администратора безопасности формируются из данных открытой, постоянно обновляемой базы знаний MITRE ATT&CK. В дальнейшем представляет интерес реализация возможности использования машинного обучения как альтернативы методу Монте-Карло с применением алгоритма UpperConfidenceBound.

Литература

1. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем : учебное пособие. Омск: Изд-во ОмГУ, 2013. 160 с.
2. Вахний Т.В., Гуц А.К., Константинов В.В. Программное приложение для выбора оптимального набора средств защиты компьютерной информации на основе теории игр // Вестник Омского университета. 2013. № 4 (70). С. 201–206.
3. Вахний Т.В., Гуц А.К., Новиков Н.Ю. Матрично-игровая программа с выбором критерия для определения оптимального набора средств защиты компьютерной системы // Математические структуры и моделирование. 2016. № 2 (38). С. 103–115.
4. Вахний Т.В., Гуц А.К., Пахотин И.Ю. Определение оптимального набора средств защиты компьютерной системы методом Монте-Карло // Математические структуры и моделирование. 2018. № 1 (45). С. 148–158.

5. Threat Intelligence по полочкам: разбираемся в стандартах обмена данными // R-Vision. 2021. URL: `https://habr.com/ru/companies/rvision/articles/553534/` (дата обращения: 30.04.2024).

CREATION OF A SERVICE FOR ANALYZING THE SECURITY OF COMPUTER SYSTEMS BASED ON A GAME-THEORETIC APPROACH AND THE MITRE ATT&CK KNOWLEDGE BASE

T.V. Vakhniy
Ph. D.(Phys.-Math.), Associate Professor, e-mail: vahniytv@mail.ru
P.V. Konstantinov
Student, e-mail: konstantinov.pavel.va@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The article describes the creation of a service for optimizing the selection of security tools and analyzing the security of computer systems based on a game-theoretic approach. The strategies of the security administrator and the attacker are based on data from the MITRE ATT&CK knowledge base, the calculation of the best strategies is based on the criteria of Wald, Laplace and Savage using the Monte Carlo method using the UpperConfidenceBound algorithm.

Keywords: computer system, digitalization, cybersecurity, matric game, optimal strategy.

Дата поступления в редакцию: 01.05.2024