Дойникова Е.В.^{1,3}, Гайфулина Д.А.¹, Крюков Р.О.²

Определение признаков целей кибератак на основе анализа данных безопасности в открытых источниках

¹Санкт-Петербургский институт информатики и автоматизации РАН

²Военно-космическая академия имени А. Ф. Можайского

³Санкт-Петербургский государственный университет телекоммуникаций им. проф.

М.А.Бонч-Бруевича

(Россия, Санкт-Петербург)

doi: 10.18411/lj-11-2019-33

idsp: lj-11-2019-33

Аннотация

В работе рассматриваются открытые базы данных безопасности. Особое внимание уделяется анализу характеристик, используемых для описания шаблонов кибератак. Анализируются связи между различными целями кибератак и значениями характеристик шаблонов кибератак для выделения тех характеристик, которые могут являться признаками целей атак. Предлагаются метрики для определения целей атак, основанные на выделенных характеристиках. Приводятся эксперименты, демонстрирующие зависимость между значениями данных метрик и целей атак, и, как следствие, их применимость для определения различных классов целей атак.

Ключевые слова: данные безопасности, базы данных, признаки, метрики, цели атаки

Abstract

The paper considers different security databases. The special attention is given to analysis of characteristics used to describe cyberattacks' patterns. The authors analyze relations among different cyberattack goals and values of cyberattacks' patterns characteristics to determine the characteristics that can be features of attack goals. The metrics for cyberattack goals determination are proposed. These metrics are based on the selected characteristics. The experiments that demonstrate correlation between values of the proposed metrics and attack goals, and, consequently, applicability of these metrics for determination of different classes of attack goals, are conducted.

Keywords: security data, databases, features, metrics, attack goals

В настоящее время большую опасность для крупных коммерческих и государственных организаций представляют целевые кибератаки. Сложность защиты от данного вида атак связана с тем, что они отличаются детальным предварительным исследованием слабых мест конкретной организации, и могут включать большое количество шагов, направленных на изучение ее инфраструктуры, незаметное внедрение, атаку и заметание следов. В тоже время многошаговость таких атак может являться основой для их своевременного выявления и предотвращения развития при наличии в организации системы мониторинга защищенности. Одним из важных элементов своевременного реагирования на атаку, а также предотвращения аналогичных атак в будущем, является корректное определение цели обнаруженной атаки, что является предметом исследования в данной статье.

К настоящему моменту исследовательским сообществом было сформировано большое количество источников, содержащих описание и характеристики разных объектов безопасности, включая базу программно-аппаратного обеспечения и его уязвимостей National Vulnerability Database (NVD) [1], базу слабых мест CWE (Common Weakness Enumeration) [2], и базу шаблонов атак CAPEC (Common Attack Pattern

Enumeration and Classification) [3]. В работе выделяются данные базы из-за наличия связи между ними и программно-аппаратным обеспечением: в NVD представлено программно-аппаратное обеспечение, которое имеет уязвимости. Уязвимости, в свою очередь, имеют ссылки на слабые места в базе CWE. Слабые места в базе CWE, в свою очередь, имеют ссылки на шаблоны атак базы CAPEC, разделенные на категории. На этой основе было сделано предположение, что в зависимости от объектов и уязвимостей, присутствующих в системе, можно определить возможные цели атак в этой системе, используя связь между NVD и CAPEC через CWE.

Данная статья посвящена выделению метрик для определения целей атак и признаков атак для их классификации с использованием открытых данных безопасности на основе взаимосвязей, выделенных в построенной ранее онтологии метрик и объектов безопасности [4]. А также проведению экспериментов по анализу значений разных признаков, представленных в базах, и по выявлению зависимостей между ними, а также между различными категориями атак.

База уязвимостей NVD является наиболее полным известным авторам словарем программно-аппаратного обеспечения, его конфигураций, и уязвимостей. К преимуществам базы можно также отнести детальное описание уязвимостей с помощью ряда признаков, которые можно разделить на три группы: признаки, описывающие уязвимость; метрики; и признаки, являющиеся ссылками на другие источники. К первой группе относится описание уязвимости, а также признаки формата CVE для описания уязвимости (уникальный идентификатор уязвимости, дата публикации, дата последнего изменения). Вторая группа включает оценки CVSS версий 2.0 и 3.0 для уязвимостей, которые могут принимать значения от 0 до 10, отдельно выделена подоценка ущерба от успешного использования уязвимости и вероятность ее успешного использования. Для CVSS версии 2.0 также отдельно задаются получаемые при использовании уязвимости привилегии (все, пользовательские, или другое) и необходимость взаимодействия с пользователем для успешной эксплуатации уязвимости. Третья группа включает ссылки на уязвимые продукты и их версии, ссылки на уязвимые конфигурации, ссылки на категорию слабых мест из базы слабых мест CWE, а также ссылки на описания в других источниках и возможные решения.

С точки зрения проводимого исследования, наибольший интерес представляют данные по метрикам CVSS, ссылки на уязвимые продукты и конфигурации, а также ссылки на слабые места CWE. Данные по сравнительным оценкам критичности CVSS для уязвимостей могут использоваться для определения цели атаки, т.к. определяют получаемые в результате эксплуатации привилегии и ущерб, являющиеся одними из основных характеристик цели атаки. Ссылки на уязвимое программно-аппаратное обеспечение и уязвимые конфигурации позволяют связать уязвимости и анализируемую информационную систему. Ссылки на слабые места позволяют, через уязвимости, связать анализируемую систему с ее слабыми местами и потенциальными атаками, а также целями этих атак.

База слабых мест CWE является наиболее полной базой слабых мест, то есть ошибок программного обеспечения, которые могут привести к появлению в нем уязвимостей [2]. Слабые места описываются с использованием ряда полей, заявленных схемой CWE [5]. Наиболее интересными, с точки зрения данного исследования, являются следующие поля: «Related Attack Patterns» (включает ссылки на записи в других базах, содержащих шаблоны атак), поскольку данное поле позволяет связать сущности базы CWE (слабые места) с сущностями базы CAPEC (атаки); «Observed Example» (ссылки на реальные примеры использования слабых мест, обычно на уязвимости), данное поле может использоваться для связи баз NVD и CWE, однако

достаточно небольшое количество примеров препятствует реальному применению. Другие интересные поля могут использоваться для выделения разных классов целей атак (например, «Applicable Platforms», т.е. языки, операционные системы, архитектуры, парадигмы, и технологии, при использовании которых может возникнуть слабое место, «Common Consequences», указывает на последствия слабого места, в том числе «Score» (какое свойство безопасности может быть нарушено), «Impact» (технический ущерб в случае успешного использования уязвимости), «Likelihood» (насколько вероятно, что будут именно эти последствия, а не другие), и другие).

База шаблонов атак CAPEC представляет собой описание методов и способов эксплуатации недостатков программного средства или системы безопасности, используемых злоумышленником для реализации угрозы информационной безопасности [3]. В основе базы лежит схема, включающая следующие основные типы элементов: сущности; элементы; элементы ссылки; перечисления; атрибуты. К сущностям относятся: каталог, представление («View»), категория («Category»), шаблон атаки.

Каталог шаблонов атак является корневым элементом схемы. Он содержит нумерованный список шаблонов атак, и организуется через представления, категории, и «External_References» (список ссылок, которые могут быть общими для всех шаблонов атак). Представления отображают перспективу, с которой рассматривается набор шаблонов атак. Категории – это коллекция шаблонов, объединенных общей характеристикой. Шаблон атаки – это абстракция, описывающая как выполняется атака, в том числе сложности, с которыми может столкнуться атакующий, методики для их преодоления и рекомендуемые методы остановки атаки. Структура базы формируется при помощи элементов ссылок: они позволяют как сформировать иерархическую структуру базы, так и связать похожие шаблоны внутри базы и вне ее. С помощью элементов и атрибутов определяются шаблоны атак и ссылки. Возможные значения элементов и атрибутов определяют перечисления.

Для определения цели атаки наибольший интерес представляет следующий элемент, описывающий шаблоны атаки: «Consequences» (последствия). А точнее его подэлементы: «Score» – нарушаемое свойство безопасности (возможные значения: «Confidentiality» (конфиденциальность); «Integrity» (целостность); «Availability» (доступность); «Access Control» (контроль доступа); «Accountability» (подотчетность); «Authentication» (аутентификация); Authorization (авторизация); Non-Repudiation («неотказуемость»); «Other» (другое)) и «Technical Impact» – технический ущерб в случае успешной атаки (возможные значения: «Modify Data» (изменение данных); «Read Data» (чтение данных); «Unreliable Execution» (ненадежное исполнение); «Resource Consumption» (истощение ресурсов); «Execute Unauthorized Commands» (выполнение неавторизованных команд); «Gain Privileges» (получение привилегий); «Bypass Protection Mechanism» (обход механизма защиты); «Hide Activities» (скрытые действия); «Alter Execution Logic» (обход логики выполнения); «Other» (другое)).

В основе предлагаемого подхода лежат связи между различными объектами предметной области, а именно, атакой, атакующим, атакуемым объектом, его уязвимостями и слабыми местами, а также целями атаки, связи между соответствующими метриками и классификация их значений.

Для отображения связей между объектами предметной области была разработана онтология, подробно описанная в статье [6]. Для текущего исследования интерес представляет фрагмент онтологии, связанный с перечисленными объектами и двумя показателями, которые могут использоваться для классификации целей атак, а именно «Score» и «Technical Impact» (рисунок 1).

Рисунок 1. Фрагмент онтологии с метриками атак и атакующего

Для того, чтобы доказать, что цели атаки можно классифицировать исходя из «Score» и «Technical Impact», была проанализирована база CAPEC. В ней имеются представления с идентификаторами '1000', '3000', '2000', '282', '283', '284', '553'. Всего в них содержится 568 шаблонов. Из них для 307 шаблонов подэлементы «Score» и «Technical Impact» имеют значения. Возможно 37 различных сочетаний значений «Score» и «Technical Impact», которые могут определять различные цели атак. В рамках базы CAPEC обнаружено 1290 сочетаний, с учетом повторений.

На рисунке 2 представлена статистика совместного использования возможных значений «Score» (по вертикали) и «Technical Impact» (по горизонтали) с учетом ситуации, когда в рамках одного шаблона возможно наличие нескольких пар «Score» и «Technical Impact» (то есть возможны различные варианты последствий атаки). Сумма частот составляет 2.271126760563381. На рисунке 3 представлена статистика совместного использования возможных значений с учетом нулевых пар (когда значения «Score» и «Technical Impact» равны «None»). Сумма частот составляет 4.201954397394137. На рисунке 4 представлена общая статистика совместного использования возможных значений. Сумма частот составляет 0.9999999999999998.

Корреляция Крамера для номинальных признаков между «Score» и «Technical Impact» без учета шаблонов с пустыми значениями составляет 0.42293458362479625, а с учетом шаблонов с пустыми значениями – 0.5209203125184796. Что позволяет заключить, что хотя эти показатели не являются зависимыми, они коррелируют.

Проведенные эксперименты позволяют заключить, что цель определяется областью атаки «Scope» и ущербом от атаки «Technical Impact», как связанными метриками.

В работе проанализированы база данных шаблонов атак CAPEC, база уязвимостей NVD и база слабых мест CWE. Анализ схемы, лежащей в основе CAPEC, позволил выделить признаки, характеризующие различные классы целей кибератак и сформировать на их основе онтологию метрик и целей атак. Эксперименты с данными базы CAPEC позволили выявить наличие зависимости между признаками и

возможность их применения для выделения разных классов целей атак. В дальнейшей работе планируется продолжить анализ, дополнительно используя для определения целей атак признаки слабых мест, представленные в базе CWE, а также использовать базу MITRE Att@ck, включающую записи о тактиках и методиках атакующих.

Рисунок 2. Статистика совместного использования возможных значений «Score» (по вертикали) и «Technical Impact» (по горизонтали), в рамках одного шаблона возможно наличие нескольких пар

Рисунок 3. Статистика совместного использования возможных значений «Score» (по вертикали) и «Technical Impact» (по горизонтали) с учетом нулевых пар

Рисунок 4. Общая статистика совместного использования возможных значений «Score» (по вертикали) и «Technical Impact» (по горизонтали)

Работа выполнена при частичной поддержке стипендии президента СП-751.2018.5 и бюджетной темы 0073-2019-0002.

1. National Vulnerability Database. Официальный веб-сайт. Режим доступа: <https://nvd.nist.gov/> (дата доступа: 20.09.2019).
2. Common Weakness Enumeration. Официальный веб-сайт. Режим доступа: <https://cwe.mitre.org/> (дата доступа: 20.09.2019).
3. Common Attack Pattern Enumeration and Classification. Официальный веб-сайт. Режим доступа: <https://capec.mitre.org/> (дата доступа: 20.09.2019).

4. Elena Doynikova, Igor Kotenko. Approach for determination of cyber attack goals based on the ontology of security metrics // Proceedings of the International Workshop "Advanced Technologies in Aerospace, Mechanical and Automation Engineering" (MIST: Aerospace-2018). October 20, 2018, Krasnoyarsk, Russia. IOP Conference Series: Materials Science and Engineering (MSE), IOP Publishing, Vol.450. 2018. 7 p. <https://doi.org/10.1088/1757-899X/450/5/052006>.
5. Common Weakness Enumeration schema. Режим доступа: <https://cwe.mitre.org/documents/schema/> (дата доступа: 12.10.2019).
6. Elena Doynikova, Andrey Fedorchenko and Igor Kotenko. Ontology of metrics for cyber security assessment // Proceedings of the 14th International Conference on Availability, Reliability and Security. August 26–29, 2019, Canterbury, United Kingdom. ACM, New York, NY, USA, 8 p. <https://doi.org/10.1145/3339252.3341496>.

Ермолаева В.В., Москвин А.С., Бредихин В.М.
Угрозы "всемирной паутины"

*Саратовский Государственный технический университет имени Ю.А.Гагарина
(Россия, Саратов)*

doi: 10.18411/lj-11-2019-34

idsp: ljjournal-11-2019-34

Аннотация

В наши дни интернет является неотъемлемой частью быта людей. Огромное количество людей ежеминутно заходят во «Всемирную паутину», дабы узнать о самых свежих новостях из разных новостных сайтов. Для людей, чья деятельность, так или иначе, связана с компьютером и информационными технологиями, Интернет является одним из основных источников дохода. Для большинства учащихся, в частности, школьников и студентов, это источник неисчерпаемого количества знаний и информации, возможность весело провести время и отдохнуть, играя в игры с друзьями, возможность удовлетворения потребности в общении посредством использования социальных сетей. Таким образом, каждый человек, который регулярно использует Интернет, может столкнуться с рядом угроз. Основными видами интернет – угроз являются социальная инженерия и технические угрозы. Самыми распространёнными техническими угрозами для нас, это вредоносные программы, DoS и ботнеты и DDoS-атаки. Эти программы выводят из строя ПК, сервер или компьютерную сеть. Такие программы могут удалять, изменять или красть наши данные компьютера, безусловно, это чревато плохими последствиями для дальнейшей работы компьютера. Вредоносные программы в большинстве случаев находятся на различных новостных сайтах и подобных популярных ресурсах, незаметно устанавливаются на компьютер пользователя, использующего данный сайт. Различные портативные носители данных, такие как USB или CD также могут быть источниками и распространителями вредоносных (вирусных) программ, а скачанные с Интернета файлы, необходимо проверять с помощью специальных программ, разработанных для поиска и уничтожения вредоносных программ. Все вирусные программы можно подразделить на троянские программы, черви и вирусы.

Ключевые слова: Сетевой червь, ботнет, компьютерный вирус, троянская программа, социальная инженерия, фишинг, DoS.

Abstract

Nowadays, the Internet is an integral part of people's lives. A huge number of people every minute go to the World Wide Web in order to learn about the latest news from various news sites. For people whose activities, one way or another, are connected with computers and information technologies, the Internet is one of the main sources of income. For most students, in particular, schoolchildren and students, this is a source of an inexhaustible amount of knowledge and information, the opportunity to have fun and relax, playing games with