УДК 004.056

Построение профиля атакующего на основе анализа сетевого трафика в критических инфраструктурах

Федорченко Е. В., Новикова Е. С., Гайфулина Д. А., Котенко И. В.

Постановка задачи: *модель атакующего является одной из ключевых моделей, применяемых в задачах анализа информационной безопасности, а ее определение является актуальной задачей. Известные способы определения модели атакующего не позволяют связать его верхнеуровневые абстрактные характеристики, определяемые стандартами, и низкоуровневые параметры, собираемые системами мониторинга и анализа информационной безопасности.* ***Целью работы*** *является определение модели атакующего при помощи набора низкоуровневых атрибутов, вычисляемых на основе журналов событий и сетевого трафика для анализа информационной безопасности критических инфраструктур.* ***Используемые методы****: для определения набора атрибутов, и связи верхнеуровневых атрибутов с низкоуровневыми, использовались методы системного анализа. Для проверки корректности отображения низкоуровневых атрибутов на верхнеуровневые использовались методы анализа данных, а именно, методы кластеризации, включая алгоритмы t-SNE, многомерного шкалирования и метод k-средних.* ***Новизна.*** *Новизна работы заключается в предложенной модели атакующего и методах определения ее параметров. Также к элементам новизны относится предложенная классификация параметров (атрибутов).* ***Результат****: в статье предложена классификация атрибутов атакующего. Вводится формальная модель атакующего, объединяющая низкоуровневые атрибуты, значения которых вычисляются на основе данных, получаемых из сетевого трафика, и верхнеуровневые характеристики атакующего. Проведенные эксперименты показывают, что выбранные атрибуты применимы для профилирования атакующего. В будущих исследованиях планируется провести дополнительные эксперименты и разработать методики анализа информационной безопасности, использующие предложенную модель атакующего.* ***Практическая значимость****: разработанная модель атакующего может использоваться в рамках систем мониторинга и анализа информационной безопасности в критических инфраструктурах для прогнозирования поведения атакующего и оптимизации выбора мер реагирования на инциденты, а также сбора информации об атакующем. Также она может использоваться при расследовании инцидентов безопасности.*

Ключевые слова: *модель атакующего, профилирование атакующего, атрибуты, сетевой трафик, информационная безопасность, анализ данных, критические инфраструктуры.*

Введение

Определение модели атакующего является важным этапом анализа информационной безопасности. Особенно это актуально для критических инфраструктур, включая информационные системы, телекоммуникационные сети и автоматизированные системы управления технологическими процессами, такие как здравоохранение, финансовая сфера, топливно-энергетический комплекс, военно-промышленный комплекс и другие. Это связано с тем, что такие систе-

Библиографическая ссылка на статью:
Федорченко Е. В., Новикова Е. С., Гайфулина Д. А., Котенко И. В. Построение профиля атакующего на основе анализа сетевого трафика в критических инфраструктурах // Системы управления, связи и безопасности. 2021. № 6. С. 76-89. DOI: 10.24412/2410-9916-2021-6-76-89.

Reference for citation:
Fedorchenko E. V., Novikova E. S., Gaifulina D. A., Kotenko I. V. Attacker profiling based on the network traffic analysis. *Systems of Control, Communication and Security*, 2021, no. 6, pp. 76-89 (in Russian). DOI: 10.24412/2410-9916-2021-6-76-89.

мы подвержены целевым атакам, осуществляемым атакующими с высокой квалификацией, и атакам с участием внутреннего злоумышленника, в случае которых важно собрать как можно больше информации об атакующем, чтобы идентифицировать его/ее и обезвредить.

Предложенные к настоящему моменту модели атакующего можно разделить на верхнеуровневые и низкоуровневые. Под верхнеуровневой будем понимать модель, определенную с использованием верхнеуровневых атрибутов. К таким атрибутам относятся цель атакующего, положение атакующего, сложность использованных уязвимостей, зафиксированные инциденты и др. Например, в [1] используется набор критических параметров, фиксируемых при каждом шаге атакующего. Такие атрибуты позволяют выделить такие классы атакующих как хакеры, шпионы, террористы, корпоративные рейдеры, профессиональные преступники, вандалы и вуайеристы. Отдельно можно выделить внутренних атакующих. Например, в [2] для их выявления используются такие верхнеуровневые атрибуты как уровень квалификация сотрудника, уровень доступа сотрудника к информационным ресурсам, должность сотрудника, стаж сотрудника. Верхнеуровневые модели обычно используются в методиках определения типа атакующего и анализа информационной безопасности, основанных на графах атак [1, 3-9], или в методиках, основанных на нечетком выводе [2, 10, 11]. Под низкоуровневыми будем понимать модель, определенную с использованием низкоуровневых атрибутов (или признаков). К таким атрибутам относятся порт назначения, сигнатура предупреждения, хост, и др. Низкоуровневые модели обычно используются в методиках анализа информационной безопасности, основанных на скрытых Марковских моделях [12-15] и нечетком выводе [16, 17]. Кроме того, они используются при атрибуции кибератак с использованием методов интеллектуального анализа данных [18, 19, 20].

Преимуществом методик, основанных на атрибуции кибератак, перед методиками, основанными на графах атак, является то, что они позволяют определить верхнеуровневые характеристики (или атрибуты) атаки и атакующего на основе объективных низкоуровневых атрибутов. К их недостаткам можно отнести высокую сложность определения связей между верхнеуровневыми и низкоуровневыми атрибутами, и недостаток подходящих наборов данных для обучения модели. В [21] авторами данной статьи был сформулирован ряд вопросов, связанных с разработкой модели атакующего, в том числе:

1. Как определить модель атакующего?
2. Как определить значения атрибутов, входящих в модель атакующего, не экспертно, а вычислить с использованием динамических данных, получаемых из сетевого трафика в процессе работы анализируемой системы?
3. Как получить подходящие для экспериментов исходные данные?
4. Действительно ли явное определение модели атакующего необходимо при анализе информационной безопасности?

В данной статье рассматриваются первые три вопроса. Как результат ответа на первые два вопроса вводится формальная модель атакующего, атрибуты модели и первичное отображение между верхнеуровневыми и низкоуровневы-

ми атрибутами модели. Как результат ответа на третий вопрос в статье приводится описание входных данных для экспериментов и процесс их обработки. В будущих исследованиях планируется расширить эксперименты, ответить на последний из поставленных вопросов и разработать методику анализа информационной безопасности для критических инфраструктур, использующую предложенную модель атакующего.

Таким образом, результаты проведенного исследования, описываемые в данной статье, следующие: формальная модель атакующего, объединяющая низкоуровневые атрибуты, значения которых вычисляются на основе данных, получаемых из сетевого трафика, и верхнеуровневые характеристики атакующего; классификация атрибутов атакующего; первичное отображение между верхнеуровневыми и низкоуровневыми атрибутами модели; требования к исходным данным для экспериментов и варианты наборов данных для экспериментов; результаты первых экспериментов с подмножеством атрибутов атакующего.

Постановка задачи

Для формальной постановки и решения задачи в работе введены обозначения, представленные в таблице 1.

Таблица 1 – Обозначения

Обозначение	Физический смысл обозначения
$At=\{hf_1,\ldots,hf_k\}$	– модель атакующего
$hf_i, i \in [1,k]$	– верхнеуровневые характеристики (атрибуты) атакующего
k	– количество верхнеуровневых характеристик атакующего
V^i	– множество возможных значений hf_i
$lf_j, j \in [1,m]$	– низкоуровневый атрибут атакующего, определяемый на основе данных, получаемых из сетевого трафика
m	– количество низкоуровневых характеристик атакующего
$func(lf_j)$	– функция вычисления верхнеуровневых атрибутов на основе низкоуровневых

Задача определения модели атакующего *At* может быть декомпозирована на следующие подзадачи:

- определение верхнеуровневых атрибутов модели атакующего;
- анализ сетевого трафика для отображения низкоуровневых атрибутов на верхнеуровневые;
- проверка корректности отображения низкоуровневых атрибутов на верхнеуровневые с использованием методов кластеризации (возврат на предыдущий шаг в случае невозможности кластеризации атакующих по выбранным атрибутам);
- разработка алгоритмов вычисления верхнеуровневых атрибутов на основе низкоуровневых с использованием методов классификации.

На формальном уровне постановка задачи исследования имеет следующий вид.

Дано: сетевой трафик, содержащий атакующие действия различных типов атакующих $At=\{hf_1,...,hf_k\}$. Найти: низкоуровневые атрибуты атакующего lf_j, вычисляемые на основе сетевого трафика, и верхнеуровневые атрибуты атакующего $hf_i = func(lf_j)$. С учетом подзадач, выделенных выше, необходимо:

- определить $hf_i, i \in [1, k]$, входящие в At;
- определить $lf_j, j \in [1, m]$ для каждого hf_i;
- разбить lf_j для каждого hf_i на кластеры V^i в соответствии с возможными значениями hf_i;
- определить корректность разбиения на кластеры.

Далее кластеризованные данные могут использоваться для обучения, чтобы определять hf_i и lf_j для обнаруженного в сети атакующего At (классификация lf_j для нового фрагмента трафика).

В исследовании, описываемом в данной статье, авторы ограничиваются одним верхнеуровневым атрибутом модели атакующего – уровнем навыков атакующего – и соответствующими ему низкоуровневыми характеристиками. Как следствие, постановка задачи для эксперимента приобретает вид:

- определить $lf_j, j \in [1, m]$ для верхнеуровнего атрибута «уровень навыков атакующего»;
- разбить lf_j для верхнеуровнего атрибута «уровень навыков атакующего» на кластеры $V^i = \{$высокий, средний, низкий$\}$;
- проверить корректность разбиения в соответствии с уровнем навыков атакующих в анализируемом сетевом трафике.

Подход к построению профиля атакующего и эксперименты

Значения верхнеуровневых атрибутов атакующего обычно определяются экспертными методами и как следствие субъективны. Можно выделить следующие классы верхнеуровневых атрибутов, описывающие различные аспекты поведения атакующего:

- собственные характеристики атакующего (например, уровень навыков атакующего, уровень мотивации, намерения);
- возможности атакующего (например, используемые ресурсы);
- характеристики, которые позволяют связать атакующего с атакуемой системой (например, местоположение атакующего, его привилегии в системе, цели, и знания о системе);
- характеристики, связывающие атакующего и атаку (например, шаги атаки/атакующего).

Атрибуты разных классов могут быть связаны между собой, так, используемые ресурсы и уровень навыков атакующего связаны через уровень сложности использования ресурсов.

Низкоуровневые атрибуты могут быть вычислены напрямую на основе данных получаемых из журналов событий и сетевого трафика, и как следствие объективны. В [18] была предложена следующая классификация атрибутов, определяемых на основе сетевого трафика, в зависимости от природы исходных данных, на основе которых они вычисляются:

– атрибуты источника;
– атрибуты цели;
– атрибуты содержимого;
– временные атрибуты.

В данной работе предлагается расширить эту классификацию за счет учета журнала событий как источника входных данных для вычисления значений атрибутов, и добавить класс наблюдаемых характеристик (атрибутов).

Атрибуты источника характеризуют источник атаки либо нормального действия. Атрибуты цели характеризуют цель атаки или нормального действия. Атрибуты содержимого характеризуют содержимое или нагрузку атакующего или нормального действия. Временные атрибуты включают частотные и временные характеристики атаки на выбранном временном интервале. Наблюдаемые атрибуты включают характеристики, связанные с наблюдениями, такие как сигнатура или категория предупреждения.

Следующим шагом определения модели атакующего является выделение связанных верхнеуровневых и низкоуровневых атрибутов, как в таблице 2.

Таблица 2 – Примеры выделения связанных верхнеуровневых и низкоуровневых атрибутов

Верхнеуровневые атрибуты	Группы низкоуровневых атрибутов	Низкоуровневые атрибуты
Уровень навыков атакующего	Скрытность атакующего	*Частота и распределенность предупреждений*
	Сложность используемых инструментов	*Количество используемых эксплойтов*. *Критичность используемых эксплойтов*
	Сложность действий атакующего, их критичность и производительность	Частота получения и отправки сетевых пакетов. Частота получения и отправки байт, или количество байт в единицу времени. Количество TCP диалогов между TCP-точками. Количество TCP-точек из сетевого трафика, т.е. пар IP адрес и порт. Количество IP-точек из сетевого трафика. Количество портов. Количество протоколов. Количество IP диалогов между IP-точками. Количество IP-адресов. *Частота и распределенность предупреждений/атак*. *Средняя критичность предупреждений*. *Количество используемых уязвимостей/эксплойтов*
Уровень мотивации атакующего	Длительность попыток атаки	Частота и распределенность предупреждений/атак. Частота получения и отправки сетевых пакетов. Частота получения и отправки байт, или количество байт в единицу времени. Количество IP диалогов. Количество TCP диалогов. Количество файлов в единицу времени. Время между сессиями. Количество сессий в единицу времени. Количество портов/протоколов/эксплойтов.

Для завершения определения модели атакующего необходимо разработать методы и алгоритмы вычисления верхнеуровневых атрибутов на основе низкоуровневых.

Для проверки корректности отображения низкоуровневых атрибутов на верхнеуровневые, необходимо провести эксперименты. В данном исследовании эксперименты проводятся на основе одного типа данных – сетевого трафика, и для одного верхеуровнего атрибута модели атакующего – уровень навыков атакующего. Эксперименты с другими источниками данных и другими верхнеуровневыми атрибутами будут проводиться в будущих исследованиях.

В общем случае задача атрибуции является задачей классификации, и для нее требуется размеченный набор данных. К набору данных были сформулированы следующие требования.

1. Набор данных должен содержать большое количество атакующих действий против одной информационной системы, выполненных атакующими с разным уровнем навыков, ресурсами, намерениями и мотивацией.
2. Набор данных должен быть размечен, т.к. для обучения модели необходимо знать какие действия каким типом атакующих были совершены.

Таким требованиям удовлетворяют наборы данных, собираемые во время соревнований «захват флага» (capture the flag, CTF). Однако в таких наборах данных нет явных меток верхнеуровневых атрибутов атакующего. Тем не менее, можно сделать выводы о значениях этих атрибутов на основе информации о победителях соревнований. В рамках исследования были выбраны 2 набора данных, содержащих сетевой трафик с соревнований DEFCON 25 и DEFCON 26 CTF [22], посвященных компрометации целевой инфраструктуры.

В данном исследовании были проведены эксперименты для проверки корректности отображения между верхнеуровневым атрибутом «уровень навыков атакующего» и рядом низкоуровневых атрибутов, вычисляемых с использованием выбранного набора данных. Поскольку в данной работе для экспериментов используется только сетевой трафик, низкоуровневые атрибуты, выделенные в таблице 2 курсивом, пока были исключены из рассмотрения.

В процессе эксперимента сетевой трафик с DEFCON 25 и DEFCON 26 CTF [22] был проанализирован и разделен на фрагменты, соответствующие отдельным командам. Для каждого фрагменты были вычислены следующие низкоуровневые атрибуты (или признаки):

- частота получения и отправки сетевых пакетов;
- частота получения и отправки байт, или количество байт в единицу времени;
- количество TCP диалогов между TCP-точками;
- количество TCP-точек из сетевого трафика, т.е. пар IP адрес и порт;
- количество IP-точек из сетевого трафика;
- количество портов;

– количество протоколов;
– количество IP диалогов между IP-точками;
– количество IP-адресов.

Перечисленные низкоуровневые атрибуты могут использоваться для определения верхнеуровнего атрибута «уровень навыков атакующего». Эксперимент был направлен на то, чтобы проверить, позволяют ли выбранные низкоуровневые атрибуты выделить группы атакующих с одинаковым значением верхнеуровневого атрибута «уровень навыков атакующего». В процессе эксперимента вначале была проведена статистическая оценка параметров набора данных с DEFCON 26 CTF и применены методы кластеризации: алгоритмы t-SNE (нелинейная проекция многомерного пространства на пространство низкой размерности, например, двумерное, позволяет преобразовать сходство между точками данных в вероятность того, что эти точки будут соседними) [23] и метод многомерного шкалирования (метод расположения точек в пространстве меньшей размерности, при котором точки размещаются так, чтобы сохранить исходные попарные расстояния между точками в пространстве) [24]. Хотя эти алгоритмы показали похожие результаты, применение многомерного шкалирования позволило выявить кластеры по атрибуту «уровень навыков атакующего» более четко. После определения количества возможных кластеров к ним был применен метод k-средних [25].

Проекция профилей команд (верхнеуровневого атрибута «уровень навыков атакующего») на двумерное пространство, полученная в результате применения метода многомерного шкалирования к векторам признаков (низкоуровневых атрибутов), представлена на рис. 1. Подписи к осям координат на рис. 1 опущены, поскольку интерес представляют не конкретные координаты, а выделенные кластеры, которые позволяют визуально оценить схожесть профилей команд. Оттенок узла на рисунке определяет принадлежность к одному из трех профилей, выделенных по верхнеуровневому атрибуту «уровень навыков атакующего», а размер узлов соответствует частоте получения и отправки сетевых пакетов. Из рисунка видно, что одна команда явно выделяется, другой кластер включает три команды, а профили остальных команд очень похожи и образуют третий кластер.

Результаты совпадают с ожиданиями, т.к. логично предположить, что все команды, участвовавшие в финале CTF, имеют похожий высокий уровень навыков. Поскольку не удалось найти соответствие между конкретными командами и их результатами, не удалось соотнести полученные кластеры с конкретными значениями уровня навыков. Тем не менее, можно заключить, что выбранные низкоуровневые атрибуты позволяют выделить разные значения верхнеуровневого атрибута «уровень навыков атакующего».

В процессе эксперимента также был проанализирован сетевой трафик с DEFCON 25 CTF. В отличие от DEFCON 26 CTF, удалось найти соответствие между конкретными командами и их результатами. Результаты эксперимента показали, что выделенных атрибутов недостаточно для определения уровня навыков атакующего, т.к. хотя команды, показавшие высокие результаты, были

выделены в отдельный кластер, команда, которая победила, оказалась в одном кластере с командами, получившими средние оценки.

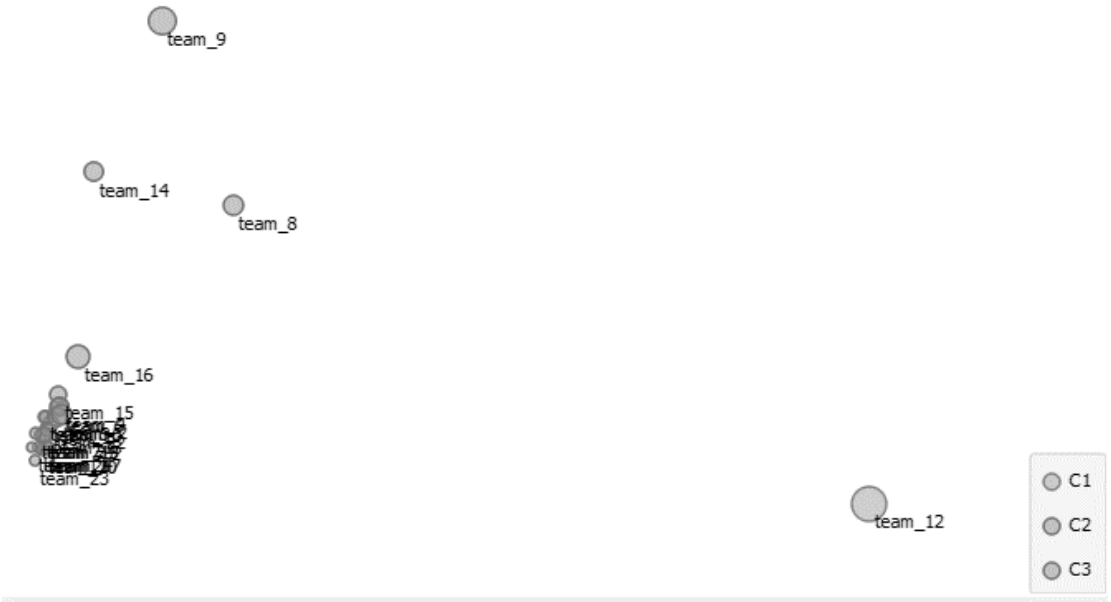

Рис. 1. Многомерное шкалирование признаков,
характеризующих поведение команд DEFCON 26 CTF

Поэтому на следующем этапе планируется включить в набор низкоуровневых атрибутов характеристики, вычисляемые на основе данных из журналов событий.

Выводы

В рамках проведённого исследования была изучена концепция модели атакующего. Определен подход к формированию объективной модели атакующего, включающий формальное определение модели атакующего на основе верхнеуровневых и низкоуровневых атрибутов, последовательное отображение низкоуровневых атрибутов на верхнеуровневые, и разработку методов и алгоритмов вычисления верхнеуровневых атрибутов на основе низкоуровневых. Разработана формальная спецификация модели атакующего на основе верхнеуровневых и низкоуровневых атрибутов. Предложена классификация верхнеуровневых и низкоуровневых атрибутов и первичное отображение между ними. Определены требования к наборам данных для экспериментов по проверке корректности отображения низкоуровневых атрибутов на верхнеуровневые. Выбраны два подходящих набора данных для экспериментов. Проведены эксперименты по кластеризации атакующих на основе уровня навыков с использованием выбранных наборов данных и соответствующего набора низкоуровневых атрибутов. Эксперименты подтвердили, что выбранные низкоуровневые атрибуты позволяют разделить атакующих на группы в соответствии с разными значениями верхнеуровневого атрибута «уровень навыков атакующего».

Новизна работы заключается в предложенной классификация параметров (атрибутов) атакующего, модели атакующего и методах определения ее параметров.

Наиболее близкой работой по подходу к профилированию атакующего является работа [18], однако основное отличие состоит в используемых признаках (низкоуровневых атрибутах, извлекаемых из сетевого трафика) и в том, что авторы [18] не знают уровня атакующих, в то время как авторы данной работы делают предположение об уровне атакующих на основе того, какое место они заняли на соревнованиях CTF.

Разработанную модель атакующего планируется использовать в рамках систем мониторинга и анализа информационной безопасности критических инфраструктур для прогнозирования поведения атакующего и оптимизации выбора мер реагирования на инциденты, а также сбора информации об атакующем, что особенно актуально для таких систем.

В будущих исследованиях планируется уточнить набор низкоуровневых атрибутов и соответствие между низкоуровневыми и верхнеуровневыми атрибутами атакующего, провести дополнительные эксперименты на новых наборах данных, разработать алгоритмы вычисления верхнеуровневых атрибутов на основе низкоуровневых, и разработать методику анализа информационной безопасности, использующую предложенную модель атакующего.

Работа выполнена при частичной финансовой поддержке проекта РФФИ 19-07-01246 А и бюджетной темы 0073-2019-0002.

Литература

1. Калашников А. О., Савенков Г. А. Разработка чистых стратегий ложной информационной системы и злоумышленника в антогонистической игре в условиях реализации атаки на информационную систему // Информация и безопасность. 2016. № 2 (19). С. 262-265.

2. Силантьев И. О., Аникин И. В. Выявление внутренних нарушителей в корпоративных сетях с помощью методов нечеткой логики // Информация и безопасность. 2017. №. 3 (20). С. 448-451.

3. Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H. A Service Dependency Model for Cost-Sensitive Intrusion Response // ESORICS Proceedings (Athens, Greece, 2010). LNCS. 2010. P. 626-642.

4. Котенко И. В., Дойникова Е. В. Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности // Информационно-управляющие системы. 2015. № 3. С. 60-69.

5. Ingols K., Chu M., Lippmann R., Webster S., Boyer S. Modeling Modern Network Attacks and Countermeasures Using Attack Graphs // Proceedings of the 2009 Annual Computer Security Applications Conference (Honolulu, HI, USA, 2009). 2009.

6. Kotenko I., Stepashkin M. Attack Graph based Evaluation of Network Security // Proceedings of the IFIP International Conference on Communications and Multimedia Security (Heraklion, Crete, Greece, 2006). Springer Berlin Heidelberg, 2006. P. 216-227.

7. GhasemiGol M., Ghaemi-Bafghi A., Takabi H. A comprehensive approach for network attack forecasting // Computers & Security. 2016. Vol. 58. P. 83-105.

8. Wang L., Islam T., Long T., Singhal A., Jajodia S. An Attack Graph-Based Probabilistic Security Metric // Proceedings of the Data and Applications Security XXII (Montreal, QC, Canada, 2008). Springer, 2008. P. 216-227.

9. Дойникова Е. В., Котенко И. В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Труды СПИИРАН. 2018. № 2 (57). С. 211-240.

10. Pricop E., Mihalache S. F. Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems // Proceedings of the 7th International Conference on Electronics, Computers and Artificial Intelligence (Bucharest, Romania, 2015). IEEE, 2015.

11. Mallikarjunan K. N., Shalinie S. M., Preetha G. Real Time Attacker Behavior Pattern Discovery and Profiling Using Fuzzy Rules // Journal of Internet Technology. 2018. Vol. 19. No. 5. P. 1567-1575.

12. Katipally R., Yang L., Liu A. Attacker behavior analysis in multi-stage attack detection system // CSIIRW Proceedings (Oak Ridge, TN, USA, 2011). ACM: New York, NY, USA, 2011.

13. Rashid T., Agrafiotis I., Nurse J. R. C. A New Take on Detecting Insider Threats: Exploring the Use of Hidden Markov Mode // Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats (Vienna, Austria, 2016). ACM, 2016. P. 47-56.

14. Bar A., Shapira B., Rokach L., Unger M. Identifying attack propagation patterns in honeypots using Markov chains modeling and complex networks analysis // Proceedings of the IEEE International Conference on Software Science, Technology and Engineering (Beer Sheva, Israel, 2016). 2016. P. 28-36.

15. Deshmukh S., Rade R., Kazi F. Attacker behaviour profiling using stochastic ensemble of hidden Markov models // Arxiv.org. 2019. – URL: https://arxiv.org/abs/1905.11824 (дата обращения 7.11.2021).

16. Shyla S., Sujatha S. Cloud security: LKM and optimal fuzzy system for intrusion detection in cloud environment // Journal of Intelligent Systems. 2019. No. 29. P. 1626-1642.

17. Kudłacik P., Porwik P., Wesołowski T. Fuzzy approach for intrusion detection based on user's commands // Soft Computing. 2016. Vol. 20. P. 10-16.

18. Fraunholz D., Krohmer D., Duque Anton S., Schotten H. D. YAAS - On the attribution of honeypot data // International Journal on Cyber Situational Awareness. 2017. No. 19. P. 31-48.

19. Rid T., Buchanan B. Attributing cyber attacks // Journal of Strategic Studies. 2015. Vol. 38. P. 4-37.

20. Шелухин О. И. Технологии машинного обучения в сетевой безопасности. – Горячая Линия - Телеком, 2021. – 360 с.

21. Doynikova E., Novikova E., Kotenko I. Attacker behaviour forecasting using methods of intelligent data analysis: a comparative review and prospects // Information. 2020. No. 11.

22. DEFCON 26 CTF официальный сайт [Электронный ресурс]. – URL: https://media.defcon.org/DEF%20CON%2026/DEF %20CON%2026%20ctf/ (дата обращения 7.11.2021).

23. Van der Maaten L., Hinton G. Visualizing data using t-SNE // Journal of machine learning research. 2008. № 9.

24. Torgerson W. S. Multidimensional scaling: I. Theory and method // Psychometrika. 1952. № 17. P. 401-419.

25. MacQueen J. Some methods for classification and analysis of multivariate observations // Proceedings of the fifth Berkeley symposium on mathematical statistics and probability. 1967. № 14 (1).

References

1. Kalashnikov A. O., Savenkov G. A. Razrabotka chistyh strategij lozhnoj informacionnoj sistemy i zloumyshlennika v antogonisticheskoj igre v usloviyah realizacii ataki na informacionnuyu sistemu [Development of pure strategies for a false information system and an attacker in an antagonistic game in the context of an attack on an information system]. *Informaciya i bezopasnost'* [Information and Security], 2016, vol. 19, no. 2, pp. 262-265 (in Russian).

2. Silantyev I. O., Anikin I. V. Vyyavlenie vnutrennih narushitelej v korporativnyh setyah s pomoshch'yu metodov nechetkoj logiki [Identifying intruders on corporate networks using fuzzy logic techniques]. *Informaciya i bezopasnost'* [Information and Security], 2017, vol. 20, no. 3, pp. 448-451 (in Russian).

3. Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H. A Service Dependency Model for Cost-Sensitive Intrusion Response. *ESORICS Proceedings*, Athens, Greece, 2010, pp. 626-642.

4. Kotenko I., Doynikova E. Countermeasure Selection in Security Management Systems. *Information and Control Systems*, 2015. no. 3, pp. 60-69 (in Russian).

5. Ingols K., Chu M., Lippmann R., Webster S., Boyer S. Modeling Modern Network Attacks and Countermeasures Using Attack Graphs. *Proceedings of the 2009 Annual Computer Security Applications Conference*. Honolulu, HI, USA, 2009.

6. Kotenko I., Stepashkin M. Attack Graph based Evaluation of Network Security. *Proceedings of the IFIP International Conference on Communications and Multimedia Security*. Heraklion, Crete, Greece, 2006, pp. 216-227.

7. GhasemiGol M., Ghaemi-Bafghi A., Takabi H. A Comprehensive Approach for Network Attack Forecasting. *Computers & Security*, 2016, vol. 58, pp. 83-105.

8. Wang L., Islam T., Long T., Singhal A., Jajodia S. An Attack Graph-Based Probabilistic Security Metric. *Proceedings of the Data and Applications Security XXII*. Montreal, QC, Canada, 2008, pp. 216-227.

9. Kotenko I., Doynikova E. Improvement of Attack Graphs for Cybersecurity Monitoring: Handling of Inaccuracies, Processing of Cycles, Mapping of Incidents and Automatic Countermeasure Selection. *SPIIRAS Proceedings*, 2018, vol. 57, pp. 211-240 (in Russian).

10. Pricop E., Mihalache S. F. Fuzzy Approach on Modelling Cyber Attacks Patterns on Data Transfer in Industrial Control Systems. *Proceedings of the 7th*

International Conference on Electronics, Computers and Artificial Intelligence. Bucharest, Romania, 2015.

11. Mallikarjunan K. N., Shalinie S. M., Preetha G. Real Time Attacker Behavior Pattern Discovery and Profiling Using Fuzzy Rules. *Journal of Internet Technology*, 2018, vol. 19, no. 5, pp. 1567-1575.

12. Katipally R., Yang L., Liu A. Attacker Behavior Analysis in Multi-stage Attack Detection System. *CSIIRW Proceedings*. Oak Ridge, TN, USA, 2011.

13. Rashid T., Agrafiotis I., Nurse J. R. C. A New Take on Detecting Insider Threats: Exploring the Use of Hidden Markov Mode. *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats.* Vienna, Austria, 2016, pp. 47-56.

14. Bar A., Shapira B., Rokach L., Unger M. Identifying Attack Propagation Patterns in Honeypots Using Markov Chains Modeling and Complex Networks Analysis. *Proceedings of the IEEE International Conference on Software Science, Technology and Engineering*. Beer Sheva, Israel, 2016, pp. 28-36.

15. Deshmukh S., Rade R., Kazi F. Attacker Behaviour Profiling Using Stochastic Ensemble of Hidden Markov Models. 2019. URL: https://arxiv.org/abs/1905.11824 (дата обращения: 07.11.2021).

16. Shyla S., Sujatha S. Cloud security: LKM and Optimal Fuzzy System for Intrusion Detection in Cloud Environment. *Journal of Intelligent Systems*, 2019, no. 29, pp. 1626-1642.

17. Kudłacik P., Porwik P., Wesołowski T. Fuzzy Approach for Intrusion Detection based on User's Commands. *Soft Computing*, 2016, vol. 20, pp. 10-16.

18. Fraunholz D., Krohmer D., Duque Anton S., Schotten H. D. YAAS - On the Attribution of Honeypot Data. *International Journal on Cyber Situational Awareness*, 2017, no. 19, pp. 31-48.

19. Rid T., Buchanan B. Attributing Cyber Attacks. *Journal of Strategic Studies*, 2015, vol. 38, pp. 4-37.

20. Sheluhin O. I. *Tekhnologii mashinnogo obucheniya v setevoj bezopasnosti* [The machine learning technology in network security].Moscow, Hot line - Telecom, 2021. 360 p. (in Russian).

21. Doynikova E., Novikova E., Kotenko I. Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects. *Information*, 2020, no. 11.

22. DEFCON 26 CTF official web-site. URL: https://media.defcon.org/DEF%20CON%2026/DEF %20CON%2026%20ctf/ (дата обращения: 07.11.2021).

23. Van der Maaten L., Hinton G. Visualizing Data using t-SNE. *Journal of machine learning research*, 2008, no. 9.

24. Torgerson W. S. Multidimensional Scaling: I. Theory and Method. *Psychometrika*, 1952, no. 17, pp. 401-419.

25. MacQueen J. Some Methods for Classification and Analysis of Multivariate Observations. *Proceedings of the fifth Berkeley symposium on mathematical statistics and probability*. 1967, vol. 1, no. 14.

Статья поступила 15 ноября 2021 г.

Информация об авторах

Федорченко Елена Владимировна – кандидат технических наук. Старший научный сотрудник лаборатории проблем компьютерной безопасности. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук. Область научных интересов: информационная безопасность; анализ и оценивание информационной безопасности; метрики защищенности; поддержка принятия решений; интеллектуальные методы анализа данных; цифровая криминалистика. E–mail: doynikova@comsec.spb.ru

Новикова Евгения Сергеевна – кандидат технических наук, доцент. Старший научный сотрудник лаборатории проблем компьютерной безопасности. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук. Область научных интересов: информационная безопасность; безопасность промышленного интернета вещей; визуальная аналитика. E–mail: novikova@comsec.spb.ru

Гайфулина Диана Альбертовна – соискатель ученой степени кандидата технических наук. Младший научный сотрудник лаборатории проблем компьютерной безопасности. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук. Область научных интересов: информационная безопасность; киберфизические системы; интеллектуальный анализ данных; обнаружение аномалий в среде передачи данных. E–mail: gaifulina@comsec.spb.ru

Котенко Игорь Витальевич – доктор технических наук, профессор. Руководитель лаборатории проблем компьютерной безопасности. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук. Область научных интересов: безопасность компьютерных сетей; управление политиками безопасности; разграничение доступа; аутентификация; анализ защищенности; обнаружение компьютерных атак; межсетевые экраны; защита от вирусов и сетевых червей; анализ и верификация протоколов безопасности и систем защиты информации; защита программного обеспечения от взлома и управление цифровыми правами; технологии моделирования и визуализации для противодействия кибер-терроризму. E–mail: ivkote@comsec.spb.ru

Адрес: 199178, Россия, Санкт-Петербург, 14 линия В.О., д. 39.

Attacker profiling based on the network traffic analysis

E. V. Fedorchenko, E. S. Novikova, D. A. Gaifulina, I. V. Kotenko

Problem statement. *The attacker's model is one of the key models used in the tasks of information security analysis, and its specification is a relevant task. The known methods of the attacker's model determination do not allow connecting his/her high-level abstract characteristics defined by the standards and low-level characteristics collected by information security monitoring and analysis systems.* ***Purpose.*** *The purpose of the research is to determine the attacker's model using a set of low-level attributes calculated on the basis of network traffic.* ***Methods.*** *To determine the set of attributes, and the relationship of high-level*

attributes with low-level ones, the methods of system analysis were used. To check the correctness of the mapping of low-level attributes to high-level ones, data analysis methods were used, namely, clustering methods, including t-SNE algorithms, multidimensional scaling, and the k-means method. ***Novelty.*** *The novelty of the research lies in the proposed attacker model and methods for determining its parameters. Also, the proposed classification of attributes belongs to the elements of novelty.* ***Results.*** *The paper proposes a classification of the attacker's attributes. A formal attacker model is introduced that combines low-level attributes, the values of which are calculated based on data obtained from the network traffic, and the high-level characteristics of the attacker. Experiments have shown that the selected attributes are applicable to profiling an attacker. In future research, it is planned to conduct additional experiments and develop methods for analyzing information security using the proposed attacker model.* ***Practical relevance.*** *The developed attacker model can be used within the framework of information security monitoring and analysis systems to forecast the attacker's behavior and optimize the selection of incident response measures. It can also be used in the investigation of security incidents.*

Key words: *attacker model, attacker profiling, network traffic, attributes, information security, data analysis.*

Information about Authors

Elena Vladimirovna Fedorchenko – Ph.D. of Engineering Sciences. Senior Researcher at the Laboratory of Computer Security Problems. St. Petersburg Federal Research Center of the Russian Academy of Sciences. Field of research: information security; information security analysis and assessment; security metrics; security decision support; intelligent methods of data analysis; digital forensics. E–mail: doynikova@comsec.spb.ru

Evgenia Sergeevna Novikova – Ph.D of Engineering Sciences. Senior Researcher at the Laboratory of Computer Security Problems. St. Petersburg Federal Research Center of the Russian Academy of Sciences. Field of research: information security; IoT security and privacy; visual analytics. E–mail: novikova@comsec.spb.ru

Diana Albertovna Gaifulina – Doctoral Student. Junior Researcher at the Laboratory of Computer Security Problems. St. Petersburg Federal Research Center of the Russian Academy of Sciences. Field of research: information security; cyber physical systems; intelligent data analysis; anomaly detection. E–mail: gaifulina@comsec.spb.ru

Igor Vitalievich Kotenko – Dr. habil. of Engineering Sciences, Full Professor. Head of the Laboratory of Computer Security Problems. St. Petersburg Federal Research Center of the Russian Academy of Sciences. Field of research: computer network security; security policy management; access control; authentication; network security analysis; intrusion detection; firewalls; deception systems; malware protection; verification of security systems; digital right management; modeling; simulation and visualization technologies for counteraction to cyber terrorism. E–mail: ivkote@comsec.spb.ru

Address: Russia, 199178, Saint Petersburg, 14th Linia, 39.