Вариант классификации процедур мониторинга сетевого трафика в интересах обнаружения вредоносной информации и компьютерных атак

Дойникова Е.В., Котенко И.В., Паращук И.Б.

Лаборатория проблем компьютерной безопасности

Санкт-Петербургский институт информатики и автоматизации

Российской академии наук (СПИИРАН)

Санкт-Петербург, Россия

ICCTI-2020, St. Petersburg, Russia, April 13-14, 2020

План доклада

- Введение
- Релевантные работы
- Существующие сложности
- Процедуры мониторинга сетевого трафика
- Классификация процедур мониторинга сетевого трафика: классификационные *признаки процедуры наблюдения*
- Классификация процедур мониторинга сетевого трафика: классификационные *признаки процедуры оценивания*
- Классификация процедур мониторинга сетевого трафика: классификационные *признаки процедуры прогнозирования*
- Заключение

Введение

Цель: определить границы и наметить теоретические предпосылки оптимизации и адаптации процедур мониторинга сетевого трафика.

Задача: определение классификационных признаков ключевой составляющей процесса контроля информационных потоков для обнаружения вредоносной информации и компьютерных атак – мониторинга сетевого трафика.

Релевантные исследования

- Подходы к построению комплексной системы компьютерной безопасности [Stuttard et al., 2014]
- Взгляд стран NATO на применение национальных стратегий снижения последствий кибератак [Geers, 2011]
- Анализ сущности современных кибероперациий, общие тенденции построения СЗКА, виды вредоносной информации и компьютерных атак [O'Leary, 2019, Schlienger&Teufel, 2003, Watts, 2011]
- Современные подходы к построению СЗКА и применению методов обнаружения атак в критически важных инфраструктурах IoT [Ruchi& Ankit Kumar, 2020]
- Машинное обучение и аналитика Больших Данных для обнаружения атак [Chio&Freeman, 2018]
- Методы обнаружения вторжений в ИТКС, основанные на онтологиях, прикладных методах статистического анализа [Eckmann et al., 2002, Salmon et al., 2017]

Существующие сложности

1. Методики обнаружения вредоносной информации и компьютерных атак не учитывают специфические свойства сетевого трафика сверхвысоких объемов и особенности параметров трафика [*Kumar Nainar et al., 2018, Uma&Padmavathi 2012*].
2. Подходы к мониторингу нацелены на измерение, классификацию и обнаружение явно выраженных аномалий сетевого трафика и рассчитаны на анализ в условиях априорных знаний о признаках данных аномалий [*Garcia-Dorado et al., 2013, Bhuvan et al., 2017*].
3. Учет при обнаружении вредоносной информации и компьютерных атак только произошедших инцидентов информационной безопасности не позволяет полноценно анализировать и прогнозировать возможные угрозы [*Bejtlich, 2013*].
4. Решение проблемы выбора средств и способов мониторинга трафика до недавнего времени базировалось на общих, не структурированных данных об особенностях реализации процедур наблюдения, оценивания и прогнозирования информационных потоков [*Collins, 2017, Daadoo, 2017*].

Процедуры мониторинга сетевого трафика

1. Наблюдение
2. Оценивание
3. Прогнозирование

Классификационные признаки процедуры наблюдения (1/2)

1. Режим наблюдения параметров сетевого трафика (*наблюдение без избыточности, с избыточностью и комбинированное*).
2. Этапы наблюдения (*выявление и сбор данных наблюдения, их накопление, регистрация и хранение, и обработка поступающей информации*).
3. Объекты наблюдения (*параметры трафика, влияющие на его аномалии извне, информация о собственных параметрах трафика, комплексное наблюдение*).
4. Ширина охвата параметров, наблюдаемых в интересах мониторинга сетевого трафика (*тотальное наблюдение и выборочное наблюдение*).

Классификационные признаки процедуры наблюдения (2/2)

5. Характер используемых данных измерений (*данные об абсолютных значениях параметров трафика, об их относительных значениях; данные, полученные путем прямых измерений, путем косвенных*).
6. Периодичность наблюдения (*непрерывно или в результате циклического последовательного опроса*).
7. Степень влияния процедуры наблюдения параметров сетевого трафика на процесс информационного обмена (*разрушающее наблюдение и неразрушающее наблюдение*).
8. Вид стимуляции в интересах добывания данных наблюдения (*рабочая (естественная) стимуляция, тестовая (искусственная) стимуляция*).

Классификационные признаки процедуры оценивания (1/2)

1. Объект оценивания (*параметры сетевого трафика и качество сетевого трафика на основе значений параметров*)
2. Критерии оценивания (*пригодность, оптимальность и превосходство*)
3. Вид оценочной шкалы (*количественная и качественная*)
4. Характер оценивания (*прямой и косвенный*)
5. Методы оценивания (*формальные, таксономические и индексные методы*)

Классификационные признаки процедуры оценивания (2/2)

6. Вид получаемых оценок параметров сетевого трафика (*интегральные и частные оценки параметров и показателей качества сетевого трафика*)
7. Временная зависимость оценивания (*методы статического и динамического оценивания параметров сетевого трафика*)
8. Вид априорной неопределенности данных наблюдения (*методы, дающие детерминированные оценки, вероятностные оценки, методы, основанные на получении неопределенных оценок*)

Классификационные признаки процедуры прогнозирования

1. Объект оценивания (*параметры сетевого трафика и показатели качества сетевого трафика*)
2. Интервал прогнозирования (*кратковременный, средневременный и долговременный*)
3. Метод прогнозирования (*аналитические и экспертные методы*)

Заключение

- Предложен вариант классификации режимов, методов и алгоритмов мониторинга сетевого трафика в интересах обнаружения вредоносной информации и компьютерных атак
- Он ориентирован на рассмотрение проблемы мониторинга сетевого трафика с точки зрения комплекса процедур наблюдения, оценивания и прогнозирования
- Выделенные признаки позволяют определить границы и наметить теоретические предпосылки оптимизации и адаптации процедур мониторинга сетевого трафика

Спасибо за внимание!

Работа выполнена при финансовой поддержке Гранта РНФ № 18-11-00302 в СПИИРАН

Контакты:

Дойникова Елена Владимировна (doynikova@comsec.spb.ru)
Котенко Игорь Витальевич (ivkote@comsec.spb.ru)
Паращук Игорь Борисович (shchuk@rambler.ru)