Труды XXIX научной конференции по радиофизике

СЕКЦИЯ
«ИНФОРМАЦИОННЫЕ СИСТЕМЫ. СРЕДСТВА, ТЕХНОЛОГИИ, БЕЗОПАСНОСТЬ»

Председатель – Л.Ю. Ротков, секретарь – А.А. Рябов.
Нижегородский государственный университет им. Н.И. Лобачевского.

ЭКСПЕРИМЕНТАЛЬНОЕ СРАВНЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ ДЛЯ РАЗНЫХ ОБЪЕМОВ ДАННЫХ

А.А. Белова, А.А. Горбунов

ННГУ им. Н.И. Лобачевского

В современных системах защиты информации для обеспечения безопасности передаваемых по линиям связи данных применяются различные криптографические алгоритмы, у каждого из которых есть свои преимущества и недостатки. В рамках данной работы сравниваются показатели производительности ряда криптосистем на основе экспериментального определения времени их работы при преобразовании данных различного объема. Рассматриваются симметричные криптосистемы (на примерах таких алгоритмов как AES, 3DES и ChaCha20), асимметричная криптосистема RSA, а также комбинации этих систем.

Гибридная (или комбинированная) криптосистема – это система шифрования, совмещающая при своем функционировании особенности асимметричных криптосистем со свойствами симметричных криптосистем. Существенным требованием для корректной работы классических симметричных систем шифрования является необходимость передачи секретного ключа по защищенному каналу связи. Реализация на практике данного условия зачастую может быть достаточно затруднена [1]. В то же время при комбинированном подходе криптосистема с открытым ключом применяется для шифрования, передачи и последующего дешифрования только секретного ключа симметричной криптосистемы. Симметричная криптосистема применяется для шифрования и передачи исходного открытого текста. В результате криптосистема с открытым ключом не заменяет симметричную криптосистему с секретным ключом, а дополняет ее, позволяя в целом повысить защищенность передаваемой информации [2].

При использовании гибридной криптосистемы отправитель создает случайный одноразовый ключ для алгоритма симметричного шифрования данных. Созданный ключ используется только для единственного сеанса симметричного шифрования файла с данными. Защищаемые данные шифруются симметричным алгоритмом с использованием одноразового сеансового ключа, сам же такой ключ зашифровывается при помощи асимметричного алгоритма с использованием открытого ключа получателя. Таким образом гарантируется, что только владелец соответствующего закрытого ключа сможет расшифровать ключ симметричного криптоалгоритма. Зашифрованные данные вместе с зашифрованным сеансовым ключом передаются получателю по открытому каналу связи. Получатель же в свою очередь использует закрытый ключ асимметричного алгоритма для расшифрования сеансового ключа, который применяется для дешифрования переданных зашифрованных данных [3].

В работе экспериментально оценивалась производительность различных криптографических систем, в том числе гибридных, как при шифровании, так и при дешифровании данных. В качестве экспериментального стенда использовался ПК с 64-разрядной ОС Windows и процессором Intel Core i5-11400H 2.70GHz. Программная реализация модулей шифрования и дешифрования была осуществлена на языке программирования C++ в среде разработки Visual Studio 2022 с использованием криптографической библиотеки OpenSSL. Под производительностью алгоритма шифрования (дешифрования) в настоящем контексте подразумевается время его работы по шифрованию

(дешифрованию) заданного объема обрабатываемых данных. Для каждого алгоритма и каждой величины объема данных производилось по 1000 замеров времени работы, на основе которых высчитывалось среднее медианное значение. Измерение времени шифрования и дешифрования осуществлялось для симметричных алгоритмов: 3DES, AES-256, ChaCha20-Poly1305, асимметричного алгоритма RSA-2048 и их комбинации.

Полученные результаты измерений показали, что, в частности, время шифрования алгоритмом RSA блока данных размером 64 байт (2^9 бит) составляет всего 0,06 мс, а дешифрования 0,89 мс. В то же время для гибридной схемы, например, AES+RSA аналогичный результат составляет 0,07 мс при шифровании и 0,93 мс при дешифровании данных. На основании полученных результатов можно говорить о допустимости использования только асимметричного алгоритма RSA без его объединения с симметричными алгоритмами для случаев, когда затруднительно использовать одноразовый ключ симметричного шифрования, а объемы передаваемых данных составляют единицы или десятки байт.

Вместе с тем время работы алгоритма RSA существенно возрастает с увеличением объема обрабатываемых данных, что делает использование только его нецелесообразным для обработки больших объемов данных. Например, для блока в 4 КБ (2^{15} бит) время шифрования RSA составляет 1,96 мс, а дешифрования – 29,12 мс. В таких случаях гибридные схемы демонстрируют свое преимущество: их время работы минимально увеличивается с ростом объема обрабатываемой информации. Тот же объем данных (4 КБ) в схеме AES+RSA обрабатывается за 0,08 мс при шифровании и за 0,99 мс при дешифровании, что соответственно в 24 и в 29 раз быстрее, чем при использовании одного лишь асимметричного алгоритма RSA.

Таким образом, исходя из результатов проведенного экспериментального сравнения производительности алгоритмов шифрования, можно сделать вывод о том, что при шифровании (дешифровании) достаточно больших объемов данных приемлемая производительность обеспечивается только при задействовании функционала симметричных криптоалгоритмов. При этом для объемов данных порядка 1 Кбита и более эффективнее использовать гибридные схемы (AES+RSA, ChaCha20+RSA). В ситуациях, когда объем данных составляет менее 1 Кбита, можно шифровать (дешифровать) их непосредственно с помощью асимметричного алгоритма, не комбинируя его с симметричными алгоритмами. В этом случае производительность криптосистемы не ухудшается при одновременном отсутствии затрат, связанных с реализацией комбинированной схемы шифрования.

[1] Владимиров С.М., Габидулин Э.М., Колыбельников А.И., Кшевецкий А.С. Криптографические методы защиты информации. – М.: МФТИ, 2020.
[2] Левина А.Б. Криптография и криптографические протоколы. Гибридное шифрование. – СПб.: СПбГЭТУ «ЛЭТИ», 2022.
[3] Хлебников А. OpenSSL 3. Ключ к тайнам криптографии / пер. с англ. А.А. Слинкина. – М.: ДМК Пресс, 2023.

ПОДХОДЫ К ИСПОЛЬЗОВАНИЮ МАШИННОГО ОБУЧЕНИЯ ДЛЯ НАЧАЛЬНОГО АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (SIEM)

Т.В. Грошкова, В.А. Мокляков

ННГУ им. Н.И. Лобачевского

Современные системы управления информационной безопасностью (SIEM) играют важную роль в мониторинге и предотвращении кибератак. К сожалению, их эффективность ограничена сложностью обработки больших объемов неструктурированных данных, поступающих от различных источников, таких как системные журналы серверов, сетевые устройства и приложения.

В работе проводилось сравнение традиционных подходов использования SIEM-систем и подходов с применением алгоритмов машинного обучения [1], которое отражено в таблице.

Таблица

Критерий	Стандартные методы	С применением Машинного обучения
Обработка текстовых данных	Ограниченный парсинг логов по шаблонам при помощи регулярных выражений (RegEx) Требуемое время: ~15мин.	Автоматическая классификация, извлечение сущностей, анализ тональности. Требуемое время: ~5мин
Корреляция событий	Жёсткие правила (if-then), статические сигнатуры, низкая гибкость Ложные срабатывания: 20-40%	Обнаружение сложных паттернов, аномалий, кластеризация Ложные срабатывания: 8-15%
Обнаружение аномалий	На основе известных шаблонов Точность: 60-75%	Выявление неизвестных угроз через анализ отклонений от нормального поведения Точность: 85-90%
Масштабируемость	Ограничена производительностью правил корреляции	Обработка больших объёмов данных в реальном времени
Автоматизация реагирования	Частичная (скрипты, триггеры)	Полная (блокировка IP, изоляция узлов, запуск сценариев реагирования)
Прогнозирование угроз	Отсутствует	Предсказание атак на основе исторических данных
Адаптивность	Требует ручного обновления правил Требуемое время: от часа до нескольких дней	Самообучение на новых данных, автоматическая оптимизация правил Требуемое время: ~ 30 мин.

Из таблицы видно, что традиционные методы, основанные на предопределенных шаблонах и правилах, не справляются с обработкой неструктурированных или нестандартных данных из-за своей негибкости, низкой точности и высокой трудоемкости настройки. Основная проблема таких подходов заключается в их неспособности адаптироваться к новым форматам данных, а в условиях постоянно меняющихся угроз и разнообразия источников, заранее заданные шаблоны часто оказываются неэффективными.

Комбинируя алгоритмы машинного обучения, можно получить достаточно эффективный подход для начальной обработки событий. А именно алгоритм обработки естественного языка (NLP) осуществляет сначала токенизацию, то есть процесс разбиения текста на отдельные элементы (токены), такие как слова, знаки препинания и другие символы, что позволяет перейти от неструктурированных данных к последовательности элементов, пригодных для дальнейшего анализа [2]. Для извлечения сущностей используется вероятностная модель, которая вычисляет вероятность принадлежности каждого токена к определенной категории сущности. Формула, лежащая в основе этого процесса, выглядит следующим образом:

$$P(y|x) = softmax(W * h(x) + b),$$

где x – входной текст, $h(x)$ – векторное представление текста, полученное с помощью нейронной сети, W и b – веса и смещение модели, y – предсказанная метка сущности.

Для применения методов машинного обучения текстовые данные необходимо преобразовать в числовые векторы. Для этого применяется метод Term Frequency-Inverse Document Frequency (TF-IDF), в котором TF измеряет частоту встречаемости термина в документе, IDF оценивает важность термина в корпусе документов [3].

Далее применяется кластеризация для группировки текстовых данных на основе их векторных представлений. Одним из популярных методов кластеризации является KMeans, который минимизирует суммарное квадратичное отклонение точек кластеров от центров этих кластеров:

$$\sum_{i=1}^{k} \sum_{x \epsilon S_i} (x - \mu_i)^2,$$

где S_i–кластер i, μ_i – центры масс векторов, k – число кластеров [4].

Данный подход позволяет осуществить начальный анализ данных в SIEM-системе, в противовес традиционным методам, исключая необходимость присутствия специалиста.

[1] https://www.anti-malware.ru/analytics/Technology_Analysis/Neural-Networks-and-Blockchain-in-SIEM
[2] Bird, S., Klein, E., & Loper, E. Natural Language Processing with Python. O'Reilly Media. 2009. P. 107.
[3] Manning C.D., Raghavan P. & Schütze H. Introduction to Information Retrieval. Cambridge University Press. 2008. P. 118
[4] Кугаевских А.В., Муромцев Д.И., Кирсанова О.В. Классические методы машинного обучения. – СПб: Университет ИТМО, 2022. С. 14.

СОСТЯЗАТЕЛЬНЫЕ АТАКИ НА СИСТЕМУ РАСПОЗНАВАНИЯ ЗНАКОВ ДОРОЖНОГО ДВИЖЕНИЯ

М.В. Капралова, С.П. Никитенкова

ННГУ им. Н.И. Лобачевского

Развитие автономных транспортных средств знаменует собой значительный технологический прогресс в автомобильной промышленности, причем искусственный интеллект (ИИ) играет центральную роль в этой трансформации. За последнее десятилетие ИИ был интегрирован в различные автомобильные системы, стимулируя инновации в таких областях, как принятие решений в реальном времени, планирование пути, обнаружение объектов и автоматизация транспортных средств. Быстрый прогресс нейронных сетей сыграл важную роль в продвижении задач обнаружения и классификации объектов, что имеет решающее значение для идентификации пешеходов, других транспортных средств и дорожных знаков. Однако использование нейронных сетей вносит новый тип уязвимостей в программное обеспечение беспилотных автомобилей.

Состязательное машинное обучение – это область, изучающая класс атак на нейронные сети, целью которых является ухудшение точности классификаторов, получение ошибочного прогноза с высокой степенью достоверности. Создавая преднамеренные слабые возмущения, получающие сильный отклик в выходных данных классификатора, злоумышленник может создавать вредоносные изображения или объекты, которые могут «обмануть» различные автомобильные системы [1].

Беспилотным автомобилям необходимо распознавание дорожных знаков для правильного анализа и понимания дорожного полотна. Правильное распознавание дорожных знаков жизненно важно для таких систем. В отличие от других методов атак, требующих внесения видимых изменений, например наклеек, блики выглядят естественно и ошибочно воспринимаются как не представляющие опасности [2].

Основной причиной проблем, созданных бликами, является локальное увеличение яркости одних областей на поверхности знака и затемнению остальных. Это приводит к искажению формы знака, размытию его границ и, как следствие, к затруднению распознавания. На рисунке 1 приведен пример атакованного изображения. Распознание дорожных знаков происходит на основе сверточной нейронной сети (CNN), обученной на основе датасета RTSD (Russian traffic sign images dataset) [3].

Рис. 1

Цель данной работы – проанализировать влияние световых бликов на точность распознавания дорожных знаков и предложить методы предобработки изображений дорожных знаков для уменьшения ошибок распознавания.

В работе предлагается метод, основанный на анализе и модификации азимутально-усредненного спектра мощности [4]. Для начала изображение дорожного знака преобразуется в оттенки серого, после чего с помощью преобразования Фурье вычисляется его двумерный спектр, который затем подвергается азимутальному усреднению. Азимутально-усредненный спектр представляет собой распределение частот в изображении и позволяет выявить частотные компоненты, наиболее подверженные влиянию бликов. На рисунке 2 представлены графики азимутально-усредненного спектра мощности обычного и атакованного дорожного знака.

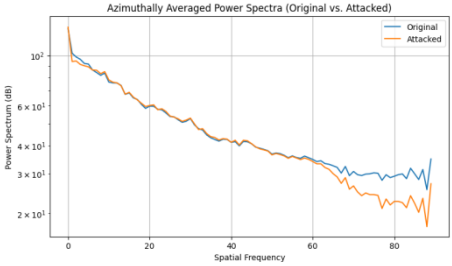

Рис. 2

Затем азимутально-усредненный спектр подвергается модификации. Сначала, происходит его обрезка, которая позволяет удалить высокочастотные компоненты и таким образом избавиться от искажений, вызванных бликами. Оставшаяся часть спектра аппроксимируется линейной функцией, а для частот, превышающих частоту обрезки, применяется экспоненциальный спад. Такой подход позволяет сохранить основные частотные характеристики изображения, в то же время подавляя шум и искажения.

В итоге на основе модифицированного азимутально-усредненного спектра восстанавливается изображение. Для этого применяется обратное преобразование Фурье, в котором используется информация о фазе исходного изображения, сохраненная до начала модификации [5]. В результате получается изображение, в котором подавлены высокочастотные компоненты, связанные с бликами, но при этом сохранена основная информация, необходимая для распознавания дорожного знака. На рисунке 3 представлены восстановленные на основе предложенного алгоритма обычное и атакованное изображения. Знак нейронной сетью и в том и другом случае определяется правильно.

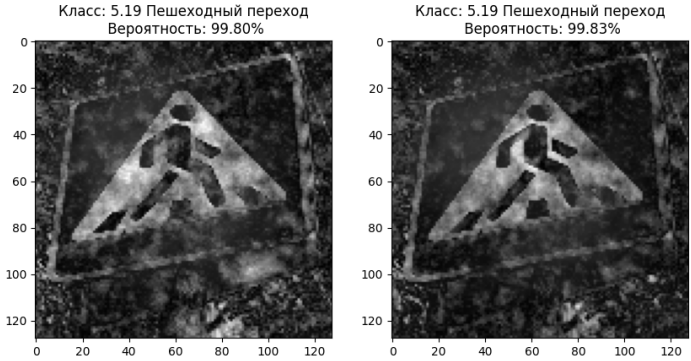

Рис. 3

Полученные результаты могут быть использованы для создания эффективных систем защиты от состязательных атак на знаки дорожного движения.

[1] Girdhar M., Hong J., Moore J. Cybersecurity of autonomous vehicles: A systematic literature review of adversarial attacks and defense models // IEEE Open Journal of Vehicular Technology. 2023. Vol. 4. P. 417.

[2] Hsiao T.-F., Huang B.-L., Ni Z.-X., Lin Y.-T., Shuai H.-H., Li Y.-H., Cheng W.-H. Natural Light Can Also be Dangerous: Traffic Sign Misinterpretation Under Adversarial Natural Light Attacks // Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV). 2023.

[3] Шахуро В.И., Конушин А.С. Российская база изображений автодорожных знаков // Компьютерная оптика. 2016. Т. 40, № 2. С. 294.

[4] Никитенкова С.П. Применение закона Бенфорда в обнаружении deepfake-изображений // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2023. № 64. С. 128.

[5] Alieva T., Calvo M.L. Image reconstruction from amplitude-only and phase-only data in the fractional Fourier domain // Optics and Spectroscopy. 2003. Vol. 95. P. 110.

ОЦЕНКА СКРЫТНОСТИ РАБОТЫ РЛС, СОПРЯЖЕННОЙ СО СРЕДСТВОМ ПАССИВНОЙ ЛОКАЦИИ БОРТОВЫХ ИЗЛУЧЕНИЙ ЛЕТАТЕЛЬНЫХ АППАРАТОВ, В УСЛОВИЯХ ПРИМЕНЕНИЯ ПРОТИВОРАДИОЛОКАЦИОННЫХ РАКЕТ

И.Н. Карельский, Л.Ю. Ротков

ННГУ им. Н.И. Лобачевского

Перспективным направлением повышения эффективности современных активных РЛС является их информационное сопряжение со средствами пассивной локации (СПЛ), позволяющими определять координаты летательных аппаратов (ЛА) по источникам бортовых радиоизлучений [1].

Современные СПЛ, например, «Vera» и др. [2] способны обнаруживать и определять координаты большинства радиоизлучающих объектов на максимальных расстояниях, ограниченных только дальностью прямой видимости: $\boldsymbol{d}_{\text{спл}\ \boldsymbol{max}} = \boldsymbol{d}_{\text{пв}} = 4{,}12(\boldsymbol{h}_{\text{а спл}}^{1/2}+\boldsymbol{h}_{\text{ЛА}}^{1/2})$, где: $\boldsymbol{h}_{\text{а спл}}$ – высота антенны СПЛ; $\boldsymbol{h}_{\text{ЛА}}$ – высота полета ЛА. Ошибки измерения координат в СПЛ соизмеримы с ошибками радиолокатора в общей для РЛС и СПЛ рабочей зоне. Это дает возможность применения СПЛ как дополнительного информационного источника, обеспечивающего скрытную работу РЛС, в том числе и в условиях применения противорадиолокационных ракет (ПРР), запускаемых по РЛС с самолета-носителя (СН).

Целью исследования является оценка повышения скрытности работы обзорной РЛС ЗРК средней дальности за счет снижения времени излучения и излучаемой мощности РЛС при реализации активно-пассивного сопровождения СН ПРР.

Если любой ЛА, приближающийся к РЛС ЗРК, считать потенциальным СН ПРР, то можно рассмотреть дуэльную ситуацию между СН ПРР и РЛС ЗРК, в которой, в случае успешности этапа наведения друг на друга ракет, выигрыш останется за тем средством, которое обеспечит огневое поражение противника на большей дальности: $d_{\text{ПРР}} \gtrless d_{\text{рлс цу}}$, где: $d_{\text{ПРР}}$ – дальность пуска ПРР по РЛС ЗРК; $d_{\text{рлс цу}}$ – дальность выдачи целеуказания (ЦУ) с РЛС, обеспечивающей пуск зенитной управляемой ракеты (ЗУР) и поражение СН в заданных границах зоны поражения (ЗП).

Пуск ПРР с СН обеспечивает система радиотехнической разведки (РТР) сигналов РЛС, состоящая из самолетной бортовой аппаратуры РТР (БА РТР) и аппаратуры самонаведения ПРР (АСН). БА РТР обнаруживает, анализирует и распознает сигналы РЛС, при необходимости уточняет координаты места их излучения, после чего отправляет ЦУ по выбранной РЛС на АСН. В АСН происходит обнаружение и захват сигнала РЛС с последующим сопровождением ИРИ по угловым координатам как до момента пуска ПРР, так и в процессе её наведения на РЛС.

Если в дуэльной ситуации основными средствами СН, обнаруживающими все необходимые параметры поражаемой РЛС, считать БА РТР и приемник АСН, то пуск ПРР возможен по главному или боковым лепесткам (ГЛ или БЛ) диаграммы направленности (ДН) РЛС с дальности: $d_{\text{ПРР}} = d_{\text{ртр}\ max\ \text{АСН ГЛ(БЛ)}} - v_{\text{СН}}\left(t_{\text{рс}} + t_{\text{ок}}\right)$, где $d_{\text{ртр БА ГЛ(БЛ)}}$ – энергетическая дальность захвата сигнала РЛС в приемнике АСН по ГЛ или БЛ; $v_{\text{СН}}$ –скорость полета СН; $t_{\text{рс}}$ – время реакции системы РТР СН с момента появления

сигнала РЛС требуемой мощности на входе БА и до его захвата в АСН на сопровождение по угловым координатам; $t_{ок}$ – время затрачиваемое БА РТР на определение координат (ОК) поражаемой РЛС.

В общем случае требуемая дальность целеуказания (ЦУ) $d_{\text{рлс цу}}$ зависит от энергетической дальности обнаружения СН радиолокатором ($d_{\text{рлс }max}$): $d_{\text{рлс цу}} \le d_{\text{рлс }max}$. С учетом информации поступающей от СПЛ требуемую дальность, обеспечивающую поражение СН на дальней границе зоны поражения ЗРК ($d_{\text{зрк д}}$), можно определить из выражения: $d_{\text{рлс цу д}} = d_{\text{зрк д}} + v_{\text{СН}}(t_{\text{рлс}} + t_{\text{раб}} + t_{\text{д}})$, где: $t_{\text{рлс}}$ – время уточнения координат СН, полученных в РЛС по данным СПЛ; $t_{\text{раб}}$ – время реакции ЗРК на полученное от РЛС ЦУ; $t_{\text{д}} = d_{\text{зрк д}}/v_{\text{ЗУР}}$ – время полета ЗУР со скоростью $v_{\text{ЗУР}}$ на дальнюю границу ЗП. В том случае, если обнаружение цели в РЛС происходит на меньшей дальности, то она должна быть не менее чем $d_{\text{рлс цу б}} \ge d_{\text{зрк б}} + v_{\text{СН}}(t_{\text{рлс}} + t_{\text{раб}} + t_{\text{б}})$, где $d_{\text{зрк б}}$ – ближняя граница ЗП. На рис. 1 схематично показаны возможные рубежи обнаружения объектов и пуска ПРР и ЗУР.

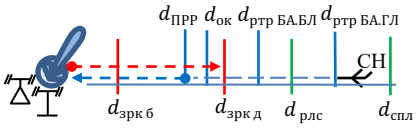

Рис. 1

При расчете максимальных (энергетических) дальностей обнаружения сигналов в РЛС и в бортовых средствах РТР учитывают вероятность правильного обнаружения сигнала на соответствующей дальности. Её можно определять по кривым обнаружения [3], задаваясь вероятностью ложной тревоги F, параметром обнаружения (коэффициентом различимости сигнала) q на уровне шумов радиоприемника, определяемых его пороговой чувствительностью ($P_{\text{пр мин}}$). Для заданной дальности d между источником сигнала и приемником эта вероятность определяется по формуле $D_{\text{обн}}(d) = Fexp[1/(1+q^2(d)]$. Если принять значение мощности сигнала на входе радиоприемника $P_{\text{вх}} = qP_{\text{пр мин}}$, то для установленной вероятности $D_{\text{обн}}$, можно определить максимальные дальности в соответствии с уравнением радиолокации (1) для активной РЛС и уравнением радиосвязи (2) для БА РТР и АСН ПРР [3, 4]:

$$d_{\text{рлс }max} = \left(\frac{P_{\text{рлс}}\, G_{\text{рлс}}^2 \lambda^2 S_{\text{эфф}}}{(4\pi)^3 q_1\, P_{\text{пр.мин 1}}}\right)^{\frac{1}{4}}, \qquad (1)$$

$$d_{\text{ртр }max} = \frac{\lambda}{(4\pi)}\left(\frac{P_{\text{рлс}} G_{\text{рлс}} G_{\text{ртр}}}{q_2 P_{\text{пр.мин 2}} K_f}\gamma\right)^{\frac{1}{2}}. \qquad (2)$$

В формулах 1, 2: $P_{\text{рлс}}$ – мощность передатчика РЛС; $G_{\text{рлс}}$, $G_{\text{ртр}}$ – коэффициенты усиления антенн РЛС и РТР, соответственно; $S_{\text{эфф}}$ – эффективная поверхность рассеяния СН; $P_{\text{пр.мин 1}}, P_{\text{пр.мин 2}}$, q_1, q_2 – чувствительности и коэффициенты различимости для РПУ РЛС и РПУ РТР, соответственно; $\gamma \approx 0{,}25$ – коэффициент, учитывающий потери сигнала в линии передачи и несовпадение поляризаций антенн РЛС и РТР; $K_f =$

$\Delta f_{\text{ртр}}/\Delta f_{\text{с}}$ – коэффициент, учитывающий несогласованность полосы пропускания РПУ РТР $\Delta f_{\text{ртр}}$ и ширины спектра сигнала РЛС $\Delta f_{\text{с}}$, равный единице, если $\Delta f_{\text{ртр}} \le \Delta f_{\text{с}}$.

На рис. 2 приведены зависимости $d_{\text{рлс}\,max}$ и $d_{\text{ртр}\,max}$ от излучаемой мощности передатчика РЛС. При этом принималось: 1) Для РЛС: максимальная дальность обнаружения СН ($d_{\text{рлс}\,max}$) с $S_{\text{эфф}} = 3$ м^2 при максимальной мощности передатчика $P_{\text{рлс}\,max}$≈12,5 КВт составляет 120 км; $G_{\text{рлс}} = 40$ дБ; $\lambda = 0{,}1$м; $P_{\text{пр.мин 1}} = -140$ дБ/Вт; $q_1 = 10$; уровень БЛ ДН РЛС: -30 дБ и -35 дБ. 2) Для средств РТР СН (типовых) [5]: дальность обнаружения РЛС по ГЛ $d_{\text{ртр max (ГЛ)}} = d_{\text{пв}}$; БА РТР: $G_{\text{БА}} = 10$ дБ; $q_2 = 10$; $P_{\text{пр.мин БА}} = -110$ дБ/Вт; $K_f = 10$; АСН: $G_{\text{АСН}} = 7$ дБ; $q_2 = 10$; $P_{\text{пр.мин АСН}} = -100$ дБ/Вт; $K_f = 10$.

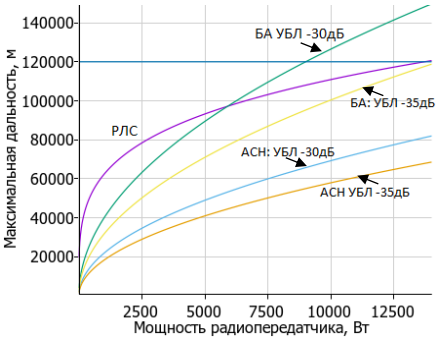

Рис. 2

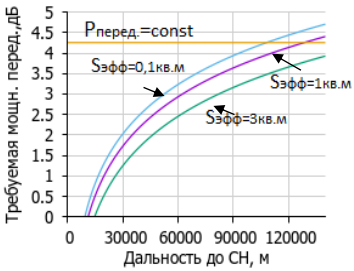

Рис. 3

Полученные результаты свидетельствуют о возможности снижения излучаемой мощности радиопередатчика в интересах повышения скрытности РЛС, до уровня, обеспечивающего своевременное ЦУ по данным СПЛ, если $d_{\text{рлс цу д}} < d_{\text{рлс}\,max}$. Регулировка требуемой мощности производится в соответствии с формулой:

$$P_{\text{рлс тр}}(d_{\text{спл}}) = (d_{\text{спл}})^4 (4\pi)^3 n_1 P_{\text{пр.мин 1}} / G_{\text{рлс}}^2 \lambda^2 S_{\text{эфф}} \qquad (3)$$

На рис. 3 показаны зависимости требуемой мощности от величин $d_{\text{спл}}$ и $S_{\text{эфф}}$ СН.

В целях повышения скрытности работы РЛС кроме регулировки мощности возможно полное выключение радиопередатчика на направлении СН и сопровождение СН только по данным СПЛ вплоть до дальности выдачи ЦУ ($d_{\text{рлс цу д}}$) с последующей работой передатчика в режиме мерцающего излучения (МРИ) [6].

В качестве показателя скрытности работы РЛС можно использовать отношение рубежей: $S = d_{\text{рлс цу}}/d_{\text{ППР}}$, равное единице при $d_{\text{рлс тр д}} \ge d_{\text{ППР}}$.

В таблице приведены результаты оценки показателя скрытности РЛС при ведении РТР с борта СН по ГЛ и БЛ ДН РЛС. Расчет рубежей $d_{\text{ППР}}$ и $d_{\text{рлс тр.}}$ производился для: СН с высотой полета $h_{\text{СН}}$ =5 км, $v_{\text{СН}}$=330 м/с; ППР AGM-88 HARM с $S_{\text{эфф}}$=0,07, средней скоростью полета 960 м/с и $d_{\text{ППР}\,max}$ =150 км. Время $t_{\text{рс}}$ при работе РЛС в режиме полного излучения составляет 15с, при МРИ 72с, Время $t_{\text{ок}}$=18с. Границы зон

поражения ЗРК для рассматриваемой высоты полета СН: $d_{\text{зрк б}}$=2,5 км и $d_{\text{зрк д}}$ =70 км, соответственно, Скорость полета ЗУР $v_{\text{зур}}$=1000 м/с. [7].

Табл.

ДН РЛС	Режим сопр. СН	$d_{\text{спл}}$, ($d_{\text{ртр АСН}}$)	$d_{\text{рлс цу}}$, км	$d_{\text{ПРР}}$, км	S
ГЛ	Без СПЛ	300	12	150	0,08
ГЛ	С СПЛ	300	97	с ОК 71	1
ГЛ	С СПЛ	300	97	без ОК 92,5	1
ГЛ	С СПЛ+МРИ	300	97	без ОК 75,4	1
БЛ: -30дБ	Без СПЛ	$d_{\text{ртр АСН}} = 212$	97	150	0,65
БЛ: -30дБ	С СПЛ	$d_{\text{ртр АСН}} = 212$	97	без ОК 80	1

Выводы:

1) В случае если $d_{\text{ПРР}} > d_{\text{рлс}\,max}$ (РЛС обнаружена с СН на дальности $d_{\text{пв}}$) и отсутствует информация о СН от СПЛ, то РЛС производит обнаружение целей в штатном режиме с максимальной мощностью $P_{\text{рлс}\,max}$. СН не входит в зону обнаружения РЛС, а обнаружение ПРР в РЛС и её поражение ЗРК возможно только на малых дальностях, поэтому скрытность работы РЛС невысокая, а её живучесть завит от результатов стрельбы ЗРК по ПРР.
2) При наличии информации о дальности и скорости СН, поступающей от СПЛ, выход РЛС на излучение и захват СН на сопровождение производится только с дальности $d_{\text{рлс цу}}$ и при соответствующей этой дальности $P_{\text{рлс тр}}(d_{\text{спл}})$. При этом скрытность работы РЛС высокая, обеспечивающая упреждающее поражение СН.
3) Применение активно-пассивного режима сопровождения СН с регулировкой мощности передатчика РЛС снижает вероятность скрытного запуска ПРР по БЛ ДН РЛС с другого носителя, так как для такого запуска СН вынужден войти в зону гарантированного обнаружения РЛС и зону поражения ЗРК.

[1] Васильев А.В., Колбаско И.В. Применение пассивных и активно-пассивных радиолокационных средств в зенитных ракетных войсках. Журнал "Военная мысль" 2023. № 6. kz@redstar.ru
[2] https://vestnik.sibsutis.ru/jour/article/view/528/511
[3] Радиотехнические системы: / Ю. П. Гришин, В.П. Ипатов, Ю.М. Казаринов и др.; Под ред. Ю.М. Казаринова. – М.: Высш. шк., 1990. 496 с.
[4] Смирнов Ю.А. Радиотехническая разведка. – М.: Воениздат, 2001. 456 с.
[5] Солонар А.С., Хмарский П.А., Мухаммедов Б.М. // Universum: технические науки: электрон. научн. журн. 2022. 10(103).
[6] Системы и средства радиоэлектронной борьбы: учеб, пособие / С. Н. Ермак и др. - Минск: БГУИР. 2019. 264 с.
[7] https://missilery.info/missile/bukm3

ВЫЯВЛЕНИЕ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА

Е.Н. Кривина, А.А. Рябов

ННГУ им. Н.И. Лобачевского

Проверка работы алгоритмов машинного обучения на синтезированных трафиках – популярная тема для исследований. Целью работы является исследование возможностей алгоритма Random Forest обнаруживать атаки в трафике реальной сети. Алгоритм Random Forest выбран, как показавший лучшие результаты при сравнении с другими алгоритмами [1].

По различным исследованиям, из трафика необходимо выделить 10-20 признаков (при небольшой вычислительной нагрузке), чтобы алгоритм показывал хорошие результаты обучения. В ряде экспериментов ключевыми признаками для классификации атак в наборе данных UNSW-NB15 часто являются: sbytes, dbytes, sttl, dttl, Sload, Dload, ct_srv_src, ct_state_ttl [2,3].

Для исследования работы модели из трафика реальной сети объемом 100000 пакетов составлен набор данных из 1959 потоков с 19 признаками. Для составления набора использовались встроенные функции библиотек языка Python.

Обучение и тестирование алгоритма проводилось на наборе данных UNSW-NB15, который включает в себя 2,5 млн. потоков. С помощью метода LabelEncoder значения признаков преобразованы в числовые значения. Пространство признаков в наборе данных UNSW-NB15 было сокращено с 49 до 19, соответствующих набору данных трафика реальной сети.

Набор поделен в соотношении 70/30, где большая часть шла на обучение алгоритма, а меньшая на его тестирование. Работа алгоритма оценивалась значением метрики «мера F1», являющейся средним гармоническим метрик precision и recall.

Идентификация аномалий в трафике происходила в два этапа. На первом этапе выделялись потоки с аномальными значениями, то есть алгоритм обнаруживал атаку. Второй этап заключался в определении категории атак. Обучение алгоритма проходило на каждом этапе. Значение «меры F1» составило 98,42% для первого этапа, и 88,28% для второго.

В задаче обнаружения атак в трафике реальной сети алгоритм классифицировал 20,16 % от общего числа потоков как аномальные. Обнаружено 3 категории атак, большую часть из которых составили Exploits (атаки, использующие известные уязвимости в программном обеспечении или протоколах).

Для анализа результатов работы алгоритма из набора, состоящего из аномальных потоков, необходимо восстановить трафик сети [4]. Восстановленный трафик содержал 71244 пакета. Проведен экспертный анализ трафика на предмет наличия атак. Экспертный анализ подтвердил наличие аномалии, схожей с DoS атакой.

Метод машинного обучения Random Forest продемонстрировал себя, как перспективный инструмент для выявления аномалий в сетевом трафике.

[1] Кривина Е.Н., Рябов А.А. // В кн.: Тр. XXVIII научн. конф. по радиофизике. – Н. Новгород: ННГУ, 2024. С. 520.
[2] Nour M. // Military Communications and Information Systems Conference (MilCIS). 2015. P. 1.
[3] Nour M., Jill S. // 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS). 2016. P. 25.
[4] Berger G.O., Lasgouttes J.M. // Springer. 2020. P. 286.

АУТЕНТИФИКАЦИЯ НА ОСНОВНЕ АНАЛИЗА РИСКОВ

А.С. Летавин, С.П. Никитенкова

ННГУ им. Н.И. Лобачевского

Несмотря на десятилетия усилий по замене паролей более безопасными альтернативами, они по-прежнему остаются основным методом аутентификации для большинства онлайн-сервисов. Таким образом, самая распространённая угроза безопасности любой информационной системы, это «взлом» пароля. Атаки с использованием подстановки учетных данных (credential stuffing) и распыления паролей (password spraying) автоматически вводят украденные учетные данные для входа (имя пользователя и пароль) в надежде, что пользователи повторно использовали их. Такие атаки можно масштабировать без особых усилий, поэтому они так популярны. Целевые методы подбора паролей (brute force) с использованием машинного обучения менее масштабируемы, но также эффективны. Двухфакторная аутентификация (2FA) является широко предлагаемой мерой для повышения безопасности учетной записи, но пользователи, как правило, отказываются от нее, если это не связано с доступом к конфиденциальным или финансовым данным. Двухфакторная аутентификация (2FA) повышает безопасность, но имеет и свои недостатки. Ключевые минусы включают необходимость в доверенном устройстве (часто телефоне), потенциальные задержки и проблемы с доступом при его потере, а также уязвимость некоторых методов 2FA, таких как SMS, к перехвату. Кроме того, 2FA может усложнять и замедлять процесс входа в систему.

Аутентификация на основе риска (Risk-Based Authentication) является решением, которое предпочтительнее 2FA во многих сценариях использования.

Захват учетной записи (взлом аккаунта) – это атака, при которой киберпреступник получает несанкционированный доступ к онлайн-аккаунту пользователя, используя украденные пароли и логины. Аутентификация на основе риска (RBA) оценивает, является ли вход в систему законным или является попыткой захвата учетной записи. RBA ликвидирует дополнительные шаги аутентификации для легитимных пользователей, позволяя им войти в онлайн-аккаунт без излишних проверок. Благодаря постоянному анализу различных показателей в режиме реального времени формируется динамическая оценка уровня риска. С высокой степенью уверенности она позволяет принять решение о предоставлении доступа к онлайн-аккаунту пользователя. Кроме того, RBA позволяет на раннем этапе обнаруживать подозрительную активность и потребовать от пользователя дополнительного подтверждения законности входа в учетную запись.

В работе разработан прототип системы аутентификации онлайн-сервиса на основе риска (RBA), использующей машинное обучение для динамической корректировки требований аутентификации. При обучении системы использовались данные аутентификации реальных пользователей на крупном онлайн-сервисе [1]. В исследуемый набор данных включены: время входа пользователя в онлайн-сервис, успешность авторизации, данные о типе устройства, операционной системе и браузере, идентификатор ASN; тип устройства (смартфон, компьютер и т.д.), геолокация (страна, город), Round Trip Time, время последнего входа пользователя в онлайн-сервис.

Риск S для отдельного пользователя u рассчитывался по формуле

$$S_u(FV) = \left(\prod_{k=1}^{d} \frac{p(FV_k)}{p(FV_k|u, legit)} \right) \frac{p(u|attack)}{p(u|legit)},$$

где FV_k (k=1..d) – перечисленный выше набор признаков,
$p(FV_k)$ – вероятность значения признака,
$p(FV_k|u,legit)$ – вероятность значения признака в истории входов в онлайн-аккаунт легитимного пользователя.

Вероятность $p(u|attack)$ оценивается на основе количества неудачных попыток входа пользователя [2]. Предполагается, что пользователи с большим количеством неудачных попыток входа, вероятно, подвергаются атакам с использованием учетных данных или паролей. Вычисленная по приведенной выше формуле «оценка риска» добавлялась в набор признаков. На основании «оценки риска» риск классифицируется как низкий, средний или высокий. При низком риске доступ пользователю предоставляется мгновенно. При среднем или высоком риске RBA может запросить дополнительную информацию для подтверждения заявленной личности или даже заблокировать доступ. Таким образом, запросы на дополнительную аутентификацию срабатывают только тогда, когда уровень риска оправдывает это, что обеспечивает баланс безопасности и удобства использования онлайн-сервиса.

Апробированы различные алгоритмы машинного обучения: метод опорных векторов, байесовская логистическая регрессия и альтернативное дерево решений. Метод опорных векторов продемонстрировал наибольшую точность обнаружения целевых попыток захвата аккаунта. Разработанный прототип системы аутентификации может использоваться в онлайн-сервисах, например, онлайн-торговых площадках.

[1] https://www.kaggle.com/datasets/dasgroup/rba-dataset
[2] Freeman D., Jain S., Dürmuth M., Biggio B., Giacinto G. Who Are You? A Statistical Approach to Measuring User Authenticity. 2016, In: NDSS ’16

СИСТЕМА МОНИТОРИНГА И АНАЛИЗА КИБЕРУГРОЗ НА ОСНОВЕ GRAYLOG: ПОДХОД К ОБНАРУЖЕНИЮ АТАК ПУТЁМ РАЗРАБОТКИ КРИТЕРИЕВ ВАЖНОСТИ СОБЫТИЙ ИБ

А.С. Морев, В.А. Мокляков

ННГУ им. Н.И.Лобачевского

В условиях роста сложности кибератак эффективное выявление инцидентов ИБ критически зависит от качества критериев важности событий в SIEM-системах. Существующие решения страдают от избыточного шума (ложных срабатываний) из-за общих правил детектирования.

Цель работы — разработка и экспериментальная проверка работоспособности критериев важности событий ИБ на базе open-source платформы Graylog.

Для проведения эксперимента построен стенд (рис.) на базе виртуальной инфраструктуры, включающей следующие компоненты:

1) Graylog Server – центральный сервер для сбора, обработки и анализа логов. Размещён на ОС Linux (ReDOS).
2) Сервер DVWA (Damn Vulnerable Web Application) – специальное приложение с множеством Web – уязвимостей, для отработки навыков и понимания механизмов реализации атак. Размещён на ОС Ubuntu.

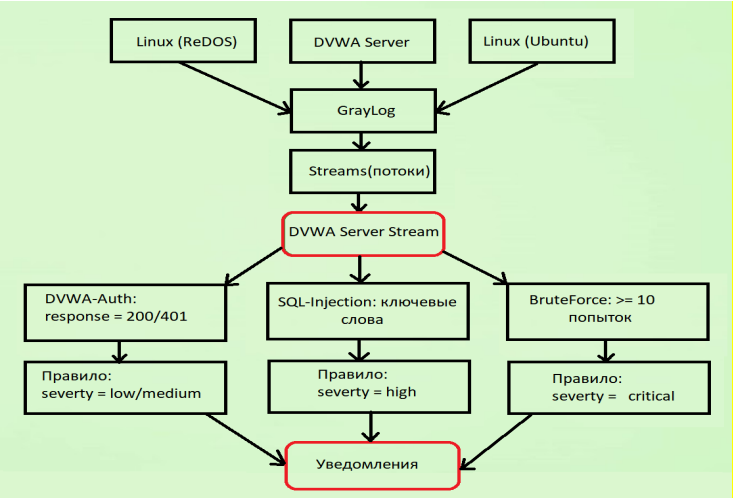

Рис.

Экспериментальный стенд позволяет исследовать следующие аспекты работы SIEM-систем:

- многоуровневый сбор данных;
- корреляция событий;
- моделирование атак и инцидентов;
- тестирование критериев важности и правил детектирования.

Критерий важности событий – это параметр, который определяет, насколько критично то или иное событие для безопасности системы. Определены 4 уровня важности (низкий, средний, высокий и критичный).

Разработаны критерии:

1) Критерий частоты – это количественная метрика, оценивающая как часто повторяется конкретное событие ИБ в заданный интервал времени. Основной критерий.
2) Источник событий (Source) – критерий характеризующий источник события (внутренний/внешний IP-адрес, использование анонимных сетей). Дополнительный критерий.
3) Контекст запроса – анализ контекста http-запросов предоставляет необходимую, но не достаточную для самостоятельной оценки информацию о потенциальных угрозах. В стандартных условиях критерий является дополнительным, но в жёстко регламентированных средах или при обнаружении явно враждебных запросов способен самостоятельной указать на критическую угрозу.
4) Уровень влияния на систему – критерий определён как основной, но его объективная оценка требует не только формальных признаков, но и профессиональной экспертной оценки.
5) Код ответа сервера – данный критерий был определён как дополнительный при оценке важности событий информационной безопасности, который приобретает диагностическую ценность только в сочетании с другими критериями важности.

Уровень важности события определяется степенью соответствия выявленного инцидента на основании значений 2-х основных и 3-х дополнительных критериев.

Экспериментальная проверка модели, реализованной на платформе Graylog, продемонстрировала практическую применимость предложенных решений.

[1] https://docs.graylog.org/
[2] https://github.com/digininja/DVWA/
[3] https://attack.mitre.org/
[4] https://redos.red-soft.ru/base/redos-7_3/7_3-administation/7_3-monitoring/7_3-graylog/
[5] https://www.ptsecurity.com/ru-ru/products/mpsiem/
[6] https://reestr.digital.gov.ru/
[7] https://docs.cntd.ru/document/1200057516
[8] https://www.junosnotes.com/linux/syslog-the-complete-system-administrator-guide/

ПРИМЕНЕНИЕ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ПРОТИВОДЕЙСТВИЯ СПУФИНГ АТАКАМ НА ОСНОВЕ МАСОК

А.А. Егорова, А.В. Никитин

ННГУ им. Н.И. Лобачевского

Технологии распознавания лиц получили повсеместное распространение в мобильных платежных системах, системах доступа и идентификации благодаря удобству и высокой точности. Однако современные системы уязвимы к спуфинг-атакам: 3D-маски, видео подмены, фото и видео с макияжем могут быть использованы для подмены идентификационных данных. Для минимизации рисков с получением несанкционированного доступа в биометрических системах используются методы Face Anti-Spoofing (FAS), предотвращающие спуфинг-атаки [1].

В работе предложен подход с применением сверточных нейронных сетей для противодействия спуфинг атакам на основе масок в системах биометрической аутентификации. На основе сверточной нейронной сети разработана модель бинарной классификации легитимности пользователя, дополненная алгоритмами Retinex и Local Binary Patterns (LBP) для верификации «живости» лица и определения атаки.

Входное изображение обрабатывается нейронной сетью, которая вычисляет вероятность принадлежности к одному из классов: легитимный пользователь (аутентичное изображение лица) или нелегитимный пользователь. Выходные данные сети нормированы в диапазоне от 0 до 1. При превышении порогового значения вероятности легитимности к исходному изображению применяются дополнительные методы проверки на спуфинг.

Для исследования использовались фотографии из набора данных LFW [2] и специально собранного для работы набора из 150 изображений лиц. С помощью методов аугментаций количество изображений было увеличено до 830 изображений. Нейросеть обучалась на черно-белых изображениях формата 128 на 128 пикселей. Точность обнаружения легитимного пользователя при пороге уверенности в 0,75 составила 99%.

Проверка «живости» лица на изображении осуществляется с помощью вариационного алгоритма Retinex, также известного как алгоритм имитации человеческого зрения, который выделяет из изображения яркостную компоненту (illumination) и отраженную (reflectance) [3]. Идея разделения на компоненты заключается в том, что разные материалы отражают свет по-разному и, если возможно выделить отраженную компоненту из изображения и сравнить ее с отраженной компонентой настоящего лица, можно обнаружить спуфинг атаку с применением масок. Выходные данные представляют собой одномерный массив, в котором находятся значения количества пикселей с яркостью от 0 до 255.

Аналогично алгоритму Retinex, для верификации «живости» применяется оператор LBP, описывающий текстуры изображения. Принцип работы оператора заключается в построении бинарной матрицы путем последовательного сравнения интенсивности каждого пикселя с его восемью соседями [4]. Получаемые матрицы содержат бинарные массив поскольку обработке подвергаются изображения в градациях серого, где каждый пиксель описывается единственным значением интенсивности.

При анализе изображения аутентичного человеческого лица бинарная матрица яркостей пикселей отличается от матриц, сформированных при анализе изображений с

лицами, закрытыми физическими масками или распечатанными снимками лиц. Это обусловлено различиями в текстурных особенностях кожи, материалов масок и печатных изображений. Обнаруженные аномалии в распределении значений яркостей служат индикатором спуфинг-атаки. Выходные данные алгоритма представляют собой одномерный массив, где каждый элемент соответствует частоте встречаемости определенного кода. Формирование этих кодов происходит путем преобразования 8-битных бинарных массивов, полученных при анализе локальных текстур, в соответствующие десятичные значения.

На рис. 1 представлено распределение значений яркости, полученное при обработке аутентичного лица методом Retinex. На рис. 2 изображено аналогичное распределение для случая спуфинг-атаки с физической маской.

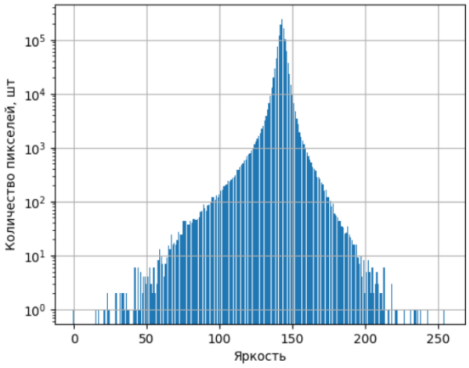

Рис. 1

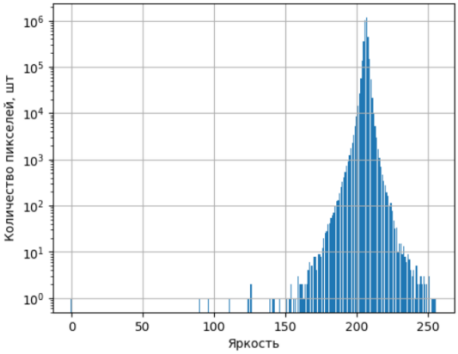

Рис. 2

Из приведенных рисунков видно, что для аутентичных лиц значения яркостей сосредоточены в диапазоне от 50 до 200. При использовании физических масок яркость смещена в область 180-250.

Далее для бинарной классификации изображений на наличие спуфинг-атаки используется метод опорных векторов (SVM), который принимает вектор признаков, полученный после обработки изображения алгоритмами Retinex и LBP.

Модель SVM обучена на данных CASIA-FASD [5], включающих в себя 3000 изображений спуфинг атак на основе масок и принт атак с использованием планшетов и плоских изображений. А также был создан собственных набор данных, включающий 120 изображений спуфинг атак на основе масок, расширенный с помощью аугментации до 960 изображений.

Для оценки модели использовались метрики Precision (точность), Recall (полнота) и F1-score (гармоническое среднее значение точности и полноты). Тестирование проводилось на выборке, включающей 13 изображений легитимных лиц и 12 образцов спуфинг-атак с использованием масок. Эти изображения не входили в обучающий набор нейронной сети. На тестовой выборке обученная модель достигла точности 80%, при этом было зафиксировано 3 ложноположительных случая - ошибочная классификация подлинных лиц как спуфинг-атак. Также была достигнута 100% полнота, корректно классифицированы все случаи спуфинг-атак без ложных пропусков. Значение F1-score составило 89%, что указывает на баланс между точностью и полнотой.

Применение сверточной нейронной сети позволило повысить точность детекции спуфинг-атак с использованием масок на 5% по сравнению с методами микротекстурного анализа [6] в системе верификации лиц.

[1] Yu Z. et al. // IEEE Transactions on Pattern Analysis & Machine Intelligence. 2023. Vol. 45, no. 05. P. 5609.
[2] https://www.kaggle.com/datasets/jessicali9530/lfw-dataset
[3] Wang X., Li D., Yang W. // 5th Computer and Computing Technologies in Agriculture (CCTA). 2011. P. 399.
[4] Ahonen T., Hadid A., Pietikainen M. // IEEE Trans. Pattern Analysis and Machine Intelligence. 2006. Vol. 28, no. 12. P. 5.
[5] Zhang Z. // Proceedings of 5th IAPR International Conference on Biometrics. // IEEE. 2012. P. 26.
[6] Kose N., Dugelay J.-L. Mask // Imageand Vision Computing. 2014. Vol. 32, no. 10. P. 779.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ КОМПЕНСИРУЮЩИХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ КИИ.

Р.Г. Нужный, Л.Ю. Ротков, В.А. Мокляков

ННГУ им. Н.И. Лобачевского

Согласно Указам Президента Российской Федерации, с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними, а также пользоваться сервисами (работами, услугами) по обеспечению информационной безопасности, предоставляемыми (выполняемыми, оказываемыми) этими организациями. Вместе с тем, запрещено к использованию иностранное программное обеспечение на значимых объектах критической информационной инфраструктуры, если иное не установлено федеральным законом.

Информационную инфраструктуру РФ, состоящую из объектов КИИ и сетей электросвязи, осуществляющих взаимодействие этих объектов, в целом можно представить, как большую распределенную сеть узлов с перетекающими между ними данными. Таким образом видно, что даже точечные успешные атаки (информационные воздействия) на узлы могут распространиться далеко за пределы атакованной части системы. И также видна необходимость в ранжировании по значимости отдельных частей/узлов системы для изолирования более значимых критических объектов от других в целях сохранения их работоспособности, когда другие окружающие его узлы сети уже атакованы злоумышленником. В этой связи, с повышением значимости возрастают требования к защите объекта в части применения организационных и технических мер, включающих необходимость внедрения средств защиты информации.

В связи с необходимостью использования отечественных сертифицированных программных продуктов и средств защиты, у владельцев информационных систем и сетей наметились пути постепенного ухода от иностранного ПО, и многие субъекты бизнеса, несмотря на значительные затраты и издержки, уже совершили значительный переход от ПО компании «Microsoft» и других корпораций на современные отечественные сертифицированные операционные системы и прикладное ПО, но в основном этот переход просматривается среди информационных систем, выполняющих стандартные задачи бизнеса, такие как финансовые, кадровые, производственные, бухгалтерские, расчетные операции, проектирование, разработка, моделирование, и прочее.

При этом на части производственных объектов машиностроения, атомной, химической, ядерной промышленности, медицинских и научных и других сфер, имеется ряд особенностей, не позволяющих применить отечественные программные средства в текущей конфигурации. Это связано в основном с отсутствием отечественных аналогов производственного оборудования, технических средств, программного обеспечения, обеспечивающего необходимое управление процессами на таком объекте. Случается, что для замены иностранного программного или программно-аппаратного модуля, интегрированного в крупный опасный производственный объект или иную конструкцию, требуется произвести сложные, в том числе строительные и монтажные работы, что

влечет за собой простой производственных процессов, потерю прибыли, штрафные санкции за невыполнение заказных государственных работ, репутационные и политические риски. Невозможность остановки производственного цикла некоторых производств также может быть вызвана рисками возникновения крупной аварии на опасном объекте, а также потерей или повреждением сырья, или выпускаемого продукта.

Искомый компромисс может состоять в том числе в поддержании существующей инфраструктуры, содержащей иностранные компоненты, но с применением компенсирующих мер защиты: наложенных средств защиты информации, физической защиты (охраны), защитных барьеров, средств экстренной ручной блокировки и останова процесса. Тогда владелец бизнеса может обойтись без остановки критически важного производства, что приоритетнее и дешевле, чем исключать риски полной остановкой цикла для замены оборудования и программного обеспечения, аналогов которого на отечественном рынке в данный момент нет, либо его невозможно приобрести за имеющиеся средства. Важно понимать, что использование иностранного программного обеспечения, равно как и отечественного, но не сертифицированного по требованиям информационной безопасности обязывает владельца информационных и неинформационных активов принимать все риски, связанные с утечкой конфиденциальной информации, ее уничтожением, подменой и модификацией, а также ущербы от последствий осуществления компьютерных атак на инфраструктуру субъекта, программные и программно-аппаратные средства. Вместе с тем, принимаются риски, связанные с наличием уязвимостей в устаревшем общесистемном и прикладном программном обеспечении, выпуск обновлений и поддержка которого уже не осуществляется производителем, либо приостановлена по причине санкционных запретов. Эти риски возникают так же из-за отсутствия возможности произвести замену на отечественный аналог или обновить программный продукт на версию, которая не содержит уязвимостей. Устаревшее ПО может не осуществлять в полной мере контроль доступа пользователей, шифрование, и другие защитные функции, однако даже при наличии возможности обновления, оно может спровоцировать каскадные сбои или отключения в других системах, которые довольно трудно предвидеть и предотвратить.

В случаях, когда требуется поддержание работоспособности системы, содержащей компоненты иностранного и/или уязвимого программного обеспечения, могут применяться следующие решения [1]:

- сегментация сети: позволяет отделить уязвимый объект логическим или физическим способом от других объектов при помощи коммутационного оборудования, требует непрерывного отслеживания нарушений доступа из открытой в изолированную сеть через разные сетевые интерфейсы;
- шифрование: позволяет при помощи современных алгоритмов шифрования и аутентификации создавать туннель между машинами, тогда как доступ вне туннеля заблокирован;
- микросегментация процессов: позволяет по возможности свести к минимуму процессы, обрабатываемые на уязвимой машине с учетом переноса большей части процессов на защищенные узлы;
- закрытый список приложений: позволяет на уязвимой машине разрешить к использованию только самые необходимые для работы программные средства, а остальные запретить;

- виртуализация: позволяет эксплуатировать уязвимое программное обеспечение поверх защищенной платформы с применением наложенных средств защиты, контроля доступа, а также песочниц и других решений внутри виртуальных машин;
- микросегментация сети: позволяет на прикладном уровне гибко конфигурировать потоки данных между приложениями в виртуальной среде;
- минимизация доступа и привилегий: позволяет при невозможности архитектуры ограничить доступ и привилегии, выполнить это административными мерами.

В случаях, когда требуется поддержание непрерывности производства на потенциально опасных объектах, и в целях снижения рисков от проведения атак и воздействий злоумышленников на конфиденциальную информацию, субъектами индивидуально могут применяться решения и компенсирующие меры в зависимости от сложности и опасности объекта, либо от степени конфиденциальности обрабатываемой и передаваемой по каналам связи информации. Некоторые из решений состоят в обеспечении своевременного противодействия угрозам за счет согласования времени получения информации от средств обнаружения, длительности задержки нарушителя физическими барьерами и времени выдвижения сил охраны к месту возникновения угрозы. Как правило, на критических объектах применяется комплексный системный подход: оценка безопасности объекта с учетом возможных рисков и прогнозируемого ущерба, разработка модели нарушителя и потенциальных угроз, тактико-экономическое обоснование, проектирование, поставка аппаратуры, строительство, монтаж, наладка, сдача комплекса под ключ [2]. В целом, защита с применением компенсирующих мер на потенциально опасных критических объектах сводится к:

- необходимости обеспечения физической защиты от вероятных внешних и внутренних угроз;
- зональному построению системы физической защиты, эшелонированию рубежей защиты, усилению защитных мер, как организационных, так и инженерно-технических, от периферии к центру;
- использованию специализированных средств для защиты информации, предаваемой по каналам связи, таких как средства однонаправленной передачи данных, средства шифрования, и других [3];
- использованию на особо опасных объектах средств физической или военизированной охраны, где невозможно полностью исключить влияние внутреннего или внешнего нарушителя;
- использованию систем автоматизированного сбора и обработки информации, поступающей от средств обнаружения, с возможностью подключения любого количества датчиков и осуществления необходимого количества процедур и тактик сдачи/приема под охрану;
- использованию средств защиты информации, в том числе программного комплекса для автоматического высокоточного обнаружения средств несанкционированного снятия информации.

Применение тех или иных защитных компенсирующих мер должно во всех случаях тщательно оцениваться в части влияния на систему или объект в целом.

[1] https://www.kaspersky.ru/blog/legacy-it-update-troubles-and-mitigations/35813/
[2] https://elib.biblioatom.ru/text/oruzhie-i-tehnologii-rossii_v14_2007/p588/
[3] Нужный Р.Г., Ротков Л.Ю., Мокляков В.А. // В кн.: Тр. XXVIII научной конференции по радиофизике (Нижний Новгород, 14—31 мая 2024 г.). – Нижний Новгород: ННГУ, 2024. С. 522.

РАЗРАБОТКА МЕТОДА СИНХРОНИЗАЦИИ ВРЕМЕНИ ПО РАДИОКАНАЛУ

О.В. Никитин, П.Е. Овчинников

ННГУ им. Н.И. Лобачевского

Описание задачи

При логическом объединении устройств в сеть часто возникает задача синхронизации часов, входящих в состав данных устройств. Если устройства подключены к локальной сети, то для решения задачи синхронизации часов используются сетевые протоколы синхронизации времени: NTP, PTP [1] и другие. Однако при непосредственном соединении двух устройств необходимо обеспечить только синхронизацию часов одного устройства относительно другого, для чего в этой работе разрабатывается упрощенный метод. С его помощью может осуществляться синхронизация часов, находящихся на значительном удалении друг от друга, в том числе на космических аппаратах. Схожая задача решается в системе TWSTFT [2], но предлагаемая в этой работе система обладает более простой структурой и опирается на технологии GPS.

Метод синхронизации

Метод синхронизации времени по радиоканалу основан на предположении о постоянстве времени передачи между синхронизируемыми устройствами. В худшем случае, за время проведения синхронизации задержки не должны измениться значительно, поскольку от этого зависит точность синхронизации. Метод предполагает двусторонний обмен радиосигналами, модулированными помехоустойчивым PRN-кодом по стандарту GPS C/A [3] и содержащими временные метки приёма и передачи.

На синхронизируемой станции формируется сигнал-запрос, содержащий метки времени для синхронизации, который затем отправляется по радиоканалу. На второй станции, где установлены эталонные часы, осуществляется приём сигнала и корреляционное демодуляция/декодирование с фиксацией времени прихода. Сразу же формируется сигнал-ответ, содержащий временные метки прихода сигнала-запроса и планируемого отправления сигнала-ответа. Он так же передаётся по радиоканалу и принимается синхронизируемой станцией, где фиксируется его время прихода. После успешного обмена сигналами на синхронизируемой станции оказывается четыре временные метки: время отправления и прихода сигнала-запроса (T_1 и T_2), время отправления и прибытия сигнала-ответа (T_3 и T_4). Зная эти четыре времени, можно вычислить задержку распространения (формула 1), полагая её одинаковой при передачах в обе стороны, и временной сдвиг между часами устройств (формула 2):

$$T_{roundtrip} = \frac{(T_3 - T_0) - (T_2 - T_1)}{2} \quad (1)$$

$$T_{offset} = \frac{(T_1 - T_0) + (T_2 - T_3)}{2}. \quad (2)$$

Для построения разрабатываемой системы синхронизируемые устройства должны обладать двусторонним радиоинтерфейсом для передачи и приёма радиосигналов, корелятором для демодуляции/декодирования и уточнения времени прихода меток и

вычислителем временных задержек по меткам времени (микроконтроллером). Все эти компоненты уже присутствуют на большинстве устройств, требующих синхронизации.

Проверка метода

Чтобы проверить работоспособность метода, был проведён полунатурный эксперимент по синхронизации часов на удалённых станциях, обменивающихся сигналами по радиочастотному каналу. Эксперимент состоял в построении двух станций (персональных компьютеров), снабжённых устройствами программно определяемого радио (*Software Defined Radio — SDR*). Для отсчёта времени использовались часы, включенные в состав SDR. Было разработано специальное программное обеспечение с применением библиотек GNU Radio [4], реализующее вышеописанный метод синхронизации, которое затем было установлено на обеих станциях.

На синхронизируемой станции сигнал-запрос формируется программным образом, затем передаётся на устройство SDR для отправки в эфир. На второй стороне (станция с эталонными часами) устройство SDR осуществляет приём сигнала и отмечает время его прихода, а корреляционное демодуляция/декодирование производится программно. Затем сигнал-ответ аналогично передаётся в обратную сторону. После успешного обмена метками времени на синхронизируемой станции производится вычисление временного сдвига между часами устройств, а также проводится оценка задержек распространения.

Работоспособность предложенной системы была подтверждена в результате проведённого эксперимента. Получаемая в экспериментальной системе точность синхронизации линейно связана с шириной спектра передаваемых сигналов, что соответствует теории [5].

[1] Edison J. Measurement, Control, and Communication Using IEEE 1588. – Springer, 2006. 284 с.
[2] Banerjee P., Matsakis D. An Introduction to Modern Timekeeping and Time Transfer. – Springer, 2023. 303 с.
[3] https://www.gps.gov/technical/icwg/IS-GPS-200K.pdf
[4] https://gnuradio.org
[5] Прокис Дж. Цифровая связь // Перевод с английского под ред. Д.Д. Кловского. – М.: Советское радио, 2000. 800 с.

РАЗРАБОТКА НЕЙРОСЕТЕВОГО МОДУЛЯ ДЛЯ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

А.А. Егорова, В.А. Павлушкин

ННГУ им. Н.И. Лобачевского

Традиционные СОВ основаны на правилах (предустановленных фильтрах) и демонстрируют различную эффективность в зависимости от реализации. Например, некоторые СОВ показывают более высокую точность при выявлении атак на уровне хоста [1]. Обычно система обнаружения вторжений состоит из трех ключевых подсистем: сбора данных, анализа и вывода. Подсистема сбора данных отвечает за захват сетевого трафика, в подсистеме анализа декодируются данные и выявляются аномалии или признаки атак, а подсистема вывода генерирует уведомления об обнаружении аномалий и рекомендации о действиях, которые следует предпринять для реагирования на угрозы.

Современные исследования [2] указывают на необходимость применения комбинированных методов анализа в подсистемах обнаружения угроз, что обусловлено усложнением кибератак. Однако для управления несколькими алгоритмами детектирования может быть необходима реализация модульной архитектуры с четким функциональным разделением [3].

В работе представлен нейросетевой модуль, разработанный для системы обнаружения вторжений. В качестве базового алгоритма модуля используется самоорганизующаяся нейронная сеть, принимающая на вход вектор признаков, сформированный модулем декодирования. Обучение нейросети проводилось на наборе данных NSL-KDD, созданном исследователями из Университета Мельбурна (Австралия) в 2009 году для оценки эффективности СОВ [4]. Набор данных NSL-KDD содержит репрезентативную выборку записей сетевого трафика, классифицированных по признакам аномальной активности, включая атаки типов DoS, Probe, U2R и R2L.

Обнаружение аномалий происходит с помощью кластеризации данных о сетевой активности, часто реализуемой самоорганизующимися картами Кохонена [5]. Однако, стандартные методы требуют задания количества кластеров и переобучения при изменении топологии сети. Чтобы избежать этих проблем, для построения детектора аномалий предусматривается использование адаптивных нейросетевых алгоритмов кластеризации.

Основная идея подхода заключается в использовании системы обнаружения аномалий на основе нейронной сети, обучаемой исключительно на нормальном сетевом трафике. В процессе обучения сеть выявляет типичные паттерны и характеристики сетевой активности. Результатом обучения является формирование кластеров - групп данных, представляющих различные виды нормального трафика, не содержащего аномалий. В данном подходе применяются алгоритмы самоорганизующихся нейронных сетей, такие как Growing neural gas (GNG) [6] и его инкрементальная модификация (Incremental growing neural gas, IGNG), которые позволяют динамически формировать и адаптировать топологию кластеров в пространстве признаков нормального трафика.

Для каждого нового массива данных система рассчитывает евклидовы расстояния до всех центров кластеров. Если расстояние до ближайшего кластера не превышает заданного порога, трафик классифицируется как нормальный. При превышении

порогового значения 7,5 условных единиц (установленного экспериментально для нормализованных данных) для всех кластеров, данные маркируются как аномальные.

Тестирование модулей на алгоритмах GNG и IGNG проводилось в двух конфигурациях: с учетом и без учета информации о хостах. Для оценки работы модулей использовались две метрики обнаружения аномалий: процент обнаружения аномалий и процент ложных срабатываний.

Получено, что для модуля GNG без хостовой информации процент обнаружения аномалий составил 78.4% при проценте ложных срабатываний 36.9%. Использование информации о хостах в GNG привело к снижению процента обнаружения до 72.5% и увеличению процента ложных срабатываний до 47.7%. Модули на основе алгоритма IGNG продемонстрировали значительно более низкую производительность: без хостовой информации – 26.8% обнаружения при 17.3% ложных срабатываний, а с хостовой информацией – 27.0% и 20.8% соответственно.

Таким образом, модули на основе алгоритма GNG обладают более высокой чувствительностью к аномалиям – точность обнаружения в 2.7-2.9 раза превышает аналогичный показатель для IGNG. Использование информации о хостах оказывает минимальное влияние на точность обнаружения аномалий в модулях с алгоритмом IGNG. Для GNG использование таких данных приводит к снижению точности и увеличению числа ложных срабатываний.

Для достижения наилучшего соотношения между точностью обнаружения угроз и минимизацией ложных срабатываний предпочтительным представляется выбор алгоритма GNG с последующей настройкой параметров модели, учитывающей специфику расширенного признакового пространства.

В рамках совершенствования модуля планируется оптимизация состава признаков в наборе данных для выявления наиболее информативных и исключения избыточных.

[1] Надейкина В.С., Маслова М.А. Анализ систем обнаружения и предотвращения вторжения с открытым кодом для интеграции с отечественными операционными системами // Научный результат. Информационные технологии. 2024. Т. 9, № 2. С. 41.
[2] Depren O., Topallar M., Anarim E. et al. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks // Expert systems with Applications. 2005. Vol. 29, no. 4. P. 713.
[3] Nguyen T.T. et al. Modular Design Principles for Modern IDS // Computers & Security. 2023. Vol. 124. P. 102964.
[4] https://github.com/Jehuty4949/NSL_KDD/tree/master
[5] Анисимова Э.С. Самоорганизующиеся карты Кохонена в задачах кластеризации // Актуальные проблемы гуманитарных и естественных наук. 2014. № 9. С. 2.
[6] Муравьев А.С., Белоусов А.А. Модифицированный алгоритм растущего нейронного газа применительно к задаче классификации // Вестник науки Сибири. 2014. № 4. С. 105.

АНАЛИЗ И СРАВНЕНИЕ СИГНАТУРНЫХ И ML-ИНТЕГРИРОВАННЫХ SIEM-СИСТЕМ

А.А. Егорова, И.Н. Шабалин

ННГУ им. Н.И. Лобачевского

В эпоху цифровой трансформации, когда киберугрозы становятся все более изощренными и сложными, вопрос эффективного мониторинга безопасности информационных систем выходит на первый план. Актуальность темы исследования обусловлена стремительным ростом количества и качества кибератак, которые ежегодно наносят многомиллиардный ущерб предприятиям по всему миру. Согласно последним исследованиям Cybersecurity Ventures, глобальные потери от киберпреступности к концу 2025 года могут достичь 10,5 триллионов долларов США [1], что делает проблему выбора оптимальных средств защиты критически важной для организаций любого масштаба.

Цель работы заключается в проведении сравнительного анализа двух принципиально разных подходов к обнаружению угроз информационной безопасности: традиционных SIEM-систем, основанных на детерминированных правилах, и современных решений, использующих методы искусственного интеллекта и машинного обучения [2]. В рамках исследования рассмотрена реализация SIEM-системы с ИИ-компонентами, проведено ее тестирование на различных типах угроз и выполнено сравнение с классическими подходами по ряду показателей.

Традиционные SIEM-системы, основанные на сигнатурах, обладают некоторыми ограничениями [3]:

- неспособность обнаруживать неизвестные угрозы (zero-day);
- сложность развёртывания системы;
- трудоемкость поддержки и обновления правил.

Решения с машинным обучением позволяют автоматизировать анализ данных, обнаруживать аномалии и адаптироваться к новым угрозам [4].

Реализованная система основана на микросервисной архитектуре. Сервисы взаимодействуют между собой синхронно. Система включает в себя следующие сервисы:

- Сервис сборки данных выполняет функцию сбора данных.
- Сервис обработки данных выполняет функцию преобразования неструктурированных данных в структурированный формат, включая очистку, извлечение признаков и обработку ошибок.
- Сервис машинного обучения выполняет функцию инициализации моделей для дальнейшего анализа событий. Для обнаружения аномалий в трафике применяется модель Isolation Forest, а для классификации угроз используется алгоритм Gradient Boosting.
- Сервис оповещений выполняет функцию создания оповещений о потенциально опасных событиях.
- Сервис аналитики выполняет функцию анализа трафика, вычисления метрик точности обнаружения, классификации аномалий и статистики наиболее опасных срабатываний за день.
- Сервис хранения данных выполняет функцию хранения полученных данных и результатов анализа.

- Веб-интерфейс выполняет функцию отображения данных, предоставления пользователю возможность взаимодействия с системой.

Для оценки систем использовались метрики:

- точность, описывающая соотношение правильно обнаруженных событий, к сумме обнаруженных с ложно-обнаруженными;
- мера F1, описывающая соотношение произведения точности и полноты, к их сумме.

Сравнение созданной системы проводилось с одной из самых популярных на рынке SIEM-систем ArcSight версии 2021.1.

Включение методов машинного обучения в SIEM позволило повысить точность обнаружения событий на 14% по сравнению с сигнатурным подходом (с 75% до 89%). Для категорий угроз Bruteforce и DDoS получены значения показателя F1-меры 0.94 и 0.89 соответственно, что на 22 и 4% выше, чем у ArcSight. Кроме того, SIEM с ML показало снижение количества ложных срабатываний на 35% в сравнении с ArcSight. Таким образом, проведенное тестирование продемонстрировало преимущество ML-интегрированной SIEM-системы перед традиционными решениями, реализованными в ArcSight.

Для тестирования выбраны два примера сложных угроз: эскалация привилегий (Event ID 4732 - повышение привилегий) и попытки подбора паролей (Event ID 4625 - неуспешная аутентификация). При обработке трафика с указанными типами атак, в веб-интерфейсе системы представлены следующие параметры: идентификатор, дата и время обработки пакета, дата и время создания пакета, идентификатор события, тип события, ip-адрес источника, категория события, тип атаки, точность обнаружения и комментарий. Для визуального выделения аномалий в SIEM используется цветовое кодирование: красный для критических угроз, розовый для опасных угроз. Система корректно идентифицировала выбранные угрозы и добавила в поле комментария соответствующие описания: «Privilege escalation: unknown added to privileged group by [IP]» и «Multiple failed logins for unknown from [IP]».

К преимуществам разработанной SIEM-системы с сервисом машинного обучения относятся: возможность обнаружения неизвестных угроз через анализ аномалий и поведенческих паттернов; снижение нагрузки на аналитиков безопасности вследствие уменьшения ложных срабатываний; масштабируемость архитектуры, обеспечиваемую микросервисным подходом.

Перспективные направления развития системы: переход от локального хранилища к распределенным решениям (таким как S3 и Elasticsearch) для обработки больших объемов данных через интеграцию с облачными сервисами; внедрение методов визуализации решений моделей (XAI-технологий) для упрощения анализа инцидентов; и автоматизацию реагирования на инциденты посредством блокировки подозрительных IP-адресов или изоляции скомпрометированных узлов через интеграцию с SOAR-платформами.

[1] Langlois P., Pinto A., Hylender D., Widup S. // Verizon. 2023. P. 89.

[2] Jacobs A.S., Ferreira R.A., Beltiukov R., Willinger W., Gupta A., Granville L.Z. // CCS '22: 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022. P. 15.
[3] Ullah K., Rashid I., Afzal H., Iqbal W., Bangash Y.A., Abbas H. // IEEE Communications Surveys & Tutorials. Vol. 10, no. 1109. P. 36.
[4] Sheeraz M., Paracha M.A., Ul Haque M., Durad M.H., Mohsin S.M., Shahab S., Mosavi A. Effective // Human-centric computing and Information Sciences. 2023. Vol. 13. P. 19.

ОБНАРУЖЕНИЕ СЕТЕВЫХ АНОМАЛИЙ В РЕАЛЬНОМ ТРАФИКЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДА МАШИННОГО ОБУЧЕНИЯ RANDOM FOREST

А.А. Софронов, А.А. Рябов, А.А. Горбунов, Л.Ю. Ротков

ННГУ им. Н.И. Лобачевского

В условиях растущих киберугроз и увеличения объемов сетевого трафика, задача обнаружения подозрительной активности становится критически важной для обеспечения информационной безопасности. Традиционные методы сигнатурного анализа часто оказываются недостаточными для выявления новых типов атак и аномалий. В этом контексте машинное обучение, и, в частности, алгоритм Random Forest, предоставляет мощный инструмент для создания интеллектуальных систем обнаружения вторжений.

В работе рассмотрена следующая реализация ансамблевого алгоритма Random Forest. Формирование модели делиться на 2 этапа обучение и тестирование. В процессе обучения алгоритма строится множества независимых деревьев решений. Каждое дерево выстраиваться на случайной выборке признаков датасета. Количество признаков определяет количество узлов, содержащихся в дереве решений. Распределение признаков по узлам происходит случайным образом. Для каждого из выбранных признаков подбираются все возможные варианты разбиения (например, разные пороги для числового признака). Для каждого варианта вычисляется качество разбиения по критерию Джини [1], после среди всех признаков и порогов выбираем те, которые дают наилучшие результаты предсказывания целевого результата и выстраивается уникальный путь, ведущий от вершины к листу дерева с итоговым предсказанием. После обучения каждого отдельного дерева выполняется их объединение в ансамбль «лес», где конечное решение принимается на основе большего количества одинаковых предсказаний на тот или иной класс потока. Такой подход позволяет получить итоговую модель, обладающую высокой точностью и устойчивостью к переобучению за счёт уменьшения влияния ошибок отдельных деревьев.

Для достижения наибольшей точности модели на реальных задачах требуется провести подбор гиперпараметров с помощью python функции GridSearchCV. Задача данного алгоритма подобрать такие параметры при котором значений ROC-кривой будет наивысшим. ROG-кривая (Receiver Operating Characteristic, ROC-curve) — это график, который показывает, как меняется соотношение истинно положительных и ложноположительных результатов для бинарного классификатора при разном пороге принятия решения. Высокий показатель кривой свидетельствует о том, что модель корректно разделяет классы и сводит к минимуму ложные срабатывания.

Для повышения производительности модели в реальных задачах необходимо сократить признаковое пространство. Для определения важности признаков использован алгоритм Random Forest с критерием Джини [1]. Степень корреляции признаков рассчитана по Пирсону. Произведя расчет корреляции Пирсона, удалось определить наиболее коррелирующие между собой пары признаков.

Разработанная модель Random Forest продемонстрировала высокую эффективность в задаче обнаружения сетевых вторжений на тестовом наборе данных UNSW-NB15 в котором количество признаков было сокращено с 49 до 32, показала точность предсказаний в 94.2%. При значениях precision (95.5%) и recall (93.9%) указывают на

сбалансированную производительность: высокая точность минимизирует ложные срабатывания, а уровень полноты обеспечивает обнаружение большинства реальных атак. F1-мера 94.7% подтверждает оптимальный баланс между метриками, а площадь под ROC-кривой 98.9% демонстрирует способность модели успешно различать виды потоков. Анализ матрицы ошибок показывает, что 7021 случая нормального трафика (94,6%) и 8495 случаев атак (93,9%) в эксперименте идентифицированы корректно, количество ложных классификаций низким — ошибочно отнесены к нормальному трафику 397 случаев (5,4%), а атак — 554 случая (6,1%).

Для эксперимента данные трафика реальной сети предварительно подготавливались специально разработанным обработчиком, использующим библиотеку «tshark» языка Python.

Применение модели Random Forest к реальному сетевому трафику показало, что система обладает способностью обнаруживать аномалии и потенциальные угрозы. На различных выборках установлено, что в выборке из 50 строк из 10 срабатываний: 3 реальные угрозы 7 ложные, при 250 строк из 20 срабатываний: 8 реальные угрозы 12 ложные, при 500 строк из 65 срабатываний: 15 реальные угрозы 40 ложные. Эти результаты свидетельствуют о способности системы обнаруживать вредоносную активность; однако высокий процент ложных срабатываний указывает на необходимость ручной проверки обнаруженных инцидентов. Уменьшение ложных срабатываний может быть достигнуто обучением модели на трафике исследуемой сети.

[1] Breiman L. Random forests // Machine Learning. 2001. Vol. 45, no. 1. P. 5. DOI: 10.1023/A:1010933404324.
[2] https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/
[3] https://statistics.laerd.com/spss-tutorials/pearson-correlation-using-spss-statistics.php

АНАЛИЗ ЗАЩИЩЕННОСТИ WEB-ПРИЛОЖЕНИЙ С ПРИМЕНЕНИЕМ GRAPHQL API

Р.А. Васильев

ННГУ им. Н.И. Лобачевского

Общие положения

Технология GraphQL, являясь относительно новым подходом к построению API, активно набирает популярность среди разработчиков web-приложений. Данный подход был предложен компанией Facebook в качестве альтернативы архитектурным принципам REST, направленной на решение проблем, связанных с этим подходом [1].

Ключевой особенностью GraphQL является перенос формирования структуры запроса к API на сторону клиента, то есть клиент сам определяет какие конкретно данные в ответе должен возвращать сервер. Это предоставляет исключительную гибкость и декларативность при формировании запросов, в отличии от строго определенного на сервере REST API, а также решает проблемы избыточности данных в ответе сервера (over-fetching), или недостатка данных при обращении к связанным ресурсам (under-fetching). В том числе GraphQL API имеет единственную конечную точку для запросов, что обеспечивает более легкую поддержку и расширение функционала сервера, а также является более удобным способом взаимодействия с клиентом, которому нужно иметь только один адрес для доступа ко всем ресурсам. Еще одной отличительной чертой GraphQL является возможность совершать несколько операций над данными в рамках одного HTTP запроса, в свою очередь в REST API для совершения каждой операции нужно отправлять отдельный, соответствующий ей запрос. Именно благодаря этим преимуществам современные компании либо создают и развивают параллельно с имеющимся REST API дополнительный ресурс, использующий GraphQL, либо полностью переходят на новую технологию в своих проектах [2-4].

Описанные особенности технологии реализуются посредством основных архитектурных компонентов: схемы, запросов, мутаций и подписок.

Схема является основой для GraphQL API, она определяет структуру данных, типы и возможные операции, которые клиент может выполнять, тем самым обеспечивая согласованность в передаче и обработке данных между клиентом и сервером. Схема определяется на стороне сервера, а клиент получает данные о схеме с помощью функции интроспекции. Интроспекция позволяет получить всю метаинформацию и информацию о возможностях API, эта функция используется в процессе разработки для автоматической генерации запросов и документации, при предоставлении общего доступа к программному продукту данную функцию рекомендуется отключать [5].

Запросы, мутации и подписки представляют из себя операции для работы с данными. Запросы используются для извлечения данных с сервера, в них указываются параметры, требующиеся сущности, их конкретные поля, а также связи с другими сущностями, если требуется извлечь сложную структуру данных с вложенными значениями. Мутации используются для операций, изменяющих состояние данных на сервере: добавление, удаление и изменение, в своем ответе они возвращают указанные клиентом поля измененных сущностей [6].

Подписки в GraphQL используются клиентом для получения уведомлений о измененных данных на сервере, таким образом реализуется передача данных в реальном времени без периодических дополнительных запросов, что отвечает требованиям современных web-приложений [7].

Теоретический анализ

Исходя из описания основных принципов GraphQL, можно сделать вывод, что взаимодействие клиента и сервера более гибкое, чем в REST-подходе. Эта гибкость достигается за счет делегирования некоторых функций сервера клиенту, что с одной стороны дает преимущество для эффективного взаимодействия, но с другой стороны подвергает систему опасности за счет расширенных полномочий на клиенте.

Вместе с эволюцией принципов построения API, развитие получили и способы атак на информационные системы. На первый взгляд, список возможных атак на GraphQL достаточно стандартный для любых web-сервисов: инъекционные атаки, эксплуатация уязвимостей в механизмах авторизации и DoS-атаки, но при подробном рассмотрении становится понятно, что злоумышленники успешно эксплуатируют особенности новой технологии. Особое внимание стоит уделить именно DoS-атакам, так как механизмы их проведения полностью задействуют специфические свойства системы.

Классическая DoS-атака на web-приложение представляет из себя загрузку ресурсов сервера путем отправки множества запросов, с целью вывести систему из строя. Подобный тип атак легко обнаруживается с помощью разных систем информационной безопасности (WAF, RASP, SIEM и др.), но не в случае использования GraphQL. Как было отмечено ранее, GraphQL позволяет упаковывать несколько операций в один HTTP-запрос, что делает атаку практически незаметной для стандартных систем информационной безопасности. На данной уязвимости основывается атака «Query Butching» представляющая из себя набор из одинаковых запросов, выполняющихся в рамках одной операции. Еще один способ вывести сервер из строя, эксплуатируя особенности GraphQl – это использование вложенных запросов. Возможность получения в одном запросе связанных сущностей в виде вложенной структуры позволяет злоумышленникам писать запросы, где сущности будут ссылаться друг на друга рекурсивно. Такие запросы создают ресурсоемкие операции на стороне сервера, что может привести к его перегрузке и снижению доступности системы [8,9].

Экспериментальные исследования

Для тестирования на уязвимость выбрана собственная разрабатываемая система по управлению электронным обучением [10]. Серверная часть состоит из базы данных MySQl и Node.js приложения, использующего GraphQL для связи с клиентом. В каждой таблице базы данных присутствует от 1 до 3 записей для тестирования. Данное GraphQL API будет тестироваться на предмет уязвимости DoS атакам типа «Query butching» и глубинных запросов, по алгоритму, представленному на рисунке.

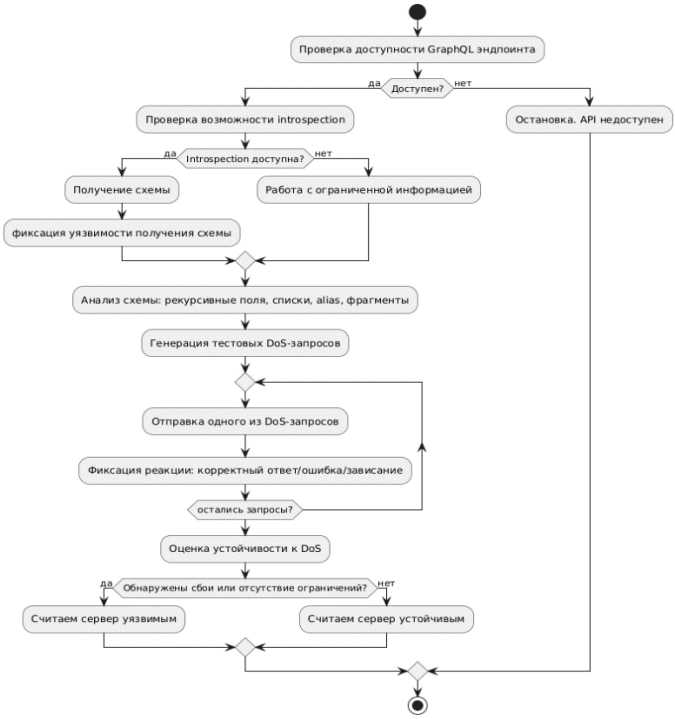

Рис.

Выводы

В ходе эксперимента имитированы DoS-атаки двух типов, характерных для GraphQl с различными размерами запросов.

Для проведения «Query butching» атаки было создано 4 запроса с разным количеством операций: 1 операция (стандартный сценарий использования), 20 операций, 50 операций и 100 операций. Тестирование показало увеличение времени ответа в зависимости от количества операций, минимальное значение-10 миллисекунд, максимальное-131 миллисекунда, что говорит о возрастающей нагрузке на сервер и отсутствии ограничений на выполнение одинаковых операций.

Для атаки с вложенными полями было создано 3 запроса с разными уровнями вложенностями: 1 уровень (стандартный сценарий использования), 20 уровней и 40 уровней. Время выполнения запросов возрастало от 6-10 миллисекунд до 64-281 миллисекунды, а при последовательной отправке 5 запросов с уровнем вложенности 40, система перестала отвечать, в связи с переполнением сетевого стека, то есть успешно был вызван отказ в обслуживании.

[1] Игнатьев А.Ю. Обзор технологии GraphQL // Молодой ученый. 2019. № 15. С. 22.

[2] Diyasa G.S.M. et al. Comparative analysis of rest and graphql technology on nodejs-based api development // Nusantara Science and Technology Proceedings. 2021. P. 43.
[3] Brito G., Valente M.T. REST vs GraphQL: A controlled experiment // 2020 IEEE international conference on software architecture (ICSA). IEEE. 2020. P. 81.
[4] Ковалев В. В., Храмков В. В., Семенова Е. И. Актуальность использования архитектуры REST для обмена данными между клиент-серверными приложениями // Актуальные проблемы авиации и космонавтики. 2019. Т. 2. С. 339.
[5] Quina-Mera A. et al. GraphQL: A systematic mapping study // ACM Computing Surveys. 2023. Vol. 55, no. 10. P. 1.
[6] Li H. et al. Ontology-based GraphQL server generation for data access and data integration //Semantic Web. 2024. no. 1. P. 1.
[7] Hartig O., Perez J. Semantics and complexity of GraphQL // Proceedings of the 2018 World Wide Web Conference. 2018. P. 1155.
[8] https://cheatsheetseries.owasp.org/cheatsheets/GraphQL_Cheat_Sheet.html
[9] McFadden S. et al. Wendigo: Deep Reinforcement Learning for Denial-of-Service Query Discovery in GraphQL // IEEE Workshop on Deep Learning Security and Privacy (DLSP). 2024.
[10] https://github.com/kospud/grecords-academy

Секция «Информационные системы.
Средства, технологии, безопасность»

Заседание секции проводилось 20 мая 2025 г.
Председатель – Л.Ю. Ротков, секретарь – А.А. Рябов.
Нижегородский государственный университет им. Н.И. Лобачевского.