алгоритмическая математика и математическое моделирование

Компьютерные инструменты в образовании, 2023
№ 3: 8–17
УДК: 004.056.5
http://cte.eltech.ru
doi:10.32603/2071-2340-2023-3-8-17

ОБНАРУЖЕНИЕ АТАК В КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУРАХ НА ОСНОВЕ АНАЛИЗА СОСТОЯНИЙ

Десницкий В. А.[1], канд. техн. наук, доцент, ✉ desnitsky@comsec.spb.ru,
orcid.org/0000-0002-3748-5414

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН), 14-я линия В.О., д. 39, 199178, Санкт-Петербург, Россия

Аннотация

В работе предложен подход к обнаружению атак в критически важных инфраструктурах с применением методов моделирования с использованием графов. Данный подход включает два основных этапа. В режиме проектирования производится интеллектуальный анализ логов, включающих исходные данные о функционировании индустриальной системы для построения графа ее состояний и переходов. Далее на этапе функционирования проводится обход графа с последовательным выявлением состояний, описывающих атаки определенных классов, осуществляющиеся на устройства системы. Помимо этого, в процессе выполнения функций системы производится обнаружение аномальных переходов между нормальными состояниями системы, что также может являться признаком некоторых видов атак на инфраструктуру. Эксперименты, проведенные на имеющихся в наличии наборах данных, описывающих функционирование двух критически важных индустриальных систем, подтвердили корректность разработанного алгоритма обнаружения атак, а также показали высокую устойчивость алгоритма к возможным потерям событий, поступающих на вход механизма обнаружения атак.

Ключевые слова: *информационная безопасность, атака, обнаружение атак, критически важная инфраструктура, граф, моделирование.*

Цитирование: Десницкий В. А. Обнаружение атак в критически важных инфраструктурах на основе анализа состояний // Компьютерные инструменты в образовании. 2023. № 3. С. 8-17. doi: 10.32603/2071-2340-2023-3-8-17

1. ВВЕДЕНИЕ

Ввиду критически важного характера современных киберфизических систем и сетей интернета вещей, таких как различные энергетические системы, системы управления водоснабжением и системы водоочистки, транспортные, логистические системы и др., научно-техническая задача обнаружения атак в них является чрезвычайно актуальной. Успешное выполнение несанкционированных воздействий как со стороны внешнего атакующего, так и внутреннего нарушителя информационной безопасности способны привести к серьезным нарушениям в функционировании таких систем, значительному

материальному ущербу, а в ряде случаев даже к катастрофическим последствиям техногенного и социального характера. В результате возникает необходимость решения задач по разработке механизмов своевременного обнаружения атак на такие системы, в том числе за счет конструирования новых, а также автоматизации и интеллектуализации существующих средств мониторинга информационной безопасности.

В данной статье предлагается подход к обнаружению атак в критически важных инфраструктурах на основе моделирования состояний киберфизической системы. Подход основан на использовании методов анализа данных и моделирования с использованием графов.

В проводимом исследовании за основу взяты два существующих, опубликованных в открытом доступе набора данных, описывающих работу индустриальных киберфизических систем, как в режиме нормального функционирования, так и под несколькими разно-видностями атак. Исходя из содержимого наборов данных, в автоматизированном режиме для каждого из них на этапе проектирования и настройки конструируется граф состояний и переходов, где каждое из состояний может быть признано либо нормальным, либо ата-кующим. На этапе выполнения, по мере поступления фактических событий от устройств системы с использованием построенного графа, производится процедура обхода этого графа. Достижение атакующего состояния сигнализирует о нахождении системы под атакой определенного вида. Формируемый инцидент позволяет выдавать также дополнительную информацию об устройстве-источнике атаки, времени ее выполнения и каких-либо других более специфических характеристиках конкретной атаки.

Помимо этого, попадание системы в некоторое состояние, в том числе атакующее в условиях отсутствия соответствующей дуги на графе, свидетельствует о неразрешенном переходе, о чем администратор системы также должен быть уведомлен. Выполнение нераз-решенного перехода, то есть перехода, для которого отсутствует дуга в графе состояний и переходов, в общем случае не обуславливает обязательно факта наличия какой-либо атаки, но такой переход является аномальным. Вместе с тем наличие аномалии может свидетельствовать как о начале какой-либо известной атаки, так и о возникновении атаки нового вида. К элементам новизны полученных результатов можно отнести сформированный набор правил, определяющих процесс обхода графа состояний и переходов с учетом используемых агрегированных состояний системы, в том числе состояний, описывающих систему, находящуюся одновременно под несколькими видами атакующих воздействий, а также разрешенных и неразрешенных переходов между состояниями системы.

2. АНАЛИЗ РАБОТ В ПРЕДМЕТНОЙ ОБЛАСТИ ИССЛЕДОВАНИЯ

В настоящее время в процессе обеспечения информационной безопасности все более существенное значение приобретают различные комплексные многошаговые атакующие воздействия, направленные на компрометацию критически важных инфраструктур, отдельных устройств в них входящих и предоставляемых ими информационных сервисов [1, 2].

Сложность эффективного выявления атак связана с разнородностью событий и видов воздействий, вовлеченных в атаку на разных ее этапах. В частности, неполнота собираемых данных, возникающая как вследствие динамизма устройств и изменчивости системы с течением времени, так и из-за возможных потерь в процессе сбора данных, может

приводить к тому, что пропуск нескольких или даже одного ключевого события не позволит однозначно сделать вывод о факте наличия атаки. Кроме того, вариации одной и той же атаки могут сделать процесс выявления цепочек событий на основе сигнатур менее эффективным и даже неработоспособным.

Поэтому одним из перспективных подходов к обнаружению атак в критически важных инфраструктурах представляется подход, основанный на анализе возможных состояний системы и переходов между ними [1]. При этом в процессе обнаружения пропуск одного или даже нескольких фактических нормальных состояний системы не должен препятствовать идентификации аномального или атакующего состояния, в которое система перешла [2].

В опубликованных к настоящему моменту времени научно-технических работах выделяют ряд отличающихся по своей сути методов и подходов к моделированию атак на критически важные инфраструктуры. В частности, в [3] представлен набор моделей прогнозирования и предупреждения атак, включающих, во-первых, дискретные модели, такие как графы и деревья атак [4–6], байесовские и марковские сети [7, 8], во-вторых, непрерывные модели, такие как временные ряды [9], в-третьих, методы интеллектуального анализа данных [10–12] и, в-четвертых, модели подобия [13] и эволюционные модели [14]. В отличие от опубликованных работ в настоящей статье предлагается комплексный подход к обнаружению атакующих воздействий в критически важных инфраструктурах, в значительной степени ориентированный на автоматизированное извлечение состояний системы из логов и их использование непосредственно в целях обнаружения атак. Кроме того, описанный в настоящей статье подход предполагает дальнейшие возможности по более раннему выявлению атак путем прогнозирования будущих шагов атаки, основываясь на предыдущем опыте и применении методов интеллектуального анализа данных. При этом последующее уточнение фактически достигнутого состояния на основе графовой модели позволит уточнить полученный ранее прогноз и сформировать прогноз на последующие состояния системы.

Для формирования подхода к обнаружению атак и проведения экспериментов в работе рассматривается наборы данных для обнаружения атак в системах, функционирующих в нескольких индустриальных областях, включающих энергетическую систему гидроаккумулирующей электростанции и инфраструктуру энергетической системы железнодорожного транспорта. Анализируемые наборы включают данные с определенным видом атак, без атак и смешанные данные. Предложенный механизм обнаружения атак был опробован на двух опубликованных наборах данных — Electra [15] и HAI [16]. Эти наборы опубликованы менее 5-и лет назад и обладают большим объемом данных, размеченных по типам атак и отличающихся количеством собираемых данных — основы для формирования признаков обнаружения атак.

3. ПОДХОД К ОБНАРУЖЕНИЮ АТАК

Предлагаемый подход к обнаружению атак основан на использовании алгоритма обхода графа состояний и переходов, характеризующего возможные состояния анализируемой системы и допустимые переходы между его состояниями. На рис. 1 схематично изображен лежащий в основе обнаружения атак алгоритм, включающий следующие основные шаги:

Шаг 1: загрузка графа состояний и переходов системы и определение начального состояния используемого графа.

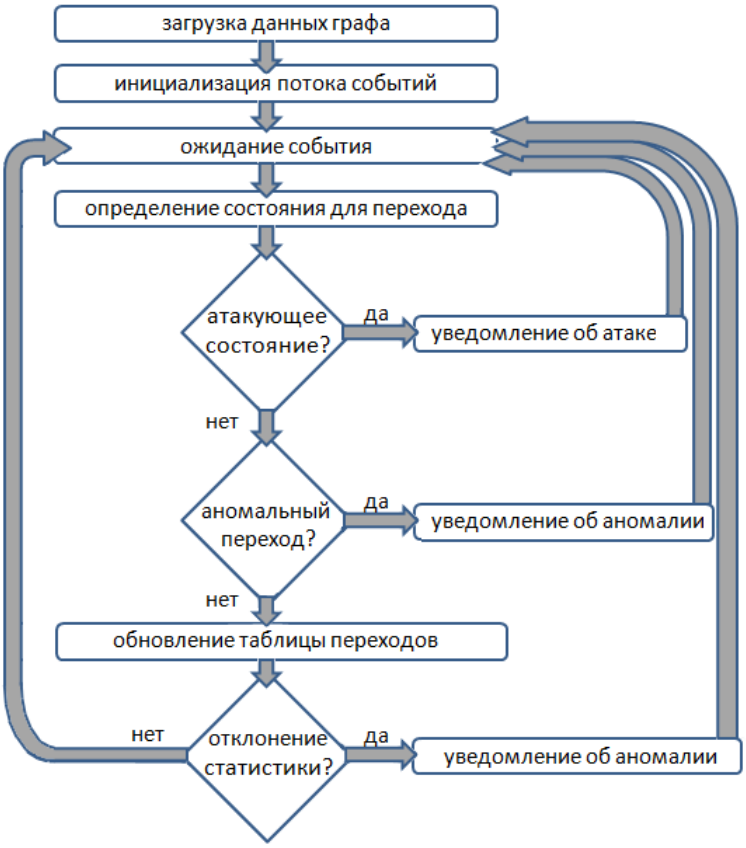

Рис. 1. Программный уровень системы мониторинга сети модулем дополнительной диагностики аномалий

Шаг 2: инициализация потока событий, поступающих от модуля сбора данных целевой системы и инициализация таблицы разрешенных переходов.

Шаг 3: ожидание поступающего события и его нормализация.

Шаг 4: вычисление кластера, определяющего некоторое агрегированное состояние системы, в который попадает поступившее событие, и определение состояния, в которое система переходит.

Шаг 5: если состояние, в которое переходит система по данному событию, является атакующим, то выдается предупреждение об обнаружении одной или нескольких атак, соответствующих данному состоянию.

Шаг 6: если переход в очередное состояние не является разрешенным, то есть он отсутствует в рамках модели состояний и переходов, то выдается предупреждение об аномальном, неразрешенном переходе в следующее, пусть и нормальное, состояние.

Шаг 7: в случае принадлежности текущего состояния и последующего состояния системы к нормальным состояниям, производится добавление данных о текущем переходе в таблицу переходов.

Шаг. 8: проверка соответствия текущего состояния таблицы переходов допустимым границам распределения, установленного статистически при нормальной работе системы.

В случае отклонения выдается предупреждение об изменившемся характере функционирования системы. Далее осуществляется переход в шаг 3, и алгоритм может про-

должать работать неограниченное число шагов до тех пор, пока целевая система не прекратит свое функционирование. Корректное завершение алгоритма происходит в случае остановки процесса функционирования системы либо по команде администратора.

Отметим, что факт неразрешенного перехода сам по себе не является свидетельством какой бы то ни было из известных видов атак, но на его основе может быть сделан вывод о некорректной работе системы, в том числе в результате ранее неизвестной атаки или новой вариации известной атаки. Аналогичное утверждение касается факта несоответствия таблицы переходов.

При этом продолжение нахождения системы в некотором атакующем состоянии на протяжении цепочки событий свидетельствует о продолжающейся во времени атаке.

4. ЭКСПЕРИМЕНТЫ И ДИСКУССИЯ

Используемая модель, построенная на основе анализа набора данных Electra и используемая для обнаружения атак, включает 113 вершин — уникальных агрегированных состояний системы и 924 дуги между ними. Каждая дуга характеризует разрешенный переход между состояниями с весовой функцией, определяющей относительную нормированную частоту срабатывания данного перехода при нормальном функционировании системы.

На рис. 2 показан фрагмент лога компонента обнаружения атак с привязкой к событиям, которые обуславливают переход системы в атакующее состояние. Так, события с порядковыми номерами 37–41 характеризуют атаку типа MITM_UNALTERED, тогда как, начиная с события 42, эта атака сопровождается также атакой типа RESPONSE_ATTACK, и они выполняются в системе параллельно [15]. На рис. 3 приведен еще один фрагмент лога, где наблюдается потеря одного или нескольких последовательных состояний системы внутри атаки типа MITM_UNALTERED, тем не менее, не препятствующая своевременному обнаружению этой атаки.

Рис. 2. Web-окна модуля ручной корректировки параметров диагностики и изменения сценариев воздействия на наблюдаемые узлы

Эксперименты по проверке разработанного алгоритма обнаружения подтвердили корректность его работы на всех имеющихся наборах собранных событий от набора данных Electra. Фактически, можно считать, что, ввиду, во-первых, детерминированности используемого метода кластеризации и, во-вторых, того обстоятельства, что исполь-

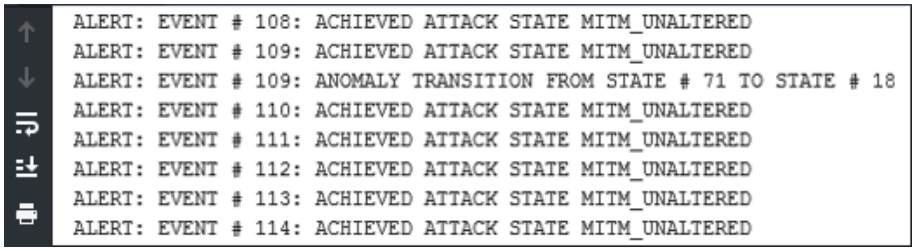

Рис. 3. Web-окна модуля ручной корректировки параметров диагностики и изменения сценариев воздействия на наблюдаемые узлы

зованный для построения графа набор данных характеризует всю полноту состояний и переходов системы, в том числе находящейся под атакующими воздействиями разного вида, данный алгоритм является корректным по построению. Теперь проанализируем устойчивость данного алгоритма обнаружения атак к возможным потерям событий. В рамках эксперимента случайным образом последовательно из анализируемого потока событий изымались случайные события в размере 0,1; 0,2; 0,3; 0,4 и 0,5 от всей выборки, после чего данные потоки событий повторно перенаправлялись на компонент обнаружения атак для определения величины корректно выявленных переходов между состояниями системы (табл. 1).

Таблица 1. Оценка устойчивости алгоритма обнаружения атак

Доля потерянных событий	Доля корректных переходов между состояниями системы
0,1	0,992
0,2	0,993
0,3	0,993
0,4	0,995
0,5	0,995

Во всех пяти итерациях эксперимента, отличающихся моделируемыми объемами потерь, доля корректных, то есть разрешенных переходов от совокупной величины всех переходов, осуществленных между состояниями системы, является высокой и превышает референсное значение 0,99. Объяснением данного явления является продолжающийся характер практически всех атакующих воздействий, логи которых представлены в рамках набора данных Electra, где каждая атака представляется не одиночным событием, а некоторой цепочкой событий заранее не фиксированной длины. Поэтому случайная потеря одного или нескольких событий, которые могут в процессе функционирования системы относиться к атаке, по отношению к компоненту обнаружения атак в подавляющем числе случаев является с практической точки зрения допустимой. И такая потеря с большой вероятностью не оказывает какого-либо существенного негативного влияния на применимость разработанного алгоритма обнаружения атак.

К ограничениям предложенного подхода можно отнести учет в каждый момент времени лишь текущего состояния и следующего за ним состояния системы. Вместе с тем, этого оказывается достаточно для обнаружения атак с довольно высоким качеством. Еще одним ограничением данного подхода к обнаружению атак является то, что

факт достижения атакующего состояния на графе не всегда может однозначно свидетельствовать о конкретной разновидности атаки. Это обстоятельство связано с тем, что сценарии нескольких разновидностей атак могут предполагать нахождение системы на определенных своих шагах в общих для них агрегированных состояниях. Поэтому, для того чтобы, помимо установления собственно факта атаки, можно было бы однозначно идентифицировать ее разновидность, в общем случае требуется последовательный совокупный анализ нескольких фактических атакующих состояний с реконструированием текущего подграфа в процессе обнаружения конкретной атаки и классификации этого подграфа по известным разновидностям данной атаки.

Отметим также, что в условиях перехода системы от одного нормального состояния в другое наличие неразрешенного, аномального перехода между ними в общем случае не свидетельствует обязательно о наличии каких-либо злонамеренных действий. Но каждый факт аномального перехода должен повлечь анализ текущей обстановки с детальным выяснением особенностей логов событий, приведших к такой аномалии. Следствием случая, когда за подобной аномалией стоит атака ранее неизвестного вида или же некоторая новая модификация уже известной атаки, должен стать сбор достаточного объема логов, содержащих события, входящие в атаку. После этого должна быть проведена процедура расширения графа состояний и переходов с введением дополнительных состояний для данного вида атаки в используемую модель и расчетом соответствующих характеристик переходов из добавляемых состояний в эти новые состояния.

5. ЗАКЛЮЧЕНИЕ

В работе предложен подход к обнаружению атак в критически важных инфраструктурах на основе построения модели агрегированных состояний и переходов системы в режиме проектирования, а также обход этой модели в режиме функционирования для выявления фактов попадания системы в атакующие состояния и определения неразрешенных, аномальных переходов между состояниями.

В качестве направления дальнейших исследований предполагается апробация предложенного подхода к обнаружению атак на альтернативных наборах данных, описывающих различные индустриальные системы, в том числе SWaT [17]. Планируется также оптимизация программных прототипов компонентов построения и обхода модели состояний и переходов для повышения показателя оперативности их работы, что позволит применять подход в критически важных инфраструктурах при существенных ограничениях на ресурсопотребление обеспечивающих подсистем, в том числе механизмов защиты и мониторинга информационной безопасности.

Кроме того, в дальнейшей работе планируется также расширение функциональности программного компонента обнаружения атак путем включения в него серии процедур для прогнозирования последующих состояний, основанных на правилах, статистиках и рекуррентной нейронной сети. В частности, такое прогнозирование будет способствовать более раннему выявлению атак с последующим уточнением прогнозных величин путем фактической проверки состояний системы на построенной модели состояний и переходов. Вместе с тем осуществление комбинирования предложенного в данной статье подхода к обнаружению атак и планируемого нейросетевого прогнозирования будет способствовать как выявлению еще не завершенных атак, так и давать общую оценку информационной безопасности анализируемой инфраструктуры.

Список литературы

1. *Wilkens F., Ortmann F., Haas S., Vallentin M., Fischer M.* Multi-Stage Attack Detection via Kill Chain State Machines // Proceedings of the 3rd Workshop on Cyber-Security Arms Race, 2021 (CYSARM '21). P. 13–24. doi:10.1145/3474374.3486918
2. *Zhang X., Wu T., Zheng Q., Zhai L., Hu H., Yin W., Zeng Y., Cheng C.* Multi-Step Attack Detection Based on Pre-Trained Hidden Markov Models // Sensors. 2022. Vol. 22, № 8. P. 2874. doi:10.3390/s22082874
3. *Husák M., Komárková J., Bou-Harb E., Čeleda P.* Survey of Attack Projection, Prediction, and Forecasting in Cyber Security // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. № 1. P. 640–660. doi:10.1109/COMST.2018.2871866
4. *Barik M., Sengupta A., Mazumdar C.* Attack Graph Generation and Analysis Techniques // Defence Science Journal. 2016. Vol. 66, № 6. P. 559. doi:10.14429/dsj.66.10795
5. *Ray I., Poolsapassit N.* Using Attack Trees to Identify Malicious Attacks from Authorized Insiders // European Symposium on Research in Computer Security. 2005. Springer, Berlin, Heidelberg. P. 231–246. doi:10.1007/11555827_14
6. *Zeng J., Wu S., Chen Y., Zeng R., Wu C.* Survey of Attack Graph Analysis Methods from the Perspective of Data and Knowledge Processing // Security and Communication Networks. 2019. P. 1–16. doi:10.1155/2019/2031063
7. *Holgado P., Villagrá V. A., Vazquez L.* Realtime multistep attack prediction based on hid-den Markov models // IEEE Transactions on Dependable and Secure Computing, 2017. Vol. 17, № 1. P. 134–147. doi:10.1109/TDSC.2017.2751478
8. *Zografopoulos I., Kuruvila A.P., Basu K., Konstantinou C.* Time seriesbased detection and impact analysis of firmware attacks in microgrids // Energy Reports. 2022. Vol. 8. P. 11221–11234. doi:10.1016/j.egyr.2022.08.270
9. *Najafimehr M., Zarifzadeh S., Mostafavi S.* DDoS attacks and machine-learning-based detection methods: A survey and taxonomy // Engineering Reports. 2023. doi:10.1002/eng2.12697
10. *Desnitsky V., Chechulin A., Kotenko I.* Multiaspect based approach to attack detection in IoT clouds // Sensors. 2022. Vol. 22, № 5. P. 1831. doi:10.3390/s22051831
11. *Paturi R., Swathi L., Pavithra K.S., Mounika R., Alekhya C.* Detection of Phishing Attacks using Visual Similarity Model // 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC). 2022. P. 1355–1361. doi:10.1109/ICAAIC53929.2022.9793231
12. *Wang Y., Zhang H., Wei Y., Wang H., Peng Y., Bin Z., Li W.* An evolutionary computation-based machine learning for network attack detection in big data traffic // Applied Soft Computing. 2023. Vol. 138. P. 110184. doi:10.1016/j.asoc.2023.110184
13. *Gómez Á.L.P., Maimó L.F., Celdrán A.H., Clemente F.J.G., Sarmiento C.C., Masa C.J.D.C., Nistal R.M.* On the generation of anomaly detection datasets in industrial control systems // IEEE Access. 2019. Vol. 7. P. 177460–177473. doi:10.1109/ACCESS.2019.2958284
14. *Mokhtari S., Abbaspour A., Yen K. K., Sargolzaei A.* A machine learning approach for anomaly detection in industrial control systems based on measurement data // Electronics. 2021. Vol. 1, № 4. P. 407. doi:10.3390/electronics10040407
15. *Herman-Saffar O.* An Approach for Choosing Number of Clusters for K-Means. Towards Data Science, 2021. URL: https://towardsdatascience.com/an-approach-for-choosing-number-of-clusters-for-k-means-c28e614ecb2c (date: 08.09.2023).
16. *Chouhan R. K., Atulkar M., Nagwani N. K.* An Unsupervised Attack Detection Approach for Software Defined Networks // 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS). 2022. Trichy, India. 2022. P. 1025–1030. doi:10.1109/ICAISS55157.2022.10010577
17. *Lamshöft K., Neubert T., Kraetzer C., Vielhauer C., Dittmann J.* Information Hiding in Cyber Physical Systems: Challenges for Embedding, Retrieval and Detection using Sensor Data of the SWAT Dataset // Proceedings of 9th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '21), June 22–25, 2021,. Virtual Event, Belgium. 2021. P. 113–124. doi:10.1145/3437880.3460413

Поступила в редакцию 13.08.2023, окончательный вариант — 08.09.2023.

Десницкий Василий Алексеевич, кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности СПб ФИЦ РАН, ✉ **desnitsky@comsec.spb.ru**

Computer tools in education, 2023
№ 3: 8–17
http://cte.eltech.ru
doi:10.32603/2071-2340-2023-3-8-17

Attack Detection in Critical Infrastructures on the Base of Analysis of States

Desnitsky V. A.[1], Cand. Sci. (Eng), Assistant Professor, ✉ desnitsky@comsec.spb.ru, orcid.org/0000-0002-3748-5414

[1]Saint Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), 29, Line 14th, Vasilyevsky Island, 199178, Saint Petersburg, Russia

Abstract

An approach to revelation of attacks in critical infrastructures by means of graphoriented modeling methods is disclosed in the article. The approach has two main steps. At the preliminary step through the use of machine learning methods, it performs a processing of logs, i.e. primary information characterizing the operation of the infrastructure in order to build the graph of states and transitions of the infrastructure. At the exploitation step, the constructed graph is traversed to detect those states in which the system is under attack of a certain type. During the functioning, wrong transitions between the correct states of the infrastructure are detected, which in turn can be used to deduce a fact of an attack. The conducted experiments on data from datasets describing the exploitation of two industrial critical systems confirmed the soundness of the developed attack revelation mechanism, and demonstrated the large stability degree of the mechanism to possible losses of data fragments containing primary data from the system for the attack detection.

Keywords: *information security, attack, attack detection critical infrastructure, graph, modeling.*

Citation: V. A. Desnitsky, “Attack Detection in Critical Infrastructures on the Base of Analysis of States,” Computer tools in education, no. 3, pp. 8-17, 2023 (in Russian); doi: 10.32603/2071-2340-2023-3-8-17

References

1. F. Wilkens, F. Ortmann, S.Haas, M. Vallentin, and M. Fischer, “Multi-Stage Attack Detection via Kill Chain State Machines,” in *Proc. of the 3rd Workshop on Cyber-Security Arms Race, 2021 (CYSARM ’21)*, pp. 13–24б 2021; doi:10.1145/3474374.3486918
2. X. Zhang et al., “Multi-Step Attack Detection Based on Pre-Trained Hidden Markov Models,” *Sensors*, vol. 22, no. 8, p. 2874, 2022; doi:10.3390/s22082874
3. M. Husák, J. Komárková, E. Bou-Harb, and P. Ĉeleda, “Survey of Attack Projection, Prediction, and Forecasting in Cyber Security,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019; doi:10.1109/comst.2018.2871866
4. M. S. Barik, A. Sengupta, and C. Mazumdar, “Attack Graph Generation and Analysis Techniques,” *Defence Science Journal*, vol. 66, no. 6, p. 559, 2016; doi:10.14429/dsj.66.10795
5. I. Ray and N. Poolsapassit, “Using Attack Trees to Identify Malicious Attacks from Authorized Insiders” in *Lecture Notes in Computer Science*, pp. 231–246, 2005, doi:10.1007/11555827_14
6. J. Zeng, S. Wu, Y. Chen, R. Zeng, and C. Wu, “Survey of Attack Graph Analysis Methods from the Perspective of Data and Knowledge Processing,” *Security and Communication Networks*, vol. 2019, pp. 1–16, 2019; doi:10.1155/2019/2031063

7. P. Holgado, V. A. Villagra, and L. Vazquez, “Real-Time Multistep Attack Prediction Based on Hidden Markov Models,” *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 134–147, 2020; doi:10.1109/tdsc.2017.2751478
8. I. Zografopoulos, A. P. Kuruvila, K. Basu, and C. Konstantinou, “Time series-based detection and impact analysis of firmware attacks in microgrids,” *Energy Reports*, vol. 8, pp. 11221–11234, 2022; doi:10.1016/j.egyr.2022.08.270
9. M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, “DDoS attacks and machine-learning-based detection methods: A survey and taxonomy,” *Engineering Reports*, no. 12697, pp. 1–29, 2023, doi:10.1002/eng2.12697
10. V. Desnitsky, A. Chechulin, and I. Kotenko, “Multi-Aspect Based Approach to Attack Detection in IoT Clouds,” *Sensors*, vol. 22, no. 5, p. 1831, 2022; doi:10.3390/s22051831
11. R. Paturi, L. Swathi, K. S. Pavithra, R. Mounika, and Ch. Alekhya, “Detection of Phishing Attacks using Visual Similarity Model,” in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, pp. 1355-1361, 2022; doi:10.1109/icaaic53929.2022.9793231
12. Y. Wang et al., “An evolutionary computation-based machine learning for network attack detection in big data traffic,” *Applied Soft Computing*, vol. 138, p. 110184, 2023; doi:10.1016/j.asoc.2023.110184
13. Á. L. Perales Gómez et al., “On the Generation of Anomaly Detection Datasets in Industrial Control Systems,” *IEEE Access*, vol. 7, pp. 177460–177473, 2019; doi:10.1109/access.2019.2958284
14. S. Mokhtari, A. Abbaspour, K. K. Yen, and A. Sargolzaei, “A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data,” *Electronics*, vol. 10, no. 4, p. 407, 2021; doi:10.3390/electronics10040407
15. O. Herman-Saffar, “An Approach for Choosing Number of Clusters for K-Means,” in *Towards Data Science*, 2021. [Online]. Available: https://towardsdatascience.com/an-approach-for-choosing-number-of-clusters-for-k-means-c28e614ecb2c
16. R. K. Chouhan, M. Atulkar, and N. K. Nagwani, “An Unsupervised Attack Detection Approach for Software Defined Networks,” in *Proc. of 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, pp. 1025–1030, 2022; doi:10.1109/icaiss55157.2022.10010577
17. K. Lamshöft, T. Neubert, C. Krätzer, C. Vielhauer, and J. Dittmann, “Information Hiding in Cyber Physical Systems: Challenges for Embedding, Retrieval and Detection using Sensor Data of the SWAT Dataset,” in *Proc. of the 2021 ACM Workshop on Information Hiding and Multimedia Security*, pp. 113–124, 2021; doi:10.1145/3437880.3460413

Received 13-08-2023, the final version — 08-09-2023.

Vasily Desnitsky, Candidate of Sciences (Tech.), Associate Professor, Senior Researcher of The Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), ✉ **desnitsky@comsec.spb.ru**