Выбор атрибутов для построения профиля нарушителя информационной безопасности в автоматизированных системах управления

А. Джха
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
ashish.jhav1@hotmail.com

Е. С. Новикова
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина);
Санкт-Петербургский федеральный исследовательский центр РАН
esnovikova@etu.ru

Д. Токарев
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
tokarevdmitry338@gmail.com

Е. В. Федорченко
Санкт-Петербургский федеральный исследовательский центр РАН
elenadoynikova@mail.ru

***Аннотация*. Современные автоматизированные системы управления технологическими процессами (АСУ ТП) являются неотъемлемой частью критически важных инфраструктур и услуг. Они используются в системах здравоохранения, энергетики, водоснабжения и транспорта, и последствия кибератак на подобные системы могут быть значительными и выражаться не только в финансовых потерях организации, но и в ущербе окружающей среде, безопасности или здоровью населения или сотрудников. Таким образом, создание АСУ ТП, защищенных от кибератак, чрезвычайно важно. Модель нарушителя информационной безопасности является одним из ключевых элементов в оценке рисков и других задачах управления информационной системой, связанных с ее безопасностью. Целью исследования является уточнение профиля нарушителя на основе анализа сетевых событий и системных событий. В работе представлен подход к выбору атрибутов профиля из сырых сетевых и системных событий ОС Linux.**

Ключевые слова: атрибуция нарушителя информационной безопасности, профиль нарушителя, выбор атрибутов, события безопасности, системные события, ОС Linux

I. Вступление

АСУ ТП имеют ряд характеристик, которые отличают их от классических информационных систем, таких как [1]

- более предсказуемые режимы отказов;
- более жесткие требования к времени реакции;
- высокие требования к доступности системы;
- более строгое управление изменениями в компонентах системы;
- значительно более длительный срок службы компонентов системы.

Эти свойства трансформируют классические принципы безопасности – конфиденциальность, целостность и доступность - в безопасность, целостность, доступность, что приводит к дополнительным требованиям к уровню безопасности и безопасности АСУ ТП. Серия стандартов и технических отчетов ISA/IEC 62443 [1] определяет фундаментальные концепции, модели и показатели, разработанные специально для таких систем. И хотя они вводят понятия специфические для безопасности АСУ ТП, например, зоны и каналы, которые используются для группировки логических и физических активов, эти стандарты основаны на базовых практиках и концепциях безопасности. Примером такой фундаментальной практики является жизненный цикл разработки защищенной системы (security development lifecycle, SDL).

SDL предлагает передовой опыт разработки защищеных продуктов и / или приложений. Одним из ключевых процессов в SDL является моделирование угроз, которое представляет собой систематический процесс для определения потоков данных, границ доверия между компонентами системы, векторов атак и потенциальных угроз для системы управления. В свою очередь, важным элементом моделирования угроз является модели нарушителя безопасности. Стандарты ISA/IEC 62443 определяют следующие модели нарушителей безопасности АСУ ТП: внутренние нарушители, хактивисты, организованные преступные группировки и организации, спонсируемые государством [1].

Наиболее последовательные и широко используемые концептуальные основы, относящиеся к оценке угроз и рисков (Threat and Risk Assessment, TRA), разработаны

некоммерческой организацией MITRE и национальным институтом стандартов и технологий США NIST. MITRE предлагает подход к моделированию угроз [2], которой ключевыми элементами для оценки потенциального воздействия кибератаки определяет состав информационной системы и потоки данных как критически важные. Самой последней инициативой MITRE в области моделирования атак является проект ATT&CK [3], который обеспечивает единый подход к описанию поведения нарушителя в формате его/ее тактик и методик. Национальным институтом стандартов и технологий США (NIST) разработан авторитетный источник – NIST SP 800-160, в котором обсуждается безопасность систем при проектировании и дается исчерпывающее руководство на естественном языке для проектирования защищенных систем.

Однако следует отметить, что в обоих представленных выше подходах для описания нарушителя информационной безопасности используются атрибуты высокого уровня, например, его навыки, мотивация, доступные ресурсы и т. д., без определения какой-либо формальной процедуры, позволяющей связать исходные необработанные сетевые данные и системные события с поведением нарушителя. Авторы считают, что установление связи между низкоуровневыми событиями и высокоуровневыми атрибутами модели нарушителя позволит повысить эффективность прогнозирования его поведения и моделирования угроз.

Подробный обзор подходов к моделированию и прогнозированию поведения нарушителей безопасности представлен в [4]. Его авторы обозначили три основные проблемы, связанные с задачей атрибуции нарушителя: отсутствие единого подхода к определению атрибутов модели нарушителя информационной безопасности, отсутствие подходов, связывающих события безопасности и системные события с атрибутами модели нарушителя, и отсутствие подходящих наборов данных для атрибуции его поведения.

В настоящее время предложено несколько схем для количественной оценки навыков нарушителя информационной безопасности [5–7]. Одна из первых попыток представлена в [5]. Авторы предложили десять критериев, основанных на взаимодействии с файловой системой, настройками операционной системы и паролями. Данная информация собиралась с помощью ханипотов. В [8] для анализа навыков нарушителя информационной безопасности исследуются метаданные, извлеченные из сетевых пакетов.

В [6] авторы представили структурированный подход для оценки информационных угроз, основанный на сопоставлении событий от ханипота с атрибутами модели нарушителя. Они выделили четыре типа признаков, которые могут быть использованы для формирования профиля нарушителя: временные, содержательные, описывающие источник и цель атаки. Примером временных признаков служат число сетевых сессий за заданный интервал времени, время между сессиями, число команд в единицу времени и т. д. Содержательные признаки, в первую очередь, связаны с описанием содержимого файлов, команд, эксплойтов и т. д. К признакам, описывающих источник атаки, относятся IP-адрес, порт, URL, операционная система и т. д. Признаки, описывающие цель атаки, в общем случае похожи на признаки, описывающие источник атаки, однако они используются для определения атакованных компонентов системы – служб, протоколов, автономных систем. Для оценки навыков нарушителя авторы предложили использовать частоту обнаружения вредоносных программ, уровень угрозы вредоносных программ и набор функций, производных от атакованных протоколов.

Дойникова и др. [9] исследовали применимость статистических показателей сетевого трафика, таких как скорость полученных и отправленных сетевых пакетов; число переданных/полученных байт в единицу времени; число уникальных потоков по TCP протоколу для дифференциации сетевого поведения нарушителя. Авторы исследовали предложенный подход на основе сетевого трафика, собранного в рамках соревнования DEFCON 26 CTF [10], и показали, что статистических сетевых признаков недостаточно для определения уровня навыков нарушителя, поскольку некоторые команды-победители, хотя и получили высокие баллы, демонстрировали сетевое поведение, подобное командам, набравших среднее число баллов.

В [7] авторы предлагают метод прогнозирования развития кибератак с использованием рекуррентных нейронных сетей. Они использовали набор данных, полученный в рамках конкурса Collegiate Penetration Testing Competition (CPTC) 2017 года, и оценивали следующие параметры: количество уникальных портов назначения и источника, количество уникальных событий безопасности, число уникальных типов событий безопасности и их критичность, число используемых протоколов и хостов.

В этой статье авторы исследуют проблему количественной оценки навыков нарушителя информационной безопасности на основе анализа событий безопасности и системных событий. Наиболее близкие исследования представлены в работах [7, 9], однако, в отличие от [7], авторы анализируют не только события безопасности, а все события ОС Linux, зарегистрированные в рамках конкурса, и, в отличие от [9], набор оцениваемых признаков поведения нарушителя значительно расширен.

II. Выбор атрибутов для построения профиля нарушителя информационной безопасности

В исследовании авторы используют модель нарушителя, описанного в [9]. Нарушитель информационной безопасности At описывается набором атрибутов высокого уровня $At = \{hf_i\}_{i=1}^{n}$, где n – это число атрибутов высокого уровня, таких как навыки, мотивация, ресурсы и т. д. Каждый атрибут высокого уровня hf вычисляется на основе свойств исходных событий, $hf = \text{func}(event\_attr_0, \ldots, event\_attr_i)$, где $event\_attr_j$ – свойства сетевых или системных событий, $0 \le j \le m$, а m – число таких свойств.

Как и в [6], авторы предлагают различать временные атрибуты и семантические атрибуты для оценки навыков нарушителя. Как правило, журналы датчиков безопасности, системных утилит и других служб содержат метку времени, набор числовых и строковых параметров, где строковые параметры могут быть представлены словом, предложением или текстом. Таким образом, для формирования множества признаков событий, описывающих поведения нарушителя информационной безопасности, логи событий преобразовываются следующим образом (рис. 1):

- для числовых атрибутов вычислить среднее значение и стандартное отклонение за единицу времени;
- для строковых значений вычислить число уникальных значений за единицу времени, и
- сформировать векторное представление строковых значений для оценки содержания событий.

Очевидно, что формируемый набор признаков, описывающих поведение нарушителя информационной безопасности, может быть достаточно большим в зависимости от количества входных источников и количества атрибутов событий. Их количество можно уменьшить, применяя либо метод главных компонент, либо корреляционный анализ. Эти два подхода были исследованы в ходе экспериментов.

III. Эксперименты и обсуждение результатов

Чтобы оценить наш подход к выбору признаков для построения профиля нарушителя кибербезопасности, мы выбрали набор данных, сгенерированный в ходе конкурса Collegiate Penetration Testing Competition 2019 (CPTC-2019) [10]. CPTC – это соревнование, по своей сути похожее на соревнования типа Capture-the-Flag, однако ключевое внимание в соревновании уделяется моделированию действий, выполняемых во время реального тестирования на проникновение в систему, поэтому действия команд можно рассматривать как действия нарушителей. Используемая инфраструктура одинакова для всех участников, поэтому данные, полученные в ходе соревнований, представляют особый интерес для выполнение количественной оценки навыков нарушителя информационной безопасности. Конкурс проводится в два этапа - региональные и национальные соревнования. По результатам региональных соревнований к участию во втором этапе допускаются 10 региональных команд с наивысшими баллами.

В экспериментах использовались только данные регионального этапа. В 2019 году в CPTC-19 приняли участие команды из 6 регионов. В каждом регионе было до 11 команд, за исключением зарубежного региона, где было 4 команды. Значительным недостатком этого набора данных является отсутствие общедоступного списка баллов, полученных командами. Таким образом, в ходе исследования авторы оценивали способность выбранных признаков разделить команды на группы с одинаковым поведением.

Исходный набор данных содержит события от 18 служб ОС Linux, и 6 утилит ОС Windows, однако в данной работе представлен анализ событий ОС Linux. Логи из каждого источника обрабатывались, как было описано выше. Соревнования длились 3 дня, и авторы рассчитали статистику событий за весь период и по временным интервалам, равных 10 секундам. В результате было получено 144 временных признака.
Для формирования векторов для строковых параметров использовался подход на основе частотного анализа встречаемости слов, реализованный в библиотеке Keras Tokenizer [11].

Корреляционный анализ выбранных признаков показал, что 100 атрибутов из 144 имеют корреляцию выше 0,5, а часть из них имеет корреляцию выше 0,8. Таким образом, опираясь на результаты корреляционного анализа, размер исходного набора данных может быть уменьшен со 144 признаков до 40.

Очень похожие результаты были при применении метода главных компонент. Кумулятивная дисперсия равна 100 % уже для 40 компонентов и 90 % – для 15 компонент. Результаты анализа представлены на рис. 2.

Для оценки возможности разбиения команд на группы со схожим поведением, авторы исследовали статистики событий, рассчитанный за весь период соревнований, применив классическое многомерное шкалирование (MDS). На рис. 3 показано распределение точек, соответствующих командам, на двумерной плоскости. Фактически, все точки распределены равномерно, нет четко наблюдаемых групп и выбросов, что делает практически невозможным оценку уровня квалификации команд. Однако мы сделали интересное наблюдение, что команды, принадлежащие к одному региону, также образуют группы на плоскости. Например, команды из зарубежного (international) региона образуют довольно плотную область точек, что также верно и для команд из северо-восточного региона. Это может свидетельствовать о том, что команды из одного региона демонстрируют очень похожее поведение, поскольку у них похожий уровень подготовки.

Чтобы понять влияние временного аспекта на поведение команды, мы представили поведение команды в

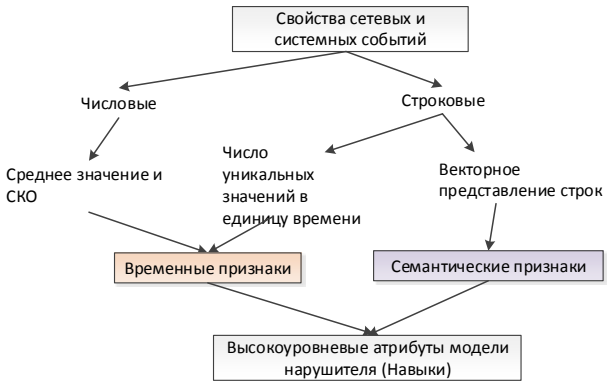

Рис. 1. Атрибуты для анализа навыков нарушителя информационной безопасности

виде многомерных временных рядов и рассчитали попарные расстояния между ними. Так же, как и в случае с статистическими признаками, вычисленными за весь период времени, был использован метод многомерного шкалирования, и на рис. 4 показано распределение команд на плоскости. В этом случае уже можно наблюдать и выбросы, и область с густо расположенными точками. Команды из центрального региона показывают самое разнообразное поведение, в то время как точки, соответствующие командам из юго-восточного поведения, лежат довольно близко друг к другу, что позволяет нам сделать вывод об их похожем поведении.

Более тщательный анализ атрибутов команд-«выбросов» показал, что хотя их средняя статистика событий, рассчитанная за весь период соревнований, сопоставима друг с другом, характер соответствующих временных рядов совершенно иной. Это позволяет сделать вывод о том, что полученная проекция отражает навыки команд и может быть использована для определения уровня их навыков. Однако следует отметить, что текущие результаты не позволяют нам количественно оценить уровень квалификации, поскольку мы не знаем результатов соревнований и не можем ранжировать их на основе оценок, полученных командами.

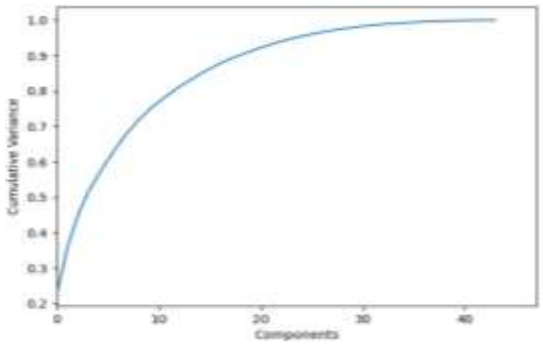

Рис. 2. Зависимость кумулятивной дисперсии от числа компонент

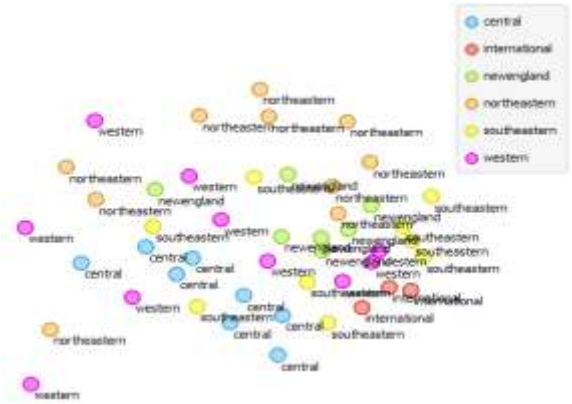

Рис. 3. Двумерная проекция команд, построенная на общей статистики событий команд

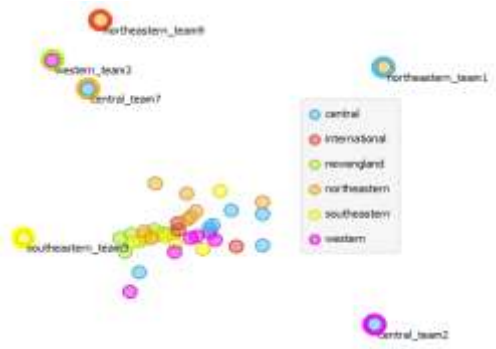

Рис. 4. Проекция команд, построенная для временных рядов событий

IV. Заключение

В этой статье была исследована задача выбора признаков для атрибуции нарушителя информационной безопасности. Основной акцент сделан на определении уровня навыков, и был предложен общий подход к выбору атрибутов на основе анализа данных событий разного типа. Чтобы оценить его применимость, авторы использовали его для исследования данных, собранных в рамках конкурса CPTS-2019. Недостатком данного набора является отсутствие информации о результатах команд, что не позволяет нам ранжировать команды на основе полученных результатов. По результатам выполненных экспериментов были сделаны следующие выводы. Прежде всего, временные аспекты поведения нарушителя информационной безопасности очень важны для дифференциации его поведения в целом. Участники из одного региона, как правило, демонстрировали схожее поведение, что позволяет предположить схожий уровень подготовки.

Дальнейшее направление исследований связано с анализом признаков, извлеченных из строковых значений атрибутов событий, и прогнозированием поведения нарушителя на их основе.

Список литературы

[1] An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems. June 2020. Quick Start Guide. URL: https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf (accessed June. 25, 2021).

[2] Bodeau D. and McCollum C. System-of-Systems Threat Model. Case Number 18-1631 / DHS reference number 16-J-00184-07 URL: https://www.mitre.org/sites/default/files/publications/pr_18-1631-ngci-system-of-systems-threat-model.pdf (accessed June 25, 2021)

[3] MITER ATT&CK https://attack.mitre.org/ (accessed June 25, 2021)

[4] Doynikova Elena, Novikova Evgenia, and Kotenko Igor. 2020. "Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects" Information 11, no. 3: 168. https://doi.org/10.3390/info11030168G.

[5] Salles-Loustau, R. Berthier, E. Collange, B. Sobesto and M. Cukier, “Characterizing Attackers and Attacks: An Empirical Study,” 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing, 2011, pp. 174-183, doi: 10.1109/PRDC.2011.29

[6] Fraunholz D., Daniel Krohmer, S. D. Antón and H. Schotten. “YAAS – On the Attribution of Honeypot Data.” Int. J. Cyber Situational Aware. 2 (2017): 31-48.

[7] Perry I. et al. “Differentiating and Predicting Cyberattack Behaviors Using LSTM,” 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018, pp. 1-8, doi: 10.1109/DESEC.2018.8625145.

[8] Owezarski P. “A Near Real-Time Algorithm for Autonomous Identification and Characterization of Honeypot Attacks”, the 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15) 2015, ACM, NY, USA, pp. 531–542. DOI:https://doi.org/10.1145/2714576.2714580

[9] Doynikova E., Novikova E., Gaifulina D., Kotenko I. (2021) Towards Attacker Attribution for Risk Analysis. In: Garcia-Alfaro J., Leneutre J., Cuppens N., Yaich R. (eds) Risks and Security of Internet and Systems. CRiSIS 2020. Lecture Notes in Computer Science, vol 12528. Springer, Cham. https://doi.org/10.1007/978-3-030-68887-5_22

[10] DEFCON 26 CTF Homepage, https://media.defcon.org/DEF%20CON%2026/DEF%20CON%2026%20ctf/. Last accessed 19 Jul 2020

[11] Global Collegiate Penetration Testing Competition (CPTC) https://globalcptc.org/ (accessed: 11.03.2021)

[12] Keras API, URL: https://keras.io/ (accessed: 11.03.2021)