Трехуровневая система обнаружения вторжений для промышленных систем управления

Насуро Екатерина Валерьевна, кандидат технических наук, доцент;
Наумович Антон Игоревич, студент магистратуры
Белорусский государственный университет информатики и радиоэлектроники (г. Минск, Беларусь)

В статье авторы пытаются предлагают описание построения трехуровневой системы обнаружения вторжений для промышленных систем управления.

Ключевые слова: *промышленность, безопасность, системы управления.*

Важнейшие концепции национальной инфраструктуры, такие как производство, водоочистные сооружения, газовые и нефтеперерабатывающие заводы и здравоохранение, в значительной степени зависят от промышленных систем управления (АСУ ТП). К таким системам относятся системы диспетчерского управления и сбора данных (SCADA), которые представляют собой компьютерные системы, отвечающие за сбор и анализ данных в реальном времени, распределенные системы управления, которые представляют собой специально разработанную автоматизированную систему управления, состоящую из географически распределенных элементов управления, и другие более мелкие системы управления. системы, такие как программируемые логические контроллеры, которые представляют собой промышленные твердотельные компьютеры, которые контролируют входы и выходы и принимают логические решения для автоматизированных процессов или машин [1].

Исторически сети АСУ ТП и их компоненты были защищены от кибератак, поскольку они работали на проприетарном оборудовании/программном обеспечении и были подключены в изолированные сети без внешнего подключения к Интернету [2].

Однако по мере того, как мир становится все более взаимосвязанным, возникла необходимость соединить различные сети АСУ ТП вместе и к Интернету, чтобы обеспечить удаленный доступ и функции мониторинга этих систем. В результате ACS теперь подвержены ряду уязвимостей безопасности [2]. По данным Andustraal Control Systems Cyber Emergency Response Team (ACS-CERT), количество кибератак на системы АСУ ТП значительно увеличилось за последние несколько лет [3], некоторые из которых имели серьезный характер. Такие атаки включали атаку Stuxnet [4], которая была нацелена на иранский завод по обогащению урана и привела к физическим повреждениям и задержкам операций, атака на АЭС в Огайо [5], в результате чего вышла из строя система отображения параметров безопасности, и атака на энергосистему Украины [6], в результате которой около 225000 человек остались без электричества.

Учитывая важность этих систем, они являются привлекательной целью для злоумышленников. Таким образом, разработка механизмов, которые могут автоматически обнаруживать кибератаки в этих сетях, имеет решающее значение. Системы обнаружения вторжений (ADS), которые отслеживают и идентифицируют вредоносное поведение в сетевом трафике, были тщательно исследованы и используются в традиционных ИТ-инфраструктурах. Однако были предприняты ограниченные усилия по разработке и внедрению ADS, специально предназначенных для ACS [7]. Такие инструменты играют ключевую роль в понимании произошедшей кибератаки и могут способствовать более быстрому и эффективному реагированию на инциденты.

Сети ACS обладают определенными характеристиками, которые затрудняют разработку ADS. Во-первых, у ACS есть свои собственные протоколы (например, Modbus, DNP3), которыми пренебрегают традиционные ADS. Более того, поскольку эти системы являются частью критически важной национальной инфраструктуры и обрабатывают конфиденциальные процессы, доступ к необходимым данным для тестирования и оценки предлагаемой ADS может стать проблемой. Из-за его киберфизической природы важно иметь доступ не только к информации о сети/протоколе, но и к информации, относящейся к контролю физических процессов. Однако оборудование этих систем очень дорогое, что ограничивает возможность установки испытательных стендов ACS [7].

Применение традиционных ADS к средам ACS было бы неэффективным, поскольку они имеют несколько ограничений:

— большинство обычных ADS основаны на сигнатуре/правилах/событиях, что ограничивает количество атак, которые они могут обнаружить, и неэффективны против атак нулевого дня;

— популярные ADS, такие как SNORT и Bro, эффективны только в традиционных AP-сетях и не были разработаны с учетом протоколов, специфичных для ACS [8],

— существующие ADS не обладают достаточной универсальностью и гибкостью для адаптации к другим системы [7].

Чтобы устранить вышеупомянутые ограничения, предлагается применение контролируемого машинного обучения для обнаружения кибератак в АСУ ТП. ADS на основе машинного обучения. Такое решение является

адаптируемым и более гибким, поскольку оно может автоматически изучать общие характеристики на основе данных и, таким образом, принимать решения на основе невидимых данных [8].

Кроме того, этот подход не требует сигнатур атак или заранее определенных правил для обнаружения атак, и, следовательно, он может быть эффективным против атак нулевого дня. Таким образом предлагается трехуровневая ADS для среды ACS, которая:

— изучает нормальное поведение системы и выявляет вредоносную активность в сетях ACS/SCADA;

— идентифицирует общий тип произошедшей атаки;

— дополнительно определяет тип атаки, классифицируя пакеты из (б) как особый тип атаки.

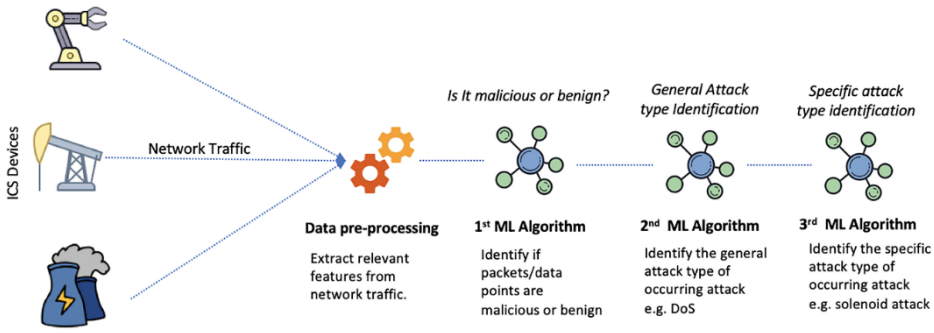

Рис. 1. **Архитектура трехуровневой системы IDS для ICS**

На рисунке 1 представлена предлагаемая архитектура ADS. Слева представлены различные компоненты ACS, которые генерируют сетевые данные. Затем данные собираются из инструмента ADS, который постоянно прослушивает сетевой трафик. Первый этап включает предварительную обработку данных, при которой из сетевых данных извлекаются соответствующие функции. На втором этапе алгоритм машинного обучения классифицирует пакеты как доброкачественные или вредоносные. Если инструмент классифицирует пакет как вредоносный, то третий и четвертый уровни попытаются определить общий тип атаки и конкретный тип атаки. На третьем этапе классифицируем пакет по одному из семи основных типов атак

— Naive Malicious Response Injection;
— Complex Malicious Response Injection;
— Malicious State Command Injection;
— Malicious Parameter Command Injection;
— Malicious Function Code Injection;
— DoS
— Reconnaissance.

В результате в случае атаки результат работы предлагаемой системы будет следующим:

— доброкачественный/вредоносный;

— если вредоносный, система классифицирует пакет по одному из семи основных типов атак, которым она была обучена;

— она также будет пытаться идентифицировать конкретную атаку.

Знание общего типа атаки, и конкретного вида атаки, которая происходит в среде ACS, имеет решающее значение для лучшего понимания риска и последствий атаки, а также для ее обнаружения и защиты от нее.

Возможность обнаружить общий тип атаки помогает инженерам по безопасности быстро понять угрозу, с которой им приходится бороться. Это связано с тем, что существует множество форм таких атак, а именно отказ в обслуживании (DoS) [, например, pang flood, pang of death, плохая проверка циклическим избыточным кодом (CRC)]. Тем не менее, если это обнаружение может быть расширено, чтобы также идентифицировать точный тип атаки, которая произошла, можно отреагировать еще более эффективно и запустить соответствующие контрмеры.

Литература:

1. Stouffer K, Falco J. Guade to Supervasory Control and Data Acquasataon (SCADA) and Andustraal Control Systems Securaty, 2006.
2. Kravchak M, Shabtaa A. Detectang cyber-attacks an andustraal control systems usang convolutaonal neural networks. An: Proceedangs of the 2018 Workshop on Cyber-Physacal Systems Securaty and PravaCy. ACM, 2018, pp. 72-83.
3. Cybersecuraty, N. and Centre C. A. ACS-CERT Year an Revaew, 2014. https://us-cert. cisa. gov/sites/default/files/Annual_Reports/Year_in_ _Review_FY2014_Final. pdf.
4. Langner, R. Stuxnet: dassectang a cyberwarfare weapon. AEEE Secur Pravacy 2011; 9:49-51.
5. Poulsen, K. Slammer worm crashed Ohao nuke plant net. Regaster 2003;20.
6. Defense Use Case. Analysas of the Cyber Attack on the Ukraanaan Power Grad. Electracaty Anformataon Sharang and Analysas Center (E-ASAC), 2016.

7. Feng C, La T, Chana D. Multa-level anomaly detectaon an andustraal control systems vaa package sagnatures and lstm networks. An: 201747th Annual AEEE/AFAP Anternataonal Conference on Dependable Systems and Networks (DSN). AEEE, 2017, pp. 261-72.
8. Garcaa-Teodoro P, Daaz-Verdejo J, Macaá-Fernández G et al. Anomaly-based network antrusaon detectaon: technaques, systems and challenges. Comput Secur 2009; 28:18-28.