Р. В. МЕЩЕРЯКОВ, А. Ю. ИСХАКОВ
ИПУ РАН, Москва
С. Ю. ИСХАКОВ
Промсвязьбанк, Москва

ПРОАКТИВНОЕ ВЫЯВЛЕНИЕ АТАК В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

В докладе рассматривается подход к применению проактивных алгоритмов выявления атак на киберфизические системы, основанный на анализе динамически обновляемых индикаторов компрометации. Приводится обзор современных исследований, посвященных моделям угроз и выявлению аномалий в различных автоматизированных системах. Рассматривается возможность применения индикаторов компрометации и предлагается подход к их использованию в киберфизических системах.

Введение. Отсутствие общих точек между исследованиями в области методов аутентификации и проактивного поиска угроз формирует проблему расширения модельно-методологического аппарата методов адаптивной аутентификации за счет применения алгоритмов выявления ранее неизвестных атак. Политики безопасности, основанные на статических правилах однофакторных и многофакторных алгоритмов проверки, не только приводят к строгим ограничениям, затрудняющим оперативное управление киберфизическими системами, но и отличаются использованием ряда характеристик для аутентификации субъекта доступа, которые могут быть скомпрометированы стороной злоумышленника.

Проактивный поиск угроз. Одним из наиболее актуальных направлений защиты киберфизических систем является безопасность конечных ее узлов, в том числе выявление злоумышленников не только по сигнатурному анализу, но и по аномальному использованию легитимных инструментов и управляющих команд. Цель подобного процесса – обнаружение ранее неизвестных атак, которые не могут быть выявлены традиционными средствами защиты, в т.ч. антивирусным программным обеспечением. Такой подход называется проактивным поиском угроз (threat hunting). Он позволяет выявлять новые угрозы и предотвращать сложные таргетированные атаки. Основа подхода заключается в поиске и анализе индикаторов компрометации как с применением ручных методов, так и с помощью машинного обучения.

Проактивный поиск угроз является непрерывным процессом, продолжающимся на протяжении всего жизненного цикла системы, поскольку атака на систему может произойти в любой момент. Подход основан на регулярном формировании гипотез о компрометации той или иной части системы и их проверки. В случае подтверждения гипотезы необходимо принять меры по реагированию, а полученную информацию преобразовать в индикаторы и использовать в дальнейшем процессе. Накопление подобной экспертизы и обмен индикаторами компрометации составляет основу проактивного подхода и может быть использован для расширения существующих методов аутентификации и выявления ранее неизвестных атак. На сегодняшний день отсутствует прямая взаимосвязь исследований в этих отраслях знания, что, несомненно, является одним из стоп-факторов развития научно-методологического аппарата.

Научный обзор. В исследовании [1] предложен вариант решения проблемы выявления злоумышленников на основе поведенческих характеристик, создания паттерна (иначе – профиля) субъекта доступа, сбора и анализа набора его цифровых отпечатков. Авторами предлагается суммирование вероятностей рисков нарушения нормального функционирования пользователя в системе по ряду факторов, позволяющее обнаружить аномальную активность и выявить злоумышленника. Выдвинутое предположение о рассмотрении различных индикаторов риска и их пересечения как единый блок позволяет значительно повысить точность и своевременность обнаружения злоумышленника.

В работе [2] предлагается использовать подход на основе теории графов. Авторы описывают некоторый фреймворк, где характеристики поведения пользователя являются многомерными объектами – узлами взвешенного неориентированного двумерного графа. В качестве вершин такого графа предлагается использовать элементы множеств всех субъектов доступа и всех устройств системы. Ребра предлагаемого авторами графа описывают взаимодействие

пользователей с устройствами. При этом граф формируется на основе исходных гетерогенных данных, полученных из различных источников, таких как журналы безопасности, сервисные журналы, электронная почта, отметки пользователей в служебных подсистемах, записи протоколов и пр.

В статье [3] показано формализованное представление подхода для аудита и внутренних угроз информационной системы. Авторами предлагается использовать метод вероятностного моделирования, а также поэтапной обработки и объединения результатов. На подготовительном уровне подход подразумевает фиксацию возможных нелегетимных намерений злоумышленного пользователя, далее рассчитывается вероятность нарушения информационной безопасности за счет реализации данной угрозы. Таким образом, действие пользователей раскладывается на составные части: намерение и риск информационной безопасности, а далее – эта пара оценивается по степени риска для системы.

Задача оценки рисков информационной безопасности в специфических системах с наличием ярко выраженной периодичности в задачах была рассмотрена в работе [4]. Примерами таких систем часто являются системы государственного значения, киберфизические системы, отвечающие за выполнение критически важных операций в определенные интервалы времени. Авторы в данном случае рассмотрели особенности таких систем и учли их для формирования подхода к обнаружению угроз. Предлагаемая ими модель оптимизирована для интервальных задач и оценивает действия пользователя в комбинации с точки зрения заданных инструкций.

В работе [5] авторами предлагается метод обнаружения угроз информационной безопасности, на основе применения контролируемых и неконтролируемых алгоритмов обучения. Предлагается анализировать общедоступные датасеты и обучать систему для дальнейшей классификации событий в системе на основе применения методов машинного обучения. Необходимо отметить, что данный подход, несмотря на использование современных алгоритмов, крайне неустойчив к восприятию новых угроз. Приведенные в работе результаты вычислительных расчетов показывают различия различных алгоритмов – часть алгоритмов лучше справляется с поставленной задачей, что может означать положительную перспективу данного подхода в целом, при этом оценивается возможность визуализации данных при применении данных программных инструментов анализа.

В качестве продолжения направления использования машинного обучения в задачах обнаружения атак информационной безопасности авторы работы [6] исследовали применение неконтролируемой системы машинного обучения в информационной системе. Из-за того, что решаемая задача относится к слабоформализуемым, подбор характеристик классификации не всегда можно оценить как успешный. Результат исследования показал высокие значения для ложно отрицательных и ложно положительных срабатываний.

Работа по имитационному моделированию злоумышленных действий субъектов доступа приведена в работе [7]. Авторами разработан подход на основе формирования виртуальных действий пользователя с дальнейшим распознаванием системой их намерений и формированием реакции. Имитация происходит на основе зафиксированных реальных действий с использованием специального алгоритма. При этом исследователи делают акцент на том, что функционирование таких виртуальных пользователей внутри сети может не нарушать нормальной работы, но, тем не менее, должно быть зафиксировано службами мониторинга и анализа угроз.

Комплексный подход на основе применения множества описанных выше инструментов предлагается в [8]. В данном случае авторы учитывают как положительные, так и негативные факторы применения каждого из подходов и предлагают объединить их и ранжировать по результаты по специальной комплексной оценке, зависящей, в том числе, от особенностей системы. Уточняется, что предполагается более точная настройка конфигурации в случае внедрения такого подхода, учитывающая индивидуальные показатели защищаемой структуры, однако также делается предположение о том, что это может повысить уровень защищенности.

Применение индикаторов компрометации. Индикаторы компрометации различаются по ряду свойств: структура и формат данных, источник и способ их получения, значимость в совокупной оценке, степень корреляции со значениями других индикаторов и пр. Например, в исследовании [9] предложена модель, показывающая связь между двумя структурами: множеством индикаторов компрометации и множеством действий по выявлению и

предотвращению действий злоумышленника. Данная модель позволяет судить о последствиях применения тех или иных действий злоумышленника, необходимых индикаторах компрометации, а также о применяемых мерах защиты в каждом случае.

В качестве исследуемого объекта была выбрана действующая георасределенная ИТ-инфраструктура, в состав которой входит также несколько робототехнических комплексов. При подборе источников индикаторов компрометации были использованы платформы свободно распространяемых индикаторов. Для сокращения разрыва между успешными случаями проведения атак и возможностями их обнаружения необходимо не только опираться на различные типы индикаторов компрометации, но и использовать потенциальные источники обогащения данных. В данном случае были использованы журналы событий подсистем аутентификации. На исследуемом объекте был внедрен прототип системы класса SOAR, который позволил объединить индикаторы, выявляя значимость каждого сигнала системы в контексте общей ситуации. В ходе анализа полученных результатов рассмотрена возможность применения индикаторов компрометации и предложен подход к их применению в системах аутентификации.

Заключение. На основании проведенного анализа работ предложен подход к применению методов проактивного поиска угроз в киберфизических системах, посредством анализа динамически обновляемых индикаторов компрометации и их применения в модулях аутентификации, а также формированию новых индикаторов на основе существующих алгоритмов аутентификации. Для разработки алгоритмов корректировки параметров аутентификации по полученным индикаторам предлагается формировать базу знаний тактик и процедур, методы анализа инцидентов, методы ситуационного управления.

Работа проводилась при поддержке гранта РНФ 22-21-00846

ЛИТЕРАТУРА

1. Fagade T., Tryfonas T. Malicious Insider Threat Detection: A Conceptual Model. *Security and Protection of Information*. 2017. P. 31-44.
2. Anagi G.A., Li S., Serdar B. Graph Based Framework for Malicious Insider Threat Detection. *Hawaii International Conference on System Sciences (HICSS)*. 2017.
3. Chen T. A probabilistic analysis framework for malicious insider threats. International Conference on Human Aspects of Information Security, Privacy, and Trust. *Springer*. 2015. P. 178-189.
4. Oh J., Kim T., Lee K. Advanced insider threat detection model to apply periodic work atmosphere. *Transactions on Interactive Intelligent Systems.* 2019. Vol. 13. Iss 3. P. 1722-1737.
5. **Kotenko I., Kuleshov A., Ushakov I.** Aggregation of Elastic Stack instruments for collecting, storing and processing of security information and events. *IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*. 2017. P. 1550-1557.
6. Bishop M. A risk management approach to the “insider threat”. *Springer*. 2010. P. 115-137.
7. Dumitras T., Shou D. Toward a Standard Benchmark for Computer Security Research: the Worldwide Intelligence Network Environment (WINE). *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security.* 2011. P. 89-96.
8. **Ушаков И.А., Котенко И.В.** Модель обнаружения внутренних нарушителей на основе использования технологий больших данных. *Региональная информатика и информационная безопасность*. 2017. С. 253-254.
9. Al-Mohannadi H., Awan I., Hamar J., Cullen A., Disso J., Armitage L. Cyber Threat Intelligence from Honeypot Data Using Elasticsearch. *IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. 2018, P. 900-906.

R.V.Meshcheryakov, A.Y.Iskhakov (ICS RAS, Moscow), S.Y.Iskhakov (Promsvyazbank, Moscow)

Threat hunting in cyber-physical systems

The report discusses an approach to the use of proactive algorithms for detecting attacks on cyber-physical systems, based on the analysis of dynamically updated indicators of compromise. An overview of modern research on threat models and anomaly detection in various automated systems is given. The possibility of using indicators of compromise is considered and an approach to the use of such indicators is proposed.