УДК 004.733

ПРИМЕНЕНИЕ ПРИНЦИПОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧ ДЕТЕКТИРОВАНИЯ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ В КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУРАХ

Десницкий В.А.
Федеральное государственное бюджетное учреждение науки
«Санкт-Петербургский Федеральный исследовательский центр
Российской академии наук», Россия, г. Санкт-Петербург

Аннотация. *В данной работе проводится исследование процессов детектирования атакующих воздействий в информационно-телекоммуникационных системах критически важных инфраструктур. Детектирование осуществляется с применением принципов и модельно-методического аппаратам имитационного моделирования на базе графов и деревьев атак, сетей Петри, Байесовский моделей, скрытых Марковских моделей и др. Для проверки качества детектирования используются наборы исходных данных, размеченных под конкретные виды атак. В качестве базовых показателей вычисляются показатели точности, полноты и f1-меры, а также их взвешенные значения с учетом пропорций мощности каждого детектируемого класса атак в исходной выборке.*
Ключевые слова: *информационная безопасность, моделирование, атакующее воздействие, детектирование, критически важные инфраструктуры.*

APPLICATION OF SIMULATION PRINCIPLES TO SOLVE PROBLEMS OF DETECTING ATTACKS IN CRITICAL INFRASTRUCTURES

Desnitsky V.A.
St. Petersburg Federal Research Center
of the Russian Academy of Sciences, Russia, St. Petersburg

Abstract. *In the paper we study the processes of detecting attacking influences in information and telecommunication systems of critical infrastructures. Detection is performed by using principles and model-methodological apparatus of simulation modeling based on graphs, attack trees, Petri nets, Bayesian models, hidden Markov models, etc. To check the quality of the detection, sets of initial data are used. The datasets are labeled for a number of specific types of attacks. As basic indicators, the indicators of accuracy, completeness and f1-measures are calculated, as well as their weighted values, taking into account the proportions of the volume of each detected class of attacks in the original samples.*

Key words: *information security, modeling, attack impact, detection, critical infrastructures.*

В настоящее время все большее значение приобретают вопросы обеспечения информационной безопасности критически важных инфраструктур, включающие системы мониторинга параметров окружающей среды, производственные системы и беспроводные сенсорные сети, разнообразные транспортные и логистические системы, имплантируемые и носимые модули диагностики состояния живых организмов и др.

В результате масштабирования и повсеместного распространения и внедрения таких систем на практике, а также их интеграции с существующими, в том числе с т.н. legacy-системами [1], возникают повышенные риски появления и успешной эксплуатации нарушителями различного вида уязвимостей программно-аппаратного обеспечения в таких системах. Одним из путей повышения защищенности подобных систем является внедрения различных механизмов защиты, включающих средства детектирования, в которые заложены знания и принципы имитационного моделирования [2, 3].

Детектирование атак на основе имитационного моделирования, во-первых, включает анализ предметной области критически важной инфраструктуры, особенностей ее устройств, связей между ними, телекоммуникационной инфраструктуры и первичных данных, которые будут поступать на вход механизма детектирования атак в качестве исходных данных. Во-вторых, необходим предваряющий анализ ожидаемых разновидностей атакующих воздействий и их критичности в контексте целей и рисков целевой инфраструктуры [4, 5]. В-третьих, необходимы подбор конкретных видов имитационных моделей и/или наличие механизмов автоматизации выбора и поддержки принятия решений по выбору имитационных моделей, адекватных целям и условиям атакующих воздействий.

В-четвертых, для каждого вида атаки, которую необходимо детектировать, производится программная реализация математического аппарата для его динамического воспроизведения в процессе функционирования [6]. В частности, в рамках механизма детектирования при поступлении определенных событий графовая модель защищаемого устройства переходит в те или иные состояния. Достижение определенного конечного состояния позволяет сигнализировать о нахождении устройства в состоянии «под атакой».

В-пятых, данные об обнаруженных инцидентах безопасности от различных подмодулей системы детектирования – для различных устройств и различных видов атак объединяются в рамках интеграционного модуля и выдаются вовне – оператору всей инфраструктуры или специалистам по безопасности [7].

Этим обеспечивается многоаспектность процесса выявления атак и, в частности, детектирование многошаговых атакующих воздействий [8], требующих вовлечение большого числа устройств в процесс обнаружения атаки с множественными точками воздействия.

Перечислим основные принципы, используемые в процессе моделирования: учет перечня актуальных видов атак, учет особенностей критической инфраструктуры, учет показателей оперативности детектирования, поддержка обработки данных в режиме близком к режиму реального времени с использованием потоковой обработки данных, достижимость требований на качество детектирования с использованием показателей точности, полноты, f1-меры и их взвешенных вариантов. Кроме того к важнейшим факторам успешного детектирования атак можно отнести также масштабируемость механизма выявления атак, высокую степень автоматизации детектирования, а также валидацию работы механизма и его тестирование на конкретных наборах данных.

Библиографический список

1. Das R., Gündüz M. Analysis of cyber-attacks in IoT-based critical infrastructures // International Journal of Information Security. – 2019. – №. 8. – P. 122-133.
2. Jasiul B., Szpyrka M., Śliwa J. Detection and modeling of cyber attacks with petri nets // Entropy. – 2014. – Vol. 16. – №. 12. – P. 6602-6623.
3. Orojloo H., Azgomi M. A. Modelling and evaluation of the security of cyber-physical systems using stochastic Petri nets // IET Cyber-Physical Systems: Theory & Applications. – 2019. – Vol. 4. – №. 1. – P. 50-57.
4. Ghafir I., Saleem J., M. Hammoudeh, H. Faour, Přenosil V., Jaf S. F., Jabbar S., Baker T. Security threats to critical infrastructure: the human factor // The Journal of Supercomputing. – 2018. – Vol. 74. – P. 4986-5002.
5. Lewis T. G., R. P. Darken, Mackin T., Dudenhoeffer D. Model-based risk analysis for critical infrastructures // WIT Transactions on State of the Art in Science and Engineering. – 2012. – Vol. 54. – P. 1-19.
6. Shameli-Sendi A., Dagenais M., Wang L. Realtime intrusion risk assessment model based on attack and service dependency graphs // Computer communications. – 2018. – Vol. 116. – P. 253-272.
7. Desnitsky V. IoTaaS based Approach to Design of a WSN for Secure Smart City Monitoring // Proceedings of 2021 IEEE International Russian Automation Conference (RusAutoCon 2021). – IEEE Xplore. – 2021. – P. 443-447.
8. Holgado P., Villagrá V. A., Vazquez L. Real-time multistep attack prediction based on hidden markov models // IEEE Transactions on Dependable and Secure Computing. – 2017. – Vol. 17. – №. 1. – P. 134-147.