УДК 004

Д. И. Кадочников[1]✉

Исследование свойств сетей Петри для анализа архитектуры программного обеспечения в контексте информационной безопасности

[1]Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: d-kad@mail.ru

Аннотация. В данной работе исследуются базовые свойства сетей Петри и свойства модифицированных сетей Петри, которые могут быть использованы для анализа информационной безопасности архитектуры программного обеспечения. В рамках данного исследования проверяется гипотеза о высокой предрасположенности моделей сетей Петри к описанию и математическому доказательству аспектов информационной безопасности на этапе построения архитектуры системы. В ходе работы определены свойства сетей Петри, удовлетворяющие поставленной цели, а также формулируются важнейшие модификации математической модели, требующиеся для наиболее тщательного, но не избыточного анализа архитектуры на соответствие требованиям информационной безопасности. Полученные результаты могут быть использованы для разработки собственной агрегатной модификации сетей Петри, направленной на анализ информационной безопасности, и, на ее основе, построения модели программного обеспечения по созданию, управлению и анализу данной модификации.

Ключевые слова: сети Петри, модифицированные сети Петри, свойства сетей Петри, архитектура программного обеспечения, анализ информационной безопасности

D. I. Kadochnikov[1]✉

Exploring the properties of Petri nets for analyzing software architecture in the context of information security

[1]National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: d-kad@mail.ru

Abstract. This paper investigates the basic properties of Petri Nets and properties of modified Petri Nets that can be used to analyze the information security of software architecture. Within the framework of this research the hypothesis of high predisposition of Petri Nets models for description and mathematical proof of information security aspects at the stage of system architecture construction is tested. In the course of the work the properties of Petri Nets satisfying the set goal are determined and the most important modifications of the mathematical model required for the most thorough, but not redundant analysis of the architecture for compliance with information security requirements are formulated. The obtained results can be used for development of own aggregate modification of Petri Nets, aimed at analysis of information security, and, on its basis, construction of software model for creation, management and analysis of this modification.

Keywords: Petri nets, modified Petri nets, properties of Petri nets, software architecture, information security analysis

Введение

С середины прошлого века сложность и запутанность разрабатываемого программного обеспечения неуклонно растет. За это время программы ЭВМ прошли путь от простых вычислительных моделей до систем, агрегирующих большое количество функций и свойств. Данное развитие принесло новую проблему: непрозрачность изучения свойств разрабатываемых систем, что в свою очередь приводит к увеличению количества угроз информационной безопасности.

Увеличить прозрачность работы системы помогает правильная техническая документация по разрабатываемому проекту, при этом ее основой является архитектура будущего программного обеспечения, отвечающая на важнейшие вопросы: как каждый элемент системы выполняет свою работу и что ему нужно для корректной работы.

Кроме того, важным аспектом правильного проектирования системы является обнаружение уязвимостей в будущем программном продукте до его непосредственной разработки. Так, по данным IBM System Science Institute исправление дефекта на этапе эксплуатации может стоить в 100 раз дороже, чем на этапе проектирования [1].

Вследствие вышеизложенных обстоятельств, появляется потребность в формальных методах анализа архитектур программного обеспечения, позволяющих систематически выявлять будущие уязвимости, оценивать корректность разрабатываемых механизмов и моделировать поведение систем в условиях атак.

Современные научные исследования описывают разные методы решения данных задач. Например, группа ученых Nacha Chondamrongkul, Jing Sun и Ian Warren в 2021 году представила фреймворк для описания и проектирования архитектуры программного обеспечения [2]. В данной работе исследователи обсуждают возможность представления архитектуры программного обеспечения как программного кода и упрощение его анализа на соответствие требованиям информационной безопасности.

Другой архитектурно-ориентированный метод анализа потоков данных представлен группой ученых N. Boltz и S. Hahner, создавших фреймворк анализа потоков данных между элементами системы [3]. Но данный метод не предполагает анализа изменений данных в самих элементах системы и не позволяет моделировать поведение систем в условиях атак.

Подход SecuRe предлагает рекомендации по использованию шаблонов проектирования безопасности для архитекторов программного обеспечения, облегчая интеграцию проверенных решений в архитектуру системы [4]. Но данный подход описывает безопасность архитектуры, не учитывая особенности конкретной разработки в рамках конкретной компании.

Другим более широким и гибким подходом может стать описание и анализ архитектуры разрабатываемого программного обеспечения на основе сетей Петри. Благодаря своей наглядности, масштабируемости и простоте модифицирования данный математический аппарат, изначально разработанный для описания асинхронных процессов, уже сейчас используется в задачах анализа рабочих

процессов и проектирования цифровых систем, но его потенциал не до конца раскрыт в области информационной безопасности. Так, возможности модифицированных сетей для моделирования систем и автоматизация проверки свойств информационной безопасности обсуждаются лишь в нескольких работах.

Например, в области сетевой безопасности команда Симонсона использовала аннотированные цветные сети Петри для автоматизированной генерации и формальной верификации протокольного программного обеспечения [5].

В анализе архитектуры программного обеспечения ученые Ду и Нинг использовали модифицированные логические сети Петри, способные моделировать неопределенность передаваемых значений и параллельные процессы в системе [6]. Также в представленной работе описывался подход по построению полного графа достижимости и его анализа на выполнение таких свойств как безопасность состояний и отсутствие тупиков.

Постановка задачи

Целью данной работы является исследование применимости свойств сетей Петри и их модификаций для формального анализа архитектур программного обеспечения с точки зрения информационной безопасности.

В ходе работы была проведена ее декомпозиция на следующие задачи:

1) сформировать классификацию формальных свойств сетей Петри с выделением структурных, поведенческих, временных и архитектурных аспектов;

2) исследовать, как модифицированные модели (вложенные, иерархические сети Петри) позволяют более точно отразить структуру и поведение компонентов ПО.

В следующих разделах будет представлен обзор ключевых формальных свойств сетей Петри и их сопоставление с задачами анализа ИБ.

Результаты работы

Рассмотрим свойства оригинальных сетей Петри и требования информационной безопасности, которые можно проверить с помощью данных свойств [7, 8].

Достижимостью называется свойство сети Петри, при котором существует такая последовательность срабатываний переходов, которая переводит систему из начальной маркировки в заданную целевую маркировку. Благодаря данному свойству можно проверять, выполнима ли атака при определенных начальных данных. В качестве цели атаки может выступать любое состояние системы от повышения уровня прав доступа до активации определенных команд в командной строке.

Ограниченностью называется свойство сети Петри, при котором в любой достижимой маркировке количество фишек в заданном месте не превышает определенного значения. Данное свойство тесно связано со свойством безопасности, являющимся частным случаем первого. Данное свойство позволяет проанализировать возможность DOS-атак, а также события, связанные с появлением новых пользователей в системе.

Живостью называется свойство сети Петри, при котором каждый переход может быть активирован при некоторой последовательности срабатываний, начиная с исходной маркировки. В рамках данного свойства возможен анализ доступности определенных частей системы, таких как системы безопасности или системы журналирования.

Обратимостью называется свойство сети Петри, при котором из любой достижимой маркировки существует такая последовательность переходов, которая возвращает сеть в ее начальное состояние. В рамках информационной безопасности данное свойство позволяет выполнить анализ системы на способность восстановления после сбоя всей системы или отказа частей программного обеспечения.

Мертвыми переходами называются такие переходы, которые не могут быть активированы ни при одной достижимой маркировке. Их наличие может сигнализировать о том, что при определенных действиях части системы можно перевести в состояние отказа.

Конфликтностью называется свойство сети Петри, при котором два или более переходов конкурируют за одни и те же фишки и не могут сработать одновременно. Данные события демонстрируют коллизии доступа к определенным элементам системы, что может быть нежелательным состоянием в ряде конфиденциальных систем.

Тупиком называется состояние маркировки сети Петри, при котором ни один переход не может быть активирован, то есть система полностью останавливается. Данный переход является отказом системы, что может быть недопустимо в ряде критически важных программных решений.

Кроме вышеперечисленных свойств, при модификации сетей Петри появляются новые свойства, которые позволяют дополнительно анализировать системы на соответствие требованиям информационной безопасности. Например, модификация «цветные сети Петри» позволяет передавать конкретные данные через переходы, то есть вместо токенов будут передаваться переменные [9].

С помощью другой модификации появляется возможность установки времени, которое потребуется на выполнение каждого перехода, что является необходимым параметром при формулировании нефункциональных требований к доступности системы.

Также вместо токенов можно использовать другие, вложенные сети Петри. Подобная конфигурация позволяет анализировать поведение на разных уровнях – от доступности всей системы до обработки конкретных переменных в ее элементах.

Данные модификации в совокупности позволяют максимально гибко и приближенно к реальному программному коду моделировать систему и ее поведение на различных этапах построения архитектуры, постепенно выстраивая ее от Бизнес-процессов до реализации конкретных механизмов обработки данных. Появляется возможность анализа потоков данных и подробного логирования событий в созданной модели архитектуры. Также практически на уровне программной реализации можно описывать обработку альтернативных сценариев, что, в свою очередь, поз-

волит избежать сложностей, с которыми сталкиваются программисты при работе с неполностью описанной архитектурой системы.

Все эти возможности критически важны для дальнейшей разработки безопасного программного обеспечения, так как любые незадекларированные возможности или нерассмотренные сценарии могут привести к критическим уязвимостям.

Заключение

В настоящей работе были проанализированы свойства классических и модифицированных сетей Петри, с акцентом на их применимость в задачах информационной безопасности программного обеспечения. Показано, что модифицированные сети Петри позволяют учитывать не только структурные, но и семантические аспекты безопасности, такие как контроль доступа, аномальное поведение и способность самовосстановления системы после сбоев.

Анализ данных свойств позволяет формально проверить соответствие проектируемых архитектур требованиям информационной безопасности на ранних этапах жизненного цикла разработки, когда цена изменений минимальна.

Тем не менее, практическое применение требует дальнейшей формализации методов анализа, разработки инструментов визуального и автоматизированного анализа, а также описания политик безопасности в терминах сетей Петри. В перспективе особый интерес представляет разработка гибридных моделей, сочетающих цветные сети Петри с логическими спецификациями, а также применение вложенных сетей для имитации распределенных систем.

Таким образом, модели на основе сетей Петри представляют собой перспективное направление для исследования, верификации и автоматического анализа безопасности проектируемых систем на этапе архитектуры.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Dawson M. et al. Integrating software assurance into the software development life cycle (SDLC) //Journal of Information Systems Technology and Planning. – 2010. – Т. 3. – №. 6. – С. 49-53.

2. Chondamrongkul N., Sun J., Warren I. Formal security analysis for software architecture design: An expressive framework to emerging architectural styles //Science of Computer Programming. – 2021. – Т. 206. – С. 102631.

3. Boltz N. et al. An extensible framework for architecture-based data flow analysis for information security //European Conference on Software Architecture. – Cham : Springer Nature Switzerland, 2023. – С. 342-358.

4. Sabau A. R., Lammers D., Lichter H. SecuRe--An Approach to Recommending Security Design Patterns //arXiv preprint arXiv:2501.14973. – 2025.

5. Simonsen K. I. F., Kristensen L. M., Kindler E. Pragmatics annotated coloured petri nets for protocol software generation and verification //Transactions on Petri Nets and Other Models of Concurrency XI. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2016. – С. 1-27.

6. Du Y., Ning Y. Property analysis of logic Petri nets by marking reachability graphs //Frontiers of Computer Science. – 2014. – Т. 8. – С. 684-692.

7. Murata T. Petri nets: Properties, analysis and applications //Proceedings of the IEEE. – 1989. – Т. 77. – №. 4. – С. 541-580.

8. Wolfgang R. Understanding petri nets-modeling techniques //Analysis Methods, Case Studies. Springer. – 2013.
9. Jensen K. Coloured Petri Nets: Basic concepts, Analysis Methods and Practical Use-Vol. 2, edn //New York, USA. – 1997.