В прошлом году началась проводиться работа над проектами национальной цифровой валюты (central bank digital currency, CBDC). Характеристики цифровой валюты выделены в отчете Банка международных расчетов и включают системные, инструментальные и институциональные составляющие.

1. Системные требования: безопасность, скорость расчетов, устойчивость, доступность, пропускная способность, масштабируемость, совместимость, гибкость и адаптируемость.

2. Инструментальные требования: конвертируемость, удобство, признание и наличие, низкие тарифы.

3. Институциональные составляющие: надежная правовая база, соблюдение стандартов [3, с. 13–14].

Такой подход позволит преобразовать деньги в цифровую форму, и тем самым предоставит ряд возможностей – от эффективности транзакций до программируемости активов. «Индустрия цифровых активов предлагает альтернативу с относительно низким уровнем риска для генерации идей и экспериментов «вживую»» [4]. А как же конфиденциальность во время проведения транзакций? Исследования показали, что взаимодействие банков с ведущими компаниями, занимающимися технологиями распределенного реестра (DLT), используя концепцию Proof of Concept (моделирование работы ПО или эксплойта с целью найти оптимальные пути защиты) успешно провели тестирование, используя «анонимные ваучеры».

Сейчас можно говорить, что стейблкоины (криптовалюта) и CBDC, выпущенные частным образом – являются новыми возможностями в цифровом мире. Они не противоречат друг другу, требуют безопасных и надежных, соответствующих нормативным требованиям, финансовых сетей для поддержки цифровых активов. В перспективе CBDC для розничной торговли будет базироваться на токенизации активов с использованием криптографии с закрытым и открытым ключом, а существующая инфраструктура рынка цифровых активов, как например, кошельки, поставщики криптовалюты, биржи, будет играть уже второстепенную роль на денежном рынке.

Библиографические ссылки

1. Будущее денег в цифровом мире : [Электронный ресурс]. URL: https://econs.online/articles/ekonomika/budushchee-deneg-v-tsifrovom-mire (дата доступа: 01.10.2021).

2. Лобас А. Стратегия современного банка в эпоху цифровых сервисов : [Электронный ресурс]. URL: https://www.finversia.ru/publication/strategiya-sovremennogo-banka-v-epokhu-tsifrovykh-servisov-27091 (дата доступа: 02.10.2021).

3. Новикова И., Криштаносов В. Цифровые валюты центральных банков: современные тенденции и возможности имплементации в Республике Беларусь // Банковский вестник. 2021. № 4 (693). С. 13–20.

4. Глобальный взгляд на цифровые валюты : [Электронный ресурс]. URL: https://www.theblockcrypto.com/post/ (дата доступа: 03.10.2021).

УДК 004.942

ИСПОЛЬЗОВАНИЕ ФОРМАЛЬНЫХ МЕТОДОВ НА РАННИХ ЭТАПАХ ПРОЕКТИРОВАНИЯ КОЛЛАБОРАЦИОННОЙ СИСТЕМЫ ПРОТИВОВИРУСНОЙ ЗАЩИТЫ

Р. Е. Шарыкин[1)], А. Н. Курбацкий[2)] (*научный руководитель*)

[1)] *соискатель, Белорусский государственный университет, Минск, Республика Беларусь, sharykin@gmail.com*

[2)] *доктор технических наук, профессор, Белорусский государственный университет, Минск, Республика Беларусь, kurb@unibel.by*

Предлагается подход, позволяющий исследовать математическую модель системы защиты от вирусов на этапе ее проектирования с помощью статистического анализа исполняемой спецификации модели, основанной на формализме Распределенных Объектно-Ориентированных Стохастических Систем. Важными аспектами модели является ее распределенный и вероятностный характер. Эти аспекты делают модель более сложной для проведения атак, но в то же время значительно усложняют понимание ее свойств разработчиком. На данном примере мы показываем, как используя спецификацию системы как модели Распределенных Объектно-Ориентированных Стохастических Систем, вкупе с ее статистическим анализом, мы можем исследовать ее свойства на раннем этапе проектирования, и как, с помощью данного подхода, мы можем обнаружить «дефекты» модели и исправить их еще в процессе создания модели.

Ключевые слова: математическое моделирование; гибридные системы; стохастические системы; спецификация моделей; групповая антивирусная защита.

THE USE OF FORMAL METHODS AT THE EARLY STAGES OF DESIGNING A COLLABORATIVE ANTIVIRAL PROTECTION SYSTEM

R. E. Sharykin[1], A. N. Kurbatskii[2] (*supervisor*)

[1] *PhD Student, Belarusian State University, Minsk, Republic of Belarus, sharykin@gmail.com*

[2] *Doctor of Technical Sciences Professor, Belarusian State University, Minsk, Republic of Belarus, kurb@unibel.by*

We propose an approach allowing to study a mathematical model of a virus protection system at the stage of its design using statistical analysis of an executable model specification based on the formalism of Distributed Object Based Stochastic Hybrid Systems. Important aspects of the model are its distributed and probabilistic nature. These aspects make the model more difficult to carry out attacks, but at the same time significantly complicate the understanding of its properties by the developer. In this example, we show how, using the specification of the system as a Distributed Object Based Stochastic Hybrid Systems model, coupled with its statistical analysis, we can investigate its properties at an early stage of design and how, using this approach, we can detect «defects» of the model and correct them during the process of creating the model.

Keywords: mathematical modeling; hybrid systems; stochastic systems; model specification; collaborative virus defense

Предлагается подход к применению формальных методов на ранних этапах дизайна системы защиты от вирусов. Подход основывается на использовании формальной модели Распределенных Объектно-Ориентированных Стохастических Гибридных Систем (РООСГС) [1], и подход к ее верификации, изложенный в [2]. Модель РООСГС, в свою очередь, основывается на переписывающей логике [3]. Использование переписывающей логики означает, что система определяется формально с самых ранних этапов проектирования. В то же время, использование переписывающей логики не ограничивает разработчика определенным формализмом. Известно, что многие математические модели, такие как сети Петри, цепи Маркова и многие другие общепринятые модели, могут быть представлены как переписывающие теории [3, 4]. Выполненные в переписывающей логике спецификации могут напрямую выполняться с помощью системы Maude [5], что позволяет экспериментировать с спецификацией системы защиты на ранних этапах разработки системы защиты. Используя данный подход можно получать быстрые оценки основных свойств системы, проверять модель защиты в различных моделях окружения, находить и исправлять недостатки дизайна модели до начала ее строгого математического анализа. После проведения предварительной, основанной на эксперименте «доводки» модели, можно переходить к проведению более сложных формальных процедур валидации на следующих этапах, когда пространство возможностей для дизайна уже сокращено.

Система защиты от вирусных атак, изученная в данной работе подробно описана в [6]. В рассматриваемом алгоритме групповой защиты от вирусных атак, локальные сети сотрудничают, объединяясь в группы, в которых исходящие маршрутизаторы информируют своих групповых партнеров посредством локальных оповещений о возможной вирусной активности. В случае, когда узел получает коллаборационные извещения о возможной вирусной активности от N или более источников, он переходит в защитный фильтрующий режим. Важным аспектом модели является ее вероятностная природа. Для моделирования системы обнаружения вирусов используются вероятности обнаружения вируса и ложноположительного обнаружения вируса. Для моделирования процессов, протекающих в системе, применяется механизм выполнения рекуррентных действий с интервалами между действиями, распределенными в соответствии с экспоненциальным распределением. Вероятностные модели для компонент системы делают модель более реалистичной, но затрудняют ее анализ. Наиболее важным аспектом системы является формирование групп оповещения случайным образом. Фиксированная структура групп в системе [7], которую мы использовали как отправную точку для разработки нашей системы защиты, позволяла провести атаку с полным заражением системы, основываясь на алгоритме формирования групп [8]. В случае вероятностного формирования групп, атаки подобного типа становятся невозможными, так как идея построения атаки критически зависит от способности атакующего предсказать точный состав групп оповещения.

Оценка полученной системы защиты производилась посредством использования сравнительных критериев, разработанные в [9]. Основой для оценочных метрик является кривая распространения вируса. Форма кривой является сигмовидной, с резким ростом вначале и последующим достижением равновесия, и остановкой эпидемии. Визуально, можно выделить три значения, которые характеризуют такой тип кривых: процент зараженных узлов при насыщении, максимальная скорость распространения инфекции и время, за которое система достигает насыщения. Запишем эти метрики по пунктам:

Метрика 1. Процент зараженных хостов по достижению вирусом полного насыщения.

Метрика 2. Максимальная скорость распространения вируса, измеренная как процент узлов, подвергающихся заражению в единичный период времени, на интервале от начала распространения и до насыщения.

Метрика 3. Временная точка, в которой вирус достигает насыщения.

Для спецификации разработанной модели использовался язык спецификации SHYMaude [2], разработанный для спецификации РООСГС. Спецификация SHYMaude, в свою очередь, была транслирована в спецификацию Maude [2], которая, в свою очередь, является выполняемой логической спецификацией в системе Maude [5]. Для анализа системы использовался инструмент MultiVeStA [10], выполняющий статистический анализ, основанный на методе Монте-Карло. Для задания свойств системы, подлежащих анализу, использовался язык MultiQuaTEx, являющийся обобщением языка QuaTEx [11], разработанного для задания темпорально-количественных свойств системы.

В результате статистического анализа изложенной системы стохастической групповой защиты от вирусов были получены доверительные интервалы трех метрик, описанных выше, а также построен усредненный график числа зараженных узлов в зависимости от времени. Усреднение проводилось для каждой временной точки по результатам Монте-Карло симуляции системы до данной временной точки. Более подробно результаты исследования изложены в [6]. Результаты анализа системы позволяют заключить, что при применении данной групповой защиты, в среднем,

пораженной оказывается менее 20 % системы. Это позволяет говорить о том, что на заданных параметрах система статистически устойчива к использованной в работе модели вируса, если под статистической устойчивостью понимать факт того, что определенная существенная часть системы остается незараженной после того, как вирус достиг своего насыщения.

Дополнительно, был проведен анализ существенности равномерного покрытия узлов группами оповещения. Для изучения значения алгоритма выбора групп была изучена модификация алгоритма защиты с «неудачным» покрытием узлов группами, не обеспечивающая равномерного покрытия. Это привело к росту числа зараженных узлов до более 60 %.

Данный результат показывает, что «дефект» системы оказывает существенное влияние на эффективность системы и наглядно демонстрирует, как статистическая верификация помогает высветлять неявные проблемы дизайна систем защиты. Данный «дефект» вполне может быть обнаружен на этапе проектирования системы и доработка может была произведена на этапе проектирования системы, до ее последующего аналитического исследования, что иллюстрирует преимущество излагаемого подхода к проектированию подобных систем.

Библиографические ссылки

1. Шарыкин Р. Е., Курбацкий А. Н. Модель распределенных объектно-ориентированных стохастических гибридных систем // Журнал Белорусского государственного университета. Математика. Информатика. 2019. № 2. С. 52–61.

2. Шарыкин Р. Е., Курбацкий А. Н. Верификация Распределенных Объектно-Ориентированных Стохастических Гибридных Систем // Вестник Гродненского Государственного Университета имени Янки Купалы. Серия 2. Математика. Физика. Информатика, вычислительная техника и управление. 2019. Том 9. № 2. С. 123–133.

3. Meseguer J. Conditional rewriting logic as a unified model of concurrency // Theoretical Computer Science. 1992. Vol. 96. Issue 1. P. 73–155.

4. Martí-Oliet N., Meseguer J. Rewriting logic: roadmap and bibliography // Theoretical Computer Science. 2002. Vol. 285. Issue 2. P. 121–154.

5. Clavel M. Maude: Specification and programming in rewriting logic / M. Clavel [et al.] // Theoretical Computer Science. 2002. Vol. 285. Issue 2. P. 187–243.

6. Шарыкин Р. Е., Курбацкий А. Н. Применение Формальных Методов при Проектировании Коллаборационной Системы Противовирусной Защиты // Журнал Белорусского государственного университета. Математика. Информатика. 2020. № 1. С. 59–69.

7. Briesmeister L., Porras P. Microscopic simulation of a group defense strategy // Proceedings: Workshop of Principles of Advanced and Distributed Simulation, Monterey, California, US, June 1–3, 2005 / eds: D. Nicol [et al]. Los Alamitos, California, US : IEEE Computer Society, 2005. P. 254–261.

8. Briesmeister L., Porras P. Automatically deducing propagation sequences that circumvent a collaborative worm defense // Proceedings: International Performance Computing and Communications Conference, Phoenix, Arizona, US, April 10–12, 2006 / eds: H. Hassanein [et al]. Los Alamitos, California, US : IEEE Computer Society, 2006. P. 587–592.

9. Briesmeister L., Porras P. Formally specifying design goals of worm defense strategies // Proceedings of the 2006 ACM Symposium on Information, computer and communications security, Taipei, Taiwan, March 31–24, 2006 / eds: L. Ferng-Ching [et al]. New York, US : Association for Computing Machinery, 2006. P. 125–137.

10. Sebastio S., Vandin A. MultiVeStA: Statistical model checking for discrete event simulators // Proceedings of the 7th International Conference on Performance Evaluation Methodologies and Tools, Torino, Italy, December 10–12, 2013 / eds.: A. Horvath [et al]. Brussels, Belgium : Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2013. P. 310–315.

11. Sen K., Viswanathan M., Agha G. On statistical model checking of stochastic systems // Lecture Notes in Computer Science. 2005. Vol. 3576. P. 266–280.