УДК 004.056
DOI: 10.52190/2073-2600_2021_3_8

Применение TLA+ нотации для описания модели изолированной программной среды субъектов доступа и ее дальнейшей верификации

А. М. Каннер
ЗАО "ОКБ САПР", Москва, Россия

Рассматриваются недостатки верификации математических нотаций моделей безопасности. Предлагается использование темпоральной логики действий Лэмпорта для представления моделей безопасности на формальном языке, пригодном для верификации с применением инструментальных средств. Рассматривается модель изолированной программной среды субъектов доступа, приводится ее спецификация в TLA+ нотации, описываются достоинства верификации данной спецификации с использованием инструментальных средств.

Ключевые слова: модель ИПСС, спецификация модели ИПСС, верификация модели ИПСС, темпоральная логика действий Лэмпорта, TLA+, метод Model Checking.

Все более актуальной становится необходимость проведения моделирования и верификации разрабатываемых средств защиты информации (СЗИ). Это связано в том числе с требованиями, предъявляемыми в ряде нормативных документов Российской Федерации к верификации функций защиты СЗИ [1, 2]. Для верификации средств защиты информации используют специальные инструментальные средства, которые позволяют проверить выполнение некоторых формальных свойств при работе данных СЗИ в автоматическом режиме. При этом такие инструментальные средства позволяют проверять в автоматическом режиме не только средства защиты информации, но и математические модели безопасности компьютерных систем.

Существующие наиболее известные формальные модели безопасности, например Белла—ЛаПадулы, сформулированы в математической нотации, с использованием некоторого математического аппарата. При этом основным компонентом таких формальных моделей является базовая теорема безопасности, с помощью которой обосновывают формальные свойства, гарантирующие безопасность системы или обрабатываемых в ней данных. Для модели Белла—ЛаПадула формальным свойством, гарантирующим безопасность данных, является невозможность возникновения информационных потоков "сверху вниз" — утечки информации с большего уровня конфиденциальности на меньший.

Необходимо отметить, что любая формальная модель в математической нотации имеет достаточно сложное описание, ошибки в базовой теореме безопасности или в самой нотации может выявить только квалифицированный специалист-математик, поэтому при проверке математической нотации всегда необходимо учитывать человеческий фактор. Однако даже после верификации модели в ней могут существовать скрытые пропущенные недостатки. При этом проверка моделей безопасности на наличие ошибок является важной задачей, так как такие модели используют в качестве фундамента для теоретической гарантии некоторых свойств безопасности в компьютерных системах.

В связи с этим для проверки формальных моделей безопасности предложено использовать инструментальные средства автоматической верификации, а математическую нотацию перевести в нотацию на некотором формальном языке, пригодном для верификации, например TLA+ (Temporal Logic of Actions). На основании данной нотации можно сформулировать условия базовой теоремы безопасности в виде инвариантов или темпоральных свойств.

Использование инструментальных средств автоматической верификации позволяет исключить человеческий фактор при проверке модели безопасности и проводить верификацию силами менее квалифицированных специалистов, осуществляющих только запуск средств верификации. Помимо этого такая верификация позволяет проверять выполнение условий базовой теоремы без-

Каннер Андрей Михайлович, программист группы программирования ПО для СЗИ отдела программирования СЗИ.
E-mail: kanner@okbsapr.ru

Статья поступила в редакцию 1 июля 2021 г.

опасности во всевозможных состояниях моделируемой системы и выявлять скрытые ошибки в математической нотации.

Материалы и методы

В работе автора [3] приведено описание математической нотации модели изолированной программной среды субъектов доступа (ИПСС), которая является развитием субъектно-ориентированной модели изолированной программной среды (ИПС) [4, 5]. В модели ИПСС в отличие от ИПС предлагается другое представление сущностей системы:

- субъекты — это пользователи и системные сервисы, а не процессы пользователей, как в ИПС;
- объекты — функционально ассоциированные с субъектами объекты (процессы) и объекты-данные с возможностью динамического изменения их состава во времени.

При этом модель ИПСС имеет следующие основные отличия от модели ИПС:

- осуществляется учет подсистемы защиты в качестве сущности системы, такой же, как и другие субъекты системы;
- приводится обоснование невозможности нарушения действующих правил управления доступом за счет свойства абсолютной корректности (изолированности) субъектов доступа.

Как уже было сказано, математическая нотация модели не позволяет гарантировать выполнения формальных свойств безопасности во всех возможных состояниях системы, а экспериментальные исследования реализаций этой модели на практике требуют повторного проведения даже при малых усовершенствованиях модели. В связи с этим авторами работы [6] проведена верификация модели ИПСС с использованием темпоральной логики действий Лэмпорта и метода Model Checking.

Спецификация модели ИПСС в TLA+ имеет следующие компоненты:

- начальное состояние — инициализация системы (Init), предикат инициализации модели ИПСС;
- переменные модели — сущности, которые могут изменяться в процессе работы (субъекты, объекты и т. д.);
- правила работы системы — возможные состояния и значения переменных модели, правила перехода из состояния в состояние, например при осуществлении доступов субъектов к объектам;
- теорема, доказываемая при верификации и проверяющая специальные предикаты (формальные свойства системы) — инварианты и темпоральные свойства.

В качестве действий в системе могут совершаться запросы модели ИПСС: создание и удаление процессов, создание пользователей и системных субъектов, удаление субъектов, а также чтение, запись, создание, удаление и исполнение объектов доступа. Предусловиями являются предикаты, выполнение которых необходимо для совершения действия. Постусловия определяют, каким образом после выполнения действия изменяются переменные модели, т. е. какое новое состояние будет иметь система.

При доказательстве теоремы в ходе верификации проверяется истинность специальных предикатов — следующих инвариантов или темпоральных свойств:

Invariants and Temporal Properties

Теорема, учитывающая инварианты и свойства: доказывается при верификации

THEOREM $Spec \Rightarrow \wedge \Box\, TypeInv$
$\wedge \Box\, ConsistencyInv$
$\wedge \Box\, BlockedInv$
$\wedge \Box\, OSKernelExists$
$\wedge \Box\, SormInits$
$\wedge \Box\, Correctness$
$\wedge \Box\, AbsCorrectnessOpp$
$\wedge\, OSUsabilityLiveness$
$\wedge\, AbsCorrectness$

Инварианты должны выполняться во всех состояниях и для каждой реализации системы. Также инварианты могут проверять условия в прошлом (например, при последнем переходе системы), используя при этом последовательности совершенных запросов к системе. В отличие от инвариантов, темпоральные свойства могут применять специальные темпоральные операторы TLA+ [6, 7]. С помощью этих операторов можно составлять предикаты, зависящие от времени выполнения и определенных событий в прошлом или будущем.

При создании TLA+ нотации модели ИПСС были выявлены скрытые ошибки математической нотации:

- нарушаются инварианты свойств корректности модели ИПСС и один субъект может опосредованно воздействовать на другой субъект доступа через операции порождения;
- существует возможность некорректной работы моделируемой системы, которая проходит этап инициализации, принимает несколько состояний и в одном из таких состояний система пере-

стает работать еще до появления пользователей из-за завершения работы единственного системного процесса — ядра ОС;

- существует возможность работы системы при завершении работы субъекта, разграничивающего доступ, или при удалении объекта, содержащего применяемые правила доступа.

Данные ошибки исправлены в TLA+ нотации. Для этого выполнена модификация свойств корректности и некоторых операций модели ИПСС, а также добавлены следующие инварианты:

OSKernelExists
В любой момент времени существует *s_0*
OSKernelExists $\triangleq$
$\wedge$ *s_0* $\in$ *S_active*
$\wedge$ *s_0.is_blocked* = FALSE

SormInits
В начальный момент времени инициализирован *s_sorm* либо функционирует только *s_0*
SormInits $\triangleq$
$\wedge$ $\vee$ $\wedge$ *s_sorm* $\in$ *S_active*
$\wedge$ *s_sorm.is_blocked* = FALSE
$\vee$ $\wedge$ *s_sorm* $\notin$ *S_active*
$\wedge$ *S_active* = {*s_0*}

OSUsabilityLiveness
Свойство возможности использования ОС
OSUsabilityLiveness $\triangleq$
хотя бы в одном состоянии есть субъекты, кроме
s_0 и *s_sorm*: пользователь или системный субъект
$\Diamond$ (*Cardinality*(*S_active*) > 2)

где OSKernelExists — инвариант для контроля работоспособности системы (постоянное наличие системного субъекта — ядра ОС);
SormInits — инвариант для контроля активизации подсистемы управления доступом;
OSUsabilityLiveness — темпоральное свойство для проверки работоспособности системы: в любой реализации системы обязательно, кроме начальных системных субъектов, должен активизироваться пользователь или еще один системный субъект.

Заключение

В результате проведенной верификации формальной модели ИПСС показано, что при верификации моделей безопасности компьютерных систем с использованием классической математической нотации возникает ряд существенных недостатков и целесообразно использовать нотацию именно на пригодных для верификации формальных языках. При этом верификацию следует проводить с использованием специальных инструментальных средств автоматической верификации, а при необходимости транслировать с их помощью описание модели с формального языка в математическую нотацию. Также необходимо отметить, что средства автоматической верификации рекомендуется использовать при написании новых моделей безопасности, так как логические ошибки можно устранять уже на раннем этапе, постепенно добавляя требуемые инварианты безопасности по мере описания основных операций модели.

Полный текст разработанной спецификации модели ИПСС доступен на сайте автора https://github.com/kanner/ipes-model

Литература

1. *Каннер А. М.* Подход к верификации подсистемы управления доступом операционной системы Linux: мат. XXV Научно-практ. конф. "Комплексная защита информации" 15—17 сентября 2020 г. — М.: Медиа Группа "Авангард", 2020. С. 24—28.
2. *Каннер А. М., Каннер Т. М.* Моделирование и верификация подсистемы управления доступом средства защиты информации Аккорд-Х // Вопросы защиты информации. 2020. № 3. С. 6—10.
3. *Kanner A. M.* Correctness of Data Security Tools for Protection against Unauthorized Access and their Interaction in GNU/Linux // Global J. Pure and Applied Mathematics. 2016. V. 12. № 3. P. 2479—2501.
4. *Щербаков А. Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с.
5. *Щербаков А. Ю.* Хрестоматия специалиста по современной информационной безопасности. Т. 1. — Saarbrucken: Palmarium Academic Publishing, 2016. — 272 с.
6. *Kanner A. M., Kanner T. M.* Verification of a Model of the Isolated Program Environment of Subjects Using the Lamport's Temporal Logic of Actions: Proceedings of the VII International Conference "Engineering & Telecommunication", IEEE. 2020.
7. *Kanner A. M., Kanner T. M.* Special Features of TLA+ Temporal Logic of Actions for Verifying Access Control Policies: Proceedings of Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, IEEE. 2021 (статья принята к публикации).

Application of TLA+ notation for describing the model of isolated program environment of subjects and it's further verification

A. M. Kanner
JSC "OKB SAPR", Moscow, Russia

The article considers the disadvantages of verification of mathematical notations of the security models. It is proposed to use the Lamport's temporal logic of actions to represent the security models in a formal language suitable for verification which will be held using specialized tools. The model of isolated program environment of subjects is considered, it's specification is given in TLA+ notation, and the advantages of verifying this specification using specialized tools are described.

Keywords: IPES model, IPES model specification, IPES model verification, Lamport's temporal logic of actions, TLA+, Model Checking method.

Bibliography — 7 references. *Received July 1, 2021*