О проблеме представления формальной модели политики безопасности операционных систем

П.Н. Девянин <peter_devyanin@hotmail.com>
Федеральное учебно-методическое объединение высших учебных заведений России по образованию в области информационной безопасности, г. Москва

Аннотация. В связи с начавшимся процессом внедрения ФСТЭК России «Требований безопасности информации к операционным системам» в работе анализируются пути выполнения требований функциональной компоненты ADV_SPM.1 «Формальная модель политики безопасности», в том числе по определению языка, глубины и детализации представления модели политики безопасности управления доступом и информационными потоками. При этом приводятся предложения по составу основных элементов модели, использованию для ее верификации инструментальных средств. Практическая возможность применения предлагаемых подходов рассматривается на примере представления описания и верификации МРОСЛ ДП-модели, как основы механизма управления доступом в ОССН Astra Linux Special Edition.

Ключевые слова: информационная безопасность; политики безопасности; формальные модели

DOI: 10.15514/ISPRAS-2017-29(3)-1

Для цитирования: Девянин П.Н. О проблеме представления формальной модели политики безопасности операционных систем. Труды ИСП РАН, том 29, вып. 3, 2017 г., стр 7-16. DOI: 10.15514/ISPRAS-2017-29(3)-1

1. Введение

Хотя моделирование безопасности управления доступом и информационными потоками можно считать первым научным направлением, заложившим фундамент современной теории компьютерной безопасности [1, 2], в рамках которого уже разработаны десятки, если не сотни формальных моделей, а модель Белла-ЛаПадулы [3] более 40 лет назад была применена в качестве основы механизма управления доступом операционной системы (ОС) *Multics*, до сих пор научным сообществом, представителями регуляторов и разработчиков в области информационной безопасности в полной мере не определён ни сам термин «формальная модель политики безопасности», ни тем

более не сформировано чётких критериев наличия представления такой модели при сертификации средств защиты информации.

Эта проблема становится особенно актуальной с учётом начавшегося процесса внедрения ФСТЭК России «Требований безопасности информации к операционным системам» [4], в которых, а также в разработанных на их основе в соответствии с ГОСТ Р ИСО/МЭК 15408 [5] профилях защиты и заданиях по безопасности для некоторых, возможно, высоких классов защиты ОС, как предполагается, будут явно указаны требования функциональной компоненты ADV_SPM.1 «Формальная модель политики безопасности».

В описании функционального компонента ADV_SPM.1 указывается, что формальная модель должна быть изложена в формальном стиле (с использованием, например, математического языка), должно быть определено понятие «безопасность» для объекта оценки (ОО) и должно быть представлено формальное доказательство того, что ОО не может перейти в небезопасное состояние, а также должно быть продемонстрировано соответствие между какой-либо функциональной спецификацией, используемой ОО, и моделью. Кроме того, указывается, что испытательная лаборатория при выполнении соответствующей проверки должна руководствоваться п. 10.7.1 ГОСТ Р ИСО/МЭК 18045 [6]. Однако в нем не даётся содержательных пояснений, как выполнить данную проверку.

Таким образом, можно говорить о наличии проблемы определения языка, применяемых научных подходов для обоснования безопасности, критериев наличия представления формальной модели политики безопасности, обоснования корректной реализации модели непосредственно в программном коде механизма управления доступом при реализации новых требований безопасности информации к ОС, решение которой может потребоваться в самое ближайшее время.

Очевидно, что язык представления модели может быть либо математическим [2], либо формализованным [7]. Тем более, что уже существуют примеры использования таких языков при разработке формальной модели для отечественной защищённой операционной системы специального назначения (ОССН) *Astra Linux Special Edition* [8]. На математическом языке изложена мандатная сущностно-ролевая ДП-модель (МРОСЛ ДП-модели) [9], на формализованный язык (нотацию) *Event-B* (*Rodin Platform*) эта же модель не только переведена, но и верифицирована [10, 11].

Однако самым существенным вопросом, требующим ответа, по-видимому, здесь является определение достаточной «глубины» проработки формальной модели. Можно ли считать удовлетворительным, например, следующее «математическое» представление механизма управления доступом ОС в рамках модели в виде кортежа (V, T), где V – множество состояний системы, как-то задающее доступы (текущие доступы или права доступа) субъектов из множества S к объектам из множества O, а T – какая-то функция переходов системы из состояния в состояние, без какой-либо детализации?

Или довольно популярной среди разработчиков отечественных защищённых ОС до сих пор является модель Белла-ЛаПадулы. Можно ли признать её адекватной современным ОС и достаточной для представления в профиле защиты, например, механизма мандатного управления доступом, реализуемого в защищённых ОС, принадлежащих семейству *Linux*? При том, что в этой модели не содержится средств описания информационных потоков по времени, иерархии сущностей (адекватной файловым системам ОС), функционально ассоциированных с субъектами сущностей, мандатного контроля целостности, различий в условиях функционирования доверенных и недоверенных субъектов и др. Ответ, очевидно, отрицательный.

2. Требования к представлению формальной модели политики безопасности управления доступом

В связи с изложенным для удовлетворение требованиям компоненты ADV_SPM.1, обеспечения должной «глубины» и детализации целесообразно предложить следующие требования к представлению формальной модели политики безопасности управления доступом, которое должно включать описание на математическом и формализованном языке:

- Множеств учётных записей пользователей, субъектов, объектов (сущностей), устанавливающих классификацию элементов этих множеств, связи между этими множествами или внутри них функций (отношений), заданных на этих множествах отношений иерархии;
- Множеств реализуемых прав доступа и доступов субъектов к сущностям, используемых для задания прав доступа и доступов (непосредственно, с использованием групп, ролей, типов, атрибутов) множеств, функций (отношений);
- Решётки уровней целостности (для большинства современных ОС без мандатного контроля целостности трудно достичь необходимого уровня защищенности), используемых для задания уровней целостности учётных записей пользователей, субъектов, сущностей функций (отношений);
- Решётки уровней конфиденциальности (при необходимости реализации в ОС мандатного управления доступом), используемых для задания уровней доступа учётных записей пользователей и субъектов, уровней конфиденциальности сущностей функций (отношений);
- Множеств, функций (отношений), используемых для задания сущностей, функционально ассоциированных с доверенными субъектами или параметрически ассоциированных с учётными записями пользователей;
- Множеств, функций (отношений), используемых для задания сущностей-контейнеров, доступ к содержащимся в которых сущностях

субъектами может быть разрешён без учёта уровней целостности или без учёта уровней конфиденциальности (при необходимости) таких сущностей-контейнеров;

- Видов информационных потоков (как минимум по памяти), используемых для задания информационных потоков между сущностями и субъектами множеств, функций (отношений);
- Элементов состояний, моделирующей ОС абстрактной системы, используемых для этого множеств, функций (отношений);
- Условий предоставления субъектам прав доступа и доступов к сущностям или субъектам и условий выполнения иных правил преобразования состояний (команд, операций, функций перехода) над учётными записями пользователей, субъектами и сущностями (создание, удаление, переименование, получение параметров), заданных для этого специальных элементов ОС (привилегией, ролей, административных ролей);
- Условий возникновения информационных потоков, за счёт реализации субъектами доступов к сущностям или субъектами, или получения субъектами контроля над другими субъектами;
- Условий получения субъектами контроля над другими субъектами за счёт использования сущностей, функционально ассоциированными с субъектами или параметрически ассоциированными с учётными записями пользователей, и информационных потоков между ними;
- Правил преобразования состояний (команд, операций, функций перехода), моделирующей ОС абстрактной системы, включая параметры каждого правила, условия и результаты его применения. Как минимум должны быть описаны: правила администрирования (создания, удаления, переименования, изменения прав доступа, уровней целостности, доступа или конфиденциальности (при необходимости), получения параметров) учётных записей пользователей, субъектов и сущностей; правила предоставления доступов субъектов к сущностям и субъектам; правила создания информационных потоков и получения субъектами контроля над другими субъектами;
- Доказательства выполнения при применении (корректности задания) правил преобразования состояний (команд, операций, функций перехода), моделирующей ОС абстрактной системы: условий предоставления субъектам прав доступа и доступов к сущностям или субъектам; условий выполнения иных правил преобразования состояний (команд, операций, функций перехода) над учётными записями пользователей, субъектов и сущностей (создание, удаление, переименование, получение параметров);

- Доказательства в рамках моделирующей ОС абстрактной системы того, что реализованный мандатный контроль целостности позволяет обеспечить защиту от несанкционированного изменения субъектом-нарушителем параметров или данных в сущностях, параметров или функциональности субъектов (захватить контроль над субъектом) с более высоким, чем у него уровнем целостности, и в результате нарушить целостность программно-аппаратной среды ОС;
- При необходимости реализации мандатного управления доступом доказательство в рамках моделирующей ОС абстрактной системы того, что реализованные мандатные контроль целостности и управление доступом позволяют обеспечить защиту от запрещённых информационных потоков (как минимум по памяти) от сущностей с более высоким уровнем конфиденциальности к сущностям с более низким уровнем конфиденциальности (защиту от информационных потоков «сверху-вниз»).

Кроме того, с учётом сложности такого представления формальной модели политики безопасности управления доступом целесообразно в соответствии с требованиями компоненты ADV_SPM.1 для формального доказательства того, что ОС не может перейти в небезопасное состояние, а также для демонстрации соответствия между какой-либо функциональной спецификацией, используемой ОС, и моделью требовать её верификации с применением инструментальных средств. Для этого представление модели должно включать описание:

- Основных функциональных возможностей, формализованного языка и порядка применения использованных для верификации модели политики безопасности управления доступом инструментальных средств;
- Представления модели политики безопасности управления доступом с использованием формализованного языка инструментальных средств верификации. При этом на формализованном языке должны быть выражены:
    - элементы состояний, моделирующей ОС абстрактной системы, используемые для этого множества, функции (отношения);
    - правила преобразования состояний (команды, операции, функции перехода), включая параметры каждого правила, условия и результаты его применения;
    - условия выполнения мандатного контроля целостности и мандатного управления доступом (при необходимости);
- Если формализованный язык инструментальных средств не может точно выразить некоторые элементы модели политики безопасности управления доступом, то описание всех таких элементов и

полуформальное обоснование того, что это не влияет на итоговый результат верификации;

- Результатов верификации модели политики безопасности управления доступом с использованием инструментальных средств верификации с указанием того, какие элементы модели были верифицированы в автоматическом режиме, а какие в полуавтоматическом (ручном) режиме;
- Результатов верификации с применением инструментальных средств выполнения следующих условий при применении (корректности задания) правил преобразования состояний (команд, операций, функций перехода), моделирующей ОС абстрактной системы:
    - условий предоставления субъектам прав доступа и доступов к сущностям или субъектам;
    - условий выполнения иных правил преобразования состояний (команд, операций, функций перехода) над учётными записями пользователей, субъектами и сущностями (создание, удаление, переименование, получение параметров);
- Результатов верификации с применением инструментальных средств того, что в рамках моделирующей ОС абстрактной системы реализованный мандатный контроль целостности позволяет обеспечить защиту от несанкционированного изменения субъектом-нарушителем параметров или данных в сущностях, параметров или функциональности субъектов (захватить контроль над субъектом) с более высоким, чем у него уровнем целостности, и в результате нарушить целостность программно-аппаратной среды ОС;
- При необходимости результатов верификации с применением инструментальных средств того, что в рамках моделирующей ОС абстрактной системы реализованные мандатные контроль целостности и управление доступом позволяют обеспечить защиту от запрещённых информационных потоков (как минимум по памяти) от сущностей с более высоким уровнем конфиденциальности к сущностям с более низким уровнем конфиденциальности (защиту от утечки конфиденциальных данных, от информационных потоков «сверху-вниз»).

3. Заключение

Возможность практического выполнения этих условий подтверждается опытом разработки и верификации МРОСЛ ДП-модели [9-11]. В совокупности эти условия позволяют сформулировать чёткие, научно обоснованные критерии наличия представления формальной модели политики безопасности ОС в

соответствии с требованиями функциональной компоненты ADV_SPM.1 при её включении в профиль защиты или задание по безопасности при сертификации средств защиты информации в рамках реализации новых требований ФСТЭК России [4].

Список литературы

[1]. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7, 2002. 1084 p.

[2]. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. М.: Горячая линия — Телеком, 2013. 338 с.: ил.

[3]. Bell D.E., LaPadula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976. MTR-2997 Rev. 1.

[4]. Информационное сообщение об утверждении Требований безопасности информации к операционным системам от 18 октября 2016 г. No 240/24/4893/ ФСТЭК России. URL: http://fstec.ru/component/attachments/download/1051.

[5]. ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

[6]. ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.

[7]. Abrial J.-R. Modeling in Event-B: System and Software Engineering. Cambridge University Press, 2010.

[8]. Операционная система Astra Linux. URL: http://www.astra-linux.ru/.

[9]. П.В. Буренин, П.Н. Девянин, Е.В. Лебеденко и др.; Под редакцией доктора техн. наук П.Н. Девянина. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие для вузов. 2-е издание, стереотипное. М.: Горячая линия – Телеком, 2016. 312 с.

[10]. P.N. Devyanin, V.V. Kuliamin, A.K. Petrenko, A.V. Khoroshilov, I.V. Shchepetkov. Using Refinement in Formal Development of OS Security Model. In Lecture Notes in Computer Sciences #9609 "Perspectives of System Informatics: 10th International Andrei Ershov Informatics Conference", Springer International Publishing, 2016 pp. 107-115. DOI: 10.1007/978-3-319-41579-6_9.

[11]. Petr N. Devyanin, Alexey V. Khoroshilov, Victor V. Kuliamin, Alexander K. Petrenko, Ilya V. Shchepetkov. Comparison of Specification Decomposition Methods in Event-B. Programming and Computer Software, 2016, Vol. 42, No. 4, pp. 198–205 DOI: 10.1134/S0361768816040022

On the problem of representation of the formal model of security policy for operating systems

P.N. Devyanin <peter_devyanin@hotmail.com>
Federal Educational and Methodological Association of Higher Educational Institutions of Russia for Education in Information Security
Russia, Moscow

Abstract. In connection with the process of implementation by the Federal Service for Technical and Export Control of Russia "Information Security Requirements for Operating Systems", the work analyzes the ways of fulfilling the requirements of the functional component ADV_SPM.1 "Formal Security Policy Model", including defining the language, depth and detail of the presentation of the access control policy and information flows. Among other things, proposals are given on the composition of the main elements of the model, the use of tools for its verification. The practical possibility of applying the proposed approaches is considered by the example of the presentation of the description and verification of the mandatory entity-role security model for logical access control and information flows as the basis of the access control mechanism in the special-purpose operating system Astra Linux Special Edition.

Keywords: information security, security policies, formal models

DOI: 10.15514/ISPRAS-2017-29(3)-1

For citation: Devyanin P.N. On the problem of representation of the formal model of security policy for operating systems. Trudy ISP RAN/Proc. ISP RAS, vol. 29, issue 3, 2017. pp. 7-16 (in Russian). DOI: 10.15514/ISPRAS-2017-29(3)-1

References

[1]. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7, 2002. 1084 p.

[2]. Devyanin P.N. Security models for computer systems. Control of access and information flows. Textbook for higher schools. 2nd ed. M.: Goryatchaya liniya – Telecom, 2013. 338 p (in Russian)

[3]. Bell D.E., LaPadula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976. MTR-2997 Rev. 1.

[4]. Information message on the approval of information security Requirements for operating systems, October 18, 2016. No 240/24/4893/ FSTEK Russian. URL: http://fstec.ru/component/attachments/download/1051.

[5]. GOST R ISO / IEC 15408-2013. Security techniques. Evaluation criteria for IT security. (in Russian).

[6]. GOST R ISO / IEC 18045-2013. Information technology - Security techniques - Methodology for IT security evaluation (in Russian)

[7]. Abrial J.-R. Modeling in Event-B: System and Software Engineering. Cambridge University Press, 2010.

[8]. Operating system Astra Linux. URL: http://www.astra-linux.ru/ (in Russian).

[9]. P.V. Burenin, P.N. Devyanin, E.V. Lebedenko and others; Under the editorship of P.N. Devyanin. Security of the special-purpose operating system Astra Linux Special Edition. Textbook for high schools. 2nd edition, stereotyped. M .: Goryatchaya liniya – Telecom, 2016, 312 p. (in Russian)

[10]. P.N. Devyanin, V.V. Kuliamin, A.K. Petrenko, A.V. Khoroshilov, I.V. Shchepetkov. Using Refinement in Formal Development of OS Security Model. In Lecture Notes in Computer Sciences #9609 "Perspectives of System Informatics: 10th International Andrei Ershov Informatics Conference", Springer International Publishing, 2016, pp. 107-115. DOI: 10.1007/978-3-319-41579-6_9.

[11]. Petr N. Devyanin, Alexey V. Khoroshilov, Victor V. Kuliamin, Alexander K. Petrenko, Ilya V. Shchepetkov. Comparison of Specification Decomposition Methods in Event-B. Programming and Computer Software, 2016, Vol. 42, No. 4, pp. 198–205. DOI: 10.1134/S0361768816040022