УДК 004.8

РАСШИРЕННАЯ МОДЕЛЬ ОТКРЫТЫХ СИСТЕМ

К.А. Бугайский
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: kabuga@ipu.ru

Д.С. Бирин
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: birin@phystech.edu

Б.О. Дерябин
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: baga_d@mail.ru

И.С. Перескоков
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: pereskokov@phystech.edu

Ан.О. Петров
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: petrovaojob@gmail.com

Ал.О. Петров
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: petrovalexandr@ipu.ru

К.В. Табаков
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: tabakov2002@mail.ru

Е.С. Храмченкова
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: hramchenkovaes@yandex.ru

С.О. Цепенда
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: tsepende.s@gmail.com

Ключевые слова: информационная безопасность, открытые системы, модель, вычислительная система, управление конфигурацией.

Аннотация: В докладе приведены основные положения расширенной модели открытых систем разработанной для описания современных вычислительных систем. Прежде всего в части касающейся вопросов взаимодействия программных и аппаратных компонент в процессе обработки данных, а также в части управления. Показано, что введение в модель слоев отображающих обрабатываемые данные и пользователей системы предоставляет новые возможности при рассмотрении вопросов защиты информации в современных вычислительных системах. Разработанные в модели механизмы коммуникаций и механизмы управления дают дополнительные инструменты для моделирования и оценки безопасности информации. Предложены правила формирования конфигураций для наборов программ и пользователей как основы для управления защитой информации.

1. Введение

Современные информационные системы представляют собой гетерогенные структуры с широким применением различных механизмов виртуализации и архитектурного приема «инфраструктура как код» [1]. Работа подобных структур повсеместно опирается на принцип открытых систем заложенного в соответствующей референсной модели – OSE/RM, развитие которой практически прекратилось. Разработка расширенной модели открытых систем (далее – модели) имеет целью адаптацию OSE/RM к современному уровню развития информационных систем и ее использования для решения задач защиты информации. Объектом моделирования является вычислительная система (ВС) как совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [2].

2. Структура модели

Общая структура модели приведена в [3] и там же показана ее связь с основными положениями OSE/RM. Из которых выделим уровни абстракций программных компонент, опирающиеся на структуру вычислительной системы: слой абстракций аппаратного уровня (HW), слой абстракций уровня операционной системы (OW), слой абстракций служб и сервисов (MW) и слой абстракции прикладного программного обеспечения (AW). Для всех этих слоев в модели введена абстракция – программная сущность (ПС), из которой образуется множество $AE = \{a_1, \cdots, a_n\}$. Также из OSE/RM перенесен в модель достаточный с функциональной и структурной точек зрения набор абстракций для представления аппаратных компонент слоя HW: CPB – процессор и системная шина, RAM – энергозависимая память (ОЗУ), DD – энергонезависимая память (диски), DIO – устройства ввода-вывода, NIC – устройства сетевого обмена данными.

Принципиальным развитием модели является введение двух слоев абстракций: IW – слой информационных единиц (ИЕ) и UW – слой пользователей. Данные слои обрамляют слои OSE/RM и расположены, соответственно, ниже HW и выше AW. Описание этих слоев и их предназначение дано в [3].

Введение слоя IW позволило рассматривать взаимодействие ИЕ и ПС в процессе обработки информации в интересах пользователя ВС с точки зрения алгоритмической реализации операций, к которым относятся:

- op^{mem} – операции с имеющимися в распоряжении программы структурами памяти (компонента ВС RAM);
- op^{proc} – операции по созданию, запуску, останову или удалению потоков или

процессов (компонента ВС СРВ);

- op^{file} – операции по созданию, удалению, записи, чтения или модификации файлов (компонента ВС DD);
- op^{net} – операции сетевого обмена данными (компонента ВС NIC);
- op^{io} – операции обмена данными через устройства ввода-вывода (компонента ВС DIO).

Поскольку данные не существуют без физического носителя, то на основе указанных операций $OPS = \{op^{mem}, op^{proc}, op^{file}, op^{net}, op^{io}\}$ в модели введены соответствующие слои базовой плоскости, каждый из которых представляет собой граф G^{op}, $op \in OPS$. В качестве корневой вершины графа принимаются монитор обращений M или ядро Kernel. Монитор обращений представляет собой ПС (в том числе драйверы) слоев HW и OW минимально необходимые для выполнения указанных операций. Ядро, в свою очередь, это объединенные в единую ПС мониторы, обеспечивающие выполнение операций op^{mem} и op^{proc}, связанных с запросами на выделение и освобождение памяти или процессов для остальных ПС данной ВС [4]. Это дает возможность описывать сложные структуры, например, такие как механизм виртуализации в ВС, который может быть представлен в виде $Kernel \to M \to mw \to Kernel' \to M'$, где через mw обозначены причастные к реализации структуры ПС слоя MW.

Введение в модель операций OPS позволяет представить ПС двумя типами функций:

- φ^t – функции типа take, обеспечивающие по результатам внутренних вычислений запрос на выполнение необходимых операций в другой ПС;
- φ^g – функции типа grant, обеспечивающие инициализацию выполнения необходимых вычислений в самой ПС в ответ на запрос от другой ПС.

Соответственно, данные функции образуют связь $\theta(i,j)$: $\varphi^g(a_i) \to \varphi^t(a_j)$, $a_i, a_j \in AE$, $i \neq j$, $i,j \in [1, \dots, |AE|]$, $\theta(i,j) \in \Theta$, возникающую при взаимодействии двух ПС. Что дает основания рассматривать ПС как вершины, связи как ребра графа, а сам граф G^{op} как орграф. Пусть ПС a3 слоя AW обращается к некой ИЕ слоя IW. Согласно структуре базовой плоскости модели, ПС a3 должна взаимодействовать с ПС a1, a2 промежуточных слоев. Пример такого взаимодействия ПС и ИЕ приведен на рис. 1

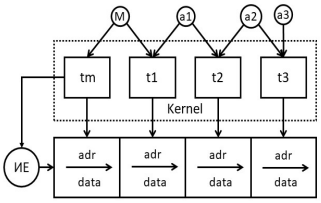

Рис. 1. Пример взаимодействия ПС и ИЕ.

На рис. 1 через tm, t1, t2, t3 обозначены разработанные в модели механизмы коммуникаций (МК), каждый из которых может быть представлен как:

$$t = \{\varphi^*(a_i), \varphi^*(a_j), \varphi^*(Kernel), buffer, C, \Theta\},$$

где C – конфигурация МК, определяющая форматы и протоколы обмена; $buffer$ – определенная структура (особый тип ИЕ) непосредственно доступная (являющуюся частью) программной реализации МК в ПС.

Роль и место buffer и Kernel в процессах взаимодействия, а также различные схемы взаимодействия, в том числе отдельных ВС, рассмотрены в [4]. Отметим, что раздельные буферы для взаимодействующих ПС создаются ядром и соответствующим монитором, которые также выполняют синхронизацию обмена данными между буферами. Из определения монитора и ядра вытекает, что МК должен быть соотнесен с типом операции или с типом физического носителя ИЕ. Что, в свою очередь, позволяет использовать МК в качестве ребер для каждого из графов G^{op} базовой плоскости.

Рис. 1 наглядно показывает, что обращение ПС a3 к ИЕ сопровождается преобразованиями циркулирующей между ПС информацией. Это может быть перевычисление адреса доступа к ИЕ или сериализация/десериализация данных. Кроме того, работа каждого последующего МК на пути p между ПС a3 и ИЕ зависит от качества работы предыдущего МК. То есть, модель дает основания утверждать, что любой процесс обработки информации в ВС представляет собой путь от ИЕ до ПС, который следует рассматривать как рекуррентную функцию $p = \psi(t_1, \dots, t_n)$, где n – число МК (длина пути), а t_i – конкретный МК в составе пути .

Слои базовой плоскости модели в виде графов G^{op} в основе которых лежат МК создают основу для изучения и моделирования вопросов обеспечения целостности, доступности и конфиденциальности в процессе функционирования ПС применительно к различным физическим носителям ИЕ.

Введение в модель слоя UW обеспечило отображение прав доступа акторов (субъектов) за счет связывания определенных ЭК с определенным аккаунтом (учетной записью) ВС [5, 6], то есть отношения актор => аккаунт => ЭК => ИЕ. Разработка данного отношения базируется на таких абстракциях как оболочка и окружение аккаунта, элемент конфигурации (ЭК). Оболочка аккаунта состоит из наборов ПС относящихся как правило к слоям OW и MW базовой плоскости и образующих графический интерфейс актора, интерфейс командной строки актора, набор утилит обеспечивающих выполнение тех или иных функций операционной системы. Окружение аккаунта, в свою очередь, определяет порядок и правила исполнения оболочки аккаунта и содержащихся в ней ПС и ИЕ с точки зрения допустимого использования ресурсов ВС. Под ЭК понимается совокупность ПС базовой плоскости модели, которая образует взаимосвязанную группу, обеспечивает выделенную функциональность при работе в составе ВС и управление которой осуществляется независимого от других ЭК. ЭК и окружение аккаунта образуют множества *CE* и *SE* соответственно. В [7] показано, что как ЭК, так и окружение аккаунта в полной мере могут быть описаны только сочетанием параметров различных типов, обозначаемых как наборы B^*. В результате разработки данных абстракций в модель были введены еще два типа операций для ПС, отнесенных к множеству $OPA = \{op^{api}, op^{aaa}\}$:

- op^{api} – операции непосредственного взаимодействия ЭК в процессе обработки информации;
- op^{aaa} – операции, обеспечивающие функции идентификации, аутентификации и авторизации в пространстве прав пользователей ВС.

В итоге получены выражения, определяющие конфигурацию для ЭК:

$$C^{ce}: \bigcup_{OPS} B^{op} + \bigcup_{IC} B^{IC} + \bigcup_{OPA} B^{api} + \bigcup_{OPA} B^{aaa} + \bigcup_{OPA} B^{dfa}.$$

А также для окружения аккаунта:

$$C^{se}: [\bigcup_{OPS} B^{op} + \bigcup_{ACE} B^{aaa} + \bigcup_{SIE} B^{dfa} + B^{CE} + B^{AS} + \bigcup_{ACE} C^{ce}].$$

Разница в использовании символов объединения и сложения в выражениях для конфигураций заключается в следующем: объединение параметров предполагает, что

функционирование ПС в аккаунте будет зависеть от порядка следования параметров, в то время как сложение обозначает аддитивность при объединении различных типов параметров в общую конфигурацию.

Кроме того, введение в модель слоя UW позволило впервые сформировать структуру плоскости администрирования (отсутствующую в OSE/RM), которая определяет соотношения между ПС, ЭК и окружением аккаунта на основе механизмов управления (МУ). Состав МУ и перечень встроенных операций определен в [7]. Разработанные в модели описания объекта и субъекта управления, предусматривают возможность разнесения по разным типам аккаунтов различных частей одного МУ, что позволяет ввести понятия владельца и пользователя конфигураций ЭК и рассматривать любой МУ модели как распределенную структуру работающую на разных уровнях как с точки зрения слоев базовой плоскости, так и с точки зрения необходимых и достаточных прав пользователей ВС.

3. Заключение

Расширенная модель открытых систем предоставляет необходимые понятия и язык описания для рассмотрения вопросов функционирования вычислительных систем с точки зрения теории управления в терминах субъект управления (пользователь системы), объект управления (конфигурации). Разработанный подход к описанию механизма коммуникаций программных сущностей и механизма управления элементами конфигурации позволяет с хорошим уровнем абстракции описывать процессы обеспечения жизненного цикла и защиты данных информационных систем состоящих из разнородных по назначению и структуре компонент. Создание плоскости администрирования позволяет рассматривать вопросы защиты информации как вопросы управления конфигурациями, описывающих работу и взаимодействие компонент программной и аппаратной части вычислительной системы.

Список литературы

1. Калашников А.О., Бугайский К.А Инфраструктура как код: формируется новая реальность информационной безопасности // Информация и безопасность. 2019. Т. 22, № 4. С. 495-506.
2. Калашников А.О., Бугайский К.А., Аникина Е.В. Модели количественного оценивания компьютерных атак // Информация и безопасность. 2019. Т. 22, № 4. С. 517-528.
3. Бугайский К.А., Бирин Д.С., Дерябин Б.О., Цепенда С.О. Расширенная модель открытых систем (Часть 1) // Информация и безопасность. 2022. Т. 25, № 2. С. 169-178.
4. Бугайский К.А., Перескоков И.С., Петров Ал.О., Петров Ан.О. Расширенная модель открытых систем (Часть 2) // Информация и безопасность. 2022. Т. 25, № 3. С. 321-330.
5. Информационная безопасность систем организационного управления: теоретические основы. В 2 т. / Под ред. Кузнецова Н.А., Кульбы В.В. М.: Наука, 2006.
6. Лимончелли Т., Хоган К., Чейлап С. Практика системного и сетевого администрирования / 3-е издание, пер. с англ. М.: Вильямс, 2018. 1104 с.
7. Бугайский К.А., Дерябин Б.О., Табаков К.В., Храмченкова Е.С., Цепенда С.О. Расширенная модель открытых систем (Часть 3) // Информация и безопасность. 2022. Т. 25, № 4. С. 501-512.