ПРИМЕНЕНИЕ МОДЕЛИ TAKE-GRANT ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ СОСТОЯНИЙ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

Д.М. Бречка

Омский госуниверситет им. Ф.М. Достоевского
E-mail: dbrechkawork@yandex.ru

В современных информационных системах для разделения доступа к информации широко применяется дискреционная политика безопасности [1,2]. Одной из наиболее полно проработанных в теоретическом плане дискреционных моделей безопасности является модель Take-Grant [3]. В рамках этой модели были доказаны теоремы, оговаривающие условия защищенности информационной системы от несанкционированных доступов (НСД). Однако способы проверки этих условий в классической модели Take-Grant не приводятся.

В работах [4,5] были предложены алгоритмы проверки безопасности состояний модели Take-Grant, имеющие полиномиальную сложность. Эти алгоритмы основаны на известных алгоритмах Дейкстры, Флойда, поиска в глубину и в ширину.

Предлагается применить алгоритмы модели Take-Grant для анализа безопасности операционной системы Windows, использующей файловую систему NTFS. Для того чтобы применение модели Take-Grant стало возможным, необходимо выяснить, присутствуют ли в Windows аналоги прав Take (брать права доступа на какой-либо объект у другого объекта) и Grant (отдавать доступ на объект другому субъекту). В системе Windows возможность передавать права на объект другим субъектам имеют администратор, владелец объекта либо любой пользователь с полными правами на объект [6]. Информация о владельце объекта и правах субъектов на объект содержится в дескрипторе безопасности объекта, потому, анализируя дескриптор безопасности можно однозначно выявить субъекты, имеющие право Grant на объект.

Помимо прочих прав доступа в Windows присутствует право Take Ownership (смена владельца). Субъект, обладающий этим правом на объект, может стать владельцем объекта и получить любые права на этот объект [6]. Таким образом, можно говорить, что субъект, обладающий правом Take Ownership, обладает правом Take на объект.

Для проведения анализа безопасности необходимо построить граф доступов, содержащий все объекты и субъекты системы. Граф доступов может быть получен из матрицы доступов, содержащей все субъекты и объекты системы и установленные между ними отношения.

Для построения матрицы доступов в Windows необходимо выполнить рекурсивный обход файловой системы и проанализировать дескриптор безопасности каждого объекта с целью выявления установленных прав доступа. При анализе дескриптора безопасности нужно просмотреть списки контроля доступа (DACL), содержащиеся в нем. DACL состоит из элементов (ACE), которые непосредственно содержат идентификатор субъекта (SID) и маску доступа, для этого субъекта. Маска доступа в ACE определяет набор разрешенных (запрещенных) действий над данным объектом для субъекта с данным идентификатором. Следует учитывать, что существуют различные типы ACE, нас в данном случае интересуют разрешающие и запрещающие ACE. Разрешающие ACE образуют «белый список» доступов, запрещающие – «черный список» доступов [6].

Тип ACE следует учитывать при построении матрицы доступов. Так, если объект имеет разрешающий ACE, то этот ACE копируется в соответствующую ячейку матрицы, если объект имеет запрещающий ACE, в матрицу помещается инвертированная копия данного ACE. Если объект имеет запрещающий и разрешающий ACE, то следует выполнить операцию побитовое «ИЛИ» над этими списками, результат операции инвертировать и поместить в матрицу доступов, так как запрещающий список имеет больший приоритет, чем разрешающий.

Таким образом, при рекурсивном обходе файловой системы для каждого нового объекта будет создаваться столбец матрицы доступов. При анализе дескриптора безопасности объекта будут создаваться строки матрицы и заполняться ее ячейки.

Очевидно, что размер матрицы и графа доступов будет довольно большим, так как только количество файлов в системе NTFS может достигать 2^{32} - 1. Таким образом, решение поставленной задачи на обычной ЭВМ будет малоэффективным. Предлагается решить задачу с применением суперЭВМ.

Для работы предполагается использовать многопроцессорную вычислительную машину кластерного типа МВС-1000/128 производства ФГУП «НИИ Квант». СуперЭВМ является собственностью Омского суперкомпьютерного центра коллективного пользования СО РАН и омских вузов, установлена в Омском государственном университете им. Ф.М. Достоевского в корпусе факультета компьютерных наук. Вычислительная машина состоит из шестидесяти четырех двухпроцессорных модулей на базе процессоров DEC Alpha 21264. Суммарный объем разделяемой оперативной памяти составляет 128 Гбайт, пиковая производительность – около 196 Gflops.

Таким образом, для решения поставленной задачи необходима программная реализация следующих алгоритмов:

1) алгоритм построения матрицы доступов для операционной системы Windows;
2) параллельный алгоритм Дейкстры;
3) параллельный алгоритм Флойда;
4) параллельный алгоритм поиска в глубину на графе;
5) параллельный алгоритм поиска в ширину на графе.

Все алгоритмы реализуются на языке C++ с использованием библиотеки MPI. На данном этапе уже реализованы алгоритмы Дейкстры и Флойда.

Литература

1. Девянин П.Н. Модели безопасности компьютерных систем: Учебное пособие для студентов высших учебных заведений. Москва: Издательский центр «Академия», 2005.
2. Гайдамакин Н.А. Разграничения доступа к информации в компьютерных системах. Екатеринбург: Издательство Уральского университета, 2003
3. Lipton R.J., Richard J. A Linear Time Algorithm for Deciding Subject Security // J. of the ACM (Addison-Wesley). 1977. No. 3. P. 455-464.
4. Бречка Д.М. Алгоритмы анализа безопасности состояний компьютерной системы для модели Take-Grant // Математические структуры и моделирование. 2009. Вып. 20. С. 160-173.
5. Бречка Д.М. Алгоритмы поиска мостов типа и в графе доступов для дискреционной модели безопасности Take-Grant // Математические структуры и моделирование. 2011. Вып. 23. С. 99-105.
6. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. Мастер-класс / Пер. с англ. 4-е изд. М.: Издательско-торговый дом «Русская редакция», 2005.