Лабораторная работа №1.

Управление доступом с помощью списков контроля доступа. Часть 1. Управление доступом к объектам операционных систем.

Теоретические основы

Список контроля доступа (Access Control List – ACL) — механизм распределения прав, с помощью которого определяется, какой субъект может получать доступ к конкретному объекту в системе и какие действия ему разрешены или запрещены по отношению к этому объекту. Списки контроля доступа являются основой систем с избирательным управлением доступа.

Традиционная модель разграничений прав доступа в файловых системах в большинстве случаев определяет 3 класса пользователей: пользователь-владелец, группа-владелец и остальные.

Список контроля доступа представляет собой структуру данных, содержащую записи (Access Control Entry – ACE), определяющие права пользователя или группы на системные объекты, такие как процессы или файлы. Каждый из трех классов пользователей представлен в виде ACE. Разрешения для дополнительных пользователей и групп содержатся в дополнительных ACE. Каждый объект в системе содержит указатель на свой ACL. Привилегии определяют специальные права доступа, разрешающие пользователю читать объект, редактировать его или исполнять. В некоторых реализациях ACL могут определять право пользователя или группы на изменение ACL объекта.

ACL по умолчанию определяет разграничения прав доступа к объектам файловой системы, которые наследуются у родительского каталога в процессе создания объекта.

Разрешения наследованного ACL доступа далее модифицируются параметром режима доступа, который имеется в каждом системном вызове создания объекта файловой системы. Этот параметр состоит из разрешений, которые представляют собой классы разрешений для владельца, группы и остальных. Эффективным разрешением для каждого класса устанавливается пересечение разрешений, определенных для класса в ACL и в параметре режима доступа.

Для доступа к объекту файловой системы процесс проверки сначала выбирает ACE, которая в наибольшей степени совпадает с запросом процесса. ACE просматриваются в следующем порядке: владелец, именованный пользователь, группа (группа-владелец или именованная группа), остальные. Доступ определяется

только одной единственной ACE. Далее проверяется, содержит ли соответствующая ACE достаточные разрешения на доступ. Права субъекта могут быть представлены в нескольких записях ACE. Если какая-нибудь из этих ACE содержит необходимые разрешения, то она и выбирается. Если ни одна ACE не содержит достаточных разрешений, то в доступе будет отказано независимо от выбора ACE.

Доступ к ACL объекта файловой системы осуществляется перед каждым решением на доступ, которое включает этот объект. Проверка доступа осуществляется на всем пути от исходного пространства пользователя до файла. Для того, чтобы избежать частого просмотра атрибутов ACL и конвертирования из архитектурно-независимого представления атрибутов в архитектурно-специфическое, реализации ряд файловых систем используют кэширующие механизмы.

Большинство UNIX-подобных систем, поддерживающих ACL, ограничивают максимальное число возможных ACE. ACL с большим числом ACE более сложны в обслуживании.

Создатель объекта файловой системы является также начальным его владельцем. Нельзя ограничить владельца файла от изменения разрешений.

Инструментальные и вспомогательные средства

Виртуальная машина с установленной ОС (Windows, Linux).

Задание для самостоятельной работы

1. Создание программы, которая позволяет настроить ACL для объектов файловой системы и проверить корректность её работы.
2. Оформление отчёта о проделанной работе.

Программа должна быть создана на выбранном языке программирования и выполнять следующие действия.

1. Создать группы пользователей group_iit1, group_iit2.
2. Создать пользователей iit11, iit12 и добавить их в группу group_iit1.
3. Создать пользователей iit21, iit22 и добавить их в группу group_iit2.
4. Предоставить пользователю iit21 административные привилегии.
5. Создать пользователя iit3.

6. Создать папку pzs.

7. Создать папку pzs11 в папке pzs с правами чтения, записи, выполнения только для владельца.

8. Создать папку pzs12 в папке pzs с правами чтения, записи, выполнения только для группы.

9. Создать папку pzs13 в папке pzs с правами чтения, записи, выполнения только для остальных пользователей.

10. Создать папку pzs14 в папке pzs с правами чтения, записи, выполнения для всех пользователей.

11. Создать папку pzs15 в папке pzs с правами чтения, записи, выполнения только для администратора (root).

12. Сменить текущего пользователя на iit11.

13. В папках pzs11, pzs12, pzs13, pzs14 создать следующие файлы:

file11 – только с правами чтения только для владельца файла;

file12 – только с правами чтения, записи только для владельца файла;

file13 – только с правами записи только для владельца файла;

file14 – с правами чтения, записи, выполнения только для владельца файла;

file15 – только с правами выполнения только для владельца файла;

file21 – только с правами чтения только для группы пользователей group_iit1;

file22 – только с правами чтения, записи только для группы пользователей group_iit1;

file23 – только с правами записи только для группы пользователей group_iit1;

file24 – с правами чтения, записи, выполнения только для группы пользователей group_iit1;

file25 – только с правами выполнения только для группы пользователей groupt_iit1;

file31 – только с правами чтения только для остальных пользователей;

file32 – только с правами чтения, записи только для остальных пользователей;

file33 – только с правами записи только для остальных пользователей;

file34 – с правами чтения, записи, выполнения только для остальных пользователей;

file35 – только с правами выполнения только для остальных пользователей;

file41 – только с правами чтения для всех пользователей;

file42 – только с правами чтения, записи для всех пользователей;

file43 – только с правами записи для всех пользователей;

file44 – с правами чтения, записи, выполнения для всех пользователей;

file45 – только с правами выполнения для всех пользователей;

file51 – только с правами чтения только для администратора;

file52 – только с правами чтения, записи только для администратора;

file53 – только с правами записи только для администратора;

file54 – с правами чтения, записи, выполнения только для администратора;

file55 – только с правами выполнения только для администратора.

Файлы, удовлетворяющие шаблону «file*x*5», содержат следующий текст

для ОС Linux

```
read testVariable
```

для ОС Windows

```
set /p testVariable=
```

Остальные файлы содержат текст

```
echo "Hello World".
```

14. Для каждого из созданных файлов проверить, можно ли прочитать, редактировать, запустить файл пользователям

iit11,

iit12,

iit21,

iit22,

iit3,

суперпользователем (root).

15. Запустить каждый из файлов, которые удовлетворяют шаблону «file*x*5» пользователем iit11. Проверить, можно ли остановить запущенный процесс пользователям

iit11,

iit12,

iit21,

iit22,

iit3,

суперпользователем (root).

16. В каждой из созданных папок проверить, можно ли прочитать содержимое папок, создать новые файлы, удалить каждый из существующих файлов.

17. Удалить созданные файлы, папки, пользователей iit11, iit12, iit21, iit22, iit3, группы groupt_iit1, group_iit2.

Отчётность

В качестве результата ожидается:

1. Демонстрация созданной программы.
2. Демонстрация работы созданной программы.
3. Отчёт о проделанной работе.

Отчёт должен быть оформлен в соответствии с http://www.bsuir.by/m/12_100229_1_80040.pdf.

Отчёт должен содержать следующую информацию.

1. Постановка задачи.
2. Описание созданной программы: код программы, задачи, которые могут быть решены с помощью созданной программы и описание полученных результатов.
3. Вывод. В выводе должны быть представлена семантическая и прагматическая составляющие проделанной работы.

Список рекомендуемой литературы

1. Олифер, В. Г. Сетевые операционные системы: Учебник для вузов. 2-е издание / В. Г. Олифер, Н. А. Олифер. – Спб.: Питер, 2009. — 669 с. стр. 342-360.
2. Таненбаум, Э. С. Современные операционные системы. 3-е издание / Э. С. Таненбаум. – СПб.: Питер, 2011. — 1120 с. стр. 724-731.