Операционные системы

Безопасность [1]

Басин А. Н., Соловьев А. В.

ПетрГУ

(Rev. 2018 06 07)

[1] По материалам «Таненбаум Э., Бос Х. Современные операционные системы. СПб.: Питер, 2015.»

Задачи и угрозы безопасности

Задачи	**Угрозы**
Конфиденциальность	Незащищенность данных
Целостность	Подделка данных
Доступность	Отказ от обслуживания

Конфиденциальность (confidentiality) – сохранение секретности данных.

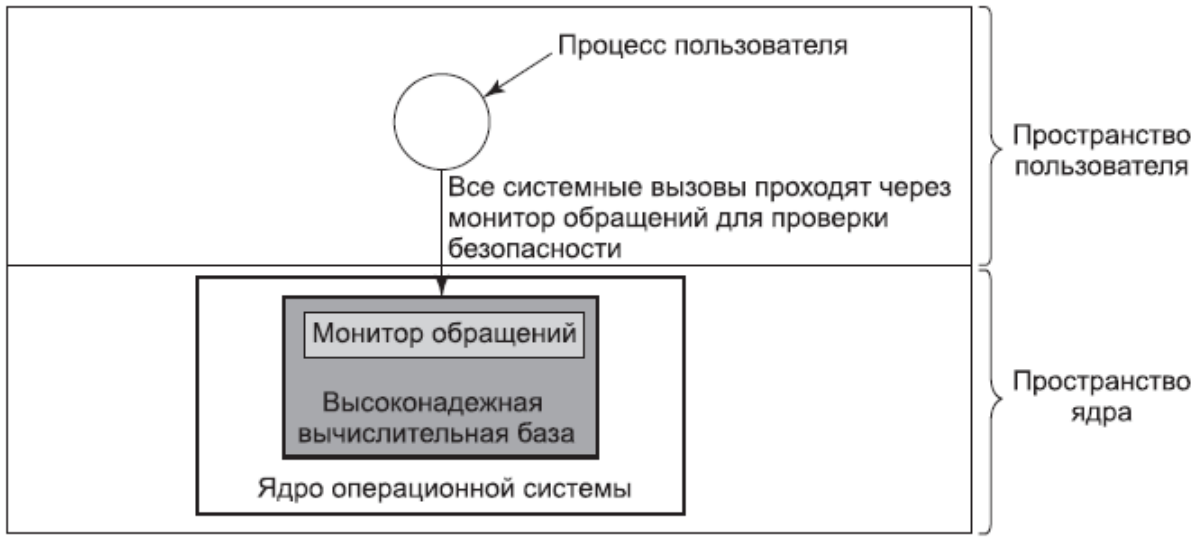
Целостность (integrity) – означает, что пользователи, не обладающие необходимыми правами, не должны иметь возможности изменять какие-либо данные без разрешения их владельцев.

Доступность (availability) – означает, что никто не может нарушить работу системы и вывести её из строя.

А также: *аутентичность* (authenticity), *идентифицируемость* (accountability), *неотвергаемость* (nonrepudiability), *закрытость* (privacy) и др.

Безопасность операционных систем

1. А нельзя ли создать защищенную компьютерную систему?
2. Если да, то почему она до сих пор не создана?



Trusted Computing Base – высоконадежная вычислительная база.

Управление доступом к ресурсам

Домены защиты

Домен (domain) представляет собой множество пар (объект, права доступа). Каждая пара определяет объект и некоторое подмножество операций, которые могут быть выполнены в отношении этого объекта.

Права доступа (rights) означают разрешение на выполнение той или иной операции.

Принцип минимальных полномочий (Principle of Least Authority (POLA)): безопасность проще соблюсти, когда у каждого домена имеется минимум объектов и привилегий для работы с ними и нет ничего лишнего.

Матрица защиты

В любой момент времени каждый процесс работает в каком-нибудь домене защиты (существует некая коллекция объектов, к которым он может иметь доступ, и для каждого объекта у него имеется некий набор прав). Во время работы процессы могут также переключаться с одного домена на другой.

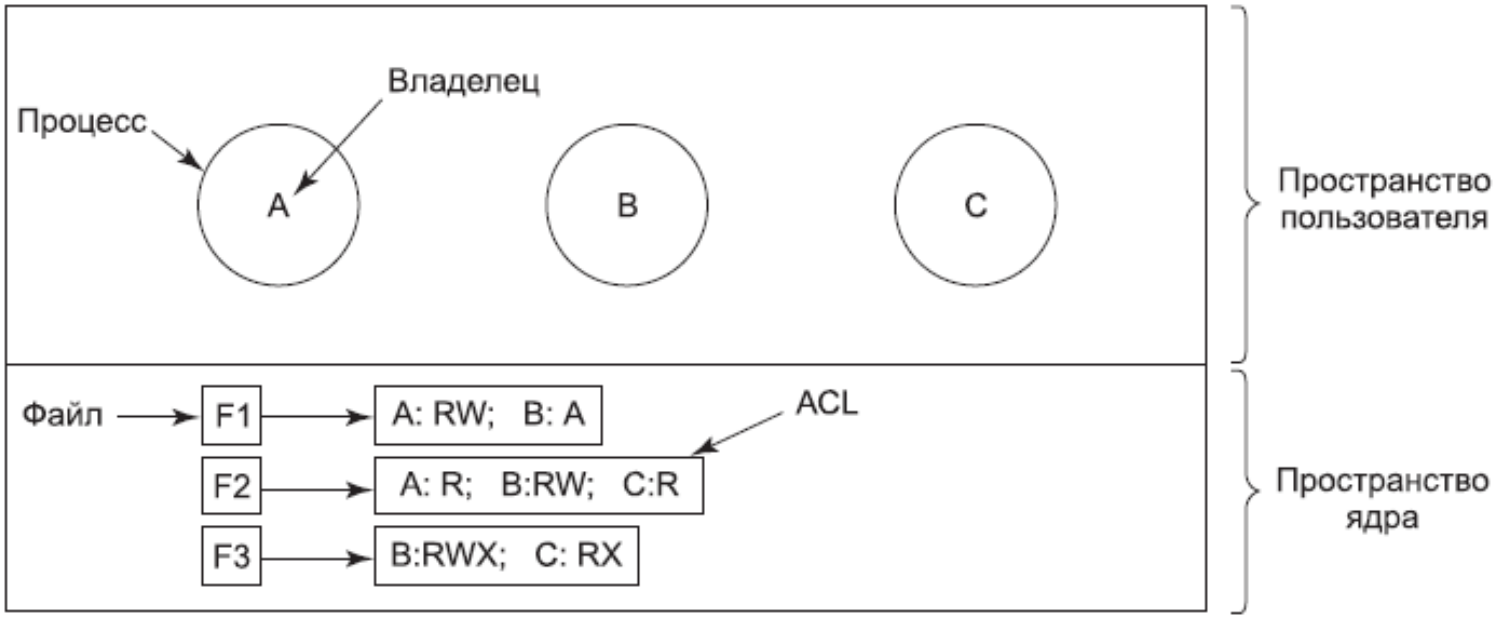
В UNIX, например, в качестве идентификатора (номера) домена можно использовать (UID,GID) процесса.

	Ф1	Ф2	Ф3	Ф4	Ф5	Ф6	Принтер	Плоттер	Д1	Д2	Д3
Д1	R	RW								Enter	
Д2			R	RWX	RW		W				
Д3						RWX	W	W			

Располагая *матрицей защиты* и номером текущего домена, ОС может определить, разрешён ли из конкретного домена определённый вид доступа к заданному объекту.

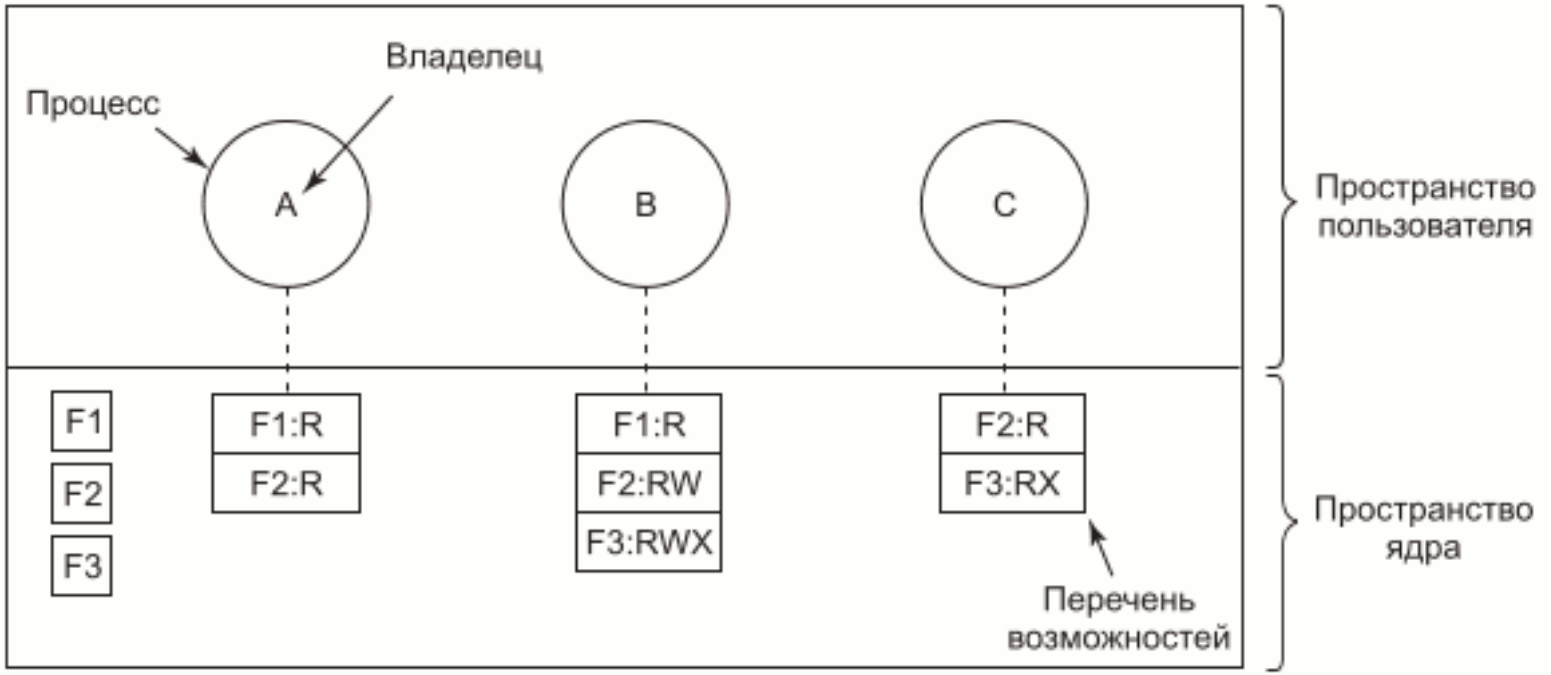
Списки управления доступом

ACL (Access Control List)



Перечни возможностей

C-list (capability list)



Способы защиты перечней возможностей от подделки:

- теговая архитектура (IBM AS/400);
- хранить перечень внутри ядра (процесс ссылается на элемент перечня по номеру) (Hydra);
- криптографическая защита элементов перечня (Amoeba).

Сравнение ACL и C-list

- C-list облегчает проверку.
- C-list легко инкапсулируются.
- В ACL сложно организовать широкий доступ (без групп).
- ACL позволяют выборочно отзывать права субъектов.
- Если объект удаляется, а C-list — нет или наоборот, возникают проблемы.

Аутентификация

Аутентификация (1)

Каждая надёжная (secured) компьютерная система должна требовать от всех пользователей во время входа проходить аутентификацию.

Аутентификация по паролю

- Слабые пароли (словари паролей)
- Хранение паролей (shadow, хэш/соль)

Одноразовые пароли

- Блокнот со списком паролей
- Односторонняя цепочка хэширования

Аутентификация (2)

Схема аутентификации «оклик – отзыв» (challenge – response)

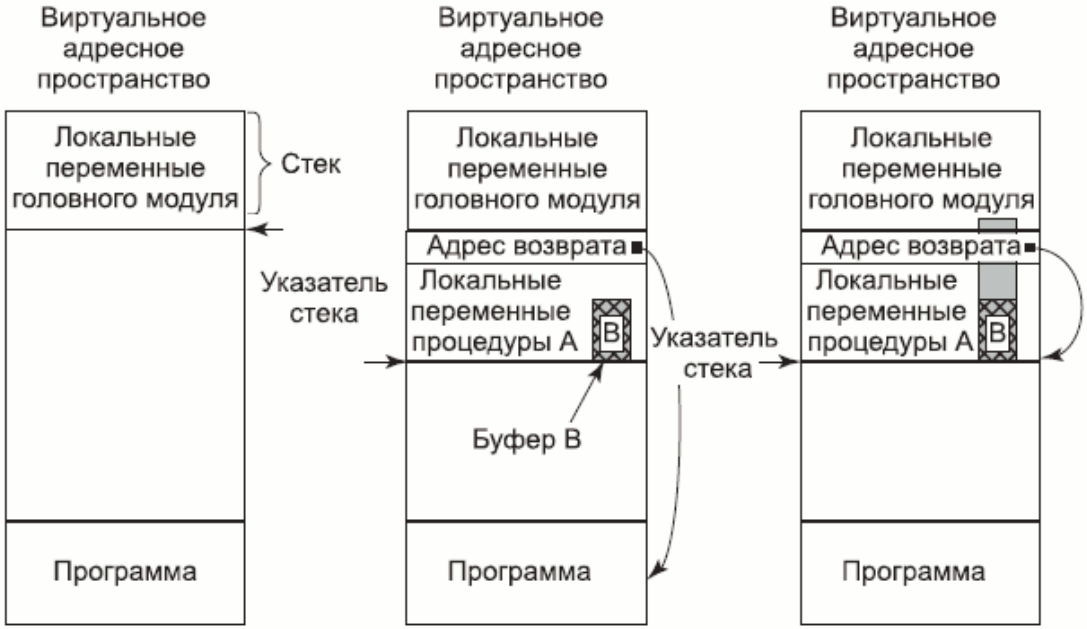
- Множество пар вопросов и ответов.
- Секретная функция расчёта отзыва по указанному сервером аргументу.
- Digest: hash(secret+random).
- Криптокомпьютеры.

Аутентификация с использованием физического объекта

Аутентификация с использованием биометрических данных

Уязвимости ПО

Переполнение буфера (1)




```
void A() {
     char B[128];
     printf("Enter message:");
     gets(B);
     writeLog(B);
}
```

- Стековый индикатор («канарейка») – обычно реализуется компилятором.
- Предотвращение выполнения данных (NX-бит, DEP – Data Execution Prevention).

Переполнение буфера (2)

Атака возврата в библиотеку

- Зачем внедрять код, когда его уже вполне достаточно в двоичном виде? Почти все программы на языке C связаны с библиотекой libc (функции system, exec, mprotect, ...).

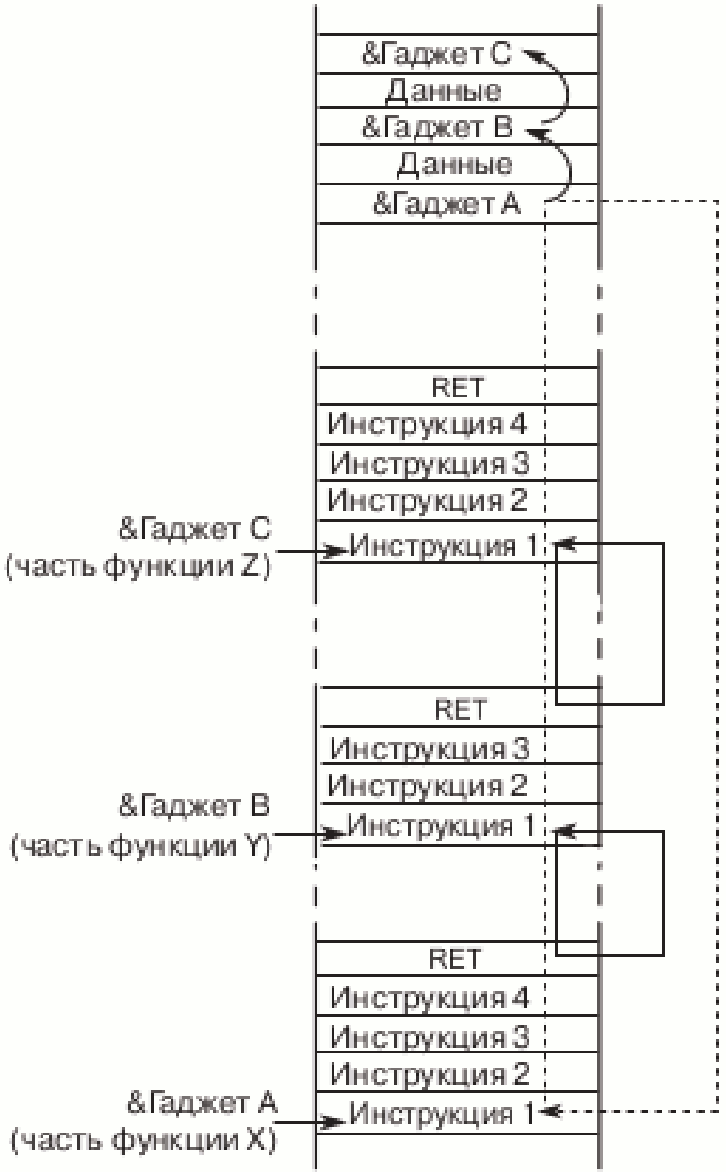
Возвратно-ориентированное программирование — Return-Oriented Programming (ROP)

- Вместо возвращения управления в точки входа в библиотечные функции взломщик может передать управление любой инструкции в текстовом сегменте (коду в середине, а не в начале функции).

Отдельные фрагменты называются *гаджетами* (gadgets).

Для борьбы с этими атаками используется технология *рандомизации распределения адресного пространства* — Address Space Layout Randomization. ASLR занимается произвольным выбором позиций исходного стека, кучи и библиотек при каждом запуске программы.
Linux – с 2.6.12 (2005). В Windows – с Vista (2007).

Иллюстрация ROP



Гаджеты примера:

Гаджет A:
Помещение операнда из стека в регистр 1
Если значение отрицательное, переход
к обработчику ошибок
В противном случае возврат управления

Гаджет B:
Помещение операнда из стека в регистр 2
Возврат

Гаджет C:
Умножение значения регистра 1 на 4
Помещение значения регистра 1 в стек
Сложение значения регистра 2
со значением на вершине стека
и сохранение результата в регистре 2

Прочие уязвимости ПО (1)

Атаки, использующие форматирующую строку (format string attack)

```
printf(g); // g - получено от пользователя
```

Указатели на несуществующие объекты (dangling pointer attack)

```
int *A = (int *) malloc (128);
...
if (...) { printf("Ошибка..."); free(A); }
else { ... }
A[0] = ...;
```

Атаки, использующие разыменование нулевого указателя

Взломщик приобретает возможность инициировать разыменование нулевого указателя из пользовательского процесса (например, вызвать функцию, использующую указатель функции, который ещё не был инициализирован). С помощью mmap пользовательский процесс может потребовать от ядра отобразить память по конкретному адресу (в данном случае 0).

Прочие уязвимости ПО (2)

Атаки, использующие переполнение целочисленных значений

Например, для работы с графикой пользователь задаёт высоту и ширину изображения. Если целевые ширина и высота были выбраны, чтобы вызвать переполнение, программа неправильно вычислит, сколько памяти ей понадобится для хранения изображения (слишком маленький буфер). Далее – атака за счёт переполнения буфера.

Атаки, использующие внедрение команд

```
// cmd = "cp " + src + " " + dst; src и dst получены от пользователя
system(cmd);
```

Пользователь вводит: `src = "file1"` и `dst="file2; rm -rf"`...

Атаки, проводимые с момента проверки до момента использования

```
if (access("./my document", W_OK) != 0) exit(1);
int fd = open("./my document", O_WRONLY);
write(fd, user_input, sizeof(user_input));
```

Инсайдерские атаки
Вредоносные программы
Средства защиты

Инсайдерские атаки

Логическая бомба —
фрагмент программного кода, созданный одним из работающих в компании программистов и тайно внедрённый в производственную систему.

Лазейка (back door)
Их создают системные программисты путем внедрения в систему такого кода, который позволяет обойти какую-нибудь обычную проверку.

```
while (TRUE) {
        printf("login: ");
        getstring(name);
        disableechoing( );
        printf("password: ");
        getstring(password);
        enableechoing( );
        v = checkvalidity(name, password);
        if (v) break;
}
executeshell(name);
```

```
while (TRUE) {
        printf("login: ");
        getstring(name);
        disableechoing( );
        printf("password: ");
        getstring(password);
        enableechoing( );
        v = checkvalidity(name, password);
        if (v || strcmp(name, "zzzzz") == 0) break;
}
executeshell(name);
```

Фальсификация входа в систему

Вредоносные программы

Троянские кони: Любой вредоносный код, спрятанный в программе или на веб-странице, которую пользователи открывают добровольно.

Вирусы: Программы, способные размножаться, присоединяя свой код к другим программам.

Черви: Программы, способные размножаться распространяясь по сети (используя уязвимости сетевого ПО).

Программы-шпионы: Тайно, без ведома собственника загружаются на его ПК и запускаются в фоновом режиме, выполняя несанкционированные действия.

Руткиты: Программы или наборы программ и файлов, пытающихся скрывать свое присутствие, даже если владелец зараженной машины прикладывает определённые усилия к их розыску и удалению. Как правило, руткиты содержат вредоносные программы, которые также скрыты.

Средства защиты: брандмауэры

Упрощённый вид аппаратного брандмауэра, защищающего сеть из трёх компьютеров

IP-адрес	Порт	Действие
207.68.160.190	80	Accept
207.68.160.191	25	Accept
207.68.160.192	21	Accept
*	*	Deny

Средства защиты: антивирусные технологии

- Программы поиска вирусов (сканирование)
  - Базы сигнатур, сжатие/декомпрессия, шифрование/расшифровка, полиморфные вирусы, детектирование мутационного механизма
- Программы проверки целостности файлов
  - Хранение контрольных сумм файлов, защита хранилища, подмена операций ввода-вывода
- Программы, контролирующие поведение
  - Перезапись boot-сектора? Перезапись исполняемого файла? (Или это компилятор?)
- Предотвращение проникновения вирусов
  - ЭЦП для ПО, отключение ненужных фич, резервное копирование