Лекция 22:
Обзор курса

Алексей Линёв
Александр Мощук
Кирилл Погорельский

somes slides are adapted from the OS course at the University of Washington

Поддержка со стороны аппаратного обеспечения

- Привилегированные инструкции
  - что это такое, кто может выполнять их?
  - как ЦП узнает, можно ли выполнять эти инструкции?
  - почему они должны быть привилегированными?
  - что управляется посредством привилегированных инструкций?
- События
  - исключения: кто их генерирует? чем отличается ловушка (trap) от сбоя (fault)?
  - прерывания: кто их генерирует?

Архитектура ОС

- Перечислите основные компоненты ОС?
- Как они структурированы?
  - чем отличаются монолитная, слоеная (многоуровневая) и микроядерная архитектуры?
    - преимущества и недостатки?

Процессы

- Что такое процесс? Виртуализованным представлением чего он является?
  - в чем отличие между программой, процессом и потоком?
  - что содержится в процессе?
    - что содержит дескриптор процесса?
  - что такое диаграмма состояний?
    - какие состояния и переходы возможны?
    - когда происходят переходы?
- Управление процессами
  - что делает fork()? exec()?
  - как работают командные интерпретаторы?

Потоки

- Что такое поток?
  - почему они полезны?
  - потоки пользовательского уровня vs. потоки ядра
- Чем отличается планирование потоков от планирования процессов?
  - что обеспечивает функционирование потоков?
  - что происходит при смене контекста потока?
  - что содержит дескриптор потока?
  - вытесняющее vs. невытесняющее планирование

Синхронизация

- Почему она необходима?
  - координация доступа к данным? координация выполнения?
  - что такое гонки? когда они возникают?
  - когда разделяются ресурсы? (переменные, объекты из кучи,…)
- Что такое взаимное исключение?
  - что такое критическая секция?
  - требования к реализации критических секций?
    - взаимное исключение, progress, граничное ожидание, производительность
  - какие механизмы используются при реализации критических секций?
    - признаки блокировки, семафоры, мониторы, условные переменные

Признаки блокировки и семафоры

- Что означает выражение "операции захвата/освобождения должны быть атомарными"?
- Как можно реализовать признаки блокировки?
  - активное ожидание? прерывания? планировщик?
  - test-and-set?
  - ограничения использования блокировок?
- Семафоры
  - P() и V()? семафоры и признаки блокировки?
  - когда потоки блокируются на семафорах? Когда они просыпаются?
  - использование кольцевого буфера
    - задача поставщик/потребитель
  - задача читатели/писатели

Планирование процессов

- Долгосрочное vs. краткосрочное планирование
- Когда работает планировщик?
  - создание задачи, изменение состояния задачи, прерывания, исключения
- Критерии оценки алгоритмов планирования
  - максимальная загрузка ЦП
  - максимальная пропускная способность
  - минимальное {оборотное время | время ожидания | время отклика}
  - пакетные системы vs. интерактивные системы: чем отличаются их назначение и задачи?
- Что такое голодание? Что является причиной голодания?
- FCFS/FIFO, SPT, SRPT, priority, RR, MLFQ…

Управление памятью

- Что положительного в использовании виртуальной памяти?
- Механизмы реализации виртуальной памяти
  - физические vs. виртуальные адреса
  - разбиение на разделы, страничное преобразование, сегментная адресация
  - таблицы страниц, TLB
- Стратегии замещения страниц
- Какие накладные расходы возникают при управлении памятью?

Виртуальное адресное пространство

- Чем отличаются виртуальные и физические адреса?
  - использование разделов фиксированного размера vs. использование разделов переменного раздела
    - регистры начала/предела…
    - внутренняя и внешняя фрагментация
- Страничное преобразование
  - преимущества, недостатки?
  - что такое таблицы страниц?
    - что такое: virtual page number? physical page number? offset? как эти термины соотносятся с виртуальными адресами?
    - что такое дескриптор страницы (PTE)? признаки изменения/обращения/корректности/прав доступа?

Страничное преобразование, TLBs

- Как уменьшить накладные расходы на использование таблиц страниц?
  - как работают многоуровневые таблицы страниц?
  - какую проблему решает TLB?
  - почему это работает?
  - что управляет TLB?
    - программное или аппаратное обеспечение?
- Страничные сбои
  - что это такое? как они используются для реализации замещения страниц по требованию?
  - какова полная последовательность шагов при трансляции виртуального адреса в физический адрес?
    - с учетом использования TLB и возможной подкачкой страницы с диска?
- Тонкости управления памятью
  - разделяемая память? файлы, отображаемые в память? копирование при записи?

Замещение страниц

- Что такое алгоритм замещения страниц?
  - какую особенность поведения приложений он использует?
  - когда вызывается алгоритм замещения?
- Основные моменты:
  - алгоритмы Белади (оптимальный), FIFO, LRU, приближения LRU, LRU clock
  - рабочее множество, частота страничных сбоев
  - что такое "режим постоянной подкачки"? когда и почему он возникает?

Жесткий диск

- Иерархия и "удаленность" памяти
- Физическая структура диска
  - пластины, поверхности, дорожки, сектора, цилиндры, штанги, головки
- Дисковый интерфейс
  - как ОС выполняет дисковые запросы?
- Производительность жестких дисков
  - время доступа = время поиска + время вращения + время передачи
- Планирование дисковых операций
  - как повысить производительность?
  - FCFS, SSTF, SCAN, C-SCAN?

Файлы и каталоги

- Что такое файл
  - какие операции поддерживаются?
  - какие характеристики имеет файл?
  - какие существуют методы доступа к файлу?
- Что такое каталог
  - для чего они используются?
  - как они реализованы?
  - что такое запись в каталоге?
- Как происходит разбор имени файла?
- Списки прав доступа vs. перечни возможностей
  - матрица
  - преимущества и недостатки обоих подходов

Размещение ФС на диске

- Основные части файловой системы?
- Основные стратегии?
  - непрерывные файлы, связные списки, использование индексов?
  - компромиссы?
- Что такое i-node?
  - чем они отличаются от каталогов?
  - как i-nodes и каталоги используются при разборе имен и поиске файлов?
- Что такое буферный кэш?
  - почему ОС использует его?

FFS, LFS

- Что такое FFS, чем именно она лучше оригинальной файловой системы UNIX?
- Что такое LFS, на каких идеях она базируется, в каких случаях следует ее использовать, в каких – не стоит?

RAID

- RAID: основные понятия
  - распределение файлов по нескольким дискам для повышения производительности
  - компенсирует потери из-за обеспечения надежности посредством использования кодов корректировки ошибок или контроля четности
- Преимущества использования различных типов дисковых массивов от RAID-0 до RAID-5

Сетевые технологии

- Семиуровневая модель ISO/OSI
- Ethernet
- Протокол IP и маршрутизация
- Протокол TCP (доставка книги на почтовых открытках)
- Инкапсуляция протоколов

RPC

- Основная идея – в чем преимущество RPC перед использованием передачи сообщений?
- Термины и положения: IDL (interface definition language), заглушки, генерация заглушек, размещение параметров и результатов, привязка, механизм доставки подсистемы RPC runtime, обработка ошибок, производительность, множества потоков (thread pools)
- Прозрачность: когда распределенная природа RPC, и когда – нет?

Распределенные системы

- Loosely-coupled (слабо связанные)
- Closely-coupled (сильно связанные)
- Tightly-coupled (плотно связанные)
- Grapevine как пример распределенной системы

Распределенные файловые системы

- Вопросы:
  - основная абстракция, способ именования, кэширование, предоставление в общее использование и когерентность
- Примеры – сходство и отличия
  - NFS
  - AFS
  - Sprite

Атаки через переполнение буфера

- Основная идея атаки через переполнение буфера
- Подробности – как именно вы бы написали эксплойт для архитектуры x86?