

Курс «Распределённые системы»

ЮФУ, мехмат, Информационные технологии, 3.11

Программа курса

Основы сетевого взаимодействия

Сокеты и сетевое программирование. Интерфейс сокетов Беркли, общая структура клиента и сервера, адресация сокетов. Объектная декомпозиция интерфейса сокетов Беркли. Сетевое программирование в языке Java. Сетевое программирование в языке C++: библиотека Boost.Asio.

Эффективное сетевое взаимодействие. Проблемы использования блокирующих вызовов. Механизмы неблокируемого ввода/вывода. Обзор серверных архитектур: последовательные, параллельные, активно-превентивные (проактивные) и взаимно-согласованные (реактивные) серверы. Метод опроса каналов и его реализация в языке Java: основные понятия, структура сервера, буферы, каналы и селекторы, хранение состояния клиента на сервере. Асинхронное взаимодействие в библиотеке Boost.Asio: основные понятия, структура сервера, операции, события и обработчики, асинхронный клиент HTTP, хранение состояния клиента на сервере.

Проектирование сетевых протоколов. Понятие сетевого протокола, типы сетевых протоколов, структура сообщений, примеры сообщений разных протоколов. Порядок обмена сообщениями, примеры. Стратегии завершения соединения, примеры.

Организация распределённых систем

Основные понятия распределённых систем. Определение и основные характеристики распределённых систем. Формы прозрачности и открытости, проблемы и технологии масштабирования. Реализация распределённых систем на базе сетевых операционных систем и промежуточного программного обеспечения. Открытость и промежуточное ПО.

Связь в распределённых системах. Проблемы низкоуровневых методов организации связи. Вызов удалённых процедур: основные понятия и приёмы, проблемы передачи данных, асинхронные вызовы. Системы удалённых объектов: принципы организации, передача удалённых объектов как параметров, удалённые объекты в технологии Java RMI. Технологии XML и веб-сервисы. Коммуникационные системы на базе передачи сообщений: сохранность и синхронность, нерезидентная передача сообщений, сохраняемая передача сообщений, очереди сообщений.

Процессы в распределённых системах. Процессы и их роли. Перенос кода: основные модели, отношения с локальными ресурсами. Программные агенты: свойства, виды, платформы, онтологии и протоколы взаимодействия.

Именованное. Способы именования сущностей в распределённой системе, пространства имен и их распределение, процесс разрешения имен. Система доменных имен и служба каталогов X.500. Проблема локализации мобильных сущностей, поиск и перемещение, масштабирование служб локализации, удаление данных об устаревших сущностях.

Распределённые алгоритмы

Время в распределённых системах. Проблемы определения времени, состояния процессов, понятие события, отметки времени. Методы синхронизации физических часов: внешняя и внутренняя синхронизация, алгоритм Кристиана, алгоритм Беркли, протокол NTP. Логические часы: отметки времени и упорядочение событий, отношение предшествования, причинность, параллельные события, логические часы Лампорта и их свойства, векторные отметки времени.

Координация процессов. Понятие координатора и алгоритмы голосования. Алгоритмы реализации взаимного исключения и их сравнение.

Непротиворечивость данных и репликация. Модели непротиворечивости хранилищ данных: строгая, линеаризованная, последовательная, причинная, FIFO. Модели непротиворечивости с синхронизацией: слабая, свободная и поэлементная. Модели непротиворечивости, ориентированной на клиента: монотонное чтение, монотонная запись, чтение собственных записей, запись за чтением. Репликация данных: типы реплик, примеры, способы и стратегии распространения обновлений, эпидемические протоколы, антиэнтропия и «распространение слухов».

Отказоустойчивость. Понятия надёжной системы, ошибки и отказы, модели отказов, избыточность. Группирование процессов, маскировка ошибок и репликация, соглашения в системах с ошибками (проблема двух армий, проблема византийских генералов). Надёжность клиент-серверной связи, проблемы RPC-взаимодействия, семантика ошибок.

Защита информации. Конфиденциальность и целостность, угрозы защиты, политики безопасности, механизмы защиты. Фокус управления и многоуровневая архитектура в системах защиты распределённых систем. Понятие защищенного канала. Методы аутентификации: системы с закрытым ключом, упрощенная схема и атака на отражении, центры распространения ключей, понятие талона, протокол Нидхема—Шрёдера, системы с открытыми ключами. Цифровые подписи. Авторизация и контроль доступа к объектам: матрица контроля доступа, списки ACL и мандаты, способы защиты объектов, брандмауэры. Управление ключами: обмен ключами по Диффи—Хеллману, распространение секретных и открытых ключей, сертификаты открытого ключа. Создание защищенного канала и аутентификация в Kerberos. Защита электронных платежных систем.

Литература

1. Э. Таненбаум. Распределённые системы: принципы и парадигмы.
2. К. Хорстманн, Г. Корнелл. Java 2.
3. В. Н. Брагилевский, А. М. Пеленицын. «Основы многопоточного и сетевого программирования».
4. Раздел курса «Распределённые системы» на сайте <http://edu.mmcs.sfedu.ru/>.
5. Документация к библиотеке Boost.Asio.

Вопросы к экзамену

1. Интерфейс сокетов Беркли, клиенты и серверы, объектная декомпозиция.
2. Сетевое программирование в Java: основные классы и их методы.
3. Метод опроса каналов и его реализация в Java.
4. Библиотека Boost.Asio: основные классы и методы блокирующих операций.
5. Реализация асинхронного взаимодействия в Boost.Asio.
6. Проектирование сетевых протоколов.
7. Прозрачность, открытость и масштабируемость распределённых систем.
8. Основания для реализации распределённых систем.
9. Вызов удалённых процедур.
10. Системы удалённых объектов, веб-сервисы.
11. Технология Java RMI.
12. Системы передачи сообщений.
13. Перенос кода.
14. Программные агенты.
15. Именованное пространство в распределённых системах, службы DNS и X.500.
16. Локализация мобильных сущностей.
17. Понятие времени, синхронизация физического времени.
18. Логическое время и расстановка отметок времени.
19. Алгоритмы координации процессов.
20. Модели непротиворечивости хранилищ данных без синхронизации.
21. Модели непротиворечивости хранилищ данных с синхронизацией.
22. Модели непротиворечивости, ориентированные на клиента.
23. Репликация данных и распространение обновлений.
24. Основные понятия, проблемы и приемы реализации отказоустойчивости.
25. Семантика ошибок при RPC-взаимодействии.
26. Основные понятия защиты распределённых систем.
27. Организация защищённых каналов.
28. Авторизация и контроль доступа к объектам.
29. Методы управления ключами.
30. Система Kerberos.
31. Защита систем электронных платежей.