**Leopoldo Ferreira de Paula**

1. Cite 3 tipos de recursos de hardware e recursos de dados ou software que possam ser compartilhados com sucesso. Dê exemplos de seu compartilhamento em sistemas distribuídos.

De Hardware: Usb, impressoras, servidores.

De Software: apks, docs e xmls.

Docs podem ser compartilhado e editado ao mesmo tempo através do google docs.

1. Considere as estratégias de implementação de jogos online(MMOG). Em particular, quais vantagens você vê em adotar a estratégia de servidor único para representar o estado do jogo para vários jogadores? Quais problemas você consegue identificar e como eles poderiam ser resolvidos?

Servidor único traz muita consistência nos dados, segurança e evita complexidade da comunicação entre vários servidores. Problemas de conexão. MMOs exigem trafego de dados constante, caso o jogador esteja muito longe do servidor, gera o famigerado delay, ou lag, a solução é usar mais servidores, e otimizar as rotas do tráfego de dados.

1. Liste os três principais componentes de software que podem falhar quando um processo cliente invocar um método em um objeto servidor. Dê um exemplo de falha para cada caso. Sugira a maneira como os componentes podem ser feitos para tolerar falhas uns dos outros.

Pode acontecer de uma requisição não ser atendida por ter muito tráfego na rede, demorar muito a resposta por diversos motivos ou a mesma requisição por diferentes clientes, portanto, uma rede deve condizer com a necessidade do ambiente e possuir recursos para caso algum desses problemas ocorram.

1. Frequentemente, os computadores usados nos sistemas *peer-to-peer* são computadores *desktop* nos escritórios ou nas casas de usuários. Quais são as implicações disso na disponibilidade e segurança dos objetos de dados compartilhados que eles contêm e até que ponto qualquer vulnerabilidade pode ser superada por meio de replicação?

O peer do peer acontece sem um mediador, ninguém precisa estabelecer essa conexão, dar o “ok” das máquinas que irão comunicar entre si, e com isso, há uma grande possibilidade de que essa falta de controle gere experiências negativas como vírus e replicação, portanto, deve-se usar peer-to-peer através de softwares que prezam pela segurança.

1. Para cada um dos fatores que contribuem para o tempo gasto para transmitir uma mensagem entre dois processos por um canal de comunicação, cite quais medidas seriam necessárias para estabelecer um limite para sua contribuição no tempo local. Por que estas medidas não são tomadas nos sistemas distribuídos de propósito geral?

A transmissão é dada por diversas verificações e requisições que tomam tempo, o tempo do usuário se conectar na rede, requisitar, da verificação se pode mandar, de colocar na fila pra mandar, tempo de viagem, chegada, etc. Tudo pode ser acelerado desde que hajam profissionais que consigam modificar e melhorar a rede, porém, o custo para acelerar todos esses tempos, não valem a demora na requisição de um arquivo.

1. Considere dois serviços de comunicação para uso em sistemas distribuídos assíncronos. No serviço A, as mensagens podem ser perdidas, duplicadas ou retardadas e somas de verificação se aplica apenas aos cabeçalhos. No serviço B, as mensagens podem ser perdidas, retardadas ou entregues rápido demais para o destinatário manipulá-las, mas sempre chegam com o conteúdo correto.

Descreva as classes de falha exibidas para cada serviço. Classifique suas falhas de acordo com seu efeito sobre as propriedades de validade e integridade. O serviço B pode ser descrito como um serviço de comunicação confiável?

A: Falhas arbitrárias. Por causa da duplicação, a integridade é comprometida.

B: Falhas por omissão. Tem integridade, porém não é confiável.

1. Considere os dois processo X e Y que utilizam o serviço de comunicação do exercício 6 para se comunicar entre si. Suponha que X seja um cliente e que Y um servidor e que uma invocação em uma mensagem de pedido de X para Y, seguida de Y executando o pedido, seguida de um a mensagem de resposta de Y para X. Descreva as classes de falha que podem ser exibidas por uma invocação.

Pode sofrer as seguintes falhas:

X ou Y pode falhar. Portanto, uma invocação pode sofrer falhas de “crash”.

Omissão, como o serviço B sofre de falhas de omissão as mensagens de pedido ou resposta podem ser perdidas.

1. Suponha que uma leitura de disco possa às vezes ler valores diferentes dos gravados. Cite os tipos de falha exibidos por uma leitura de disco. Sugira como se faz para mascarar a falha benigna.

Gera falhas arbitrárias

Isso pode ser mascarado usando checksum em cada bloco de disco (tornando improvável que

valores errados não sejam detectados) . Quando um valor incorreto é detectado, a leitura

retorna nenhum valor em vez de um valor errado (uma falha de omissão).

As falhas de omissão podem ser mascaradas replicando cada bloco de disco em dois discos

independentes o que tornar falhas de omissão improváveis.

1. Defina a propriedade de integridade da comunicação confiável e liste as ameaças possíveis à integridade dos usuários e dos componentes do sistema. Quais medidas podem ser tomadas para garantir a propriedade de integridade diante dessas fontes de ameaças.

Integridade: a mensagem recebida é idêntica à enviada e nenhuma mensagem é entregue

mais de uma vez.

Ameaças dos usuários:

-injectar mensagens falsas, reproduzir mensagens antigas, alterar mensagens durante a

transmissão.

Ameaças de componentes do sistema:

-mensagens podem ser corrompidas no caminho.

-mensagens podem ser duplicadas por protocolos de comunicação que retransmitem as

mensagens.

Medidas que podem ser adotadas:

Para ameaças de usuários - use canais seguros ou técnicas de autenticação.

Para ameaças de componentes do sistema. Checksums para detectar mensagens corrompidas

- mas depois temos um problema de validade (mensagem perdidas). As mensagens duplicadas

podem ser detectadas se números de sequência forem anexados a mensagens.

1. Descreva as possíveis ocorrências dos principais tipos de ameaças à segurança (ameaças aos processos, ameaças aos canais de comunicação, negação de serviço) que poderiam ocorrer na Internet.

Ameaças aos processos: sem autenticação servidores, existem muitas ameaças. Um inimigo

pode acessar os arquivos ou caixas de correio de outros usuários ou configurar servidores

'spoof'. Por exemplo. Um servidor pode ser configurado para 'spoof' serviço de um banco e

receber detalhes de transações financeiras do usuário.

Ameaças aos canais de comunicação: IP spoofing - enviar solicitações para servidores com um

endereço de fonte falsa, ataques man-in-the-middle.

Negação de serviço: inundar um serviço publicamente disponível com mensagens irrelevantes.