

2.1 - Hardware: os sistemas distribuídos são cada vez mais heterogêneos com PCs (geralmente baseados em Intel), smartphone, rede de servidores de recursos limitados e computadores com clusters de recursos em processadores de vários núcleos.

S.O: um sistema distribuído pode incluir computadores com windows, MAC OS, vários tipos diferentes de Unix e também muitos sistemas operacionais especializados para smartphones ou móveis de servidores.

Redes: a Internet também é cada vez mais heterogênea abrangendo tecnologias sem fio e estendendo ad-hoc as redes.

2.2 - ~~Revisão de Redes Distribuídas~~

Exemplo a Web: Os navegadores são clientes de servidores de Names de Domínio (DNS) e servidores web (HTTP). Alguns intranets são configuradas para interpor um servidor proxy. Os servidores proxy empregam rotas proprietárias - quando estas localizadas no mesmo local que o cliente, reduzem os atrasos da

rede. Quando eles estão no mesmo ritmo que o servidor, eles formam um ponto de verificação de segurança e podem reduzir a carga no servidor.

2.2 - O cliente e o servidor estão intimamente ligados, o que dificulta a flexibilidade na gestão de falhas e mudanças. É mais difícil operar em ambientes voláteis, onde algumas unhas das partes podem estar indisponíveis. O desacoplamento espacial proporciona mais liberdade para lidar com mudanças, permitindo que novos servidores assumam rotatões. O desacoplamento de tempo permite que as entidades comuniquem quando necessário, independentemente da disponibilidade.

2.4 - As páginas da Web são armazenadas em um único servidor, mas a Web, muitas vezes populares, podem usar replicação para manter várias cópias idênticas. As solicitações HTTP podem ser distribuídas entre servidores usando compartilhamento de carga.

PNS ou servidores proxy com réplicas em cache. Os navegadores também replicam páginas com um cache local

2.5 - A sincronização necessária é alguma sistema de locking para os índices de cache. Os clientes estão requisitando informação deles enquanto o crawler está alimentando-o com informações. ~~deles~~ Para evitar que o índice seja corrompido, o crawler deve bloquear as áreas do índice em que ele vai modificar / adicionar ou remover entradas.

2.6 - Como os sistemas querem que funcione de maneira que as máquinas não dividem e sejam no mesmo tempo, existe uma abertura no firewall do computador que diz a máquina mais vulnerável quando está conectada por um sistema. A integridade dos recursos compartilhados para ver um problema sério nesse meio

2.7 - Podem ser vulneráveis tanto o sistema operacional quanto os programas e aplicativos instalados no computador do usuário, os arquivos de dados, textos, planilhas, imagens e outros, assim como os dispositivos locais do computador do usuário e seus dispositivos remotos, aos quais se esteja conectado.

2.8 - Podem ilustrar exemplos, com instalação e utilização de programas pela internet, software de auditoria computacional e de gerenciamento de configuração, atendimento sob demanda de notícias, imagens multimídia, áudios, entre outras fontes.

2.9 - Uma solução de três níveis consiste em:

1. ~~O~~ Um gerant-end que fornece a interface do usuário para o cliente de aluguel de carros (lógica de apresentação).
2. Um nível intermediário que reporta operações de negócios, como locação de carros, verificação de disponibilidade e preços, geração de orçamento e compra (lógica de aplicação)

3. Um banco de dados que armazena dados persistentes relacionados ao topo (logica de dados)

2.10 - O argumento de end-to-end de Saltzer afirma que as funções de comunicação só podem ser implementadas com sucesso com o conhecimento e a ajuda da aplicação. Portanto, considerar suas funções como parte do sistema de comunicação (hardware) não sempre é correto. Um exemplo disso é a comunicação segura, onde apenas fornecer criptografia no software de comunicação não é suficiente, pois o caminho entre o usuário e o software de aplicação pode ser comprometido. Além disso, medidas como a proteção de checksum em rotas individuais na rede não abordam adequadamente a corrupção de dados por má intermediação ou sistemas finais.

2.11 - A tweca provável de chegada de pedidos de clientes pode causar problemas para os servidores. Um ataque pode executar solicitações simultaneamente, podendo resultar em falta de tempo para

atender a um pedido dentro de um limite de tempo. Colocar as reuniões em fila e executá-las uma de cada vez pode causar espera indesejável.

A solução é limitar o número de clientes de acordo com a capacidade da rede, mas resultaria com mais procuradores para lidar com mais clientes. A replicação contínua do serviço é outra opção, mas pode não causar redução no número de procuradores disponíveis para atender reuniões desejadas e manutenção de réplicas caras.

2.12 - No sistema sincrono existe um limite de tempo finito e conhecido, dependente do sistema sincrono que não existe um limite de tempo. É impossível determinar se o sistema está simplesmente abarrotado por sobrecarga ou se está com defeito.

2.13 - Qualquer cliente que utilize o serviço NTP deve comunicar com ele por meio de mensagens paradas por um canal de comunicação.

É um limite por definido no momento que transmite uma mensagem através de um canal de comunicação. ~~Sendo transmitida~~
então a diferença entre o relógio do cliente e o valor fornecido pelo serviço NTP também será limitada. Com um tempo de transmissão de mensagens limitado, as diferenças de relógios são necessariamente limitadas.

2.14 - O serviço A pode ter: falhas arbitrárias:

- como os checksums não são aplicados nos corpos das mensagens, estes podem ser corrompidos
- Mensagens duplicadas, juntas de amíão (mensagens perdidas). Como é usado é um sistema distribuído sincronizado, ele não pode reparar de falhas de temporização

O serviço B pode ter:

- falhas de amíão

2.15 - Uma invocação pode reparar os seguintes falhos: Falhar de verificá-lo X ou Y pode falhar. Portanto, uma invocação pode reparar falhos de verificação de omnínio: caso o serviço B não responda devido a um erro de aplicação ou resposta perdida

2.16 - Uma leitura básica de disco aparenta falhos arbitrários. Isto pode ser evitado marcando um checksum em cada bloco de disco. Tornando impraticável que valores errados não sejam detectados. Quando um valor incorreto é detectado, a leitura retorna um valor em vez de um valor errado. Os falhos de omnínio podem ser evitados replicando cada bloco de disco em dois discos independentes de que forma falhos de omnínio impossíveis.

2.17 -

2.18 - Invadir os serviços: rev autenticacão
servidores, existir muitos arquivos. Um invasor
pode aceder os arquivos ou caixas de correio de
outras máquinas ou configurar servidores (spoof).

Por exemplo, um serviço de um banco a receber
detalhes de transações financeiras do usuário.
Invasor nos canais de comunicação: IP spoofing
- enviar solicitações para servidores com um
endereço de fonte falso; ataque man-in-the-middle
negócio de serviço: invadir um serviço pub-
blicamente disponivel com mensagens ironicamente