Sistemas Distribuídos

Modelos Fundamentais
Modelo de Falhas e Segurança

Altamira de Souza Queiroz

Modelo de Falhas

- Os processos e canais de comunicação podem falhar.
- Quais falhas podem ocorrer e suas consequências.
  - falhas de processos e falhas dos canais de comunicação.
- O modelo de falhas define os modos nos quais, falhas podem ocorrer, para prover um entendimento dos efeitos das falhas.
  - falhas por omissão
  - falhas arbitrárias
  - falhas de sincronização.

Falhas por Omissão de Processos

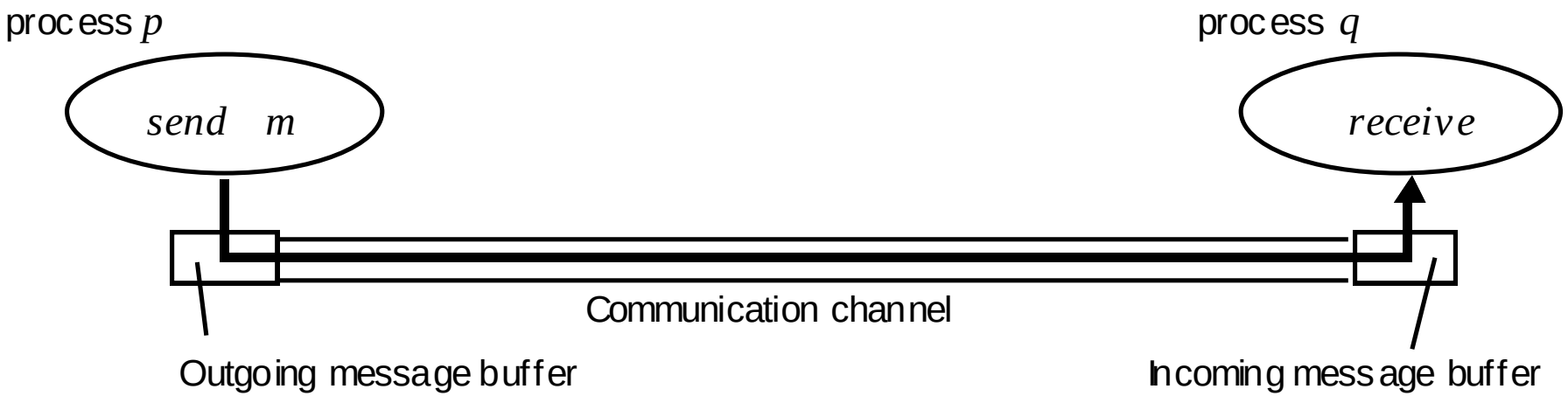
- A principal falha é quando o processo entra em colapso.
- O projeto de serviços simplificado assume-se que os processos poderão entrar em *colapso*.
- O processo repetidamente falha para responder a mensagens de invocação.
- o método de detecção é baseado no uso de *timeouts*
  - Sist. Assíncronos: o processo não está respondendo.
  - Sistemas síncronos: detectar quando outros processos deixam de responder a mensagens entregues.

Falhas por Omissão Processos

- Um exemplo:
  - o processo *q* responder a uma mensagem de *p*,
  - se o processo *p* não recebe nenhuma resposta de *q*,
  - então o processo *p* pode concluir que o processo *q*, falhou.

Falhas por Omissão de Comunicação

- Considere as primitivas de comunicação *send* e *receive*.
- Os buffers são fornecidos pelo sistema operacional.



Falhas por Omissão na Comunicação

- *Perda de mensagens*
  - falta de espaço no buffer do receptor,
  - por um erro de transmissão.
- Falhas por omissão de envio
- Falhas por omissão de recepção
- Falhas por omissão de canal

Falhas Arbitrárias

- o pior dos casos possíveis na semântica de falhas.
  - Um processo pode estabelecer valores errados em seus itens de dados
  - O processo podem retornar um valor errado em resposta a uma invocação.
- Falha arbitrária de um processo.
- Canais de comunicação podem sofrer de falhas arbitrárias:
  - o conteúdo de mensagens pode ser corrompido,
  - ou mensagens não-existentes podem ser entregues,
  - ou mensagens reais podem ser entregues mais de uma vez.

Falhas Arbitrárias

- Falhas arbitrárias de canais são raras, porque o software de comunicação (protocolos) é capaz de reconhecer falhas e rejeitar as mensagens com falha.

- *Checksums* são usados para detectar mensagens corrompidas,

- Numeração das mensagens são usadas para detectar mensagens não existentes ou mensagens duplicadas.

Falhas de Temporização

- Aplicadas a Sistemas Distribuídos Síncronos, onde os limites de tempo são estabelecidos:
  - tempo de execução de processos
  - tempo de entrega de mensagens
  - Desvio do relógio (*clock drift rate).*
- Resulta em respostas não disponíveis a clientes, dentro de um intervalo de tempo especificado.
- Em SD assíncrono não há falha de temporização.

Falhas de Temporização

- Temporização é mais relevante em sistemas multimídia, com áudio e canais de vídeo.
- Informações de vídeo podem requerer uma quantidade muito grande de informação sendo transmitida.
- Impõe exigências especiais sobre o sistema operacional e o sistema de comunicação.

Mascaramento Falhas

- É possível construir serviços confiáveis, mas na presença de componentes que exibem falhas.
- Exemplo: múltiplos servidores que armazenam réplicas de dados, podem continuar a prover um serviço, quando um dos servidores entra em colapso.
- Um conhecimento das características da falha de um componente
  - Oculta a falha completamente
  - Converte a falha em um tipo mais aceitável.

Mascaramento Falhas

- *Checksums*
  - falha arbitrária
  - falha por omissão
  - Retransmissão da mensagem
- Replicação
- Novo processo

Confiabilidade de Comunicação Um-a-Um

- Canal de comunicação básico - falhas por omissão
  - serviço de comunicação que mascare algumas das falhas.

- Comunicação confiável
  - Validade: qualquer mensagem no *buffer de saída* é **eventualmente** entregue ao *buffer de entrada*.
  - Integridade: a mensagem recebida é idêntica a aquela enviada, e nenhuma mensagem é entregue duas vezes.

Confiabilidade de Comunicação Um-a-Um

- As ameaças para a **integridade** vem de duas fontes independentes:

  I. Qualquer protocolo que retransmite mensagens, mas não rejeita uma mensagem que chega duas vezes.

  II. Usuários maliciosos que podem injetar mensagens espúrias, repetem mensagens antigas ou falsificar mensagens.

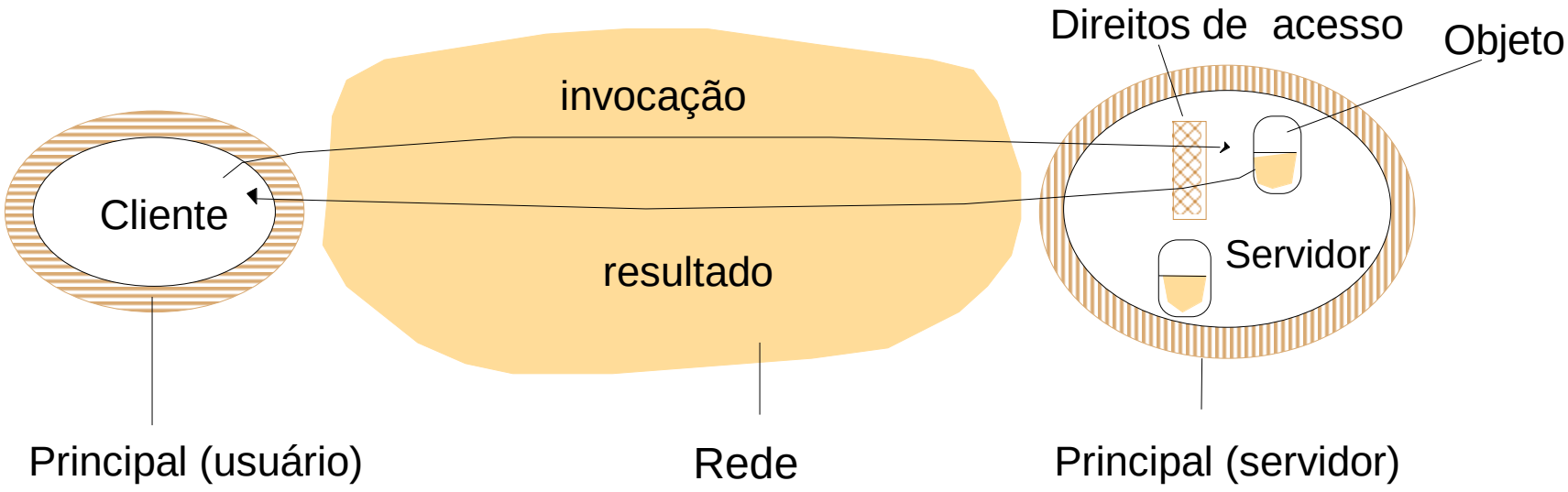
Modelo de segurança

- Compartilhamento de recursos: motivador de SDs
  - Através de processos que interagem com outros processos.
  - Processos: objetos encapsulados.
- A segurança de um SD: contra acesso não autorizado.
- A proteção é descrita por objetos

Proteção de objetos

- Os objetos são usados de diversas formas, por diversos usuários
  - dados privativos como caixa de correio.
  - Dados compartilhados como páginas Web.
- Direitos de acesso dão suporte como usá-los
  - P. ex. quem pode ler ou gravar em seu estado
- usuários = beneficiários, no modelo de segurança
  - Associa a cada invocação e a cada resultado, o tipo de autorização de quem a executa

Proteção de objetos



Processos e interações seguros

- Os processo interagem enviando mensagens.
- As mensagens ficam expostas a ataques.
- Servidores e processos peer-to-peer publicam suas interfaces para que invocações sejam enviadas.
- Frequentemente os SDs são implementados e usados em tarefas sujeitas a ataques externos

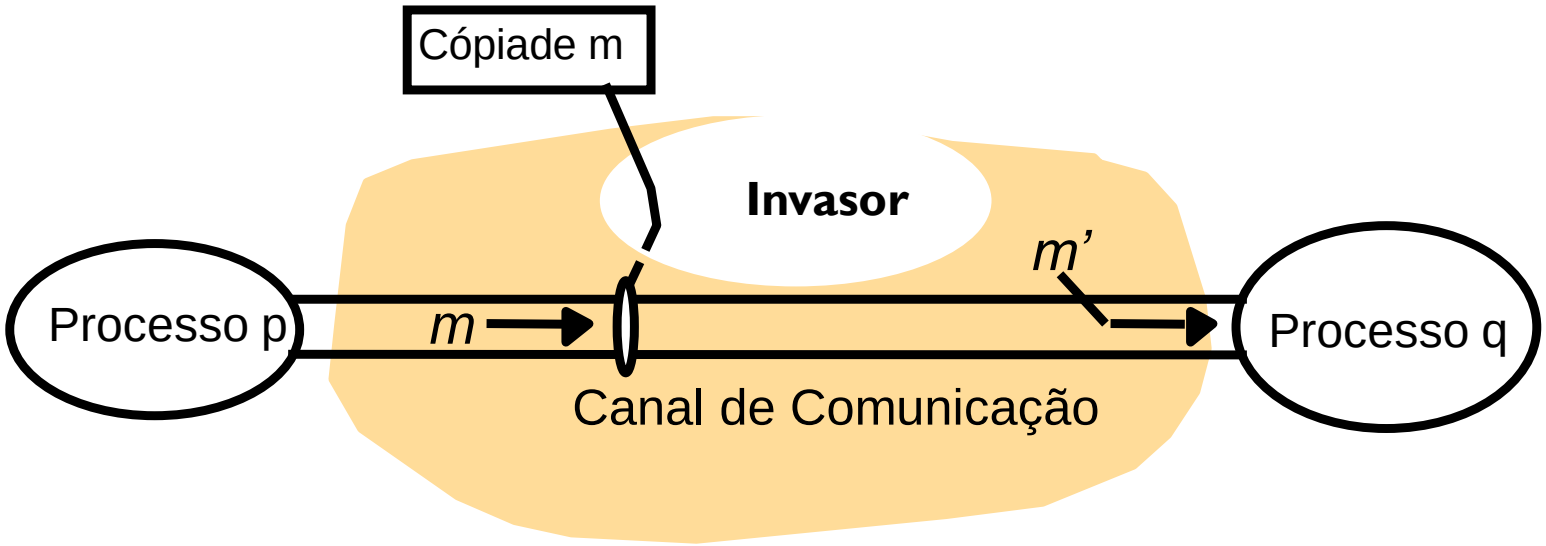
Processos e interações seguros

- A integridade é ameaça por violações de segurança como falhas de comunicação
  - Existem prováveis ameaças aos processos e as mensagens que trafegam entre eles
  - Como podemos analisar essas ameaças para identificá-las e anulá-las?

O invasor

- Capaz de enviar qualquer mensagem para qualquer processo e ler ou copiar qualquer mensagem entre dois processos.
  - Programa que lê mensagens endereçadas a outro computador da rede
  - Programa que gera mensagens de pedidos falsos de usuários atualizados.
  - O ataque pode vir de computador conectados a rede de maneira legítima ou não autorizada.

O invasor



- As ameaças do invasor são:
  - Ameaças aos processos
  - Ameaças aos canais de comunicação
  - Negação de serviço

Ameaças aos processos

- Processos que não sejam capazes de identificar o remetente.
  - Ex. protocolo IP coloca o endereço de origem.
- Falta de reconhecimento
  - Servidor: pode não determinar a identidade do principal ou uso de identidade falsa
  - Clientes: quando recebe o resultado de um servidor e não identifica a origem da mensagem.

Ameaças as canais de comunicação

- Cópia, alteração ou injeção de mensagens
- Ameaça a integridade e a privacidade das informações.
- Outra forma é a tentativa de salvar cópias de mensagens e reproduzi-las posteriormente.
  - Solicitação de transferência entre contas.
- Solução: criptografia e autenticação.

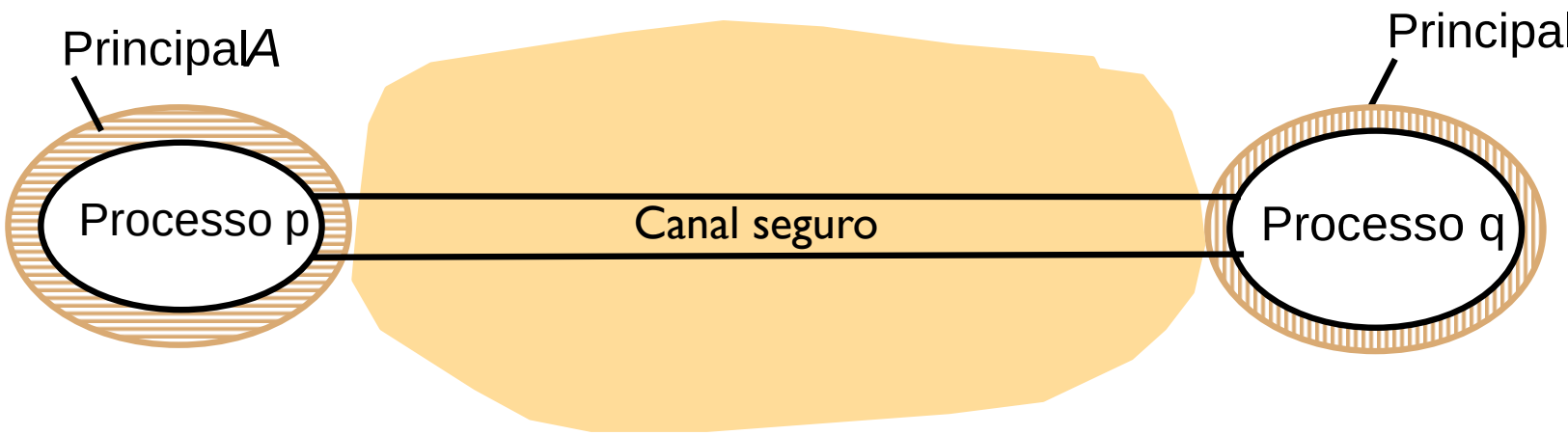
autenticação

- Provar as identidades dos remetentes
- Técnica básica é incluir na mensagem uma parte cifrada para garantir sua autenticidade.
  - P. ex. pedido de leitura de um arquivo.
  - Inclui a identidade do principal, a id. do arquivo e data e hora do pedido, tudo cifrado.
  - decifraria o pedido e verificaria se os mesmo correspondem realmente ao pedido.

Canais seguros

- Criptografia e autenticação como uma camada de serviço sobre os serviços de comunicação existentes.
- Propriedades:
  - Cada processo conhece com certeza a identidade do principal
  - Garante integridade e privacidade
  - Cada mensagem inclui uma indicação de relógio lógico ou físico, para impedir reprodução ou reordenação das mensagens.

Canais seguros



- Importante ferramenta prática para proteger o comércio eletrônico
  - VPN e o protocolo SSL
- Outras ameaças: DoS e código móvel.

Uso dos modelos de segurança

- Pode-se pensar que a obtenção de segurança em SD seria uma questão simples.
  - Controle do acesso a objetos e uso de canais seguros
- Custos de processamento e de gerenciamento substanciais.
- Os custos são mantidos em um mínimo.
- Análise nos ambientes da rede, físico e humano
- A eficácia e o custos das técnicas podem ser ponderadas em relação às ameaças.