

Sistemas Distribuídos

Modelos Fundamentais
Prof. Tales Viegas

<https://facebook.com/ProfessorTalesViegas>

Modelos Fundamentais

- ▶ Os Sistemas Distribuídos podem ainda ser analisados segundo 3 aspectos transversais a todos os sistemas:
 - Modelo de Interação (ou de sincronismo)
 - Modelo de Falhas (ou avarias)
 - Modelo de Segurança

1 – Modelo de Interação

- ▶ Interação é a ação (comunicação e sincronização) entre as partes para realizar um trabalho qualquer.
- ▶ É afetada por dois aspectos:
 - Performance dos canais de comunicação
 - Inexistência de um tempo global

Performance – Latência

- ▶ “*Intervalo de tempo entre o início da transmissão de uma mensagem por um processo e o início da sua recepção pelo outro processo*”
- ▶ Depende de:
 - Demora (“delay”) de transmissão pela rede
 - Tempo requerido pelo SO em ambos os lados da comunicação
 - Demora no acesso aos recursos da rede

Performance – Largura de Banda

- ▶ “Bandwidth”
- ▶ “*Total de informação que pode ser transmitida pela rede em um dado tempo*”

Performance – Jitter

- ▶ *Variação no tempo necessário para enviar grupos de mensagens consecutivos constituintes de uma informação transmitida de um ponto para outro na rede*
- ▶ Importante na transmissão de som e imagem
- ▶ As vezes é mais prejudicial utilizar buffer do que perder alguns pacotes.

Inexistência de um tempo global

- ▶ Cada computador tem um relógio “clock” interno
- ▶ Cada relógio tem um drift (desvio) do tempo de referência
- ▶ Os drifts de dois relógios distintos, também são distintos (o que significa que o tempo entre eles sempre será divergente)

Inexistência de um tempo global

- ▶ Uma solução passa por obter o tempo fornecido por GPS (Global Positioning System) e enviar aos participantes do Sistema Distribuído
- ▶ Problema: Delays no envio desta mensagem

Variantes no Modelo de Interação

- ▶ Sistemas Distribuídos Síncronos
- ▶ Sistemas onde podem existir limites máximos de tempo conhecidos para:
 - Tempo de execução dos processos
 - Atrasos na comunicação
 - Variações no tempo de referência

Variantes no Modelo de Interação

- ▶ Sistemas Distribuídos Síncronos
- ▶ Se:
 - O tempo necessário para executar cada passo de um processo tem um limite inferior e um limite superior conhecidos
 - Cada mensagem transmitida por um canal é recebida dentro de um limite de tempo conhecido
 - Cada processo tem um relógio cujo desvio máximo para o tempo de referência é conhecido
- ▶ Podem ser definidos “timeouts” para detectar falhas

Variantes no Modelo de Interação

- ▶ Sistemas Distribuídos Assíncronos
- ▶ Não possui limites para:
 - Tempo de execução dos processos – cada passo de execução pode levar um tempo arbitrariamente longo
 - Tempo de transmissão de mensagens – uma mensagem pode chegar rapidamente ou demorar dias
 - O desvio para o tempo de referência pode ser qualquer

Variantes no Modelo de Interação

- ▶ Sistemas Distribuídos Assíncronos
- ▶ Exemplo: Internet
- ▶ Como lidar com longos tempos de espera:
 - O sistema pode avisar o usuário que o tempo de espera pode ser longo e solicitar uma alternativa
 - O sistema pode dar oportunidade para o usuário fazer outras coisas
 - ...

Ordenação dos Eventos

- ▶ Por vezes é importante conhecer a ordem pela qual ocorreu um conjunto de eventos
- ▶ Exemplo 1:
 - Sejam os usuários X, Y, Z e A que trocam e-mails para marcar uma reunião
 - X envia uma mensagem com o assunto: “Reunião” para Y, Z e A
 - Y e Z respondem para os outros com o assunto “Re: Reunião”

Ordenação dos Eventos

- ▶ Uma vez que não há limites no tempo de comunicação, as mensagens pode ser entregues de tal forma que o usuário A receba as mensagens pela ordem:

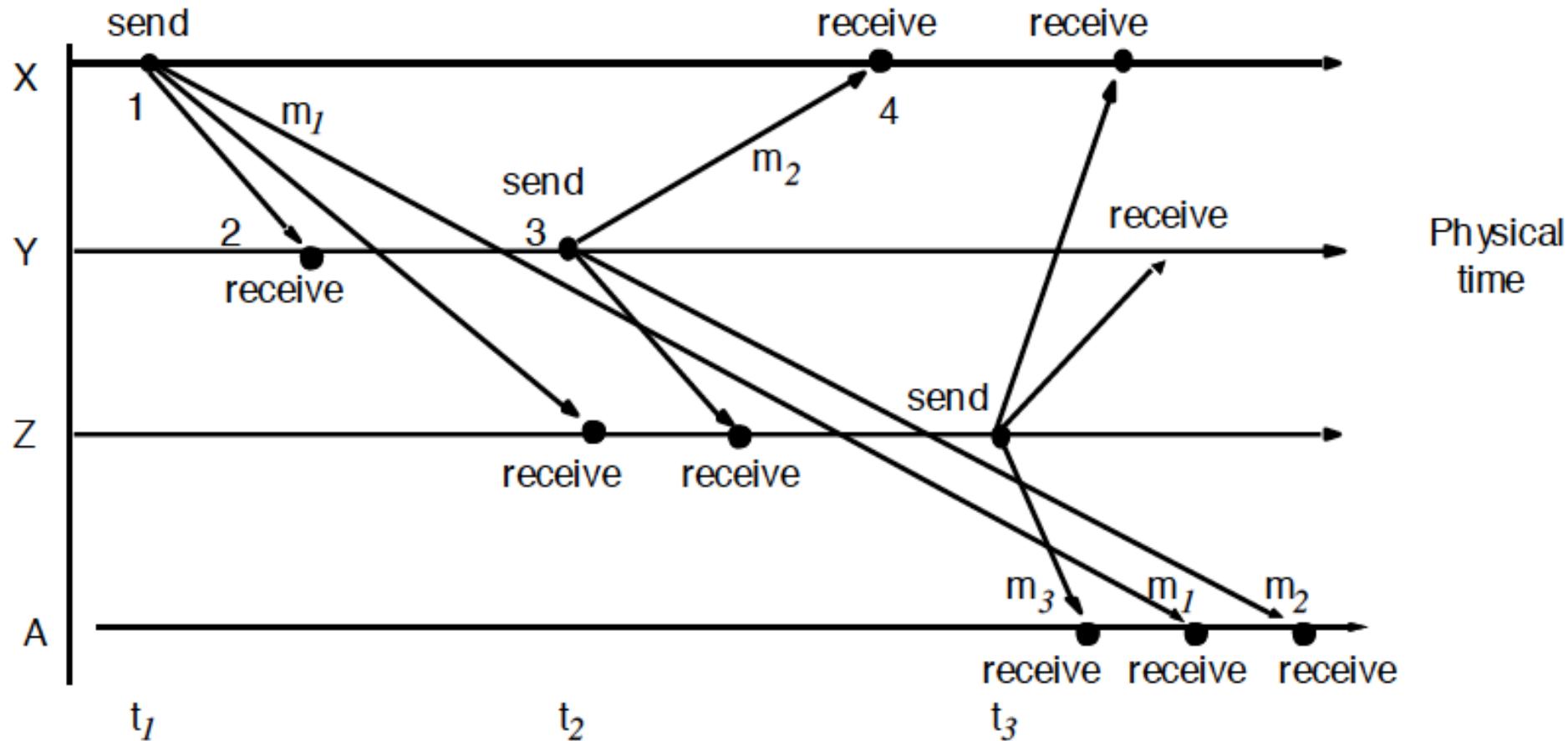
De: Assunto:

Z Re: Reunião

X Reunião

Y Re: Reunião

Ordenação dos Eventos



Ordenação dos Eventos

- ▶ Solução proposta por Lamport (1978)
- ▶ Criar um tempo lógico para marcar a sequência de eventos e determinar a ordem correta em que eles aparecem no tempo

2 – Modelo de Avarias

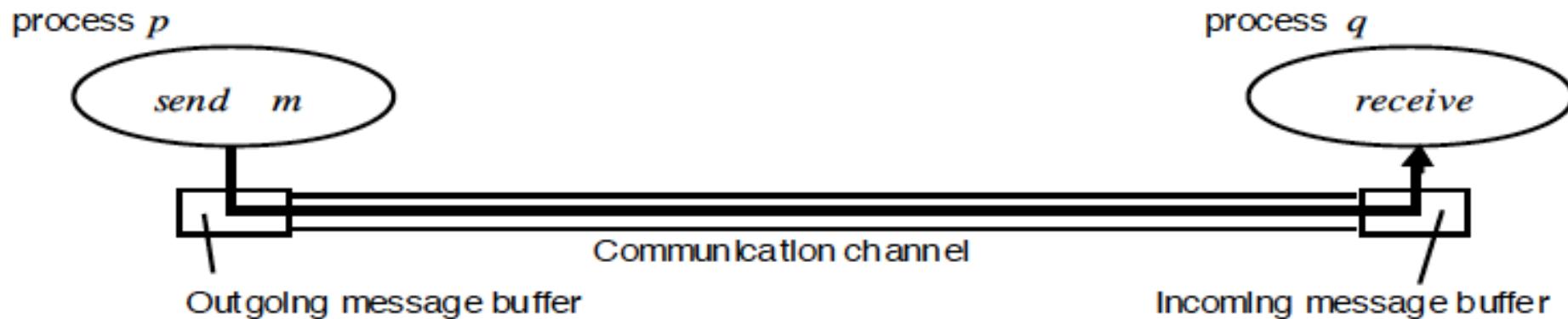
- ▶ Uma avaria é qualquer alteração do comportamento do sistema em relação ao esperado (em relação a sua especificação)
- ▶ Define de que maneira as avarias podem ocorrer
 - Podem atingir os processos ou os canais de comunicação

Tipos de Avarias

- ▶ Avarias por Omissão
- ▶ Avarias Arbitrarias
- ▶ Avarias em Tempo

Avarias por Omissão

- ▶ Quando um processo “deixa de funcionar” em algum ponto do Sistema Distribuído
- ▶ Quando o canal de comunicação falha



Tipos de Avarias por Omissão

- ▶ Fail–Stop
 - O processo bloqueou (crashed) e este fato não pode ser detectado por outros processos
- ▶ Crash
 - O processo aparentemente bloqueou, mas não é possível garantir que:
 - Apenas deixou de responder por estar muito lento ou...
 - As mensagens que enviou não chegaram

Avarias Arbitrárias (ou Bizantinas)

- ▶ Qualquer tipo de erro pode acontecer
- ▶ Nos processos:
 - O processo não responde
 - O estado do processo é corrompido
 - Responde de forma errada
 - Responde fora de tempo

Avarias Arbitrárias (ou Bizantinas)

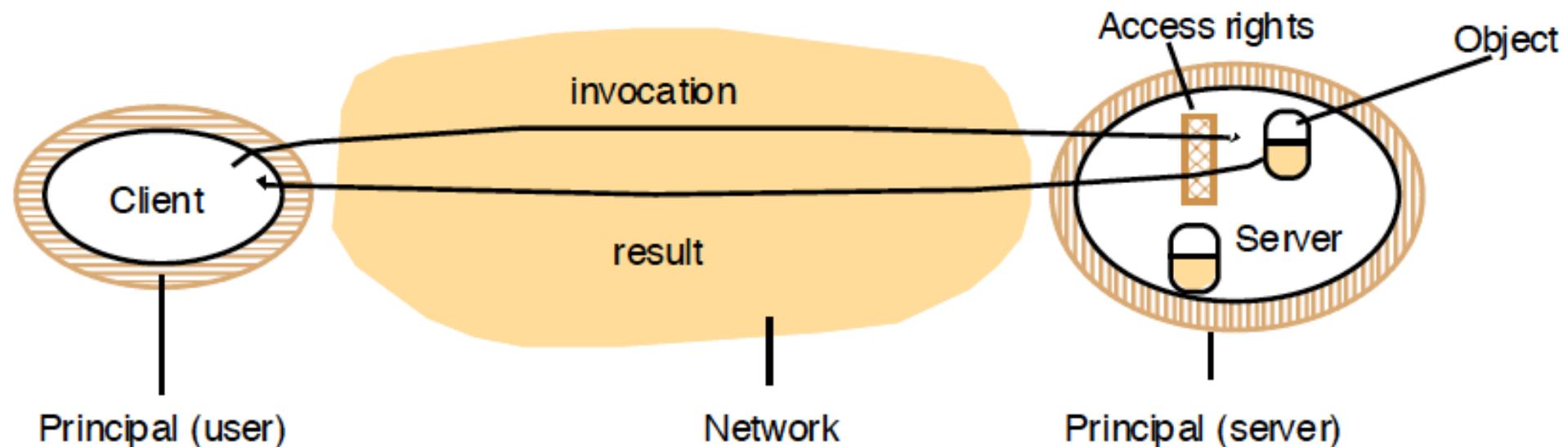
- ▶ Nos Canais de Comunicação
 - Mensagens corrompidas
 - Mensagens não-entregues
 - Mensagens duplicadas
 - Mensagens inexistentes são entregues
- ▶ São raras de ocorrer nos canais de comunicação porque o software de comunicação protegê as mensagens com somas de verificação (*checksum*), números de sequenciamento, etc

Avarias em Tempo

- ▶ Ocorrem quando o tempo limite para um evento ocorrer é ultrapassado
- ▶ Em sistemas eminentemente síncronos, é um indicativo seguro de falha
- ▶ Importante em sistemas de tempo real

Modelo de Segurança

- ▶ Proteção das entidades do sistema, processo/usuário (Principal)
- ▶ Direitos de acesso especificam que entidades podem acessar quais recursos e de que forma



Modelo de Segurança

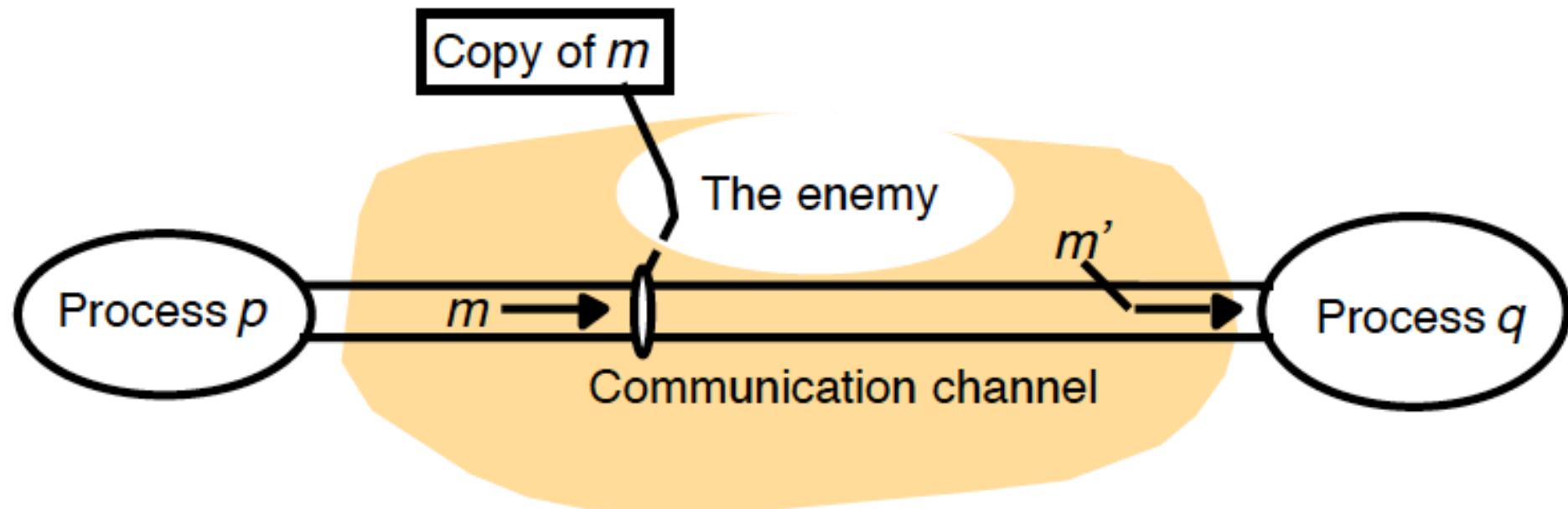
- ▶ O servidor é responsável por verificar
 - A identidade de quem (entidade) fez o pedido
 - Verificar se essa entidade tem direitos de acesso para realizar a operação pretendida
- ▶ O cliente deverá verificar
 - A identidade de quem lhe enviou a resposta, para ver se a resposta veio da entidade esperada

Que Ameaças?

- ▶ Supondo que existe um processo inimigo (adversário) capaz de:
 - Enviar qualquer mensagem para qualquer processo
 - Interceptar (ler/copiar) qualquer mensagem trocada entre dois processos
- ▶ Classificação das ameaças:
 - Aos processos
 - À comunicação
 - Negação de serviço

Ameaças aos Processos

- Um processo inimigo pode fazer-se passar pela entidade (cliente/servidor) e enviar a mensagem solicitada (*man-in-the-middle*)



Ameaças a Canais de Comunicação

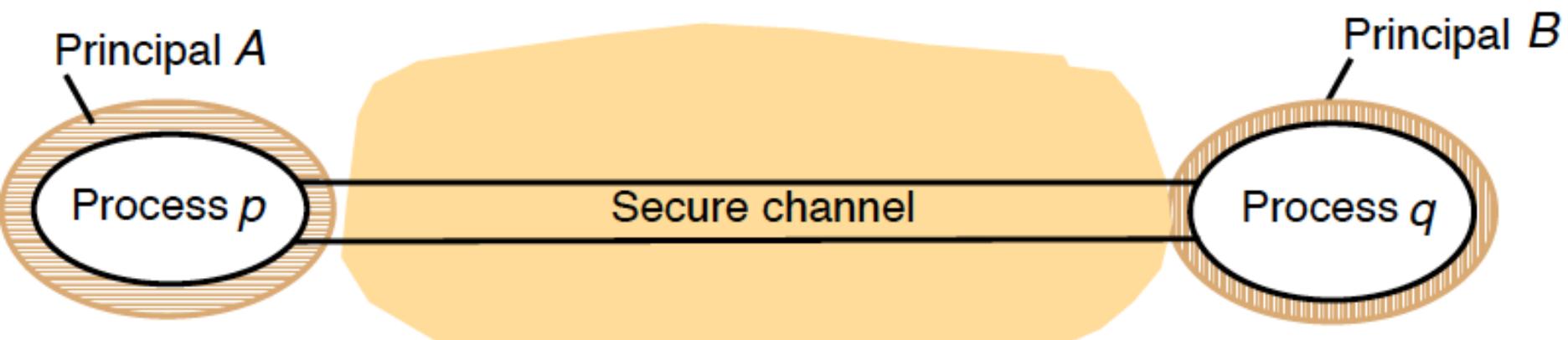
- ▶ Um processo inimigo pode copiar, alterar ou injetar mensagens na rede
- ▶ A comunicação pode ser violada por processos que observam a rede à procura de mensagens significativas
- ▶ Essas mensagens podem posteriormente ser reveladas a terceiros

Ameaça de Negação de Serviço

- ▶ Um processo intruso **captura** uma mensagem de solicitação de serviço e **retransmite-a** inúmeras vezes ao destinatário...
- ▶ fazendo-o executar sistematicamente o mesmo serviço e...
- ▶ Ultrapassar a sua capacidade de resposta

Como lidar com estas ameaças

- ▶ Utilização de canais seguros



Definição de Canal Seguro

- ▶ Canal utilizado para comunicação entre dois processos com as seguintes características:
 - Cada processo pode identificar com 100% de confiança a entidade responsável pela execução do outro processo
 - As mensagens que são transferidas de um processo para outro são garantidas do ponto de vista da integridade e da privacidade
 - As mensagens tem garantia de não repetibilidade ou reenvio por ordem distinta (cada mensagem inclui um tempo físico ou lógico)

Criptografia

- ▶ Técnica de codificar o conteúdo de uma mensagem de forma a “esconder” o seu conteúdo
- ▶ É necessário que ambos os processos possuam a chave de codificação/decodificação

Autenticação

- ▶ Incluir na mensagem uma porção (encriptada) que contenha informação suficiente para identificar a entidade e verificar os seus direitos de acesso

Criar um Modelo de Segurança

- ▶ Analisar as principais ameaças
 - Riscos envolvidos
 - Possíveis consequências
- ▶ Fazer o balanço entre o custo de proteger o sistema e o risco de fato que as ameaças representam