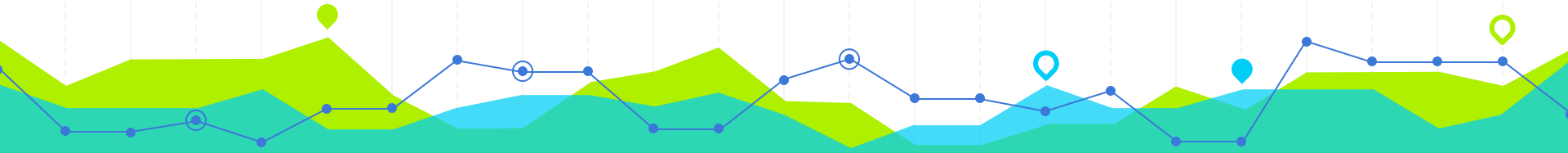


Modelo de Segurança

Nome: Miguel Gut Seara
Disciplina: Sistemas Distribuídos
Universidade Católica de Pelotas

Pelotas, abril de 2022.

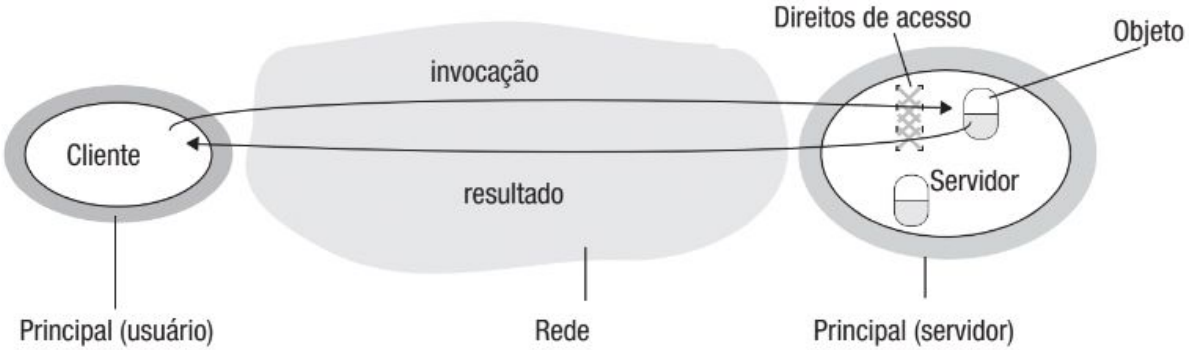
Modelo de Segurança

- Após identificar compartilhamento de recursos e descrição de arquitetura, precisamos de um princípio para a base do modelo de segurança:

> *"A segurança de um sistema distribuído pode ser obtida tornando seguros os processos e os canais usados por suas interações e protegendo contra acesso não autorizado os objetos que encapsulam."*

1. Proteção de Objetos

A figura abaixo exemplifica um servidor gerenciando um conjunto de objetos para alguns usuários:



Vamos considerar que usuários podem executar programas clientes que enviam invocações para o servidor para realizar operações. Ao fim, o servidor envia o resultado ao cliente.

1. Proteção de Objetos

- Para dar suporte às diferentes ações e a diferentes usuários, utiliza-se o conceito de **direitos de acesso**
- Usuários precisam ser incluídos no modelo de segurança
- Associa-se a cada invocação e resultado uma entidade que a executa (*principal)*
- Responsabilidade do servidor: **verificação de identidades** e **conferência de direitos de acesso**

2. Tornando processos e interações seguras

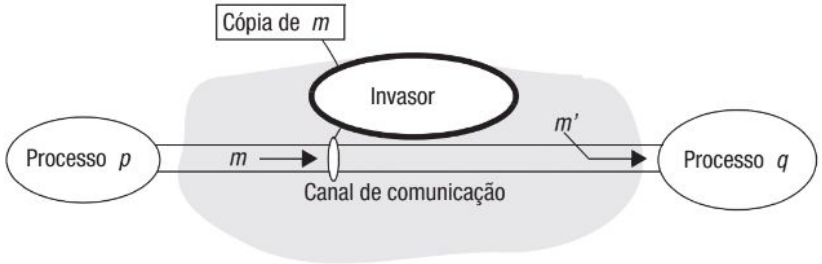
- Os processos interagem através de mensagens
- Mensagens são expostas (consequentemente, inseguras)
- Servidores e processos P2P publicam interfaces (para permitir comunicações)
- Integridade ameaçada por diversas naturezas

  Como analisar ameaças para identificar e anulá-las?

2.1 O invasor

- Capaz de enviar qualquer mensagem para qualquer processo
- Ler ou copiar qualquer mensagem entre dois processos
- Geralmente um computador é um exemplo suficiente

Que ameaças um invasor apresenta?



3.1 Ameaças aos processos

- Falta de capacidade de determinar a identidade do remetente
  - Identidades falsificadas
- Prejudicar o andamento de um processo no sistema distribuído
- Pode acontecer com servidores ou clientes

3.1 Ameaças aos processos

Servidores

- Recebe muitos pedidos, pode não necessariamente determinar a ID do principal
- Pode ser uma ID falsa
- Necessário implementar um reconhecimento garantido
- Ex.: Servidor de e-mail recebe uma solicitação de leitura de mensagens particulares

3.1 Ameaças aos processos

Clientes

- O resultado de uma invocação pode não ter sido enviada do servidor desejado ou de um servidor falso
- *Spoofing*
- Ex.: Uma mensagem de e-mail falsa (não existe realmente no servidor)

3.2 Ameaças aos canais de comunicação

- Ocorre quando um invasor copia, altera ou injeta mensagens pela rede
- Ameaça à privacidade e integridade das informações
- Ex.: Um e-mail tem seu conteúdo alterado ou revelado a outro cliente

3.3 Negação de serviço

- Ocorre quando o atacante interfere nas atividades dos usuários autorizados
- Invocações sem sentido ou mensagens incessantes para sobrecarregar os recursos
- Retardar ou impedir invocações válidas de outros usuários
- Ex.: Sobrecarregar as trancas eletrônicas de um prédio para impedir entrada e saída de usuários

3.4 Código móvel

- Interage com processos que recebem e executam códigos provenientes de outros lugares
- “Cavalo de troia” - dá a entender que tem um propósito inocente, porém acessa ou modifica recursos disponíveis ao usuário
- Ex.: Anexos virulentos de e-mails

4. Medidas de proteção

- Cada tipo de ataque requere medidas diferentes
- É necessário avaliar cada processo no sistema distribuído para implementação de um projeto seguro
- Construir um *modelo de ameaças*, listando formas de ataque e avaliando riscos e consequências

4. Medidas de proteção

- Cada tipo de ataque é combatido através de medidas diferentes
- É necessário avaliar cada processo no sistema distribuído para implementação de um projeto seguro
- Construir um *modelo de ameaças*, listando formas de ataque e avaliando riscos e consequências

4.1 Criptografia

- Através da *cifragem* as mensagens são embaralhadas para que as mensagens trocadas entre cliente e servidor sejam escondidas
- Chaves baseadas em algoritmos modernos e difíceis de adivinhar

4.2 Autenticação

- Usando a criptografia é possível *autenticar* mensagens, escondendo parte do conteúdo
- A mensagem é cifrada com a chave secreta previamente conhecida entre o cliente e servidor

4.3 Canais Seguros

- Criptografia e autenticação constroem canais seguros para comunicação
- Cada um dos processos conhece com certeza a identidade do principal
- Garante privacidade e integridade
- Cada mensagem possui indicação de relógio lógico ou físico para impedir que mensagens sejam reordenadas ou reproduzidas

Obrigado!

Perguntas?

miguel.seara@sou.ucpel.edu.br