Segurança

Maicon Giovane Pazin
Willian Nalepa Oizumi

Introdução a Segurança

Segurança em sistemas distribuidos pode ser dividida em duas partes

- **Comunicação entre usuários ou processos em diferentes máquinas**
- **Autorização de acesso a recursos disponíveis**

Introdução a Segurança

Segurança em um sistema está relacionado a CONFIABILIDADE:

- Condidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Não Repúdio

Ameaças de Segurança

Existem 4 tipos de ameaça de segurança a serem consideradas:

- Interceptação
- Interrupção
- Modificação
- Fabricação

Políticas de Segurança

Descrevem precisamente quais ações as entidades de um sistema terão permissão de executar e quais ações serão proibidas

Mecanismos de Segurança

Principais mecanismos de segurança:

- Encriptação
- Autenticação
- Autorização
- Auditoria

Questões de Projeto Gerais

- Foco no controle
  1. Proteção contra operações inválidas
  2. Proteção contra chamadas não autorizadas
  3. Proteção contra usuários não autorizados
- Níveis dos Mecanismos de Segurança
- Distribuição de Mecanismos de Segurança
- Simplicidade

Criptografia

Fundamental para segurança em sistemas distribuídos. Encriptação e decriptação são acompanhados pelo uso de métodos de criptografia parametrizados por chaves

- Sistema simétrico de criptografia
- Sistema assimétrico de criptografia
- Funções Hash

Canais Seguros

Ao pensar em segurança em Sistemas Distribuídos, é útil pensar em termo de clientes e servidores. Neste contexto, duas questões são predominantemente importantes:

- Como realizar uma comunicação segura entre os clientes e os servidores
- Como um servidor pode ficar sabendo se determinado cliente que está requerindo um seviço tem autorização para tê-lo

Autenticação

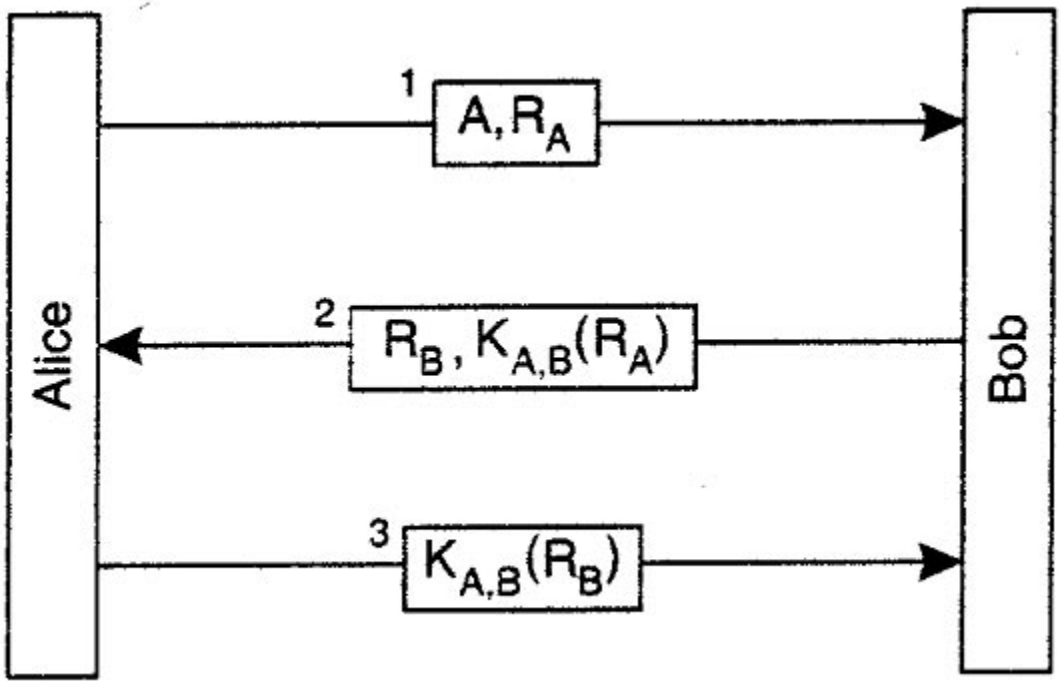
Autenticação e Integridade das mensagens devem sempre ser garantidos pois um não funciona sem o outro.

Três abordagens são propostas:

- Autenticação baseada em uma Chave Secreta Compartilhada
- Autenticação usando um Centro de Distribuição de Chaves (KDC)
- Autenticação usando Criptografia com Chave Pública

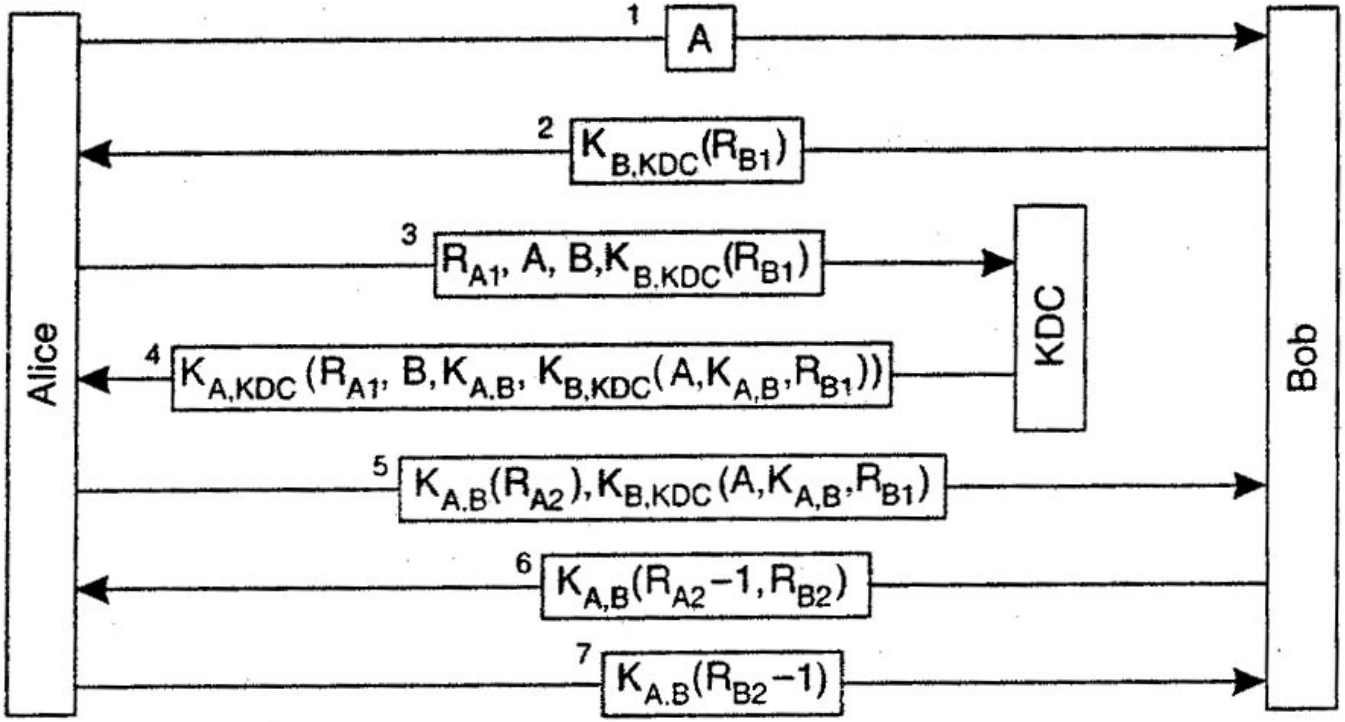
Autenticação

Autenticação baseada em uma Chave Secreta Compartilhada:



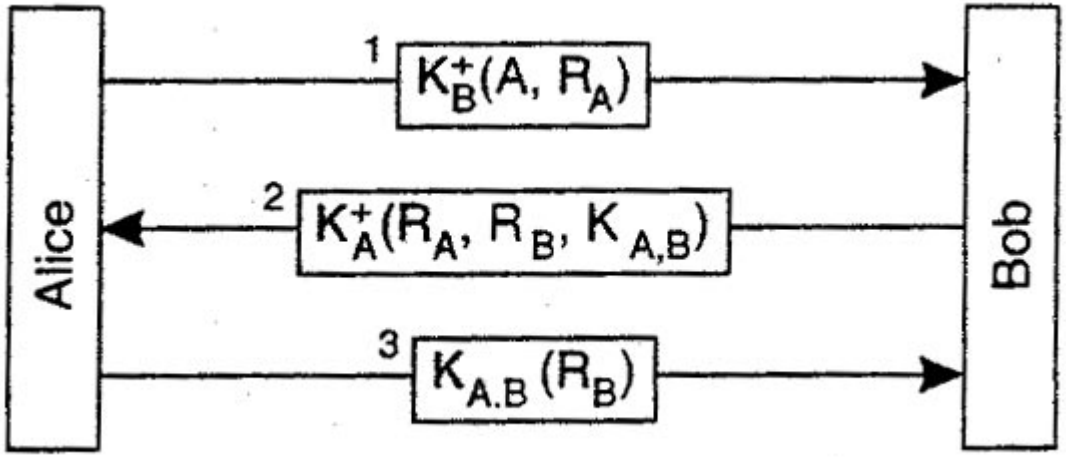
Autenticação

Autenticação usando um Centro de Distribuição de Chaves (KDC):



Autenticação

Autenticação usando Criptografia com Chave Pública:



Confidencialidade e Integridade

A Confidencialidade das mensagens pode ser garantida através da encriptação utilizando chaves secretas.

A Integridade das mensagens pode ser mantida de duas formas:

- Através de Assinaturas Digitais
- Através de Chaves de Sessão

Comunicação Segura em um Grupo

Assim como na comunicação entre dois hosts, em um grupo de servidores também é necessária a proteção das mensagens contra modificação, fabricação e interceptação.

- Confidencia em um Grupo
- Segurança de Servidores Replicados

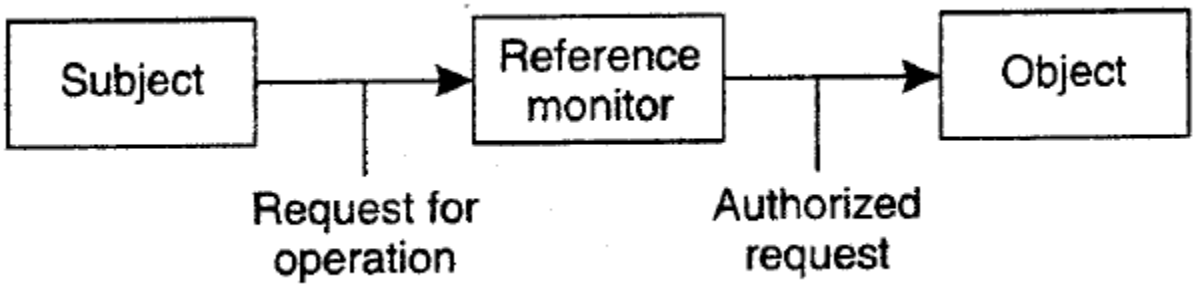
Controle de Acesso

Em um modelo cliente-servidor, quando um cliente faz uma requisição ele só deve ser atendido se tiver **direitos de acesso** para as operações realizadas naquela requisição.

Formalmente, a **verificação** de **direitos de acesso** é referenciada como sendo **controle de acesso**, enquanto que autorização trata da garantia dos direitos de acesso.

Questões Gerais sobre Controle de Acesso

Modelo básico para controle de acesso: (i) Um **sujeito** emite uma requisição para acessar um objeto; (ii) O **monitor de referência** verifica os direitos de acesso do sujeito e decide se ele tem permissão para acessar o objeto. (iii) em caso positivo a requisição é recebida e respondida pelo **objeto** requisitado.



Questões Gerais sobre Controle de Acesso

É extremamente importante que o monitor de referência seja **inviolável**: um invasor não deve ser capaz de burlar seu mecanismo de proteção

Proteção pode incluir também questões relacionadas com o gerenciamento de objetos (ex. criação, renomeação e deleção)

Abordagens Utilizadas: **Matriz de Controle de Acesso**, **ACL** e **Proteção de Domínios**

Firewall

Tipo especial de **monitor de referência**

Controla os acesso aos recursos do sistema.

Serve como uma proteção onde **todo o tipo de comunicação**, tanto de saída quanto de entrada, deve ser verificada para identificar sua autorização.

Segurança de Código Móvel

O compartilhamento de códigos entre hosts provê uma quantidade de questões de segurança.

- **Proteção do Agente**
  - Read-only state: Assinatura para verificar se o agente foi alterado;
  - Append-only logs: Informações são armazenadas no agente na forma de logs (sem alterações);
  - Selective revealing of state to certain states: array onde cada posição é de um servidor (criptografado).
- **Proteção do Alvo**: Host deve ter controle sobre as ações do agente. Diversas abordagens:
  - Sandbox (JVM), playground isolado (acesso por RPC).

Negação de Serviço (DDoS)

Ataques de negação de serviço em SDs tentam derrubar uma rede de serviço:

- Depleção de Largura de Banda: ocorre quando muitas mensagens são enviadas para uma simples máquina.
- Depleção de Recursos: faz o receptor usar seus recursos para atender a mensagens inúteis.

Defesa:

- Por meio dos roteadores **filtrar** apenas pacotes de dados da organização
- **Bloquear** hosts que estejam enviando muitos pacotes para o sistema (sem justificativa)

Gerenciamento de Chaves

É necessário um procedimento de segurança para manter chaves de criptografia seguras:

- **Estabelecimento de chave**: Criptografia das chaves por meio de algoritmos (Diffie–Hellman);
- **Distribuição da chave**: O envio de chave pública deve ser feito por meio de uma conexão segura. Os hosts envolvidos devem possuir certificados de autoridades;
- **Tempo de vida dos certificados**: Os certificados geralmente têm um tempo de vida restrito. Sendo assim, sua validade deve ser sempre verificada com a autoridade certificadora.

Gerenciamento de Autorização

Gerenciamento de segurança também está relacionado com o gerenciamento de direitos de acesso:

- Capacidades
  - Estrutura de dados impossível de falsificar
  - Determina os direitos de acesso do portador
- Certificados de Atributos
  - Lista de pares (atributo, valor) que se aplicam para uma entidade específica
  - Autoridades de certificação garantem a validade
- Delegação
  - Delegar direitos de acesso de um processo para outro (ex. impressão de um arquivo protegido)

Questões

1) O que um sistema distribuído deve oferecer para ser considerado confiável?

2) Cite e explique quais são os quatro principais tipos de ameaça a segurança de um sistema distribuído.

3) Cite e explique quais são os principais mecanismos de segurança para sistemas distribuídos.

4) Qual é o objetivo dos mecanismos de autenticação? Quais são as principais abordagens utilizadas?

5) Explique como funciona o ataque de negação de serviço e como é possível se defender desse tipo de ataque.