

Segurança em Sistemas Distribuídos



Segurança

- confidencialidade
- autenticidade
- integridade
- não repudição



comunicação



Ameaças

- interceptação
- interrupção
- modificação
- fabricação



ataques a canais de comunicação

- **escuta**
 - obtenção de informação na rede
 - senhas, etc
- **masquerading**
 - uso de identidades incorretas
- **message tampering**
 - alteração de mensagens trocadas
- **replay**
 - reenvio de mensagens obtidas por escuta
- **negação de serviço**
 - inundação de rede ou servidor



mecanismos

- criptografia
- autenticação
- autorização
- auditoria

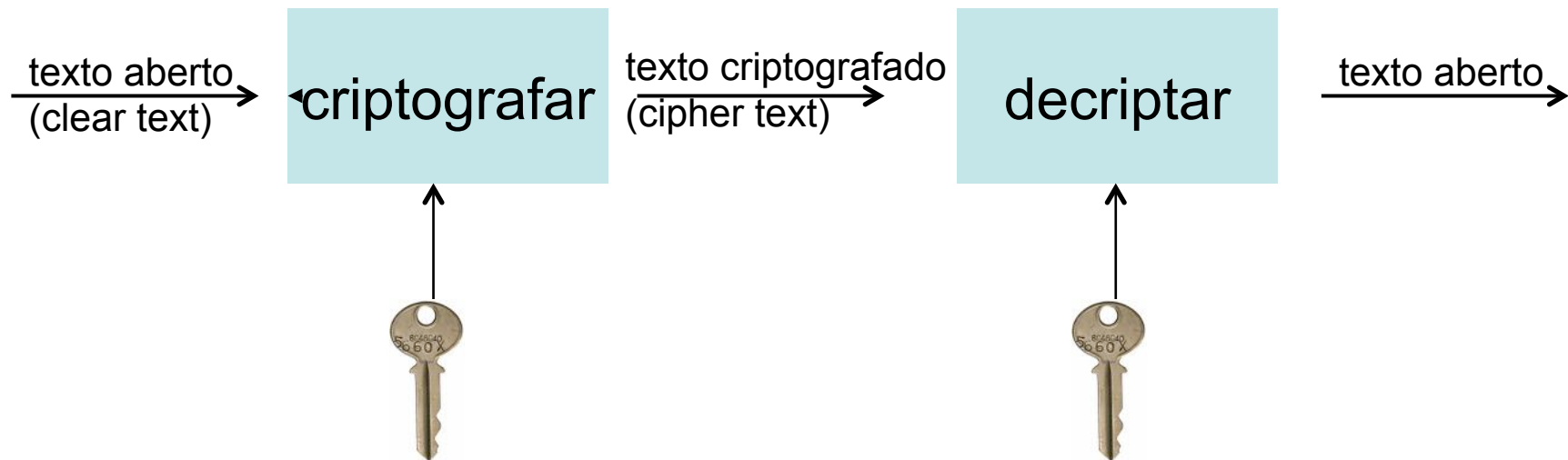


política de segurança

- equilíbrio entre custos
 - risco X sobrecarga



Criptografia de chave secreta



- mesma chave nas duas direções
- também chamada de criptografia simétrica



algoritmos de chave secreta

- técnicas de embaralhamento
- muitas vezes pensados para implementação em hardware

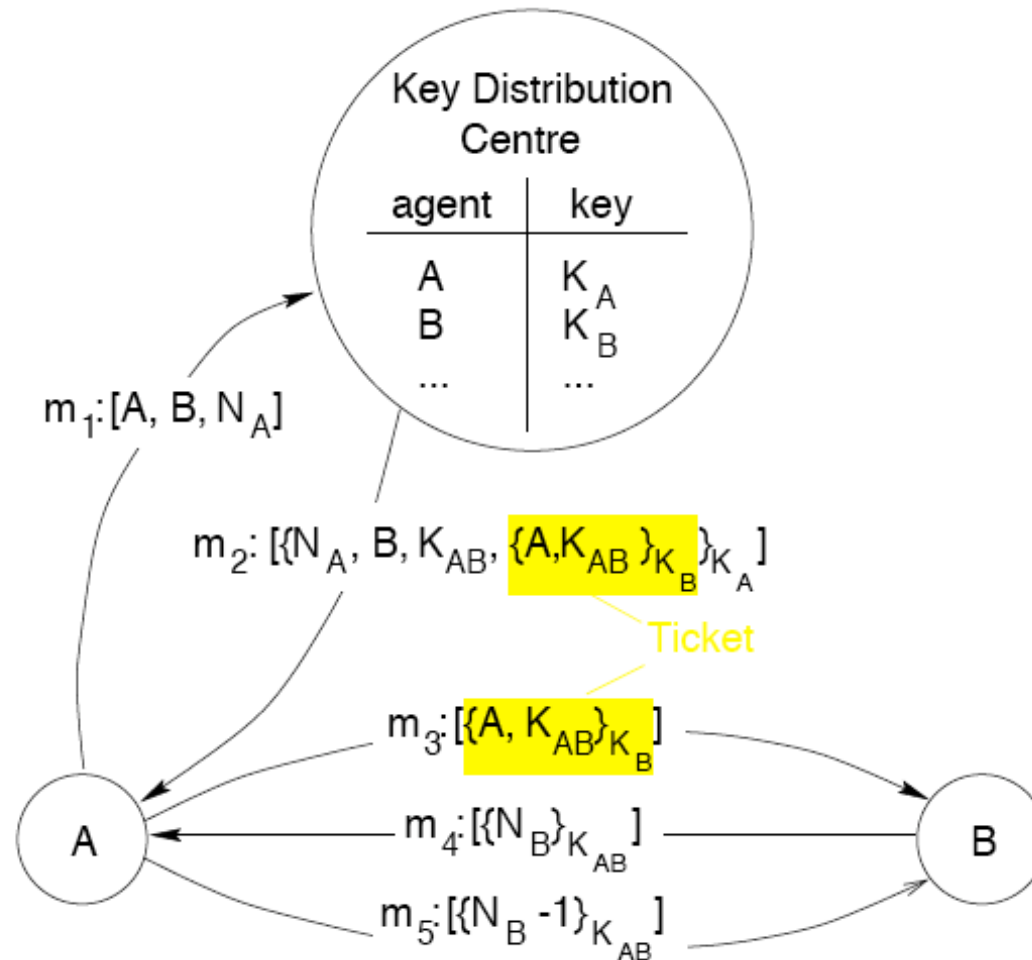


Distribuição de chaves secretas

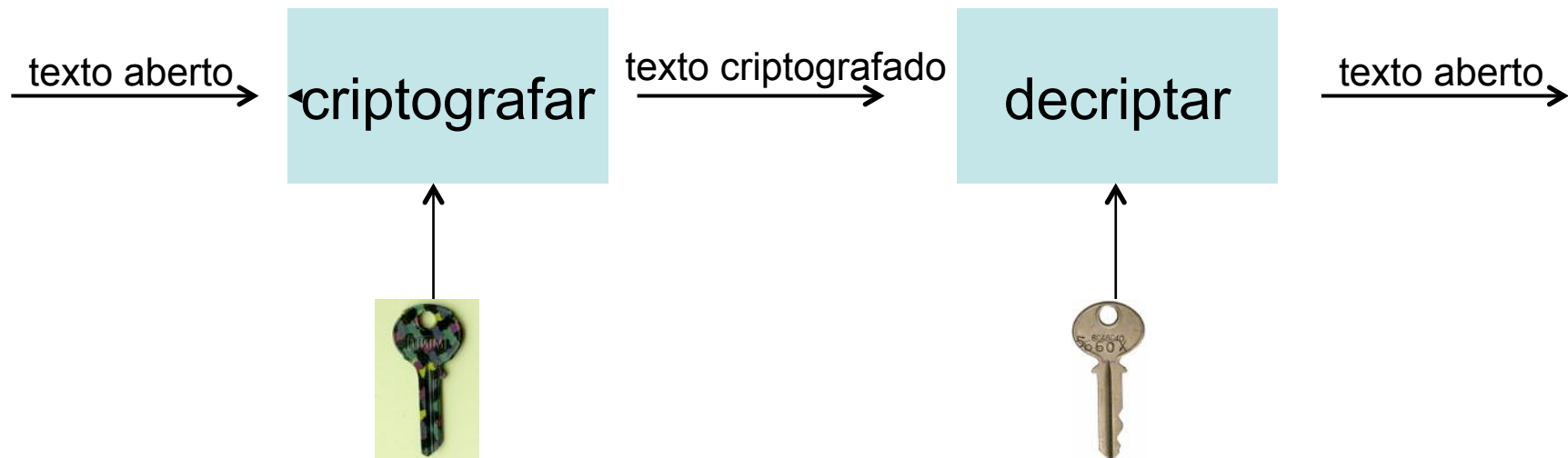
- como fazer para as duas partes compartilharem um segredo?
- uso de Key Distribution Centers
 - ex Kerberos



protocolos de acesso a KDCs



Criptografia de chave pública e privada



- chaves diferentes em cada direção
 - também chamada de criptografia assimétrica
- uma das chaves pode ser pública sem problemas



algoritmos de chave pública e privada

- técnicas aritméticas
 - manipulação de números primos muito grandes
- surgimento do conceito com Diffie-Hellman, em 1976
 - D-H apenas para estabelecimento de segredo compartilhado
- processamento mais custoso que o de algoritmos de chave secreta



Distribuição de chave pública

- intruso ainda pode fazer crer que sua chave pública é a de outra entidade
- infraestutura de distribuição
 - certificados
 - autoridades de certificação
 - infraestruturas de chaves públicas



algoritmos de hash

- funções de hash:
 - dado um blobo de dados de tamanho arbitrário, retornam um string de bytes de tamanho fixo
 - entrada: mensagem
 - saída: hash ou digest
 - pequenas alterações nos dados de entrada devem alterar o valor do hash
 - não é possível descobrir a mensagem a partir do hash
 - duas mensagens diferentes dificilmente levam ao mesmo hash



ataques para descoberta de chaves

- Diferentes níveis de dificuldade se atacante dispõe de:
 - apenas texto criptografado
 - pares (texto aberto, texto criptografado)
 - pares escolhidos
- ataques de “força bruta”
 - tentativa de quebra com cada chave possível
 - tamanho de chaves e o “computacionalmente difícil”



usos em comunicação

- confidencialidade
- autenticidade
- não repudição
- integridade
 - aplicação de criptografia sobre *digest* da msg
 - uso combinado de criptografia simétrica e assimétrica



Autenticação

- login e senha
- biometria
- algoritmos de autenticação



algoritmos de autenticação

- uso de desafios e criptografia
 - simétrica e assimétrica



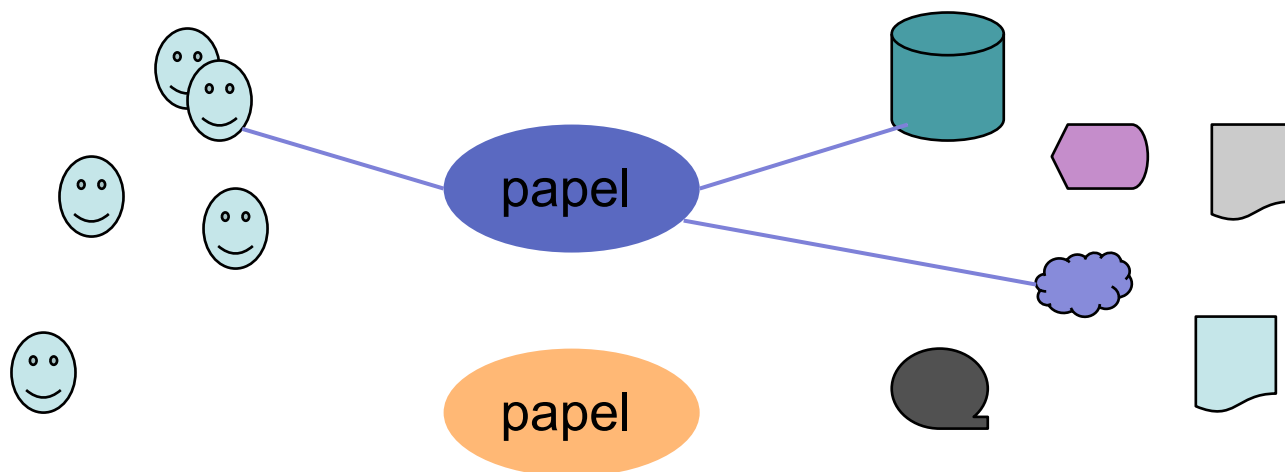
Controle de acesso

- matrizes de acesso
 - usuários X recursos
- normalmente esparsas
- opções:
 - lista de recursos para cada usuário/grupo
 - lista de usuários/grupos para cada recurso



RBAC

- direitos nem sempre associados a usuários individuais
 - papel do usuário na organização
 - um mesmo usuário pode desempenhar diferentes papéis



Autenticação em sistemas distribuídos

- acesso a serviços em diferentes pontos
 - (administrativos e geográficos)
 - escalabilidade
- cada um deles deve identificar o usuário individualmente?
 - cenários como grades, bibliotecas digitais, etc
 - autenticação e controle de acesso



soluções clássicas

- cadastro individual de cada usuário em cada serviço
 - ônus para administrador de serviço
 - cadastro de cada usuário e de seus direitos
 - ônus para usuário:
 - senha (ou outra coisa) para cada serviço?
- conta única para todos os usuários de certa instituição
 - ônus para administrador de serviço:
 - não há como fazer auditoria
 - ônus para usuário
 - não há como diferenciar direitos

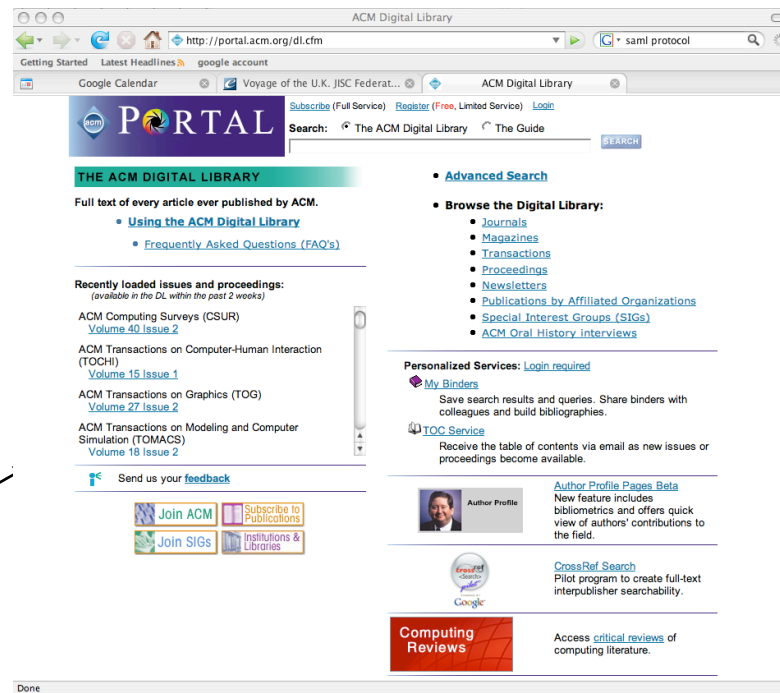


arquiteturas distribuídas

- provedor de serviço:
 - responsável por serviço controlado
- provedor de identidade
 - responsável por autenticação de usuários
- provedor de atributos
 - fornece informações que podem ser usadas pelo controle de acesso
 - rede de confiança entre provedores
 - propostas específicas para aplicações web



exemplos



acesso a editoras online

- reconhecimento de usuários de intuições cadastradas



exemplos



vendas com descontos p/
estudantes

- como saber que usuário é estudante?
- certificado? mas serviço tem que conhecer cada usuário?



uso de provedores de identidade

- provedores de serviços confiam em algumas fontes de identidade



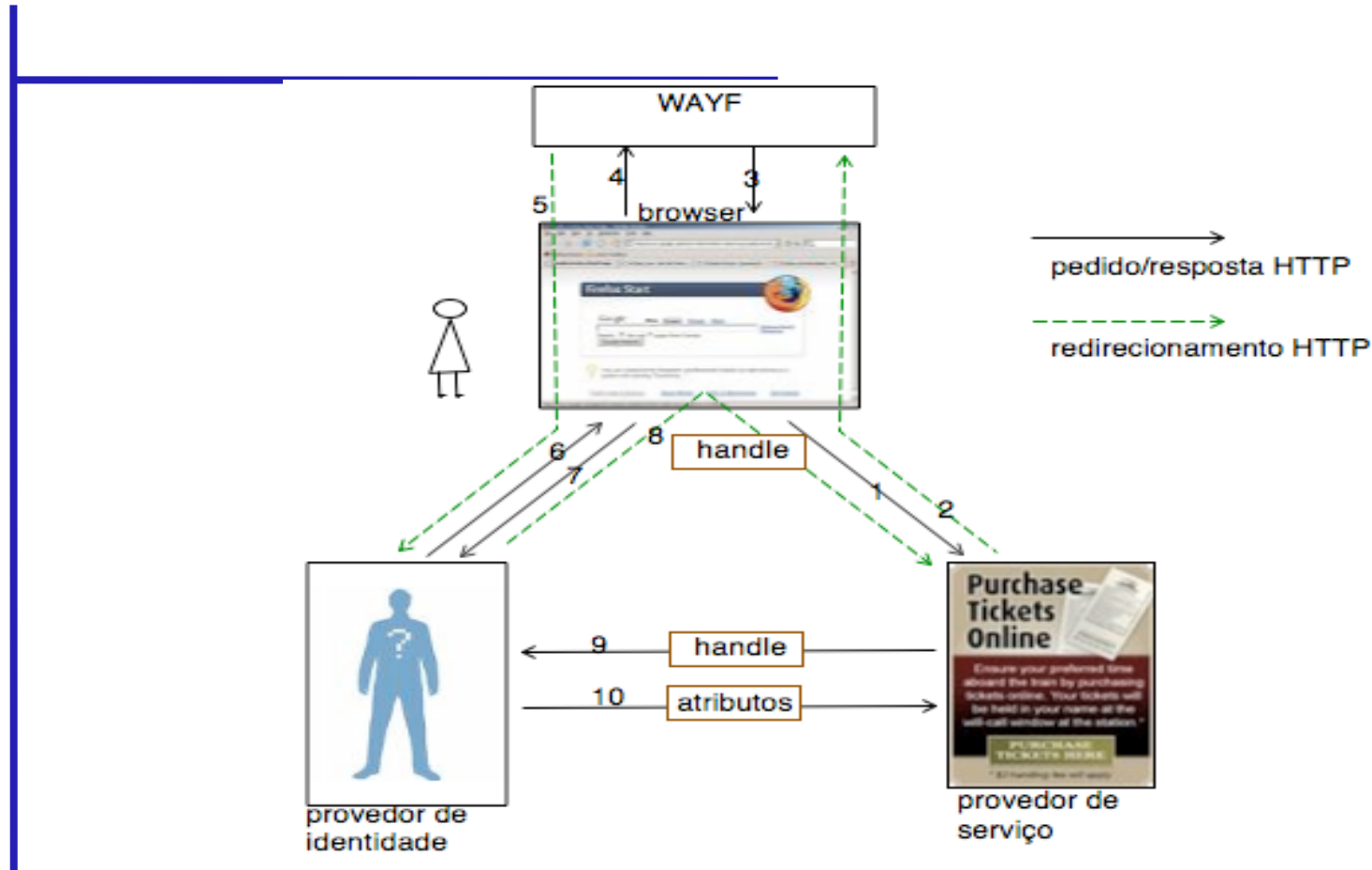
provedor de identidade



serviço em qualquer lugar



exemplo: uso de shibboleth



- protocolo SAML usado na comunicação (shib 2.x)



federações

- em andamento em muitos países
- acoplamento com projetos de infraestruturas de chaves públicas
- privacidade: fornecimento do conjunto mínimo de atributos necessários
- foco atual em aplicações web



Bibliografia

- Charlie Kaufman, Radia Perlman, Mike Speciner. Network Security: Private Communication in a Public World. Prentice-Hall, 1995.
- Ihor Kuz, Felix Rauch, Manuel M. T. Chakravarty, Gernot Heiser. Security in Distributed Systems. Notes for Lectures on COMP9243. University of New South Wales
www.cse.unsw.edu.au/~cs9243/lectures/
- Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, 1996.

