UNIVERSIDADE FEDERAL DE UBERLÂNDIA
SISTEMAS OPERACIONAIS

Segurança em Sistemas Operacionais

Igor Augusto Costa e Souza 11221EMT008
João Victor de Oliveira 11611BSI215
Nicolas Fischmann 12011EMT032
Lucas Albino Martins 12011ECP022

Link apresentação:

- https://drive.google.com/file/d/1AM2-XTIbHMTdzbLbqLuS_vRLIiCd9Tps/view

Perguntas

- O que é segurança em s.o e como garanti-la?
- Quais são os diferentes métodos de proteção dos usuários do sistema operacional ?
- Quais são os 4 tipos de ataques?
- Qual a diferença entre DoS e DDoS ?
- Traduzir a seguinte criptografia:

texto cifrado: nkn. s gktc wky. mgsbc.

Introdução

A segurança de um sistema está ligada a 5 pontos principais

- Confidencialidade
- Integridade
- Autenticidade
- Disponibilidade
- Não Repúdio

Confidencialidade

- Garantir que o conteúdo de uma mensagem enviada está seguro, e não será conhecido por usuários indesejados.
- Uma das formas mais seguras e práticas de garantir a confidencialidade de uma mensagem é a utilização de criptografia.

Integridade

- Garantir que a mensagem não foi alterada no decorrer do percurso entre o remetente e o destinatário.
- Para evitar esse tipo de adulteração, podem ser utilizados assinaturas digitais, chaves de sessão ou a implementação de hashes.

Autenticidade

- Garantir que uma mensagem recebida seja, de fato, do remetente da qual se espera a mensagem.
- Para isso, podem ser utilizados assinaturas digitais, chaves de sessão ou a implementação de hashes.

Disponibilidade

- Garantir que o sistema estará em pleno funcionamento durante o seu tempo de operação.

Não Repúdio

- Garantir que não haja nenhuma atividade sem a identidade de quem a executou.

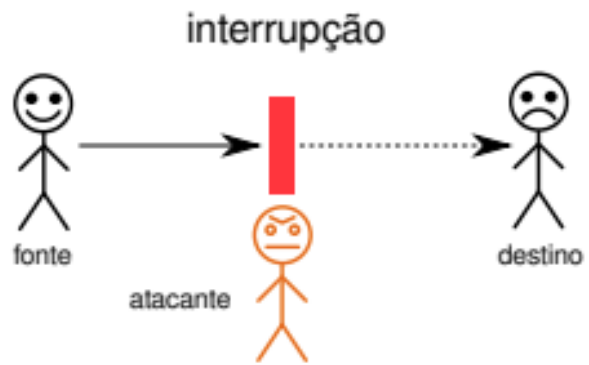
Resposta

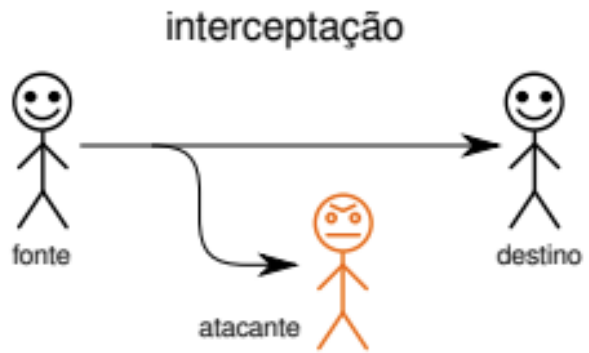
- O que é segurança em S.O. e como garanti-la?
  - Segurança é ter a maior inviolabilidade e disponibilidade possível
  - Negando por padrão
  - Controle de acessos
  - Desativando recursos desnecessários
  - Gerenciando atualizações

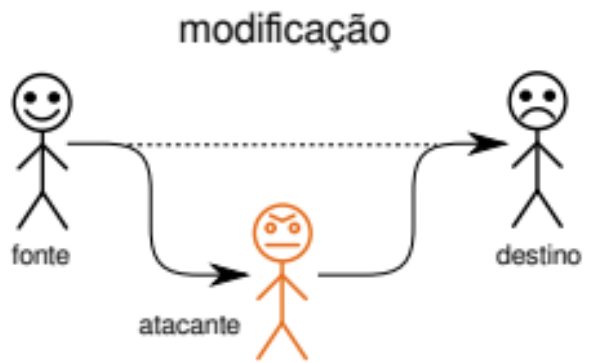
Ataques e Invasões

- Um ataque é o ato de utilizar (ou explorar) uma vulnerabilidade para violar uma propriedade de segurança do sistema.
- Existem basicamente 4 tipos de ataques:
  - Interrupção
  - Interceptação
  - Modificação
  - Fabricação

Ataques e Invasões







Ataques e Invasões

Outras características

- Passivo
- Ativo

- Local
- Remoto

Ataques e Invasões

- Quando o ataque é bem sucedido, frequentemente o intruso efetua novos ataques para aumentar seu nível de acesso no sistema, o que é denominado *elevação de privilégio*.
- Mas por outro lado, os ataques de negação de serviços visam prejudicar a disponibilidade do sistema, impedindo que os usuários válidos do sistema possam utilizá-lo, ou seja, que o sistema execute suas funções.
  - Qual a diferença entre DoS e DDoS ?

Ataques e Invasões

- Antes…

  - Ataque fork bomb

```c
#include <unistd.h>

int main()
{
  while (1)    // laço infinito
     fork() ;  // reproduz o processo
}
```

  - Resposta: A principal diferença entre os dois é na forma com que eles são feitos. Enquanto o ataque DDoS é distribuído entre várias máquinas, o **ataque DoS** é feito por apenas um invasor que envia vários pacotes

Malwares

- Denomina-se genericamente malware todo programa cuja intenção é realizar atividades ilícitas, como realizar ataques, roubar informações ou dissimular a presença de intrusos em um sistema.
- As funcionalidades mais comuns dos malwares são:

  - Vírus
  - Worm
  - Trojan horse

Interceptação de dados

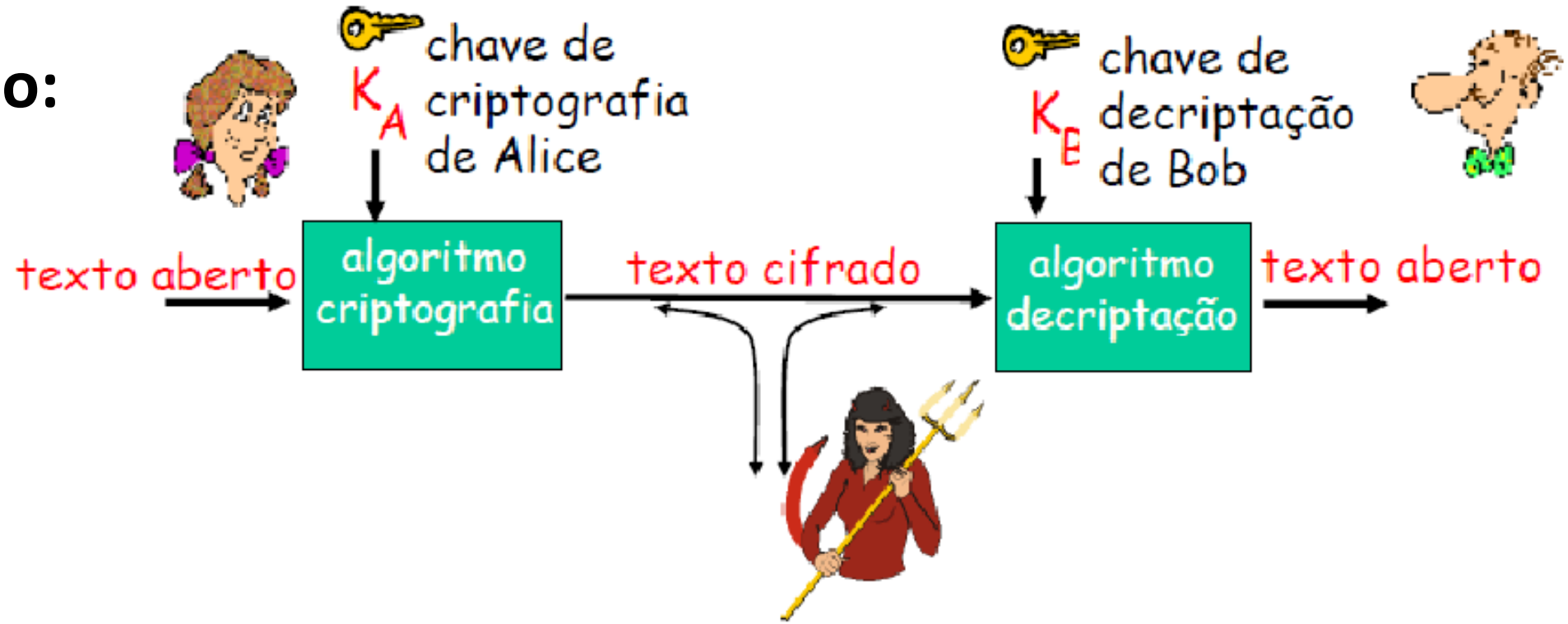
- Uma preocupação na transferência de dados entre sistemas, é a garantia da confidencialidade dos dados.
- Atualmente, os dados trafegam em rede, de maneira “exposta”.
- A melhor forma de proteger esses dados é por meio de criptografia

Proteção contra acessos indevidos

- Para proteger um sistema de acessos indevidos, diversas medidas podem ser tomadas, como:
- Utilização de senhas seguras e política de troca regular.
- Autenticação em duas etapas.
- Controle de acesso por IP
- Negação de acesso por natureza.

Criptografia.

Questão:



m mensagem em texto aberto

$K_A(m)$ texto cifrado, criptografado com chave K_A

$m = K_B(K_A(m))$

Criptografia.

- **Questão:**

  texto cifrado: nkn. s gktc wky. mgsbc.

- Esquema de criptografia simples

  - cifra de substituição: substituir uma coisa por outra.

  - cifra monoalfabética: substituir uma letra por outra.

  - **texto aberto**: abcdefghijklmnopqrstuvwxyz

  - **texto cifrado**: mnbvcxzasdfghjklpoiuytrewq

Criptografia.

- Maneira de encriptar(disfarçar) o conteúdo de uma mensagem ou informação enviada por um emissor de modo que apenas o receptor na qual foi direcionada a mensagem consiga desencriptar(ler).

Princípios fundamentais da criptografia.

Segundo tanenbaum existem dois princípios fundamentais de criptografia:

- Redundância ou informações desnecessárias.
- Histórico de mensagens.

Tipos de Criptografia.

- **Criptografia de chaves assimétricas.**
- **Criptografia de chaves simétricas.**

Criptografia.

Resposta:

- texto aberto: **abc**defghijk**l**mn**o**pqrst**uv**wx**y**z.
- texto cifrado: **mnb**v**c**xza**s**df**g**hj**k**lpoiu**yt**re**w**q

b = n , o = k, i = s, l = g, v = t , e = c, y = w, u = y, a = m, c = b.

Mensagem: texto aberto: **bob. i love you. alice**

texto cifrado: **nkn. s gktc wky. mgsbc.**

Pergunta

Quais são os diferentes métodos de proteção do usuário do S.O ?

-Estrutura de proteção

-Autenticação

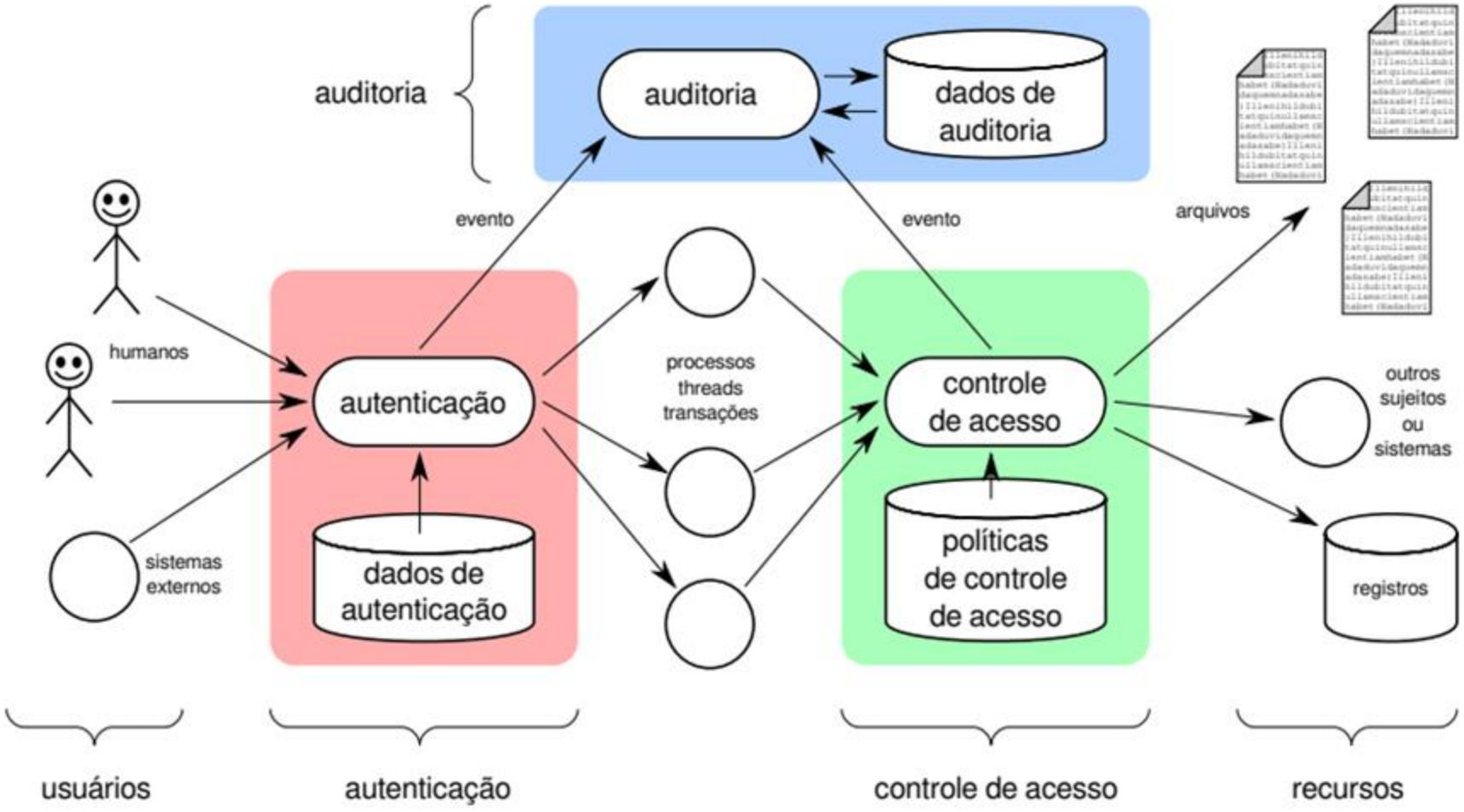
-Senha

Estrutura de proteção

-TCB (Trusted Computing Base ou núcleo de segurança) : Conjunto de Hardwares Softwares que podem apresentar um risco para a segurança em caso de falha.

-Para garantir a segurança, o S.O. usa várias técnicas de autenticação, controle de acesso e auditoria

Base de computação confiável de um sistema operacional



Fonte: Sistemas Operacionais: Conceitos e Mecanismos (Carlos Maziero)

Autenticação

- Para identificação de um usuário e recursos em um sistema.

- Técnicas de Autenticação: login/senha, esquemas de biometria, certificados criptográficos,...

  -Uma autenticação permite ao usuário acessar a sessão dele para criar processos, threads ou transações representando o usuário.

- Em função do usuário é definida uma política de controle de acesso

Senha e segurança da senha

- O nível de segurança da senha depende da arquitetura de armazenamento de senha do sistema, mas também do formato da senha (número de caracteres da senha, uso de numero, caracteres especiais, lógica da senha, número de sites onde a senha é usada, ...).

- Técnicas de armazenamento de senha (pouco recomendadas) : banco de dados, Criptografia, hashes de senha, hashing and salting, ...

Referências

- SEGURANÇA EM SISTEMAS DISTRIBUÍDOS. Disponível em: <https://sites.google.com/site/proffdesiqsistemasdistribuidos/aulas/10-seguranca-em-sistemas-distribuídos>. Acesso em: 01 de outubro de 2021.
- SEGURANÇA EM SISTEMAS DISTRIBUÍDOS. Disponível em: <http://www.inf.puc-rio.br/~noemi/sd-10/seguranca.pdf>. Acesso em: 01 de outubro de 2021.
- Sistemas Operacionais: Conceitos e Mecanismos (Carlos Maziero): http://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=socm:socm-26.pdf . Acesso em: 24 de Outubro de 2021
- KUROSE, James F. **Redes de computadores e a Internet**: uma abordagem top-down. São Paulo: Pearson Education do Brasil, 2013. xxii, 634 p., il. Inclui bibliografia e índice. ISBN 9788581436777 .
- TANENBAUM, Andrew S. **Redes de computadores**. São Paulo: Pearson Education, 2011. xvi, 582 p., il., grafs., tabs. Inclui bibliografia e índice. ISBN 9788576059240 (broch.).