



# **Administração & Segurança de Redes de Computadores**

Introdução à Segurança da Informação

# Quem sou eu na fila do pão?

- Quase 20 anos trabalhando com desenvolvimento web e administração de sistemas Linux
- Faixa Laranja em Seg. da Informação?
  - “Você não precisa ser faixa preta para ensinar um faixa branca.” Ricardo Jordão Magalhães



# Nesse vídeo

- Segurança: conceitos básicos
- Alguns tipos de ataques
- Alguns mecanismos de prevenção




# Conceitos básicos



# Segurança da Informação

- Confidencialidade: manter em segredo dados secretos
- Integridade: os dados estão corretos?
- Disponibilidade: os dados estão acessíveis?

- 
- Acidentes x Ataques
    - Segurança da informação lembra ataques mas muitos problemas são causados por acidentes
  - Tipos de acidentes
    - Fenômenos naturais: fogo, água, terremoto, poeira, animais, etc
    - Falhas de software: erros em programas, bugs diversos
    - Falhas de hardware: problemas em servidores, discos, etc
    - Falhas humanas: uso incorreto de software e/ou hardware



# Prevenindo acidentes

- Backup (“quem tem dois tem um, quem tem um não tem nenhum”);
- Manter backup em local físico diferente;
- Testar backup;

# Tipos de atacantes

- Usuários leigos curiosos
- Pessoal técnico interno
- Agentes externo
  - “Script kiddies”
  - Fraudes de engenharia social: spammers
  - Profissionais externos: ataque à bancos
  - Governos x governos : espionagem industrial





# Tipos de ataques

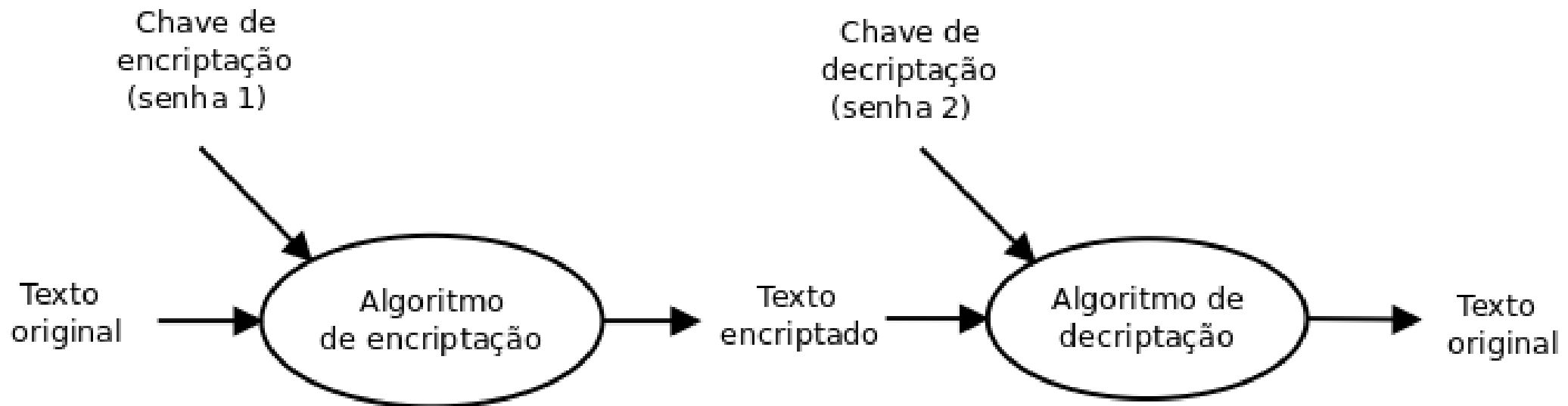
- Ataques remotos
- Ataques locais
  - Ladrões comuns
  - Atacantes especializados



# Criptografia

- “[...] área que estuda e pratica princípios e técnicas para comunicação segura na presença de terceiros [...]”
  - <https://pt.wikipedia.org/wiki/Criptografia>
- Tipos
  - Chave pública
  - Chave privada

# Criptografia



Fonte: Autor, inspirado por Tanenbaum  
(Sistemas Operacionais)



# Criptografia de chave privada

- Baseada em compartilhar uma chave (“senha”) entre dois agentes confiáveis
- Problema básico: como compartilhar a senha?
- Exemplo clássico: cifra de César

# Cifra de César

- Trocar uma letra por outra, aplicando uma rotação
- Exemplo 1 (rotação = 3):
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - DEFGHIJKLMNOPQRSTUVWXYZABC
- Exemplo 2 (rot = 3):
  - A LIGEIRA RAPOSA MARROM SALTOU  
SOBRE O CACHORRO CANSADO
  - D OLJHLUD UDSRVD PDUURP VDOWRX  
VREUH R FDFKRUUR FDQVDGR



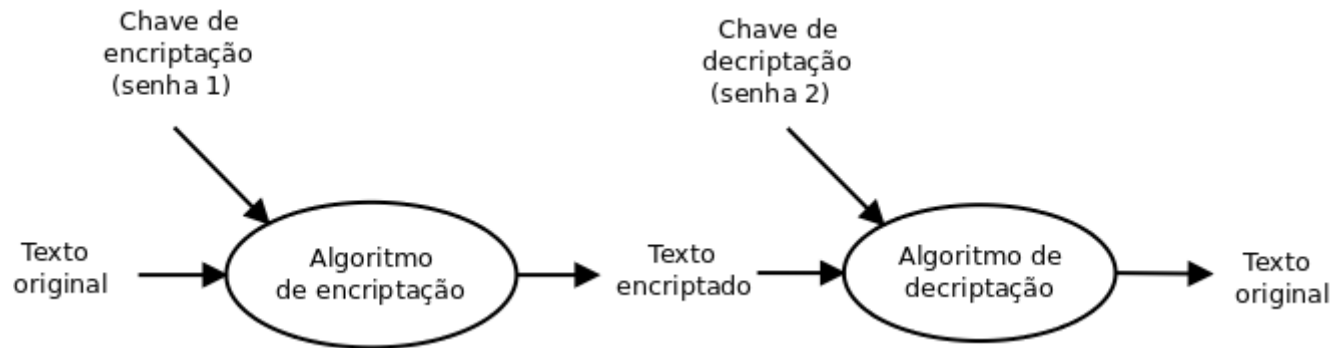
# Cifra de César (2)

- Método simples e intuitivo
  - Foi “inventado” várias vezes ao longo da história
- Possível de ser quebrado com criptoanálise (baseada na frequência das letras em um determinado alfabeto)

# Criptografia de chave pública

- Se baseia no fato de que algumas funções são de mão única, ou seja
  - Calcular:  $f(a) = b$ , é fácil
  - Mas calcular  $\text{InvF}(b) = a$ , é inviável computacionalmente
  - Exemplo:
    - Descubra quais números primos que multiplicados resultam em 187. Resposta: 11 e 17
    - Qual o resultado da multiplicação de dois números primos 11 e 17?

# Criptografia de chave pública (2)



- Nessa caso a chave de encriptação é a chave pública (conhecida). A chave de deciptação é a chave privada.
- Se A quer mandar uma mensagem para B, ele criptografa a mensagem usando a chave pública de B. Só B pode ler a mensagem pois só ele tem a chave privada.



# Tipos de autenticação

- Baseados em algo que você sabe:
  - Senhas e códigos
- Baseados em algo que você é:
  - Digitais, íris, etc
  - Contras: não dá pra mudar
- Baseados em algo que você tem:
  - Pendrives, crachás, etc
  - Contras: caro de fabricar, pode ser roubado/perdido

# O problema das senhas

- Quanto maior melhor
- Se a senha for muito difícil o usuário não vai decorar
  - Vai trocar por algo mais fácil
  - Vai anotar em algum lugar
- Frases (geralmente) são melhores do que sopa de letrinhas:
  - “Eu gosto de viver em Pelotas” é melhor do que “Xkfldffnez”

# Roubo de digitais?



<https://search.creativecommons.org/photos/acdc0fad-fdb2-4bd6-8dad-a83758b1df78>



# Nomes

- Cracker x hacker
- Black hat, white hat, grey hat



# Segurança por obscuridade

- “Se eles não verem meu código não irão me atacar”
  - Não garante segurança
  - Gera falsa segurança
  - Não permite que os usuários corrijam problemas

# Segurança por obscuridade (2)

- Software livre é sempre mais seguro então?
  - Só botar o código no github não resolve;
  - Mais usuários → Mais segurança
  - Questão Android:
    - Mais usuários → Mais interesse dos crackers → Mais exploração de falhas



## Alguns tipos de ataques

# Alguns tipos de ataques

- Engenharia social: “oi, eu sou da XYZ e vim limpar o seu datacenter”;
  - Contra-medida: Educação dos usuários
- Ataques de negação (indisponibilidade): muitos acessos artificiais em um servidor;
  - Contra-medida: Bloquear endereços IPs e firewall ajudam um pouco;



# Alguns tipos de ataques (2)


- Acesso shell. Ex: Exemplo servidor web que aceita comandos
  - Contramedidas:
    - Evite dar acesso!
    - Virtualização ajuda um pouco
- Escalada de privilégios: usuário transformar usuário em super-usuário
  - Contramedidas:
    - Mantenha sistema atualizado


# Alguns tipos de ataque (3)

- SQL Injection: Permitir ao usuário executar comandos SQL direto no banco de dados.
  - `$sql = "SELECT FROM USERS WHERE SENHA = " + $_POST['senha'];`
    - E se `$_POST['senha']` tiver `" 'senha'; 1=1"`
  - Contra-medida: Redobre cuidado com dados enviados pelo usuário
- Ransomware: Dados são criptografados e criminoso cobra pela senha:
  - Contra-medida: backup; restringir privilégios dos usuários;



Como vírus funcionam?

- 
- Como ocorre o começo de uma infecção?
    - Vulnerabilidades de softwares;
    - Usuário executa programa com vírus (software pirata?);
  - Vírus ao executar pela primeira vez procura outros executáveis para infectar

- 
- Vírus pode se copiar:
    - Para sobreescrever outros programas (mas o original para de funcionar e o usuário percebe algo errado)
    - Para o início de outros programas (mas isso pode afetar os endereços do programa original – que pode parar de funcionar)
    - Para o fim de outros programas ou para a invocação de métodos ou funções

- 
- Código sem vírus

JUMP FUNC

..

FUNC:

ADD 1, 2

RET

- Código com vírus

JUMP VIRUS

...

VIRUS:

CODIGO\_VIRUS

JUMP FUNC

FUNC:

ADD 1,2

RET



## Medidas de prevenção



# Medidas gerais

- Usar gerenciador de senhas
- Máquinas virtuais para acessar bancos e lojas
- Cartões virtuais (cancelar após uso)
- Não instalar software pirata





# Segurança para Devs

- Desenvolver pensando em segurança
- Testes automatizados
- Uso de bibliotecas e frameworks bastante usados
- Conhecer principais tipos de ataques



# Segurança para SysAdmins

- Manter sistemas atualizados
- Negar acesso por padrão
- Firewall

Se possível:

- Ter equipe de segurança
- Equipe de segurança simula tentativa de ataque



# Finalizando

- Não brinque de invasão – Mesmo dar uma “espiadinha” é crime
  - Chantagem é um crime pior ainda
  - Se descobrir algo: avise os responsáveis e siga com sua vida
- Programas de “bug bounty”: empresas pagam por vulnerabilidades

# Links e Referências

- Referência
  - Tanenbaum, Andrew. Sistemas Operacionais Modernos. Ed. Pearson, 2ª edição, 2003.
- Links
  - Como a máquina Enigma funcionava
  - Coding horror: Regras para senhas são bobagens
  - Coding horror: Hacker: hackeie-se a si mesmos
  - OWASP: Top 10
  - Como se tornar um hacker