

# Auditoria e Segurança de Sistemas

# Sumário

- Introdução à Segurança
- Criptologia
- Assinatura Digital
- Serviços
- Vírus
- Segurança de Rede
- Firewall
- Defesas de Rede
- Estratégias de Segurança
- Segurança em Linux
- Auditoria de Sistemas

# Introdução à Segurança

- Popularização da Internet
- O que se procura proteger?
  - Dados:
    - segredo
    - integridade
    - disponibilidade
  - Recursos
  - Reputação

# Introdução à Segurança

- Contra o que se proteger?
  - Tipos de ataques:
    - Intrusão: os invasores são capazes de realmente usar os computadores.
    - Negação de serviço: é aquele que é completamente orientado para impedi-lo de usar seus próprios computadores.
    - Roubo de informações: Permitem a um atacante obter dados sem sequer precisar usar diretamente seus computadores.

# Introdução à Segurança

- Tipos de atacantes:
  - Vândalos: pessoas que estão dispostas a causar danos, seja por causa de sua tendência a destruir coisas ou por vingança.
  - Marcadores: pessoas que querem deixar uma marca que consigam invadir o site.
  - Espiões: pessoas que pretendem roubar informações.
- Em quem você confia?

# Introdução à Segurança

- Como é possível proteger o seu site?
  - nenhuma segurança
  - segurança através da obscuridade
  - segurança de host
  - segurança de rede

# Criptologia

- Conceitos
  - Criptologia: ciência das mensagens secretas. É composta pelas disciplinas de criptografia e de criptanálise.
  - Criptografia: disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo, impedir modificações e o uso ilegal dos mesmos.
  - Criptoanálise: métodos para analisar mensagens cifradas com o objetivo de decifrá-las.

# Criptologia

- Esteganografia

- Comunicação secreta por ocultação de mensagem.

- Do grego:

- steganos* = coberto

- graphein* = escrever

- Atualmente é utilizada para esconder textos em imagens ou em outros textos.

- Segurança por obscuridade.



# Criptologia

- Esteganografia

- Exemplo

*O Senhor Evandro quer usar este salão temporariamente.*

*Relembre o fato ocorrido, isto poderia estragar relíquias, florais e imagens talhadas. Obrigado.*

O sequestro foi perfeito.

# Criptologia

- Esteganografia
  - Ferramentas:
    - Tatu – Esteganografia pela Web
      - <http://www.geb.com.br/tatu>
    - Outguess
      - <http://packages.debian.org/unstable/utils/outguess>
    - Camaleão
      - <http://www.dcc.unicamp.br/~ra030014/ic/estego/index.php3>

# Criptologia

- Criptografia

- Surgiu da necessidade de se enviar informações sensíveis através de meios de comunicação não confiáveis.
- Comunicação secreta por cifragem de mensagem.
- Do grego:
  - kriptos* = oculto
  - graphein* = escrever
- Evolução paralela à Esteganografia.
- A mensagem é misturada de acordo com um protocolo específico estabelecido previamente entre o transmissor e o receptor.
- Vantagem: leitura ilegível no caso de interceptação.

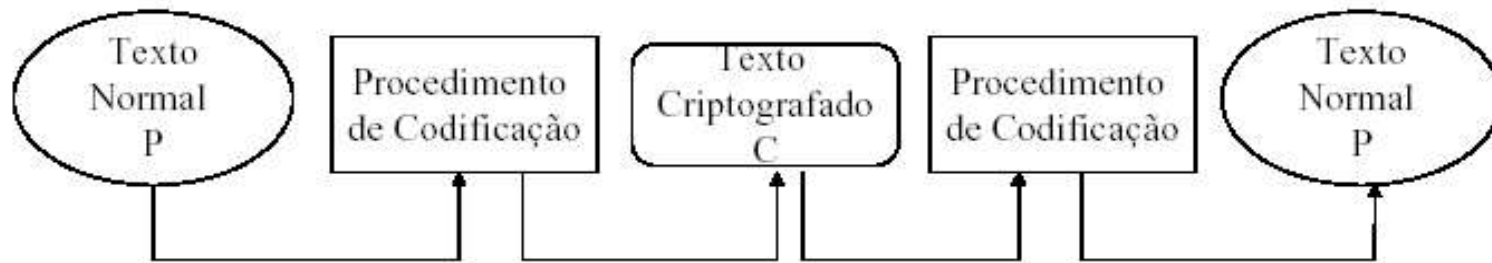
# Criptologia

- Criptografia
  - A criptografia pode ser utilizada em conjunto com a Esteganografia.
  - Exemplo: Microponto (utilizado pela Alemanha durante a Segunda Guerra Mundial) Redução fotográfica de uma página de texto a um ponto com menos de 1mm de diâmetro.

# Criptologia

- Criptografia

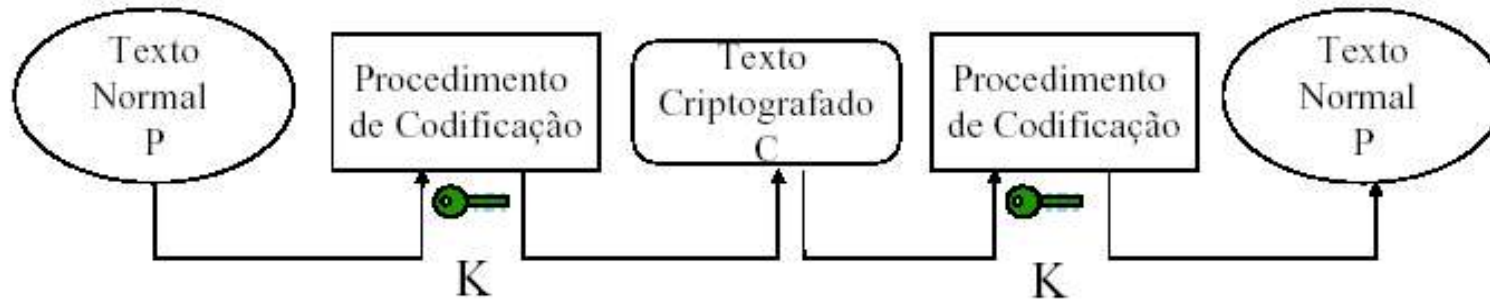
- Esquema básico dos métodos de criptografia:



# Criptologia

- Criptografia

- O uso de chaves faz com que o intruso precise conhecer o método de criptografia e as chaves.
- Método de criptografia usando chaves.



# Criptologia

- Criptografia simétrica
  - Os algoritmos de chave simétrica são também conhecidos como algoritmos de chave única e caracterizam-se por utilizar a mesma chave tanto para a cifragem como para a decifragem dos dados.
  - Esse método funciona em aplicações limitadas, como as militares, onde o emissor e o receptor podem se preparar antecipadamente para trocar a chave.
  - Também conhecido como tradicional.
  - Computacionalmente leves e rápidos.

# Criptologia

- Criptografia simétrica
  - Técnica de Substituição
    - Letras da mensagem são substituídas por outras letras e/ou símbolos conforme uma tabela de conversão.
    - Exemplo: A = X; C = Y; T = K; R = Z. ATACAR = XKXYXZ
    - Esta técnica possui duas variantes:
      - Monoalfabéticas (substituição simples).
      - Polialfabéticas.
    - Este tipo de técnica é considerada pouco segura e deve utilizada apenas para textos pequenos.



# Criptologia

- Criptografia simétrica

- Técnica de Transposição

- O conteúdo da mensagem é rearranjado, gerando um anagrama.
    - Exemplo: ema = eam, aem, mea, mae, ame.
    - Outro exemplo: mensagem original escrita alternando as letras em duas linhas (uma abaixo da outra).
    - A mensagem cifrada é então escrita concatenando-se as duas linhas.
    - Exemplo:
      - Encontro às cinco horas no pátio da escola.

O	H	O	R	A	S	E
C	A	E	S	C	N	N

# Criptologia

- Criptografia simétrica
  - Algoritmo
    - É o próprio processo de substituição ou transposição.
    - Consiste nos passos a serem tomados para realizar a encriptação.
  - Chave
    - Define o alfabeto cifrado exato que será utilizado em uma codificação em particular.
  - O algoritmo utilizado em um processo de encriptação pode ser divulgado sem problemas. A chave, porém, deve ser uma informação confidencial do remetente e do destinatário.

# Criptologia

- Criptografia simétrica
  - Cifra
    - Nome dado a qualquer forma de substituição criptográfica, no qual cada letra é substituída por outra letra ou símbolo.
  - Alfabeto Original
    - Conjunto de caracteres usado para escrever a mensagem original (antes de ser encriptado).
  - Alfabeto Cifrado
    - Conjunto de caracteres usado na substituição de uma mensagem em uma encriptação.

# Criptologia

- Data Encryption Standard (DES)
  - Desenvolvido no período da Guerra Fria.
  - Proposta inicial tinha o nome de Lucifer.
  - Desenvolvido pela IBM em 1977.
  - Utilizado como um padrão para comunicação segura.
  - Principal algoritmo derivado da criptografia simétrica.
  - Utiliza uma chave de 64 bits de comprimento.
  - Mensagem é codificada em blocos também de 64 bits.
  - Em 1998, uma equipe conseguiu fazer a quebra do código em apenas 46 horas.

# Criptologia

- Data Encryption Standard (DES)
  - Funcionamento:
    - Uma transposição inicial.
    - 16 ciclos intermediários de substituições e transposições.
    - Uma transposição final.
  - O principal problema, assim como todos os algoritmos simétricos, é a exigência que o transmissor e o receptor de uma mensagem conheçam a chave secreta, e única, usada na codificação e na decodificação.

# Criptologia

- Data Encryption Standard (DES)
  - Triple-DES
    - É apenas o DES efetuado três vezes com duas chaves na mesma ordem.
    - Funcionamento:
      - Uma primeira chave é utilizada para cifrar a mensagem em DES.
      - Uma segunda chave é utilizada para decifrar a mensagem cifrada (como a chave não é a correta, apenas faz embaralhar ainda mais os dados).
      - A mensagem é então novamente cifrada com a primeira chave, chegando ao código final.
      - Este procedimento em três etapas é chamada de 3DES.
    - É possível também utilizar três chaves, ao invés de duas.

# Criptologia

- Criptografia assimétrica
  - Os algoritmos de chave pública e privada, também chamados de algoritmos de chave assimétrica, utilizam duas chaves: uma pública que pode ser divulgada e outra secreta conhecida somente por pessoas autorizadas.
  - Baseada em princípios de manipulação matemática.
  - Computacionalmente pesados e lentos.

# Criptologia

- RSA Ron Rivest / Adi Shamir / Leonard Adleman
  - Criado em 1977.
  - É o algoritmo de chave pública mais utilizado.
  - Utiliza números primos.
  - A premissa por trás do RSA é que é fácil multiplicar dois números primos para obter um terceiro número, mas muito difícil recuperar os dois primos a partir daquele terceiro número.
  - Isto é conhecido como fatoração.
  - Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. Levou cerca de 7 meses e foram utilizadas 300 estações de trabalho para a quebra.



# Criptologia

- RSA Ron Rivest / Adi Shamir / Leonard Adleman
  - Cerca de 95% dos sites de comércio eletrônico utilizam chaves RSA de 512 bits.
  - O desenvolvimento dos algoritmos de criptografia assimétrica possibilitou o aparecimento de aplicações que trafegam dados internet de forma segura, notadamente do e-commerce.

# Assinatura Digital

- Certificado Digital
  - É um documento criptografado que contém informações necessárias para identificação de uma pessoa ou entidade jurídica.
  - Objetivo é garantir a autenticidade da origem.
  - Para validade do certificado é necessária a participação de duas entidades:
    - uma AR (Autoridade de Registro).
    - uma AC (Autoridade Certificadora).
  - O papel de uma AR é requisitar a emissão de certificados digitais de uma AC.

# Assinatura Digital

- Certificado Digital
  - É um arquivo no computador que identifica o usuário, servindo para comprovar a identidade para outra pessoa ou outro computador.
  - Um certificado digital normalmente contém as seguintes informações:
    - A chave pública do usuário.
    - Nome e endereço de e-mail.
    - Validade da chave pública.
    - Nome da Autoridade Certificadora (AC).
    - Número de série do certificado digital.
    - Assinatura digital da AC.

# Assinatura Digital

- Certificado Digital
  - A obtenção do certificado é feito através de uma CA. Para isso é necessário que o certificado digital venha de uma CA que proveja confiança das principais companhias que trabalham na internet.
  - Exemplo:
    - Quando o usuário consulta o seu banco on-line, este tem que se certificar de que o usuário é a pessoa que pode receber a informação sobre a conta. Como uma carteira de motorista ou um passaporte, um certificado digital confirma a identidade para o banco on-line.

# Assinatura Digital

- Certificado Digital
  - Princípios básicos para manutenção da segurança:
    - Preservar a chave privada e os certificados.
    - As ACs e ARs devem ser confiáveis em si.
    - Em caso de suspeitas de fraude, como roubo ou clonagem, do certificado, deve-se fazer imediatamente o pedido de revogação.
    - Nunca deixar a chave privada em locais de acesso público.  
Exemplos: CD-ROMs, disquetes, diretórios compartilhados etc.

# Assinatura Digital

- Assinatura Digital
  - A assinatura digital de uma mensagem consiste na anexação da parte pública do certificado digital, juntamente com outras informações que garantem a integridade do e-mail.
  - Antes do envio a mensagem passa por um processo de codificação, chamado de algoritmo hash, através do qual a mensagem que está sendo enviada é utilizada para gerar matematicamente um conjunto de caracteres (letras e números), que só podem ser criados pela mensagem do usuário (message digest).
  - O algoritmo hash funciona rapidamente numa direção, mas é muito difícil funcionar na direção inversa.

# Assinatura Digital

- Assinatura Digital
  - Uma vez criado a message digest, o programa utiliza a chave privada do usuário para criptografá-lo.
  - O receptor utiliza o programa para decifrar o message digest, utilizando a chave pública do usuário.

# Questões Práticas

- Tamanho da chave
  - A criptoanálise, ciência de decodificação de cifras, se baseia no fatoramento de números grandes.
  - Quanto maior a chave mais difícil de decifrá-la.
- Revogação de certificado
  - O que acontece quando uma chave privada é comprometida ou uma chave pública passa a ser inválida?
  - Nesse caso, os certificados deixam de ser confiáveis, pois as informações que eles estão verificando não mais verdadeiras.
  - A solução atual é a divulgação através de listas.



# Questões Práticas

- Fazer ou não caução
  - Muitas empresas afirmam que, como a comunicação dos funcionários é propriedade da empresa, a organização deverá ter acesso às chaves dos funcionários e recuperar mensagens.
  - Problema de privacidade por parte dos funcionários.
- O que fazer com todas essas informações
  - O arquivamento de chaves e de dados criptografados é uma questão difícil.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Permite encriptar dados, assim somente o destinatário terá acesso aos dados, adicionalmente poderá verificar se a origem dos dados é confiável (através da assinatura de arquivos).
  - O sistema PGP se baseia no conceito de chave pública e privada: a chave pública do usuário é distribuída para as pessoas que ele deseja trocar dados/mensagens e a chave privada fica na sua máquina (ela não pode ser distribuída). As chaves públicas e privadas são armazenadas nos arquivos `pubring.gpg` e `secring.gpg` respectivamente, dentro do subdiretório `~/.gnupg`.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Os dados que recebe de outra pessoa são criptografados usando sua chave pública e somente o usuário (de posse da chave privada) poderá descriptar os dados. Quando assina um arquivo usando o PGP, ele faz isto usando sua chave privada, o destinatário de posse da chave pública poderá então confirmar que a origem dos dados é confiável.
  - O GPG vem largamente sendo usado para transmissão segura de dados via internet.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Instalando o PGP
    - `apt-get install gnupg`
    - Após instalar o gnupg, execute o comando `gpg` para criar o diretório `~/.gnupg` que armazenará as chaves pública e privada.
  - Criando um par de chaves pública/privada:
    - Para gerar um par de chaves pessoais use o comando `gpg --gen-key`.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Ele executará os seguintes passos:
    1. Chave criptográfica Algoritmos: DSA, ELGamal e RSA.
    2. Tamanho da chave - 1024 bits traz uma boa combinação de proteção/velocidade.
    3. Validade da chave - 0 a chave não expira. Um número positivo tem o valor de dias, que pode ser seguido das letras w (semanas), m (meses) ou y (anos). Por exemplo, "7m", "2y", "60". Após a validade, a chave será considerada inválida.
    4. Nome de usuário - Nome para identificar a chave
    5. E-mail - E-mail do dono da chave
    6. Comentário - Uma descrição sobre a chave do usuário.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Ele executará os seguintes passos:
    7. Confirmação - Tecle "O" para confirmar os dados ou uma das outras letras para modificar os dados de sua chave.
    8. Digite a FraseSenha - Senha que irá identificá-lo(a) como proprietário da chave privada. É chamada de FraseSenha pois pode conter espaços e não há limite de caracteres.
    9. Confirme e aguarde a geração da chave pública/privada.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Encriptando dados
    - Use o comando `gpg -e arquivo` faz a encriptação de dados:
      - `gpg -e arquivo.txt`
    - Será pedida a identificação de usuário, digite o nome que usou para criar a chave. O arquivo criado será encriptado usando a chave pública do usuário (`~/.gnupg/pubring.gpg`) e terá a extensão `.gpg` adicionada (`arquivo.txt.gpg`). Além de criptografado, este arquivo é compactado (recomendável para grande quantidade de textos). A opção `-a` é usada para criar um arquivo criptografado com saída ASCII 7 bits:
      - `gpg -e -a arquivo.txt`
    - O arquivo gerado terá a extensão `.asc` acrescentada (`arquivo.txt.asc`) e não será compactado.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Decriptando dados com o gpg
    - Agora vamos fazer a operação reversa da acima, a opção -d é usada para decriptar os dados usando a chave privada:
    - `gpg -d arquivo.txt.asc >arquivo.txt`
    - `gpg -d arquivo.txt.gpg >arquivo.txt`
    - Descriptografa os arquivos `arquivo.txt.asc` e `arquivo.txt.gpg` recuperando seu conteúdo original. A sua "FraseSenha" será pedida para descriptografar os dados usando a chave privada (`~/.gnupg/secring.gpg`).



# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Assinando arquivos
    - Assinar um arquivo é garantir que você é a pessoa que realmente enviou aquele arquivo. Use a opção -s para assinar arquivos usando sua chave privada:
    - `gpg -s arquivo.txt`
    - A "FraseSenha" será pedida para assinar os dados usando sua chave privada. Será gerado um arquivo `arquivo.txt.gpg` (assinado e compactado).

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Checando assinaturas
    - A checagem de assinatura consiste em verificar que quem nos enviou o arquivo é realmente quem diz ser e se os dados foram de alguma forma alterados. Você deverá ter a chave pública do usuário no seu chaveiro para fazer esta checagem. Para verificar os dados assinados acima usamos a opção --verify:
    - `gpg --verify arquivo.txt.asc`
    - Se a saída for "Assinatura Correta", significa que a origem do arquivo é segura e que ele não foi de qualquer forma modificado.
    - `gpg --verify arquivo.txt.gpg`
    - Se a saída for "Assinatura INCORRETA" significa que ou o usuário que enviou o arquivo não confere ou o arquivo enviado foi de alguma forma modificado.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Extraindo sua chave pública do chaveiro
    - Sua chave pública deve ser distribuída a outros usuários para que possam enviar dados criptografados ou checar a autenticidade de seus arquivos. Para exportar sua chave pública em um arquivo que será distribuído a outras pessoas ou servidores de chaves na Internet, use a opção `--export`:
    - `gpg --export -a usuario >chave-pub.txt`
    - Ao invés do nome do usuário, poderá ser usado seu e-mail, ID da chave, etc. A opção `-a` permite que os dados sejam gerados usando bits ASCII 7.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Adicionando chaves públicas ao seu chaveiro pessoal
    - Isto é necessário para o envio de dados criptografados e checagem de assinatura do usuário, use a opção `--import`:
    - `gpg --import chave-pub-usuario.txt`
    - Assumindo que o arquivo `chave-pub-usuario.txt` contém a chave pública do usuário criada em `Extraindo sua chave pública do chaveiro`. O `gpg` detecta chaves públicas dentro de textos e faz a extração corretamente.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Listando chaves de seu chaveiro
    - Use o comando `gpg --list-keys` para listar as chaves pública do seu chaveiro. O comando `gpg --list-secret-keys` lista suas chaves privadas.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Apagando chaves de seu chaveiro
    - Quando uma chave pública é modificada ou por qualquer outro motivo deseja retirá-la do seu chaveiro público, utilize a opção --delete-key:
    - `gpg --delete-key usuario`
    - Pode ser especificado o nome de usuário, e-mail IDchave ou qualquer outro detalhe que confira com a chave pública do usuário. Será pedida a confirmação para excluir a chave pública.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Apagando chaves de seu chaveiro
    - OBS: A chave privada pode ser excluída com a opção `--delete-secret-key`. Utilize-a com o máximo de atenção para excluir chaves secretas que não utiliza (caso use mais de uma), a exclusão acidental de sua chave secreta significa é como perder a chave de um cofre de banco: você não poderá descriptografar os arquivos enviados a você e não poderá enviar arquivos assinados.
    - Mesmo assim se isto acontecer acidentalmente, você poderá recuperar o último backup da chave privada em `~/.gnupg/secring.gpg`.

# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Mudando sua FraseSenha
    - Execute o comando `gpg --edit-key usuário`, quando o programa entrar em modo de comandos, digite `passwd`. Será lhe pedida a "Frase Senha" atual e a nova "Frase Senha". Digite "save" para sair e salvar as alterações ou "quit" para sair e abandonar o que foi feito.
    - O `gpg --edit-key` permite gerenciar diversos aspectos de suas chaves é interessante exploralo digitando "?" para exibir todas as opções disponíveis.



# Criptologia

- O GPG (GNU PGP, versão livre da ferramenta PGP)
  - Listando assinaturas digitais
    - Execute o comando `gpg --list-sigs` para listas todas as assinaturas existentes no seu chaveiro. Opcionalmente pode ser especificado um parâmetro para fazer referência a assinatura de um usuário: `gpg --list-sigs usuario`.
    - O comando `gpg --check-sigs` adicionalmente faz a checagem de assinaturas.

# Serviços

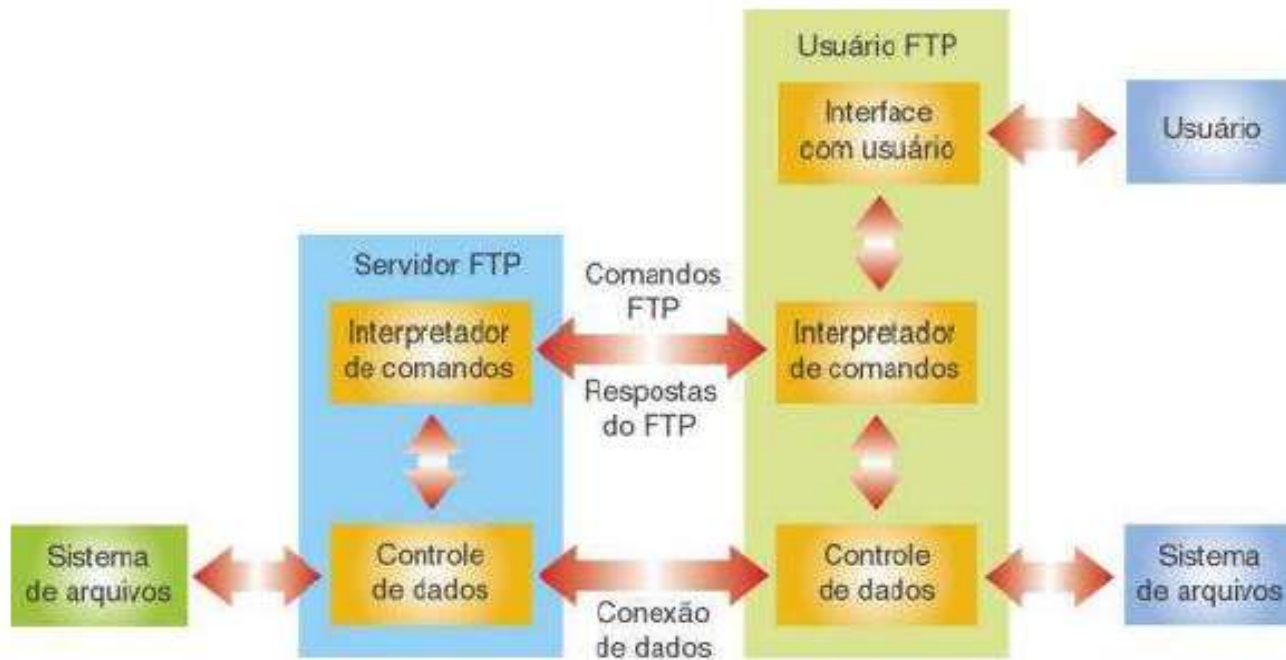
- File Transfer Protocol (FTP)
  - Surgiu em 1971 para satisfazer a necessidade que o MIT tinha em transferir arquivos.
  - O FTP é o método-padrão de transferir arquivos de um sistema para outro.
  - Os seus objetivos são (RFC 0765):
    - Promover compartilhamento de arquivos.
    - Encorajar utilização indireta ou implícita de computadores remotos.
    - Proteger um usuário das variações em sistemas de armazenamento de arquivo entre hosts.
    - Transferir dados de forma confiável e eficiente.

# Serviços

- File Transfer Protocol (FTP)
  - É necessária a autenticação do usuário para que seja permitida a sua conexão.
  - Muitos servidores utilizam o chamado FTP anônimo.

# Serviços

- File Transfer Protocol (FTP)
  - Arquitetura



# Serviços

- File Transfer Protocol (FTP)

- Principais comandos de FTP

- ftp (IP/DNS): conexão
    - lcd: muda o diretório local.
    - hash: habilita as marcas de progressão.

- Tipos de arquivos:

- ascii: arquivos do tipo texto.
    - binary: todos os outros tipos.

- Baixar os arquivos:

- get: faz o download de um arquivo por vez.
    - mget: faz o download de vários arquivos.
    - reget: continua o download a partir do final do arquivo que está em sua máquina local (espécie de resume).

- Enviar arquivos:

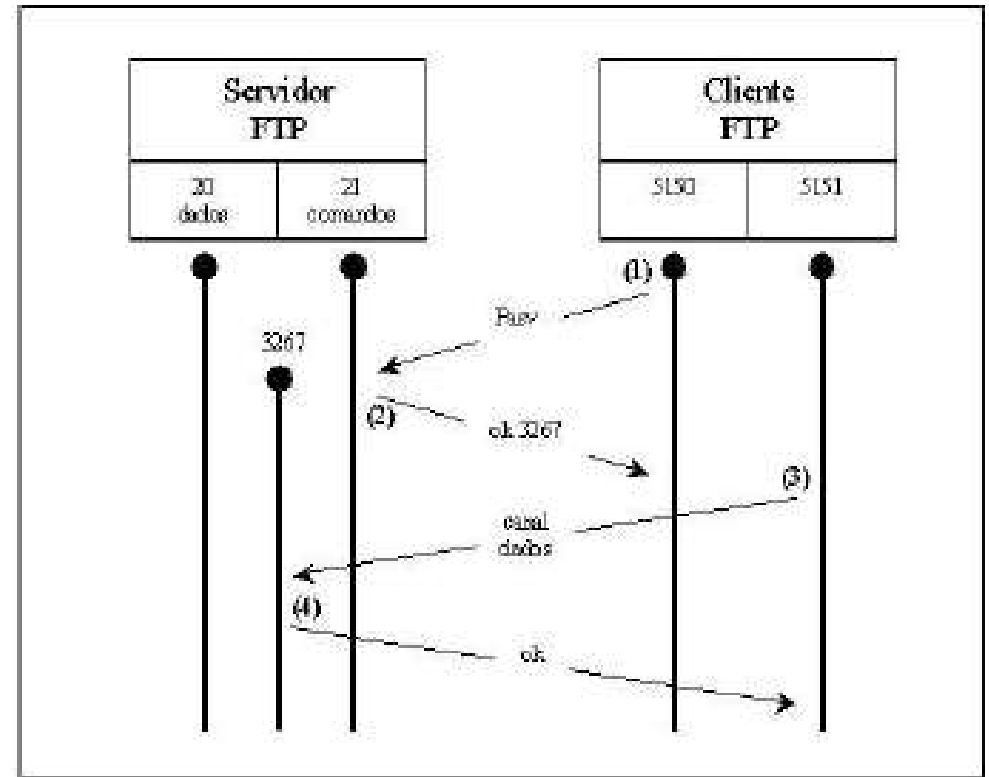
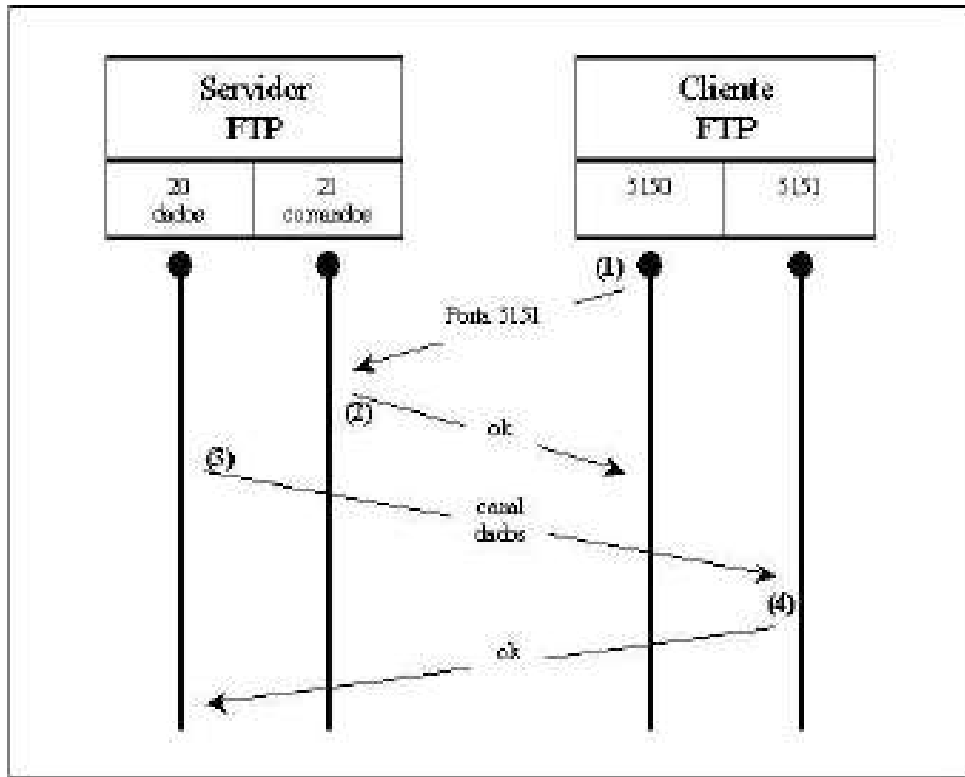
- put: faz o envio de um arquivo por vez.
    - mput: faz o envio de vários arquivos por vez.

# Serviços

- FTP Modo Normal vs. Passivo
  - Configurar o serviço de FTP em modo passivo (passive mode) permite, ao administrador do sistema, delimitar o número (range) de portas pelas quais se dará a transferência dos dados. Isso representa um considerável incremento de segurança, não especificamente para o serviço de FTP, mas para a máquina que provê o serviço.
  - Numa conexão FTP normal, o cliente indica, aleatoriamente, a porta em que deseja que os dados sejam transferidos.

# Serviços

- FTP Passivo x Normal



# Serviços

- As principais deficiências do FTP são:
  - O FTP utiliza a autenticação de nome de usuário/senha-padrão. Como resultado, o servidor não pode determinar de forma confiável se um determinado usuário é realmente quem ele afirma ser.
  - Por padrão, as senhas são transmitidas em texto simples. Isso permite aos invasores interceptar eletronicamente e capturar senhas.
  - As sessões de FTP não são criptografadas e, portanto, não oferecem nenhuma privacidade.



# Serviços

- TELNET
  - O serviço telnet oferece o login remoto em um computador, permitindo ao usuário trabalhar conectado à distância, como se estivesse em frente da máquina remota.

# Serviços

- TELNET

- Características:

- Conexão rápida (não utiliza transmissão de dados criptografada), recomendado para ambientes seguros.
    - Possui uma versão com suporte a criptografia via ssl.
    - Possui controle de acesso tcpd (usando /etc/hosts.allow e /etc/hosts.deny).
    - A maioria dos sistemas operacionais trazem este utilitário por padrão como sistema de acesso remoto a máquinas UNIX.
    - Suporte a terminais ANSI (cores e códigos de escape especiais para o console) e uma grande variedade de outros terminais.
    - A porta padrão é a 23 e pode ser modificada no arquivo /etc/services.
    - Como os dados transferidos são texto-pleno, estes podem ser capturados por sniffers e aumentar o risco na segurança.

# Serviços

- Ficha técnica do TELNET:
  - Pacotes:
    - telnet - Cliente telnet com suporte a autenticação.
    - telnetd - Servidor telnet com suporte a autenticação.
    - telnet-ssl - Cliente telnet com suporte a autenticação e ssl. Também suporta conexão a servidores telnet padrão quando o servidor não suporta ssl. Por padrão é tentada a conexão usando ssl, se esta falhar será assumida a transmissão em texto plano.
    - telnetd-ssl - Servidor telnet com suporte a autenticação e ssl. Também suporta conexão de clientes telnet padrão (sem suporte a ssl).

# Serviços

- Ficha técnica do TELNET:
  - Utilitários:
    - in.telnetd - Servidor telnet.
    - telnet - Cliente telnet padrão.
    - telnet-ssl - Cliente telnet com suporte a ssl.

# Bibliografia

# Serviços

- Principais comandos do TELNET:
  - telnet [endereço] [porta]
- Principais opções:
  - -l [usuário] : envia o nome do usuário ao computador remoto.
  - -a : tentar fazer o login automático usando o nome de usuário local.
  - -r : emula o comportamento do programa rlogin.

# Serviços

- SSH
  - O serviço de ssh permite fazer o acesso remoto ao console de uma máquina, em outras palavras, o usuário poderá acessar uma máquina como se estivesse conectado localmente ao seu console.
  - A principal diferença com relação ao serviço telnet padrão, rlogin e rsh é que toda a comunicação entre cliente/servidor é feita de forma encriptada usando chaves públicas/privadas RSA para criptografia garantindo uma transferência segura de dados.
  - A velocidade do console remoto conectado via Internet é excelente, dando a impressão de uma conexão em tempo real.

# Serviços

- SSH
  - A compactação dos dados também pode ser ativada para elevar ainda mais a velocidade entre cliente-servidor ssh.
  - Em conexões sem criptografia (rsh, rlogin) os dados trafegam de forma desprotegida e caso exista algum sniffer instalado em sua rota com a máquina destino, todo o que fizer poderá ser capturado (incluindo senhas).



# Serviços

- SSH Características
  - Conexão de dados criptografada entre cliente/servidor.
  - Cópia de arquivos usando conexão criptografada.
  - Suporte a ftp criptografado (sftp).
  - Suporte a compactação de dados entre cliente/servidor.
  - Controle de acesso das interfaces servidas pelo servidor ssh.
  - Autenticação usando um par de chaves pública/privada RSA ou DSA.
  - Algoritmo de criptografia livre de patentes.
  - Suporte a caracteres ANSI (cores e códigos de escape especiais no console).

# Serviços

- SSH Características
  - Uma outra característica favorável é que, por ser muito semelhante ao TELNET, facilita o seu uso.
  - O SSH permite criar um produto extensível mais flexível. A arquitetura dele é tal que o protocolo de base não importa com qual algoritmo é utilizado. Portanto, pode-se, futuramente, alterar o algoritmo sem alterar as suas funcionalidades.

# Serviços

- SSH Ficha técnica:
  - Arquivos de configuração:
    - `/etc/ssh/sshd_config` Arquivo de configuração do servidor ssh.
    - `/etc/ssh/ssh_config` Arquivo de configuração do cliente ssh.
    - `~/.ssh/config` Arquivo de configuração pessoal do cliente ssh.

# Serviços

- Aplicativos de SSH
  - Secure Shell (SSH)
    - O ssh funciona quase da mesma forma que um cliente telnet. Uma vez conectado ao servidor, você pode utilizar ssh para realizar comandos básicos de sistema e em cada aspecto sua sessão de ssh se parecerá com uma sessão de telnet.
    - Comando: `ssh usuario@ip/nome_do_servidor_ssh`
    - Caso o nome do usuário seja omitido, será utilizado o login atual do sistema.
    - Opções:
      - C : ativa o modo de compactação de dados (útil em conexões lentas).
      - l : determina o nome do usuário.
      - p : especifica o número da porta. A porta padrão é a 22.

# Serviços

- Aplicativos de SSH
  - Secure Shell Copy (SCP)
    - O programa Secure Shell Copy fornece um meio seguro de copiar arquivos de um host para outro. Funciona quase da mesma maneira que o rcp, mas utiliza ssh para facilitar as transferências.
    - Comando:
      - scp [origem] [destino]
      - Exemplo: usuario@host\_remoto:/diretório/arquivo
  - Aplicativos de SSH
    - Secure FTP (SFTP)
    - Permite realizar transferência de arquivos segura, através do protocolo SSH.
      - Comando: sftp usuario@host\_remoto

# Serviços

- Secure Socket Layer - SSL
  - É um padrão (protocolo) desenvolvido pela Netscape Communications para transferir informações de modo seguro na Internet, desde que ambos, o servidor e o cliente, apoiem o protocolo.
  - O SSL permitirá que o cliente se conecte ao Web Site e, de forma transparente, será criado um canal de comunicação seguro entre o Site e o Cliente.
  - Uma vez que esta conexão é feita, informações, como o número de cartões de crédito, senhas de contas corrente, poderão ser fornecidas sem que alguma outra pessoa possa interceptar os dados, ou seja, de uma maneira segura.

# Serviços

- Secure Socket Layer - SSL
  - Esta segurança é garantida pela encriptação, os usuários que interceptarem a mensagem no caminho, ficam impedidos de acessar o conteúdo da mensagem, já que não conseguirão entender o que está sendo transmitido.
  - O SSL utiliza como protocolo de transporte o TCP, que providencia uma transmissão e recepção confiável dos dados. Uma vez que o SSL reside no nível de socket, ele é independente das aplicações de mais alto nível, sendo assim considerado um protocolo de segurança independente do protocolo aplicativo. Como tal, o SSL pode providenciar serviços seguros para protocolo de alto nível, como por exemplo TELNET, FTP e HTTP.

# Serviços

- Secure Socket Layer - SSL
  - Como funciona SSL?
  - Existem três componentes principais para um site Web seguro:
    - - 1. Servidor: o melhor lugar da Internet para armazenar o Web Site.
    - - 2. Software Seguro: este é o software instalado no servidor, que faz todo o trabalho de criptografia.
    - - 3. Certificado de Assinatura: é como uma "assinatura digital".



# Serviços

- HTTPS x SHTTP
  - Existem duas grandes abordagens para a solução do problema de segurança no nível dos protocolos da camada de aplicação na arquitetura Internet: o HTTPS e o SHTTP.
  - HTTPS é a utilização do protocolo HTTP (HyperText Transfer Protocol) em conjunto com o protocolo SSL (secure Sockets Layer), que é um protocolo proposto por um grupo liderado pela Netscape Communications, pela Verisign e pela Sun desenvolvido e especificado para prover uma camada de segurança entre a camada de transporte (TCP) e os protocolos de aplicação tais como HTTP, TELNET, FTP, NNTP, SMTP, etc.
  - Este protocolo provê encriptação de dados, autenticação de servidor, integridade de mensagem e, opcionalmente, autenticação de cliente para uma conexão TCP/IP.

# Serviços

- HTTPS x SHTTP
  - SHTTP (secure HTTP) é uma extensão do protocolo http proposta pelo EIT no começo de 1994 que provê transações seguras pela incorporação de criptografia, mecanismos de autenticação no protocolo HTTP permitindo transações seguras fim-a-fim entre cliente e servidor WWW.
  - SSL e SHTTP têm diferentes motivações: as camadas de segurança SSL ficam sob os protocolos de aplicação, como HTTP, NNTP e TELNET, enquanto que HTTPS adiciona segurança baseada nas mensagens especificamente do protocolo HTTP no nível da aplicação.
  - Estas duas aplicações, longe de serem mutuamente exclusivas, podem coexistir perfeitamente de forma complementar com o protocolo HTTPS atuando sobre a camada SSL.

# Vírus

- Introdução

- Pesquisas mostram que 50% dos prejuízos em software são culpa de mau uso ou inexperiência dos usuários.
- O usuário inexperiente destrói muito mais dados do que qualquer vírus.
- Existem mais de 20.000 vírus reconhecidos.
- Um vírus de computador é um programa que pode infectar outro programa de computador através da modificação daquele, de forma a incluir uma cópia de si mesmo.
- O vírus de computador foi a primeira forma de vida construída pelo homem Stephen Hawking .

# Vírus

- Conseqüências
  - Erro na hora da execução de um arquivo.
  - Baixa de memória.
  - Lentidão para entrar em programas.
  - Danificação de dados.
  - Danificação drivers.
  - Formatação indesejada de HD.
  - Alocação desnecessária de memória de computador.

# Vírus

- Vírus de arquivos
  - O vírus se agrega a arquivos executáveis. Ex.: .exe, .com e .scr.
  - Podem ser classificados em dois tipos: ação direta e residentes.
  - Os vírus de ação direta selecionam um ou mais programas para infectar cada vez que o programa que o contém é executado.
  - Os vírus residentes escondem-se em algum lugar na memória na primeira vez que um programa infectado é executado. Esse tipo de vírus também pode ser ativado a partir de eventos ou pré-condições determinadas pelo criador.

# Vírus

- Vírus de Sistema ou de Boot
  - Infectam códigos executáveis localizados nas áreas de sistema do disco.
  - Uma outra técnica é exibir os arquivos de boot originais sempre que for feita uma solicitação de leitura do sector 1 da trilha 0.

# Vírus

- Vírus Múltiplos
  - São aqueles que visam tanto os arquivos de programas comuns como os setores de boot do DOS.
- Vírus de Macro
  - O Concept foi primeiro vírus de macro do Microsoft Word (1995).
  - Se esconde em arquivos de dados. Ex: planilhas e editores de texto.
  - Grande propagação devido ao grande número de usuários desses aplicativos.
  - São construídos a partir da própria linguagem dos aplicativos.
  - Ele se autocopia para o modelo global do aplicativo e, a partir daí, se propaga para todos os documentos que forem abertos.

# Vírus

- Vírus Stealth ou Furtivo
  - Utiliza técnicas de dissimulação para que sua presença não seja detectada nem pelo antivírus, nem pelos usuários.
- Vírus Encriptados
  - São vírus que, por estarem codificados, dificultam a ação de qualquer anti-vírus.
  - Não são comuns pelo fato de serem difíceis de serem criados.



# Vírus

- Vírus Mutantes ou Polimórficos
  - Têm a capacidade de gerar cópias de si mesmo, utilizando-se de chaves de encriptação diversas, fazendo que as cópias finais possuam formas diferentes.
  - O objetivo é dificultar a detecção de utilitários anti-vírus, já que as cópias não podem ser detectadas a partir de uma única referência do vírus.
- Vírus Stealth ou Furtivo
  - Utiliza técnicas de dissimulação para que sua presença não seja detectada nem pelo antivírus, nem pelos usuários.

# Vírus

- Vírus Encriptados
  - São vírus que, por estarem codificados, dificultam a ação de qualquer anti-vírus. Não são comuns pelo fato de serem difíceis de serem criados.
- Vírus Mutantes ou Polimórficos
  - Têm a capacidade de gerar cópias de si mesmo, utilizando-se de chaves de encriptação diversas, fazendo que as cópias finais possuam formas diferentes.
  - O objetivo é dificultar a detecção de utilitários anti-vírus, já que as cópias não podem ser detectadas a partir de uma única referência do vírus.

# Vírus

- Vermes
  - É um pedaço de programa para computadores em rede.
  - Ele é um programa de autoduplicação, que não se esconde em outro programa, como faz um vírus.
  - Robert Morris lançou o verme mais famoso em 1988.
  - Causou uma falha em cerca de 6000 computadores (10% da internet).

# Vírus

- O vírus cavalo-de-tróia
  - Utiliza o mesmo princípio dos cigarros-explosivos ou de um daqueles livros que dão choque.
  - Não se reproduz.
  - É também conhecido como programas que capturam senhas sem o conhecimento do usuário.

# Vírus

- Precauções:
  - Possuir um bom software de anti-vírus e atualizado.
  - Deixar a auto-proteção ligada.
  - Checagem de disquetes desconhecidos.
  - Antes de baixar um arquivo da Internet, fazer uma verificação.
  - Possuir um disquete de boot limpo.
  - Proteção para o arquivo NORMAL.DOT.

# Vírus

- Programas anti-vírus:
  - O método mais comum é procurar por uma seqüência de bytes que constituem o programa vírus.
  - Eles mantêm um banco de dados de pegadas de vírus trechos de código que são conhecidos como parte de vírus.
  - Recursos especiais:
    - Tecnologia Push: atualiza a lista de vírus.
    - ScreenScan: varre o disco rígido enquanto o sistema está ocioso.

# Vírus

- Principais programas anti-vírus:
  - VirusScan:
    - Produzido pela McAfee
      - É o mais conhecido.
      - Possui 10.160 vírus listados.
    - Norton
      - Produzido pela Symantec.
      - Possui 9.600 vírus listados.
      - Monitora a presença de vírus durante a realização de download na internet.
      - Conseguir trabalhar em segundo plano.

# Vírus

- Principais programas anti-vírus:
  - Dr. Solomons
    - Possui 13.000 vírus listados.
    - Possui um módulo para analisar a chegada de arquivos contaminados pela internet.
    - Pode trabalhar em segundo plano.



# Vírus

- Classificação do Modus Operandis:
  - Vírus de disco - Stoned, Michelangelo, Ping-Pong
    - Infectam o boot-sector.
  - Vírus de arquivo - Jerusalém, Athenas, Freddy
    - Infectam arquivos executáveis ou de extensão .SYS, .OVL, .MNU.
  - Vírus residentes
    - São vírus muito simples e que funcionam apenas como programas auto-reprodutores.
  - Vírus não-residentes
    - São mais sofisticados, pois permanecem na memória após o uso do programa infectado.

# Vírus

- Detecção
  - Um vírus, como todo programa, ocupa espaço em disco.
  - A sua execução faz o programa aumentar de tamanho e alterar a data de gravação. Ex: Jerusalém.
  - Companheiros
    - São vírus que não infectam programas (.exe).
    - Criam um arquivo de extensão (.com) cujo atributo é alterado para hidden.
  - Polimórficos
    - O vírus se altera a cada vez que infecta um novo arquivo.
    - Dessa forma o vírus cria N variações de si próprio.
    - O objetivo é que se pelo menos uma variação escapasse ao anti-vírus, ela poderia reinfectar todos os arquivos novamente.

# Vírus

- Detecção
  - Retrovírus
    - São vírus que têm como alvo antivírus.
    - Alguns têm código para desativar antivírus residentes.

# Vírus

- Sintomas:
  - Demora maior na execução de um programa.
  - Aumento do tamanho dos programas.
  - Alteração na data de criação do programa.
  - No caso de vírus de disco, é possível que alguns arquivos do disquete simplesmente desapareçam.
  - Programa Windows deixar de funcionar ou congela rapidamente.

# Segurança de Rede

- O mundo atual em rede pode ser mais conveniente, mas é também muito mais desprotegido.
- Segurança do IP
  - À medida que os pacotes passam de um roteador para outro, os dados estão abertos a qualquer um queira vê-los.
  - Maior interesse pelos pacotes com senhas.
  - A quebra dos pacotes permite inserção de código.
  - Ataque no roteamento.
- Segurança do DNS
  - Problemas nas tabelas do DNS.
  - Propagação para outros servidores DNS.

# Segurança de Rede

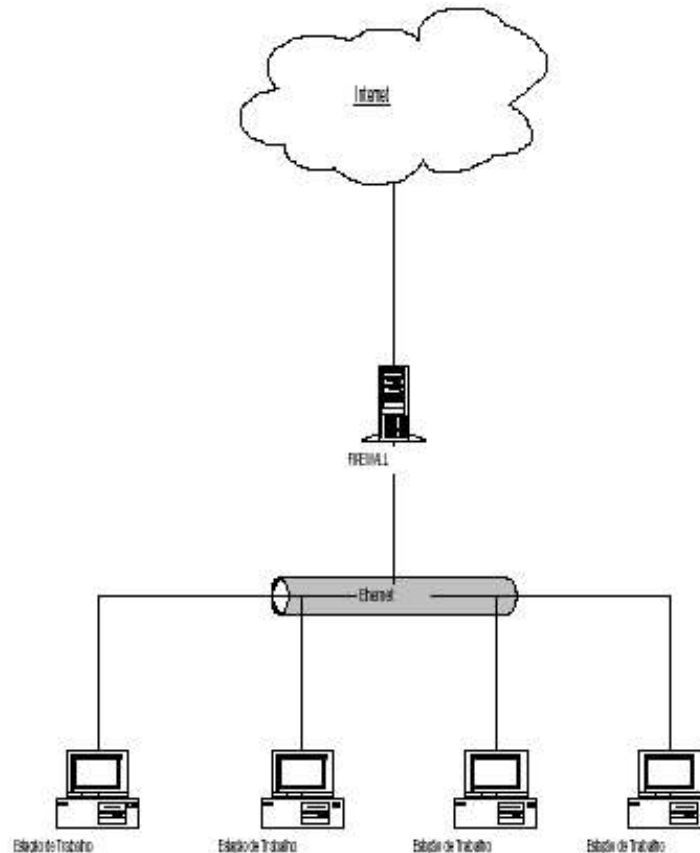
- Ataques de Negação de Serviço
  - Em 1996, hackers inundaram um provedor de serviços (ISP) com 50 mensagens por segundo.
  - A idéia é o envio de muito material que faça o host parar.
  - Uma solução seria forçar o cliente a realizar um cálculo complexo para completar a conexão.
- Ataques de Negação de Serviço Distribuída
  - São diversas origens de ataque.
  - Procedimento:
    - Invasão de milhares de computadores desprotegidos (zumbis).
    - Instala um programa de ataque.
    - Coordena para atacar o alvo no mesmo momento.

# Firewall

- O que é um firewall da Internet?
  - É uma forma de proteção que permite a rede se conectar à Internet ao mesmo tempo que mantém um certo grau de segurança.
- Quais são os propósitos de um firewall?
  - Limita a entrada das pessoas a um ponto cuidadosamente controlado.
  - Impede que os atacantes cheguem perto de suas outras defesas.
  - Limita a saída das pessoas a um ponto cuidadosamente controlado.

# Firewall

- Conceito:
  - Conjunto de componentes de hardware um roteador, um computador host ou alguma combinação destes com software apropriado.





# Firewall

- O que um firewall pode fazer?
  - Controle da segurança da rede.
  - Impõe uma política de segurança.
  - Permite registrar as atividades da Internet.
  - Limita a exposição de segmentos de rede.

# Firewall

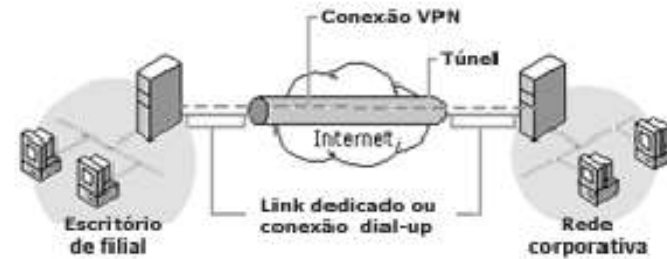
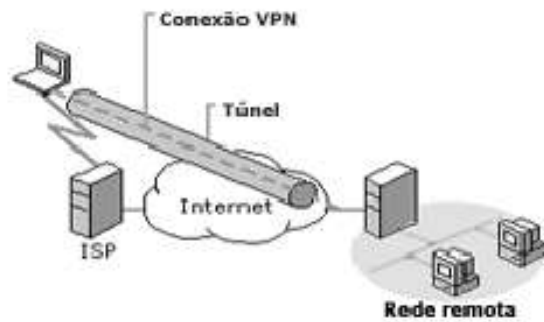
- O que um firewall não pode fazer?
  - Não garante uma segurança completa.
  - Não pode proteger a rede contra usuários internos maliciosos.
  - Não pode proteger a rede contra conexões que não passam através dele.
  - Não pode proteger a rede contra ameaças completamente novas.
  - Não pode proteger completamente a rede contra vírus.
  - Não pode configurar a si próprio corretamente.

# Defesas de Rede

- Redes Privadas Virtuais (VPNs)
  - É uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a internet.
  - Possuem duas aplicações principais:
    - Conectar pedaços separados da mesma rede.
    - Conectar usuários móveis
  - Um dos objetivos é a diminuição de custos.

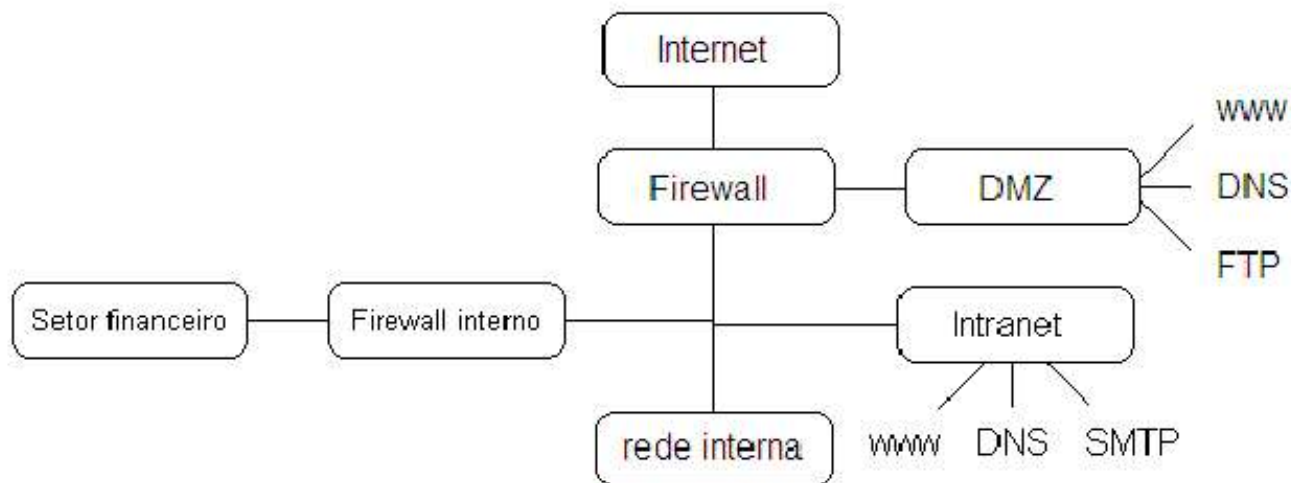
# Defesas de Rede

- Redes Privadas Virtuais (VPNs)



# Defesas de Rede

- Zonas Desmilitarizadas (DMZs)
  - Lugar da rede onde são colocados os serviços públicos.
  - Necessidade de dois firewalls.
  - O resultado é uma parte semipública da rede e uma mais privada da rede.



# Defesas de Rede

- Sistemas de Detecção de Intrusão (IDSs)
  - O que são?
    - São monitores de rede.
  - O que fazem?
    - Alertam sobre um ataque bem-sucedido, ou até mesmo de um ataque em desenvolvimento.
    - Informa qual é o ataque e de onde está vindo.
  - O problema mais difícil são os alarmes falsos.
  - Tipos:
    - Detecção por mau uso.
    - Detecção por anomalia.

# Defesas de Rede

- Potes de Mel e Alarmes Contra Roubo
  - Os alarmes contra roubo são específicos na rede, projetadas para dispararem se um hacker tocar neles.
  - Os potes de mel são alarmes contra roubo enfeitados para que se pareçam particularmente atraentes aos hackers.
  - Os primeiros são mais simples de serem construídos.
  - Exploram a vantagem que o administrador da rede tem sobre o hacker: conhecimento da rede.

# Defesas de Rede

- Analisadores de Vulnerabilidade
  - Programa automatizado que analisa a rede para uma imensa lista de fraquezas conhecidas.
  - Possuem limitações, pois não podem analisar realmente todas as vulnerabilidades, e nem podem realmente medir os efeitos de suas ações.



# Segurança de Rede

- Segurança do E-mail
  - O que se espera?
  - Queremos nos certificar de que ninguém, além do destinatário intencionado, possa ler a mensagem.
  - Queremos nos certificar de que uma mensagem de e-mail veio da pessoa que afirma ter vindo, e que ninguém poderá forjar as mensagens do e-mail.
  - Uma solução é o uso de criptografia.

# Confiabilidade do Software

- Falhas no código
  - É difícil acabar com bugs de software que afetam o desempenho; localizar falhas de software que afetam a segurança é ainda mais difícil.
  - As falhas que afetam o desempenho são observadas, enquanto que as falhas de segurança podem permanecer invisíveis por um longo tempo.
- Estouros de buffer
  - São a forma mais comum de vulnerabilidade de segurança nos últimos dez anos.
  - Fácil de ser explorada.

# Confiabilidade do Software

- Onipresença do código com falhas
  - Estimativas da Universidade de Carnegie Mellon mostram que mil linhas de código normalmente possuem de cinco a quinze bugs.
  - Estimativas informam que mais de 99% de todos os ataques na internet poderiam ser impedidos se os administradores de sistema simplesmente usassem as versões mais recentes do seu software no sistema.
  - A evolução do software não é garantia da eliminação de bugs.

# Hardware Seguro

- Resistência à falsificação
  - Em geral, o hardware à prova de falsificação é perfeito para relacionamentos de confiança complexos, onde uma parte deseja colocar um dispositivo seguro nas mãos de outra, com a certeza de que a segunda parte não poderá modificar o interior do dispositivo seguro.
  - O problema básico é que o hardware à prova de falsificação não existe.
  - Apesar de ser um grande mito, a resistência à falsificação oferece uma barreira para a entrada.
  - A resistência à falsificação deverá ser reforçada por outras contramedidas.
  - Qualquer sistema onde o dispositivo e os segredos dentro dele estiverem sob o controle de diferentes pessoas possui uma falha de segurança fundamental.

# Hardware Seguro

- Ataques colaterais
  - São ataques que visam detalhes de implementação específicos.
  - A análise crítica no ataque de temporização.
  - Exemplo: verificador de senhas.

# Hardware Seguro

- Ataques contra cartões inteligentes
  - Os cartões inteligentes são ferramentas de finalidade múltipla que podem ser usadas para controle de acesso, e-commerce, autenticação, proteção de privacidade e uma série de outras aplicações.
  - O processador e a memória dentro dele são (supostamente) invulneráveis a ataques.
  - Como existe uma grande quantidade de partes envolvidas, torna esses cartões muito suscetíveis a muitas classes de ataques.

# Truques de Segurança

- Acesso do governo às chaves.
  - O governo americano tem tentado forçar o público americano a aceitar a idéia de que eles deverão dar, a algum parceiro aprovado pelo governo, acesso à sua privacidade.
  - Eufemismos:
    - Recuperação de chaves.
    - Criptografia confiada a terceiros.
    - Acesso excepcional.
    - Recuperação de mensagem.
    - Recuperação de dados.

# Truques de Segurança

- Funcionamento:
  - Primeiro, um mecanismo, externo ao sistema principal, pelo qual um terceiro pode obter acesso completo ao texto dos dados criptografados.
  - Segundo, a existência de uma chave de recuperação secreta altamente sensível (ou coleção de chaves) que precisa ser protegida por um período de tempo estendido.
- Dificuldades:
  - São sistemas menos seguros.
  - Mais caros.
  - Mais difíceis de se usar.
  - Exige proibição legal de produtos diferentes.
  - Desconhecimento atual por parte dos profissionais da área.



# Truques de Segurança

- Segurança do Banco de Dados
  - Os bancos de dados podem ser configurados para mostrarem apenas certos campos a certos usuários.
  - Uso de protocolos de autenticação e listas de controle de acesso.
  - Muito mais difícil é lidar com consultas em que o usuário pode ver informações de agregação, mas não pode ver entradas individuais.
  - O problema é de fazer inferência.

# Truques de Segurança

- Esteganografia
  - A esteganografia apenas não é suficiente.
  - Um problema é a largura de banda.
  - Uma alternativa é usar uma mensagem secreta muito, muito menor do que a mensagem pública.
  - Isso é chamado de canal subliminar.

# Truques de Segurança

- Marca D Água Digital
  - O objetivo é manter o controle sobre a propriedade intelectual.
  - Problemas:
    - Os mecanismos para a marca d água acabarão se tornando público.
    - Outra vulnerabilidade é que ela não resolve o problema básico. "

# Truques de Segurança

- Proteção contra cópia
  - Problema se aplica a vários produtos, além de software: livros, filmes, vídeos etc.
  - Algumas soluções:
    - Código incorporado no software que desativa a cópia.
    - Código que utiliza aspectos não copiáveis do disco original.
    - Dispositivos de hardware que o software precisa para rodar.
  - Porém, qualquer esquema de proteção contra cópia pode ser quebrado.
  - O dongle é um dispositivo de hardware, largamente utilizado, que se encaixa no computador, normalmente na porta paralela.
  - Possível estratégia comercial: Se algo será pirateado, então que seja o meu produto e não o do concorrente (Microsoft).

# Truques de Segurança

- Apagando informações digitais
  - A maneira de realmente apagar um arquivo de um disco magnético é regravá-lo com um novo arquivo.
  - Alguns utilitários de arquivo para apagar fazem isso.
  - Existe uma técnica chamada microscopia de força magnética que pode ser usada para recuperar dados mesmo depois que eles foram regravados várias vezes.
  - Os dados também são difíceis de se apagar no hardware. Tanto SRAM quanto DRAM retêm alguns restos dos dados após a perda da energia. Os bits podem ser recuperados detectando-se eletronicamente as mudanças nos patamares da célula com base no conteúdo anterior da célula.

# Fator Humano

- Introdução
  - As pessoas normalmente representam o elo mais fraco na corrente da segurança e cronicamente são responsáveis pela falha dos sistemas de segurança.
- Risco
  - As pessoas não sabem como analisar riscos.
  - Grande parte das proteções são baseadas em probabilidades.
- Tratamento de exceção
  - Um perigo dos sistemas computadorizados é que eles cometam erros tão raramente que as pessoas não saibam como lidar com eles.

# Fator Humano

- Interface Homem-Máquina
  - As pessoas querem segurança, mas não querem vê-la funcionando.
- Transferência Homem-Máquina
  - O problema fundamental é que você pode não ter idéia alguma quanto ao que o computador está realmente fazendo quando você lhe diz para fazer algo.

# Fator Humano

- Internos maliciosos
  - O principal problema é que, implicitamente, eles são considerados confiáveis.
  - A auditoria normalmente determina as partes culpadas, mas não consegue evitar os fatos.
  - Possíveis soluções:
    - Contratação de pessoas honestas (mais fácil no discurso).
    - Difusão da confiança.
    - Auditoria.



# Fator Humano

- Engenharia Social

- Um modo de ação do invasor é telefonar para os empregados da empresa.
- A engenharia social é o termo de cracker para um jogo de trapaça: persuadir a outra pessoa a fazer o que você deseja.
- Ela consegue contornar a criptografia, segurança de computador, segurança de rede, atingindo o elo mais fraco: o ser humano.

# Estratégias de Segurança - Vulnerabilidades

- Em geral, existem cinco etapas para um ataque bem-sucedido:
  - Identificar o alvo específico que será atacado e coletar informações sobre esse alvo.
  - Analisar as informações e identificar uma vulnerabilidade no alvo, que realizará os objetivos do ataque.
  - Obter um nível de acesso apropriado ao alvo.
  - Realizar o ataque no alvo.
  - Completar o ataque, o que pode incluir a eliminação da evidência do ataque, evitando a retaliação.

# Estratégias de Segurança - Vulnerabilidades

- Contramedidas
  - São métodos para reduzir as vulnerabilidades.
  - Assim como o ataque a um sistema é mais complicado do que simplesmente encontrar uma vulnerabilidade, a defesa de um sistema é mais complicada do que a inclusão de uma contramedida.
  - Existem três partes de um conjunto eficaz de contramedidas:
    - Proteção. Ex: criptografia, firewalls, senhas.
    - Detecção. Ex: sistema de detecção de intrusão.
    - Reação. Ex: sistema de login que trava o usuário.

# Estratégias de Segurança - Vulnerabilidades

- Contramedidas

- Mecanismos de proteção fortes significam que você não precisa de bons mecanismos de detecção e reação.  
Mecanismos de proteção fracos - ou ainda nenhum mecanismo de proteção significam que você precisa de melhores mecanismos de proteção e detecção.
- A confiança singular da segurança digital nos mecanismos de proteção é errada e é o principal motivo por que vemos ataques após ataques contra os sistemas.

# Estratégias de Segurança - Vulnerabilidades

- O panorama da vulnerabilidade
  - Pode ser dividido em quatro categorias:
    - Mundo físico.
    - Mundo virtual.
    - Modelo de confiança.
    - Ciclo de vida do sistema.

# Estratégias de Segurança - Vulnerabilidades

## – Segurança física

- A segurança física é um problema que o mundo tem tentado solucionar desde o início dos tempos: a noção de propriedade.
- Paredes, cadeados, guardas armados são ferramentas da segurança física.
- Ao montar sistemas de segurança digital, os projetistas normalmente se esquecem da segurança física. Ex: roubo de laptops.

## – Segurança virtual

- Um bom sistema utiliza várias contramedidas diferentes em conjunto: firewalls protegendo o acesso aos sistemas por pessoas de fora, autenticação forte para garantir que somente os usuários autorizados se conectem e haja criptografia de dados de ponta a ponta.

# Estratégias de Segurança - Vulnerabilidades

## – Modelo de confiança

- O modelo de confiança representa como uma organização determina a quem ela confia seus ou partes de seus bens.
- No mundo físico é relativamente fácil identificar aqueles indivíduos que são confiáveis e aqueles que não são.

# Estratégias de Segurança - Vulnerabilidades

- Ciclo de vida de um sistema
  - O ambiente de trabalho no mundo virtual é o software rodando nos computadores da rede.
  - Os crackers podem atacar esse software em qualquer parte do seu ciclo de vida.
  - Exemplos:
    - Um desenvolvedor de software malicioso poderia intencionalmente deixar uma porta aberta dos fundos na última versão do sistema operacional.
    - Um adversário poderia colocar um cavalo de tróia em um browser na internet e distribuí-lo gratuitamente.
    - Poderia escrever um vírus e colocá-lo em um anexo executável de uma mensagem de e-mail.



# Estratégias de Segurança - Vulnerabilidades

- Aplicando contramedidas de modo racional
  - Faz mais sentido aplicar contramedidas uniformemente através do panorama.
  - A idéia é se proteger contra as ameaças que impõem o maior risco, em vez de se proteger contra as ameaças mais aparentes enquanto se ignora todas as outras.
  - A idéia também é tomar decisões de investimento racionais na aplicação de contramedidas.
  - O valor normalmente depende do contexto e nem sempre é o mesmo para atacantes e defensores.

# Estratégias de Segurança – Avaliação de Risco

- Introdução
  - A modelagem de ameaça é a primeira etapa em qualquer solução de segurança.
  - A modelagem de ameaça é algo difícil de ser feito, sendo uma habilidade que só se adquire com a experiência.
  - Ela envolve pensar sobre um sistema e imaginar o vasto panorama da vulnerabilidade.

# Estratégias de Segurança – Avaliação de Risco

- Eleições justas
  - Considerando um sistema eleitoral, é possível identificar muitos pontos de ataque. Pode-se atacar os eleitores, os juízes eleitorais, as caixas de cédulas, as máquinas de contagem de votos, as ligações telefônicas ou o ponto central.
  - O suborno aos eleitores é um modo consagrado de fraudar uma eleição.
  - Pode-se tentar enganar os juízes eleitorais.
  - As urnas podem ser completadas com cédulas.
  - O ataque à máquina de contagem de votos é mais fácil.
  - O objetivo deste exemplo é mostrar que existem muitos caminhos de ataque contra um sistema, e como poucos deles envolvem a parte computadorizada do processo.

# Estratégias de Segurança – Avaliação de Risco

- Telefones seguros
  - Há muitas coisas que podemos fazer que não envolvem diretamente o telefone seguro: instalar escutas dentro de telefones seguros, subornar as pessoas que fazem e recebem as chamadas e assim por diante.
  - Um outro ataque comum é fazer com que os telefones não funcionem.

# Estratégias de Segurança – Avaliação de Risco

- E-mail seguro
  - A criptografia faz duas coisas: oferece uma assinatura digital para autenticidade e criptografia para privacidade.
  - A criptografia de e-mail é mais arriscada do que a criptografia de ligações telefônicas. Para telefones, a informação só está em risco pela duração da chamada. Para o e-mail, que pode estar armazenado nos dois lados por períodos de tempo consideráveis, a informação está em risco também enquanto repousa.

# Estratégias de Segurança – Avaliação de Risco

- Avaliação de risco
  - Não basta apenas listar as ameaças, mas é preciso saber o quanto deve se preocupar com cada uma delas.
  - A idéia básica é apanhar as ameaças, estimar a perda esperada por incidente e o número esperado de incidentes por ano e depois calcular a expectativa de perda anual.
  - Exemplos:
    - Se o risco for uma intrusão na rede por hackers procurando algo para fazer, a perda esperada por incidente poderia ser de R\$ 10.000,00
    - O número de incidentes por ano poderia ser três por dia, ou mil por ano.
    - Isso significa que a expectativa é de R\$ 10.000,00.
    - Então a aquisição de um firewall por R\$ 25.000 seria bem razoável.

# Estratégias de Segurança – Avaliação de Risco

- Avaliação de risco
  - Alguns riscos possuem uma probabilidade de incidência muito baixa.
  - O setor de seguros faz esse tipo de cálculo o tempo todo; é assim que eles calculam os prêmios. Eles descobrem a expectativa para um determinado risco, incluem algum extra para seu custo operacional, mais o risco e usam o resultado como o custo de um prêmio de seguro contra esse risco.
  - É comum também muito chute nesse valor da expectativa.
  - Para a análise de risco relacionada ao computador, uma série de ferramentas comerciais oferece modelos e metodologias para se realizar a análise de risco.

# Estratégias de Segurança – Avaliação de Risco

- A finalidade da modelagem de ameaça
  - Ao projetar um sistema de segurança, é vital fazer esse tipo de modelagem de ameaça e avaliação de risco.
  - Atividades:
    - Entender as ameaças reais ao sistema e avaliar o risco dessas ameaças.
    - Descrever a diretriz de segurança exigida para defender contra as ameaças.
    - Projetar as contramedidas que imponham a diretriz descrita anteriormente.
  - Naturalmente, esse modelo sequencial é ideal, e o mundo real normalmente não coopera. Provavelmente, seu caminho de engenharia irá se parecer mais com um espiral, onde você repete as três etapas anteriores várias vezes, cada uma chegando mais e mais perto da segurança real.



# Estratégias de Segurança – Diretrizes de Segurança

- Introdução

- O truque é projetar sistemas que sejam protegidos contra as ameaças reais, e não usar tecnologias de segurança a esmo, acreditando que isso fará algo útil.
- O modo como isso deve ser feito é criar uma diretriz de segurança, baseada na análise de ameaça, e depois projetar mecanismos de proteção que implementem a diretriz de segurança e lidem com as ameaças.

- Diretriz de segurança

- A diretriz de segurança para um sistema deve definir os alvos e os objetivos.
- Boas diretrizes referem-se a ameaças.
- Infelizmente, a maioria das organizações não possui uma diretriz de segurança. Ou então possui, mas ninguém a segue.

# Estratégias de Segurança – Diretrizes de Segurança

- Software de cliente confiável
  - Sempre existirá uma comunidade interessada em crackear programas.
  - A única solução possível é colocar o mecanismo de criptografia no hardware seguro e depois esperar que isso atrase os profissionais por alguns anos.
  - Foi isso que a indústria de DVD aprendeu em 1999.
  - Qualquer diretriz de segurança nacional reconhecerá que não se pode defender contra os piratas profissionais com tecnologia.

# Estratégias de Segurança – Diretrizes de Segurança

- Software de cliente confiável
  - A solução implica que os provedores de conteúdo seriam inteligentes para encontrar meios alternativos de ganhar dinheiro. Exemplo: as pessoas compram o CD original porque gostam do encarte que vem junto.
  - Uma outra alternativa consiste no financiamento público de bons serviços: televisão pública, arte pública e artistas de rua. A performance é gratuita, mas as contribuições individuais fazem com que ela aconteça.

# Estratégias de Segurança – Diretrizes de Segurança

- Máquinas de caixas automáticas
  - Os modelos de confiança e segurança são mais complicados do que parece a princípio.
  - Funcionamento:
    - A máquina apanha os dados do usuário.
    - Envia-os para algum servidor central em algum lugar.
    - Recebe uma mensagem de retorno (fornecer dinheiro, não fornecer dinheiro, não retornar o cartão etc.)
  - Deve-se ter segurança contra:
    - Alguém mexendo no link de comunicação.
    - Alguém arrombando o cofre.

# Estratégias de Segurança – Diretrizes de Segurança

- Máquinas de caixas automáticas
  - Outras questões:
    - O pessoal de manutenção precisa ter acesso, tanto em horários definidos, para manutenção programada, quanto ocasionalmente, no caso de um problema.
    - Além de uma eventual mudança no contrato de manutenção e guarda.
    - Além de uma questão financeira (qualquer caixa eletrônico só vale o custo de substituição mais o dinheiro no seu interior).

# Estratégias de Segurança – Diretrizes de Segurança

- Máquinas de caixas automáticas
  - O outro lado:
    - O link de comunicação não precisa ser criptografado, apenas autenticado.
    - Os logs de auditoria, protegidos com funções de hash, devem ser armazenados no caixa eletrônico e no servidor.
    - O software deverá ser difícil de se modificar, para evitar o problema do pessoal de manutenção injetar cavalos de Tróia no sistema.
    - A segurança física é direta. O dinheiro deve ser mantido num cofre.

# Estratégias de Segurança – Diretrizes de Segurança

- Terminais de loterias computadorizados
  - Basicamente, os vendedores de loteria adquirem um par computador/impressora seguro, que imprime e valida apostas de loteria.
  - As ameaças são:
    - Os próprios vendedores podem comprar os bilhetes depois que os resultados forem conhecidos;
    - Ou alterando os bilhetes já comprados após os resultados serem conhecidos;
    - Ou operando um terminal falso que colete dinheiro mas não pague prêmio algum.
  - A solução é que os terminais deveriam estar on-line, e registrar todas as apostas com um servidor central.

# Estratégias de Segurança – Teste e Verificação do Produto

- Introdução

- O teste de segurança normal falha por vários motivos:
- As falhas de segurança podem aparecer em qualquer lugar (modelo de confiança, no projeto do sistema, nos algoritmos e protocolos, na implementação, no código-fonte&).
- Uma única falha pode quebrar com a segurança do produto inteiro.
- As não podem ser descobertas pelo teste beta normal.



# Estratégias de Segurança – Teste e Verificação do Produto

- A falha do teste
  - O teste funcional não encontrará falhas de segurança. Ao contrário de quase todos os outros critérios de projeto, a segurança independe da funcionalidade.
  - Exemplo: teste de impressão de um editor de texto.
  - A segurança trabalha com o imprevisível.
  - O que um desenvolvedor de sistemas pode fazer?
    - O ideal é que ele pare de confiar nos seus desenvolvedores de casa e testadores beta. Ele precisa contratar especialistas de segurança para realizar seu teste de segurança.
  - Atualmente as empresas lançam os produtos inseguros e consertam os problemas de segurança que são descobertos e publicados após o fato.

# Estratégias de Segurança – Teste e Verificação do Produto

- Descobrimos as falhas de segurança após o fato
  - A segurança está ficando melhor, muito mais rapidamente, por causa da ampla divulgação.
- Padrões abertos e soluções de código-fonte aberto
  - Um bom projeto de segurança não possui segredo em seus detalhes.
  - Os sistemas de segurança públicos provavelmente serão examinados minuciosamente, sendo mais seguros do que os sistemas que não são públicos. Esse raciocínio se aplica diretamente ao software.
  - O contra-argumento é que a publicação do código-fonte só oferece aos hackers a informação de que eles precisam para encontrar e explorar as vulnerabilidades.
  - No entanto, o código-fonte aberto não garante segurança.

# Estratégias de Segurança – Teste e Verificação do Produto

- Engenharia reversa e a lei
  - Algumas empresas americanas tentaram se defender da divulgação do seu código-fonte tornando ilegal a engenharia reversa de seu software.
  - Isso abre um precedente perigoso. As leis não aumentam a segurança dos sistemas e nem impedem os atacantes de encontrarem falhas, culpando outros por sua própria inaptidão.
- Disputas de cracking e hacking
  - As empresas premiam pessoas que conseguem penetrar na sua rede.
  - As disputas são um modo terrível de demonstrar insegurança.
  - As disputas geralmente são injustas.
  - A análise não é controlada.

# Estratégias de Segurança – Teste e Verificação do Produto

- Avaliando e escolhendo produtos de segurança
  - Normalmente, as empresas não criam seus próprios produtos de segurança. Elas são forçadas a escolher entre um conjunto de soluções prontas e esperar pelo melhor.
  - A realidade é que a maioria dos problemas de segurança simplesmente não está sob o controle da maioria das pessoas.

# Estratégias de Segurança – O Futuro dos Produtos

- Introdução
  - As futuras tecnologias ajudarão aos problemas de segurança?
  - Há uma grande discussão se a segurança está se tornando melhor ou pior!

# Estratégias de Segurança – O Futuro dos Produtos

- Complexidade e segurança do software
  - Os sistemas digitais têm se tornado cada vez mais complexos.
  - A complexidade é o pior inimigo da segurança. Razões para isso:
    - O número de bugs de segurança.
    - A modularidade dos sistemas complexos.
    - A interconectividade dos sistemas complexos (sistemas distribuídos e em rede são inerentemente arriscados).
    - Quanto mais complexo for um sistema, mais recôndito ele será.
    - A dificuldade de análise.
    - São os maiores requisitos de teste para sistemas complexos.

# Estratégias de Segurança – Processos

- Introdução
  - A insegurança no computador é inevitável.
  - A tecnologia pode repelir a maioria dos invasores casuais.
  - As leis podem deter ou, pelo menos, perseguir a maioria dos criminosos. Mas os invasores passarão pelas barreiras.
  - A tecnologia sozinha não pode nos salvar.

# Estratégias de Segurança – Processos

- Princípios

- Compartimento

- A compartimentação é uma segurança inteligente, pois limita o dano de um ataque bem-sucedido.
    - Um preceito semelhante é o de menor privilégio.
    - Exemplo: chave da porta de casa para a empregada doméstica.
    - Uma forma de ataque comum é quando um invasor recebe acesso a uma conta de usuário quebrando uma senha ou algo assim -, ele tenta diversos ataques a fim de obter privilégios de raiz.

- Proteja o seu elo mais fraco

- O melhor lugar para direcionar as contramedidas é no elo mais fraco.



# Estratégias de Segurança – Processos

- Use pontos de estrangulamento
  - Um ponto de estrangulamento força os usuários a passarem por um canal estreito, que você pode monitorar e controlar com mais facilidade.
  - Exemplos: catracas de uma estação de trem, portas de casas, firewalls e roteadores.
  - No entanto, eles só funcionam se não houver um meio de contorná-los. Exemplo: uma conexão dial-up desprotegida na rede.
  - As redes possuem brechas mais sutis desse tipo. Às vezes uma empresa possui uma forte segurança de rede montada e, por algum motivo, liga a rede à de outra empresa não tão segura.

# Estratégias de Segurança – Processos

- Ofereça defesa em profundidade
  - Defesa em profundidade é outro princípio universal de segurança que se aplica a computadores e também a tudo mais.
  - Exemplo: cartões de crédito resistentes à falsificação funcionam melhor quando combinados com a verificação online e um sistema de backend especializado, que procura padrões de gastos suspeitos.

# Estratégias de Segurança – Processos

- Segurança contra falha
  - Muitos sistemas possuem uma propriedade chamada de default para insegurança.
  - Se o sistema falha, então o usuário reverte para um sistema de reserva menos seguro.
  - O que as pessoas desejam é que os sistemas falhem com segurança, ou seja, falhem de tal maneira que se tornem mais seguros, e não menos.
  - Exemplo: se o sistema de verificação de senha de um caixa eletrônico não funciona, ele deverá falhar de tal forma que não lance dinheiro para fora.

## Estratégias de Segurança – Processos

- Aproveite a imprevisibilidade
  - A segurança por obscuridade deve ser evitada.
- Um dos pontos fortes que um defensor tem contra um atacante é o conhecimento do terreno.
- Use a simplicidade
- Aliste os usuários
- Garanta-se
- Questione

# Estratégias de Segurança – Processos

- Detecção e resposta
  - Detecção é muito mais importante do que prevenção.
  - Os mecanismos de prevenção são bons, mas a prevenção é apenas uma parte da solução de segurança - e a parte mais frágil.
  - A segurança eficiente também inclui detecção e resposta.
- Terceirização de processos de segurança
  - Os processos de segurança são um meio de suavizar os riscos.

# Segurança em Linux

- Instalação
  - Existem diferenças entre as distribuições GNU/Linux:
    - Algumas ferramentas de instalação especificam automaticamente quais servidores de rede estão ativos e quais não estão, outras perguntam isso ao usuário.
    - Isso pode afetar a segurança do sistema, pois podem existir inúmeros pacotes de software e servidores instalados, sobre os quais você não conhece nada.

# Segurança em Linux

- Partições

- O que são partições?
  - As partições são áreas em sua unidade de disco que são reservadas para os sistemas de arquivos.
- Quando não se usa múltiplas partições, os dados podem ficar espalhados, tornando-se inadmissíveis e desorganizados.
- Um cenário comum de partição no Linux é separar os arquivos de troca, de um lado, e o sistema de arquivos de outro.
- Outro cenário comum é quando você instala dois ou mais sistemas operacionais na mesma unidade de disco, mas em partições diferentes e elas podem coexistir livres de problemas.

# Segurança em Linux

- Linux com outros sistemas de arquivos numa única partição:
  - Se os sistemas de arquivos raiz e os sistemas de arquivos de usuários estiverem na mesma partição, aumentará as chances de invasores explorarem áreas restritas.
  - Além disso, colocar o Linux em uma única partição nativa, junto com outros sistemas de arquivos torna difícil a vida do administrador.
  - A separação melhora a segurança e torna gerenciável o backup e a recuperação.



# Segurança em Linux

- As partições múltiplas oferecem outras vantagens:
  - Fácil gerenciamento de backup e atualização.
  - Inicialização mais rápida (em alguns casos).
  - Capacidade de controlar como cada sistema de arquivos é montado.
  - Evita a negação acidental de serviços.
  - Protege o sistema de arquivos raiz contra inundações (spamming). Ex: arquivos de log do / var.

# Segurança em Linux

- Administração Básica
  - Contas
    - Você nunca deve utilizar o root para propósitos pessoais, exceto quando absolutamente necessário, como durante uma situação de recuperação.
    - Uma conta, no sentido geral, consiste de dois elementos:
      - Autorização para efetuar login.
      - Autorização para acessar serviços.

# Segurança em Linux

## – Contas

- Se for necessário conceder acesso de shell a usuários enquanto estiver construindo uma rede Linux, deve-se observar os seguintes passos:
  - Disponha uma máquina especificamente para acesso de shell.
  - Restrinja essa máquina somente para utilização de shell.
  - Mantenha fora dela os serviços não-essenciais de rede.
  - Proíba relacionamentos de confiança entre shell e outras máquinas.
  - Redirecione logs para um servidor de log ou, se seu orçamento permitir, uma mídia write-once e registre tudo em log.
- No sentido estrito, uma conta consiste no seguinte:
  - Um nome de usuário e uma senha válida.
  - Um diretório inicial (home).
  - Acesso de shell.

# Segurança em Linux

## – Contas

- Quando um usuário tenta se conectar, o Linux verifica se esses pré-requisitos estão corretos examinando o arquivo `passwd`.
- O arquivo `/etc/passwd` consiste em entradas de contas de usuário.
- Cada linha armazena um registro de conta e cada registro consiste em sete campos separados por dois pontos.
- Exemplo:
  - `tiago:x:501:501:Tiago de Melo:/home/tiago:/bin/bash`
  - Campo 1: nome do usuário.
  - Campo 2: senha criptografada.
  - Campo 3: user ID (UID).
  - Campo 4: grupo ID (GID).
  - Campo 5: nome verdadeiro.
  - Campo 6: posição inicial do usuário.
  - Campo 7: usuário de shell.

# Segurança em Linux

- A adição de um novo usuário pode ser realizada de três maneiras:
  - Através de ferramentas gráficas.
  - Utilizando linhas de comando.
  - Editando o `/etc/passwd` manualmente.
- A remoção do usuário é através de dois passos:
  - Remoção das suas entradas de `/etc/passwd`.
  - Remoção do diretório inicial `/home/username`.

# Segurança em Linux

- Controle de acesso
  - O controle de acesso é qualquer técnica que seletivamente concede ou nega acesso de usuários a recursos de sistema, o que inclui arquivos, diretórios, volumes, unidades, serviços, hosts, redes e assim por diante.
  - No Linux é possível limitar o acesso do usuário aos arquivos através de permissões.
  - Exemplo:  
`drwxr-xr-x 12 root root 4096 Apr 24 2003 .TeXmacs`
  - Existem duas permissões especiais de arquivo:
    - SGID (configura o ID de grupo).
    - SUID (configura o ID de usuário).

# Segurança em Linux

- Eles são ditos especiais porque as permissões de proprietário são impostas mesmo quando outros usuários os executam.
- Isto é, um programa configurado como SUID de root sempre executará como root, mesmo se um usuário comum estiver utilizando.
- Por essa razão, os arquivos SGID e SUID podem ser um perigo de segurança.

# Segurança em Linux

- Ataques de senha
  - O que é um ataque de senha?
    - Qualquer ação para quebrar, decriptar ou excluir senhas, ou de outro modo superar mecanismos de segurança de senha.
  - Como o Linux gera e armazena senhas:
    - As senhas de Linux são criadas utilizando um algoritmo de criptografia chamado Data Encryption Standard (DES).
    - As senhas podem ser quebradas por duas razões:
      - O fator humano. Os usuários normalmente escolhem senhas com características fracas.
      - Comprimento limitado. As senhas de Linux são curtas.
    - Um tipo de ataque comum é o chamado de ataques de dicionários.



# Segurança em Linux

- Ele segue os seguintes passos:
  - Nestes, os invasores pegam dicionários longas listas de palavras e os criptografam utilizando DES.
  - Depois compara com as senhas de `/etc/passwd`.

# Segurança em Linux

- Sombreamento de senha
  - O sombreamento de senha é uma técnica em que `/etc/passwd` permanece legível, mas não contém mais senhas.
  - Em vez disso, as senhas de usuário são armazenadas em `/etc/shadow`.
  - Isso impede o atacante de ter acesso às passwords codificadas com a qual executa um ataque de dicionário.
  - A ferramenta Password Shadow Suite (`shadow`) é a mais popular.
  - O arquivo `/etc/shadow` assemelha-se a `/etc/passwd`.

# Segurança em Linux

- Sombreamento de senha
  - O shadow implementa dois novos conceitos muito além da manutenção básica de banco de dados de senha:
    - Password com tempo de expiração.
    - Bloqueio de conta automático.
  - Referências:  
<http://www.microlink.com.br/~buick/dragons/op1/howtos/br-sh>
  - O sombreamento de senha é uma técnica em que `/etc/passwd` permanece legível, mas não contém mais senhas.
  - Em vez disso, as senhas de usuário são armazenadas em `/etc/shadow`.
  - A ferramenta Password Shadow Suite (shadow) é a mais popular.

# Segurança em Linux

- Sombreamento de senha
  - O arquivo `/etc/shadow` assemelha-se a `/etc/passwd`.
  - O shadow implementa dois novos conceitos muito além da manutenção básica de banco de dados de senha:
    - Idade de senha.
    - Bloqueio de conta automático.
  - Escolha de senha por humanos
    - Os usuários criam senhas, frequentemente, baseados em:
      - Data de nascimento.
      - CPF.
      - Nomes dos filhos, artistas famosos.
      - Palavras do dicionário.
    - Programas de quebra de senha podem trabalhar com mais facilidade com esse tipo de senha.

# Segurança em Linux

- Sombreamento de senha
  - Verificação preventiva de senha
    - Na verificação preventiva de senha você elimina senhas fracas antes que elas sejam inseridas no banco de dados de senhas.
    - Ferramentas:
      - passwd+
      - Anlpasswd
      - npasswd

# Segurança em Linux

- Recuperação de senha do root
  - Passos:
    - Dar o boot na máquina.
    - Entrar no modo monousário (single).
      - linux = single.
      - boot -s (FreeBSD).
    - Mude a senha
      - Através do comando passwd.
      - Através da edição do arquivo /etc/passwd.
    - Reinicie a máquina.

# Segurança em Linux

- Ferramenta Crack
  - Objetivo
    - Auditoria de senha para a plataforma UNIX.
  - Requisitos
    - Linguagem C.
    - Usuário deverá ser root.
  - Download

[www.users.dircon.co.uk/~crypto/index.html](http://www.users.dircon.co.uk/~crypto/index.html)
  - Fases para funcionamento
    - Desempacotar o crack.
    - Criar o crack.
    - Executar o crack.
    - Visualizar seus resultados.

# Segurança em Linux

- Boas regras para o administrador:
  - Usar um sistema sombreado.
  - As senhas devem expirar a cada 60-90 dias, com um aviso de 5 dias e um bloqueio de 1 semana.
  - Imponha regras para a definição de senhas.
  - Execute, uma vez por mês, o Crack.
  - Se mantenha atualizado, através dos informes do fornecedor e às listas de segurança.
  - Forneça pelo menos uma educação básica sobre segurança de senha aos seus usuários.



# Auditoria de Sistemas

- Introdução

- É cada vez maior o número de empresas que utilizam de tecnologia da informação para automatizar suas operações. Por isso, cada vez mais as equipes de auditoria terão que usar como evidência dados provenientes de sistemas informatizados.
- Porém, não se deve partir do princípio de que dados extraídos do computador são confiáveis.
- É possível que erros e fraudes não sejam detectados por causa da enorme quantidade de dados controlados pelos sistemas, da possível discrepância entre o que está armazenado e o que é efetivamente em relatórios de saída, e da mínima necessidade de intervenção humana no processo.

# Auditoria de Sistemas

- Introdução

- Para usar dados de computador, a equipe deverá levar em consideração as seguintes questões:

- Qual a importância desses dados para o alcance dos objetivos da auditoria?
    - Os dados podem ser considerados completos e exatos?
    - O que se sabe sobre o sistema que os processou?

- Para qual finalidade os dados serão utilizados?

- Fornecimento de histórico ou relato de fatos não significativos para os resultados do trabalho.
    - Atingir os objetivos da auditoria.

# Auditoria de Sistemas

- A equipe terá que planejar um procedimento alternativo, no caso dos dados não serem confiáveis:
  - Obter dados de outras fontes, cuja confiabilidade possa ser confirmada;
  - Coletar dados primários para atender aos objetivos, em vez de utilizar fontes secundárias.
  - Redefinir os objetivos da auditoria, para eliminar a necessidade de utilizar dados não confiáveis.
  - Utilizar os dados, explicando sua limitação e abstendo-se de extrair conclusões ou recomendações.
  - Interromper a tarefa se nenhuma outra alternativa for possível.

# Auditoria de Sistemas – Métodos de Avaliação

- Existem basicamente dois métodos para a avaliação da confiabilidade de dados extraídos de computadores:
  - Avaliação do sistema
    - Testa e avalia com profundidade todos os controles num sistema informatizado, abrangendo suas aplicações e produtos.
    - Os procedimentos são: (1) exame dos controles gerais e de aplicativos do sistema; (2) teste da observância dos controles; (3) teste dos dados produzidos pelo sistema.
    - Este tipo de avaliação tende a consumir muito tempo e exige a participação de um especialista na área de Auditoria de Sistemas Informatizados.

# Auditoria de Sistemas – Métodos de Avaliação

## – Avaliação limitada

- É direcionada para dados específicos.
- Ela requer uma avaliação menos profunda dos controles gerais e de aplicativos, podendo ser realizada por equipes compostas, somente por técnicos generalistas.

# Auditoria de Sistemas – Métodos de Avaliação

- A avaliação limitada segue os seguintes passos:
  - Determinação do uso dos dados.
    - O primeiro passo é decidir como eles serão utilizados para se alcançar os objetivos de auditoria.
  - Definição dos dados que deverão ter sua confiabilidade avaliada.
    - Em seguida, determina-se quais grupos de dados precisarão ter sua confiabilidade avaliada.
    - Podem acontecer três situações: (a) dados classificados como única evidência; (b) dados classificados como evidência auxiliar; (c) dados classificados como de informação geral.

# Auditoria de Sistemas – Métodos de Avaliação

- A avaliação limitada segue os seguintes passos:
  - Levantamento do conhecimento prévio sobre o sistema e/ou os dados.
    - Informações favoráveis sobre a confiabilidade do sistema ou dos dados podem reduzir o risco de confiabilidade e diminuir o trabalho de avaliação dos controles do sistema e de teste de dados. Informações desfavoráveis levarão ao aumento do risco, exigindo maior cuidado na avaliação dos controles.
  - Avaliação dos controles do sistema de processamento dos dados.
    - A regra geral diz que quanto menor a confiabilidade dos controles gerais ou de aplicativo, maior a extensão do teste necessário para determinar a confiabilidade dos dados.

# Auditoria de Sistemas – Métodos de Avaliação

- A avaliação limitada segue os seguintes passos:
  - Determinação do risco de confiabilidade dos dados e da extensão do teste de dados.
    - O risco de confiabilidade dos dados é definido como sendo o risco de que os dados utilizados não sejam suficientemente confiáveis para o fim a que se destinam.
  - Teste de dados.
    - Embora seja improvável que qualquer sistema de computador contenha dados completamente livres de erro, o conceito de confiabilidade não exige dados perfeitos. Ele pressupõe, no entanto, a execução de procedimentos para avaliar a integridade e autenticidade dos dados e a exatidão do seu processamento por computador.



# Auditoria de Sistemas – Métodos de Avaliação

- A avaliação limitada segue os seguintes passos:
  - Divulgação da fonte dos dados e da confiabilidade atribuída aos mesmos.
    - Concluído o processo de avaliação da confiabilidade dos dados, é necessário documentar os resultados obtidos, mediante o preenchimento de papéis de trabalho e a inclusão de um parecer no relatório de auditoria.

# Auditoria de Sistemas de Informação

- Controles gerais
  - Consistem na estrutura, políticas e procedimentos que se aplicam às operações do sistema computacional de uma organização como um todo.
  - O primeiro passo numa auditoria é avaliar os controles gerais que atuam sobre o sistema computacional da organização.
  - Controles gerais deficientes acarretam uma diminuição da confiabilidade a ser atribuída aos controles das aplicações individuais.

# Auditoria de Sistemas de Informação

- Existem seis categorias de controles gerais utilizadas numa auditoria:
  - Controles organizacionais.
  - Programa geral de segurança.
  - Continuidade do serviço.
  - Controles de software de sistema.
  - Controles de acesso.
  - Controles de desenvolvimento e alteração de softwares aplicativos.

# Auditoria de Sistemas de Informação

- Controles organizacionais
  - Organização do departamento de tecnologia da informação.
  - Segregação de funções.
  - Unidades organizacionais bem definidas.
  - Atividades dos funcionários controladas e políticas claras de seleção, treinamento e avaliação de desempenho.
  - Política de segregação de funções e controles de acesso.
  - Recursos computacionais gerenciados de forma eficiente e econômica.

# Auditoria de Sistemas de Informação

- Programa geral de segurança
  - Princípios da gestão da segurança.
  - Avaliação do risco.
  - Estrutura de segurança.
  - Avaliação periódica do risco.
  - Documentação do programa de segurança.
  - Estrutura de gerência de segurança com atribuição clara de responsabilidades.
  - Políticas de segurança eficazes.
  - Supervisão da eficácia do programa de segurança.

# Auditoria de Sistemas de Informação

- Continuidade do serviço
  - Avaliação da vulnerabilidade das operações computadorizadas e identificação dos recursos que as apoiam.
  - Adoção de medidas para prevenir e minimizar danos e interrupções potenciais.
  - Desenvolvimento e documentação de um plano geral de contingência.

# Auditoria de Sistemas de Informação

- Controles de acesso
  - Classificação dos recursos de informação de acordo com a sua importância e vulnerabilidade.
  - Manutenção de lista atualizada de usuários autorizados e níveis de acesso.
  - Controles lógicos e físicos para prevenção e detecção de acesso não autorizado.
  - Supervisão do acesso, investigação de evidências de violações de segurança e adoção de medidas corretivas.

# Auditoria de Sistemas de Informação

- Controles de software
  - Acesso limitado ao software de sistema.
  - Caminhos de acesso.
  - Controle das alterações do software de sistema.



# Auditoria de Sistemas de Informação

- Controles de desenvolvimento e alteração de softwares aplicativos
  - Características de processamento e alterações nos programas são devidamente autorizadas.
  - Todos os softwares novos ou alterados são testados e aprovados.
  - Bibliotecas de controle do software.
- Controles de aplicativos
  - Controles de aplicativos são aqueles incorporados diretamente em programas aplicativos, nas três áreas de operação, com o objetivo de garantir um processamento confiável e acurado.

# Auditoria de Sistemas de Informação

- Controle da entrada de dados
  - Estes controles devem detectar transações não autorizadas, incompletas, duplicadas ou errôneas, e assegurar que sejam controladas até serem corrigidas.
  - Documentos ou telas de entrada de dados.
  - Rotinas de preparação dos dados (batch).
  - Autorização para entrada de dados.
  - Validação dos dados de entrada.
  - Tratamento de erros.

# Auditoria de Sistemas de Informação

- Controles do Processamento de Dados
  - Estes controles devem assegurar que todos os dados de entrada sejam processados e que o aplicativo seja executado com sucesso, usando os arquivos de dados, as rotinas de operação e a lógica de processamento corretos.
  - Integridade do processamento.
  - Validação do processamento.
  - Tratamento de erros do processamento.

# Auditoria de Sistemas de Informação

- Controles da Saída de Dados
  - Revisão dos dados de saída.
  - Distribuição dos dados de saída.
  - Segurança dos dados de saída.

# Auditoria de Sistemas de Informação

- Desenvolvimento de sistemas
  - Objetiva avaliar a adequação das metodologias e procedimentos de projeto, desenvolvimento, implantação e revisão pós-implantação dos sistemas produzidos dentro da organização auditada.
  - Fases:
    - Fase 1: Planejamento.
    - Fase 2: Elaboração do plano de desenvolvimento e início do projeto.
    - Fase 3: Organização do projeto.
    - Fase 4: Elaboração do projeto do sistema.
    - Fase 5: Revisão e aprovação pelos dirigentes.
    - Fase 6: Desenvolvimento e implantação.
    - Fase 7: Revisão de pós-implantação.

# Auditoria de Sistemas de Informação

- Redes de computadores
  - O principal risco oferecido pelas redes é o de acesso não autorizado a dados e programas da organização, que pode resultar em danos ou prejuízos intencionais ou acidentais.
  - A auditoria de redes de comunicação deve abranger os seguintes elementos críticos:
    - Gerência de rede: devem existir procedimentos e políticas para auxiliar a gerência do ambiente de rede e padrões definidos para controle do hardware e do software.
    - Segurança dos dados e da rede: devem existir mecanismos de controle de hardware e software que garantam a segurança e integridade dos dados mantidos no ambiente de rede e dos recursos físicos que a compõem; bem como limitem e controlem o acesso a programas e dados.

# Auditoria de Sistemas de Informação

- Operação da rede: a organização deve oferecer condições para uma operação eficiente da rede, incluindo normas e procedimentos de treinamento de pessoal, execução de cópias de segurança, avaliação da eficiência do serviço e rotinas de recuperação da rede após interrupções inesperadas.
- Software de rede: a gerência de rede deve monitorar e controlar o software de comunicação e o sistema operacional instalado.

# Bibliografia do Curso

- Stallings, William. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 1999. 569p.
- Dias, Cláudia Augusto. *Segurança e Auditoria da Tecnologia da Informação*. Axcel Books, 2000.
- Scheier, Bruce. *Segurança .com – Segredos e mentiras sobre a proteção na vida digital*. Editora Campus: 2001.
- Autor Anônimo. *Segurança Máxima para Linux*. Rio de Janeiro, Campus: 2000.



# Bibliografia Complementar

- Pfleeger, Charles P. Security in Computing. New Jersey: Prentice Hall, 1996. 574p.
- Stinson, Douglas R. Cryptography: Theory and Practice. New York: CRC Press, 1995. p.
- Zwicky, Elizabeth D. Construindo Firewalls para Internet. Rio de Janeiro, Campus: 2000.
- Dhajani, Nitesh. Hack Notes – Segurança no Linux e Unix. Campus: 2004.\_

# Links

- <http://www.numaboa.com.br/criptologia/>

(Site com bastante material sobre criptografia).

- <http://www.cacr.math.uwaterloo.ca/hac/>

(Excelente livro sobre o assunto. Totalmente disponível para download. Idioma: inglês).

- <http://focalinux.cipsga.org.br/>

(Material sobre a distribuição Debian. Pode também ser aproveitado para outras distribuições. É organizado por níveis de conhecimento.)