# Segurança da Informação

## Conceitos Iniciais

# Agenda

- Introdução
- Segurança e Política de Segurança
- Classificação da Informação
- Classificação dos Sistemas
- Análise de Riscos
- Analisando Ameaças

# Introdução

- O que é tecnologia da informação?
  - É um conjunto composto por hardware e software usado por uma organização para armazenar, processar, transmitir, e disseminar informações.
- Por que usar Sistema de Informação?
  - Para melhorar a qualidade e a disponibilidade de informações e conhecimentos importantes para a sociedade.
- Por que preocupar-se com segurança de Sistemas de Informação?
  - Dependemos dos Sistemas de Informação.
    - Os sistemas oferecem suporte para as principais atividades do ambiente social, sem eles a sociedade pára.
    - A informação é o principal patrimônio das organizações.

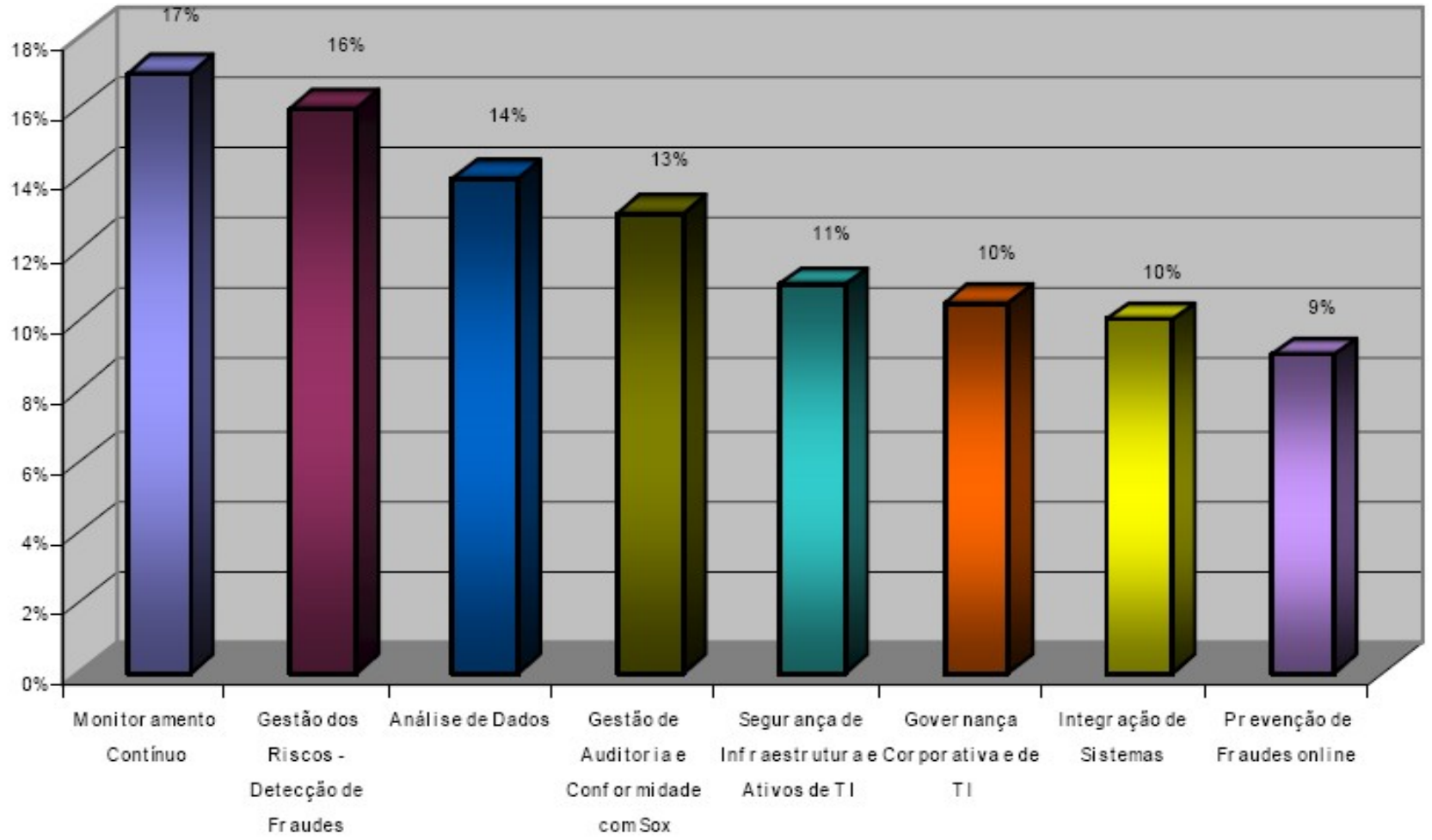
# Introdução

- Por que preocupar-se com segurança de Sistemas de Informação? (Continuação)
  - Os Sistemas de Informação são vulneráveis.
    - Esse sistema necessita de um ambiente estável e protegido de hackers, ladrões e espionagem industrial.
    - A empresa necessita de informações confiáveis para conduzir seus negócios.
  - Investimos em Sistemas de Informação
    - Como as empresas fazem altos investimentos em tecnologia da informação e esses bens são bastante atrativos para ladrões, as empresas precisam protegê-los.

Integrity Forum 2007
* Special Edition *

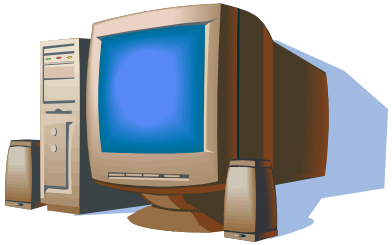
# Introdução

## Quais os temas que mais preocupam a sua empresa hoje?



# Segurança e Política de Segurança

- Segurança da Informação
  - Definição: É a área do conhecimento dedicada à proteção de **ativos da informação** contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.
  - Mas o que é Ativos da Informação?
    - Todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio onde ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

# Segurança e Política de Segurança

- Segurança da Informação
  - Objetivos de Segurança
    - Quando pensamos em segurança da informação, a primeira idéia que nos vem à mente é a proteção das informações, sem nos importar onde esteja essa informação.
    - Porém, segurança não é só isso. Existem várias formas de implantação de segurança da informação, os objetivos de segurança variam de acordo com o tipo de ambiente computacional e a natureza da sistema.
    - Como identificar os objetivos mais prioritários?
      - Para realizar identificação é necessário fazer uma análise da natureza da aplicação, dos riscos e impactos prováveis.

# Segurança e Política de Segurança

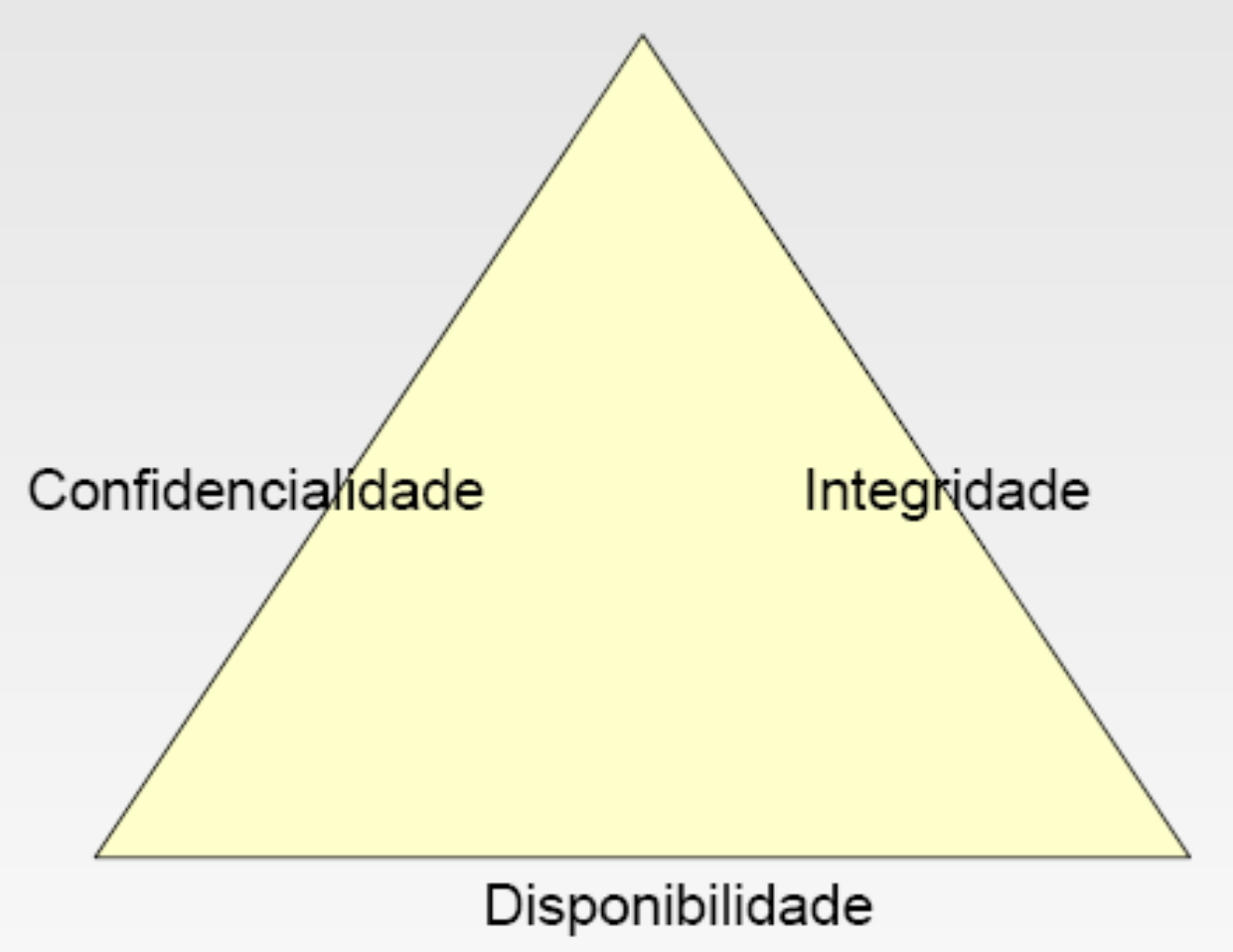
- Segurança da Informação
  - Objetivos de Segurança:
    - **Confidencialidade** – Toda informação deve ser protegida de acordo com seu grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.
    - **Integridade** – Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
    - **Disponibilidade** – Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que necessitem para qualquer finalidade.

# Segurança e Política de Segurança

- Segurança da Informação
  - Objetivos de Segurança
    - **Consistência** – certifica que o sistema atua de acordo com as expectativas dos usuários autorizados.
    - **Isolamento ou uso legítimo** – regula o acesso ao sistema. O acesso não autorizado é sempre um problema, pois além de ser necessário identificar quem acessou e como, é preciso se certificar de que nada importante do sistema foi adulterado ou apagado.
    - **Auditoria** – protege os sistemas contra erros e atos maliciosos cometidos por usuários autorizados. É utilizado para identificar os autores e sua ações.
    - **Confiabilidade** – Garante que, mesmo em condições adversas, o sistema atuará conforme o esperado. Exemplo: Sistema de Energia Nuclear, de Controle de tráfego aéreo e de controle de vôo.

# Segurança e Política de Segurança

- Segurança da Informação
  - A segurança da informação é caracterizado pela garantia de três fundamentos essencial, conforme ilustrado na figura ao lado.



# Segurança e Política de Segurança

- Segurança da Informação
  - Mas o que preciso fazer antes de implementar um programa de segurança da informação?
    - Antes é necessário responder as seguintes perguntas:
      - O que se quer proteger?
      - Contra que ou o quem?
      - Quais são as ameaças mais prováveis?
      - Qual a importância de cada recurso?
      - Qual o grau de proteção desejado?
      - Quanto tempo, recursos financeiros e humanos se pretende gastar para os objetivos de segurança desejado?
      - Quais as expectativas dos usuários e clientes em relação à segurança de informação?
      - Quais as conseqüências para a instituição se seus sistemas e informações forem corrompidos ou roubados?

# Segurança e Política de Segurança

- **Classificação da Informação**
  - Existem diferentes tipos de informação que devem ser protegidas de diferentes maneiras. Por isso, a classificação das informações é um dos primeiros passos para o estabelecimento de um política de segurança.
  - A classificação mais comum de informações é aquela que as divide em quatro níveis:
    - Pública
    - Interna
    - Confidenciais
    - Secretas

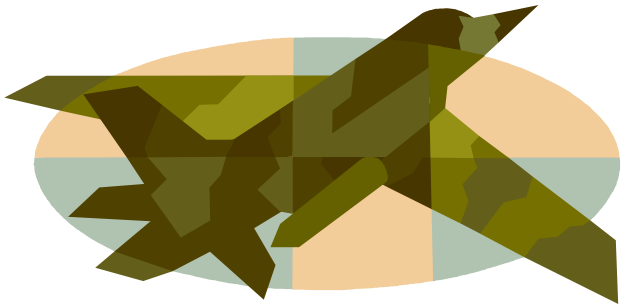
# Segurança e Política de Segurança

- **Classificação da Informação**
  - **Pública** – informação deste tipo pode ser divulgada a qualquer pessoa sem que haja implicação para a organização. A integridade dos dados não é vital, exemplo: serviços de informação ao público em geral, informações divulgadas à imprensa ou pela internet.

  - **Interna** – informações deste tipo não deve sair do âmbito da instituição. Porém, se isso ocorrer, as conseqüências não serão criticas. Ex: documentos de processo de trabalho da empresa.

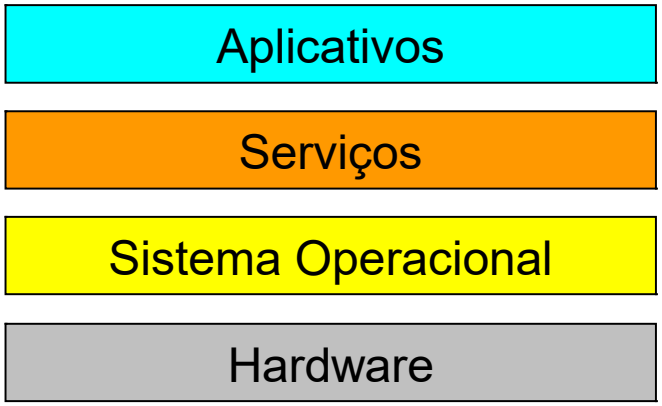
# Segurança e Política de Segurança

- **Classificação da Informação**
  - **Confidenciais** – informações protegidas contra acesso externo. O acesso a essa informação pode comprometer o funcionamento da instituição. Ex: dados pessoais de clientes e funcionários, senhas, contratos, etc.
  - **Secretas** – o acesso interno e externo não autorizado é extremamente crítico para instituição. Ex: dados militares e de segurança nacional.



# Segurança e Política de Segurança

- **Classificação dos Sistemas**
  - Como os ambientes computacionais são complexos, a melhor estratégia de implantação de segurança é utilizar controles em vários níveis diferentes.
  - Podemos subdividir os sistemas informação em 4 camadas, veja abaixo.



# Segurança e Política de Segurança

- **Classificação dos Sistemas**
  - **Aplicativos** – projetado para atender a necessidade especificas do usuário.
  - **Serviços** – utilizado pelos aplicativos, como por exemplo os serviços prestados por um banco de dados.
  - **Sistema Operacional** – presta os serviços de mais baixo nível, tais como gerenciamento de impressora e gerenciamento de arquivos.
  - **Hardware** – o processador e a memória que suportam o sistema operacional.

# Segurança e Política de Segurança

- **Análise de Risco**
  - É o processo pelo qual são identificados os riscos a que estão sujeitos os dados, sistemas de informação e redes de comunicação que lhes dão suporte.
  - Risco é uma combinação de componentes, tais como ameaças, vulnerabilidades e impactos.
  - A análise de riscos engloba tanto a análise de ameaças e vulnerabilidades quanto a análise de impactos, a qual identifica componentes críticos e o custo potencial ao usuário do sistema.
  - É o ponto chave da política de segurança.

# Segurança e Política de Segurança

- **Análise de Risco**
  - **Ameaça**
    - Evento ou atitude indesejável ( roubo, incêndio, vírus, etc) que potencialmente remove, desabilita, danifica ou destrói um recurso.
  - **Vulnerabilidade**
    - Fraqueza ou deficiência que pode ser explorada por uma ameaça. Pode ser associada à probabilidade da ameaça ocorrer.
  - **Impactos**
    - Conseqüência de uma vulnerabilidade do sistema ter sido explorada por uma ameaça, ou seja, é o resultado da concretização de uma ameaça.
  - Logo **Risco** = MEDIR (**Ameaças + Impactos + Vulnerabilidade**)

# Segurança e Política de Segurança

- **Analisando Ameaças**
  - Antes de decidir como proteger um sistema, é necessário saber contra que ele será protegido.
  - A segurança pode ser definida em termos de combate às ameaças identificadas.
  - **Mas como fazer essa analise?**
    - Nessa análise deve levar em consideração todos os eventos adversos que podem explorar as fragilidades de segurança do ambiente e acarretar danos.
  - Durante a análise é importante levar em consideração que o custos para se proteger contra uma certa ameaça pode ser mais alto do que o dano que essa ameaça possa causar, ou seja, nem todas ameaças merecem ser combatidas.

# Segurança e Política de Segurança

- **Analisando Ameaças**
  - É fundamental fazer a análise de custo-benefício.
  - Ameaça é tudo aquilo que pode comprometer a segurança do sistema.
  - **Uma ameaça pode ser:**
    - **Passiva** - falha de hardware, erros de programação, desastres naturais, erros de usuário, etc.
    - **Ativa** – roubo de senha, espionagem, fraude, sabotagem, invasão de hackers, entre outros.

# Segurança e Política de Segurança

- **Analisando Ameaças**
  - Independente do tipo, ativa ou passiva, as ameaças consideradas fundamentais são:
    - **Vazamento de informação (ativo ou passivo)** – informações desprotegidas ou reveladas a pessoa ou programas não autorizados.
    - **Violação de integridade** – comprometimento da consistência de dados.
    - **Indisponibilidade de serviços de informática** – impedimento deliberado de acesso aos recursos computacionais por usuários autorizados.
    - **Acesso e uso não autorizado** – um recurso computacional é utilizado por pessoas não autorizada ou de forma não autorizada.

# Segurança e Política de Segurança

- **Analisando Ameaças**
  - Independente do tipo, ativa ou passiva, as ameaças consideradas fundamentais são: (continuação)
    - **Mascaramento** – uma entidade (pessoa ou programa) se faz passar por outra entidade.
    - **Desvio de controles (*bypass*)** – um hacker, por exemplo, explorar uma falha ou vulnerabilidades de segurança burlando os controles para obter direitos de acesso não autorizados.
    - **Violação autorizada** – uma usuário ou programa autorizado usa o sistema com propósitos não autorizados.
    - **Ameaças programadas** – código de software que se alojam no sistema com intuito de comprometer sua segurança, alterando seu comportamento, violando controles de segurança, alterando ou destruindo dados.

# Segurança e Política de Segurança

- **Analisando Ameaças**
  - Lembre-se que ameaças exploram as vulnerabilidades ou fragilidades do sistema para causar impactos.
  - A análise dessas ameaças e vulnerabilidades tenta definir a probabilidade de ocorrência de cada evento adverso e suas conseqüências.

# Auditoria de Sistemas

## Ameaças

# Agenda

- Engenharia Social
- Aplicativos Maliciosos
- Cavalo de Tróia
- Rootkit
- Outras Ameaças
- Explorando Falhas

# Engenharia Social

# Engenharia Social

- Definição
  - Em “Segurança da informação”, chama-se Engenharia Social as **práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas**.
  - Para isso, o golpista (Engenheiro Social) pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc.
  - É uma forma de entrar em organizações que não necessita da força bruta ou de erros em máquinas. Explora as falhas de segurança das próprias pessoas que, quando não treinados para esses ataques, podem ser facilmente manipuladas.

# Engenharia Social

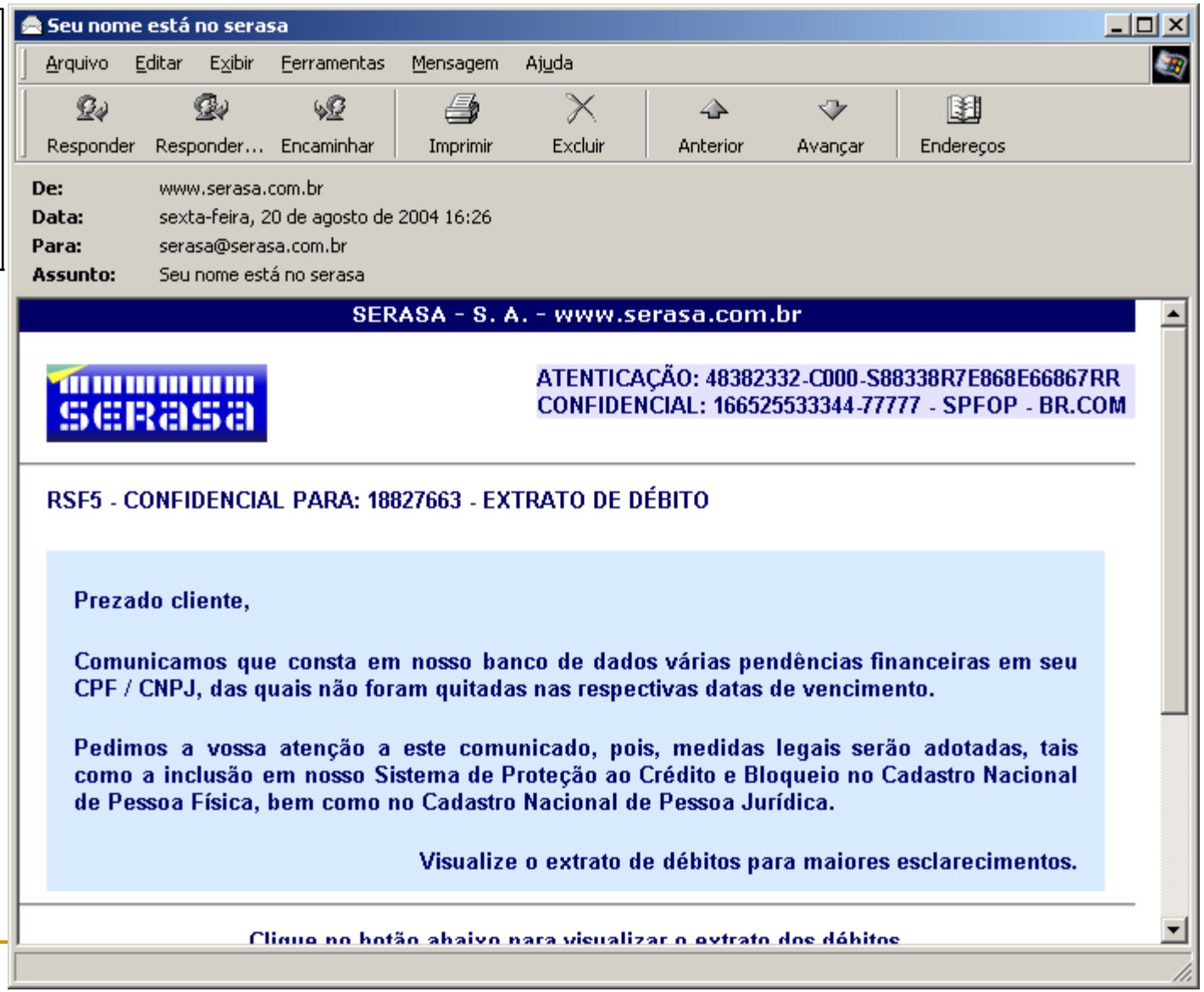
- Como identificar o engenheiro social?
  - Os engenheiros sociais são pessoas cultas, de papo agradável e que consegue fazer que a vítima caia em suas armadilhas.
  - Ele pode usar meios digitais, telefônicos e até pessoalmente, observam e estudam a vítima sem que a mesma percebam.
  - Por tanto, sempre confirme a identidade de todos que entram em contato com você e tome cuidado com o tipo de informação que cede a essas pessoas.

# Engenharia Social

- Como identificar o engenheiro social?
  - Existem três maneiras básicas de agir:
    - **Por e-mail ou carta**: É enviado um e-mail ou carta para a vítima contendo informações que ele quer. Pode ser pedindo um documento importante ou fingindo ser do centro de processamento de dados e requerendo uma mudança de senha, por exemplo. Independente do meio utilizado a comunicação sempre fica perfeita.

# Engenharia Social

Exemplo da aplicação engenharia social utilizando e-mail.



# Engenharia Social

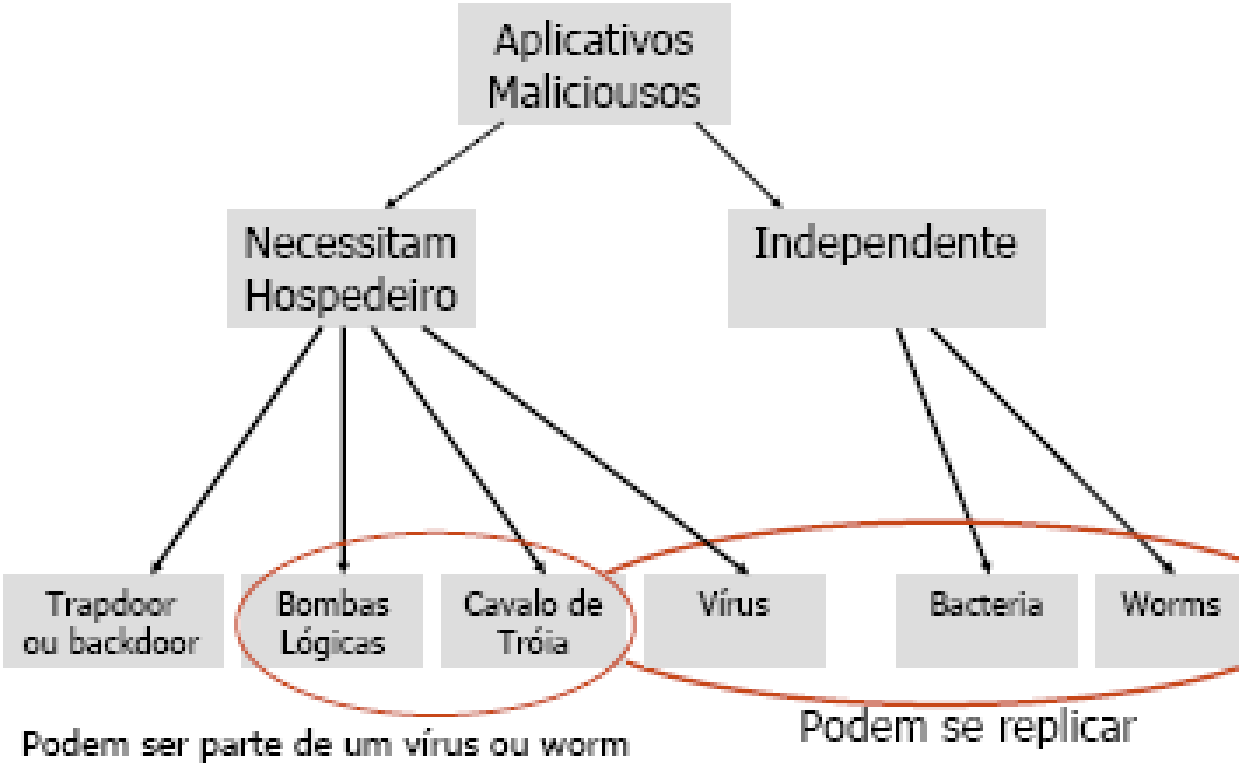
- Como identificar o engenheiro social?
  - Existem três maneiras básicas de agir:
    - **Pessoalmente**: É o método mais arriscado, mas também o mais eficiente. O engenheiro social arruma terno, um relógio de aparência cara e uma maleta com um notebook. Isso tem como objetivo se passar por um consultor de negócio ou cliente. Esta técnica é mostrada no filme “A Caçada Virtual” – filme que conta história de Kevin Mitnick.
    - **Por telefone**: O Engenheiro Social se passa por alguém importante, finge precisar de ajuda ou mesmo se oferece para ajudar. Nesse caso ele visa mexer com o sentimento das vítimas, fazendo com que elas acabam entregando o que ele deseja saber, sem que vítimas saiba.

# Aplicativos Maliciosos

- **Definição**
  - Aplicativos ou programas que exploram vulnerabilidades nos sistemas computacionais.
  - Podem ser divididos em duas categorias:
    - Os que precisam de um aplicativo hospedeiro;
    - Os que são independentes.
  - Também são diferenciados por poderem ou não se replicar.

# Aplicativos Maliciosos

- **Taxonomia dos *Malwares***



# Cavalo de Tróia

- Definição
  - Esse tipo de ferramenta começou a se popularizar na Internet em 1997, quando foi lançado o famoso *Back Orifice* - na verdade foi uma brincadeira com o nome *Back Office* da Microsoft.
  - Um cavalo de tróia ou *trojan*, é um programa que, quando instalado geralmente abre uma porta TCP ou UDP para receber conexões externas.
  - Esses programas normalmente fornecem o *shell*, *prompt* de comando, do sistema infectado para um possível invasor.

# Cavalo de Tróia

- Definição
  - Os *trojans* atuais são disfarçados de programas legítimos, embora, diferentemente de vírus ou de *worms*, não criem réplicas de si. São instalados diretamente no computador. De fato, alguns *trojan* são programados para se auto-destruir com um comando do cliente ou depois de um determinado tempo.
  - Os trojans atuais são divididos em duas partes:
    - Servidor
    - Cliente

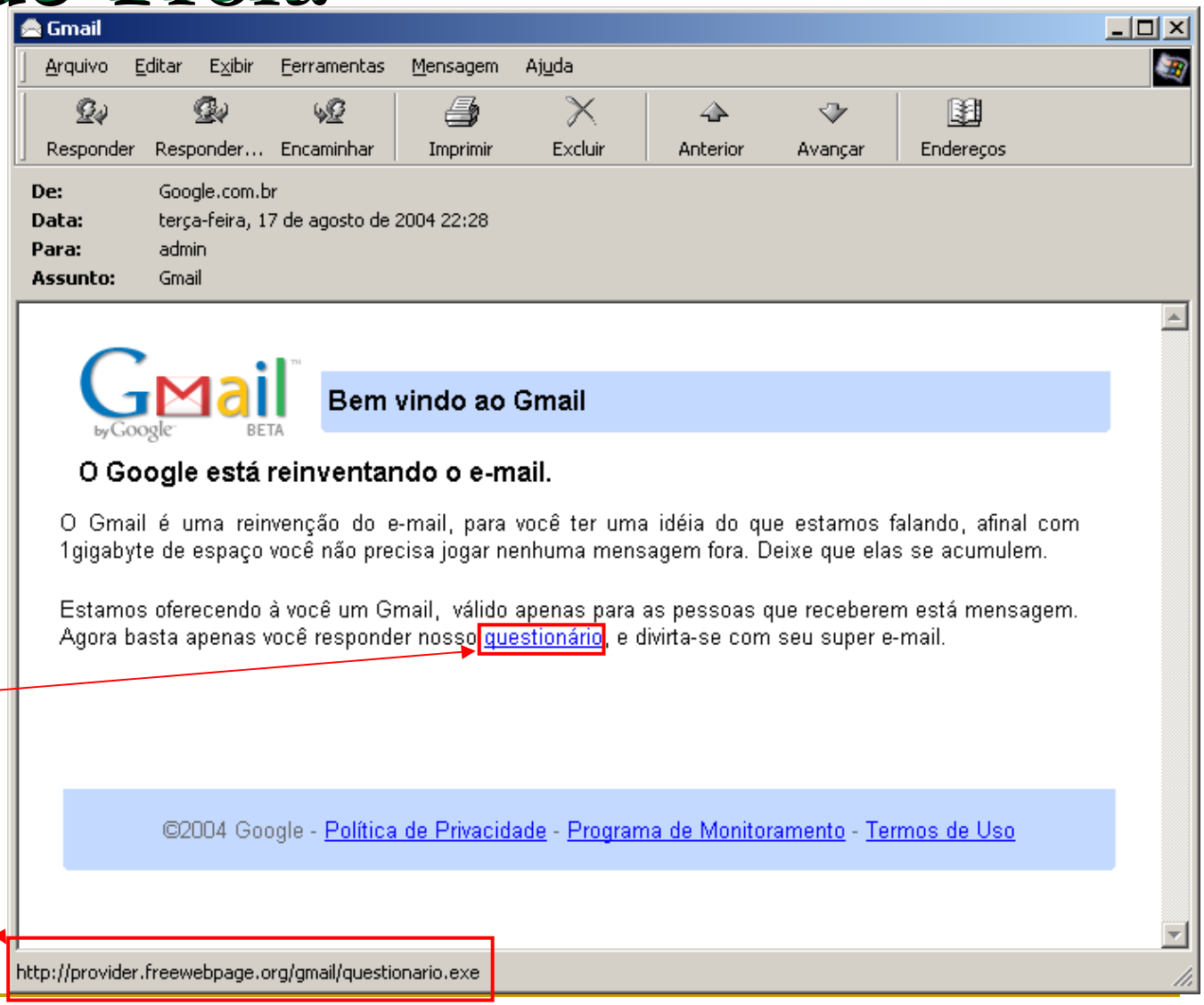
# Cavalo de Tróia

- Definição
  - O servidor se instala e se oculta no computador da vítima, normalmente dentro de algum outro arquivo. No momento que esse arquivo é executado, o computador pode ser acessado pelo cliente, que irá enviar instruções para o servidor executar certas operações no computador da vítima.
  - Dentro do servidor existem dois tipos de conexões:
    - Conexão Direta: precisa do IP da Vítima para funcionar.
    - Conexão Reversa: tem o IP do dono do *trojan*, assim fazendo a conexão.
  - Geralmente um *trojan* é instalado com o auxílio de um ataque de **engenharia social**, com apelos para convencer a vítima a executar o arquivo do servidor, o que muitas vezes acaba acontecendo, dada a curiosidade do internauta, como um e-mail atraindo a pessoa a ver fotos de um artista, pedindo a instalação de um *Plugin*, onde o *Trojan* fica "Hospedado".

# Cavalo de Tróia

Exemplo de *Trojan* instalado através de **Engenharia Social**.

Quando a vítima clica no link é executado o programa **questionario.exe**, veja o rodapé do e-mail.



# Cavalo de Tróia

- Tipos de Cavalo de tróia
  - ***Keylogger***
    - É um programa de computador cuja finalidade é monitorar tudo o que é digitado.
    - Muitas vezes esses programas são utilizados com objetivos ilícitos, através de *spywares*, "***trojan horses***", entre outros.
    - Alguns casos de *phishing*, assim como outros tipos de fraudes virtuais, se baseiam no uso de algum tipo de Keylogger, instalado no computador sem o conhecimento da vítima, que captura dados sensíveis e os envia a um *cracker*, que posteriormente irá utilizá-los com finalidades fraudulentas.

# Cavalo de Tróia

- Tipos de Cavalo de tróia
  - ***Keylogger (continuação)***
    - Como se proteger: existem softwares apropriados para se defender deste tipo de ameaça. É sempre oportuno que todo computador conectado à internet esteja protegido por um software "*Anti-Spyware*", um "*Firewall*" e um "Antivírus".
    - Os Keylogger na maioria das vezes se infiltram no computador da vítima através de e-mails e links falsos. Geralmente, a pessoa só nota que o Keylogger foi instalado depois que o *cracker* responsável pelo mesmo já tenha entrado no sistema através das senhas capturadas.

# Cavalo de Tróia

- Tipos de Cavalo de tróia
  - ***Backdoor***
    - É uma falha de segurança que pode existir em um programa de computador ou sistema operacional, que pode permitir a invasão do sistema por um *cracker* para que ele possa obter um total controle da máquina. Muitos *crackers* utilizam-se de um *Backdoor* para instalar vírus de computador ou outros programas maliciosos, conhecidos como *malware*.
    - Como se proteger: proteção mais comum contra *Backdoors* em computadores pessoais é o uso de *firewall* e de **IDS** (Sistema de detecção de intrusos). De modo geral, *Backdoors* que atuam através da internet podem ser facilmente detectados pelo sistema IDS ou impedidos de atuar pelo *firewall*.

# Rootkits

O conjunto de programas que possibilitam a realização de ataques escondendo e assegurando a presença do invasor no computador

Um rootkit pode fornecer programas com as mais diversas funcionalidades.

Dentre eles, podemos citar:

- Programas para esconder atividades e informações deixadas pelo invasor, tais como arquivos, diretórios, processos, conexões de rede;
- Programas para remoção de evidências em arquivos de logs;

# Rootkit

- **Ferramentas**
  - ***Tripwire***: ferramenta utilizada para teste de integridade em ambientes UNIX. Auxilia o administrador a monitorar os sistemas de arquivos.
    - Disponível em: http://sourceforge.net/projects/tripwire/
  - ***Chkrootkit:*** verifica localmente por sinais de um rootkit.
    - Disponível em: http://www.chkrootkit.org

# Vírus

- **Conceito**
  - É um programa malicioso desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios.
- **Forma de contaminação**
  - A contaminação entre máquinas pode ser realizada através de dispositivos removíveis como disquetes, CDs, etc. ou pela rede (ao abrir arquivos anexados aos e-mails, abrir arquivos Word, Excel, abrir arquivos em outros computadores). Observe que os arquivos precisam ser executados.

# Ciclo de Vida dos Vírus

- **Fase de hibernação**
  - Talvez para enganar o usuário, fazendo que o mesmo propague o vírus sem saber.
- **Fase de propagação**
  - Coloca cópias idênticas em outros aplicativos ou certas áreas do disco.
- **Fase de ativação**
  - Acorda após ocorrer determinado evento, como uma data, ou instalação de pen-drive.
- **Fase de execução**
  - A função do vírus é ativada, sendo que a mesma pode ser inofensiva, como uma mensagem na tela, ou perigosa, como a exclusão de arquivos.

# Tipo de Vírus

- **Parasitas**
  - Quando um aplicativo infectado é executado, ele se replica.
- **Residentes em memória**
  - Fica na memória, como parte residente do sistema, e contamina qualquer aplicativo que seja executado.
- **Setores de boot**
  - Infecta o ***Master Boot Record*** e se espalha quando o sistema é ligado.
- **Oculto**
  - Desenvolvido para ficar oculto contra sistemas anti-vírus.
- **Mutante**
  - Faz uma mutação a cada infecção, visando dificultar a detecção dele através das “assinaturas”, usadas pelos anti-vírus.

# Worms

- Faz uma cópia dele mesmo e utiliza as conexões de rede para se disseminar de sistemas em sistemas.
- Diferente do vírus, não necessita ser explicitamente executado para se propagar.
- Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados.
- São responsáveis por consumir muitos recursos como por exemplo: podem lotar o disco rígido fazendo grande quantidade de cópias de si mesmo e enviar pela rede.

# Worms

- Em sua fase de propagação o *worms* pode fazer:
  - Procura por outros sistemas para infectar, para isso ele examina a tabela de hosts, catálogo de endereços, etc.
  - Uma conexão com o sistema remoto acessando dispositivo compartilhado, enviando e-mail, etc.)
  - Uma cópia dele mesmo para o sistema remoto e executar essa cópia.

# Worms

- Como se proteger?
  - Alguns programas antivírus podem detectá-los e impedir que eles se propaguem.
  - Utilize seu computador quando:
    - O sistema operacional e softwares instalados não possuam vulnerabilidades, ou seja, certifique que todas atualizações e correções disponibilizados foram na sua máquina.
    - Firewall: pode evitar que um *worm* explore uma possível vulnerabilidade em algum serviço disponível em seu computador ou pode evitar que explore vulnerabilidades em outros computadores.

# Bactéria

- **Conceito**
  - São aplicativos que não possuem como finalidade a danificação de qualquer outro arquivo.
  - Seu único objetivo é de se replicar, podendo esta replicação ser exponencial.
  - Geralmente, consomem toda a capacidade do processador, memória, disco, gerando assim uma negação de serviço.

# Bots

- **Conceito**
  - Similar aos *Worms*.
  - É capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração.
  - Diferença: dispõe de mecanismos de comunicação com o invasor, permitindo que o ***bot*** seja controlado remotamente.
    - O ***bot*** se conecta a um servidor de IRC (Internet Relay Chat) e entra em um canal (sala) determinado.
    - O invasor, ao se conectar ao mesmo servidor de IRC, envia mensagens compostas por seqüências especiais de caracteres, que são interpretadas pelo ***bot***.

# Bots

- Um invasor pode enviar instruções para:
  - Desferir ataques na Internet;
  - Executar um ataque de negação de serviço;
  - Furtar dados do computador onde está sendo executado, como por exemplo números de cartões de crédito;
  - Enviar e-mails de *phishing*;
  - Enviar spam.
- **Botnets**
  - Redes formadas por computadores infectados com *bots;*
  - Para aumentar a potência dos ataques e*nvia centenas de milhares de e-mails de phishing ou spam,* desferir ataques de negação de serviço, etc.

# Bots

- **Como se proteger?**
  - Identificar a presença de um ***bot*** em um computador não é uma tarefa simples. Alguns programas antivírus permitam detectar a presença de ***bots***.
  - Prevenção
    - Mantenha o sistema operacional ou software instalados atualizados ou corrigidos;
    - Utilize um bom antivírus e mantendo-o sempre atualizado;
    - Firewalls pessoais: não eliminam os ***bots***, mas, se bem configurados, podem ser úteis para barrar a comunicação entre o invasor e o ***bot*** instalado em um computador.

# Outras Ameaças

# Buffer Overflow

- Falha de segurança comumente encontradas em software, apesar de ser uma falha bem-conhecida e bastante séria, que se origina exclusivamente na incompetência do programador durante a implementação de um programa.
- Alguns programas já são famosos por freqüentemente apresentarem a falha, como o Sendmail, módulos do Apache, e boa parte dos produtos da Microsoft.

# Buffer Overflow

- Um buffer overflow é resultado do armazenamento em um buffer de uma quantidade maior de dados do que sua capacidade . É claro que apenas linguagens de programação que não efetuam checagem de limite ou alteração dinâmica do tamanho do buffer são frágeis a este problema.
- Pode-se assim executar código arbitrário com os privilégios do usuário que executa o programa vulnerável. Daemons de sistema (syslogd(8), mountd(8)) ou aplicações que rodam com privilégios de super-usuário (sendmail(8), até pouco tempo) são portanto alvo preferencial.

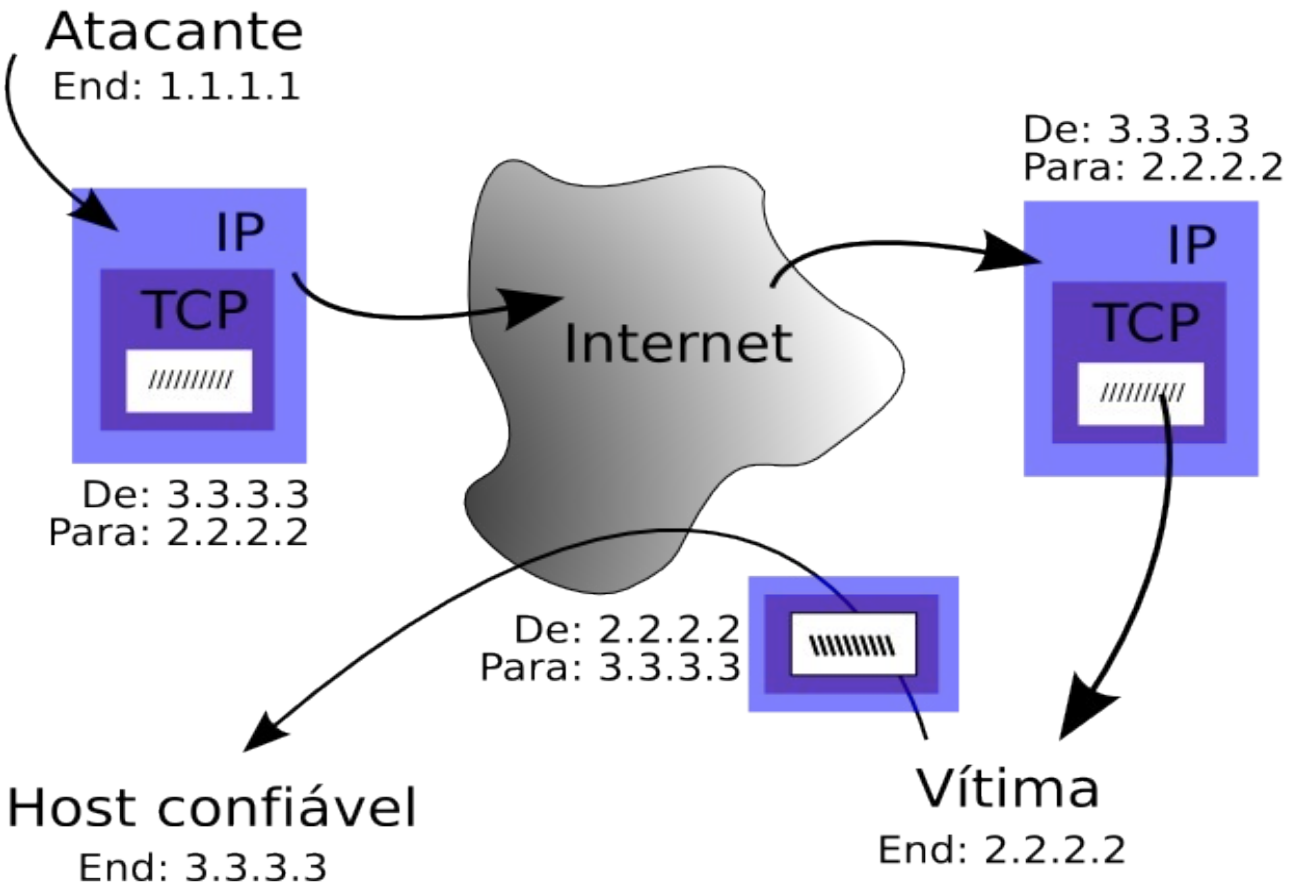
# Spoofing

- Técnica onde um atacante mascara-se como um host confiável. Existem várias formas de aplicar este ataque:
  - IP
  - ARP
  - DNS

# Spoofing

- IP Spoofing
  - Devido às características do protocolo IP, o reencaminhamento de pacotes é feito com base numa premissa muito simples: o pacote deverá ir para o destinatário (endereço-destino) e não há verificação do remetente — não há validação do endereço IP nem relação deste com o router anterior (que encaminhou o pacote). Assim, torna-se trivial falsificar o endereço de origem através de uma manipulação simples do cabeçalho IP.
  - Vários computadores podem enviar pacotes fazendo-se passar por um determinado endereço de origem, o que representa uma séria ameaça para os sistemas baseados em autenticação pelo endereço IP.

# IP Spoofing


Atacante
End: 1.1.1.1
IP
TCP
De: 3.3.3.3
Para: 2.2.2.2
Internet
De: 3.3.3.3
Para: 2.2.2.2
IP
TCP
De: 2.2.2.2
Para: 3.3.3.3
Host confiável
End: 3.3.3.3
Vítima
End: 2.2.2.2

# Denial of Service

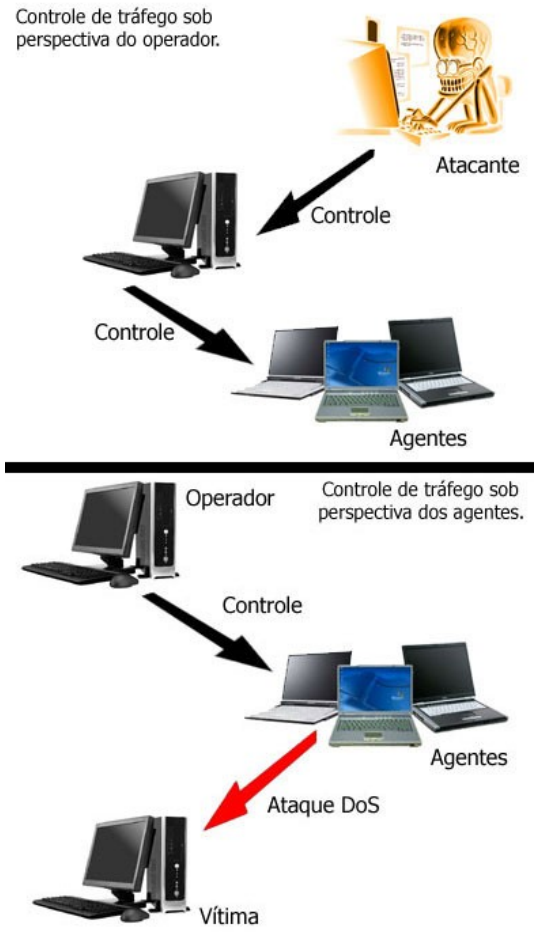
- Técnica que permite a uma atacante indisponibilizar um serviço vulnerável, possibilitando a indisponibilidade total de um serviço ou host até a execução de códigos arbitrários com previlégios de administrador.

# Denial of Service

- Este tipo de ataque precisa ser planejado. Primeiro, conseguindo domínio sobre as máquinas que efetuarão a negação ( Zumbis ).
- Busca-se computadores vulneráveis que são invadidos e têm os códigos de ataque instalados neles. A seguir, o atacante estabelece laços de controle entre as máquinas sob seu comando

# Denial of Service

- Ferramentas DDoS constroem uma hierarquia operador (handler) / agentes, nas quais o atacante controla a rede agente através de comandos diretos impostos ao operador, que os repassa aos agentes, às vezes usando um conjunto de comandos e semântica diferentes.



# Denial of Service

- Tipos de ataques:
  - Por Inundação ( Flood )
  - Reflexivo
  - À Infraestrutura de rede
  - De Vulnerabilidade

# Denial of Service
# Tipos de Ataques

- Por Inundação:
  - É dos tipos de ataque de DoS mais comuns. Ocorre inundação de tráfego TCP SYN, explorando a abertura de conexões do protocolo de TCP, utilizado em serviços que necessitam de entrega com confiável de dados, e que se inicia com a negociação de determinados parâmetros entre o cliente e o servidor.

# Denial of Service
# Tipos de Ataques

- Reflexivo:
  - Variação de um ataque de inundação, que visa exaurir recursos da vítima. Neste há a presença de um agente intermediário entre o atacante e a vítima.
  - Utiliza-se este intermediário para espelhar o tráfego de ataque em direção à vítima, o que dificulta ainda mais a identificação dos atacantes, pois o tráfego que chega à vítima é originado no intermediário, e não no próprio atacante.

# Denial of Service
# Tipos de Ataques

- Reflexivo ( cont. ):
  - Para este ataque, é necessário que o atacante envie uma requisição (REQ) ao agente intermediário, forjando o endereço da vítima (IP Spoofing) ao invés de usar seu próprio endereço. Ao receber o REQ, o agente não consegue verificar a autenticidade da origem da requisição (que de fato não é autêntica) e envia uma resposta (RESP) diretamente para a vítima.

# Denial of Service
# Tipos de Ataques

- À Infraestrutura de rede:
  - Ataque muito usado contra os grandes sites da Internet como Yahoo, Amazon e Microsoft, que em geral possuem grandes recursos de processamento e de memória.
  - Contra eles, DDoS de pequena escala não conseguem exaurir os suficientemente rápido para que a vítima tenha o serviço negado a usuários legítimos.

# Denial of Service
# Tipos de Ataques

- À Infraestrutura de rede ( cont. ):
  - Pode-se ainda concentrar esforços em algum elemento vital para o fornecimento do serviço, mas que não dependa da vítima, como por exemplo consumir toda a banda passante da vítima com o tráfego de ataque, o que causaria  perda de requisições na infra-estrutura de rede.
  - Este tipo de ataque de difícil combate, já que os pacotes não precisam ter nenhum padrão semelhante que possibilite filtrá-los.

# Denial of Service
# Tipos de Ataques

- De Vulnerabilidade:
  - O objetivo deste ataque é deixar a vítima inoperante. Uma das maneiras é explorar alguma vulnerabilidade na implementação da pilha de protocolos ou da própria aplicação da vítima.
  - Por exemplo, Está vulnerabilidade ocorreu na implementação do protocolo TCP em sistemas operacionais Microsoft Windows. O atacante precisava construir um pacote TCP particular e enviá-lo para a vítima. Ao receber o pacote, o sistema operacional da vítima abortava, causando congelamento total do processamento.

# Ferramentas de Ataques

- Trinoo: Arquitetura operador / agentes.
  - Atacante se comunica com o operador via TCP;
    - O operador se comunica com os agentes via UDP. Permite senhas para operadores e agentes, e gera pacotes UDP para portas aleatórias para múltiplos recipientes.

- Tribe Flood Network (TFN): Usa uma arquitetura diferente da do Trinoo.
  - O atacante não precisa se logar ao operador. Os agentes podem atacar via UDP ou TCP.

# Ferramentas de Ataques

- Stacheldraht (Arame farpado): Combina características do Trinoo e do TFN, com comunicação encriptada via TCP entre atacante e operador.
- 
- Shaft: Combina características dos três anteriores. Permite mudança de portas de comunicação entre operador e agentes durante a conexão e tem recursos de coleta de estatísticas.

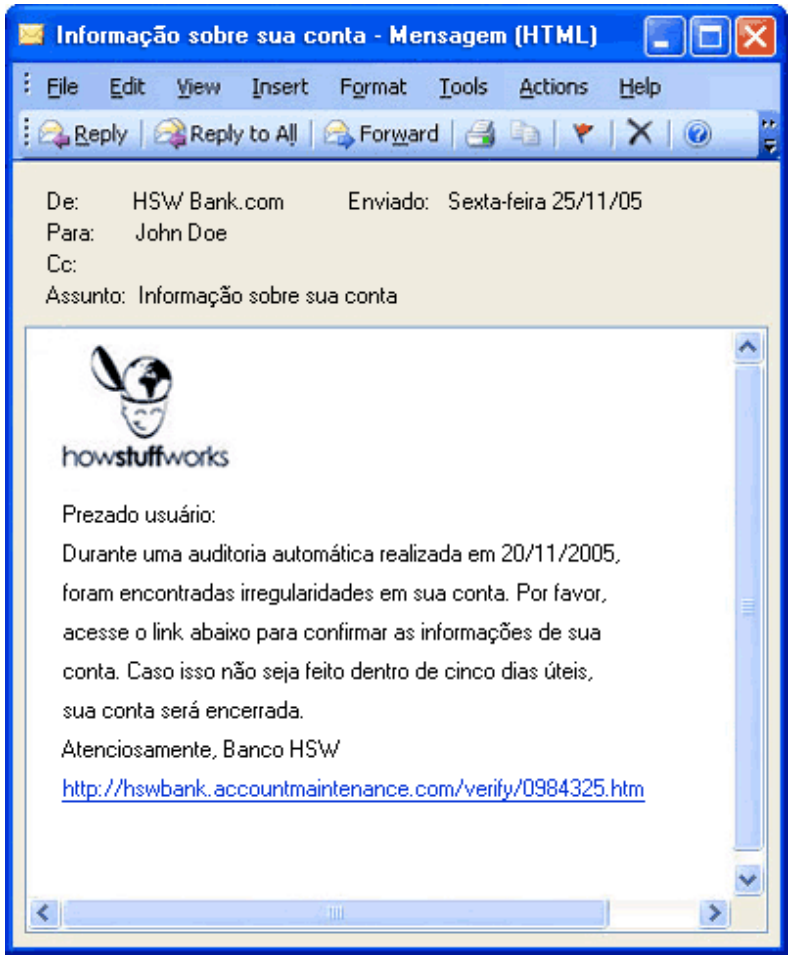
- Tribe Flood Network 2000 (TFN2K): Versão melhorada do TFN, adiciona características para dificultar detecção do tráfego e controle remoto da rede de agentes.

- Mstream: Gera inundações com tráfego TCP; Operadores podem ser controlados remotamente por mais de um atacante, e a forma de comunicação entre operadores e agentes é manipulável em tempo de compilação.

# Phishing

- Técnica usada como forma de fraudar eletrônicamente, caracterizada por tentativas de adquirir informações sensíveis, tais como senhas e números de cartão de crédito.
- O atacante se faz passar como uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial, como um correio ou uma mensagem instantânea.

# Phishing




- Muitas mensagens de phishing induzem a vítima a uma ação imediata,, fazendo-o agir primeiro e pensar depois.
- As mensagens muitas vezes ameaçam a vítima com o cancelamento da conta caso ele não responda imediatamente. Algumas agradecem a vítima por fazerem uma compra que nunca fizeram.
- Já que a vítima não quer perder dinheiro que não gastou, ele segue os links da mensagem dando ao phisher exatamente o tipo de informação que ele deseja.

# Fases de um ataque

# Fases de um ataque
# Fase 1 - Reconhecimento

- Quando o invasor obtém o máximo de informação sobre a vitima.

- Podemos dividir em 2 tipos:
  - Reconhecimento Passivo
  - Reconhecimento Ativo

# Fases de um ataque
# Fase 1 - Reconhecimento

- Reconhecimento Passivo
  - Obter informações sobre a vitima de forma furtiva sem que ela perceba.
  - Técnicas de engenharia social são muito utilizadas neste tipo de reconhecimento.
    - Recomendo leitura do livro A arte de enganar – Kevin Mitcnik
  - As ferramentas mais usadas são:
    - Google - http://penguim.wordpress.com/2008/03/21/usando-o-google-como-ferramenta-hacker-parte1/

# Fases de um ataque
# Fase 1 - Reconhecimento

- Reconhecimento Passivo ( cont. )
  - Registro.br - http://registro.br/
  - DNSStuff - http://www.dnsstuff.com/
  - Sniffing:
    - Wireshark
    - Kismet
    - Airdump

# Fases de um ataque
# Fase 1 - Reconhecimento

- Reconhecimento Ativo
  - Envolve em sondar a rede para descobrir endereços IPs e serviços na rede.
  - Este tipo de reconhecimento é mais arriscado que o passivo, a possibilidade de ser detectado e bloqueado é muito grande.
  - Porém os resultados são mais avançados. Por exemplo: Ao obter informações sobre um webserver você facilmente poderá descobrir as vulnerabilidades do SO e obter acesso.

# Fases de um ataque
# Fase 2 – Scanning

- É o tratamento das informações obtidas durante reconhecimento e usá-las para examinar a rede
- As ferramentas mais usadas por hackers nesta fase incluem dialers, port scanners, network mappers, e scanners de vulnerabilidade.
- Exemplos de ferramentas:
  - Nmap
  - Nessus
  - Nikto

# Fases de um ataque
# Fase 3 – Obtendo acesso

- Está é a fase onde o invasor faz a invasão propriamente dita, após detectar e estudar as vulnerabilidades descobertas durante as fases anteriores é nesta fase que elas deverão ser exploradas obtendo assim o tão desejado acesso não autorizado.
- Os métodos de conexão usados pelo invasor pode ser dentro da própria LAN ( cabeada ou wireless ) da vitima, acesso local a uma máquina, a Internet, ou offline.
  - Exemplos incluem buffer overflows, denial of service (DoS), e session hijacking.

# Fases de um ataque
# Fase 3 – Obtendo acesso (cont.)

- Exemplos de ferramentas utilizadas durante esta fase:
  - Metasploit Framework
  - Pirana
  - DNSspoof
  - Aircrack
  - SpoonWEP
  - John the ripper

# Fases de um ataque
# Fase 4 – Mantendo o acesso

- O objetivo de qualquer invasão é manter-se sempre a vitima pronta para um novo acesso para futura explorações e novos ataques.

- Em alguns momentos os invasores fortalecem os sistemas contra outros invasores permitindo acesso exclusivo, para isso eles utilizam de backdoors, rootkits e trojans.

- Uma vez que o invasor é dono do sistema,ele pode usá-lo como base para outros ataques. Neste caso o sistema invadido servirá como um zombie.

# Fases de um ataque
# Fase 4 – Mantendo o acesso (cont.)

- Ferramentas usadas durante está fase:
  - Privoxy
  - Netcat

# Fases de um ataque
# Fase 5 – Limpando o rastro

- Após o invasor concretizar o ataque é hora de apagar os rastros evitando assim ser detectado pelo pessoal da segurança e contra problemas legais e também para manter o acesso constante ao sistema, também chamamos está técnica de anti-forense.

- Ações como remover arquivos de log ou alarmes de IDS. Exemplos de atividades realizadas durante está fase incluem o uso de steganografia, tunelamento de protocolos, e alteração de arquivos de log.

# Explorando Falhas

# Explorando Falhas

- **Exploits**
  - Conceito
    - É um programa criado para testar falha de segurança. Geralmente é utilizado para realizar provas de conceito, ou seja, tentar descobrir falhas em um determinado ambiente para posterior correção. Mas também pode ser utilizado com fins maliciosos para realmente explorar e invadir o sistemas.
  - Técnicas
    - Existem diversas técnicas de exploração para diversos tipos de falhas, como *Stack Overflows*, *Heap Overflows* e outros.

# Explorando Falhas

- **Exploits**
  - **Solução**
    - Para evitar que falhas no seu sistema sejam exploradas, existem algumas soluções que podem ser tomadas. Veja abaixo algumas delas:
      - Aplicar, aos sistemas de IDS, regras que identifiquem diferentes tipos de *exploits*. Desta forma, saberá quando algum *exploit* for utilizado contra seu sistema.
      - Utilizar um ferramenta como o *Metasploit* para testar suas aplicações mais importantes que usem Internet. Não deve ser testados apenas servidores Web, FTP e de banco de dados. Teste também as aplicações desenvolvidas pela empresa.

# Explorando Falhas

- **Exploits**
  - Ferramentas
    - **Core Impact:**
      - Disponível em: www.coresecurity.com
    - **MetaSploit:**
      - Disponível em: www.metasploit.org

# Auditoria de Sistemas

# Aula 4 – Mecanismos de Defesa

# Agenda

- Controles de Segurança
- Definindo Serviços de Segurança
- Definindo Mecanismos de Segurança

# Controles de Segurança

- Uma vez identificados os impactos e ameaças e calculados os riscos, são desenvolvidas estratégias para controlar esse ambiente vulnerável.
- A primeira estratégia é estabelecer quatro linhas de ação para:
  - Eliminar o risco;
  - Reduzir o risco a um nível aceitável;
  - Limitar o dano, reduzindo o impacto;
  - Compensar o dano, por meio de seguros.
- Para cada linha de ação apresentada acima devemos implementar essas quatro linhas de ação.
- Com objetivo de eliminar ou minimizar o impacto do risco controlando o ambiente.

# Definindo Serviço de Segurança

- De acordo com o padrão **ISO 7498-2**, o qual aborda aspectos relacionados com segurança no modelo **OSI** (**Open Systems Interconnection**), serviços de segurança são medidas preventivas escolhidas para combater ameaças identificadas.
- Esse modelo foi criado para se referir a serviços de segurança de redes, seus conceitos pode ser usado para qualquer tipo de ambiente computacional.

# Definindo Serviço de Segurança

- No modelo ISO 7498-2 os serviços são classificados em cinco categorias básicas:
  - **Autenticação**
    - **Autenticação da entidade** – verifica a identidade de quem está solicitando o acesso ao recurso. No caso de redes, normalmente ocorre no início da conexão e tenta impedir o mascaramento ou a reutilização de uma conexão anterior.
    - **Autenticação da origem (relativa apenas a ambientes de rede)** – comprova para a entidade que solicita o acesso ao recurso que a origem é realmente quem diz ser.
  - **Controle de acesso** – fornece proteção contra uso não autorizado de recursos, como leitura, alteração ou destruição de dados, execução de programas, uso de meios de comunicação, etc.

# Definindo Serviço de Segurança

- **Confidencialidade de dados** – provê proteção de dados contra leitura não autorizada.
- **Integridade de dados** – provê proteção contra ameaça ativas à validade e à consistência de dados.
- **Disponibilidade** – garante que os recursos computacionais estão em condições normais de funcionamento, portanto, disponíveis aos usuários.
- **Não repúdio** – em comunicação, tenta evitar que remetente ou destinatário neguem que enviaram ou receberam dados.

- Os chamados serviços de segurança são uma classe especial de medidas preventivas relacionadas com o ambiente lógico. No âmbito mais geral, existem ainda outras medidas preventivas importantes.

# Definindo Serviço de Segurança

- **Segurança física** – alarmes, chaves e outros controles físicos.
- **Segurança dos recursos computacionais** – controles sobre sistema operacional, base de dados, etc.
- **Segurança administrativa** – treinamento de segurança, análise de trilhas de auditoria, procedimentos para investigar quebras de segurança, etc.
- **Segurança de meio magnéticos** – proteção de dados armazenados, escaneamento de arquivos para detecção de vírus e outros controles.

# Definindo Serviço de Segurança

- **Controles de desenvolvimento de aplicativos** – padrões de desenvolvimento, controles de documentação, projeto adequado, etc.

# Definindo Mecanismos de Segurança

- É o meio utilizado para atender a um serviço de segurança, isto é, um mecanismo que existe para prover e suportar os serviços de segurança.
- **Alguns mecanismos de segurança:**
  - **Sistema de criptográficos** – utilizam criptografia ou algoritmos cifrados para proporcionar confidencialidade de dados e de informações de fluxo de dados.
    - A vantagem desse sistema é mesmo que os outros métodos de proteção de dados (lista de controle de acesso, permissões de arquivos e senhas) falhem, os dados serão ilegíveis.

# Definindo Mecanismos de Segurança

- **Alguns mecanismos de segurança:**
  - **Assinatura digital** – conjunto de mecanismo que podem prover serviços de não repúdio, de autenticação da origem. Esse mecanismo permite a proteção das partes envolvidas na comunicação quanto a violação da autenticidade de uma delas e da integridade da mensagem.
  - **Mecanismo de controle de acesso** – o proprietário decide quem e como poderá acessar um determinado recurso. Esse mecanismo é composto por listas de direitos de acesso, perfis, etc.

# Definindo Mecanismos de Segurança

- **Alguns mecanismos de segurança:**
  - **Mecanismo de integridade de dados** – tem como finalidade prover proteção contra modificação de dados, podendo atender aos serviços de integridade de dados e de autenticação da origem.
  - **Mecanismos de disponibilidade** – backup e recuperação de dados, equipamentos de controle de temperatura e umidade, dispositivos, sistemas e equipamentos redundantes, que garantem a disponibilidade dos sistemas.

# Definindo Mecanismos de Segurança

- **Alguns mecanismos de segurança:**
  - **Trocas de autenticações** – atendem ao serviço de autenticação da entidade que solicita acesso ao recurso. Consiste na especificação de uma série de mensagens criptografadas intercambiadas entre um par de entidades de comunicação entre um par de entidades de comunicação, definindo uma espécie de protocolo para troca de mensagens.

# Definindo Mecanismos de Segurança

- **Alguns mecanismos de segurança:**
  - **Enchimento de tráfego** – usado, em conjunto com sistemas criptográficos, para proporcionar confidencialidade de informações de fluxo de dados, impedindo a análise de tráfego de rede.
    - **Forma de funcionamento** – Esse serviço gera mensagens aleatórias, sem informação útil, para que seja mais difícil identificar quais são os nós mais importantes da rede, em função do tráfego.
    - **Desvantagem** – prova degradação do desempenho do sistema pela geração contínua de mensagem sem valor, por isso ele é pouco utilizado.

# Definindo Mecanismos de Segurança

- **Alguns mecanismos de segurança:**
  - **Controles de roteamento** – usando para prevenir tráfego de dados críticos em canais de comunicação inseguros.
    - **Para que serve?**
      - Serve para escolher rotas mais seguras ou até mesmo para proibir rotas cujos componentes de rede não sejam confiáveis.
  - No caso dos serviços de segurança mais genéricos, como por exemplo segurança física, os mecanismos são os cadeados, os alarmes, a vigilância, isto é, tudo aquilo que permite a implantação daquele serviço de segurança.

# Segurança da Informação

## Conceitos Iniciais