

Capítulo 1 – Introdução à Segurança de Redes

- ✓ 1.1 – Introdução à segurança da informação
- ✓ 1.2 – Histórico da segurança
 - 1.2.1 – Surgimento da Internet, o Internet Worm e a criação do CERT
 - 1.2.2 – Segurança no Brasil
 - 1.2.3 – Segurança de redes hoje
- ✓ 1.3 – Princípios básicos da segurança
 - 1.3.1 – Menor privilégio
 - 1.3.2 – Defesa em profundidade
 - 1.3.3 – Gargalo

- 1.3.4 – Ponto mais fraco
- 1.3.5 – Falha com segurança
- 1.3.6 – Participação universal
- 1.3.7 – Diversidade de defesa
- 1.3.8 - Simplicidade

1.1 – Introdução à segurança da informação

- ✓ Em se tratando de computadores, “**segurança** envolve uma série de atitudes que visam proteger a informação contida nos computadores”
- ✓ Uma organização não é feita só de computadores e a informação está em toda parte:
 - pasta
 - arquivo
 - fita K7
 - fita VHS
 - cérebro das pessoas
 - etc

- ✓ Não podemos tratar de segurança apenas dentro dos computadores
- ✓ Tentamos proteger é a informação que pode residir ou não dentro dos computadores
- ✓ De acordo com a norma **NBR ISO-IEC 17799:2001**, “**informação** é um ativo que, como qualquer outro ativo importante para os negócios, tem valor para a organização e, conseqüentemente, necessita ser protegida de maneira adequada”
- ✓ Em se tratando de computadores, a informação pode estar:
 - nos registros de um banco de dados
 - num arquivo texto
 - numa planilha
 - trafegando por cabos de cobre ou ondas eletromagnéticas
 - etc

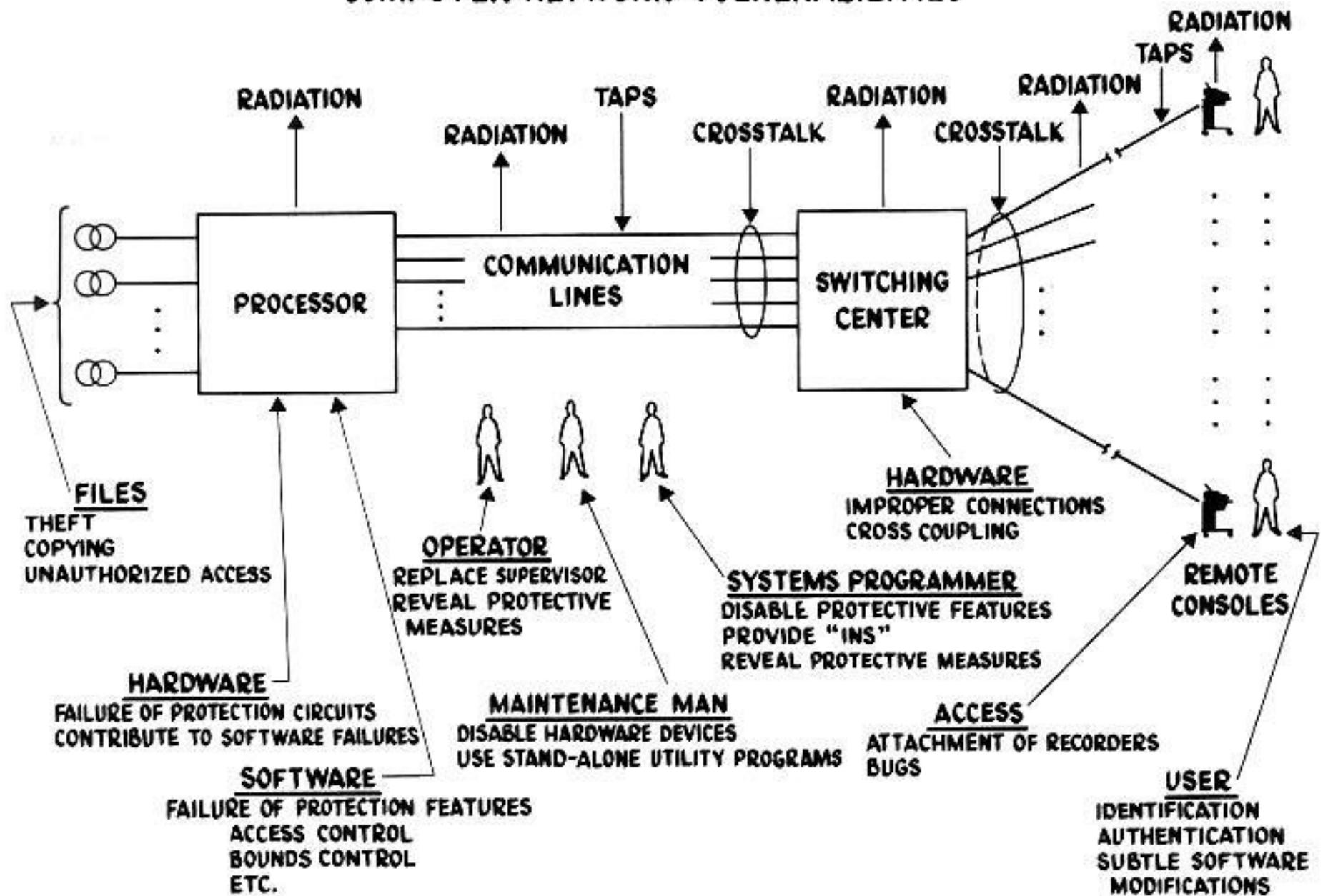
- ✓ **Segurança da Informação** abrange todo tipo de informação, computadorizada ou não
- ✓ De acordo com a norma **NBR ISO-IEC 17799:2001**, a segurança da informação consiste na preservação de três características básicas:
 - **Confidencialidade**: a informação só deve ser acessada por pessoas autorizadas
 - **Integridade**: a informação deve estar exata e completa
 - **Disponibilidade**: a informação deve estar acessível sempre que necessária
- ✓ Segurança da informação abrange outras áreas como:
 - segurança física
 - segurança de pessoas
 - segurança de computadores
 - segurança de redes
 - segurança de programas
 - segurança de sistemas

1.2 – Histórico da segurança

- ✓ A segurança da informação é tão velha quanto a própria informação
 - um ano depois da criação do telégrafo, um código de criptografia foi desenvolvido para manter seguras as mensagens transmitidas
 - cinco anos após a criação do telefone foi desenvolvido um “embaralhador” de voz para garantir o sigilo das conversas telefônicas
 - Em 1920, foi criada uma legislação para proibir escutas telefônicas
- ✓ A segurança nos computadores se deu início assim que eles começaram a guardar informações
- ✓ Antigamente, a segurança nos computadores se restringia ao controle do acesso físico ao computador
- ✓ Hoje, as principais ameaças são as “invisíveis” e estão por todo o lado (computadores em rede)

- ✓ Em 1950, criou-se o primeiro padrão de segurança, o **TEMPEST**, e a primeira organização governamental sobre segurança nos EUA, o **COMSEC**
 - **TEMPEST**: definia níveis aceitáveis de radiações elétrica e eletromagnética emanadas por equipamentos usados para processar informações confidenciais
- ✓ Nos anos 60, o departamento de defesa americano (**DoD**) começou a se interessar em segurança para proteger os computadores militares e suas informações confidenciais
- ✓ Em 1967, uma força-tarefa do DoD começou a examinar sistemas e redes para descobrir vulnerabilidades e ameaças. Resultados são apresentados em 1970 no documento *Security Controls for Computer Systems* – <http://cryptome.org/sccs.htm> – uma publicação histórica

COMPUTER NETWORK VULNERABILITIES



- ✓ DoD, em conjunto com a indústria, patrocinou trabalhos na área de segurança em três categorias diferentes:
 - **tiger teams**: grupo de pessoas que tentavam descobrir e corrigir falhas em sistemas computacionais
 - **estudos sobre segurança**: objetivo de identificar requerimentos de segurança, formular modelos de política de segurança, definir controles e recomendações, modelos matemáticos de segurança
 - **sistemas operacionais seguros**: tornar seguro o sistema **Multics**, da AT&T, que deu origem ao **Unix**, introduzindo controle de acesso por login e senha, ACL's, auditoria, memória virtual segmentada e paginada
- ✓ Em 1977 surgiu o **DES** (*Data Encryption Standard*): método oficial de proteção de dados não confidenciais em computadores das agência agências do governo
 - tornou-se padrão ANSI
 - hoje é pouco utilizado devido ao avanço dos processadores
- ✓ Em 1983, foi lançado o documento **TCSEC** (*Orange Book*), bíblia para o desenvolvimento de sistemas de computação seguros

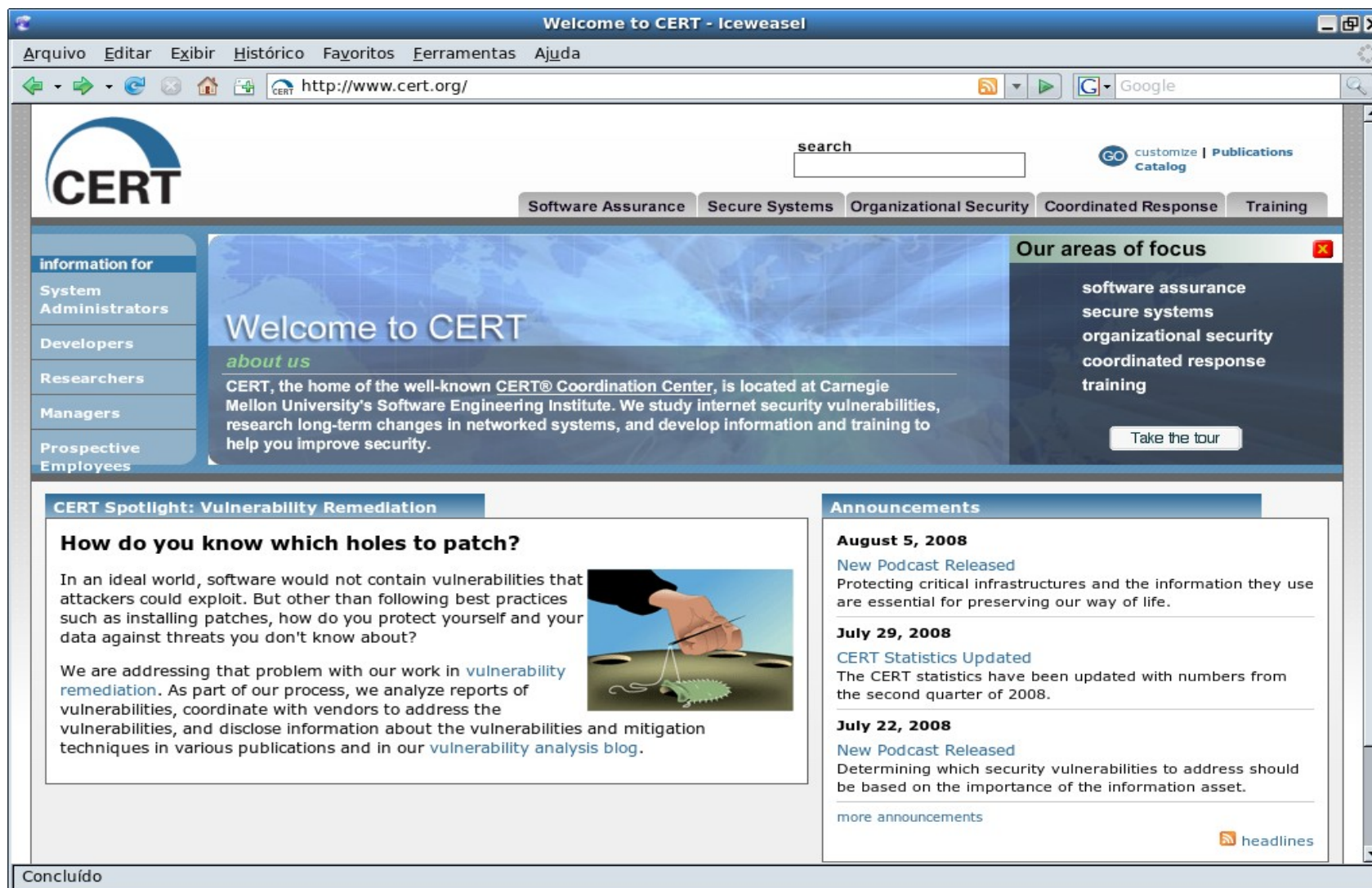
1.2.1 – Surgimento da Internet, o Internet Worm e a criação do CERT

- ✓ Em 1969, tornou-se realidade a **ARPANET**
 - consistia interligar máquinas entre quatro instituições acadêmicas
- ✓ Ken Thompson, junto com Ritchie e Ossana, desenvolveram a primeira versão do Unix, que teve grande participação no desenvolvimento da ARPANET
- ✓ Em 1974, foi inventado o protocolo TCP
- ✓ Em 1975, a ARPANET era totalmente funcional e foi entregue a uma organização governamental
 - Unix se torna o SO oficial da ARPANET
- ✓ Em 1980, a ARPANET deu origem a Internet de hoje

✓ Em 1988, **Roberto T. Morris** desenvolveu um programa capaz de auto-replicar e se auto-propagar: o **Internet Worm**

- o programa estava se propagando e infectando máquinas numa velocidade maior que Morris esperava: havia um erro no programa e Morris havia perdido o controle
- pediu ajuda a um amigo para encontrar uma solução e foi tarde demais: diversos computadores já haviam sido infectados
- explorava uma falha no ***sendmail*** e no ***fingerd***
- foram necessárias várias equipes de programadores para conter o *worm*: enquanto isso várias redes foram desconectadas da Internet
- Morris foi condenado a três anos de prisão, 400 horas de serviços comunitários e multa de US\$ 10 mil
- o *worm* não acarretava em danos físicos, mas chamou atenção para a fragilidade da Internet

- ✓ Como consequência do Internet Worm foi criado o **CERT** (*Computer Emergency Response Team*)
 - é hoje uma das entidades mais importantes em coordenar e informar sobre problemas de segurança
 - **<http://www.cert.org>**



1.2.2 – Segurança no Brasil

- ✓ Internet no Brasil começou em 1988, através de uma ligação de 4.800 bps com Chicago
- ✓ Em 1989, foi criada a **RNP** (Rede Nacional de Ensino e Pesquisa) pelo MCT
 - objetivo de construir uma infra-estrutura de rede Internet nacional de âmbito acadêmico
- ✓ Em 1995, a Internet comercial teve início no Brasil
- ✓ Nesta época, foi criado o **CGI.br** (Comitê Gestor de Internet no Brasil) – **<http://www.cgi.br>**
 - contava com a participação do MC, MCT, entidades operadoras e gestoras de *backbones*, representantes de provedores, representantes de usuários, e a comunidade acadêmica
 - deu origem a subdivisões, como o **NIC.br**, responsável por registro de domínios e endereços IP
 - **NBSO** (*NIC BR Security Office*), responsável por receber, revisar e responder a relatos de incidentes de segurança envolvendo a Internet brasileira

- ✓ A RNP possui sua própria entidade responsável por tratar de incidentes de segurança: o **CAIS** (Centro de Atendimento a Incidentes de Segurança).

Catálogo de fraudes - Icweweasel

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://www.rnp.br/cais/fraudes.php

RNP Rede Nacional de Ensino e Pesquisa
Promovendo o uso inovador de redes avançadas no Brasil

english | español

buscar no site:

Sobre a RNP | Parcerias | Contato

Rede RNP | Serviços | Operação | Segurança | P&D | Capacitação | Eventos

RNP > Segurança em redes > Catálogo de fraudes

SEGURANÇA CAIS Centro de Atendimento a Incidentes de Segurança

Fraudes identificadas e divulgadas pelo CAIS

A partir de 2008, todas as fraudes identificadas pelo CAIS estão sendo ordenadas de acordo com a data de distribuição e disponibilizadas para consulta, com o intuito de conscientizar a comunidade sobre os principais golpes que estão em circulação.

Adicionalmente, o CAIS envia alertas de segurança através da lista **CAIS Alerta** quando uma fraude mostra-se particularmente perigosa aos usuários de computadores.

Reporte fraudes:

- links maliciosos: artefatos@cais.rnp.br
- páginas falsas de instituições: phishing@cais.rnp.br

FRAUDES IDENTIFICADAS

Total de fraudes cadastradas: 288

tipo	Fraude Atualização Cadastral VISA	ID: 295
data	06/07/2008	
de	VISA (aviso@visa.com.br)	
assunto	comunicado importante cliente visa.	
informações	Imagem da mensagem Texto da mensagem	
arquivo malicioso	formulario_atualizacao_cadastral_visa.exe	
comentário	Mensagem supostamente da VISA Brasil que informa sobre a necessidade de uma "atualização cadastral". Como de costume, a mensagem é concluída com uma	

Formulário para notificação de incidentes de segurança

Esta página tem função informativa e educativa. Exibe uma coleção de imagens de *phishing scam* (fraudes eletrônicas) ou *malware* (código malicioso) veiculados por meio de *spam* (e-mail não-solicitado). Trata-se de conteúdo exemplificativo, não exaustivo, uma vez que não é possível contemplar todos os casos de fraudes existentes. Assim, caso você tenha conhecimento de um exemplar que não esteja aqui presente, isto não significa que não seja válido ou real. Inclusive incentivamos que você o envie para análise do CAIS para que, se for o caso, passe a integrar o nosso acervo.

Aviso Legal - Isenção de responsabilidade

Com a disponibilização pública deste serviço, não é intenção do Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP) violar direitos autorais sobre marcas registradas ou logotipos de empresas que porventura constem das amostras. O objetivo é tão somente alertar os usuários sobre as espécies de golpes que se utilizam de tais propriedades intelectuais ou industriais de forma criminosa.

Portanto, o CAIS não se responsabiliza pelos conteúdos aqui expostos, limitando-se tão somente a reproduzi-los na íntegra, tais como foram encontrados, recebidos ou enviados por terceiros.

Listas de fraudes publicadas:
2008

Consulta em fraudes:

1.2.3 – Segurança de redes hoje

- ✓ Praticamente todos os fabricantes de *hardware* e *software* possuem uma área específica só para tratar problemas de segurança e lançar correções de *software*
- ✓ Padrões de segurança desenvolvidos:
 - **ISO 17799:2001**
 - **NBR ISO/IEC 17799**
 - **CCITSE**, conhecido como Common Criteria
 - **ICSA**
 - **NBSO** (Cartilha de Segurança para Internet e Práticas de Segurança para Administradores de Redes Internet) – <http://www.cert.br/docs/seg-adm-redes/>

1.3 – Princípios básicos de segurança

- ✓ Filosofia do AA:
 - “Um dia de cada vez”
 - “Só por hoje”
- ✓ Segurança é um processo contínuo: “um sistema seguro hoje será um sistema vulnerável amanhã”
- ✓ Um sistema deve ser sempre revisto e atualizado
- ✓ A cada dia novas vulnerabilidades são descobertas, novas correções são lançadas e novos padrões são definidos

1.3.1 – Menor privilégio

- ✓ Princípio fundamental da segurança
- ✓ Vale para qualquer objeto: usuário, administrador, programa, serviço, etc)
- ✓ Cada objeto deve possuir apenas o mínimo privilégio para realizar suas ações, e nenhum outro.
- ✓ Com isso, limita-se o nível de estrago que um ataque bem sucedido pode causar
- ✓ Exemplos da vida real:
 - Visita a uma empresa: acesso somente ao setor informado
- ✓ Pergunte-se sempre se não está implementando sistemas com mais privilégios do que devia

1.3.2 – Defesa em profundidade

- ✓ Mecanismos de defesa em cascata
- ✓ Se um mecanismo falhar haverá um outro em seguida que poderá compensar o que falhou
- ✓ Exemplos da vida real:
 - portas com mais de uma tranca
 - cartões magnéticos e senhas
- ✓ Na computação:
 - colocar serviços em máquinas separadas
 - acesso remoto em cascata

1.3.3 – Gargalo (*choke point*)

- ✓ Obriga intrusos a utilizar um canal estreito, que pode ser monitorado e controlado
- ✓ Todos os acessos devem ser feitos por um único ponto
- ✓ Exemplos na vida real:
 - pedágio
 - caixa de supermercado
 - bilheteria
- ✓ Na computação:
 - **firewall**: funciona como um canal estreito que pode ser monitorado e controlado. Qualquer intruso, obrigatoriamente, tem que passar por ele
- ✓ Basta uma única saída alternativa na sua rede para comprometer todo o seu esquema de segurança

1.3.4 – Ponto mais fraco

- ✓ A segurança é como uma corrente: é tão forte quanto o seu ponto (elo) mais fraco
- ✓ Um invasor sabe que provavelmente terá mais sucesso se atacar o ponto mais fraco da sua rede
- ✓ O administrador deve estar ciente do ponto mais fraco da sua rede, de modo que possa tomar medidas para eliminá-lo ou monitorá-lo
- ✓ Sempre haverá um ponto mais fraco: muita atenção a ele sem se esquecer dos outros pontos
- ✓ Exemplo na vida real:
 - roubo num estacionamento de carros
- ✓ Na computação:
 - Na grande maioria das vezes, um invasor não está interessado em um rede em particular

1.3.5 – *Fail-safe stance* (falha segura)

- ✓ Quando um sistema de segurança falha, deve falhar de tal forma que bloqueie o acesso de um invasor, em vez de deixá-lo entrar
- ✓ Isso também impedirá o acesso de usuários legítimos
- ✓ O sistema pode ficar indisponível até que o reparo seja feito (aceitável, é melhor que uma invasão na rede)
- ✓ Exemplo na vida real:
 - disjuntor elétrico
 - travas de elevador para impedir queda
- ✓ Na computação:
 - derrubar um sistema ao menor sinal de invasão
 - cuidado com falsos positivos

1.3.6 – Participação universal

- ✓ A participação de todas as pessoas envolvidas no sistema é muito importante
 - podem relatar problemas e medidas implantadas
 - pessoas que não participam do processo podem se tornar opositoras
 - opositores são pessoas que fazem de tudo para contornar suas medidas de segurança
- ✓ A participação pode ser voluntária ou involuntária
 - voluntária: através do convencimento
 - involuntária: por imposição da chefia

1.3.7 – Diversidade de defesa

- ✓ Uso de sistemas diferentes torna o sistema como um todo mais seguro, pois a vulnerabilidade de um sistema provavelmente não estará presente nos outros
- ✓ Envolve conhecer sistemas diferentes: complexidade de configuração e de manutenção
- ✓ Analisar a relação custo benefício
- ✓ Falhas podem existir em todos os sistemas, mesmo sendo diferentes

1.3.8 – Simplicidade

- ✓ Manter as coisas simples faz com que sejam mais fáceis de entender
- ✓ O entendimento é fundamental para se conhecer o nível de segurança
- ✓ Programas complexos escondem falhas de segurança

1.4 – Atividades

1. Na Internet, faça uma busca por notícias recentes relacionadas à segurança de redes (novos vírus/ameaças, invasões em servidores conhecidos, fraudes, novas vulnerabilidades em programas e sistemas, prisão ou investigação bem sucedida de um invasão). Selecione duas notícias e participe de um debate que será mediado pelo professor. Procure colocar seu ponto de vista sobre a situação atual, além de suas expectativas sobre o futuro.
2. O professor apresentará um tema bastante atual sobre a segurança de redes. Utilizando a Internet, procure o máximo de informação sobre o tema e participe do mini-debate mediado pelo professor para discutir o assunto.
3. Escolha um dos temas abaixo e prepare um pequeno resumo sobre o assunto, pesquisando na Internet:
 - a. Worms
 - b. Spyware
 - c. Vírus
 - d. Engenharia social
 - e. Internet Worm
 - f. Phishing