Engenharia de Segurança

Prof. Dr. Rodolfo I. Meneguette
meneguette@icmc.usp.br
Adaptado da Profa Kalinka

INTRODUÇÃO

- Computadores são mais úteis ligados em rede, compartilhando informação e recursos
  - Disponibilização ampla de informação
  - Interoperabilidade e intercâmbio de informação
  - Mobilidade de acesso e gerenciamento remoto
  - Sistemas de processamento distribuído
- A partir dos anos 80: evolução das interconexões de redes de computadores
- Aumento de extensão das redes e do acesso: mais necessidade de cuidado e controle

INTRODUÇÃO

- A todo momento surgem novos casos de redes invadidas ou comprometidas por ação de hackers, vírus e outros fatores de risco

Hackers podem controlar quase meio milhão de veículos Chrysler a distância

Por: Adam Clark Estes
21 de julho de 2015 às 16:44

0

Uma investigação em andamento sobre a segurança de veículos da Chrysler pode tem uma conclusão assustadora. Em algumas semanas, pesquisadores de segurança irão revelar os detalhes de uma falha de Dia Zero que afeta cerca de 471.000 carros. E ainda pior: hackers a

http://gizmodo.uol.com.br/hackers-podem-controlar-quase-meio-milhao-de-veiculos-chrysler-a-distancia/

Como impedir que hackers interfiram nos sistemas de um avião em pleno voo

Por: Yijun Yu e Andrew Smith
21 de maio de 2015 às 9:53

34 0

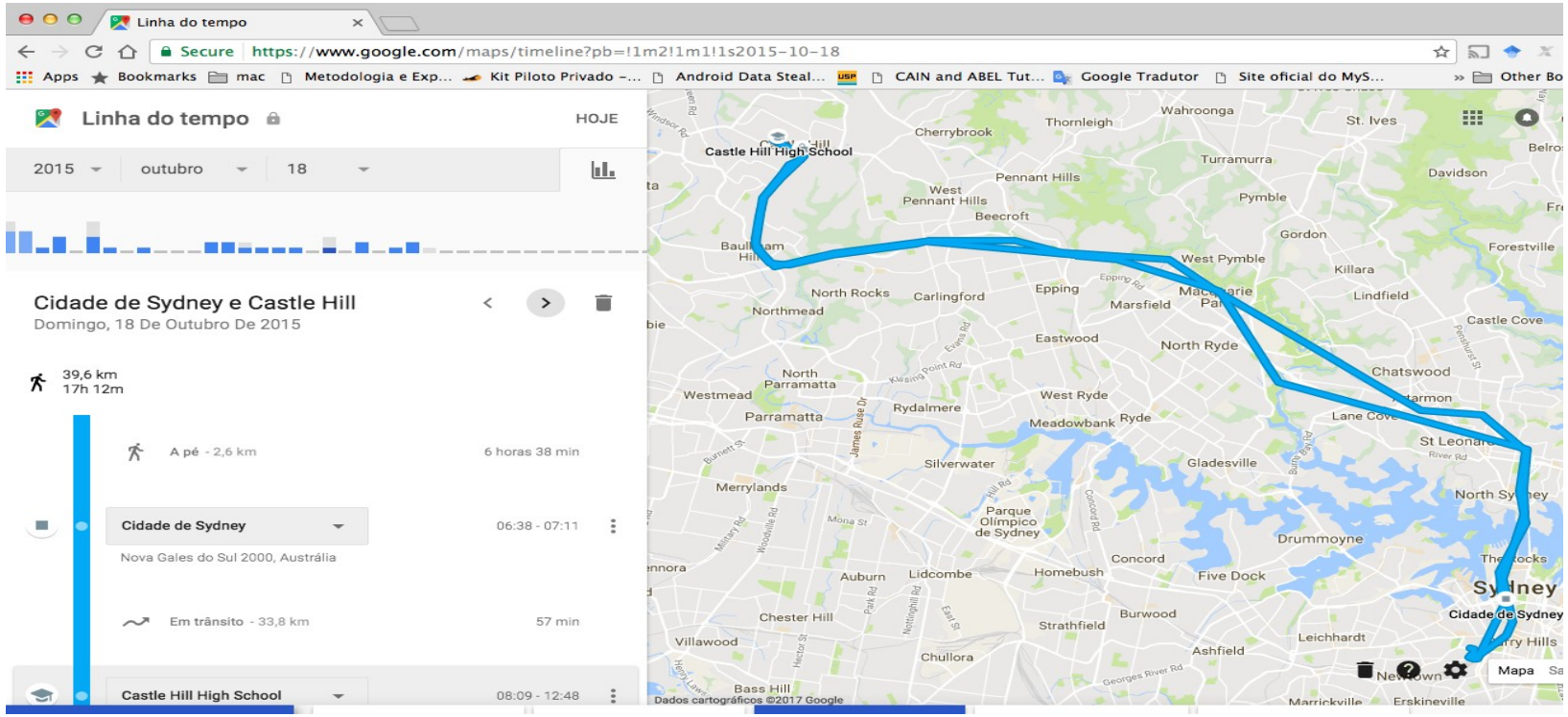
Segundo o FBI, um especialista em cibersegurança diz ter hackeado com sucesso um avião enquanto ele estava sentado na poltrona de passageiros. Especialistas em geral concordam

http://gizmodo.uol.com.br/canais/fui/como-impedir-que-hackers-interfiram-nos-sistemas-de-um-aviao-em-pleno-voo/

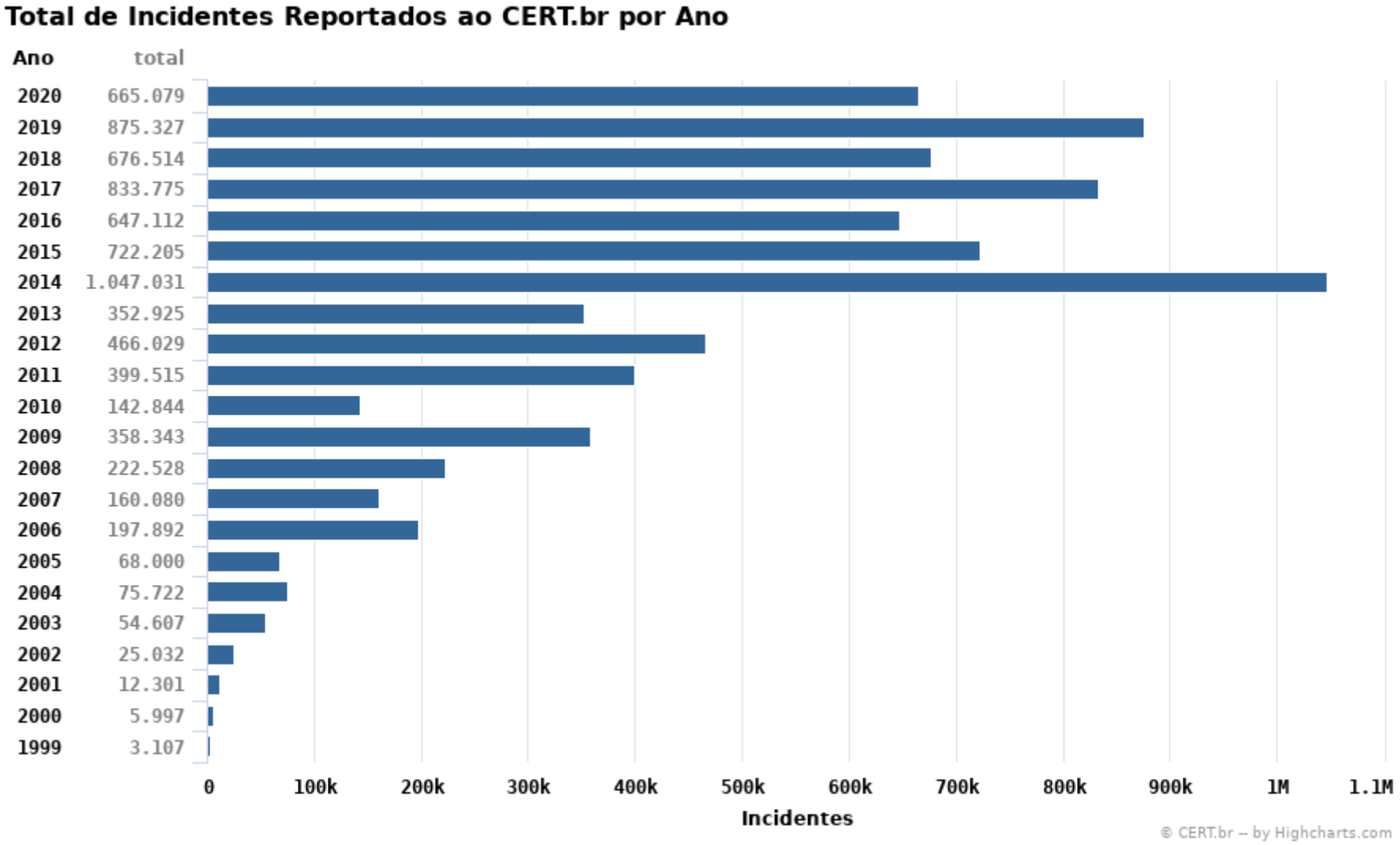
E A MINHA PRIVACIDADE?

Can't remember last night? Google's Location History can tell where you were

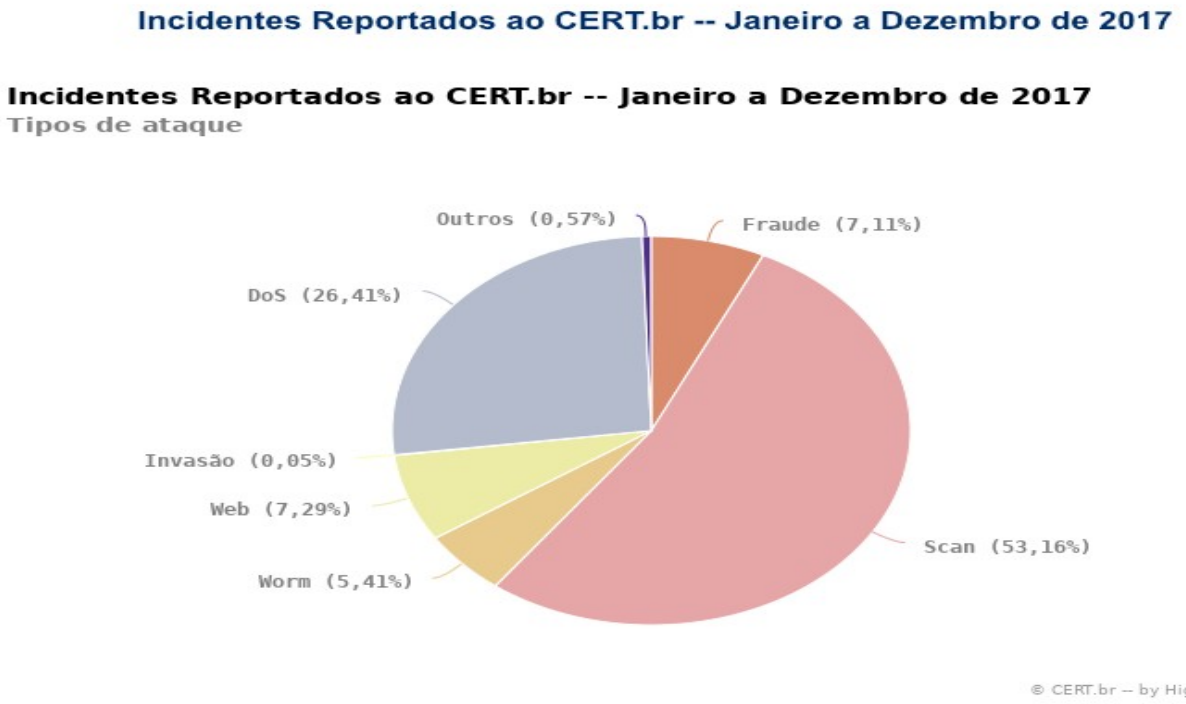
By **Marc Knoll** - November 28, 2016 27

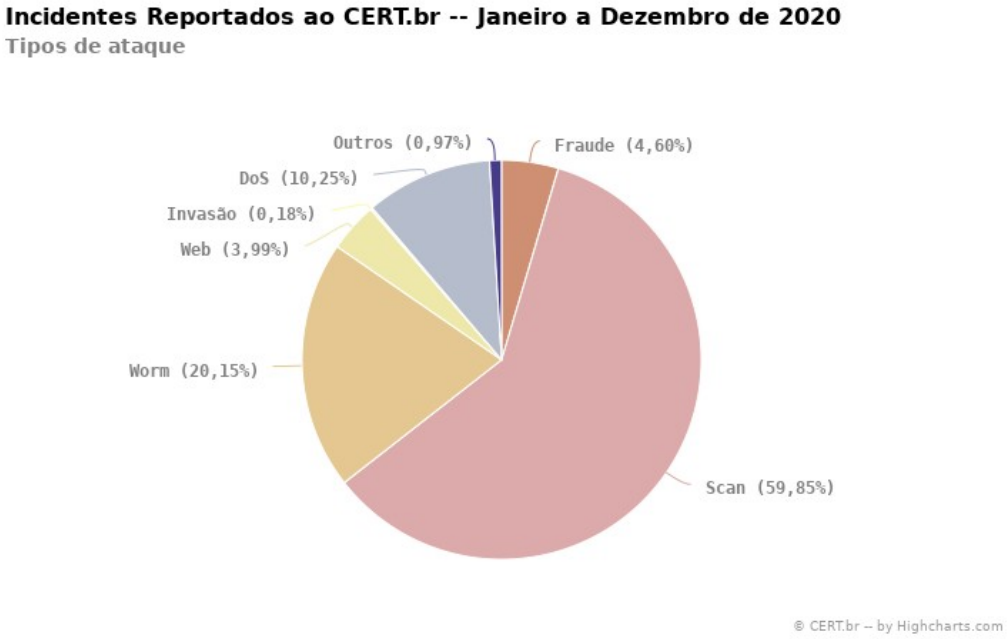


NÚMEROS BRASIL – 1999-2020

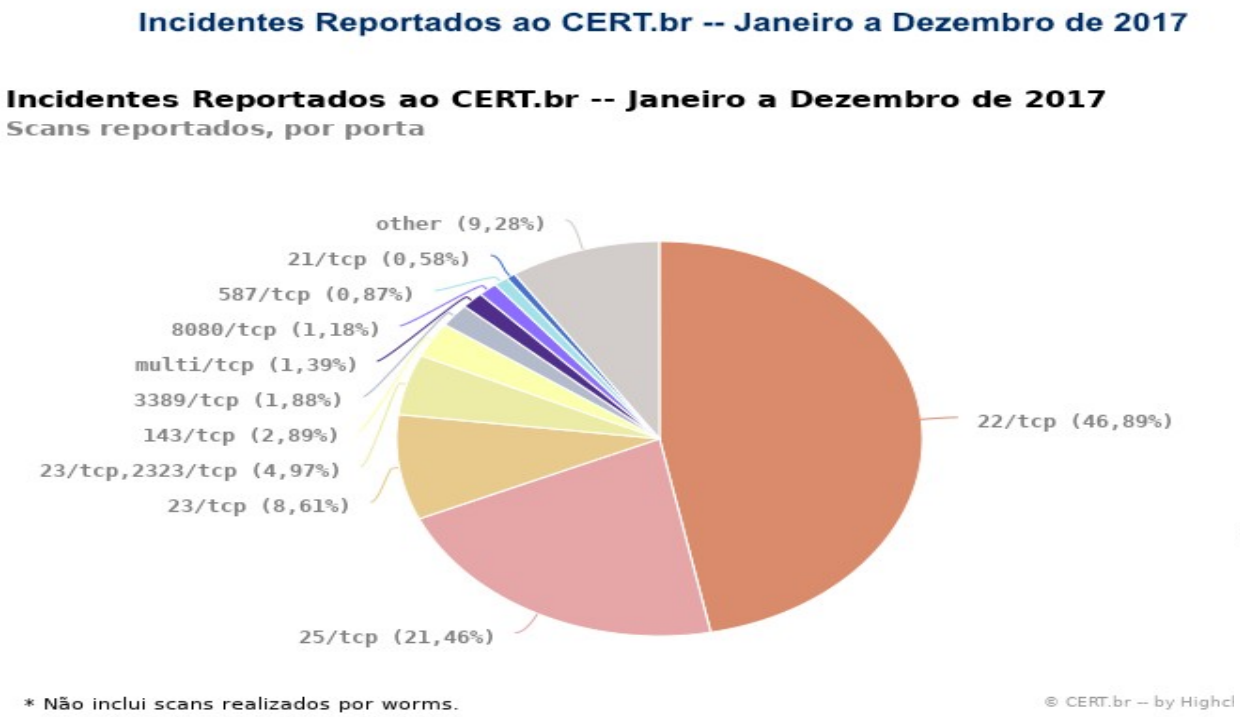


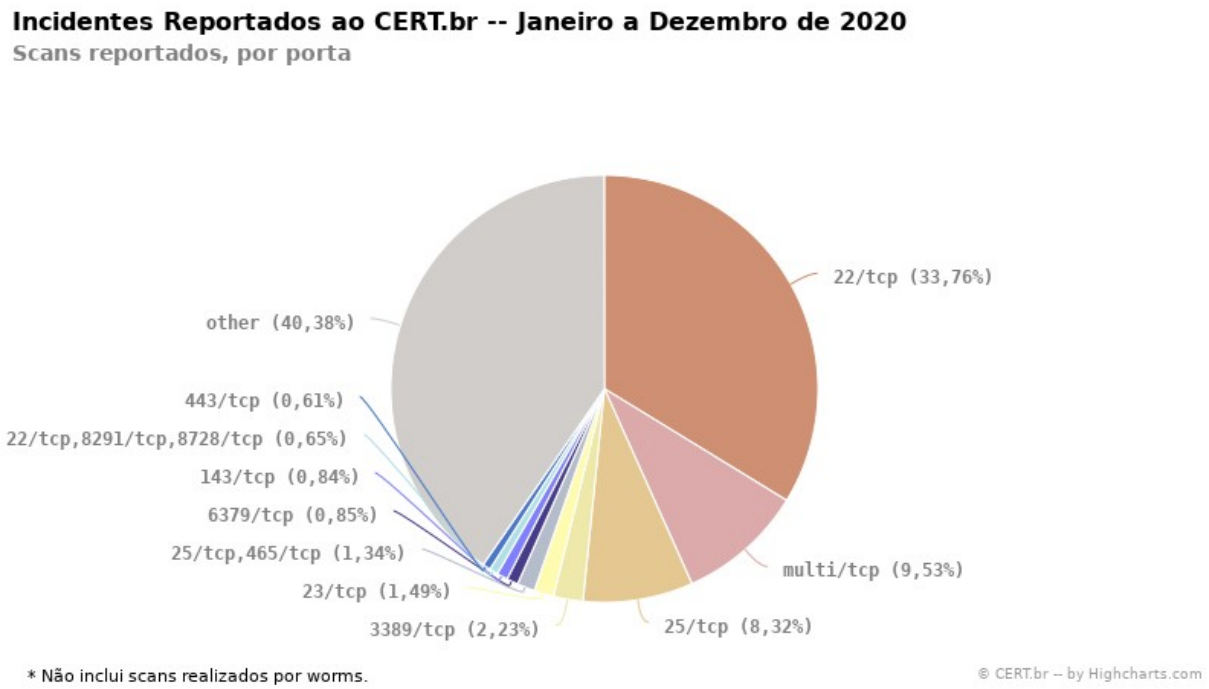
NÚMEROS BRASIL 2016





NÚMEROS BRASIL 2020 – Por portas





SEGURANÇA

- O que é segurança????
- O que é seguro???
- O que é segurança em rede de computadores??

Definição de Segurança

- A segurança de um sistema, aplicação ou protocolo é sempre relacionada à:
  - Conjunto de propriedades desejadas;
  - Um adversário com capacidades específica.
- Por exemplo, arquivos com permissões padrão em Linux e Windows não são efetivos contra um adversário que pode dar um boot a partir de um CD.

SEGURANÇA

- Importância da segurança de redes
  - Proteção de patrimônio (em especial: informação)
  - Credibilidade e vantagem competitiva
  - Cumprimento de responsabilidades
  - Continuidade de operação/atividade
- Segurança de redes
  - Segurança de computadores
  - Segurança da informação
- Segurança da informação = proteção + integridade + disponibilidade + autenticação

SEGURANÇA

- Prática: Prevenção, Detecção e Resposta

- Toda segurança é relativa, pode ser tomada em níveis e deve ser um balanceamento:
  - custo da segurança × valor do patrimônio
  - provável × possível
  - necessidades de segurança × do negócio

SEGURANÇA

- Análise de risco
  - Identificar e priorizar valores (patrimônio)
  - Identificar vulnerabilidades
  - Identificar ameaças e suas probabilidades
  - Identificar contramedidas (respostas)
  - Desenvolver análise de custo-benefício
  - Planejar políticas e procedimentos de segurança
    - Políticas e procedimentos de segurança
- Políticas: gerais, focam o que e porquê
  - Procedimentos: específicos e detalhados, focam quem, quando, como

Políticas vs. Mecanismos

Política de segurança:

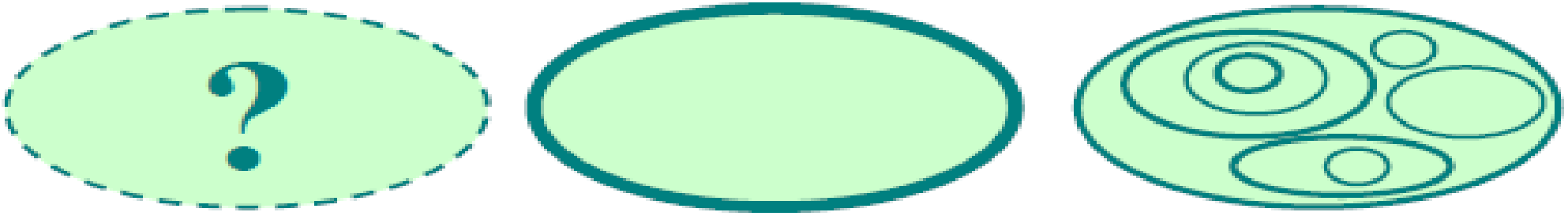
– Definição do que é permitido e do que é proibido

Mecanismo de segurança:

– Método, ferramenta ou procedimento para implementar uma política de segurança

SEGURANÇA

- Modelos de segurança
  - Obscuridade
    - proteção pelo sigilo e desconhecimento
  - Defesa perimetral
    - proteção concentrada nos limites/bordas da rede
  - Defesa extensiva
    - cuidar da segurança de cada sistema componente



Objetivos da Segurança - Conceitos

- C.I.A. - CID

SEGURANÇA

- Elementos e requisitos de segurança
  - **Confidencialidade**: proteção da informação contra descoberta ou interceptação não autorizada; privacidade
  - **Integridade**: impedir informação/transmissão de ser alterada/danificada de forma ñ-autorizada, imprevista ou acidental
  - **Disponibilidade**: confiabilidade de redes, sistemas e equipamentos sobre evitar ou se recuperar de interrupções

Confidencialidade

Segredo, ocultação, encobrimento de informações ou recursos

Necessária em áreas sensíveis:

– Instituições civis ou militares (governamentais) compartimentalizam informações -> need to know

– Acesso restrito àqueles que necessitam dela

Ex.: companhias com projetos proprietários

Confidencialidade

Mecanismo de suporte:

- Controle de acesso

Implementação do mecanismo de suporte:

- Criptografia

A chave controla o acesso

Precisa-se proteger a confidencialidade da chave!

Problemas... Ex.: WEP

Aplica-se à existência de dados

- Comunicações cifradas de extra-terrestres

Confidencialidade

Aspecto importante: ocultação de informações

- Equipamentos de uma organização
- Configurações
- Versões de sistemas e aplicações

Mecanismos para garanti-la dependem de

- Serviços de suporte confiáveis e premissas:

  kernel é capaz de lidar com o serviço

  agentes proveem dados corretos

  ambiente não comprometido

Integridade

Confiança nos dados ou recursos

Relacionada à prevenção de mudanças

impróprias ou não-autorizadas

Integridade dos dados:

- O conteúdo da informação não foi alterado

Integridade da origem:

- Fonte de dados (autenticação)

  Precisão, credibilidade e confiança na informação

Integridade

Aspecto importante: credibilidade!

Ex.: jornal imprime informação obtida de um vazamento do Palácio do Planalto e atribui a fonte errada (integridade dos dados, mas não da origem)

Mecanismos podem ser divididos em 2 classes:

- Prevenção
- Detecção

Integridade

Mecanismos de prevenção:

– Mantêm a integridade pelo bloqueio de qualquer tentativa não-autorizada de modificação dos dados ou tentativas de modificar o dado de maneira não autorizada

Usuário tenta mudar dado sem autoridade para tal

Usuário autorizado tenta mudar dado de outras maneiras não correspondentes a sua autorização

Ex.: intruso mexer nos registros de um contador vs. contador sonegar impostos

Integridade

Mecanismos de detecção:

- Alertam que a integridade dos dados não foi preservada (sem credibilidade)

Garantia depende de premissas sobre a fonte e confiança nesta fonte

Avaliação inclui corretude e confiança do dado

- Como e de quem foi obtido?
- O caminho do dado foi protegido?
- O destino do dado é protegido?

Disponibilidade

Habilidade de se usar a informação ou recurso desejado

Aspecto importante da confiabilidade e projeto de um sistema:

– Sistema indisponível é tão ruim quanto um sistema inexistente

– Alguém pode deliberadamente negar acesso a um dado ou serviço, tornando-o indisponível

Disponibilidade

Ex.: projetos de sistemas podem assumir um modelo estatístico para analisar padrões de uso esperado (garantidos por mecanismos)

Se esse uso é manipulado (tráfego de rede), a premissa não é mais válida -> falha

– Mecanismo para manter o recurso/dado disponível não suporta um ambiente para o qual ele não foi projetado

– Ex.: conexões do Apache

Disponibilidade

Tentativas de bloquear a disponibilidade são difíceis de se detectar:

– O padrão de acesso incomum é uma anomalia momentânea, uma falha de dispositivo/recurso ou um ataque proposital?

Se um sistema indisponível é essencial para o funcionamento de outro, a negação do serviço ocorre em cascata (e.g., interface de consulta e banco de dados remoto)

SEGURANÇA

- Elementos e requisitos de segurança
  - **Identificação e Autenticação**: distinguir, determinar e validar a identidade do usuário/entidade (se é quem diz ser)
  - **Controle de acesso**: limitar/controlar nível de autorizações de usuários/entidades a uma rede, sistema ou informação
  - **Não-repúdio**: impedir que seja negada a autoria ou ocorrência de um envio ou recepção de informação

SEGURANÇA DA INFORMAÇÃO

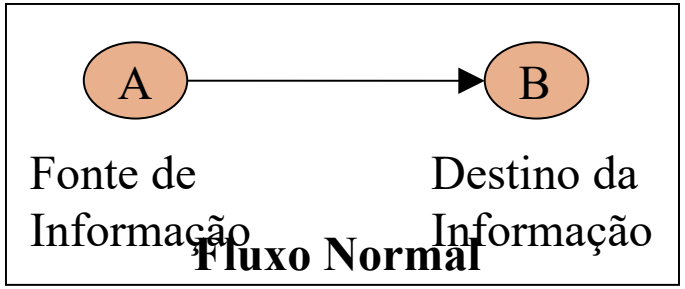
AMEAÇAS E ATAQUES

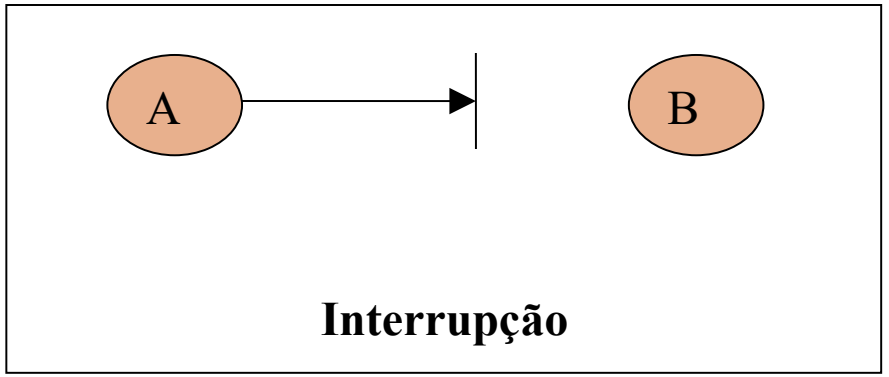
- Vulnerabilidade
  - Fraqueza inerente de um elemento do sistema
  - Brecha: ponto fraco ou falha que pode ser explorado
- Ameaça
  - Qualquer coisa que possa afetar ou atingir o funcionamento, operação, disponibilidade, integridade da rede ou sistema
- Ataque
  - Técnica específica usada para explorar uma vulnerabilidade
- Contramedidas
  - Técnicas ou métodos usados para se defender contra ataques, ou para fechar ou compensar vulnerabilidades

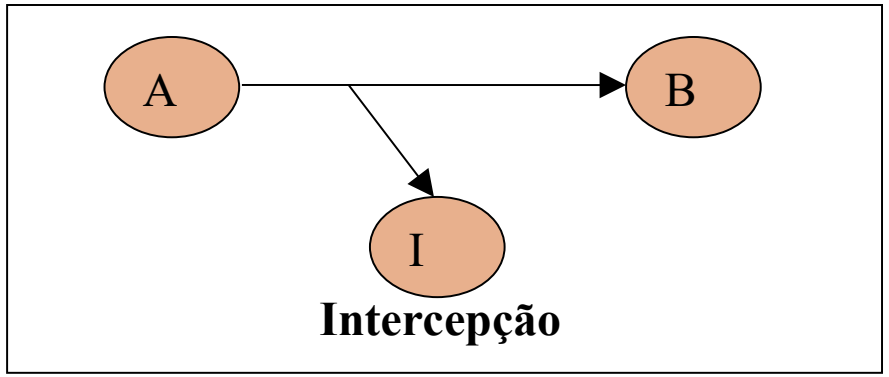
AMEAÇAS E ATAQUES

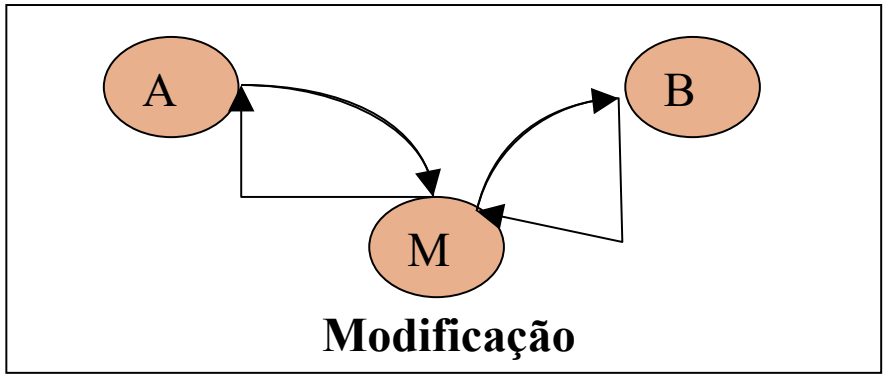
- Vulnerabilidades
  - Principais origens
    - Deficiência de projeto: brechas no hardware/software
    - Deficiência de implementação: instalação/configuração incorreta, por inexperiência, falta de treinamento ou desleixo
    - Deficiência de gerenciamento: procedimentos inadequados, verificações e monitoramento insuficientes
  - Exemplos
    - Instalação física: má proteção física de equipamentos e mídia
    - Hardware e Software: situações não previstas, limites, *bugs* no projeto, deixando brechas que podem ser exploradas
    - Mídia: roubo, perda, danificação, desgaste de discos, fitas etc.
    - Transmissão: interceptação de sinal, monitoramento, *grampo*
  - Humana: desleixo, preguiça, estupidez, ganância, revolta etc.

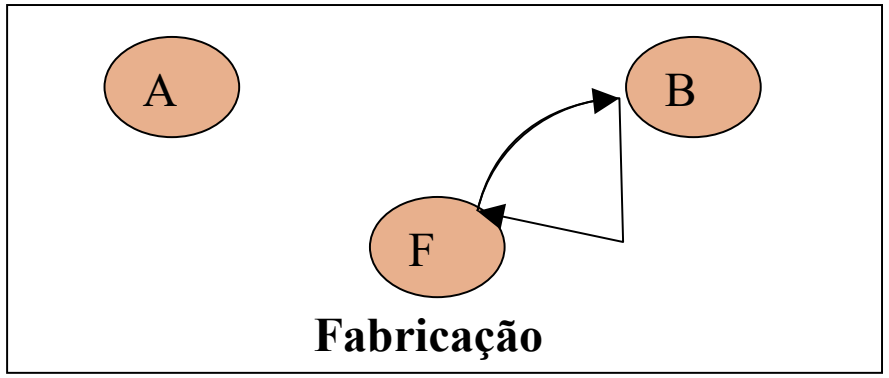
AMEAÇAS NA SEGURANÇA











AMEAÇAS E ATAQUES

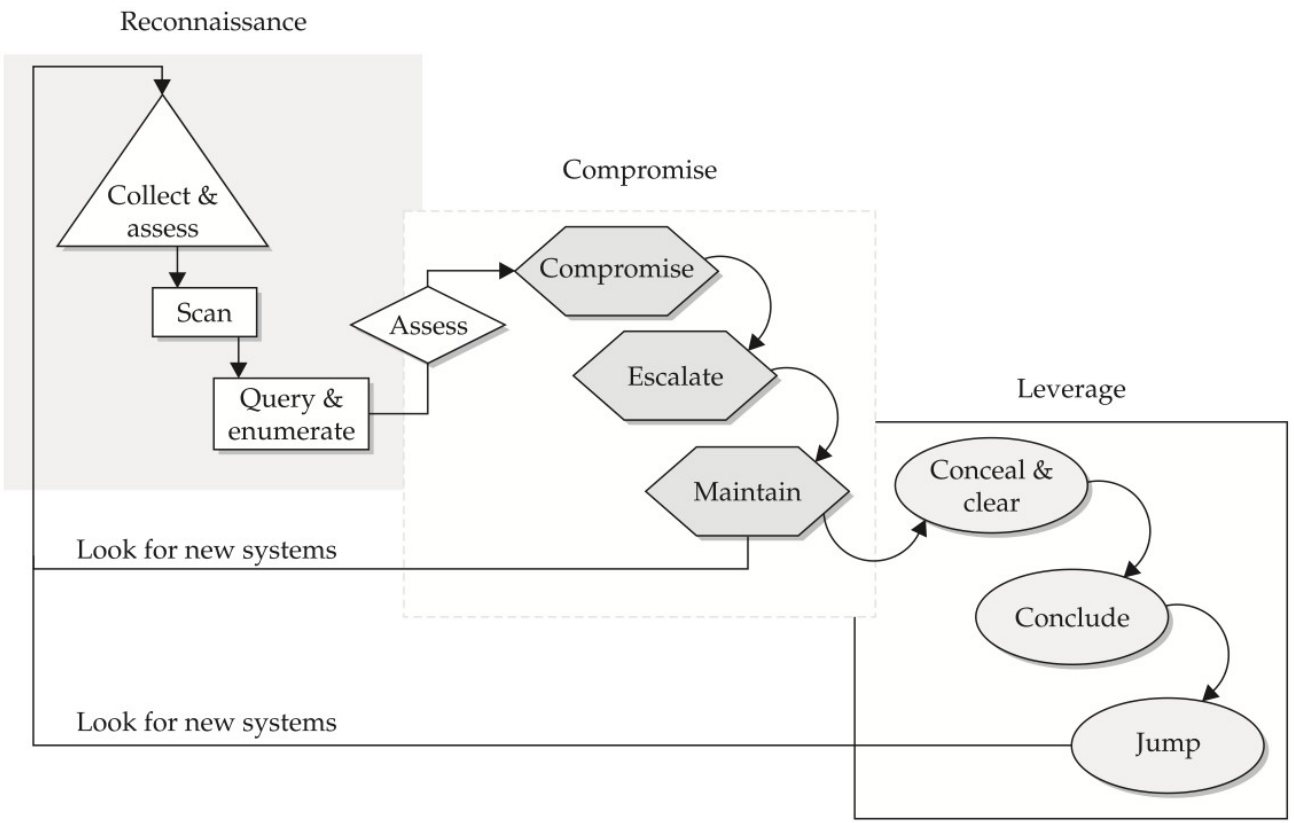
- Ataques
  - Ataques sobre o fluxo de informação
    - Interrupção: ataca a disponibilidade
    - Interceptação: ataca a confidencialidade
    - Modificação: ataca a integridade
    - Fabricação: ataca a autenticidade
  - Passivo
    - Interceptação, monitoramento, análise de tráfego (origem, destino, tamanho, frequência)
  - Ativo
    - Adulteração, fraude, reprodução (imitação), bloqueio

Passos de um Ataque

Um ataque consiste de um conjunto de etapas para ter sucesso:

- Reconhecimento e enumeração;
- Ganho de acesso (intrusão);
- Manutenção do controle (persistência);
- Ocultação de traços (limpeza);
- Fazer o alvo trabalhar para o atacante.

Modelagem de Ataques



Fonte: Ha rton, Clinton Mugge. McGraw-Hill, 2003.

Reconhecimento

- Levantamento de dados do alvo:
  - Obtenção de informações publicamente disponíveis (estrutura do alvo, informações de funcionários, domínios/endereços IP; determinação de quais dados usar na varredura).
- Varredura:
  - Processo para identificar recursos ``acessíveis'' na rede ou sistema alvo.
- Enumeração:
  - Obtenção de detalhes sobre os recursos online identificados (versão do SO, serviços em execução, vulnerabilidades).

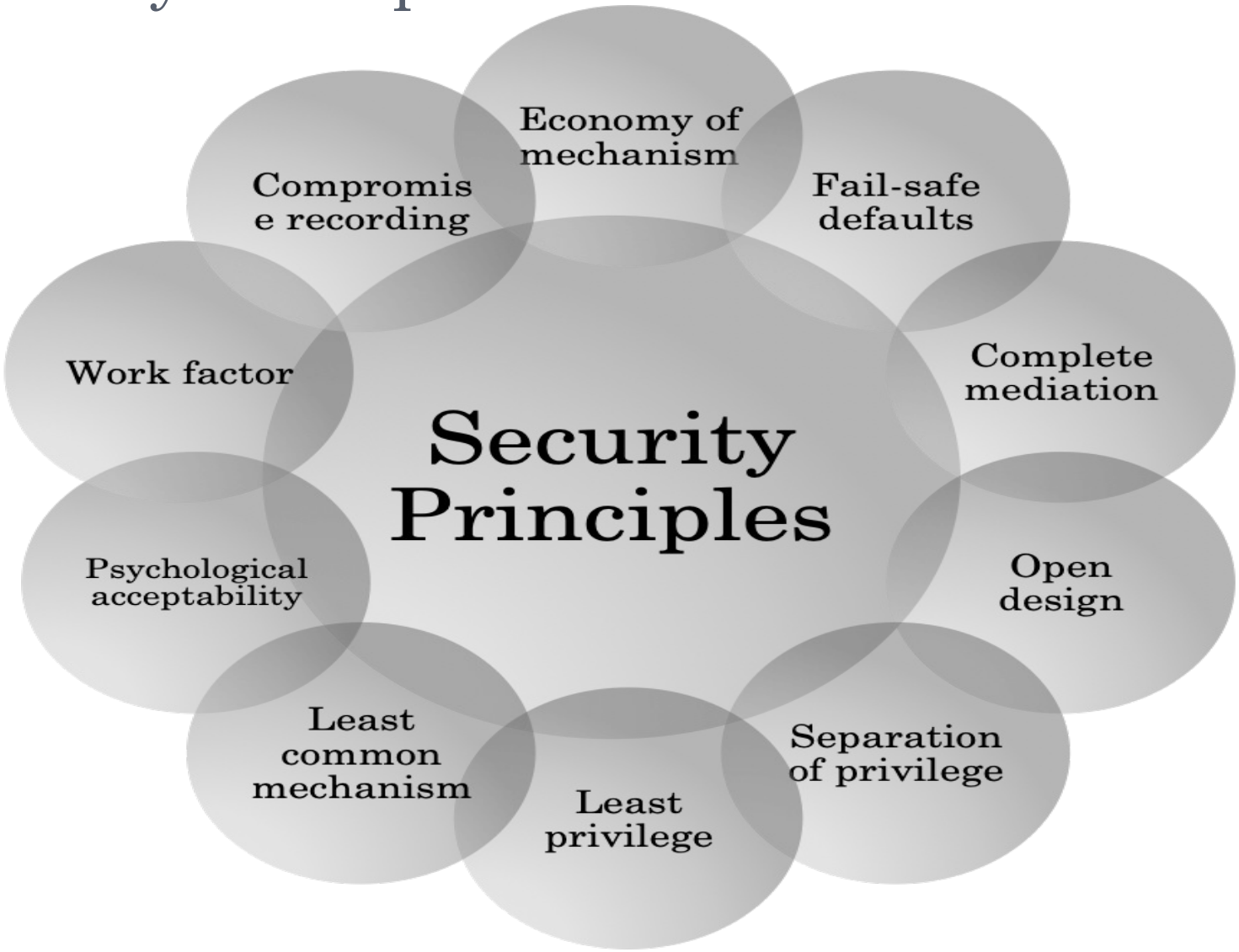
Reconhecimento

- Coleta de informações
  - Identificação de domínios
    - whois <DOMÍNIO>
  - Identificação de endereços IP (hostnames comuns, como ns1, ns2, www, smpt...)
  - dig, nslookup
  - Enumeração de serviços ``disponíveis''
    - nmap -T5 -iL <LISTA DE ALVOS>

Alavancagem

- Ocultando rastros:
  - Listagem das atividades realizadas e artefatos gerados para remoção de evidências;
- Conclusão das atividades pretendidas:
  - Ex.: Atacante corrige vulnerabilidade explorada para evitar perder a máquina.
- Trampolim:
  - Migração para outro host (volta à fase de reconhecimento ou abusa alguma credencial já obtida).

The Ten Security Principles



Economy of mechanism

- Esse princípio foca na **simplicidade** do projeto e da implementação das medidas de segurança.
  - Enquanto aplicável a maioria dos empreendimentos de engenharia, a noção de simplicidade é especialmente importante no domínio de segurança, uma vez que um simples framework de segurança facilita o entendimento aos desenvolvedores e usuários permitindo desenvolvimento e validação eficientes.

Fail-safe defaults

- Esse princípio diz que a configuração padrão (default) de um sistema deve ter um **esquema de proteção** conservador.
  - Por exemplo, quando adicionar um novo usuário no sistema operacional, o grupo default deve conter um mínimo de direitos de acesso a arquivos e serviços. Infelizmente, sistemas operacionais e aplicações frequentemente apresentam opções que focam mais na usabilidade em detrimento a segurança.
  - Esse é o caso para um número grande de aplicações populares, tais como browsers da web que permitem a execução de códigos baixados de servidores web.

Complete mediation

- A ideia por detrás desse princípio é que cada acesso a um recurso deve ser checado para o **cumprimento de um regime de proteção**.
  - Como consequência, deve-se ter o cuidado de técnicas de melhoria de desempenho que salvam os resultados dos controles de autorização anteriores, uma vez que as permissões podem mudar ao longo do tempo.
  - Por exemplo, um web site de um banco on-line deve requerer que usuários façam login novamente após um determinado tempo (em geral 15 minutos é o intervalo definido).

Open design

- De acordo com esse princípio, a arquitetura de segurança e **projeto** de um sistema devem ser **disponibilizados ao público**.
  - Segurança deve ser preocupar apenas em manter as chaves criptográficas secretas.
  - Projeto aberto permite que o sistema seja examinado por várias partes, o que leva a descoberta e correção precoce das vulnerabilidades de segurança causadas por erros de projeto.
  - O princípio de projeto aberto é o oposto da abordagem conhecida como **segurança por obscuridade**, que tenta alcançar a segurança mantendo os algoritmos criptográficos secreto e que tem sido historicamente usando sem sucesso por várias organizações.

Separation of privilege

- Esse principio diz que **condições múltiplas** são requeridas para alcançar acesso a recursos restritos ter um programa que execute uma ação.

Least privilege

- Cada programa e usuário de um sistema de computador deve operar com os **privilégios mínimos** necessários para funcionar corretamente.
  - Se este princípio for aplicado, o abuso de privilégios é restrito e os dados causados pelo comprometimento de uma conta de aplicativo ou usuário é minimizado.
  - O conceito militar **necessidade de saber** é um exemplo deste princípio.

Least common mechanism

- Em sistemas com múltiplos usuários mecanismos que permitam que os recursos sejam **compartilhados por mais de um usuários devem ser minimizados**.
  - Por exemplo, se um arquivo ou uma aplicação precisa ser acessada por mais de um usuário, então esses usuários devem ter canais separados para cada acesso a esse recurso para prevenir consequências imprevistas que podem ser causadas por problemas de segurança.

Psychological acceptability

- Este princípio estabelece que interfaces de usuário devem ser **bem projetadas e intuitivas**, e todas as configurações relacionadas a segurança devem aderir ao que um usuário comum poderia esperar.

Work factor

- De acordo com esse princípio, o **custo a ser contornado** por um mecanismo de segurança devem ser comparador com os recursos de um atacante ao projetar um esquema de segurança.
  - Um sistema desenvolvido para proteger as notas dos alunos em um banco de dados da Universidade, que pode ser atacado por bisbilhoteiros ou estudantes que queiram mudar suas notas, provavelmente precisa de medidas de segurança menos sofisticados do que um sistema construído para proteger segredos militares, que podem ser atacados por organizações de inteligência do governo.

Compromise recording

- Este princípio estabelece que, por vezes, é mais desejável **gravar os detalhes** de uma intrusão do que adotar medidas sofisticadas para evitá-la.
  - Câmeras de vigilância conectadas a internet são um exemplo típico de um sistema de registro que pode ser desenvolvido para proteger um edifício em vez de reforçar portas e janelas.
  - Os servidores em uma rede no escritório podem manter registros de todos os acessos a arquivos, todos os emails enviados e recebidos e todas as sessões dos navegadores.

AMEAÇAS E ATAQUES

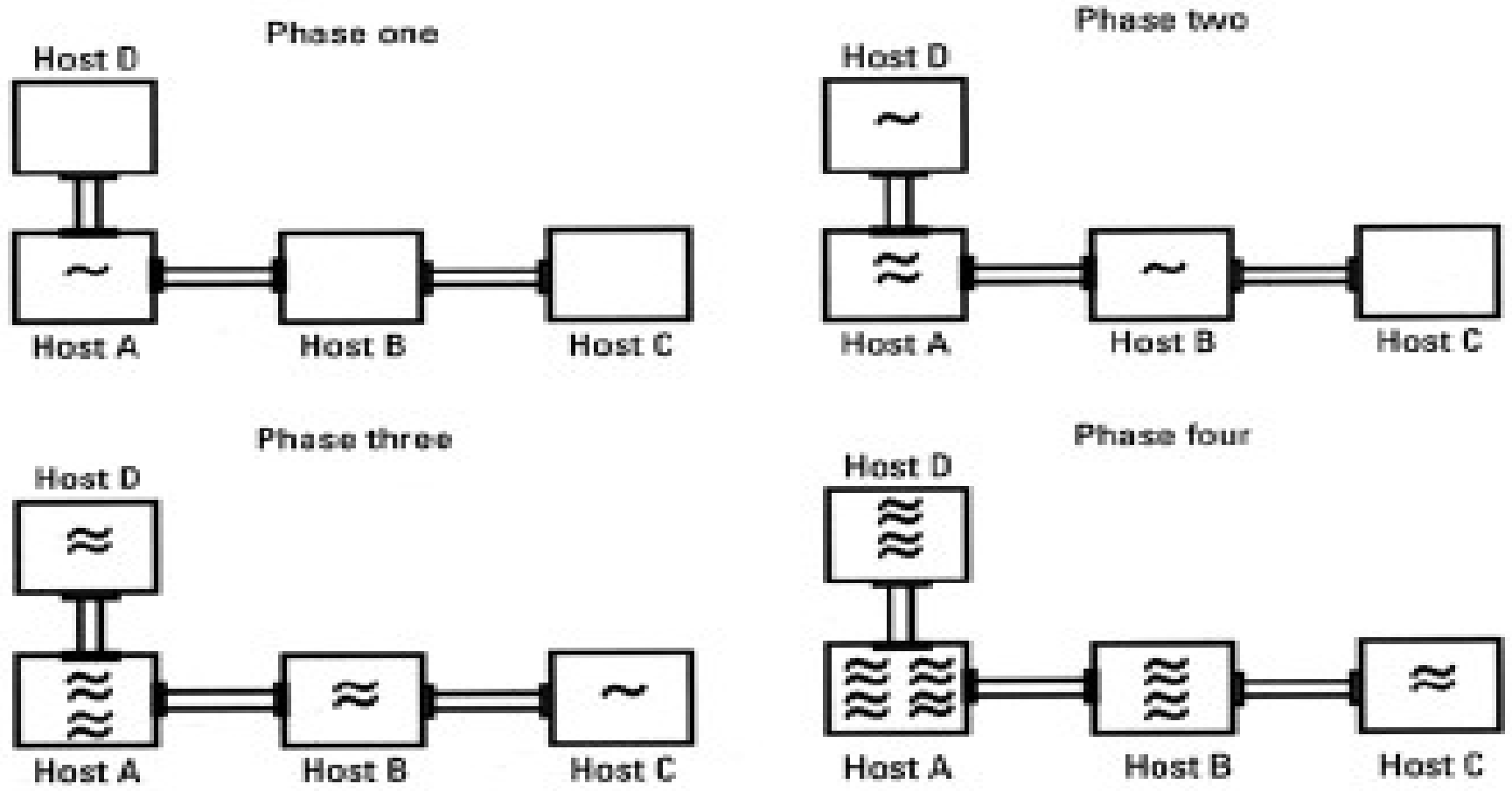
- TCP/IP e Ataques
  - Muitos ataques são baseados em características de TCP/IP
  - TCP/IP: arquitetura de protocolos padrão da Internet, para interconexão de redes
    - IP (*Internet Protocol*): protocolo de camada de rede sem conexão, baseado no endereço internet *n.n.n.n* (32-bit)
    - TCP (*Transfer Control Protocol*): protocolo orientado a conexão (fim-a-fim lógica entre dois nodos), com controle de fluxo, detecção de erro e seqüenciamento de dados
    - UDP (*User Datagram Protocol*): protocolo na camada de transporte, com datagramas sem conexão, adequado para transmissão simplificada de porções de dados

AMEAÇAS E ATAQUES

- Exemplos de ameaças e ataques
- Vírus
  - Programa ou fragmento de código parasita, que não funciona de forma autônoma; requer um hospedeiro (programa “autêntico”) ao qual se anexa para funcionar
  - Ativado pela execução de programa infectado
  - Se propaga pela infecção de outros programas ou envio de programa infectado por e-mail (auto-propagação), ou ainda pela cópia de programa infectado
- Verme
  - Tipicamente é um programa independente (autônomo) feito para se propagar ou ativar nos sistemas infectados e procurar outros sistemas nas redes acessíveis
  - Hoje existem intrusos mistos entre vírus e verme

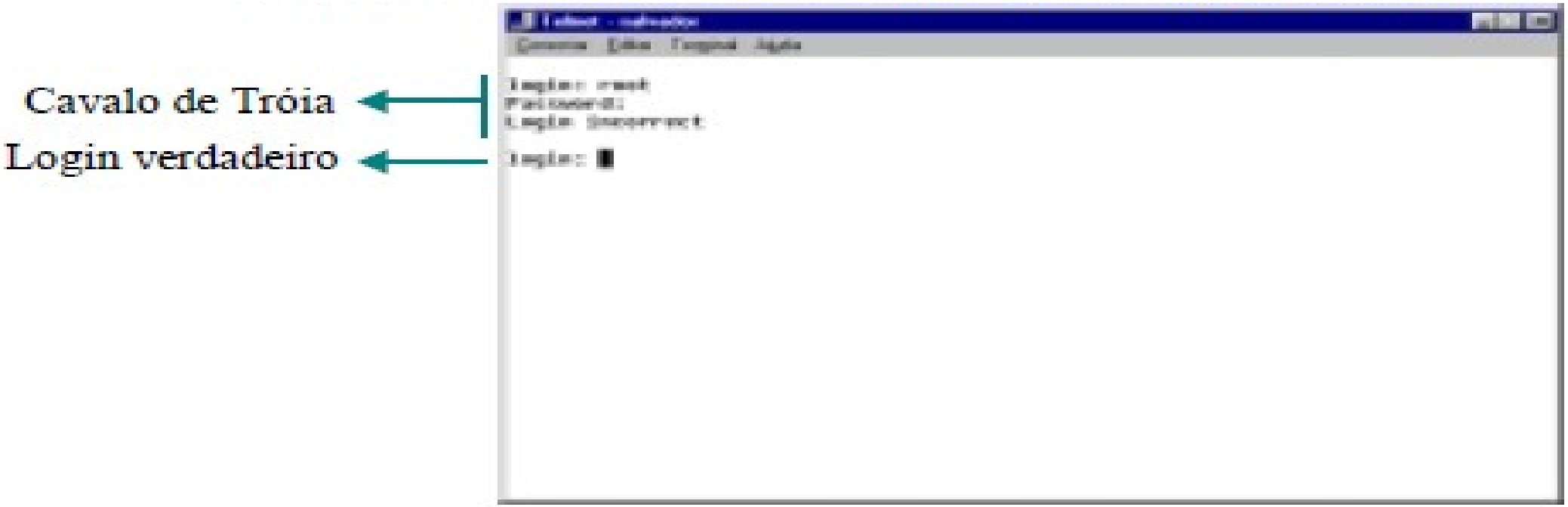
AMEAÇAS E ATAQUES

- Exemplos
  - Internet worm (Robert Morris, 1988)



AMEAÇAS E ATAQUES

- Exemplos
  - Cavalo de Tróia (Trojan Horse)
    - Programa ou fragmento de código maléfico que se esconde dentro de um programa, ou se disfarça de programa legítimo



AMEAÇAS E ATAQUES

- Exemplos
  - Back Door (Porta dos Fundos) ou Trap Door (Armadilha, Alçapão)
    - Forma não documentada de ganhar acesso a um sistema, criada no sistema por quem o projetou
    - Pode ser também um programa alterado ou incluído no sistema para permitir acesso privilegiado a alguém
  - Bomba Lógica
    - Programa ou seção de um programa projetado com intuito malicioso, que é ativado por determinada condição lógica
    - Caso mais comum: funcionário programador mal intencionado

AMEAÇAS E ATAQUES

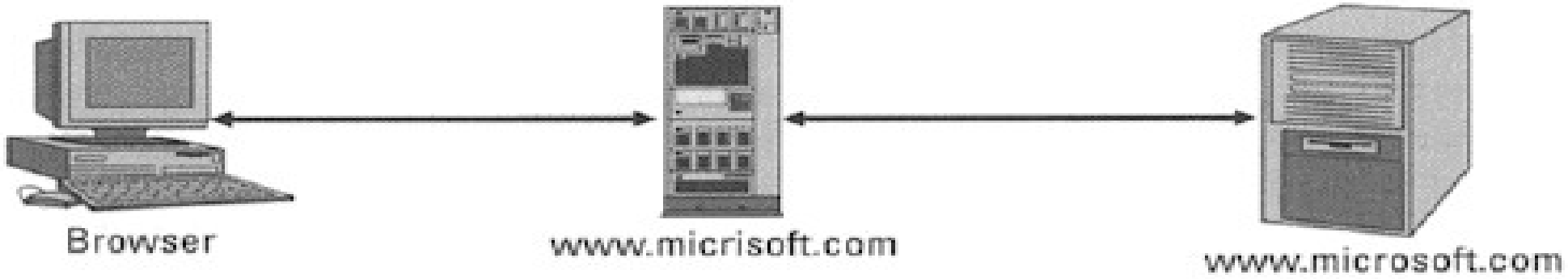
- Exemplos
  - Port Scanning (Varredura de Portas)
    - Técnica comum a hackers para reconhecimento
    - Programa que ouve a números de porta bem conhecidos para detectar informações e serviços em execução no sistema
    - Exemplos de portas comuns padrão da Internet:
      - 20 FTP dados (transferência de arquivos)
      - 21 FTP controle
      - 23 Telnet (terminal)
      - 25 SMTP (envio de e-mail)
      - 80 HTTP (WWW)
      - 110 POP3 (recepção de e-mail)

AMEAÇAS E ATAQUES

- Exemplos
  - Spoofs (Falsificação ou Disfarce de identidade)
    - IP Address Spoofing
      - Todo dispositivo em rede TCP/IP tem um endereço IP único, que é sua identificação (ex: 147.34.28.15)
      - IP Spoof: usar máquina configurada com IP aceito pelos sistemas de validação (roteador, firewall)
    - Sequence Number Spoofing
      - Conexões de rede TCP/IP usam nºs de sequência, incluídos em transmissões e trocados por transação
      - Se o algoritmo de geração de números é previsível, um hacker pode monitorar, gravar a troca de números de sequência e prever os próximos para se inserir na conexão

AMEAÇAS E ATAQUES

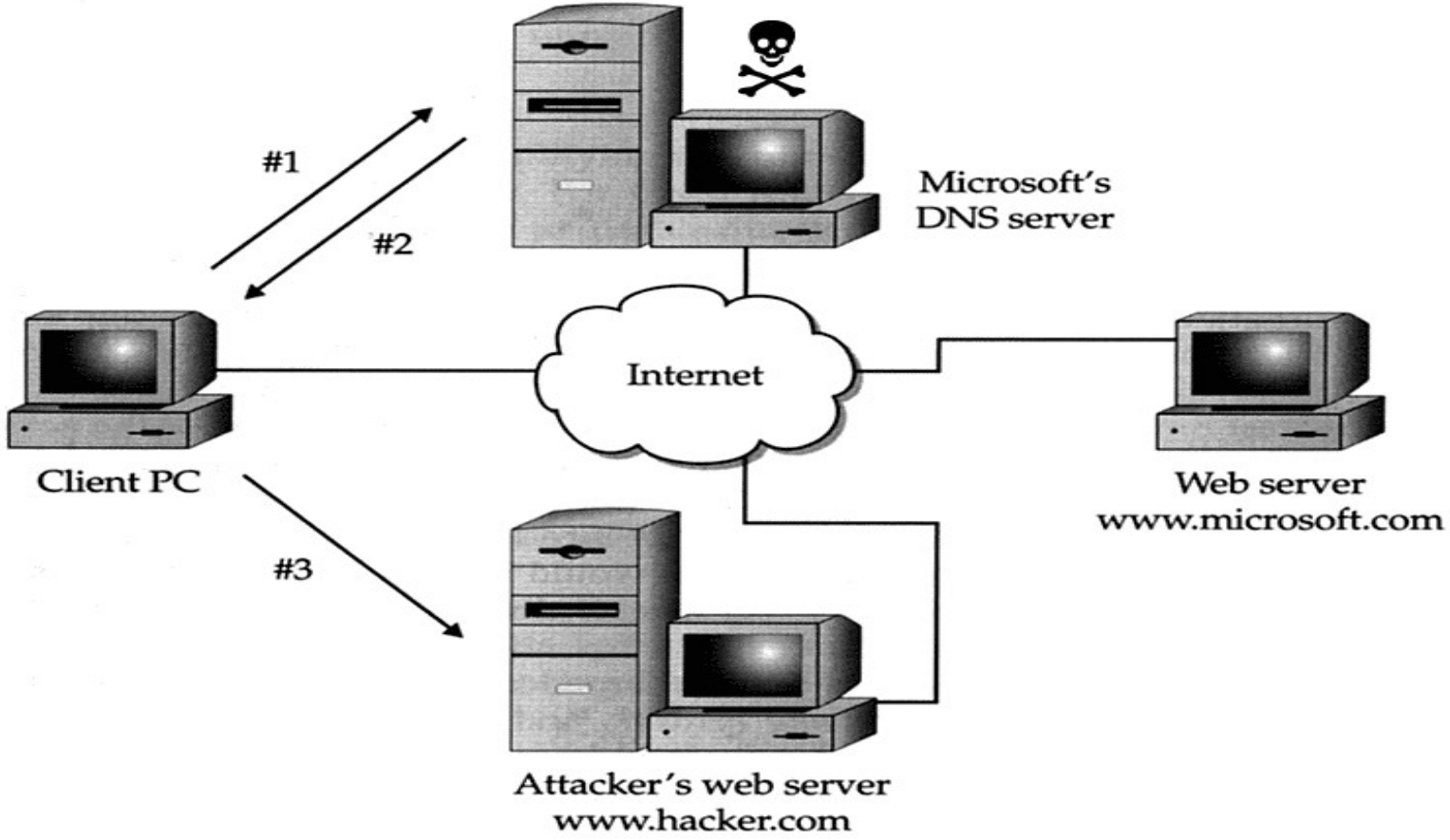
- Exemplos
  - DNS Spoof
    - MIM - Man In the Middle (Homem No Meio)
      - Técnica de se interpor no meio da comunicação
      - Ex.: registrar domínio parecido. Quando se comete erro de digitação, atacante se interpõe e pode repassar a comunicação c/ domínio correto, mas captura dados



      - Redirecionamento: inserir links para destinos falsos

AMEAÇAS E ATAQUES

- Exemplos
  - Envenenamento de DNS (DNS *Poisoning*)



AMEAÇAS E ATAQUES

- Exemplos
  - Spoofs (Falsificação ou Disfarce de identidade)
    - Replay (Reprodução)
      - Interceptar e capturar uma transmissão legítima entre dois sistemas e retransmitir esta mais tarde
      - Pode-se evitar com *timestamp* (controle de tempo)
  - Estouro de Pilha (Stack Overflow)
    - Consiste em preencher um buffer alocado na pilha com informação que excede o tamanho previsto, de forma que o endereço de retorno da função seja modificado

AMEAÇAS E ATAQUES

- Exemplos
  - Quebra de Senha (Password Cracking)
    - Tentar várias possibilidades de senha para ver se uma coincide com a de algum usuário/recurso
    - Geralmente usa-se o mesmo algoritmo que codifica (protege) as senhas de um sistema para codificar cada tentativa e comparar o resultado com a lista de senhas do sistema
    - Comum o uso de “dicionário” de palavras/expressões comuns
    - Existem muitos programas quebra-senha disponíveis, para a maioria dos sistemas operacionais e de rede
  - Engenharia Social
    - Métodos não-técnicos para obter acesso a um sistema, em geral um processo de convencer alguém a revelar informação
    - Exemplo típico: ligar para alguém pertencente ou com acesso a uma corporação, fingindo ser do suporte técnico desta e inventar uma história p/ solicitar a senha de acesso da vítima

AMEAÇAS E ATAQUES

- Exemplos
  - Sniffing (Monitoramento, “Grampo”)
    - Monitoramento de pacotes transitando na rede (passivo)
    - Muitas vezes são usadas ferramentas de fabricantes ou comerciais, criadas com propósitos legítimos (gerenciamento e manutenção de rede)
    - Conteúdo = informação: endereços IP, senhas etc. (Ex.: telnet e rlogin não criptografam as senhas digitadas pelo usuário)
    - Estatísticas = análise de tráfego: Ex.: servidores mais usados
  - Web Site Defacement
    - Ataque muito comum na Internet, para inserir mensagem de protesto, aviso, ridicularização etc. na home-page de um site
    - Normalmente hackers exploram alguma configuração frágil ou vulnerabilidade conhecida de um servidor web, do sistema operacional ou dos protocolos e componentes envolvidos

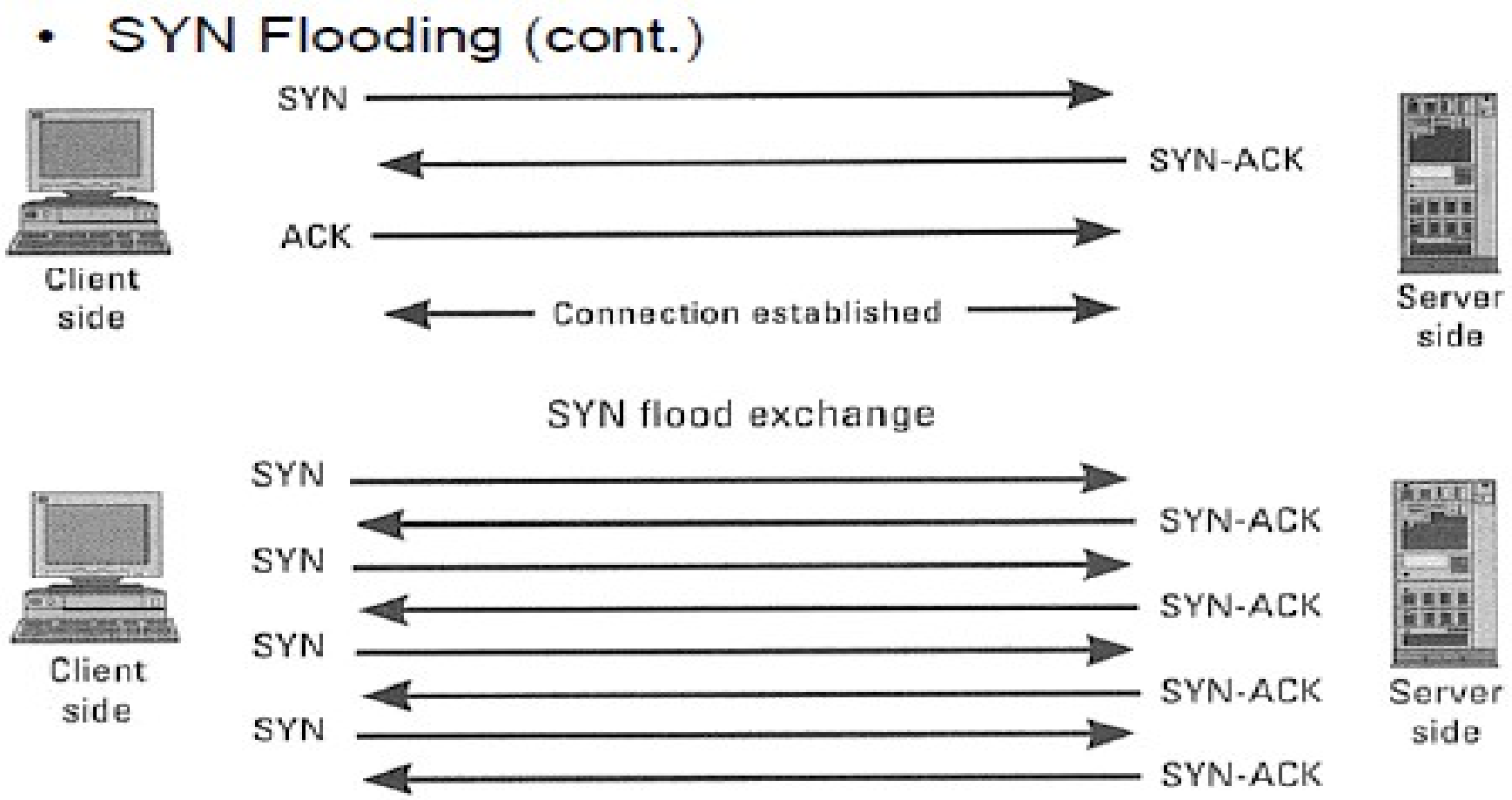
AMEAÇAS E ATAQUES

- DoS - Denial of Service (Interrupção de Serviço)
  - Ação que interrompe um serviço ou impede totalmente seu uso por usuários/entidades legítimos
  - Objetivo principal é “tirar do ar” (indisponibilizar) um serviço, apenas para causar o transtorno/prejuízo da interrupção ou para eliminar uma proteção que assim permita atingir outras formas de acesso não autorizado
  - Tipos de ataques DoS
    - Consumo de banda de rede: atacante tem banda maior que a da rede alvo ou vários atacantes simultâneos para sobrecarga
    - Consumo de recursos de sistema: criar situações de abuso ou sobrecarga que ultrapassem o limite do recurso (buffer, HD...)
    - Atingir falhas que levam à interrupção
    - Adulteração de rotas/DNS: ao invés de desativar um serviço, impede o acesso ao serviço legítimo (usa DNS *Poisoning*)

AMEAÇAS E ATAQUES

- Exemplos
  - Interrupção de Serviço (DoS - Denial of Service)
    - SYN Flooding (Inundação de SYN)
      - Ataca o *handshake* de 3-vias do estabelecimento de conexão TCP: cliente envia bit SYN (*synchronize sequence number*), servidor reconhece e responde com SYN-ACK, cliente reconhece a resposta enviando ACK e inicia a transferência de dados
      - Ataque: enviar SYNs e não responder aos SYN-ACK, deixando em aberto os estabelecimentos de conexão até ocupar todos os *buffers* de conexão no servidor
      - Outros clientes não conseguem estabelecer conexões legítimas e o ataque pode derrubar o sistema operacional se a situação consumir toda a memória livre do servidor

AMEAÇAS E ATAQUES

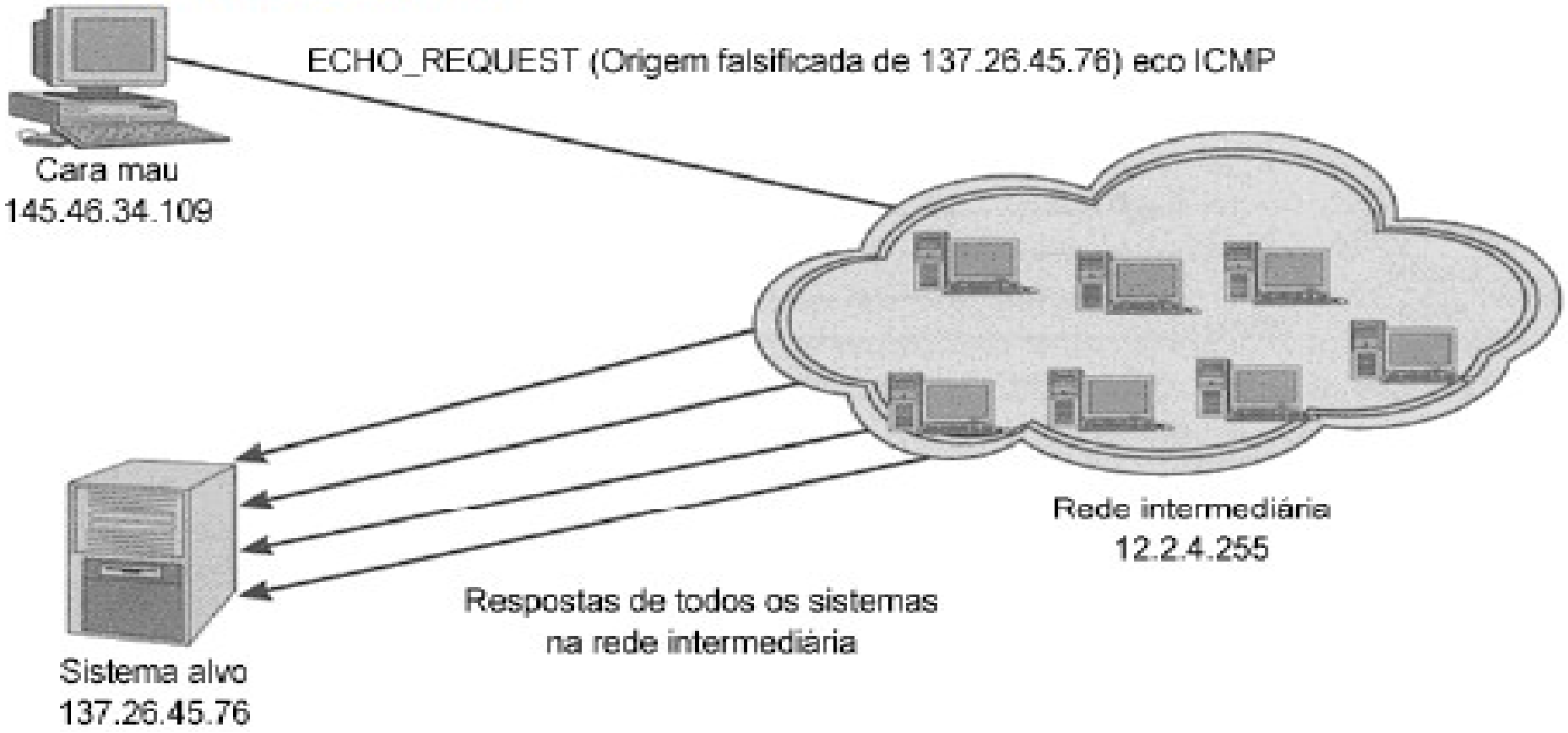


AMEAÇAS E ATAQUES

- Exemplos
  - Interrupção de Serviço (DoS - Denial of Service)
    - Ping da Morte (Ping of Death)
      - De aplicação simples, baseado em vulnerabilidade
      - Ping: comando TCP/IP que envia um pacote IP p/ um endereço, para testar se existe e está "vivo"
      - Vulnerabilidade: sistemas que não tratam adequadamente pacotes ICMP (pacote de controle a nível de IP) maiores do que o normal
      - Ataque: enviar seqüência de ping com campo ICMP de tamanho máximo (maior que o comum)
    - Smurf
      - Atacante envia um ECHO_REQUEST ICMP geral fazendo spoof do endereço origem como o endereço IP da máquina alvo = solicita uma resposta (eco) ICMP a todas as máquinas de uma rede, fingindo ser a máq. alvo
      - Todas as máquinas da rede respondem para a máquina alvo real, sobrecarregando a rede e o sistema alvo

AMEAÇAS E ATAQUES

- Smurf (cont.)



AMEAÇAS E ATAQUES

- Exemplos
  - SPAM / Junk Mail
    - Prática do envio de e-mail não solicitado, em larga escala
    - Normalmente são mensagens de propaganda ou solicitação de marketing de empresa tentando vender ou divulgar algo (que não queremos / não precisamos)
    - Grandes quantidades de SPAM podem ser usados para causar sobrecarga de servidores de e-mail (DoS)
  - Mensagem-Bomba (Mail Bomb)
    - Enviar e-mail enorme p/ sobrecarregar servidor e/ou o usuário
  - War Dialing
    - Método força-bruta para encontrar um telefone ligado a um modem (acesso discado a um sistema ou rede)
    - Normalmente automatizado, tentando uma faixa de um prefixo de telefone associado a uma grande empresa