Sistemas Operacionais

Prof. Me. Pietro M. de Oliveira

Aula de Hoje

Unidade IV

- Hardware/Software de Entrada/Saída.
- Relógio/Timer.
- Clientes Magros (Thin Clients).
- Gerenciamento de Energia.
- Proteção.
- Segurança.
- Ameaça e vulnerabilidade.
- Ataques/Malwares.

.

Hardware de Entrada e Saída

Usado para interagir com a máquina

Mouse, teclado, monitor, HD, Pen Drive, relógio.

Dispositivos de blocos:

Armazena dados.

Blocos de tamanho fixo (HD, pen drive).

De caractere:

Envia ou recebe cadeias de dados (*stream*).

Fluxo de caracteres (Mouse, teclado).

Outros

Relógio.

Hardware de Entrada e Saída

Alguns dispositivos/barramentos e suas velocidades de transmissão

Teclado	1.5 KB/seg
Modem 56K	7 KB/seg
Canal de telefone	8 KB/seg
Serial (RS-232)	28.8 KB/seg
Scanner	400 KB/seg
CD-ROM 40x	6 MB/seg
USB 2.0 High Speed	60 MB/seg
Disco Sata III	600 MB/seg
Ethernet	12.5 GB/seg
PCI Express 3.0	31.5 MB/seg

Hardware de Entrada e Saída

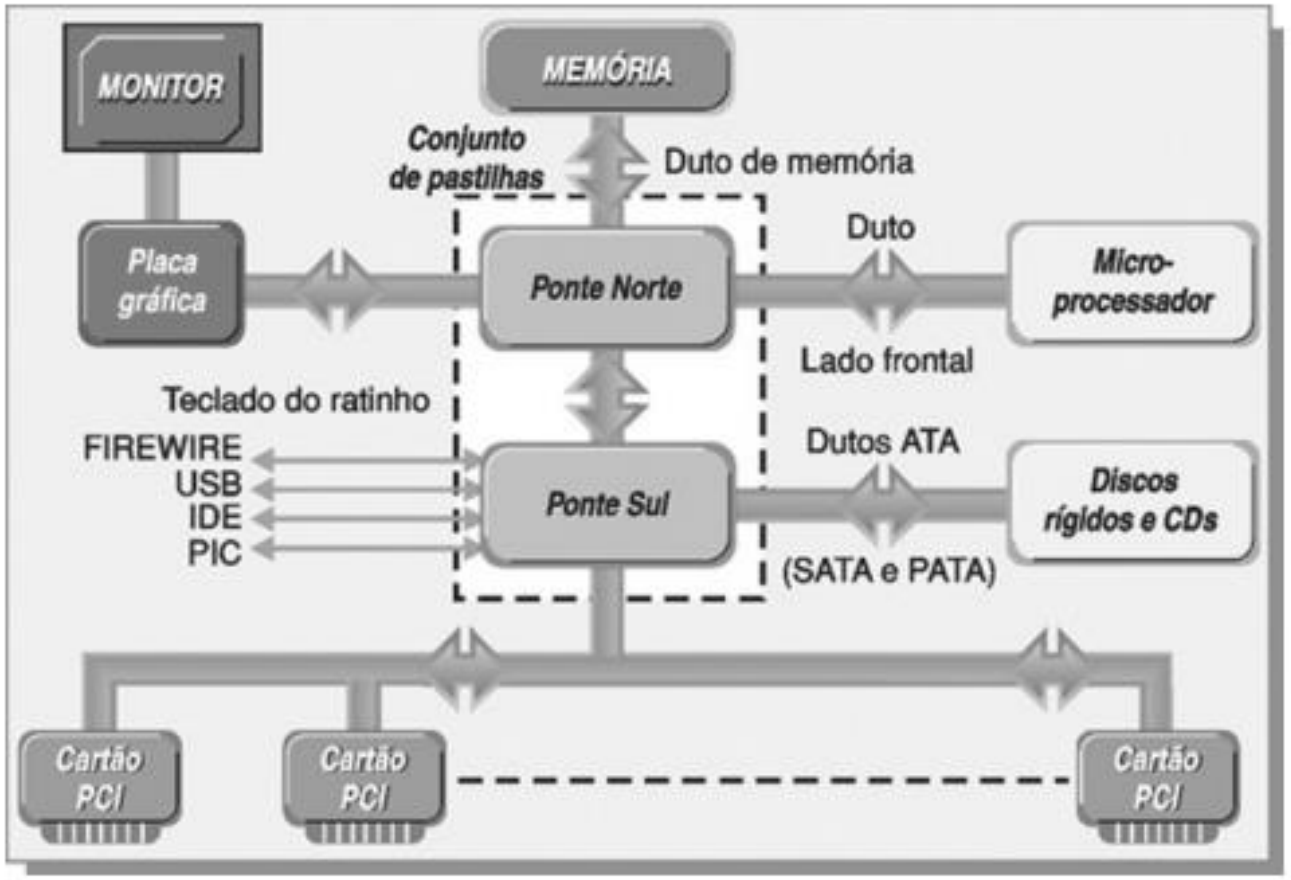
Placa mãe:

- Conecta todos os dispositivos por meio de barramentos.
- Controladores ou *Chipsets.*
- Ponte Norte.
  - Processador, RAM, GPU, monitor
- Ponte Sul
  - HD, USB, teclado, mouse, IDE

Interação c/ processador por meio de interrupções:

- Número do dispositivo solicitante.

Hardware de Entrada e Saída



Fonte: <www.sabereletronica.com.br/files/image/Nova-geracao_01_1_.jpg>

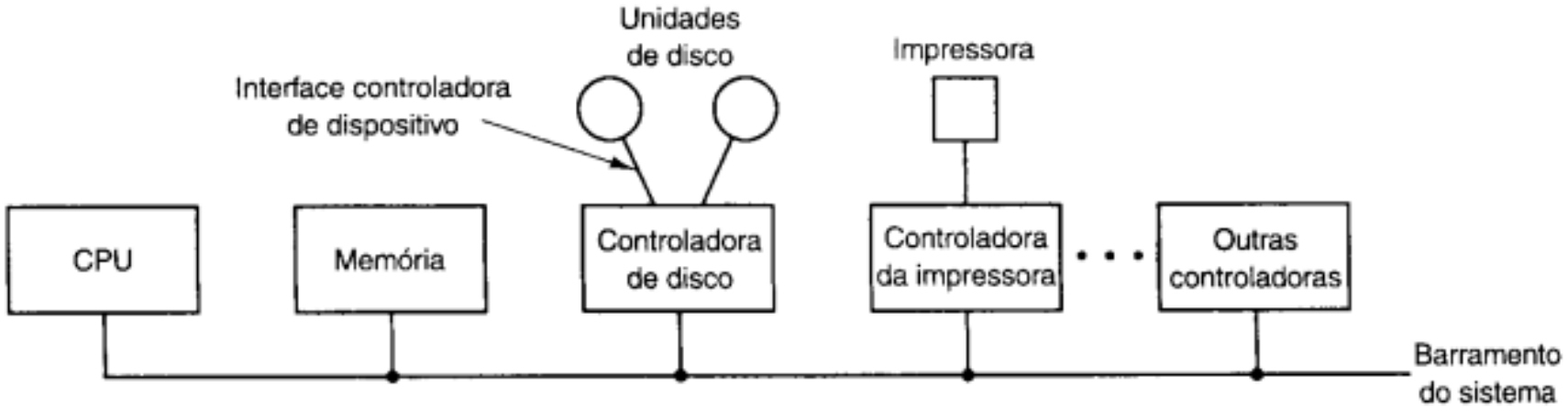
Hardware de Entrada e Saída

Controladoras

- Função:
  - Manipular streams e blocos de dados.
  - Correção de erros.
  - Bufferização.
- Registradores de controle:
  - Passar/receber dados.
  - Ligar/desligar dispositivo.
  - Determinar o estado do dispositivo.
  - SO utiliza para passar comandos.

Hardware de Entrada e Saída

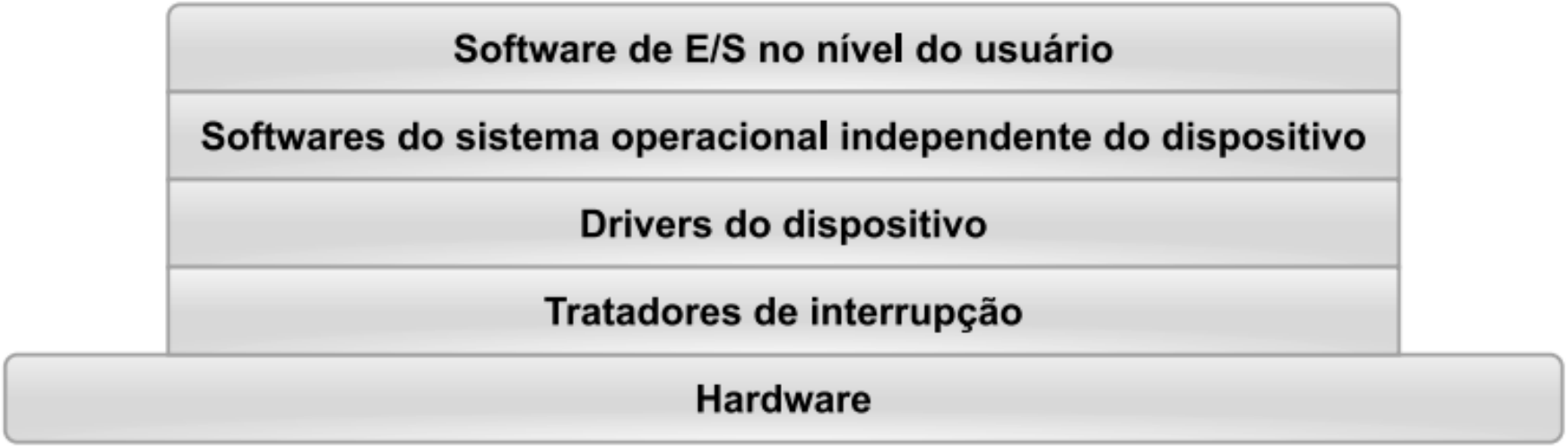
Modelo genérico de conexão de dispositivos



Fonte: Tanenbaum (2010, p. 114)

Software de Entrada e Saída

Quatro camadas



Fonte: Tanenbaum (2010, p.215)

Software de Entrada e Saída

Tratadores de interrupção

- Código específico executado no processador.
- Bloquear o driver.
- Processador realiza troca de contexto.
- Atender o dispositivo até completar a E/S.

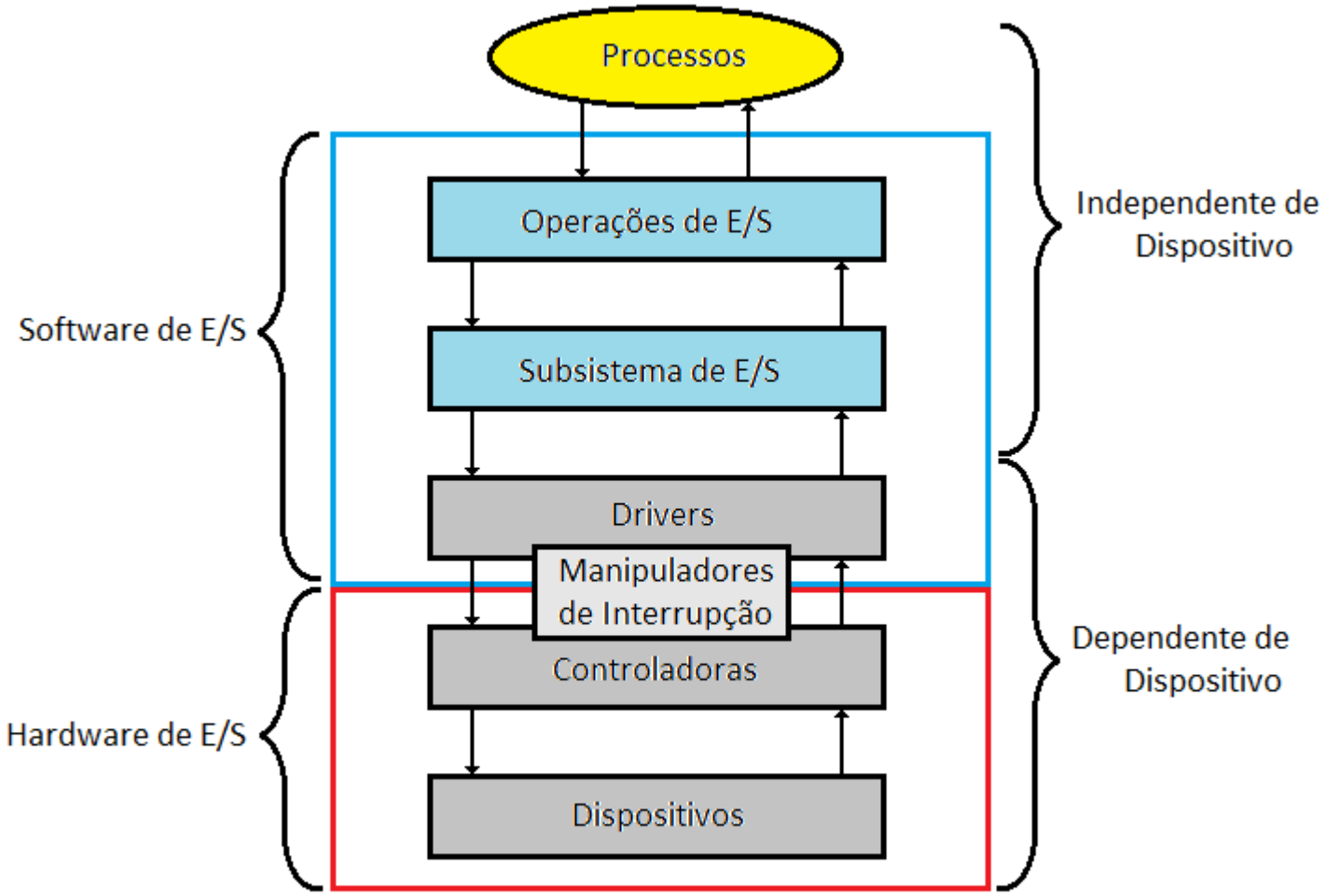
Drivers

- Alta diversidade de dispositivos existentes.
- Cada dispositivo.
- Código para o SO controlar o dispositivo.

Software de Entrada e Saída

- Software de E/S independente
  - Funções comuns a todos dispositivos.
  - Interface com funções:
    - Armazenar no buffer.
    - Reportar erros.
    - Alocar/liberar dispositivos dedicados.
- Software de E/S do usuário
  - Operações personalizadas.
  - Utiliza as funções da camada anterior.

Esquema Geral de E/S



Fonte: O autor

Dispositivos de Entrada e Saída

Exemplo:

- Teclado.
- Mouse.
- HD.
- Timer.
  - Manter data/hora.
  - Escalonamento preemptivo (*quantum*).
  - Controle de consumo de energia.
- Clientes Magros (*Thin Clients*)
  - “Terminal burro”.

Controle de Consumo de Energia

Temporizador:

- Sempre ativo (placa mãe).
- Contabiliza o tempo de inatividade.

Monitores

- Alto consumo de energia.
- SO desliga automaticamente.

HD

- Alta frequência/consumo.
- Modo Hibernar/Suspender.
  - SO salva o contexto atual no HD.

Thin Clients

Terminais com dispositivos de entrada/saída

- Teclado, mouse, monitor, portas USB.

Servidor

- Processamento, memória, HD
- SO:
  - Usuário/senha para iniciar uma sessão

Vantagens

- Melhor gerenciamento de arquivos/programas.
- Economia em consumo.
- Economia financeira.

Thin Clients

Terminais com dispositivos de entrada/saída

- Teclado, mouse, monitor, portas USB.

Servidor

- Processamento, memória, HD
- SO:
  - Usuário/senha para iniciar uma sessão.

Ideia semelhante aos *mainframes.*

Thin Clients

Vantagens

- Melhor gerenciamento de arquivos/programas.
- Economia em energia.
- Economia financeira.

Desvantagens

- Compartilhamento de recursos entre usuários.
- Perda de desempenho.

Proteção × Segurança

Segundo Tanenbaum, a distinção entre proteção e segurança não é bem definida.

Para nós

- Proteção: mecanismos internos ao SO
  - Controle de acesso a dados.
  - Políticas de uso de recursos (*r*,*w*,*x*).
- Segurança: aspectos externos
  - Invasões.
  - Ataques.
  - Vírus.

Segurança

Ameaça

Vulnerabilidades.

Correções: patches.

Ataque

Exploração de uma ameaça.

SO deve garantir:

Confidencialidade.

Integridade.

Disponibilidade.

Segurança – Principais Aspectos

- Perda de dados
  - “Ações divinas”.
  - Erros de hardware ou software.
  - Erros humanos.
  - Solução: Backup!
- Intrusos
  - Passivos.
  - Ativos.
  - O que fazer?

Segurança – Tipo de Inimigo

Usuários não técnicos

- Pessoas comuns bisbilhotando aleatoriamente.

Espionagem interna

- Alunos ou técnicos, por diversão.

Tentativa de fazer dinheiro

- Programadores de instituições bancárias.
- Hackers praticando extorsão.

Espionagem comercial ou militar

- Grandes corporações ou países.
- Alto investimento financeiro.

Ataques

Interrupção:

Impedir fluxo de dados ou processos.

Denial of Service (DoS).

Interceptação:

Acessar, consultar dados confidenciais.

KeyLogger.

Modificação:

Modificar o sistema.

Fabricação:

Informações falsas, componentes maliciosos.

Ataques

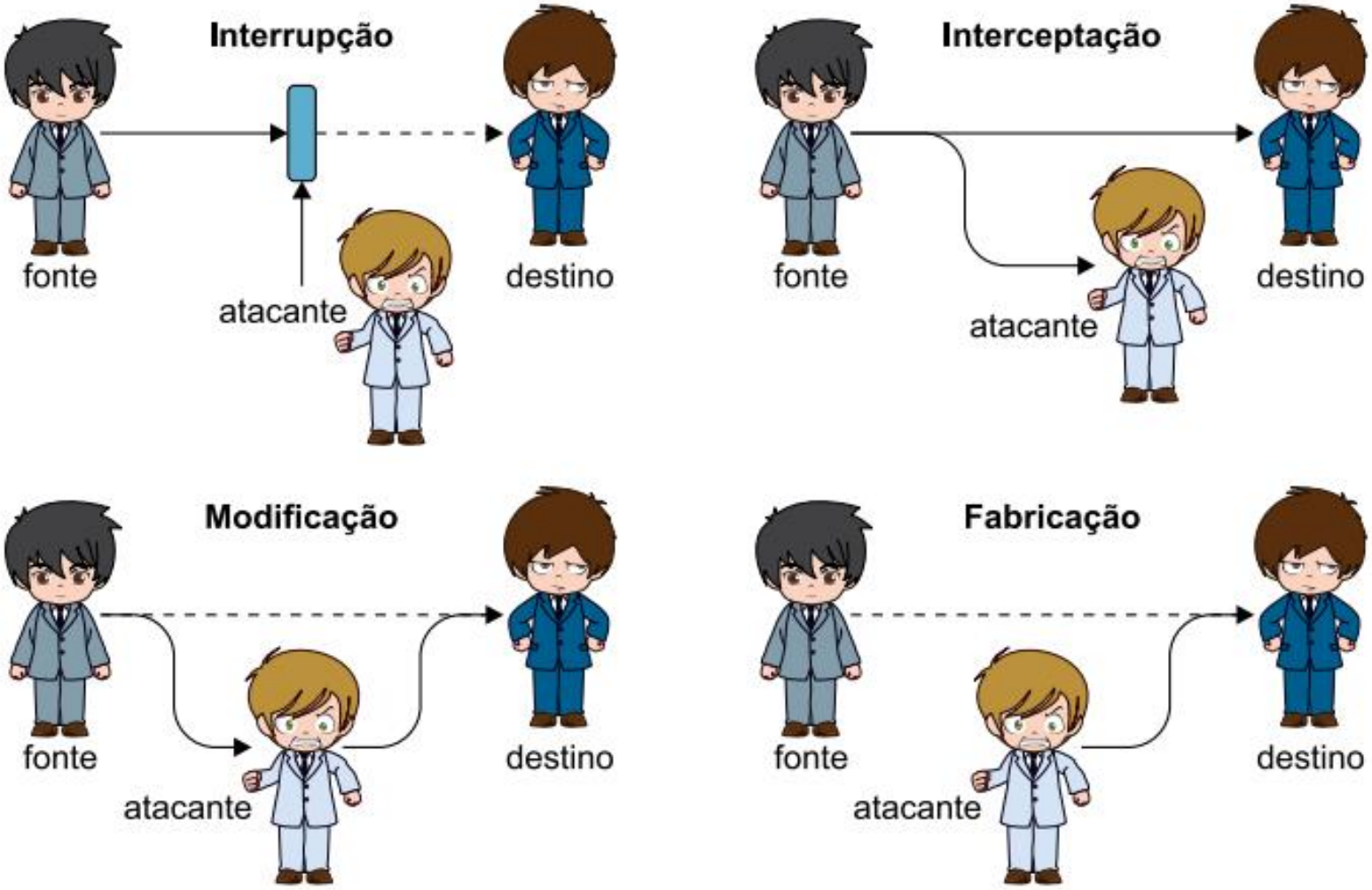


Figura 1: Tipos básicos de ataques (inspirado em [Pfleeger and Pfleeger, 2006]).

Fonte: Adaptado de Maziero (2013, cap. 8, p. 10). Disponível em: <http://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=so:so-cap08.pdf>

Malwares

Softwares maliciosos

Exploram ameaças já identificadas.

Característica de atuação:

- Vírus: infiltra-se e se replica em outros programas.
- *Worm*: infiltra-se mas não se replica (se espalha na rede).
- *RootKit*: oculta a presença de um intruso.
- *Trojan* (Cavalo de Tróia): promete algo, mas permite a entrada de um *worm* ou *rootkit.*

Malwares

- *Exploit*: detecta ameaças não corrigidas.
- *Packet Sniffer*: monitora pacotes de rede.
- *BackDoor*: abre portas de rede.
- *Keylogger*: captura tudo o que foi digitado.

Nenhum sistema operacional é 100% imune

Windows, Android, IOs, Mac OS, Linux.

Atualizações (*patches*).

Firewall.

Anti-vírus.

Exemplos Práticos

Bomba lógica

- Programador contratado.
- Inserção de código que exige senha:
  - Se a senha estiver OK, tudo bem.
- Programador demitido
  - Sem senha, o sistema trava.
- Chantagem: só o programador malicioso pode “corrigir” o travamento.
- Crime: extorsão.
- Recontratar o programador – é confiável?

Exemplos Práticos

- Malware
  - Infectar dispositivos computacionais
  - Apagar, modificar ou criptografar dados
  - Danificar inicialização do dispositivo
    - Ex.: infectar o BOOT
  - Extorsão (chantagem)
- Mais fácil previnir do que remediar
  - Software pirateado (torrents), links maliciosos, emails maliciosos, pornografia, deepweb, atualizações de correção, firewall, anti-vírus

Exemplos Práticos

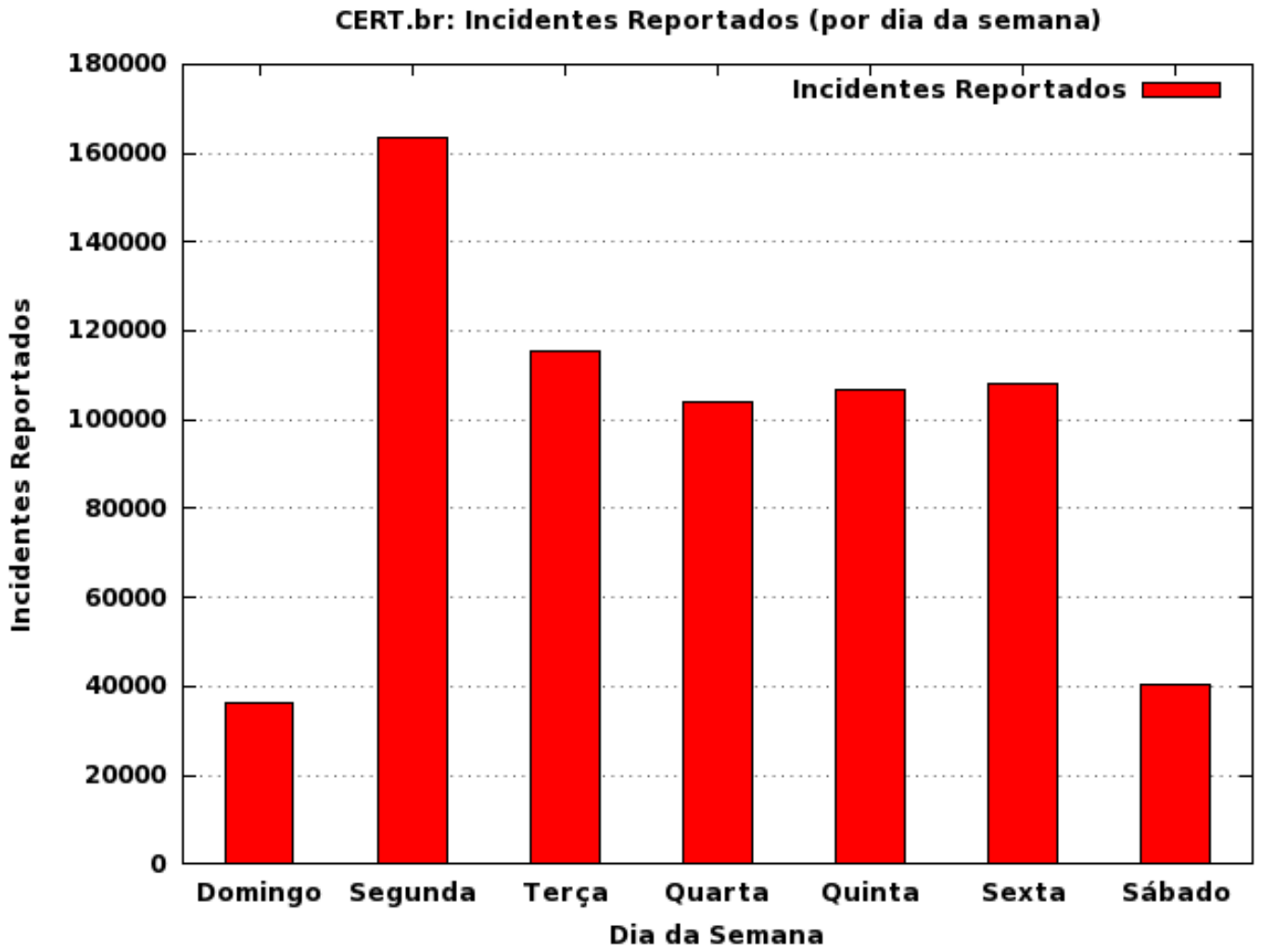
Hardware e Software são desenvolvidos em camadas

- Vulnerabilidades dentro de uma camada
- Vulnerabilidades entre uma camada e outra

Exemplo:

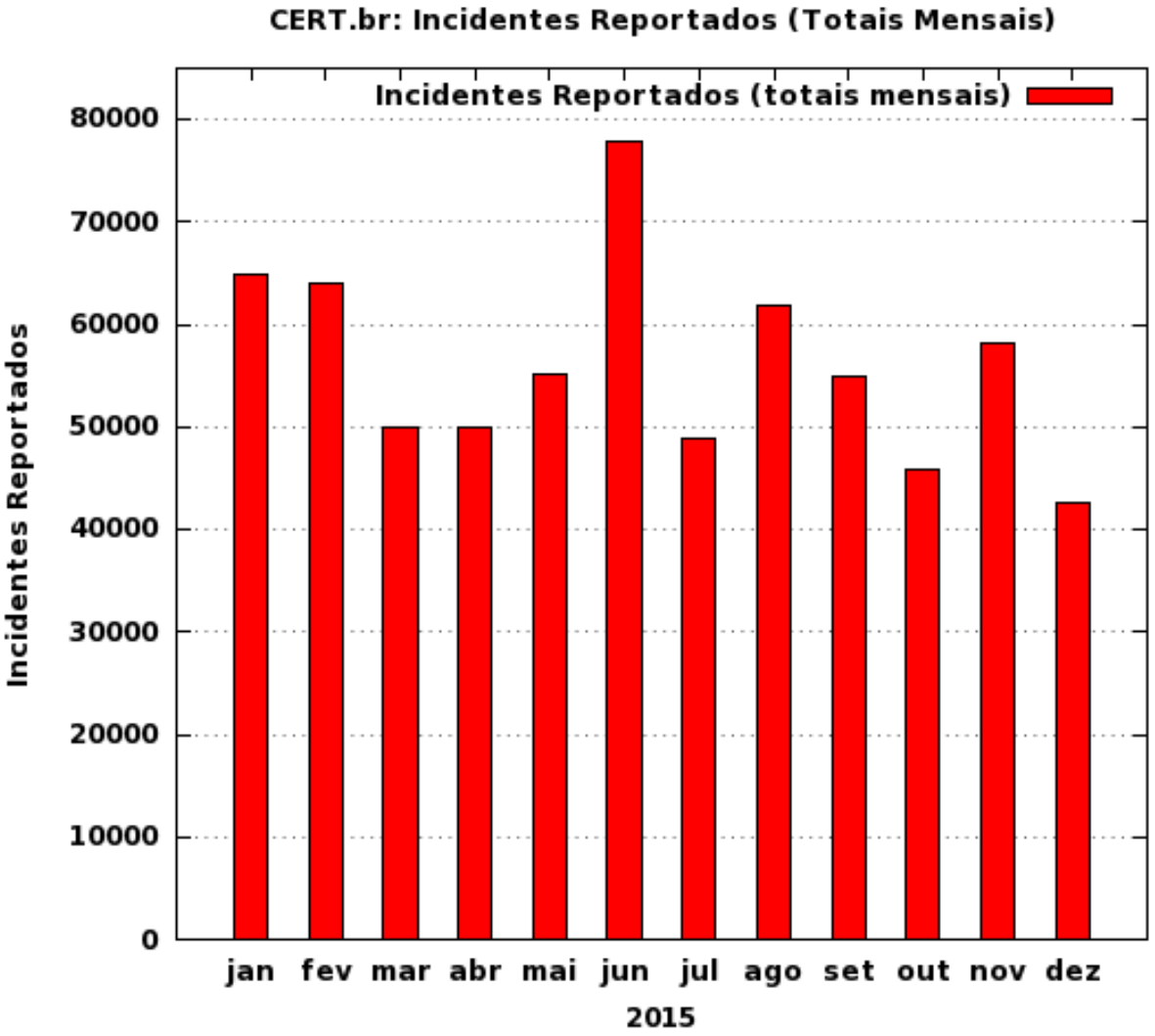
- Java - JVM
- Adobe - Flash Player
- Instaladores passo-a-passo - Toolbars

Estatísticas



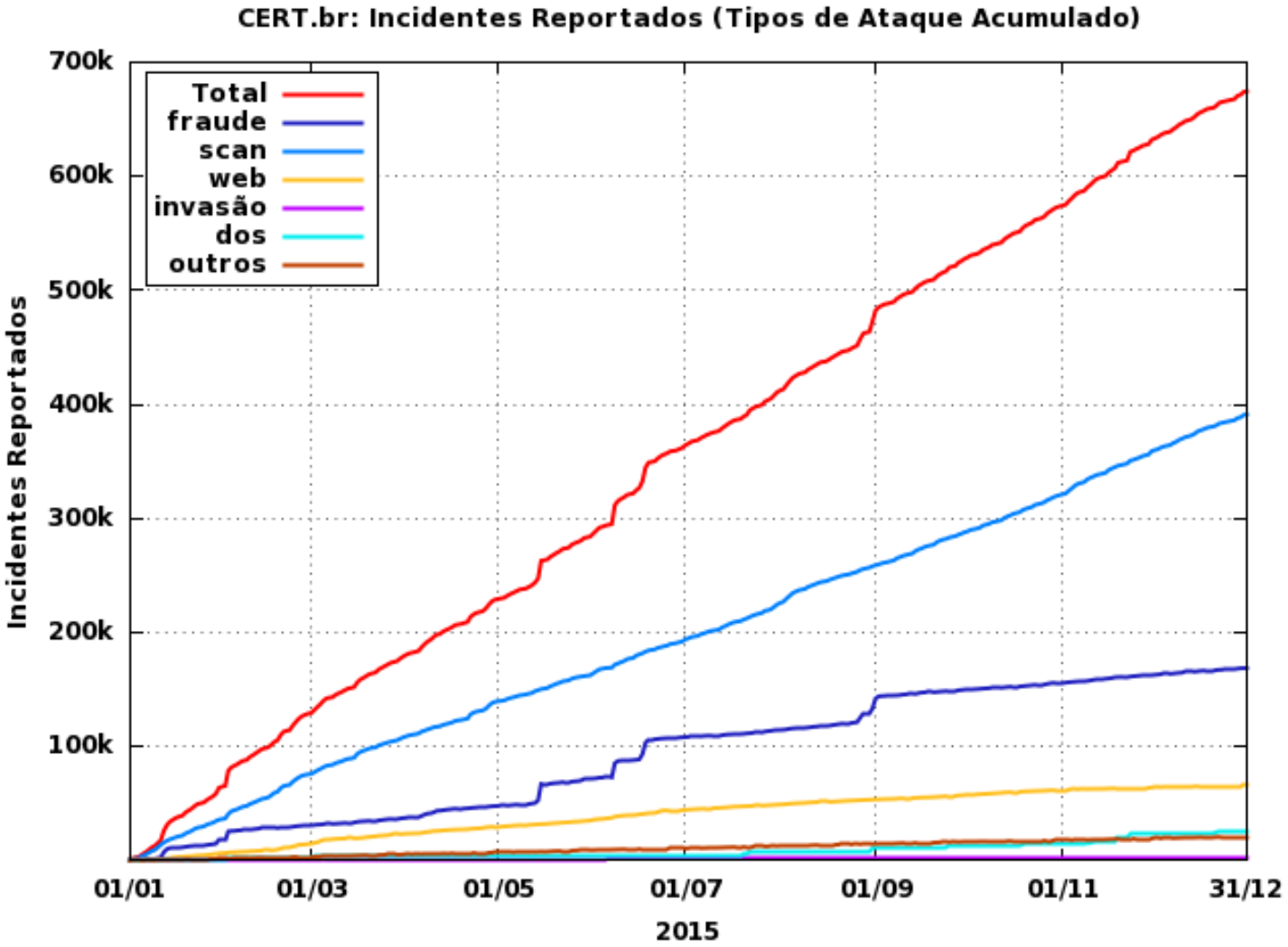
Disponível em: <http://www.cert.br/stats/incidentes/2015-jan-dec/weekdays-incidentes.html>

Estatísticas



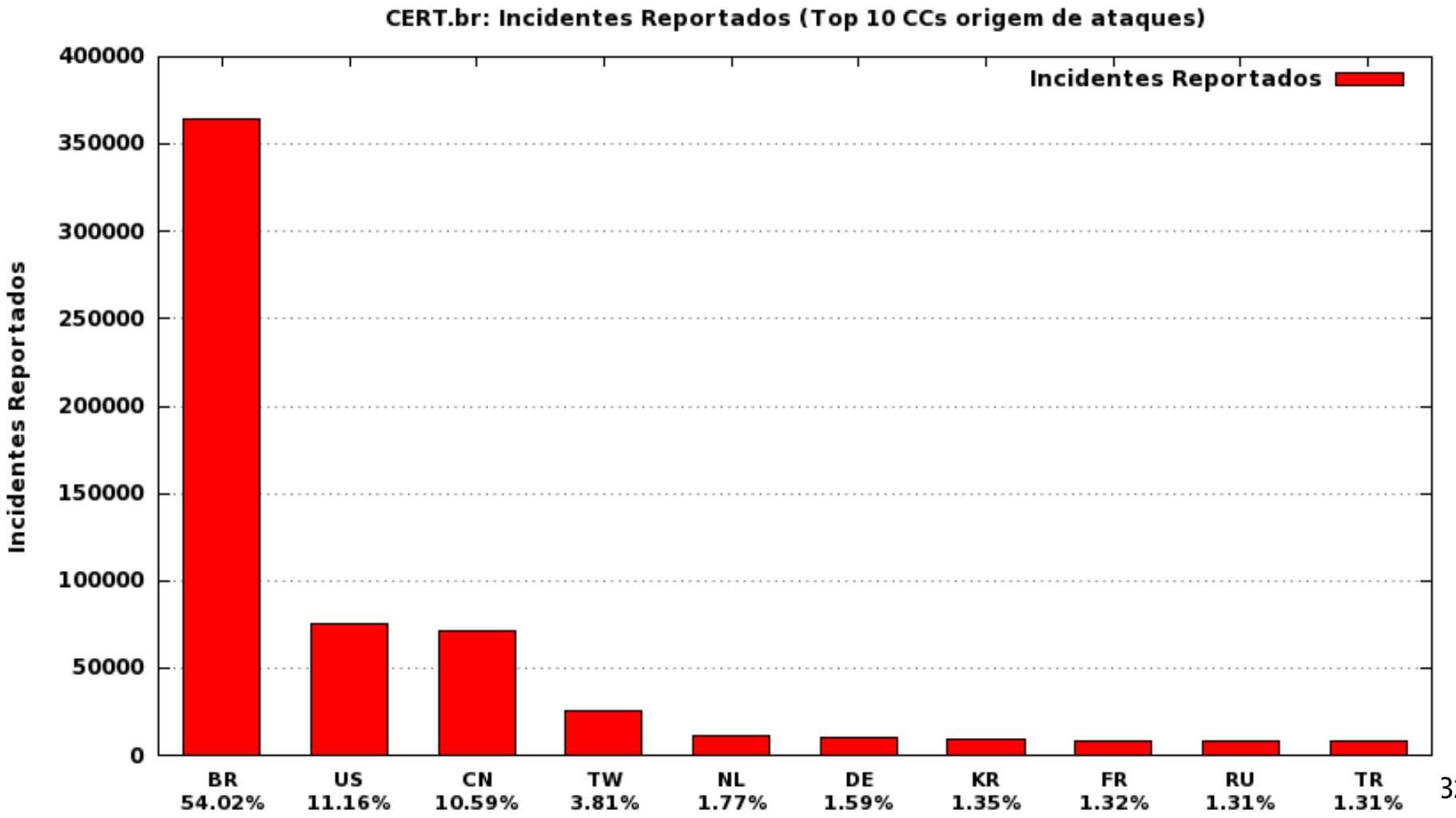
Disponível em: <http://www.cert.br/stats/incidentes/2015-jan-dec/ataques-mensal.html>

Estatísticas



Disponível em: <http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque-acumulado.html>

Estatísticas



Disponível em: <http://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.html>

Resumo

Hardware de entrada e saída

- Controladoras.

Software de entrada e saída

- Tratadores de interrupção, drivers, software de e/s independente, software de e/s do usuário.

Dispositivos de entrada e saída.

Controle de consumo de energia.

- Placa mãe – *timer.*

Thin clientes.

Resumo

Proteção

Segurança

- Ameaças,
- Perda de dados,
- Intrusos,
- Tipos de “inimigos”
- Ataques
- *Malwares*
- Casos práticos

Sistemas Operacionais

Prof. Me. Pietro M. de Oliveira