ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

P.PORTO

Sistemas Operativos

Licenciatura em Engenharia Informática

Licenciatura em Segurança Informática em Redes de Computadores

Princípios de Segurança em Sistemas Operativos

Agenda

- Objetivos de segurança em S.O.
- Proteção da Memória
- Modos CPU
- Chamadas ao sistema
- Conceitos básicos de controlo de acessos

Objetivos de segurança em S.O.

Que objetivos de segurança disponibiliza o Sistema Operativo?

- Originalmente: computadores com partilha de tempo: permite que vários utilizadores partilhem um computador com segurança
  - Há a separação e partilha de processos, memória, arquivos, dispositivos, etc.

Que objetivos de segurança disponibiliza o Sistema Operativo?

- O que é modelo de ameaça?
  - Os utilizadores podem ser mal-intencionados, os utilizadores têm acesso ao terminal aos computadores, o *software* pode ser mal-intencionado/com *bugs* e assim por diante

Que objetivos de segurança disponibiliza o Sistema Operativo?

- Proteção de memória
- Modos de processador
- Autenticação de utilizador
- Controlo de acesso a diretorias

Que objetivos de segurança disponibiliza o Sistema Operativo?

- Recentemente: computadores em rede, garantir uma operação segura em ambiente de rede

Que objetivos de segurança disponibiliza o Sistema Operativo?

- Uma nova ameaça?
  - Atacantes através da rede. Programas orientados para a rede em computadores podem apresentar erros. Os utilizadores podem ser prejudicados via comunicação *online*.

Que objetivos de segurança disponibiliza o Sistema Operativo?

- Mecanismos de segurança?
  - Autenticação; Controlo de acessos
  - Comunicação segura (usando criptografia)
  - Registo (logging) e auditoria
  - Prevenção e deteção de intrusões
  - Recuperação

Que objetivos de segurança disponibiliza o Sistema Operativo?

- Mais recentemente: dispositivos de computação móvel

Que objetivos de segurança disponibiliza o Sistema Operativo?

- Uma nova ameaça?
  - Aplicações (programas) podem ser maliciosos.
  - Mais intimamente ligado à vida pessoal do proprietário.

Que objetivos de segurança disponibiliza o Sistema Operativo?

- Mecanismos de segurança?
  - Isolamento de cada aplicação
  - Ajudar os utilizadores a avaliar os riscos dos aplicações
  - Comunicação do risco

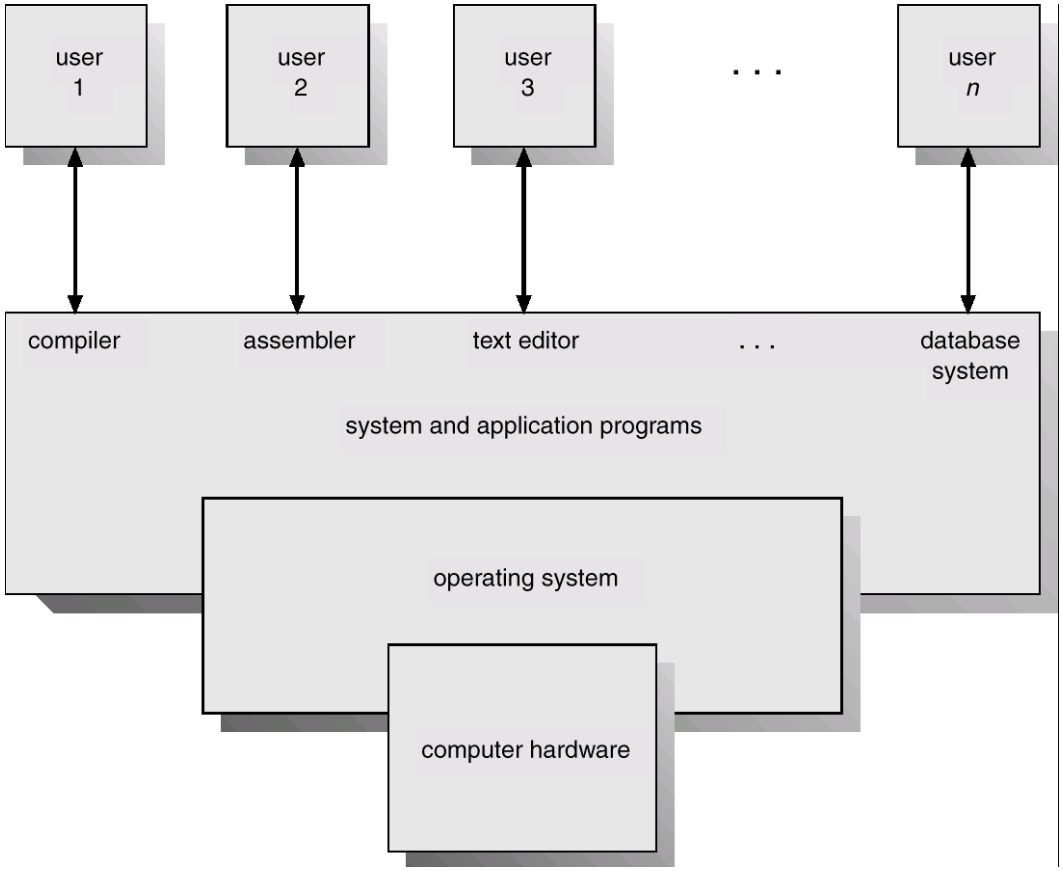
Segurança é um compromisso entre a separação e partilha

- Garanta a separação
  - Física
  - Temporal
  - Lógica
  - Criptográfica
- O sistema operativo também precisa garantir a partilha

Componentes de um sistema computacional

- *Hardware*
  - Fornece recursos básicos de computação (CPU, memória, dispositivos de E/S).
- Sistema Operativo
  - Controla e coordena o uso do *hardware* entre os diversos programas aplicativos.
- Programas aplicacionais
  - Definir as maneiras pelas quais os recursos do sistema são usados para resolver os problemas de computação dos utilizadores.
- Utilizadores
  - Por exemplo, pessoas, máquinas, outros computadores.

Vista abstrata dos componentes do sistema



Componentes de um sistema computacional

- *Hardware*
  - Fornece recursos básicos de computação (CPU, memória, dispositivos de E/S).
- Sistema Operativo
  - Controla e coordena o uso do *hardware* entre os diversos programas aplicativos.
- Programas aplicacionais
  - Definir as maneiras pelas quais os recursos do sistema são usados para resolver os problemas de computação dos utilizadores.
- Utilizadores
  - Por exemplo, pessoas, máquinas, outros computadores.

Proteção da memória

Controlo de acessos à memória

Proteção da memória

- Garante que o processo de um utilizador não possa aceder a memória de outro
  - cerca
  - realocação
  - registo base/limites
  - segmentação
  - paginação
  - …
- O sistema operativo e os processos do utilizador precisam de ter privilégios diferentes

Modos CPU

Modos de CPU (também conhecidos como modos de processador ou privilégios de CPU)

Modos de CPU

- Modo de sistema (modo privilegiado, modo mestre, modo supervisor, modo *kernel*)
  - Pode executar qualquer instrução
  - Pode aceder qualquer local de memória, por exemplo, aceder a dispositivos de *hardware*
  - Pode ativar e desativar interrupções
  - Pode alterar o estado privilegiado do processador
  - Pode aceder a unidades de gestão de memória
  - Pode modificar registos para diversas tabelas de descritores

Modo de Utilizador

- Modo de utilizador
  - O acesso à memória é limitado
  - Não é possível executar algumas instruções
  - Não é possível desabilitar interrupções
  - Não é possível alterar o estado arbitrário do processador
  - Não é possível aceder a unidades de gestão de memória
- A transição do modo de utilizador para o modo de sistema só pode acontecer através de pontos de entrada bem definidos, ou seja, através de chamadas de sistema

Chamadas ao sistema

Chamadas ao sistema

- Portões protegidos do modo de utilizador para o modo *kernel*
  - usa uma instrução especial do CPU (geralmente uma interrupção), transfere o controlo para um ponto de entrada predefinido em código mais privilegiado; permite que o código mais privilegiado especifique onde ele será inserido, bem como o estado importante do processador no momento da entrada.
  - o código com maior privilégio, examina o estado do processador definido pelo código menos privilegiado e/ou sua pilha (*stack*) e determina o que está sendo solicitado e se deve permitir isso.

Chamadas ao sistema

Espaço do *kernel* vs. Espaço do utilizador

- Parte do sistema operativo é executado no modo *kernel*
  - conhecido como o *kernel* do sistema operativo
- Outras partes do sistema operativo são executadas no modo de utilizador, incluindo programas de serviço (programas *daemon*), aplicações de utilizador, etc.
  - eles são executados como processos
  - eles formam o espaço do utilizador (ou o terreno do utilizador)
- Qual é a diferença entre o modo *kernel* e processos executados como *root* (ou superutilizador, administrador)?

Conceitos básicos de controlo de acessos

Controlo de acessos

A razão pela qual o controlo de acessos ajuda a proteger os sistemas operativos

- O controle de acesso ajuda a proteger os sistemas operativos, impedindo que os utilizadores não autorizados ou mal-intencionados acedam ou modifiquem recursos confidenciais ou críticos, como arquivos, processos, dispositivos ou redes
- Ao implementar um modelo de controlo de acesso apropriado, pode-se garantir que apenas os utilizadores que precisam aceder um recurso possam fazê-lo, e somente com as permissões necessárias. Dessa forma, é possível reduzir o risco de violações de dados, infeções por *malware*, falhas do sistema ou problemas de desempenho

Controlo de acessos

- **Controlo de acesso discricionário (DAC)** é um modelo de controlo de acesso em que o proprietário de um recurso pode decidir quem pode acedê-lo e com quais permissões.
  - Por exemplo, você pode criar um arquivo e atribuir permissões de leitura, gravação ou execução a si mesmo, a outros utilizadores ou grupos.

Controlo de acessos

- **Controlo de acesso obrigatório (MAC)**é um modelo de controlo de acesso onde o sistema impõe uma política predefinida com base nos rótulos de segurança dos recursos e dos utilizadores.
  - Por exemplo, pode-se classificar arquivos e utilizadores de acordo com seus níveis de sensibilidade e folga, e o sistema só permitirá o acesso se eles corresponderem. O MAC é mais seguro e consistente do que o DAC, mas também tem alguns desafios.

Controlo de acessos

- **Controlo de acesso baseado em função (RBAC)** é um modelo de controlo de acesso em que o sistema atribui permissões a funções e, em seguida, atribui as funções a utilizadores.
  - Por exemplo, pode-se criar funções como administrador, gestor ou funcionário e conceder a eles diferentes níveis de acesso a diferentes recursos. Em seguida, pode-se atribuir utilizadores a uma ou mais funções de acordo com suas funções e responsabilidades. O RBAC é mais escalável e sustentável do que o DAC ou o MAC, mas também tem algumas limitações.

Controlo de acessos

- **Controlo de acesso baseado em atributos (ABAC)** é um modelo de controle de acesso em que o sistema concede ou nega acesso com base nos atributos dos recursos, dos utilizadores e do ambiente.
  - Por exemplo, podem-se definir regras que permitam o acesso a um ficheiro somente se o utilizador estiver em um determinado local, em um determinado horário ou em um determinado dispositivo. O ABAC é mais flexível e dinâmico que o RBAC, mas também tem algumas desvantagens.

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

P.PORTO

Sistemas Operativos

Licenciatura em Engenharia Informática

Licenciatura em Segurança Informática em Redes de Computadores