Segurança Informática e nas Organizações

Resumos
2016/2017

João Alegria | 68661

Capítulo 9

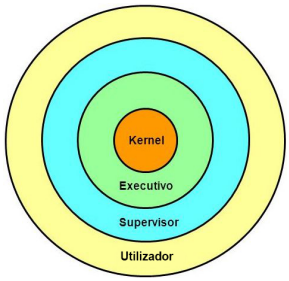
Segurança em Sistemas Operativos

Objetivos do Núcleo do SO

- Inicializar os dispositivos de hardware (*booting*)
- Visualizar o hardware, fornecendo uma interface para aplicações (Modelo Computacional)
- Aplicação das políticas de proteção e fornecimento de mecanismos de proteção, contra enganos involuntários e contra atividades não autorizadas
- Fornecer um sistema de ficheiros virtuais (VFS)

Modos de Execução

- Diferentes níveis de privilégio, em que normalmente são ilustrados por um conjunto de anéis concêntricos. São usados em CPU's para evitarem que aplicações não privilegiadas executem instruções privilegiadas, como por exemplo: IN/OUT
- Os processadores atuais têm 4 anéis, mas os SO's normalmente só usam 2, em que o 0 corresponde ao modo supervisor e o 3 ao modo de utilizador.
- A transferência de controlo entre anéis requer mecanismos de passagem especiais, os quais são usados pelas *system calls*.



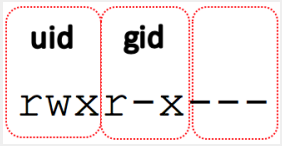
Modelo Computacional

Conjunto de entidades (objetos) geridos pelo núcleo do SO

Identificadores de Utilizadores	Identificadores de Grupos
- Para um sistema operativo, um utilizador é um número, estabelecido durante a operação de login -> userID (UID) - As atividades executadas num computador fazem-se sempre associadas a um UID, permitindo assim estabelecer o que é permitido ou negado às atividades. - Em Linux, o UID 0 é omnipotente (*root*) - A administração da máquina é feita recorrendo a atividades com UID 0 - Em Windows, existe o conceito de privilégios de administração - Não existe um UID único e bem estabelecido para um administrador - Privilégios de administração podem ser dados a diversos UIDs	- Um grupo é um conjunto de utilizadores - Um grupo (GID) pode ser definido à custa de outros grupos - Um utilizador pode pertencer a vários grupos - Os privilégios são determinados através do conjunto de privilégios atribuídos a si e aos grupos a que pertence *Direitos = Direitos UID + Direitos GID* - Em Linux, as atividades executadas são sempre associadas a um conjunto de grupos - **Grupo Primário** - usado para definir proteções de novos ficheiros - **Grupo Secundário** - usado juntamente com o anterior, para definir se tem ou não acesso a recursos

Processos	Memória Virtual
- Um processo contextualiza uma atividade para efeitos de decisões de segurança e para outros fins. - Contexto com relevância para a segurança - Identidade (UID e GID) - fundamental para efeitos de controlo de acesso do processo - Recursos actualmente em uso - ficheiros abertos (incluindo canais de comunicação); áreas de memória virtual reservada; tempo de CPU usado - Um processo pode alterar livremente o seu *effective UID* para *real UID*	- É um espaço de memória onde têm lugar ações efetuadas por uma atividade - Tem uma dimensão máxima que é definida pela arquitetura do hardware - 32 bits -> 2^{32} B (4GB) máximo - 64 bits -> 2^{64} B máximo - A memória virtual não precisa e não pode ser usada na integra, apenas é usada uma paralela - A memória virtual é mapeada em memória física (RAM) quando é necessário nela ler ou escrever - Num dado instante, a memória física possui partes de várias memórias virtuais - A escolha automática dessas partes é uma das funções mais importantes de um SO.
Ficheiros	**Sistemas de Ficheiros**
- Servem para armazenar dados de forma duradoura, sendo a longevidade dada pelo suporte físico e não pelo conceito de ficheiro - São sequências ordenadas de bytes associadas a um nome - O seu conteúdo pode ser alterado, removido ou acrescentado - Possuem uma proteção que controla o seu uso - Permissões de leitura, escrita, execução e remoção - O modelo de proteção depende do sistema de ficheiros - O direito de alterar o dono de um ficheiro está vedado (excepto se for *root*) - Porém é possível alterar o seu set-UID	- Estruturas hierárquicas de arrumação de ficheiros - São formados por diretorias (nós) e ficheiros (folhas) - A diretoria no topo é a raíz do sistema de ficheiros
Canais de Comunicação	**Proteção com ACLs**
- Permite a troca de dados entre atividades distintas mas cooperantes - Processos do mesmo SO/máquina (Socks UNIX, streams) - Processos em máquinas distintas (Sockets TCP/IP e UDP/IP)	- Lista de controlo de acessos (ACL) - cada “objeto” possui uma ACL (diz quem pode fazer o quê) - A ACL pode ser: - **discricionária** - quando pode ser alterado pelo dono do objeto - **obrigatória** - não se consegue alterar (é fixado pelo criador) - É verificada quando uma atividade pretende manipular o “objeto” - se o pedido de manipulação não estiver autorizado, é negado - quem faz as validações das ACL é o núcleo do SO (monitor de segurança)

Proteção de Ficheiros em Linux

ACLs de dimensão e estrutura fixa	Entidades
- Cada elemento do sistema de ficheiros possui uma ACL onde atribui 3 tipos de direitos a 3 entidades e onde apenas o dono do elemento pode mudar a ACL - Direitos: - R (read) ; W (write) ; X (execute) - Para ficheiros normais significa direito de: leitura; escrita; execução - Para as diretorias significam direito de: listagem; adição/remoção de ficheiros ou subdiretorios; uso como diretoria corrente do processo	- Um UID (dono do ficheiro) - Um GID (grupo associado ao ficheiro) - Os Demais 

Elevação de Privilégios

• ***Mecanismo Set-UID*** - Esta funcionalidade serve para fazer uma distribuição do UID do processo que executa um determinado programa.
  - Se um programa possuir o UIDx e o bit set-UID ativa na sua ACL, então ele será executado num processo com UIDx independentemente do UID de quem o mandar executar
  - Na prática, esta funcionalidade serve para disponibilizar programas que realizam operações privilegiadas a utentes em que não se confia
  - Resumindo: O set-UID é um mecanismo de elevação de privilégios que serve para que se possa dar permissão a terceiros para executar curtas operações

• ***Mecanismo SUDO*** - A administração pelo *root* não é adequada
  - Aproximação preferível a vários utilizadores que podem ser administradores temporários (usam o UID 0, temporariamente) e o comando sudo
  - Sudo é uma aplicação set-UID com UID = 0

Redução de Privilégios

• ***Mecanismo Chroot*** - Permite diminuir a visibilidade do sistema de ficheiros.
  - Menor visibilidade - menor risco de ver o que não interessa
  - Cada descritor do processo possui o *i-number* do *i-node* raiz, a partir da qual começa a resolução de nomes completos (nome/nome/nome/etc)
  - Chroot permite mudar esse número para referir o *i-node* de outra diretoria arbitrária
    - A vista do sistema de ficheiros de aplicações potencialmente perigosas
    - Servidores públicos, aplicações descarregadas
  - A manipulação da raíz do sistema de ficheiros por cada processo permite contextualizar políticas de privilégio mínimo

Real UID	***Effective UID***
Identifica o verdadeiro dono do processo e afeta as permissões para o envio de sinais. Um processo sem privilégio de super utilizador pode sinalizar outro processo apenas se UID real do remetente corresponde com o UID real do receptor. Como os processos filho herdam as credenciais do pai, eles podem sinalizar um ao outro.	Afeta a criação e o acesso de ficheiros. Durante a criação do ficheiro, o kernel define os atributos do proprietário do ficheiro para o UID efetivo e o GID efetivo do processo de criação. Durante o acesso ao ficheiro, o kernel usa o UID efetivo e o GID efetivo do processo para determinar se ele pode aceder o ficheiro.