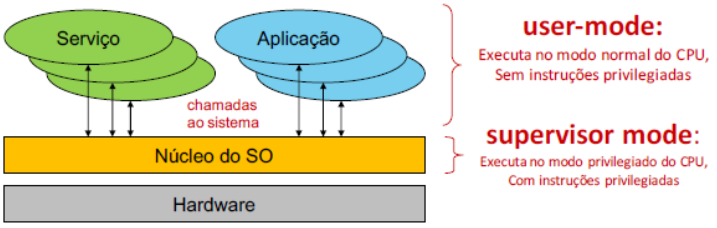
Capítulo 9 – Segurança em Sistemas Operativos

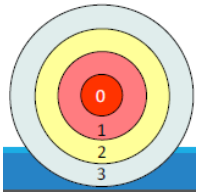


Objetivos do Núcleo do SO

- 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 virtual (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.



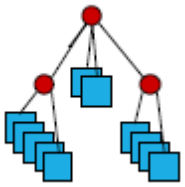
Execução em Máquinas Virtuais

Aproximação Típica	Virtualização assistida por Hardware
- Virtualização baseada em software - Execução direta de código em modo de utilizador (anel 3) -Tradução binária de código priveligiado(anel 0)	- Virtualização completa (Full) - Utiliza-se anel-1, abaixo do anel 0 - Virtualizador consegue executar vários SO's em nível 0, sem necessidade de tradução binária e com performance proxima da nativa.

Modelo Computacional

Conjunto de entidades (objetos) geridos pelo núcleo do SO

Identificadores de utilizadores	Identificadores de Grupos
- Para um SO um utilizador é um número estabelecido durante a operação de login. USER ID (UID) - As actividades executadas num computador fazem-se sempre associadas a um UID, onde este permite estabelecer o que é permitido/negado às atividades. Em linux o UID 0 é omnipotente (root), onde a administração da máquina é normalmente feita recorrendo a atividadea com o UID 0. Em Windows existe o conceito de privilégrios de administração, de configuração do sistemas, entre outros. Não existe um identificador único e bem estabelecido para o administrador. Os privilégios de administração podem ser dados a diversos UIDs.	- Existem identificadores de grupo, onde um grupo é um conjunto de utilizadores e um grupo pode ser definido à custa de outros grupos. GROUP ID (GID). - Um utilizador pode pertencer a diversos grupos, onde os seus privilégios são determinados atraves do conjunto de privilegios atribuidos a si e aos grupos a que pertence. Direitos = Direitos UID + Direitos GIDs - Em Linux as atividades executadas fazem-se sempre associadas a um conjunto de grupos: ♦ Grupo primário, normalmente usado para definir proteções de novos ficheiros. ♦ Grupos secundários, usados, juntamente com o anterior, para definir se tem ou não acesso a recursos.

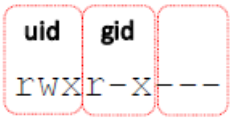
<table>
<tr><th>Processos</th><th>Memória Virtual</th></tr>
<tr><td>- Um processo contextualiza uma atividade para efeitos de decisões de segurança e para outros fins.
- Contexto com relevancia para a segurança:
♦ Indentidade (UID e GIDs), fundamental para efeitos de controlo de acesso do processo
♦ Recursos atualmente de uso, em ficheirs abertos incluindo canais de comunicação, areas de memoria virtual reservadas e tempo de CPU usado</td><td>- É um espaço de memoria onde têm lugar ações efetuadas por uma atividade, com uma dimensão maxima que é definida pela arquitetura de hardware.
- A memoria virtual não precisa de ser usada na integra, apenas é usada uma parcela necessária.
- A memoria virtual é mapeada em memória fisica (RAM) quando é necessário nela ler ou escrever. Num dados instante, a memoria fisica possui partes de varias memorias virtuais. A escolha automatica dessas partes é uma das funções mais importantes de um SO.</td></tr>
<tr><th colspan="2">Ficheiros e sistemas de ficheiros</th></tr>
<tr><td>Ficheiros</td><td>Sistemas de ficheiros</td></tr>
<tr><td>- Servem para armazenar dados de forma permanente, mas a longevidade é dada pelo suporte fisico e não pelo conceito de ficheiro.
- São sequencias ordenadas de bytes associadas a um nome. O nome permite recuperar/reutilizar esses bytes mais tarde
- O seu conteudo pode ser alterado, removido, ou acrescentado.
- Possuem uma proteção que controla o seu uso, como permissoes de leitura, escrita, execução, remoção. O modelo de proteção depende do sistema de ficheiros.</td><td>- São estruturas hierarquicas de arrumação de ficheiros.
- São formados por diretorias (nós) e ficheiros (folhas)
- As diretorias também possuem nome
- A diretoria no topo é a raiz do sistema de ficheiros.
  </td></tr>
<tr><th colspan="2">Canais de comunicação</th></tr>
<tr><td colspan="2">- Permitem a troca de datos entre entidade distintas mas cooperantes como processos do mesmo So/máquina (pipes, Spckets UNIX, streams) e processos em máquinas distintas (Sockets TCP/IP e UDP/IP).
- Mecanimos essencial para operação de um sistema.</td></tr>
<tr><th colspan="2">Dispositivos fisicos</th></tr>
<tr><td colspan="2">- Suportes de armazenamento (discos magnéticos, oticos, de memória, cassetes)
- Interfaces de rede com cabo e sem fio
- Interface Humano-Computador, como teclados, ecrãs, ratos.
- Interface I/O série/paralelo, como barramentos USB, portas série, portas paralelas, infravermelhos.</td></tr>
<tr><th colspan="2">Proteção com ACLs</th></tr>
<tr><td colspan="2">- Lista de controlo de acesso (Access Control List, ACL), onde cada “objeto” possui uma ACL, onde diz quem pode fazer o quê e a entidade tem o direito de operação.
- A ACL pode ser discriminatória quando pode ser alteradas pelo dono do objeto ou obrigatória (mandatory) quando não consegue contornar é ficada pelo seu 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 ACLs é o núcleo do SO, monitor de segurança.</td></tr>
<tr><th colspan="2">Controlo de acesso obrigatório</th></tr>
<tr><td colspan="2">Existem inúmeros casos de controlo de acesso mandatório num sistema operativo. São mecanismos de controlo embebidos na própria lógica do modelo computacional do sistema operativo e que não são moldáveis pelos utentes e administradores.

- Exemplo: envio de sinais entre processos UNIX, onde apenas o root ou mesmo o UID o pode fazer. Não há qualquer controlo sobre esta funcionalidade</td></tr>
</table>

Proteção de ficheiros no Linux:

ACLs de dimensão e estrutura fixa

- 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 W X
  - Para ficheiros normais significa direito de: leitura, escrita e execução
  - Para as diretorias significam direito de: listagem, adição/remoção de ficheiros ou subdiretorias e uso como diretoria corrente do processo
- Entidades
  - Um UID (dono do ficheiro)
  - Um GID (grupo associado ao ficheiro)



ACLs flexíveis

- ACL Básica pode ser aumentada com restrições granulares por grupo ou utilizador. Necessita de suporte do sistema de ficheiros. Sobrepõem-se às ACLs do sistema, onde a presença de ACLs adicionais é indicada com o símbolo +.
- *setfacl*: permite adicionar ACLs, como por exemplo: setacl –m u:www-data:rx fich, define que o user www-data poderá ler e executar um ficheiro
- *getfacl*: permite obter as ACLs de um ficheiro, como por exemplo: getfacl fich

Proteção de ficheiros no NTFS do Windows: ACLs de dimensão variável

Cada elemento do sistema de ficheiros possui uma ACL e um dono. A ACL atribui 14 tipos de direitos a uma lista de entidade. O dono pode ser um utilizador singular ou um grupo. O dono não possui direitos especiais por esse facto.

-Entidades:

- Utilizadores singulares
- Grupos de utilizadores, onde há um grupo, "Everyone", que representa os "demais".

Elevação de Privilégios

Mecanismo Set-UID	Mecanismo Sudo	Mecanismo Chroot
Esta funcionalidade serve para fazer uma alteração do UID do processo que executa um determinado programa. Se um programa possuir o UID X e o bit set-UID ativo na sua ACL, então ele será executado num processo com UID X independentemente do UID de quem o mandar executar. Na praticam esta funcionalidade serve para disponibilizar programas que realizam operações privilegiadas a utentes em quem não se confia. Exemplo: alteração da senha do utente no ficheiro que guarda as senhas.	A administração pelo root não é adequada. Aproximação preferível a vários utilizadores que podem ser administradores temporários (usam temporariamente o UID 0) e sudo comando. **Sudo** é uma aplicação Set-UID com UID = 0, um registo adequado pode ser realizado por cada comando executado via sudo.	- Permite diminuir a visibilidade do sistema de ficheiros (menor visibilidade, menor risco de ver o que não interessa). - cada descritor de processo possui o i-number do i-node raiz, a partir do qual começa a resolução de nomes completos (/nome/nome/etc). - Chroot permite mudar esse número para referir o i-node de outra diretoria arbitrária. A vista do sistema de ficheiros do processo fica reduzida ao que existe abaixo dessa diretoria. - É usado para proteger o sistema de ficheiros de aplicações potencialmente perigosas, como por exemplo: servidores públicos, aplicações descarregadas.