Capítulo 9 - Segurança

EMERSON DOS SANTOS - 2018014304
GIOVANY DA SILVA SANTOS - 2018007758
IVAN LEONI VILAS BOAS - 2018009073
JOÃO PEDRO JOSUÉ - 2018011044

- COM120 - Sistemas Operacionais

Introdução

- O valor da Informação
- Globalização da Internet
- Vulnerabilidade
- Exploração Manual ou Automática

Ambiente de Segurança

- Segurança X Proteção

Ambiente de Segurança - Ameaças

- Segurança pode ser decomposta em:

Objetivo	Ameaça
Confidencialidade de Dados	Exposição de Dados
Integridade de Dados	Adulteração de Dados
Disponibilidade do Sistema	Recusa de Serviço

Ambiente de Segurança - Ameaças

- Ferramentas usadas tanto por atacantes quanto defensores

Ambiente de Segurança - Atacantes

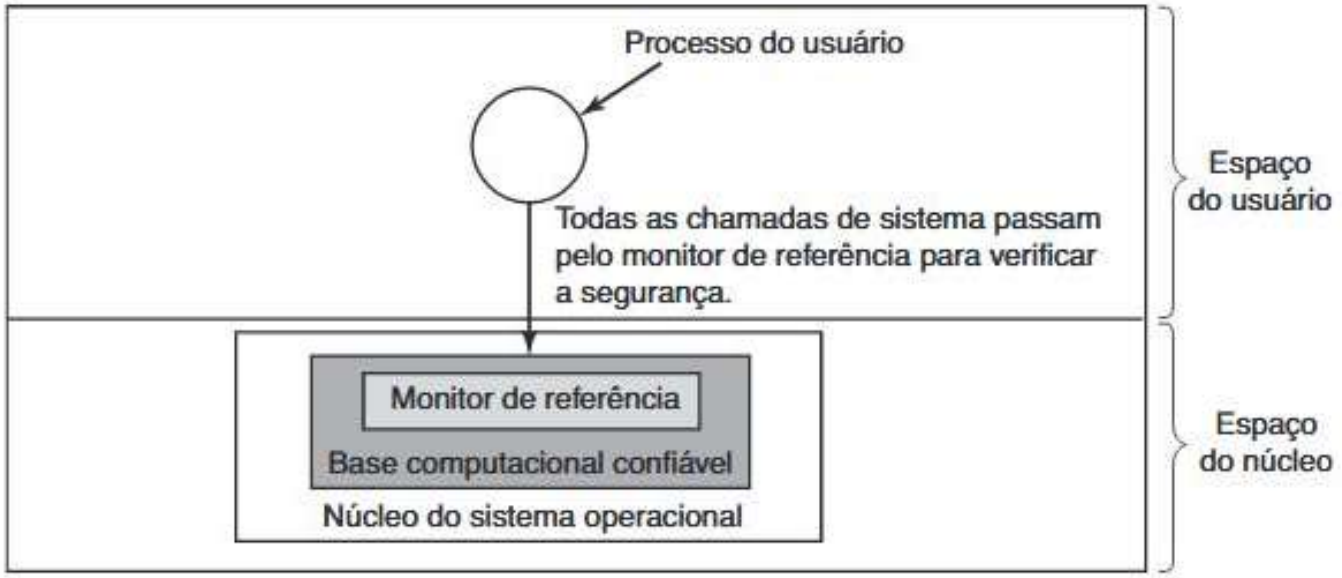
- Motivos para uma invasão

Segurança de sistemas operacionais

- Segurança
- Ataques
- Ataque passivo x Ataque ativo
- Endurecimento X Criptografia

Base computacional confiável-Imagem

Um monitor de referência.



Segurança de sistemas operacionais -Temos condições de construir sistemas seguros?

É possível construir um Sistema computacional seguro?

- Razões para insegurança dos sistemas
  - ⇨ Usuários
  - ⇨ Necessidade de Simplicidade das funcionalidades

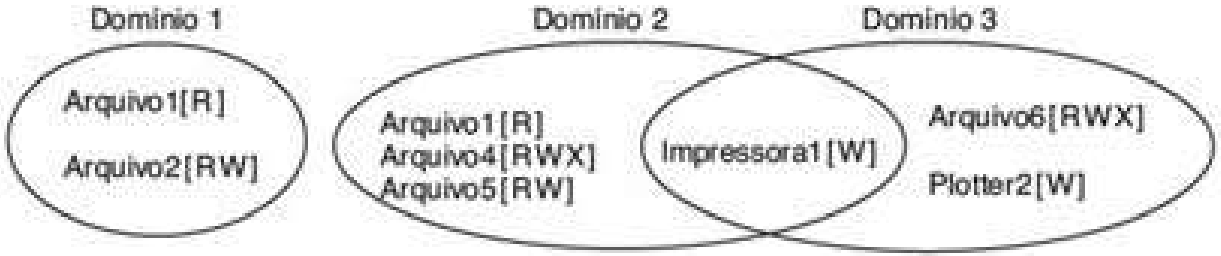
Segurança de sistemas operacionais-Base computacional confiável

- Sistemas confiáveis
- TCB(Trusted Computing Base — Base Computacional Confiável)
- Monitor de referência

Controlando o acesso aos recursos

- O que deve ser protegido, e quem pode fazer o que (Domínio e Direito)

FIGURA 9.3 Três domínios de proteção.



Examinando o Unix

- Domínio do processo definido por UID e GID
- Chamadas de sistema podem mudar o domínio
- SETUID ou SETGID

Como o sistema controla quais objetos pertencem a qual domínio?

FIGURA 9.4 Uma matriz de proteção.

	Objeto							
	Arquivo1	Arquivo2	Arquivo3	Arquivo4	Arquivo5	Arquivo6	Impressora1	Plotter2
Domínio 1	Leitura	Leitura Escrita						
2			Leitura	Leitura Escrita Execução	Leitura Escrita		Escrita	
3						Leitura Escrita Execução	Escrita	Escrita

Lista de Controle Por Acesso

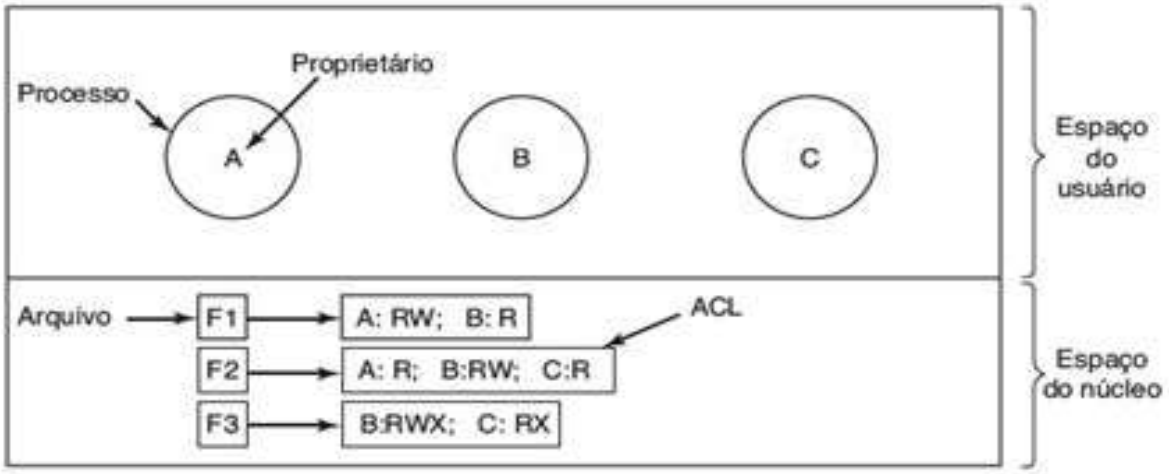
- Problemas da Matriz de proteção

- Solução: Armazenar por colunas ou linhas

Armazenar por Colunas

ACL - access control list

FIGURA 9.6 Uso de listas de controle de acesso para gerenciar o acesso a arquivos.



ACL - Grupos - GID

Possuem Duas semânticas. Sendo a primeira:

FIGURA 9.7 Duas listas de controle de acesso.

Arquivo	Lista de controle de acesso
Senha	tana, sysadm: RW
Dados_pombos	bill, fanpombo: RW; tana, fanpombo: RW; ...

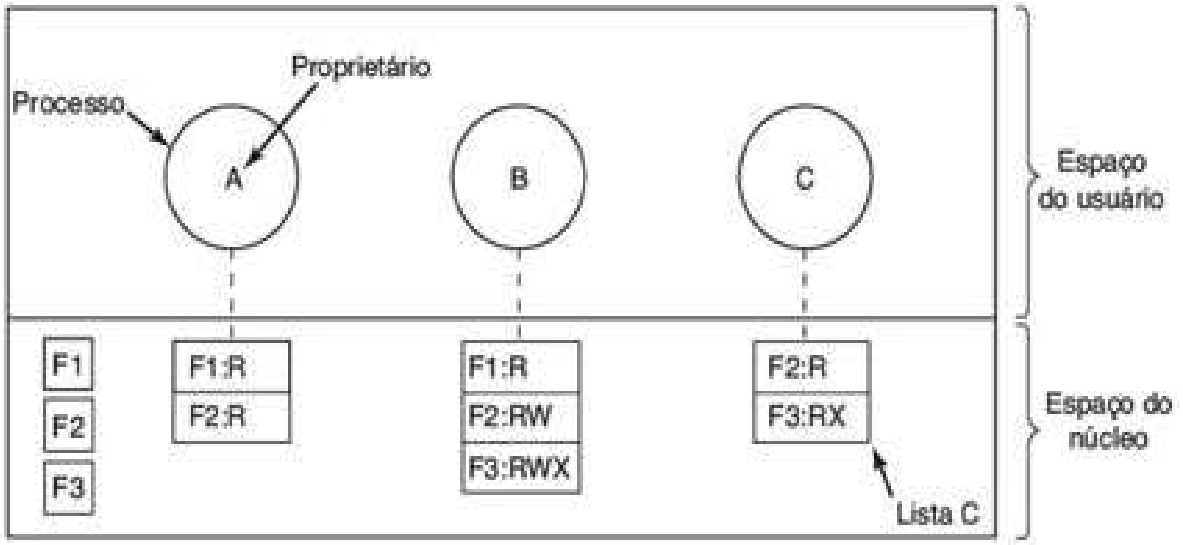
Segunda Semântica

Cada entrada tem apenas UID ou um GIG.

- Ex: debbie: RW; fapombo: RW

Capacidade - Armazenar por Colunas

FIGURA 9.8 Quando as capacidades são usadas, cada processo tem uma lista de capacidades.



Listas de Capacidade

Devem ser protegidas dos usuários: 3 métodos de proteção.

- Arquitetura Marcada
- Manter lista c Dentro do SO
- Manter lista c no espaço do Usuário

ACL e Capacidade

Se Complementam

ACL :  UNIX

Capacidade :   FreeBSD

Perguntas?