U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

[dcc]

CONTROLO DE ACESSO

ADMINISTRAÇÃO DE SISTEMAS

2022/2023

ROLANDO MARTINS

(ADAPTADOS DE PEDRO BRANDÃO)

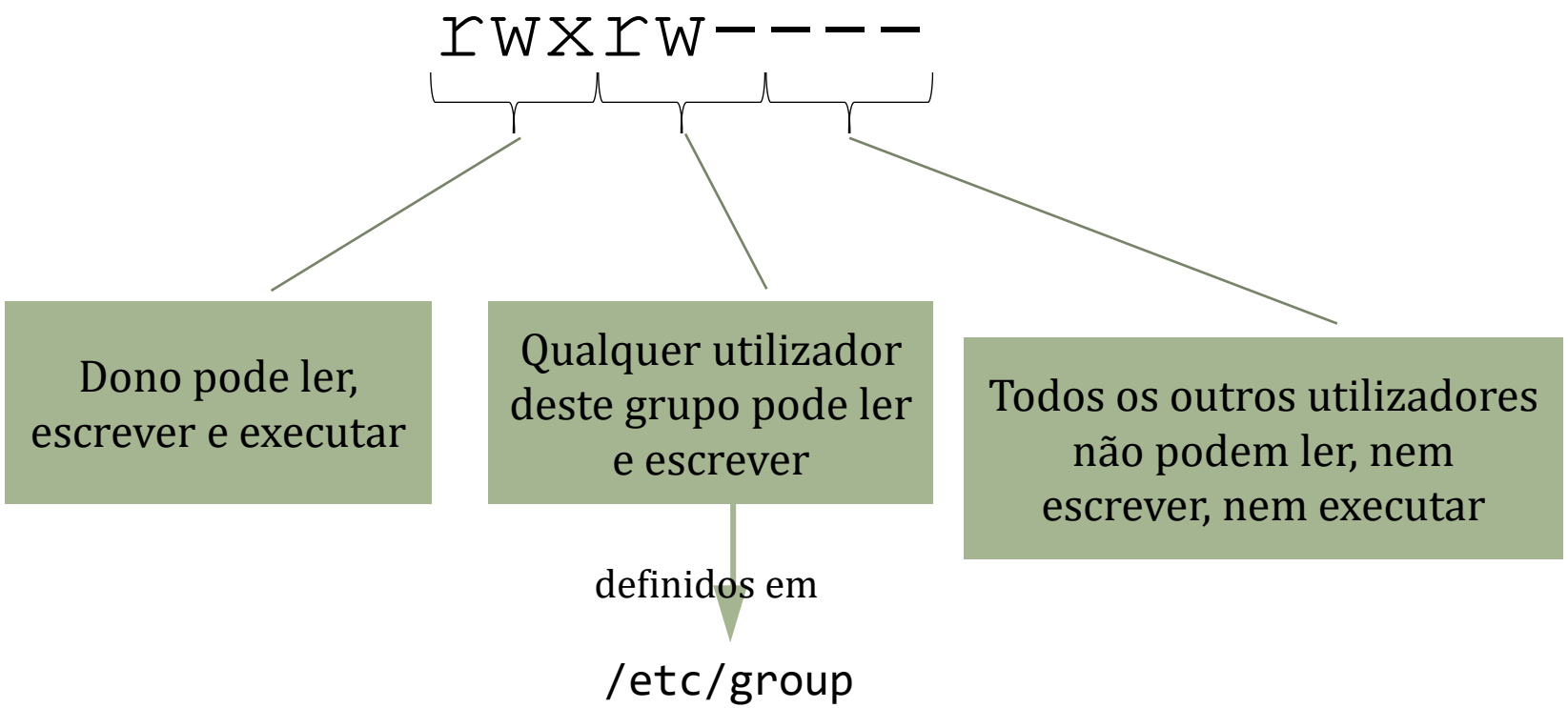
Referências dos slides

- O conteúdo destes slides é baseado no livro da disciplina: “Unix and Linux System Administration Handbook (4ªEd)” por Evi Nemeth, Garth Snyder, Trent R. Hein e Ben Whaley, Prentice Hall, ISBN: 0-13-148005-7
- As imagens usadas têm a atribuição aos autores ou são de uso livre.

Elementos do controlo de acesso

- Sujeito – entidade que pode aceder a objetos
  - Um processo
  - Em geral mapeado em 3 classes: dono, grupo e todos
- Objeto – recurso a que se controla o acesso
  - Ex.: ficheiros, diretórios, registos, programas
  - Número/tipo depende do ambiente
- Direito de acesso – modo como o sujeito acede ao objeto
  - Ex.: ler, escrever, executar, apagar, criar, procurar

Controlo de acesso a ficheiros em UNIX



Exemplo de ficheiros

```
aix$ ls -l /home/garth/todo
-rw------- 1 garth staff 1258 Jun 4 18:15 /home/garth/todo
```

- Username ➔ UID: `/etc/passwd`

```
aix$ ls -n /home/garth/todo
-rw------- 1 1001 1201 1258 Jun 4 18:15 /home/garth/todo
```

- Grupos e membros: `/etc/group`

Mas mesmo após execução…

- Existe outro controlo após execução. Ex.:
  - `kill` (enviar sinais a outros processos sem ser os da root)
    - Noção de dono do processo (quem o executou)
  - `timedatectl` (mudar o relógio do sistema)

ROOT POWER

root account

- Utilizador de admin em Linux, superuser (su), UID: `0`
- Exemplos de operações restritas ao UID `0`
  - `chroot`, mudar o diretório raiz de um processo
  - Criar ficheiros de dispositivos
  - Acertar o relógio
  - Prioridades de processos (`nice` e `renice`)
  - Mudar limites de utilização de recursos
  - Nome do Sistema (`hostname`)
  - Configurar interfaces de redes
  - Abrir portas privilegiadas (abaixo de 1024)

setuid, setgid

- Como funciona o comando `passwd`?
  - Permite mudar a palavra passe de um utilizador.
  - Mas esta, está no `/etc/shadow`, que não tem sequer permissões de leitura para os utilizadores
- `passwd` tem o bit setuid a 1
  - Permite elevar os privilégios para os do dono do ficheiro (root)

```
$ ls -l `which passwd`
-rwsr-xr-x. 1 root root 27768 `Feb 11  2017 /usr/bin/passwd
```

Problemas com sist. de controlo de acesso

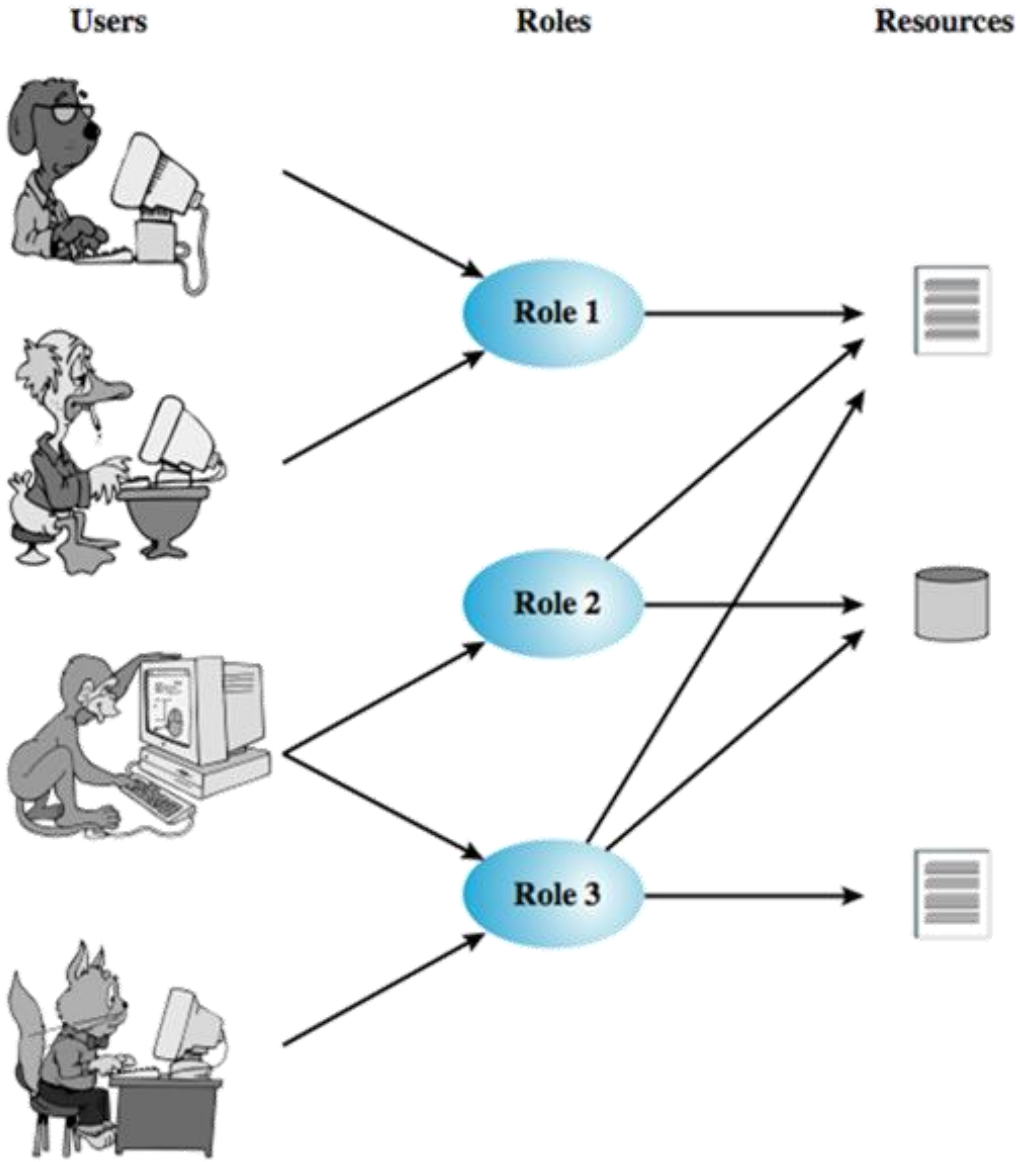
- root: ponto singular de falha
- Sub-divisão de privilégios com programas setuid
  - Dificuldade de os tornar seguros
- Controlo de acesso embebido nos programas
  - Mudar implica recompilar
- Utilizadores com acesso físico à máquina tornam-na insegura na rede onde está
- Multi-Level-Security (MLS) não é possível sem extras
- Pouco suporte para auditoria

Extensões para controlo de acesso

- RBAC (Role Based Access Control)
- SELinux (Security Enhanced Linux)
- PAM (Pluggable Authentication Modules)
- POSIX capabilities
- Kerberos (e hoje em dia Oauth 2)
- ACLs (Access Controlo Lists)

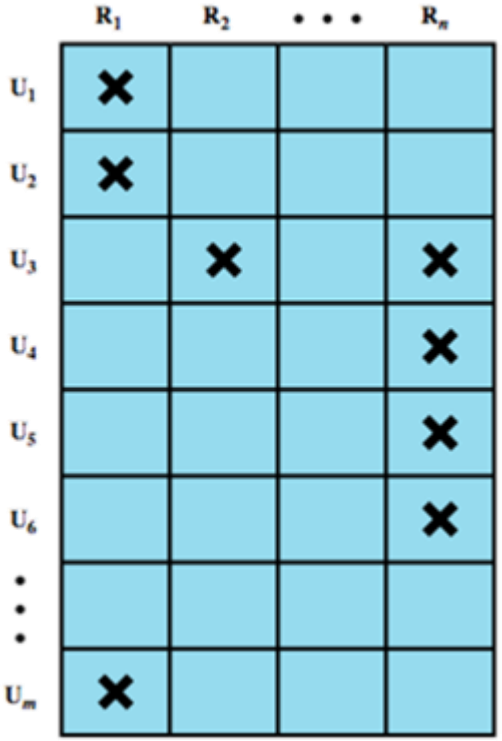
ROLE-BASED ACCESS CONTROL

From Dr Lawrie Brown (UNSW@ADFA) for "Computer Security: Principles and Practice", 1/e, by William Stallings and Lawrie Brown



ROLE-BASED ACCESS CONTROL

From Dr Lawrie Brown (UNSW@ADFA) for "Computer Security: Principles and Practice", 1/e, by William Stallings and Lawrie Brown

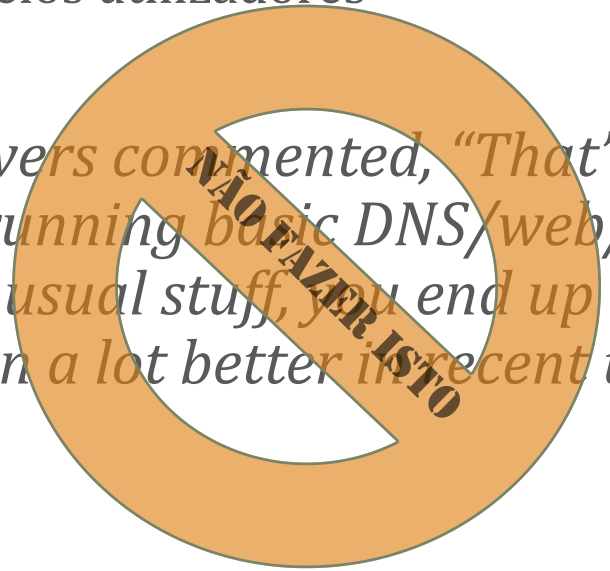


OBJECTS

ROLES	R1	R2	Rn	F1	F1	P1	P2	D1	D2
R1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R2		control		write *	execute			owner	seek *
Rn			control		write	stop			

SELinux

- Projeto da NSA, disponível e integrado no kernel (desde 2.6)
- Mandatory Access control, MAC (ou contrário de DAC)
  - Não há delegação de privilégios
- Controlo "compilado" em regras
- Política de acesso definida no sistema
  - vs. permissões regidas pelos utilizadores



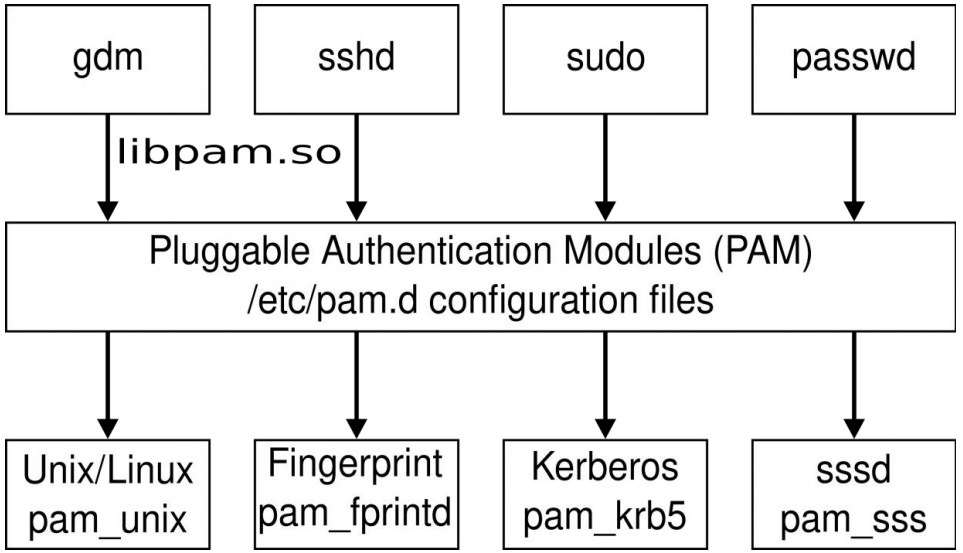
One of our technical reviewers commented, "That's certainly not the intent. In fact, it's the average sites running basic DNS/web/email service that do best with SELinux. If you're doing unusual stuff, you end up in policy hell and turn it off. SELinux has actually gotten a lot better in recent times. Of course, I still turn it off…"

SELinux II

- **Type Enforcement (TE):** Type Enforcement is the primary mechanism of access control used in the **targeted** policy
- **Role-Based Access Control (RBAC):** Based around SELinux users (not necessarily the same as the Linux user), but not used in the default configuration of the **targeted** policy
- **Multi-Level Security (MLS):** Not commonly used and often hidden in the default **targeted** policy.
- **Multi-Category Security(MCS):** An extension of Multi-Level Security, used in the **targeted** policy to implement compartmentalization of virtual machines and containers through

PAM (Pluggable **Authentication** Modules)

- Sistema Modular de autenticação
  - O utilizador fornece o seu user name e password que podem ser guardadas localmente ou num remotamente, e.g. LDAP ou Kerberos



Matriz de acesso

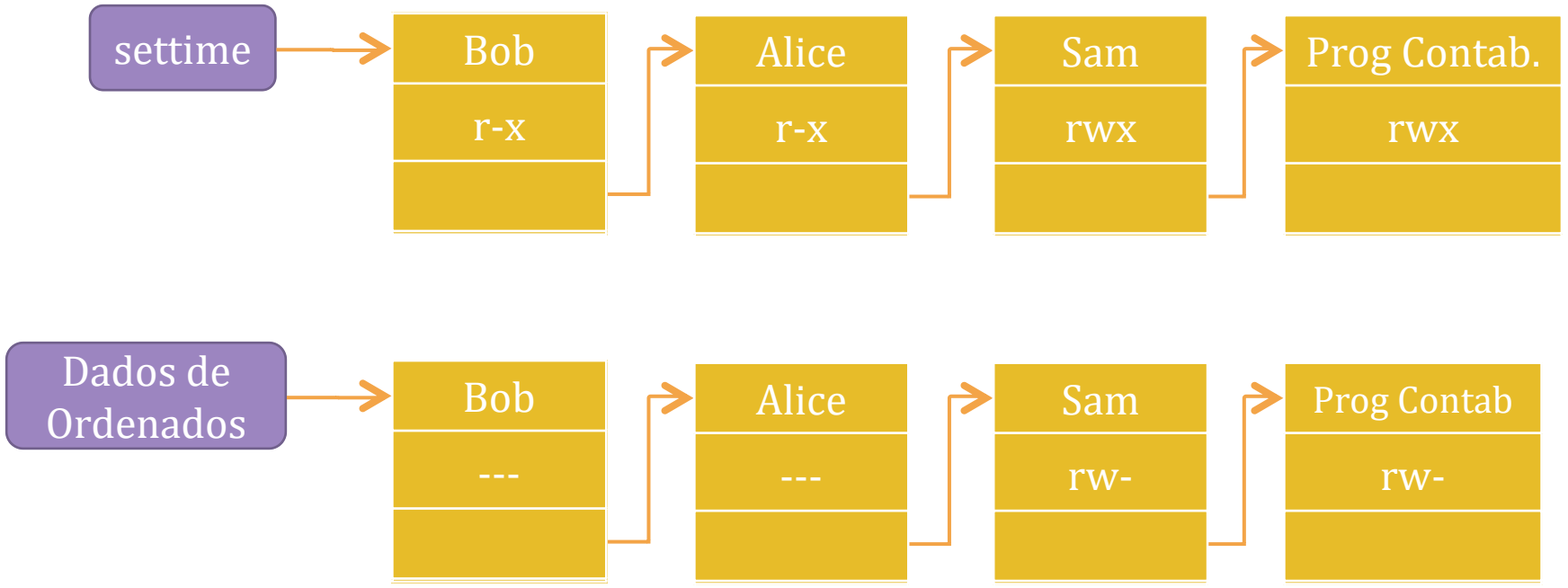
Qual o problema com esta aproximação?

	Bob	Alice	Sam	Prog. Contab
settime	r-x	r-x	rwx	rwx
Dados de ordenados	---	---	rw-	rw-
Prog. Contab.	---	r-x	r-x	n.a.

From Dr Lawrie Brown (UNSW@ADFA) for "Computer Security: Principles and Practice", 1/e, by William Stallings and Lawrie Brown

Access Control Lists

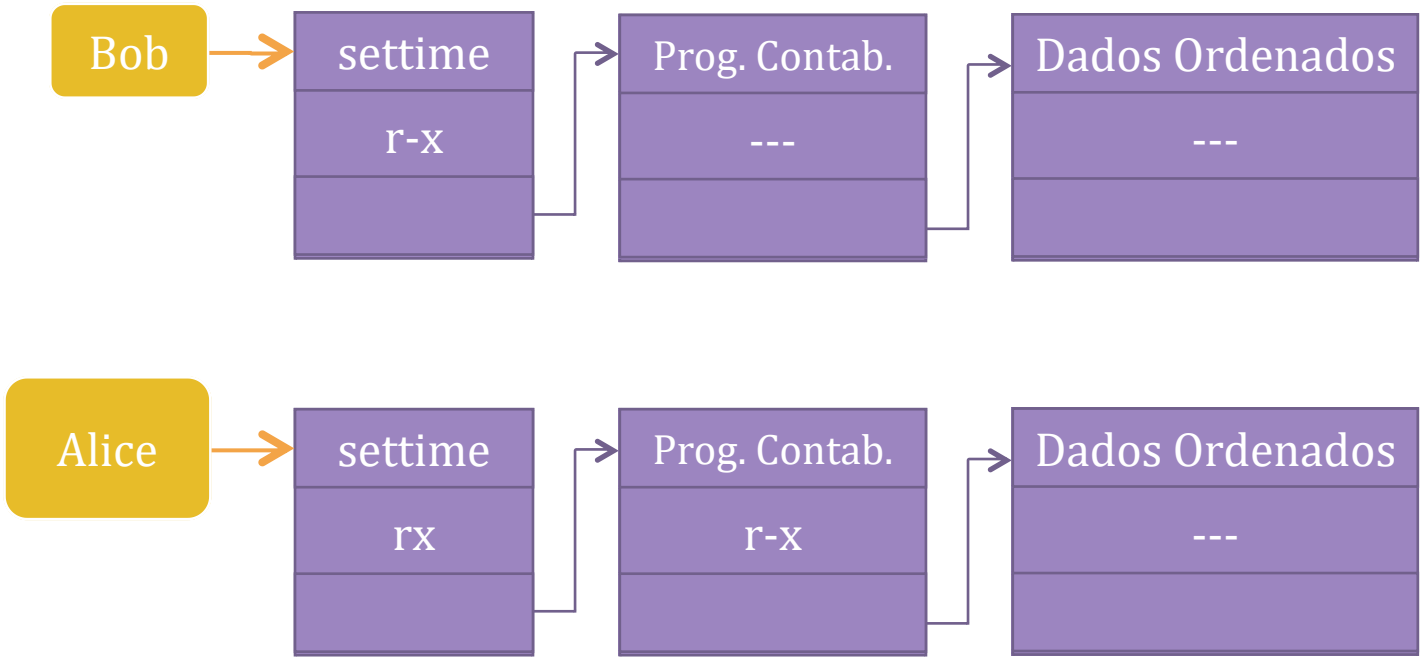
- Controlo de acesso por recurso



From Dr Lawrie Brown (UNSW@ADFA) for "Computer Security: Principles and Practice", 1/e, by William Stallings and Lawrie Brown

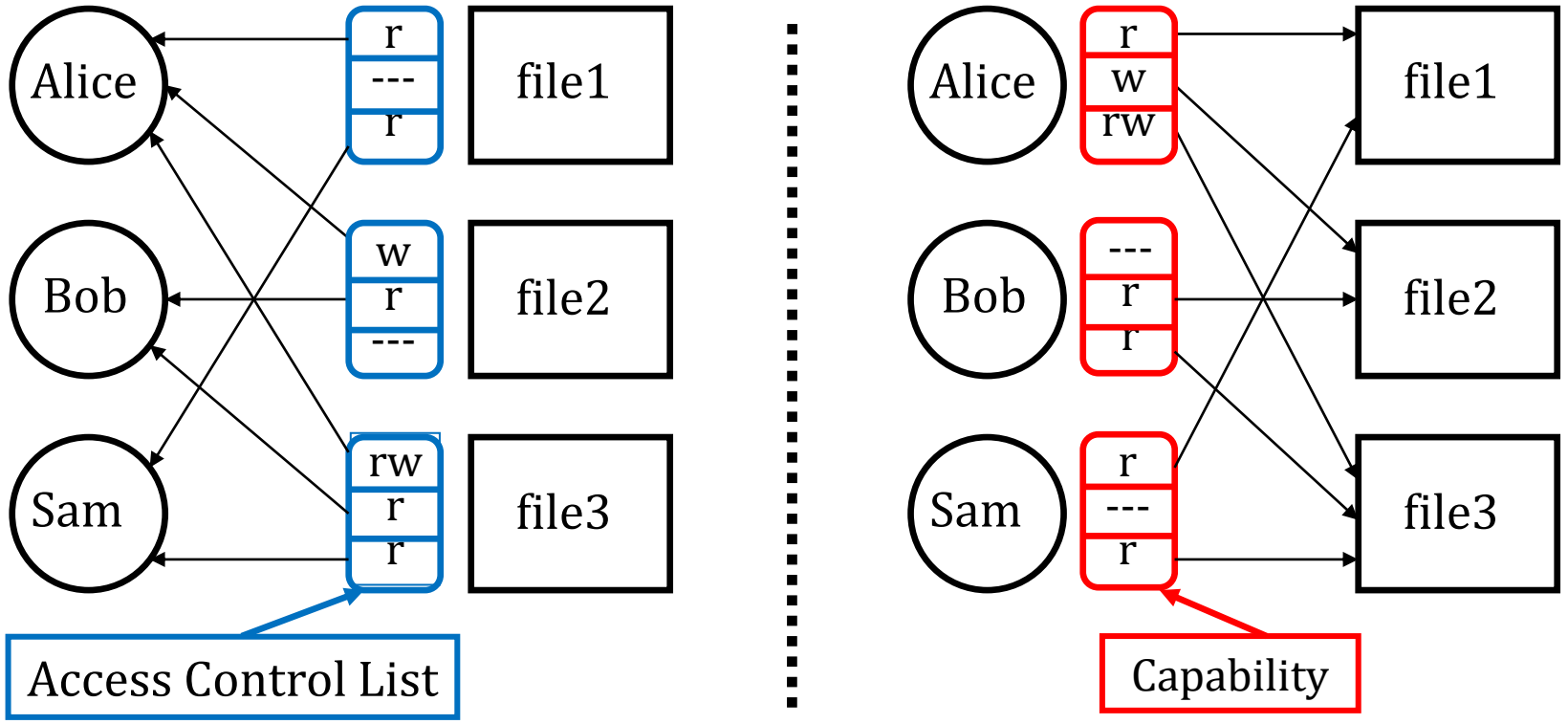
Capabilities (C-lists)

- Controlo de acesso por utilizador



From Dr Lawrie Brown (UNSW@ADFA) for "Computer Security: Principles and Practice", 1/e, by William Stallings and Lawrie Brown

ACLs vs Capabilities



- Setas apontam na direção oposta
- Com ACLs, é necessário associar utilizadores a ficheiros

[dcc]

U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

MULTI LEVEL SECURITY

MLS MODELS

Access Control

Classifications and Clearances

- **Classifications** apply to **objects**
- **Clearances** apply to **subjects**
- US Department of Defense (DoD) uses 4 levels:

  TOP SECRET

  SECRET

  CONFIDENTIAL

  UNCLASSIFIED

Clearances and Classification

- To obtain a **SECRET** clearance requires a routine background check
- A **TOP SECRET** clearance requires extensive background check
- Practical classification problems
  - Proper classification not always clear
  - Level of granularity to apply classifications
  - Aggregation — flipside of granularity

Subjects and Objects

- Let O be an **object**, S a **subject**
  - O has a classification
  - S has a clearance
  - Security **level** denoted L(O) and L(S)
- For DoD levels, we have

  TOP SECRET > SECRET >

  CONFIDENTIAL > UNCLASSIFIED

Multilevel Security (MLS)

- MLS needed when subjects/objects at different levels use/on **same system**
- MLS is a form of **Access Control**
- Military and government interest in MLS for many decades
  - Lots of research into MLS
  - Strengths and weaknesses of MLS well understood (but, almost entirely theoretical)
  - Many possible uses of MLS outside military

[dcc]

U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

MUNDO REAL

SUGESTÕES

Conta root - Password

- O normal relativamente à escolha de passwords
- Ver XKCD 936 e a geração de passwords
- Mudar a password:
  - Periodicamente?
    - NIST: "Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)."
  - Mudança de staff
  - Suspeita de quebra de segurança
- Escrevê-la?
  - Bruce Schneier: "Really, it's smart to use a password manager. Or to write your passwords down on a piece of paper and secure that piece of paper."
- Uso de chaves ssh

Login como root

- Desabilitado em muitos sistemas
- Em Ubuntu nem é possível na consola
  - Depende de configuração
- Ao fazer login como root não se sabe quem o fez

Mudar de Utilizador

- su – substitute user

```
su - change user ID or become superuser
su [options] [-] [user [argument...]]
…
-c, --command=command
```

- Se `user` não for dado ➔ root
- Se `command` não for dado ➔ shell
- `-` ➔ Shell em modo login
- Necessário a password do utilizador `user`

Lançar como root: sudo

`sudo, sudoedit – execute a command as another user`

- Verificação da permissão de acordo com:
  - `/etc/sudoers`
  - `/etc/groups`
- Password do utilizador que lança o `sudo`
  - Tem que ter permissão
- Mantem registo dos comandos efetuados

Exemplos /etc/sudoers

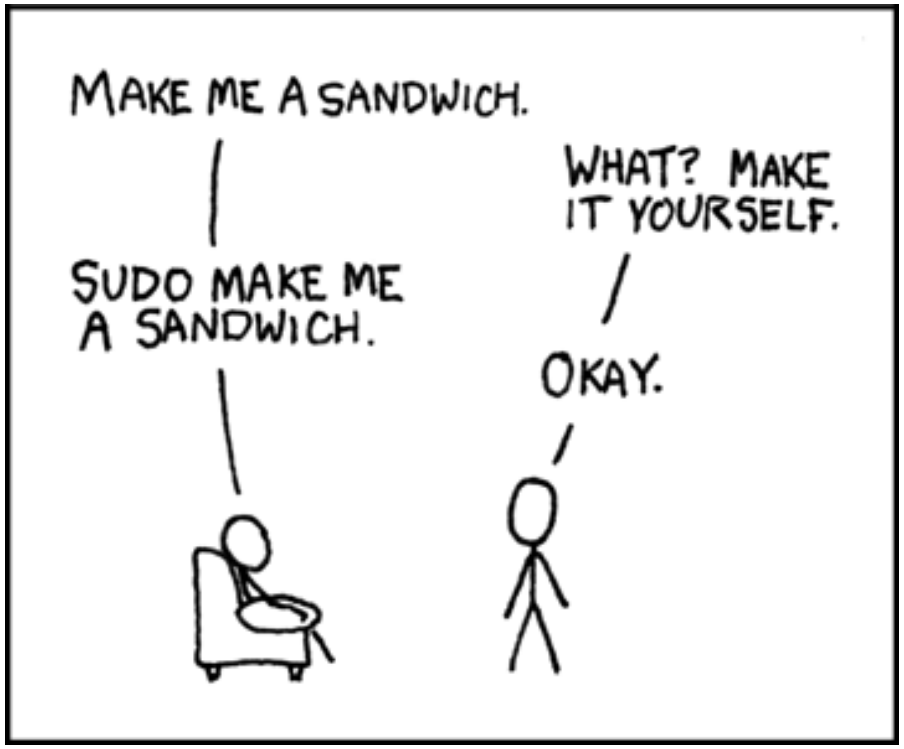
```
# Define aliases for machines in CS & Physics departments
Host_Alias    CS = tigger, anchor, piper, moet, sigi
Host_Alias    PHYSICS = eprince, pprince, icarus
# Define collections of commands
Cmnd_Alias    DUMP = /sbin/dump, /sbin/restore
Cmnd_Alias    PRINTING = /usr/sbin/lpc, /usr/bin/lprm
Cmnd_Alias    SHELLS = /bin/sh, /bin/tcsh, /bin/bash, /bin/ksh, /bin/bsh
# Permissions
mark, ed      PHYSICS       = ALL
herb          CS = /usr/sbin/tcpdump : PHYSICS = (operator)DUMP
lynda         ALL = (ALL) ALL, !SHELLS
%wheel        ALL, !PHYSICS = NOPASSWD: PRINTING
```

Vantagens sudo

- Registo dos comandos efetuados e por quem
- Operadores podem executar sem ter privilégios de root
- Mais rápido do que su (password)
- Revogação de privilégios sem mudar password de root
- Único ficheiro para controlar o acesso de toda a rede
- …

SUDO POWER

xkcd Sandwich, with extra



Desvantagens sudo

- Conta de utilizador passa a ser ponto de falha
- sudo su

Incident

xkcd, incident

Resumo

- Elementos de controlo de acesso
- Ficheiros
- Root power
- Extensões
- Login como root, su, sudo

[dcc]

U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

QUESTÕES/ COMENTÁRIOS