UNIVERSIDADE PORTUCALENSE

Autenticação e controlo de acessos

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Autenticação

- É fundamental na segurança
- É o processo de verificar a identidade reivindicada por alguém ou sistema
- Tem dois passos:
  - Identificação
  - Verificação
- Distinto de autenticação de mensagens

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Autenticação

- Formas de identificar um utilizador baseado em algo individual
  - Por exemplo: password, pin
  - Por algo que possui: chave, cartão
  - Por algo que é: (Biométrico estático) - impressão digital, retina
  - Por algo que faz (Biométrico dinâmico) - voz, sinal
- Podem ser usados individualmente ou combinados
- Todos fornecem autenticação e têm problemas

UNIVERSIDADE PORTUCALENSE

Passwords

- Escolha uma boa password
- Mude-a várias vezes
- Valide a última vez que entrou no sistema (last login)
- Monitore ficheiros novos ou alterados, algo que não tenha feito.

UNIVERSIDADE PORTUCALENSE

Passwords

Passwords

- **Passwords fracas**
  - Baseadas em palavras do dicionário
    - Incluindo as que foram alteradas:
      - Revertidas (ex:, “secreta”)
      - Caso misturado (ex:., SeCreTA)
      - Troca de caracteres/símbolos (ex:, “$ecreta”)
      - Palavras com vogais removidas (ex:, “scrt”)
  - Baseadas em nomes comuns
  - Baseadas no login do utilizador
  - Curta (menos de 6 caracteres)
  - Baseada em padrões do teclado (ex:, “qwerty”)
  - Composta apenas por um caractere
  - Assemelhar-se com a matrícula
  - Ser difícil de decorar

UNIVERSIDADE PORTUCALENSE

Passwords

- **Práticas fracas com passwords**
  - Reciclar passwords
  - Escrever as passwords
  - Utilização de passwords em dois ou mais sistemas
    - Especialmente quando as passwords são utilizadas em sistemas pouco seguros (ex: jogos online)

UNIVERSIDADE PORTUCALENSE

Passwords

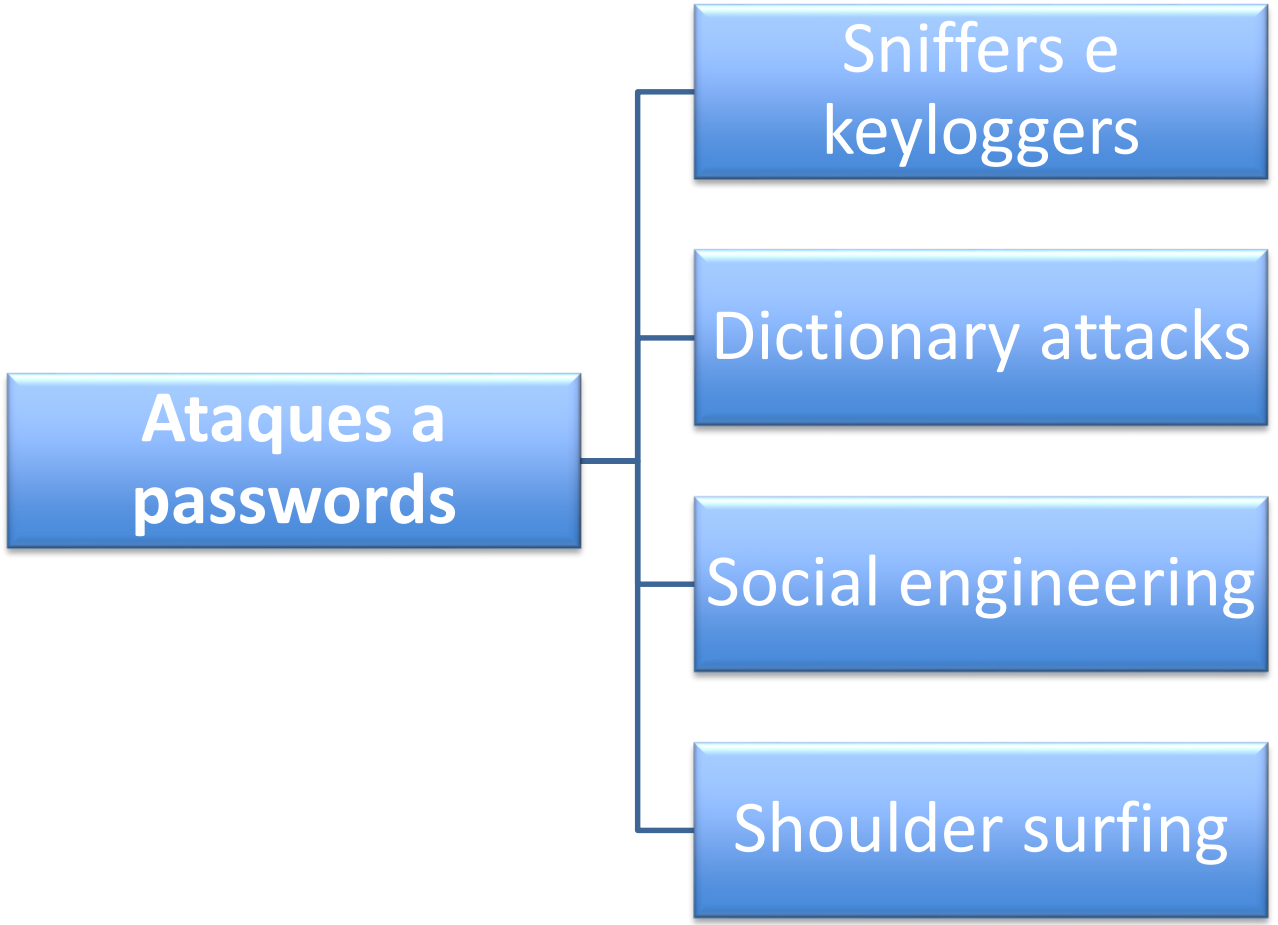
- **Passwords fortes**
  - Contêm pelo menos um caracter de cada um dos grupos:
    - Dígitos (0..9)
    - Letras (a..Z)
    - Sinais de pontuação (., !?:)
  - São baseadas numa frase
    - Por exemplo: s2s0i1f3 derivada do nome da UC
    - Algumas vezes referenciadas como passwords virtuais
  - São fáceis de lembrar e difíceis de adivinhar pelos outros

UNIVERSIDADE PORTUCALENSE

Passwords

- **Boas práticas com passwords**
  - Não reciclar nem escrever as passwords
    - Exceção (escrever passwords em aplicações para guardar passwords)
  - Utilize uma password diferente para cada contexto
  - Cuidado com os Trojan que simulam os écrans de login
  - Cuidado com os keylogger
  - Mude as passwords ocasionalmente
  - Troque a password se suspeita que foi conhecida por terceiros
  - Cautela com a utilização da característica de recordar passwords "Remember Password"

Passwords


Ataques a passwords
Sniffers e keyloggers
Dictionary attacks
Social engineering
Shoulder surfing

Passwords

AAA – segurança das passwords	**Authentication**	Determina que o utilizador é quem diz ser.
	Authorization	O processo usado para decidir se a pessoa autenticada tem permissão para aceder a informações específicas ou funções.
	Access Control	Restrição de acessos

UNIVERSIDADE PORTUCALENSE

Passwords

- **Como são guardadas as passwords**
  - Nos antigos sistemas UNIX eram guardadas num ficheiro: /etc/passwd/
  - Ficheiro que podia ser lido e copiado por todos os utilizadores do sistema;
  - Assim podiam “cracar” o ficheiro “noutra máquina)

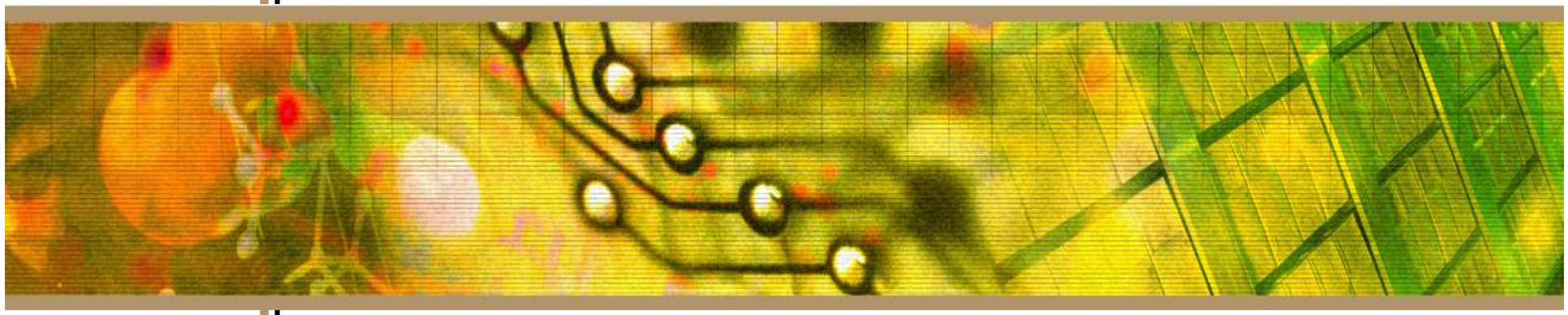
UNIVERSIDADE PORTUCALENSE

Passwords

- Windows
- Utiliza 2 funções de “hashing” de passwords:
  1. LAN Manager hash (LM hash)
  2. NT hash (NT hash)
- Guardadas pelo Security Accounts Manager (SAM)
  - Bloqueado pelo kernel enquanto o Sistema está em execução.
  - Localização - C:\WINNT\SYSTEM32\CONFIG

PURDUE
UNIVERSITY

Password Best Practices



SECURE
PURDUE

VAÇÃO
OGIA

Password Best Practices

UNIVERSIDADE PORTUCALENSE

- *Never* share your login ids and/or passwords
- Remember: you are responsible for any activities associated with your login and password.
- Use strong passwords Be creative: use a hobby:
  - Watching Sci Fi: SciFicTV
  - Better variation: Sc2F3c&TV ; longer = better
  - Use acronyms rather than dictionary words: EGBDF, which means for music students “Every Good Boy Does Fine”
  - Use 6 to 16 characters – a minimum of 8 is best – that includes at least one number and one special character, such as % or &.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Password Best Practices

- ***Always*** change the password provided by a vendor or other system provider
- Change your password frequently – at least once every three to six months
- If you think your password has been compromised, *change it immediately*
- Protect your security codes and passwords by keeping them secret. Do not write them down or store them on your computer!

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Passphrase

- Sequência de caracteres mais longa do que a palavra-passe.
- Substitui as palavras passe
- Pode ser mais segura do que as passwords porque é mais complexa.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

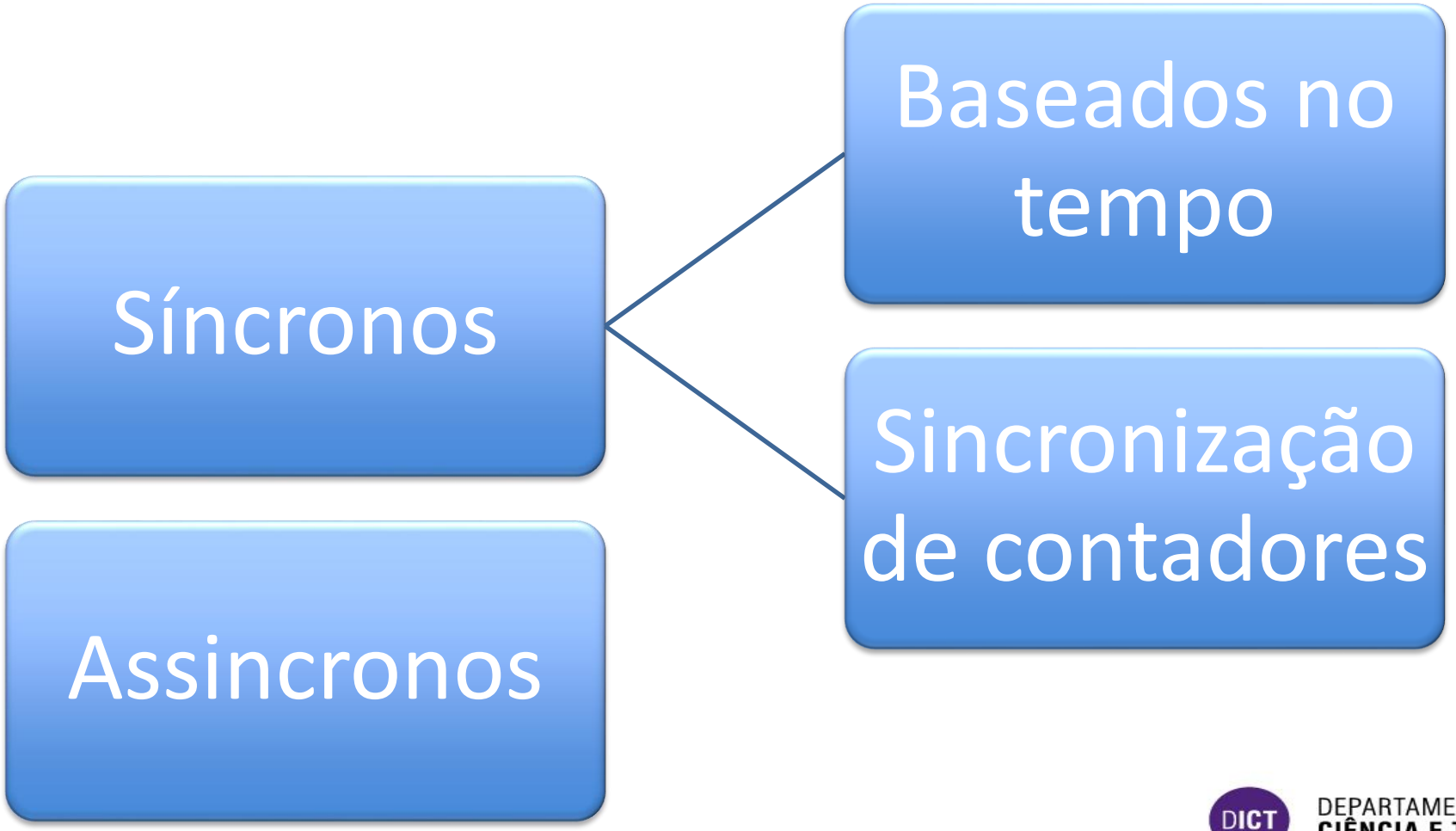
UNIVERSIDADE PORTUCALENSE

Palavras-chave de uma utilização

- Palavras-chave de uma utilização (One Time Passwords)
- Utilizadas para autenticação e são
- Utilizadas para fins de autenticação e são boas apenas uma vez.
- Podem ser geradas por software ou por hardware

UNIVERSIDADE PORTUCALENSE

Geradores de passwords



UNIVERSIDADE PORTUCALENSE

Smart Cards & Memory Cards

- Memory Cards: Guardam, mas não processam a informação
- Smart Cards: Guardam e processam a informação
  - Com contacto
  - Sem contacto
    - Híbridos
    - Combinados

UNIVERSIDADE PORTUCALENSE

Controle de acessos

É um mecanismo usado para limitar as ações que um utilizador legítimo de um sistema pode realizar, com base nas autorizações aplicáveis ao mesmo no momento do acesso.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Controle de acessos

Tipos

- Controle de acesso baseado em papeis
- Single sign-on
  - Capacidade de um utilizador para ter acesso a vários recursos depois de uma operação de autenticação única;
  - Todas as autorizações seguintes acontecem “em background", sem necessidade de qualquer intervenção adicional do utilizador.
- One-Way Authentication
  - necessária quando remetente e recetor não estão em comunicações ao mesmo tempo (por exemplo e-mail)

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Kerberos

- Desenvolvido pelo MIT
- Partilha forte de autenticação
- Disponibiliza a capacidade de single sign-on capability
- As passwords não são enviadas pela rede
- Tecnologia utilizada single sign-on

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

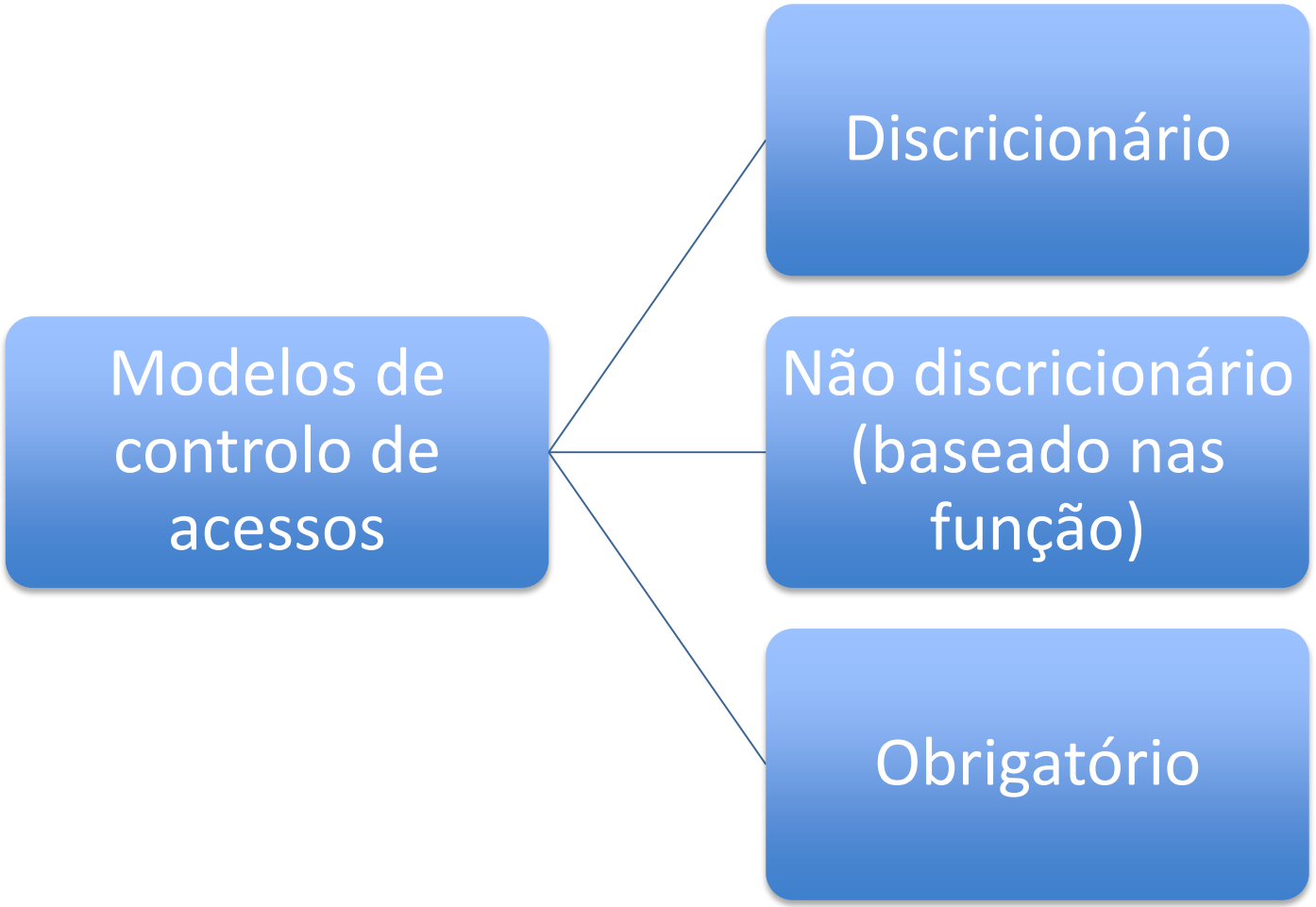
UNIVERSIDADE PORTUCALENSE

Kerberos

- Tem um servidor de autenticação - Authentication Server (AS)
  - Utilizadores inicialmente negoceiam com o AS de modo a serem identificados
  - O servidor de autenticação disponibiliza uma credencial de autenticação não corruptível (ticket granting TGT)
- Tem um servidor Ticket Granting (TGS)
  - Os utilizadores solicitam acessos subsequentes a outros serviços a partir do TGS como utilizadores do TGT

UNIVERSIDADE PORTUCALENSE

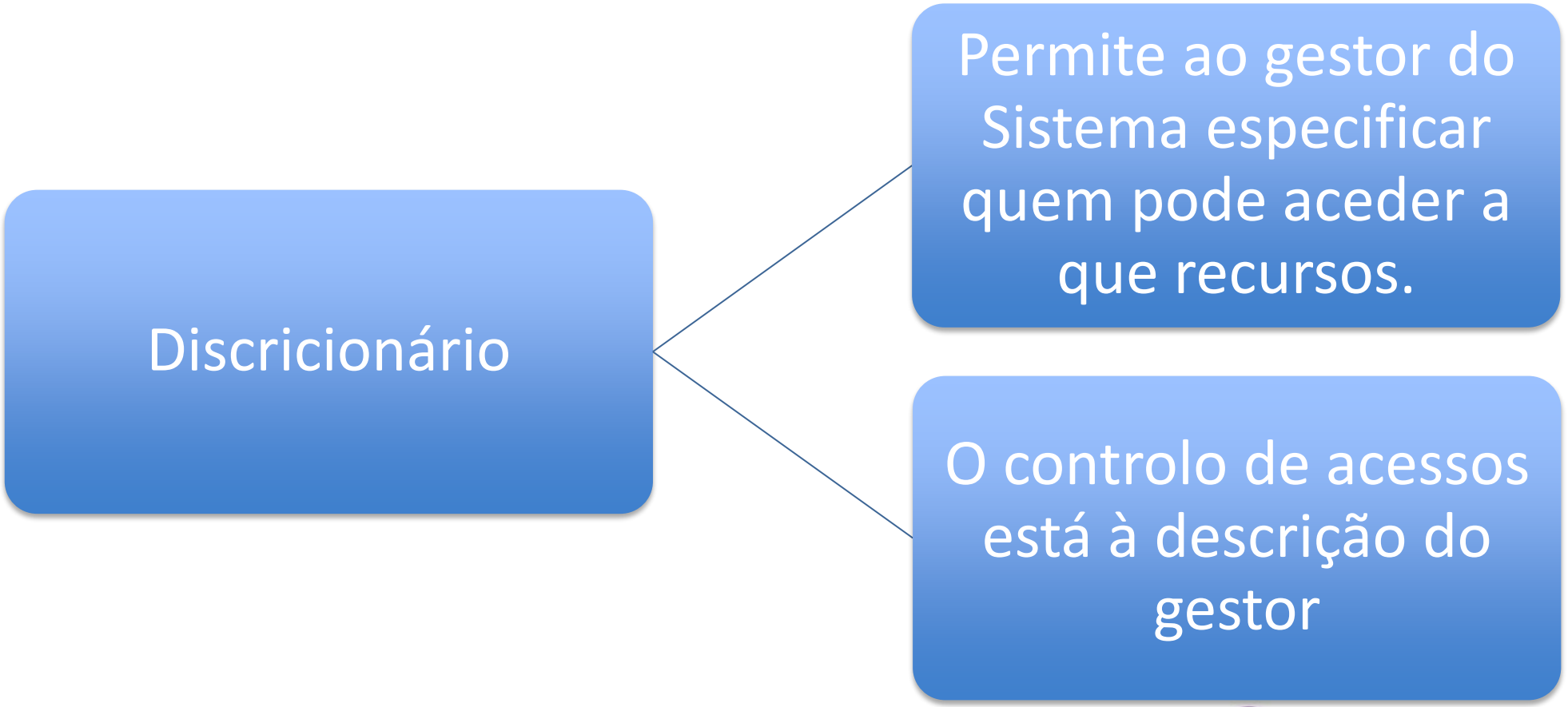
Modelos de controlo de acessos



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Modelos de controlo de acessos



UNIVERSIDADE PORTUCALENSE

Modelos de controlo de acessos

Não discricionário

- As permissões são dadas de acordo com os papeis do utilizador.
- Sistema utilizado em instituições que têm muita rotatividade.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Modelos de controlo de acessos

Obrigatório

O controlo de acesos é baseado em etiquetas (labels)

Os utilizadores habilitações de segurança e os recursos têm etiquetas que contêm classificações.

É utilizado por exemplo em ambientes militares onde a classificação da informação é importante.

UNIVERSIDADE PORTUCALENSE

Técnicas de controlo de acessos

Há uma série de controlos de acesso e tecnologias diferentes disponíveis para suportar os diferentes modelos.

- Controlo baseado em regras
- Restrição da interface
- Matriz de controlo de acessos
- Acesso dependente do conteúdo
- Acesso dependente do contexto

UNIVERSIDADE PORTUCALENSE

Técnicas de controlo de acessos

Baseado em regras

- Utiliza regras especificas para indicar o que pode acontecer entre o sujeito e o objeto
- Não necessariamente baseado na identidade.
- Tradicionalmente utilizado no modelo obrigatório

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Técnicas de controlo de acessos

Restrição na interface

- O utilizador pode ou não executar uma função dependendo da interface
- Grandes tipos
  - Menus e Shells
  - Database Views
  - Interfaces restringidas fisicamente (ex.: ATM)

UNIVERSIDADE PORTUCALENSE

Técnicas de controlo de acessos

Matriz de controlo de acessos

- Tabela com utilizadores e funções indicando as funções que um utilizador pode executar

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Técnicas de controlo de acessos

- Baseado no conteúdo
  - O acesso a um objeto é determinado pelo conteúdo desse objeto. (Ex. Acesso a determinados campos de uma base de dados)

- Baseado no contexto
  - As decisões sobre o acesso são baseadas no contexto de um conjunto de informações. (Ex.: menus de contexto do Office)

UNIVERSIDADE PORTUCALENSE

Administração do controle de acessos

- Centralizado
  - Radius (Remote Authentication Dial In User Service)
  - Tacacs (Terminal Access Controller Access Control System)

- Descentralizado
  - As decisões sobre o acesso são baseadas no contexto de um conjunto de informações. (Ex.: menus de contexto do Office)