Protocolo *Kerberos*

Notas para a UC de “Segurança Informática”

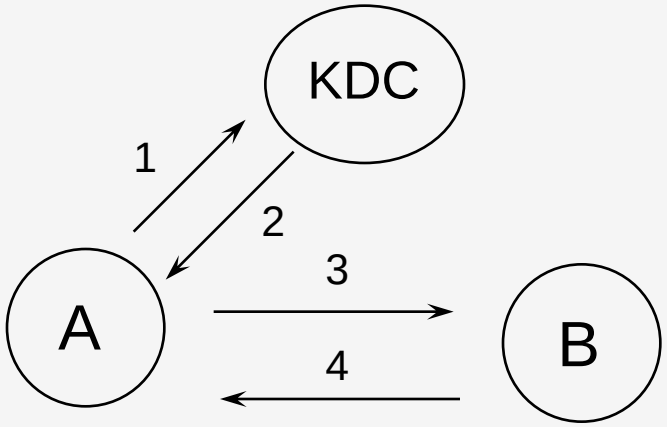
Inverno de 11/12

Pedro Félix (pedrofelix *em* cc.isel.ipl.pt)

Instituto Superior de Engenharia de Lisboa

Kerberos (1)

- Iniciação: A e B partilham chaves secretas com KDC (k_{AT} e k_{BT})
- Notação:
  - Bilhete: $tck_B = AE(k_{BT})(k, A, L)$
  - Autenticador: $auth_A = AE(k)(A, ts_A)$



- 1 - A pede um bilhete para B
  - $A \rightarrow$ KDC: A, B, N_A
- 2 - KDC gera chave de sessão k e responde com o bilhete para B e a chave de sessão k cifrada com k_{AT}
  - $A \leftarrow$ KDC: tck_B, $AE(k_{AT})(k, N_A, L, B)$
- 3 - A envia a B o bilhete e o autenticador (prova possuir k)
  - $A \rightarrow B$: tck_B, $auth_A$
- 4 - B autentica-se perante A (prova possuir k)
  - $A \leftarrow B : AE(k)(ts_A)$

Kerberos (2)

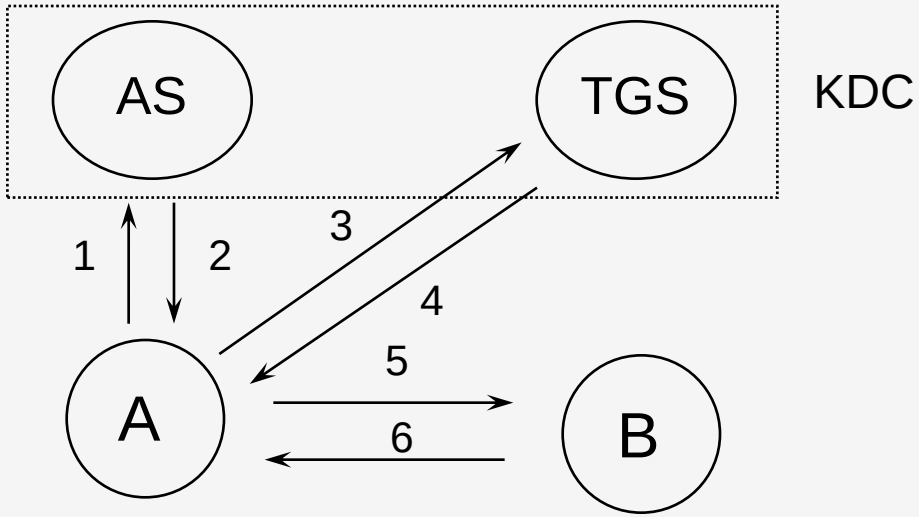
- Interacção com o KDC realiza-se em duas fases:
  - *Authentication Service* (aquando do *login*)

    $A \rightarrow KDC: A, TGS, N_A$

    $A \leftarrow KDC: tck_{TGS}, AE(k_{AT})(k_1, N_A, L, TGS)$
  - *Ticket Granting Service* (quando pretende aceder a um serviço)

    $A \rightarrow TGS: tck_{TGS}, auth_A, B, N'_A$

    $A \leftarrow TGS: tck_B, AE(k_1)(k_2, N'_A, L, B)$



Kerberos (3)

- Função **AE** – *cifra autenticada*
- Exemplo de utilização: *Windows* 2000
  - Serviço de autenticação (local e remota)
  - *Remote Procedure Calls* (RPC) - autenticação e confidencialidade
- Chaves entre entidades e KDC
  - Derivadas da *password* de *login*
- A ligação entre o cliente *A* e o servidor *B* implica a obtenção, por parte de *A*, dum bilhete para *B*
  - comunicação com o KDC
- Utilizado em *Intranets* (ex. domínios *Windows*)
- Inadequado na *Internet*
  - Quem seria o KDC?
  - Obrigatoriedade de comunicação *online* com o KDC/TGS

“Cifra Autenticada”

- Seja **(E,D,G_1)** um esquema de cifra e **(T,V,G_2)** um esquema MAC

- Função de “cifra autenticada”

  $AE(k)(m) = E(k_1)(IV,m,pad), T(k_2)(IV,m,pad)$

  – Onde

  - **k_1** e **k_2** são chaves derivadas de **k**
  - **IV** é um vector inicial (E pode ser determinístico, ex: CBC com IV = 0)
  - **pad** é uma sequência de *padding*

- Função de “decifra autenticada”

  $AD(k)(c,t)$ =

  $(IV, m, pad) = D(k_1)(c)$

  Se **$V(k_2)(t,(IV,m,pad))$** = *false* então retornar *false*

  retornar **m**