Modelo de Clark e Wilson

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

Introdução

- Clark, Wilson, “A comparison of Commercial and Military Computer Security Policies”, IEEE Symposium on Security and Privacy, 1987.
- *Modelo* para a integridade da informação, baseada em práticas de processamento de informação comerciais.
- Definição de integridade - “No user of the system, even if authorised, may be permitted to modify data items in such a way that assets or accounting records of the comparny are lost or corrupted”
- Os mecanismos de alto nível para garantir a integridade, antecessores do advento dos sistemas de computação, são:
  - Transacções bem formadas (“Well Formed Transaction”)
  - Separação de direitos (“Separation Of Duty”)

Transacções bem formadas

- O utilizador não acede directamente à informação
- O acesso é realizado através de procedimentos que garantem a integridade

- Exemplo: “double entry bookkeeping”
- Objectivo: consistência interna da informação

Separação de deveres

- Separação duma operação em diferentes partes
- Realização das diferentes partes por diferentes utilizadores

- Exemplo:
  - processo de compra, recepção e pagamento de produtos
  - Certificação e utilização dum procedimento

- Objectivo: consistência entre o estado interno e o “mundo real”

Modelo

- Classificação dos dados
  - CDI – “Constrained Data Items”
  - UDI – “Unconstrained Data Items”
- Classificação dos procedimentos
  - IVP – “Integrity Verification Procedures”
  - TP – “Transformation Procedures”
- O acesso a CDI apenas pode ser realizado por TP

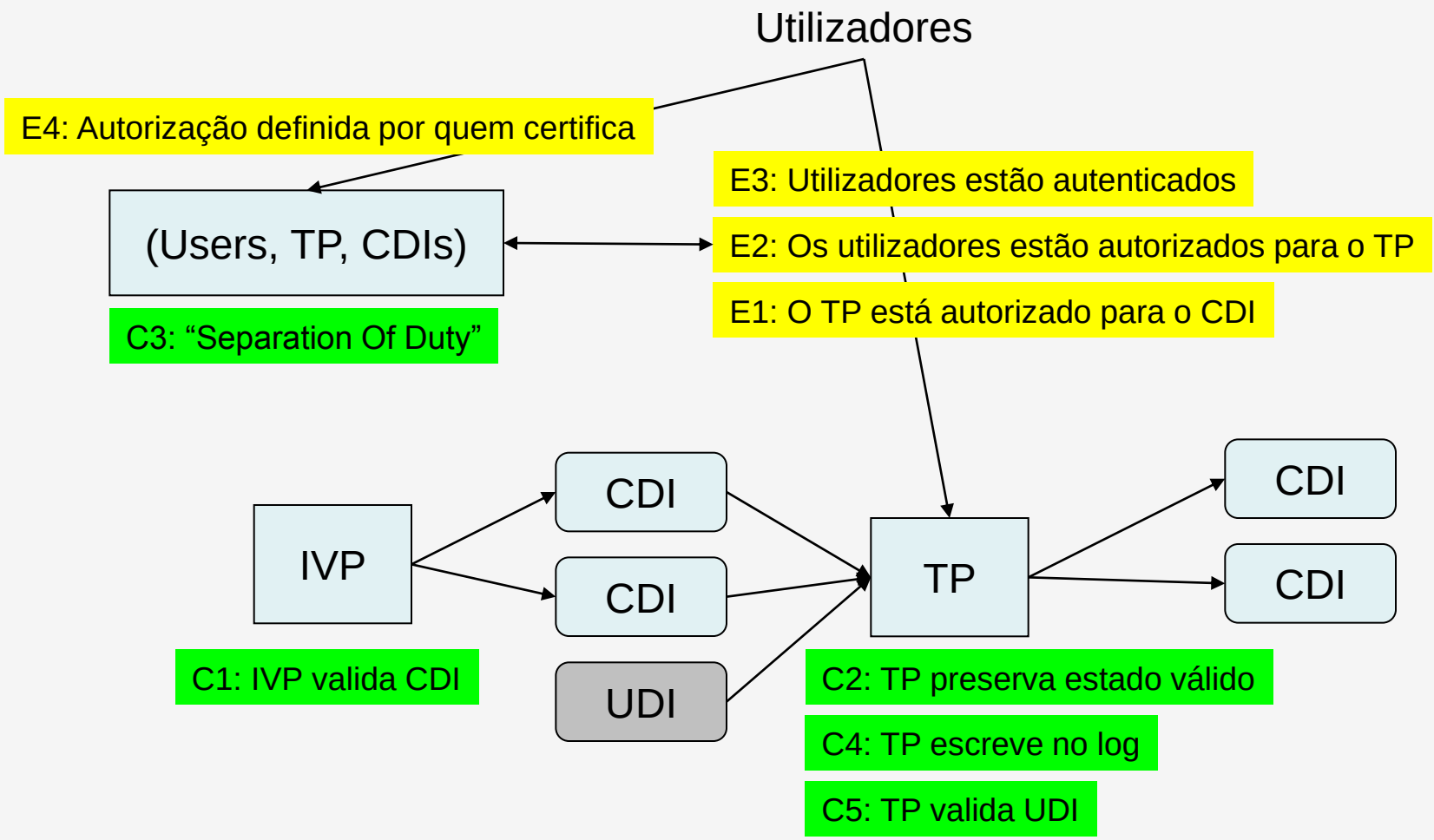
Regras (1)

- C1: Todos os IVP devem ser certificados como garantindo a validade do CDI no momento em que o IVP é executado
- C2: Todos os TP devem ser certificados como válidos
  - Dado um conjunto de CDI de entrada válidos, devem produzir um conjunto de CDI válidos
  - O conjunto de CDI que o TP pode aceder faz parte da certificação
- E1: O acesso a CDI apenas pode ser realizado por TP certificados para esse CDI
- E2: O sistema deve manter uma lista de tuplos (User, TP, CDIs) e garantir que apenas as execuções correspondentes a um tuplo são executadas
- C3: A lista de tuplos de E2 deve estar certificada como garantindo “Separation Of Duty”

Regras (2)

- E3: O sistema deve autenticar cada utilizador que execute um TP
- C4: Todos os TP devem estar certificados em como escrevem toda a informação relevante da operação para um CDI “append-only”
- C5: Todos os TP que recebem um UDI devem estar certificados em como apenas realizam transformações válidas
  - Transformar o UDI num CDI
  - Rejeitar o UDI
- E4: Apenas os utilizadores que certificam entidades podem alterar a associação destas entidades. Um utilizador que certifica uma entidade não a pode utilizar (SoD).

Diagrama



Adaptado de Clark, Wilson, “A comparison of Commercial and Military Computer Security Policies”,