Aspectos de Segurança no Windows Vista

Notas para a UC de “Segurança Informática”

Inverno de 11/12

José Simão (jsimao *em* cc.isel.ipl.pt)

Instituto Superior de Engenharia de Lisboa

Sumário

- Componentes para controlo de acessos [1]
- User Account Control (UAC) [2]
- Modelo de Integridade [2]

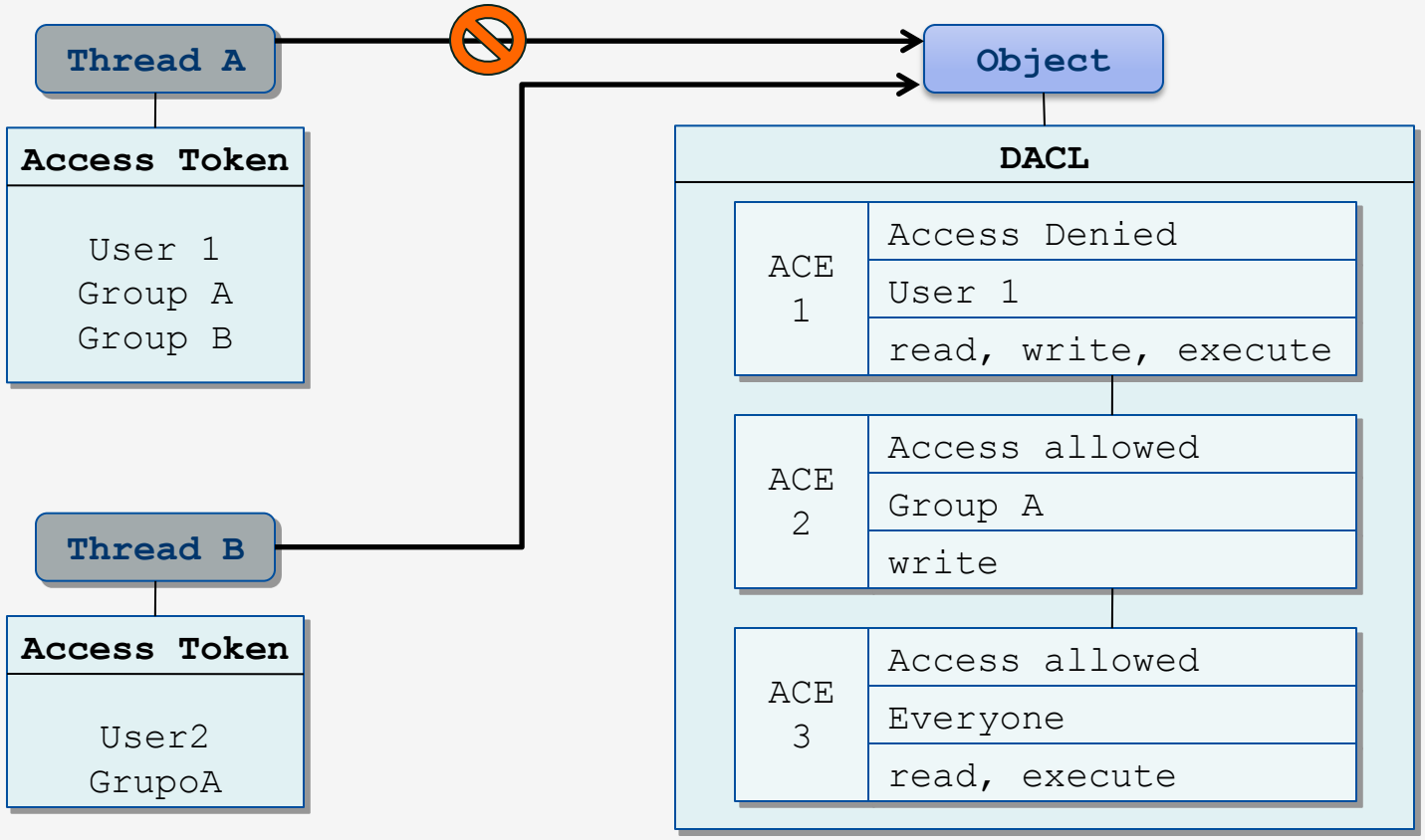
Componentes para controlo de acessos

- Após *login* é atribuído ao utilizador um *access token*
  - Em cada *access token* estão presentes *security identifiers (SID)* com a identificação do utilizador e dos grupos a que pertence

- Após a criação de um objecto (recurso) é lhe associado um *security descriptor* com:
  - O SID do seu dono
  - Discretionary Access Control List (DACL)
  - System Access Control List (SACL) com a política do sistema para auditar o acesso ao objecto e o “nível de integridade” do mesmo

- Uma ACL é uma lista de Access Control Entry (ACE), onde consta:
  - SID (utilizador ou grupo), Permissão ou Negação, Acções

Controlo de acessos através de DACL



- Para determinar se o acesso é autorizado ou não, a DACL é percorrida até à negação de uma das acções ou permissão de todas as acções requeridas
- À cabeça ficam as ACE que negam

User Account Control

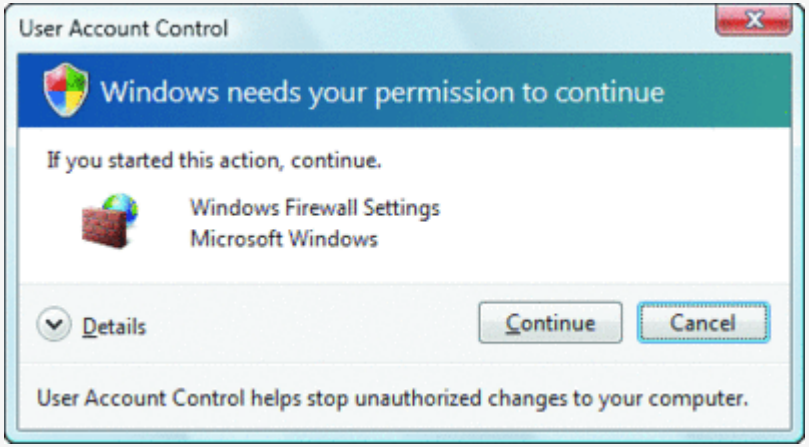
- O UAC tem por objectivo dar suporte ao princípio do privilégio mínimo
  - No Windows XP se o utilizador tivesse um *access token* de *administrator*, todas as operações seriam realizadas com esse token
  - O sistema estava exposto a danos acidentais ou propositados (ex: provacados por *malware*) a zonas vitais do sistema

- As permissões atribuídas a administradores foram revistas
  - Ex: “Administrator” pode mudar hora, “Standard User” pode mudar fuso horário
- Aquando do *login*, os utilizadores administradores são *standard user*
- Elevação de privilégios apenas quando necessário
- Virtualização em aplicações legadas (i.e. 32 bits, não estão a ser executadas com direitos de administrador, não tem ficheiro de manifesto)
  - Directorias críticas (ex: %System Root%) e algumas sub-árvores do registry

User Account Control – Administrator Approval Mode

- Para algumas tarefas é inevitável ter direitos de administração
  - Instalação de software, configuração de propriedades globais
  - No Windows XP o utilizador utiliza a conta de *standard user* ou de *administator*
- Aquando do *login,* um utilizador que pertence ao grupo de Administrators fica com dois *access tokens*: Standard User e Administrator
- Para executar as aplicações para as quais é necessário ter direitos do grupo Administrators, é pedido o consentimento do utilizador para os activar
  - Manifesto da aplicação exige direitos de administrador
  - Run as Administrator
  - Heurísticas para detectar programas “instaladores”
- Consentimento pedido num “desktop seguro”

User Account Control – Administrator Approval Mode



Local Security Policy -> Security Settings -> Security Options ->

UAC: Behavior of the elevation prompt for Admin Approval Mode: {Credentials | Consent}

UAC: Behavior of the elevation prompt for standard users: {Credentials | Automatically deny}

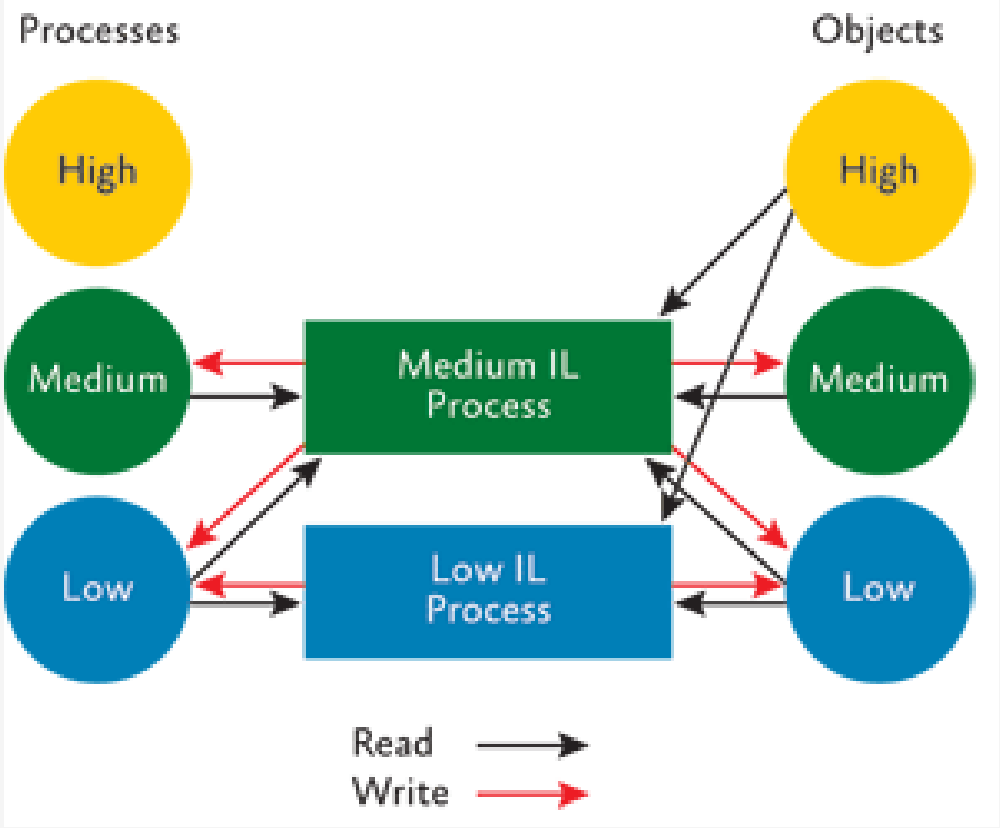
Políticas e Níveis de Integridade

- Política MAC para todos os objectos:
  - Não é permitido que processos escrevam em níveis de integridade superior ao seu (“No Write Up”)
- Política MAC adicional para objectos que representam processos:
  - Não é permitido que processos leiam dados de outros processos com nível de integridade superior ao seu (“No Read Up”)

- Níves de integridade e políticas guardados na System ACL do objecto
  - Níveis (Low, Medium, High, System), Políticas (No_Write_Up, No_Read_Up)

- A alteração do nível de integridade só pode ser feita por processos com nível de integridade superior e para níveis de integridade igual ao seu ou inferior

Política para acesso a processos e objectos



Níveis de integridade e exemplos de aplicações

Nível de Integridade	Exemplos de processos
Low Mandatory Level	Protected Mode Internet Explorer e processos lançados por Protected Mode Internet Explorer
Medium Mandatory Level	Standard user e processos sem direitos elevados
High Mandatory Level	Processos a executar com direitos de administração
System Mandatory Level	Local System, Local Service e Network Service

User Interface Privilege Isolation

- O Windows Vista impede que processos com direitos de *standard user* enviem mensagem para processos com direitos de administrador (i.e. processos elevados)

- Este mecanismo, designado por User Interface Privilege Isolation (UIPI), tem por base níveis de integridade associados a processos e objectos

- O sub-sistema de mensagens do Windows tem em conta os níveis de integridade dos processos origem e destino
  - Não é possível enviar mensagens para processos com IL superior
  - Não é possível instalar *hooks* em processos com IL superior

Referências

[1] MSDN Library, “Access Control Components”

[2] MSDN Junho 2007, “Inside Windows Vista User Account Control”, Mark Russinovich