GRUPO DE SEGURIDAD INFORMÁTICA

Fundamentos de la Seguridad Informática

Seguridad en Sistemas Windows

control de acceso (parte 2)

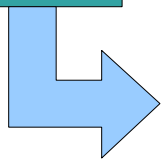
Decisiones sobre acceso (2)

- Windows Access controls pueden usarse de distinta forma:
  - **Impersonation**: El proceso (subject) “inpersonates” el SID del usuario (principal) de su token
  - **Role-Centric**: usamos grupos y alias para darle a un proceso los permisos para realizar su tarea
  - **Object-Centric:** los objetos a nivel de las aplicaciones obtienen un SD. (mucho mas complejo)

DACL

- Es una lista de ACEs (*access control entries*)
- Es posible unir propiedades en conjuntos

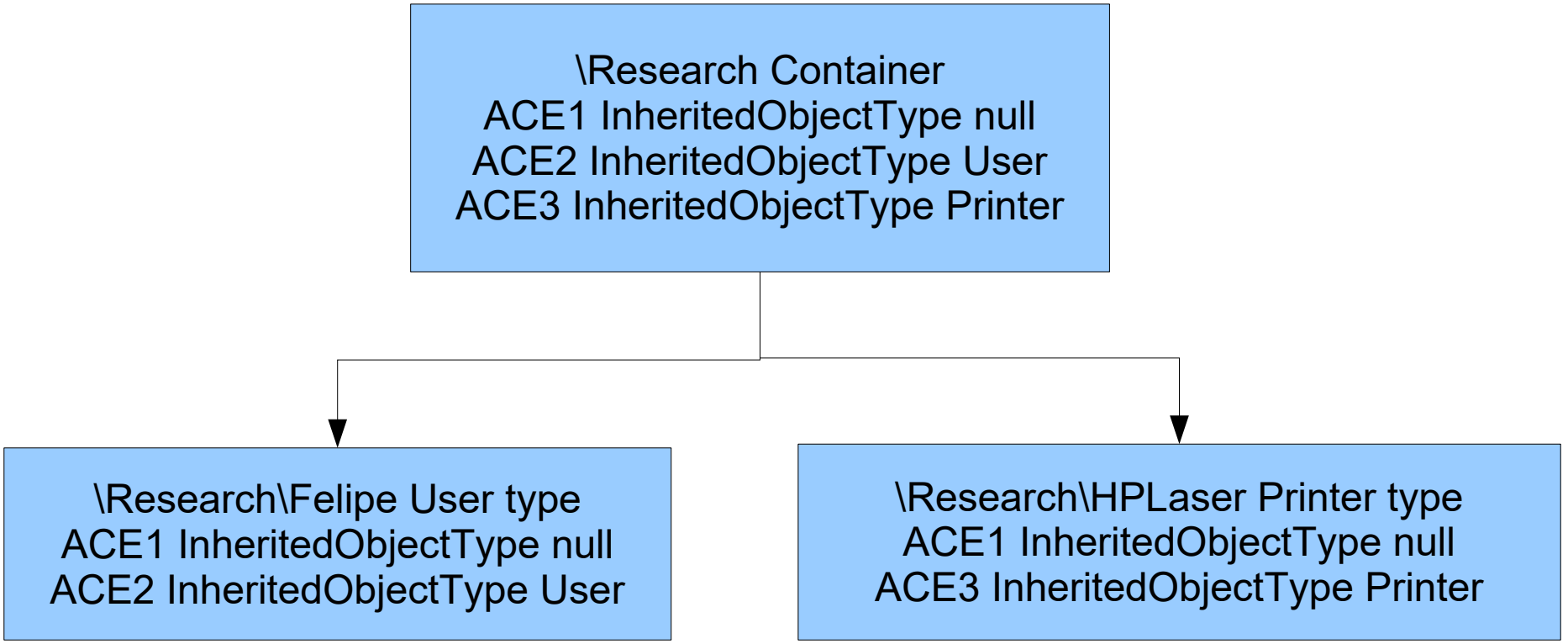
Tipo: grant o deny
Flags
ObjectType
InheritedObjectType
Access Rights
SID Principal: al qué la ACE aplica



ACE1
Tipo: ACCESS_ALLOWED_OBJECT_ACE
Tipo de objeto:GUID para página web
Heredado de: GUID para usuarios
Access Rights: Write
SID Principal: PRINCIPAL_SELF

Herencia de ACEs

- Al crearse un nuevo objeto, se heredan del contenedor en el cual están



Restricted Tokens

- El control de acceso está referido (implícitamente) a usuarios
- Se puede implementar una variante de *code-based access control* usando *restricted tokens*
- Un proceso ejecutando con un restricted token es un *restricted context*
- Estos tokens eliminan privilegios de un token dado, son versiones limitadas de un access token

Restricted Tokens

- Un proceso ejecutando con un “restricted token” se denomina “restricted context”
- Se pueden construir a partír de un access token del usuario:
  - Deshabilitando grupos: no se eliminan, son marcados como USE_FOR_DENY_ONLY,
  - Agregando un restricted SID representando la identidad y permisos del programa ejecutándose; este SID se usa en las ACL de los objetos para darle acceso al programa (sujeto)
  - eliminando privilegios,
- restricted SIDs pueden crearse por:
  - programas y agregado a las ACLs de los recursos requeridos (object types);
  - tipo de objeto y agregado a los “restricted tokens”

Contexto restringido (2)

- Los SIDs de grupos pueden deshabilitarse marcándolos como USE_FOR_DENY_ONLY
- Se puede usar cuando un thread del servidor inpersona a un cliente, x ej ejecuta en el contexto del token de acceso del cliente
- Mediante el agregado de un SID restringido al token, un proceso tiene acceso solamente si ambos el SID y el SID restringido tienen acceso

Contexto restringido

Algoritmo de control de acceso

```
BOOLEAN RestrictedAccessCheck (Acl: ACL, DesiredAccess : AccessMask,
                               RestrictedToken : AccessToken)
 if (AccessCheck(Acl, DesiredAccess, RestrictedToken.PrincipalSids) &&
    (AccessCheck(Acl, DesiredAccess, RestrictedToken.RestrictedSids)
         return SUCCESS;
  else
          return FAILURE;
```

Contexto restringido Ejemplo

User SID	Dieter
Group SIDs	Administrators *use for deny only* Users
Restricted SIDs	MyApp
Privileges	(none)

En el caso 1: Access: read
En el caso 2: Access: none
En el caso 3: Access: none

Ace 1: (Allow)
Access Rights: read, write
Principal SID: Dieter

Ace 2: (Allow)
Access Rights: read
Principal SID: MyApp

Ace 1: (Allow)
Access Rights: read
Principal SID: Admin

Ace 2: (Allow)
Access Rights: read
Principal SID: MyApp

Ace 1: (Allow)
Access Rights: read
Principal SID: Dieter

Extensiones de seguridad: MIC

Mandatory Integrity Control (**MIC**)

- Nuevo conjunto de security principals llamados integrity levels (IL) que se agregan a los Access Token y ACLs:
  - Low
  - Medium
  - High
- Se chequean los IL del sujeto y objeto al que se está accediendo

Extensiones de seguridad: UAC

- UAC = User Access Control (**UAC**) o Least User Access (LUA)
  - Desarrollador marca aplicaciones que requieren privilegios elevados
  - LSA es modificado para asignar dos tokens al momento de logon: *filtered* (restricted) y *linked*
  - Aplicaciones ejecutan con *filtered* token
  - Token con los privilegios completos (*linked*) es usado solo con aplicaciones marcadas que requieren privilegios elevados
- Usuarios sin privilegios de administrador ejecutan con *medium* IL, cuando el proceso eleva privilegios ejecuta con *high* IL

Security Templates

- Una herramienta muy util que proveen los sistemas Windows 2000 es la “Windows Configuration Tool Set”
- Provee un mecanismo centralizado para verificar y aplicar políticas de seguridad a un sistema Win2k
- Archivos de texto donde se especifican configuraciones de seguridad del sistema

Security Templates

- Podemos **modificar**, **crear** o **exportar** un template de seguridad usando los “snap-in” de la MS Management Console (MMC):
  - Security Configuration and Analysis Tool
  - Security templates
- La aplicación de las políticas definidas en un security template, podemos aplicarlas usando:
  - Group Policy Object (Domain Environment)
  - Secedit.exe command line utility (workgroup environment)

Gestión de Logs y Auditoria

- Win2k professional cuenta con capacidades importantes de auditoría
  - Logon events, account management, directory server access, object access, policy change, privilege use, process tracking, system events
- Archivos individuales pueden ser auditados
- Los eventos auditados los accedemos usando la herramienta “Event Viewer”

Gestión de Logs y Auditoría

- El sistema de registro de eventos (log) almacena los datos estructurados en campos:
  - “Type”, “User”, “Computer”, “Category”, etc
- Provee una API para acceder en forma segura a la información de logs,
- Contamos con acceso remoto desde otras computadoras con S.O. Windows

Gestión de Logs y Auditoría

- No es sencillo hacer búsquedas de “texto libre” sobre los registros de eventos (solo usando los campos predefinidos)
- No provee mecanismos para el almacenamiento de logs en un servidor central ....
- a menos de incorporar soluciones extras (SCOM, System Center Opertation Manager), más costosas y complejas

Bibliografía y material de referencia

- **D. Gollman**, *Computer Security*, Wiley, 2006
- **Michael M Swift et al**, Improving the granularity of access control for Windows 2000, ACM Trans Inf Syst Secur, 2002
- **NIST, Special Publication 800-43,** Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System