CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

LES ÉLÉMENTS CLÉS DE WINDOWS

LES ÉLÉMENTS CLÉS DE WINDOWS
Introduction

- Windows NT est un système d'exploitation très riche et complexe
- Ne pouvant tout traiter, ce chapitre n'aborde que quelques éléments clés du fonctionnement de Windows :
  - Les objets (handles, process, threads)
  - La configuration (base de registre)
  - Quelques mécanismes (interruptions, exceptions, entrées / sorties, interface graphique)
  - Le modèle de sécurité (privilèges, identifiants de sécurité, autorisations d'accès)

LES ÉLÉMENTS CLÉS DE WINDOWS

Les objets

- Les objets sont des éléments clés du fonctionnement de Windows NT
- Il existe une quarantaine d'objets dans Windows 7
- Les objets principaux :
  - Le fichier (file) : fichier réel ou virtuel comme un canal (pipe)
  - Le périphérique (device) : périphérique réel ou virtuel
  - Le pilote (driver) : pilote d'un périphérique
  - Le processus (process), le « job », le « thread »
  - La clé de registre (key) : entrée dans la base de registre
  - L'événement (event), le mutex (mutant), le sémaphore (semaphore), le « timer » : objets de synchronisation et de communication inter-processus

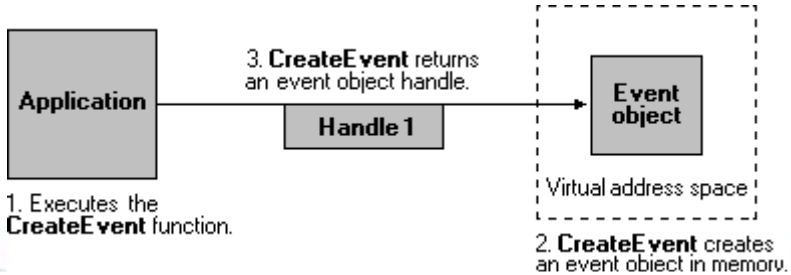
LES ÉLÉMENTS CLÉS DE WINDOWS
Attributs d'un objet

- Les objets ont une structure commune d'attributs
- Parmi ces attributs, les plus importants sont :
  - « Objet name » : permet de l'identifier afin de le rendre accessible
  - « Objet Directory » : Chemin où l'objet se trouve
  - « Security descriptor » : ACLs (Liste de droits d'accès)
  - « Type objet pointer » : définit le type de l'objet
  - « Open handler database » : liste des processus en cours d'utilisation de l'objet
  - « Open handle counter » : compteur du nombre d'ouvertures de l'objet
  - « kernel/user mode » : Permission d'accès en mode Utili.

LES ÉLÉMENTS CLÉS DE WINDOWS

Les Handles

- Tout objet est manipulé par l'intermédiaire d'une référence appelée « Handle »
- L'ouverture ou la création d'un objet génère un handle qui est associé au processus qui a fait la demande
- Un handle contient un pointeur sur l'objet ainsi que les droits qu'a le processus sur l'objet
- Un processus a une liste de handles correspondant à tous les objets auxquels il a accès
- Un objet peut être accédé par plusieurs processus, chaque processus a un handle sur cet objet



LES ÉLÉMENTS CLÉS DE WINDOWS

Les Processus

- Un processus est constitué de plusieurs éléments :
  - Un PID (Process IDendifier) : numéro du process
  - Un « Working Set » : espace d'adressage mémoire virtuel privé du processus (code exécutable + données)
  - Une liste de threads : au minimum 1 pour son exécution
  - Une liste de handles : descripteur pointant sur les objets ouverts par le processus
  - Un jeton d'accès (Access token) : contexte de sécurité de l'utilisateur qui exécute le processus
  - Des variables héritées du processus parent
  - Une classe de priorité d'exécution et d'entrée/sortie
  - Une ACL : liste des permissions d'actions du processus

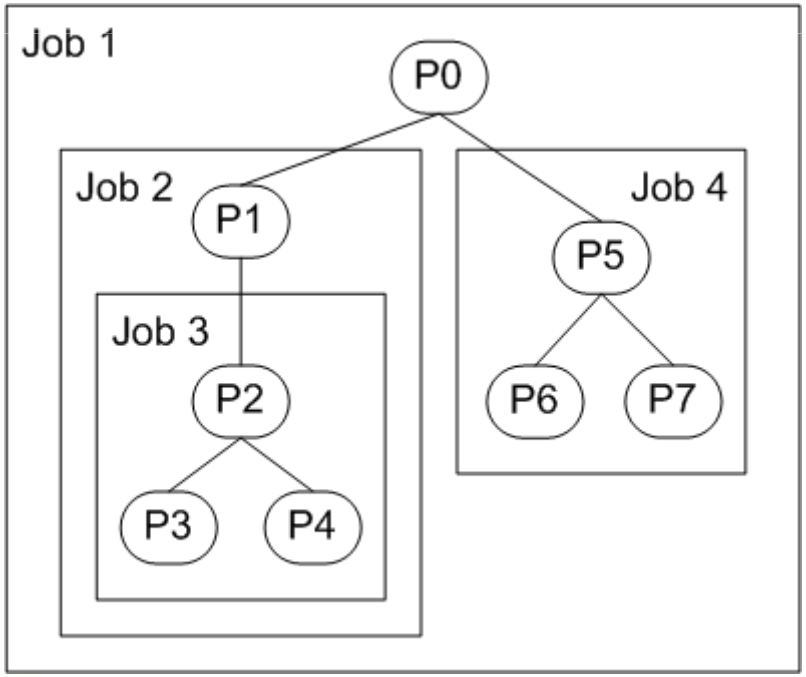
LES ÉLÉMENTS CLÉS DE WINDOWS

Les Threads

- Un thread est une unité d'exécution qui réalise l'exécution de code
- Un thread comprend plusieurs éléments qui sont rassemblés sous un contexte de thread :
  - Pointeur d'instruction (EIP/RIP)
  - Environnement, pile en mode utilisateur et pile en mode noyau
  - Des registres (correspondant à ceux du processeur)
  - Espace d'adressage de données privées
  - L'état du thread, un jeton d'accès ainsi qu'une ACL
- Un thread ne peut appartenir qu'à un seul processus et ne peut utiliser que les ressources de ce processus

LES ÉLÉMENTS CLÉS DE WINDOWS
Les jobs

- Un « Job » est un objet pouvant contenir un ou plusieurs processus. Il permet de regrouper plusieurs processus d'une même application afin de pouvoir appliquer des quotas et de terminer tous les processus d'un seul coup



LES ÉLÉMENTS CLÉS DE WINDOWS

Le stockage de la configuration de Windows

- **Windows NT stocke la configuration du système et des applications dans une base de données appelée « Base de registre »**
- **Structurée hiérarchiquement à partir de 5 ruches :**

Ruche (Clé racine)	Description
HKEY_CLASSES_ROOT	Extension des noms de fichier
HKEY_CURRENT_USER	Profil de l'utilisateur connecté
HKEY_LOCAL_MACHINE	Config matérielle et logicielle locale
HKEY_USERS	Profils des utilisateurs qui se sont connectés localement
HKEY_CURRENT_CONFIG	Configuration du matériel actif

LES ÉLÉMENTS CLÉS DE WINDOWS

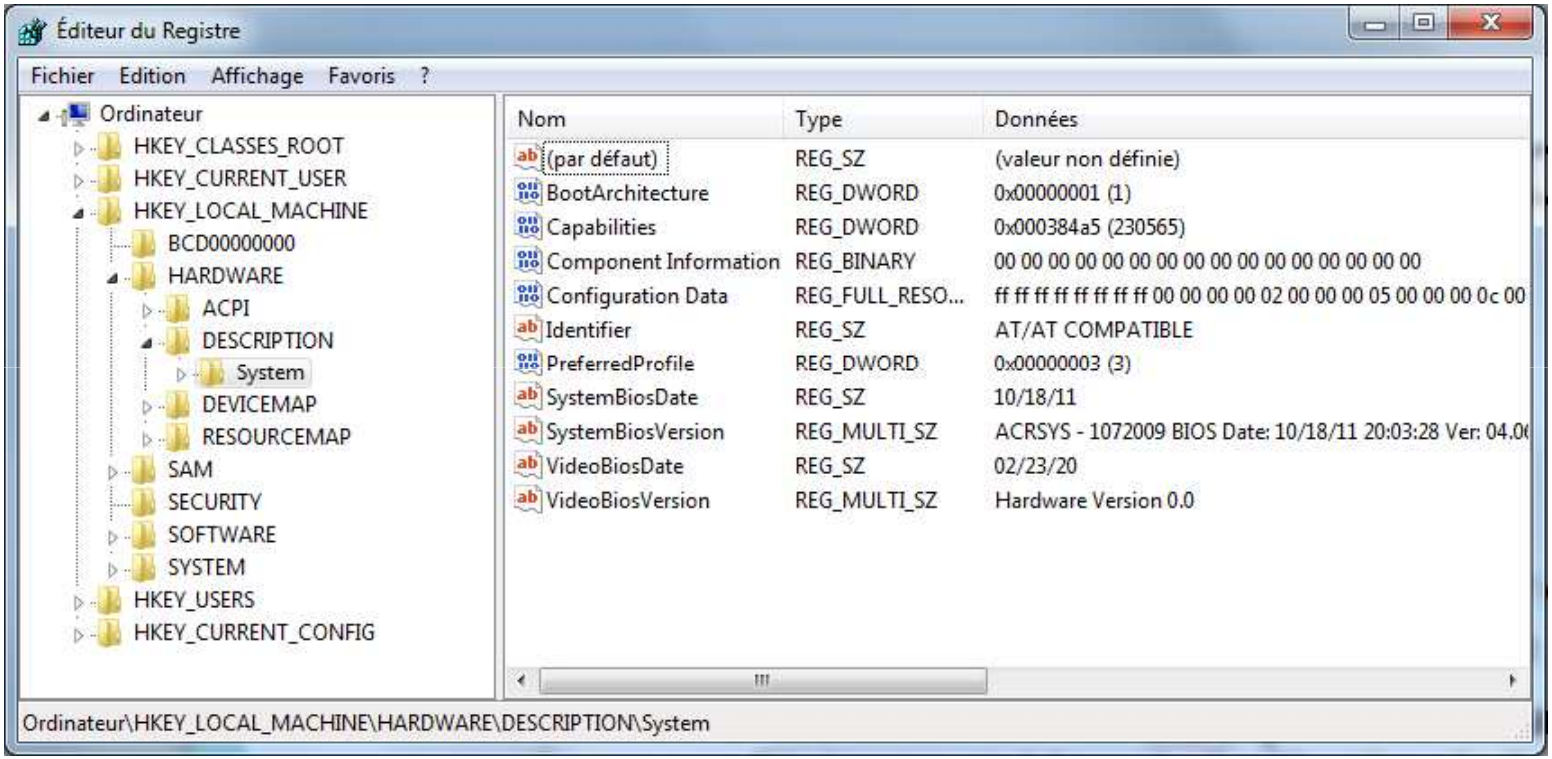
Une clé de registre

- **Les éléments d'une base de registre sont appelés Clé registre et ils sont constitués d'un nom, d'un type et d'une valeur, d'une date de modification et d'une ACL**
- **Principaux types de clés de registre:**

Type	Description
REG_NONE	Valeur non typée
REG_BINARY	Type binaire
REG_DWORD	Nombre sur 32 bits
REG_SZ	Chaine de caractère codée en UNICODE
REG_EXPAND_SZ	Chaine de caractère contenant des variables d'environnement ex : %Path%

LES ÉLÉMENTS CLÉS DE WINDOWS

Visualisation de la base de registre avec regedit.exe



LES ÉLÉMENTS CLÉS DE WINDOWS

Les fichiers de la base de registre

- La base de registre est stockée et répartie dans plusieurs fichiers différents.
- En dehors des clés utilisateur, les fichiers sont stockés dans : %SYSTEMROOT%/SYSTEM32/CONFIG

Fichier	Chemin
SAM	HKEY_LOCAL_MACHINE\SAM
SECURITY	HKEY_LOCAL_MACHINE\Security
SOFTWARE	HKEY_LOCAL_MACHINE\Software
SYSTEM	HKEY_LOCAL_MACHINE\System HKEY_CURRENT_CONFIG
DEFAULT	HKEY_USERS\.DEFAULT
Ntuser.dat (stocké dans : \Users\{username})	HKEY_CURRENT_USER

LES ÉLÉMENTS CLÉS DE WINDOWS

Les interruptions

- 3 types d'interruptions :
  - Processeurs (Ex : Divide by Zero) => Exception
  - Matérielle (IRQ : Interrupt ReQuest)
  - Logicielle : appel à un sous-programme (ex : Int 21h avec AH=2 permet d'afficher un caractère)
- Il n'y a pas de différence de traitement des interruptions. Lors d'une interruption, le système sauvegarde le contexte de l'application qui est en cours d'exécution avant d'exécuter la routine d'interruption. Quand le traitement de l'interruption est fini, le contexte de l'application est restauré et l'exécution reprend

LES ÉLÉMENTS CLÉS DE WINDOWS

Gestion des interruptions par Windows : IRQL

- Windows utilise des niveaux afin de définir des priorités au code exécuté : IRQL (Interrupt ReQuest Level)
- Tableau des niveaux IRQL :

Valeur x86	Valeur AMD64	Nom	Description
31	15	HIGH_LEVEL	Niveau le plus haut. Toutes les interruptions sont masquées (normalement jamais utilisé)
28	13	CLOCK_LEVEL	Interruption d'horloge
3 – 26	3 – 11	(DIRQL)	Interruptions matérielles
2	2	DISPATCH_LEVEL	C'est à ce niveau que s'exécutent les DPC (*Deferred Procedure Calls*)
1	1	APC_LEVEL	C'est à ce niveau que s'exécutent les APC (*Asynchronous Procedure Calls*)
0	0	PASSIVE_LEVEL	C'est à ce niveau que s'exécutent les threads en mode utilisateur et la plupart des threads en mode noyau

- Un thread utilisateur ne pourra pas s'exécuter tant qu'il y aura des interruptions avec un IRQL supérieur à 0

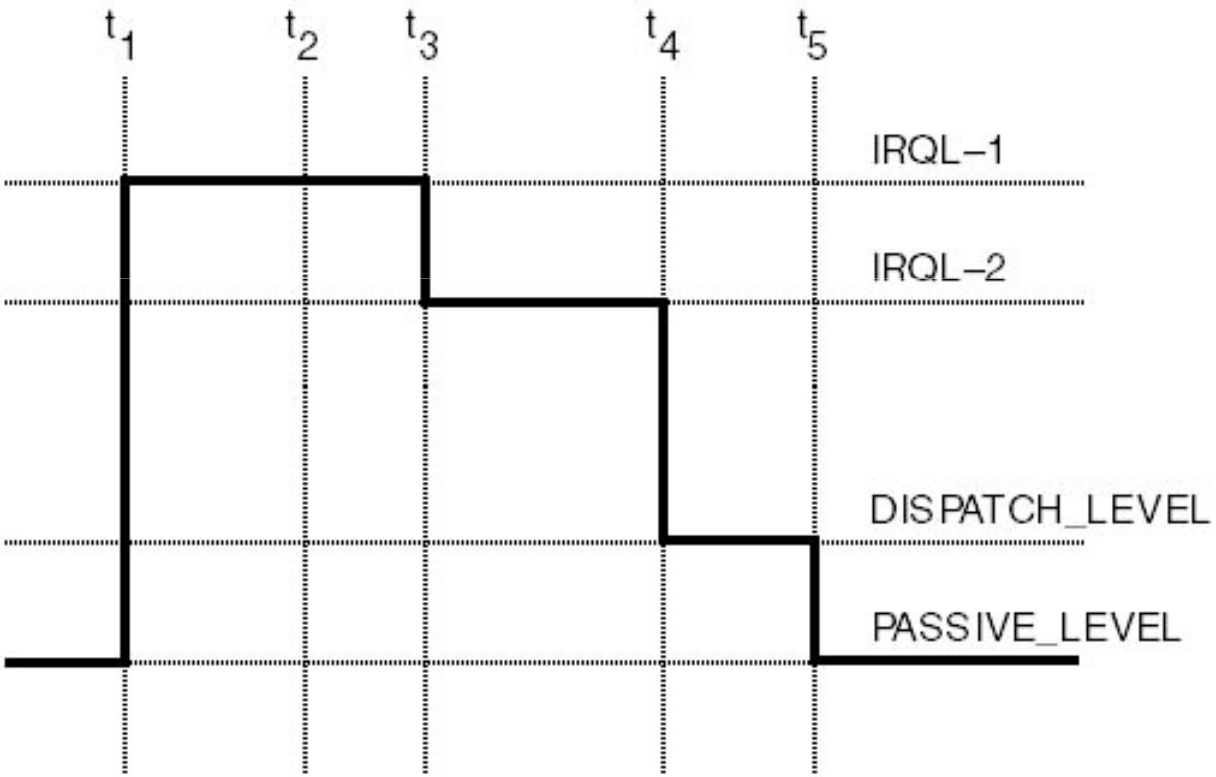
LES ÉLÉMENTS CLÉS DE WINDOWS

Interruption matérielle

- Lors d'une interruption liée à un matériel, l'IRQL est positionné à la valeur définie par le driver, plus aucun processus ou matériel avec une valeur inférieure ne peut l'interrompre
- Afin de réduire l'impact sur le reste du système, une première routine simple (ISR) met en file d'attente au niveau DISPATCH_LEVEL une routine DPC (Deferred Procedure Call)
- Les routines DPC sont des traitements plus longs mais avec un niveau plus bas, ce qui permet le traitement des interruptions d'autres matériels

LES ÉLÉMENTS CLÉS DE WINDOWS

Exemple d'interruption matérielle



LES ÉLÉMENTS CLÉS DE WINDOWS

Les exceptions

- Une exception est une interruption générée par le processeur lors d'une opération non valide
- Codes des exceptions les plus souvent rencontrés :

Numéro	Nom	Description
0	#DE	Division par zéro
3	#BP	Breakpoint (exécution de l'instruction INT3)
6	#UD	Opcode invalide (exécution d'une instruction inexistante)
8	#DF	Double faute (exception pendant la gestion d'une première exception)
11	#NP	Faute de segmentation (erreur liée aux registres de segments)
12	#SS	Faute de pile (débordement de la pile par exemple)
13	#GP	Faute de protection générale (toutes les fautes qui ne génèrent pas une autre exception)
14	#PF	Faute de page (tentative d'accès à une page non présente en mémoire)

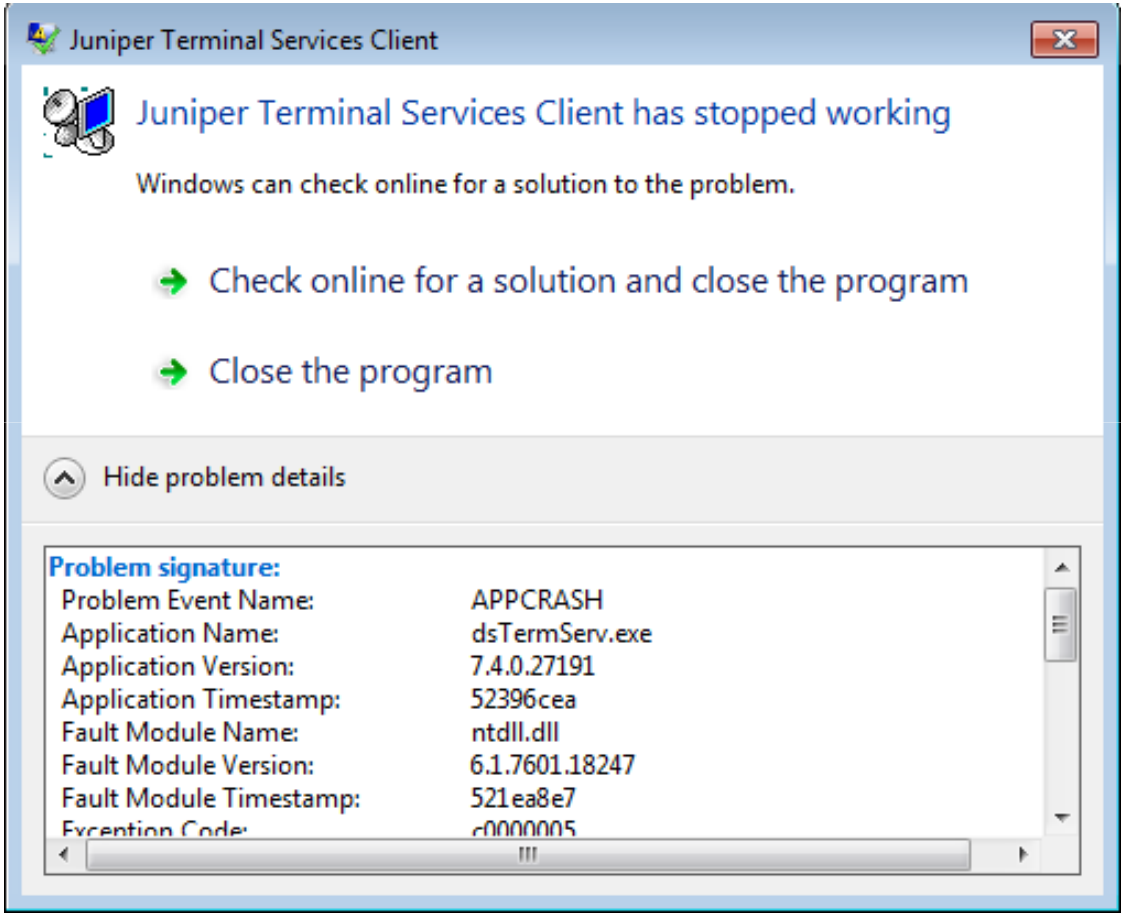
LES ÉLÉMENTS CLÉS DE WINDOWS

Traitement des exceptions

- Dans le mode utilisateur, si le programme est bien conçu, celui-ci est capable de traiter l'exception. Si le programme n'en n'est pas capable, le noyau va terminer le programme et informer l'utilisateur par un message : « Le programme a généré une exception … »
- Dans le mode noyau, si l'exception n'est pas gérée, c'est un arrêt du système avec le fameux BSOD
- Dans l'immense majorité, les BSODs sont liés à des erreurs de programmation des drivers qui s'exécutent en mode noyau ou à des erreurs de matériel, rarement à Windows NT lui-même. Un antivirus installe un drivers ;)

LES ÉLÉMENTS CLÉS DE WINDOWS

Exemple de message lors d'une exception applicative



LES ÉLÉMENTS CLÉS DE WINDOWS

Cas des défauts de page

- Le défaut de page est un cas particulier d'une exception
- Le noyau utilise un fichier de swap pour augmenter virtuellement la capacité physique de la mémoire vive. Lorsqu'un thread accède à une page mémoire qui n'est plus ou pas en mémoire physique, le processeur déclenche alors une exception de type défaut de page. Le noyau replace la page de mémoire demandée en mémoire et rend l'exécution au thread.
- C'est un cas d'exception qui est sans impact sur l'exécution de l'application (sauf pour les performances)

LES ÉLÉMENTS CLÉS DE WINDOWS

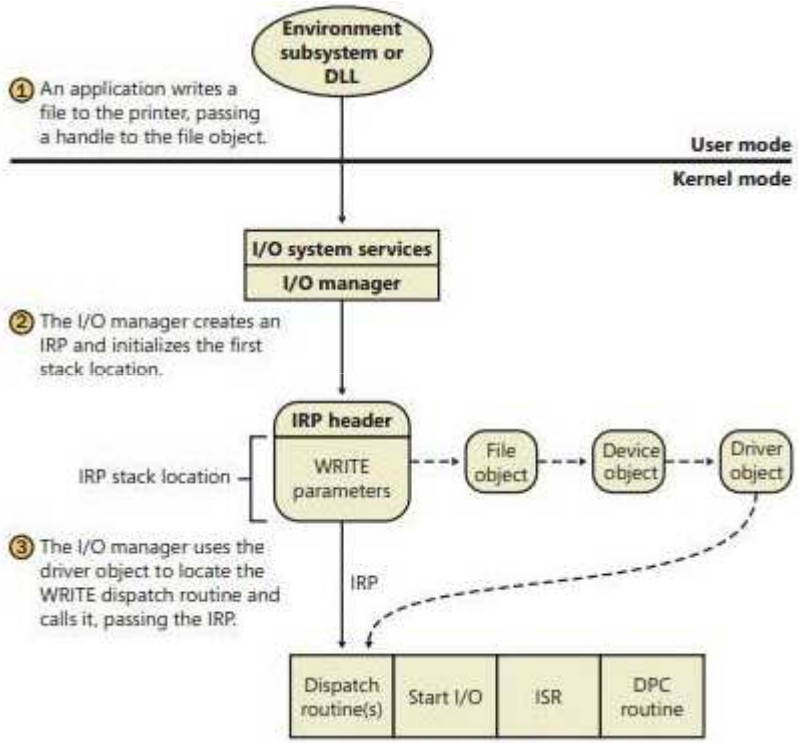
Les entrées / sorties

- Sous Windows NT, une opération de lecture, d'écriture ou d'échange particulier avec un périphérique se traduit par la construction par le système, d'une structure appelée IRP (I/O Request Packet)
- Un IRP contient toutes les données relatives à l'opération d'entrée/sortie
- Un IRP va passer de couche en couche (IO Manager -> NTFS -> Driver Disque). Chaque couche réalise si besoin un traitement sur l'IRP et un filtrage

⇒Un attaquant va essayer de passer au travers des filtres

LES ÉLÉMENTS CLÉS DE WINDOWS

IRP : Cas d'une écriture d'un fichier



- Utilisation de l'API : NtWriteFile
- Création de l'IRP
- Passage au système de fichier : NTFS.sys
- Passage au gestionnaire de partition : Partmgr.sys
- Passage au driver du disque: disk.sys
- Passage au driver du bus ATA : atapi.sys
- Ecriture sur le disque dur

LES ÉLÉMENTS CLÉS DE WINDOWS

L'interface graphique

- L'interface graphique de Windows gère le système de fenêtrage et les périphériques de type souris ou clavier
- Windows utilise des messages pour communiquer avec les applications pour signaler des évènements
- Exemples de message :
  - clic sur un bouton (WM_COMMAND)
  - touche clavier enfoncée (WM_KEYDOWN)
- Il existe environ 1200 types de messages
- Chaque thread possède une file d'attente de messages
- Le processus csrss.exe génère des messages liés au clavier et à la souris, les envoie aux applications et déplace le curseur de la souris à l'écran

LES ÉLÉMENTS CLÉS DE WINDOWS

Modèle de Sécurité de Windows NT

- Windows NT utilise deux éléments pour contrôler et restreindre les actions des utilisateurs :
  - Les privilèges : droits sur les actions
  - Une liste de contrôle d'accès (ACL) : droits d'accès sur un objet
- Ces éléments de sécurité sont regroupés dans un jeton qui est attaché à un processus lors de sa création

⇒L'un des principaux objectifs d'un attaquant est de réussir à modifier ce jeton pour augmenter ses privilèges

LES ÉLÉMENTS CLÉS DE WINDOWS

Les privilèges

- **Un privilège est une autorisation pour utiliser certaines fonctions du système**
- **Exemples de privilèges :**

Nom du privilège	Description
SeAssignPrimaryTokenPrivilege	Assigner un jeton d'accès à un processus
SeBackupPrivilege	Accéder à tous les fichiers en lecture même sans en avoir l'autorisation
SeCreateTokenPrivilege	Créer un jeton d'accès
SeDebugPrivilege	Déboguer n'importe quel processus et le noyau
SeIncreaseBasePriorityPrivilege	Augmenter la priorité d'exécution d'un processus ou d'une thread
SeIncreaseQuotaPrivilege	Ajuster les quotas d'un processus ou du registre
SeLoadDriverPrivilege	Charger (ou décharger) un driver en mémoire
SeRestorePrivilege	Accéder à tous les fichiers en écriture même sans en avoir l'autorisation
SeShutdownPrivilege	Éteindre ou redémarrer l'ordinateur
SeSystemtimePrivilege	Modifier la date et l'heure
SeTakeOwnershipPrivilege	Prendre possession de n'importe quel objet (fichier ou dossier par exemple)
SeTcbPrivilege	Effectuer des opérations très particulières normalement réservées au système
SeTimeZonePrivilege	Modifier le fuseau horaire de l'ordinateur

LES ÉLÉMENTS CLÉS DE WINDOWS

Les identifiants de sécurité SID

- Pour identifier un utilisateur, un groupe, une machine ou un domaine, Windows NT utilise un SID (Security Identifier)
- Un SID est structuré, voici un exemple :

  S-1-5-21-583907252-1078145449-1957994488-500

  - S-1 : une révision (1 : unique version pour l'instant)
  - 5 : un identifiant d'autorité (5 pour un compte Windows NT)
  - 21-583907252-1078145449-1957994488 : Identifiant du domaine ou de la machine, il est généré aléatoirement lors de l'installation de l'AD ou de Windows
  - 500 : Identifiant de l'utilisateur (RID : Relative ID)
- Certains SID sont réservés comme par exemple le groupe Virtuel « Tout le monde » : S-1-1-0

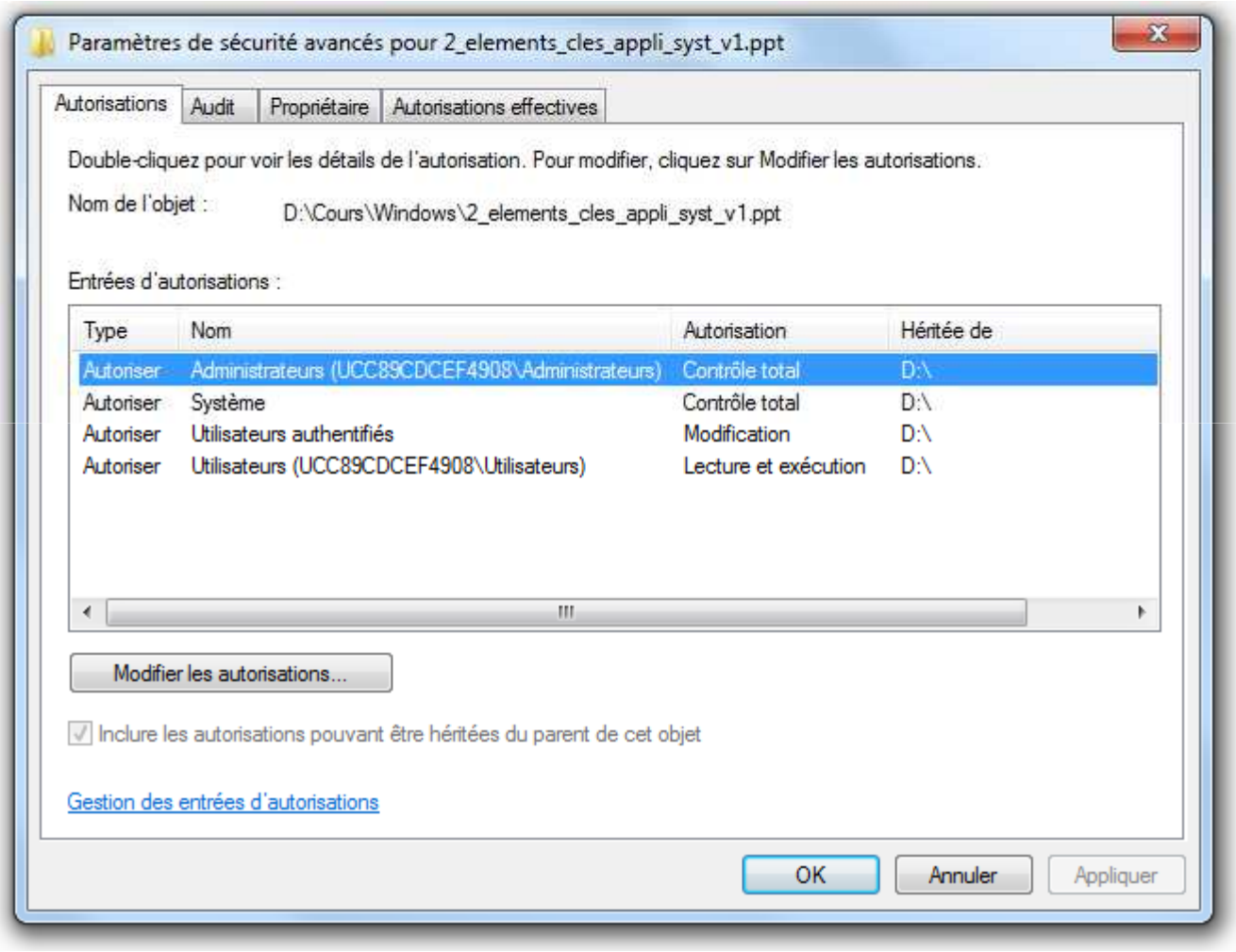
LES ÉLÉMENTS CLÉS DE WINDOWS

La sécurité des objets

- Le descripteur de sécurité d'un objet contient :
  - Un SID pour identifier son propriétaire
  - Un SID pour identifier à quel groupe il appartient
  - Une liste DACL (Discretionary Access Control List) contenant les SIDs qui vont avoir des autorisations de lecture, d'exécution et d'écriture ...etc
  - Une liste SACL (System Access Control List) contenant les SIDs qu'il faudra auditer (journaux d'événements) lors de l'utilisation de l'objet
- Si la liste DACL est vide, même l'administrateur ne pourra rien faire sur l'objet !
- Dans chaque liste un SID est soit autorisé, soit refusé; la priorité en cas de conflit est au refus

LES ÉLÉMENTS CLÉS DE WINDOWS

Exemple de gestion des droits sur un fichier



LES ÉLÉMENTS CLÉS DE WINDOWS

Ce qu'il faut retenir pour la suite

- La base de registre stocke la configuration de Windows
- Les exceptions en mode noyau génèrent les BSOD
- Les privilèges associés au jeton d'un processus définissent ses droits d'actions
- Les ACLs contiennent les droits des utilisateurs au format SID
- Les messages IRP permettent de communiquer avec les périphériques