

CONSTRUISONS **ENSEMBLE**  
LA DÉFENSE DE DEMAIN

# COURS WINDOWS ET LA SÉCURITÉ



# LES APPLICATIONS ET LE SYSTÈME



# LES APPLICATIONS ET LE SYSTÈME

## Introduction

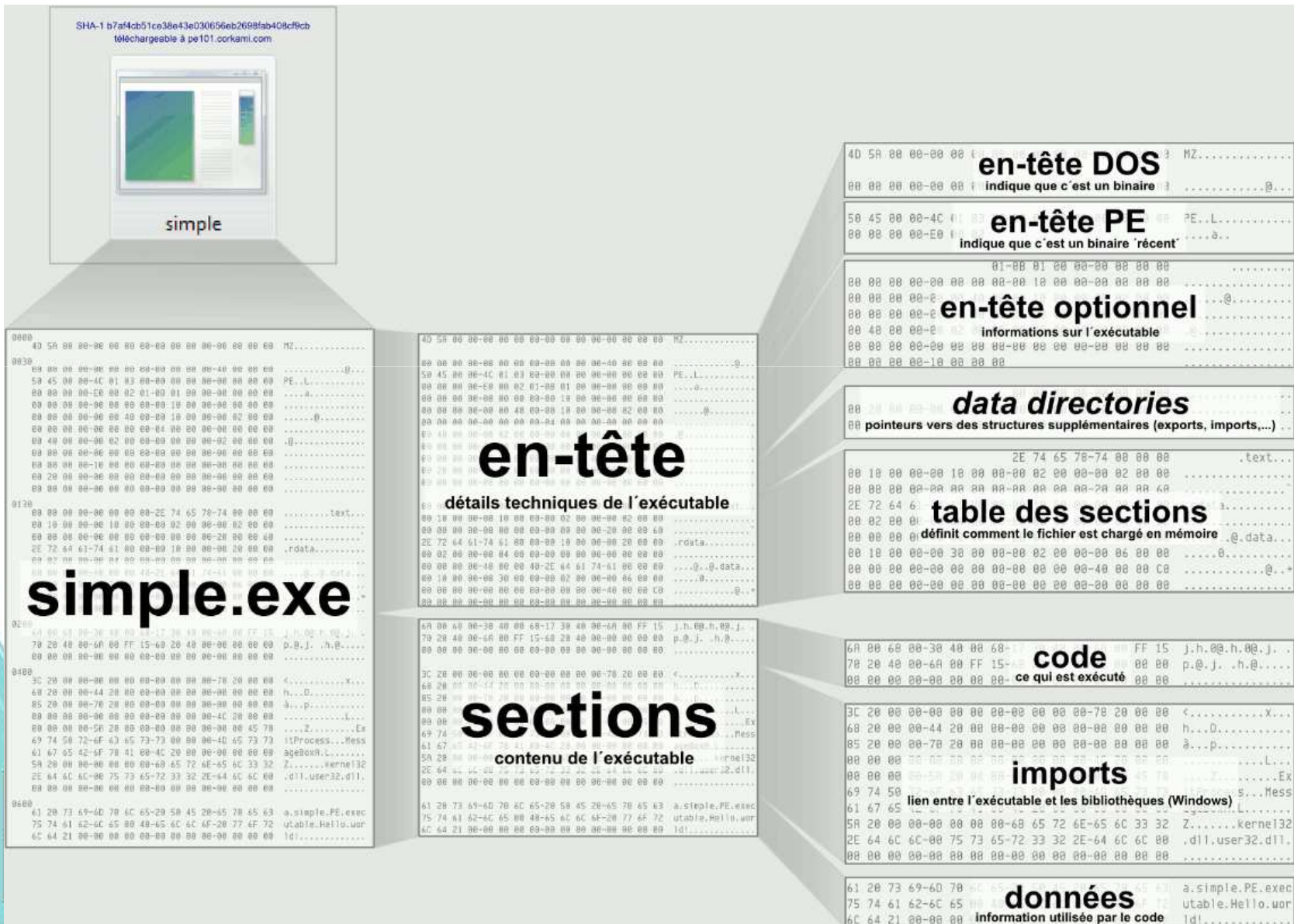
- Nous allons maintenant nous éloigner du cœur du système pour nous intéresser au fonctionnement des applications et des bibliothèques
- Nous allons aussi étudier les applications lancées en tâche de fond ainsi que les étapes du démarrage de Windows

# LES APPLICATIONS ET LE SYSTÈME

## Une application sous Windows NT

- Sous Windows NT, une application est un fichier exécutable qui est au format PE (Portable Executable)
- Le format PE est utilisé pour les fichiers suivants :
  - .exe (programme)
  - .dll (bibliothèque)
  - .sys (driver)
  - .ocx (OLE et ActiveX)
  - .cpl (élément panneau de configuration)
- PE est l'équivalent du format ELF sous Linux
- Le type de CPU et l'architecture (32 ou 64bits) d'un exécutable sont définis dans l'en-tête du PE

# Structure d'un exécutable PE



# LES APPLICATIONS ET LE SYSTÈME

## Les DLLs

- Les DLLs (Dynamic Link Library) sont des bibliothèques logicielles contenant des lots de fonctions autour d'un même sujet (ex: netapi32.dll pour l'API réseau)
  - Un exécutable utilise les DLLs du système pour communiquer (I/O, Réseau, Fenêtre, ...) ainsi que ses propres DLLs (souvent dans le même répertoire que l'exécutable)
  - Un défaut de DLL peut faire planter un exécutable si une fonction de la DLL est appelée
- => Une corruption de DLL fera réaliser des actions malveillantes par les exécutables qui l'utilisent**

# LES APPLICATIONS ET LE SYSTÈME

## La gestion des DLLs par le système

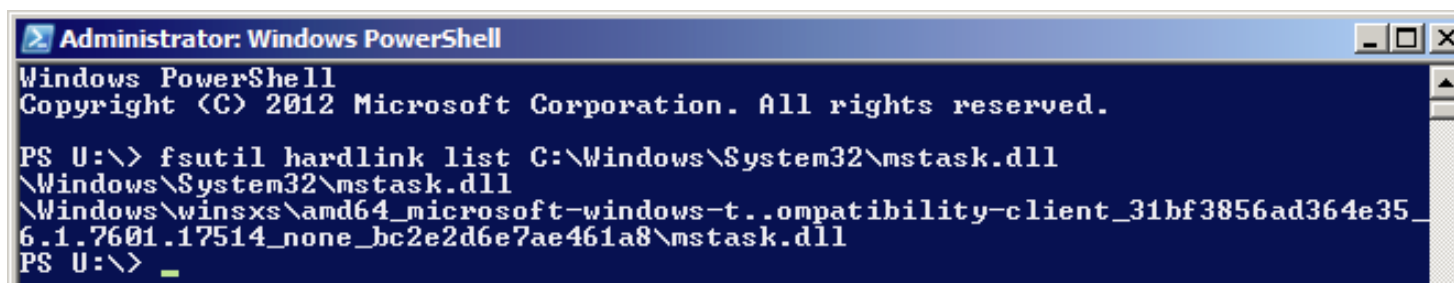
- Un risque d'incompatibilité d'une application qui a été compilée, testée sur une version d'une DLL et devient instable avec une autre version de la DLL
- Chaque application est conçue avec une version particulière de chaque DLL
- L'idée de WinSxS (Side-by-Side) est de garder les différentes versions de DLLs utilisées par les applications et le système



# LES APPLICATIONS ET LE SYSTÈME

## WinSxS

- Le repertoire %WINNT%\winsxs\ peut contenir, en plus des DLLs, l'ensemble des drivers et ressources système (service pack, mise à jour, etc ...)
- Windows s'appuie sur la fonction du système de fichier NTFS qui lui permet de réaliser des liens « Hardlink »
- Exemple de link :



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS U:\> fsutil hardlink list C:\Windows\System32\mstask.dll
\Windows\System32\mstask.dll
\Windows\winsxs\amd64_microsoft-windows-t..ompatibility-client_31bf3856ad364e35_6.1.7601.17514_none_bc2e2d6e7ae461a8\mstask.dll
PS U:\>
```

- Attention, volumétrie du répertoire important



# LES APPLICATIONS ET LE SYSTÈME

## Les applications en tâche de fond

- Windows NT utilise la notion de « service » pour les applications qui tournent en tâche de fond et qui fournissent des services au système et aux applications
- Un service est une application qui n'a pas d'interaction avec l'utilisateur, ni de fenêtre
- Un service est lancé par le système soit au démarrage, soit sur demande
- C'est l'équivalent des daemons sous Linux

# LES APPLICATIONS ET LE SYSTÈME

## Les services

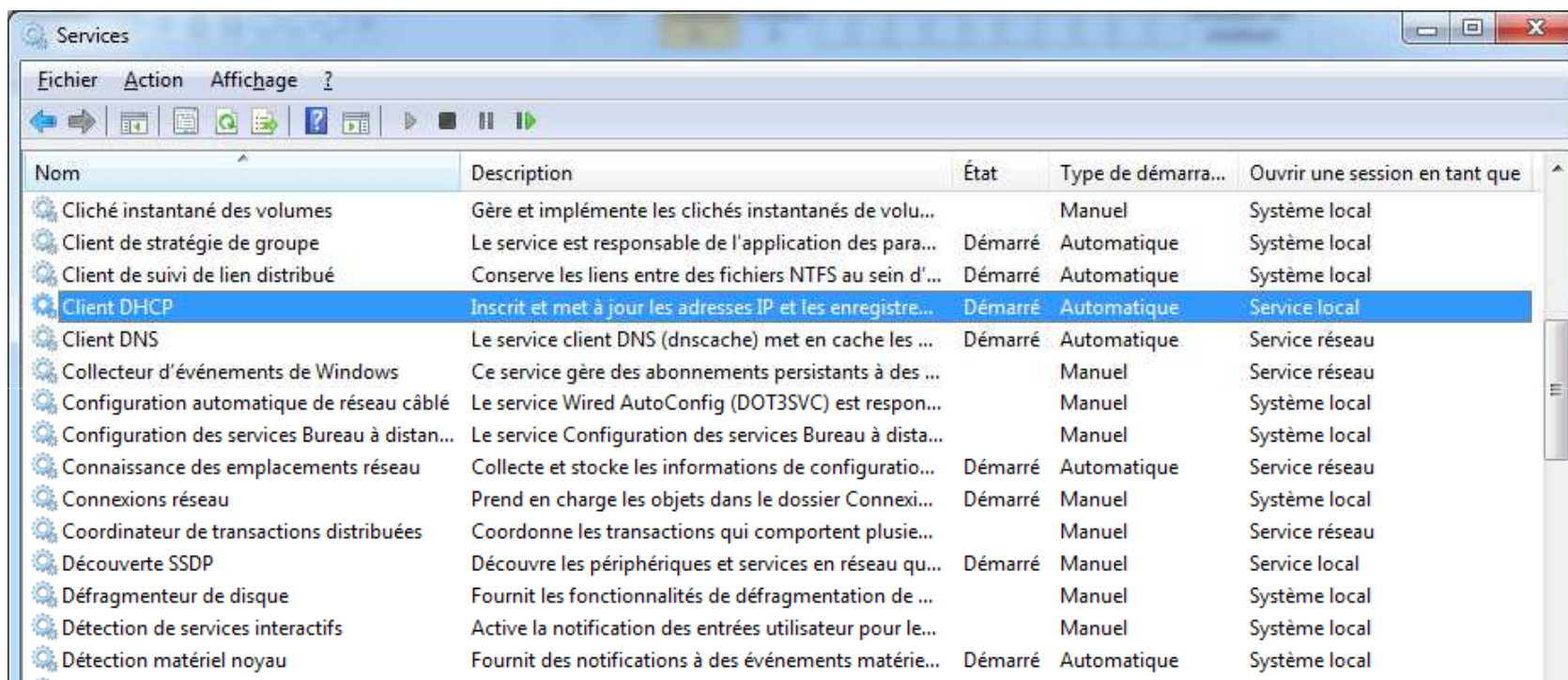
- Un service, comme une application est lancé sous l'identité d'un utilisateur avec des privilèges et des ACLs
- Les services sont souvent lancés sous l'utilisateur Administrateur
- Certains services fournissent des fonctionnalités de sécurité (ex : Pare-Feu, Antivirus, mise à jour , ...)

⇒ **Les services sont des cibles d'attaque, par exemple :**

- désactivation des services de protection
- exploitation d'une faille d'un service pour élever les privilèges
- lancement au démarrage d'un programme illégitime

# LES APPLICATIONS ET LE SYSTÈME

## Le gestionnaire de service

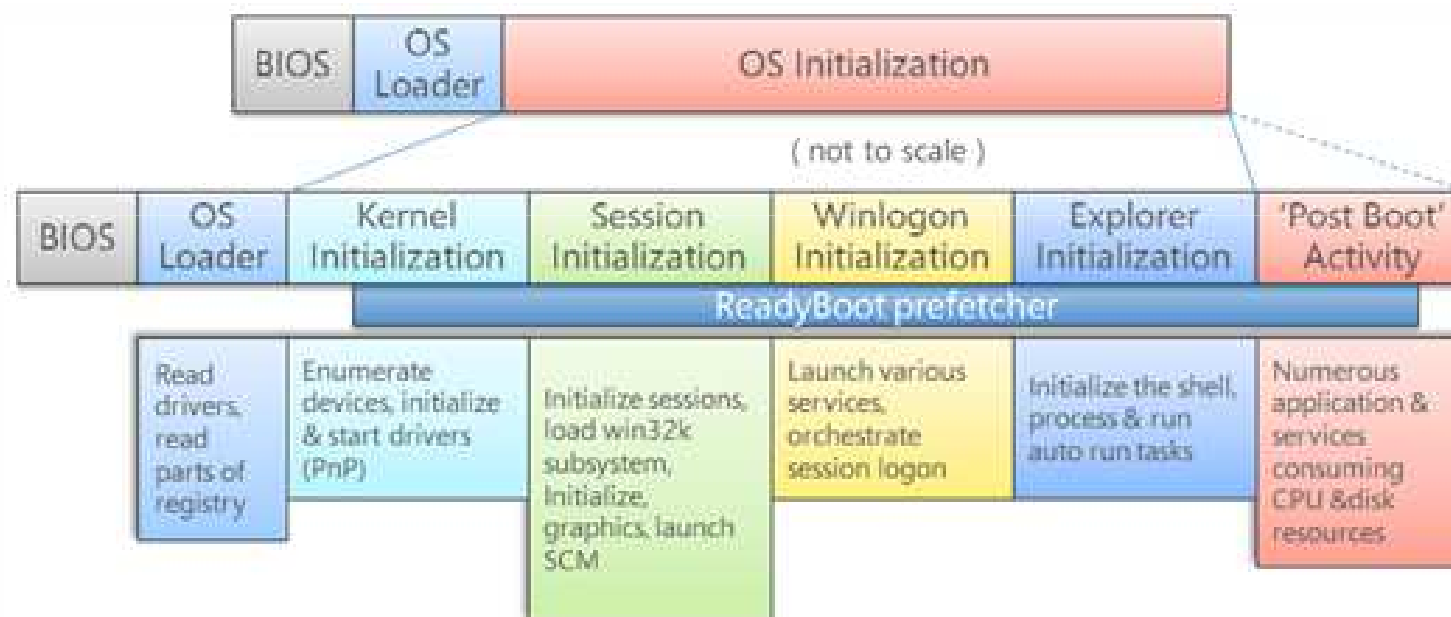


Nom	Description	État	Type de démarra...	Ouvrir une session en tant que
Clichié instantané des volumes	Gère et implémente les clichés instantanés de volu...		Manuel	Système local
Client de stratégie de groupe	Le service est responsable de l'application des para...	Démarré	Automatique	Système local
Client de suivi de lien distribué	Conserve les liens entre des fichiers NTFS au sein d'...	Démarré	Automatique	Système local
<b>Client DHCP</b>	<b>Inscrit et met à jour les adresses IP et les enregistre...</b>	<b>Démarré</b>	<b>Automatique</b>	<b>Service local</b>
Client DNS	Le service client DNS (dnscache) met en cache les ...	Démarré	Automatique	Service réseau
Collecteur d'événements de Windows	Ce service gère des abonnements persistants à des ...		Manuel	Service réseau
Configuration automatique de réseau câblé	Le service Wired AutoConfig (DOT3SVC) est respon...		Manuel	Système local
Configuration des services Bureau à distan...	Le service Configuration des services Bureau à dista...		Manuel	Système local
Connaissance des emplacements réseau	Collecte et stocke les informations de configuratio...	Démarré	Automatique	Service réseau
Connexions réseau	Prend en charge les objets dans le dossier Connexi...	Démarré	Manuel	Système local
Coordinateur de transactions distribuées	Coordonne les transactions qui comportent plusie...		Manuel	Service réseau
Découverte SSDP	Découvre les périphériques et services en réseau qu...	Démarré	Manuel	Service local
Défragmenteur de disque	Fournit les fonctionnalités de défragmentation de ...		Manuel	Système local
Détection de services interactifs	Active la notification des entrées utilisateur pour le...		Manuel	Système local
Détection matériel noyau	Fournit des notifications à des événements matéri...	Démarré	Automatique	Système local

# LES APPLICATIONS ET LE SYSTÈME

## Les étapes de démarrage de Windows NT

- Le Bios ou l'UEFI exécute un « Boot Loader » qui a pour rôle d'accéder au noyau sur le disque et de l'exécuter



# LES APPLICATIONS ET LE SYSTÈME

## Emplacements de démarrage automatique

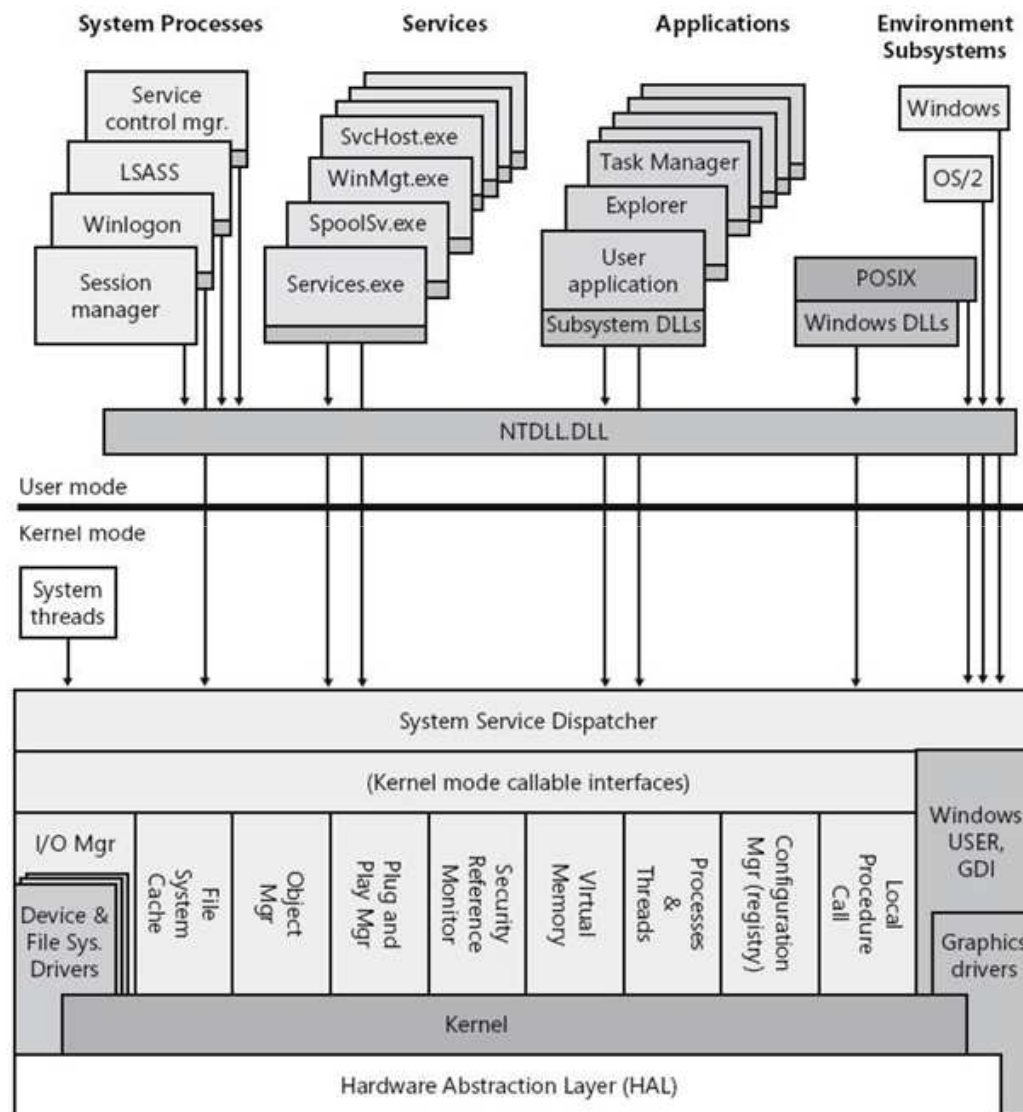
- **Boot Loader (sauf dans le mode Secure Boot)**
- **Base de registre :**
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
- **Fichiers :**
  - %USERPROFILE%\Start Menu\Programs\Startup\
  - %ALLUSERSPROFILE%\Start Menu\Programs\Startup\
- **Les services**
- **Les drivers**

**=> Les emplacements de démarrage sont la cible des malwares et des attaquants afin d'être persistants**



# LES APPLICATIONS ET LE SYSTÈME

## Synthèse



Hardware interfaces (buses, I/O devices, interrupts, interval timers, DMA, memory cache control, etc.)

# LES APPLICATIONS ET LE SYSTÈME

Ce qu'il faut retenir pour la suite

- Les binaires sont au format PE
- Une application utilise les librairies DLL du système pour communiquer avec Windows
- Les services sont lancés au démarrage et tournent en tâche de fond pour apporter des fonctionnalités à Windows NT
- Windows démarre des applications automatiquement à partir de nombreux emplacements