CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

INTRODUCTION

INTRODUCTION
Présentation personnel

- Mon parcours professionnel en quelques mots

- Actuellement : Expert technique en Lutte Informatique Défensive à DGA MI dans le laboratoire Technique de Détection

INTRODUCTION
Présentation de DGA-MI

- « DGA Maîtrise de l'information est l'expert technique du ministère de la Défense pour la maîtrise de l'information, la cybersécurité, la guerre électronique et les systèmes de missiles. »

- Points clés :
  - Héritier du CELAR et du LRBA
  - 1 250 personnes sur site, 2/3 d'ingénieurs
  - 60 M€ d'achats annuels, dont 30 M€ en région Bretagne
  - Situé à Bruz, à 15 km de Rennes, sur un site de 100 ha

INTRODUCTION
Activités du LABO TD de DGA-MI

- Etude des produits de détection d'intrusion
- Conception d'architecture de détection
- Contribution aux programmes d'armement en apportant la composante de détection
- Expertise des solutions déployées
- Accompagnement technique des programmes d'investissements des industriels (PIA, Rapid, …)
- Veille technologique (attaque, défense & détection)

INTRODUCTION

Usages de Windows au Ministère de la Défense

- Utilisation massive de Windows dans le parc informatique et sur le théâtre des opérations
- Différents types de risques : physique, logiciel, humain, nomadisme, compatibilités, …
- Fortes contraintes opérationnelles : MCO (Maintien en Condition Opérationnelle), MCS (Maintien en Condition de Sécurité), protection de données, disponibilité
- De plus Windows est présent sur certains socles de produits de sécurité intégrés dans la supervision de la sécurité

⇒ Il est indispensable de comprendre le fonctionnement interne de Windows pour sécuriser et détecter des attaques

INTRODUCTION
Plan - Jour 1

- Introduction
- Historique de Windows
- Architecture interne
- Les éléments clés de Windows
- Les applications et le système
  - TP : Découverte des binaires et des DLLs. Exploiter une faille pour élever les privilèges. Manipulation de la base de registre. Manipulation d'un emplacement de démarrage auto. Manipulation des services. Générer un BSOD
- Mécanismes de protection de Windows
  - TP : Mise à jour de Windows . Signature des binaires et des drivers. Chiffrement de volume. Analyse mémoire. Désinstallation d'un patch

INTRODUCTION
Plan - Jour 2

- **Gestion des comptes locaux**
  - TP : Les privilèges utilisateurs. Attaque du processus lsass.exe . Injection de code à la volée. Modification hors-ligne de la base SAM. Crackage de mot de passe par table Rainbow
- **Le système de fichiers NTFS**
  - TP : Lecture d'un fichier hors ligne. Récupération d'un fichier effacé
- **Infrastructure Réseau**
  - TP : Création d'un domaine AD. Création d'un utilisateur dans l'AD. Création d'un partage de fichiers. Intégration d'un poste sur l'AD
- **Les Malwares**
  - TP : Récupérer les mots de passe des applications . Nettoyage d'un ranconware. Process explorer et Virus Total

HISTORIQUE DE WINDOWS

HISTORIQUE DE WINDOWS
Microsoft

- Paul Allen et Bill Gates entourés de “Personal Computer”

- En 1975 ils créent l’entreprise Microsoft

HISTORIQUE DE WINDOWS

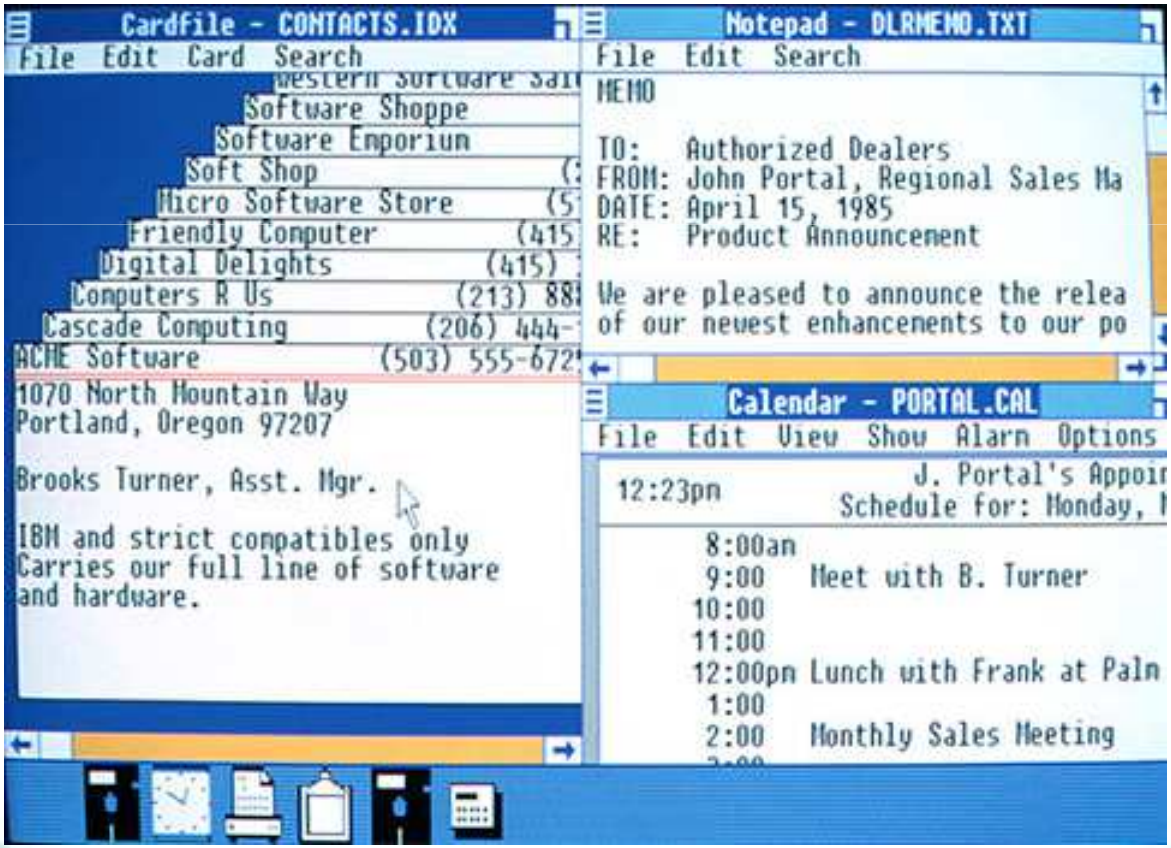
Avant Windows

- Création en 1981 de MS-DOS 1.0 (Microsoft Disk Operating System)
- Caractéristiques :
  - Fonctionne en mode réel (pas de protection de la mémoire, des I/O et du BIOS; adressage mémoire limité à 1Mo)
  - Mono-tâche et donc mono-utilisateur (un programme doit se finir avant le lancement d'un autre)
  - Son interface est en ligne de commande
- MS-DOS 6.22 sorti en 1994 sera la dernière version autonome, les suivantes seront intégrées à Windows

HISTORIQUE DE WINDOWS

Naissance de Windows

- **Windows 1.0 est sorti en 1985 : limité à une interface graphique au dessus de MS-DOS**



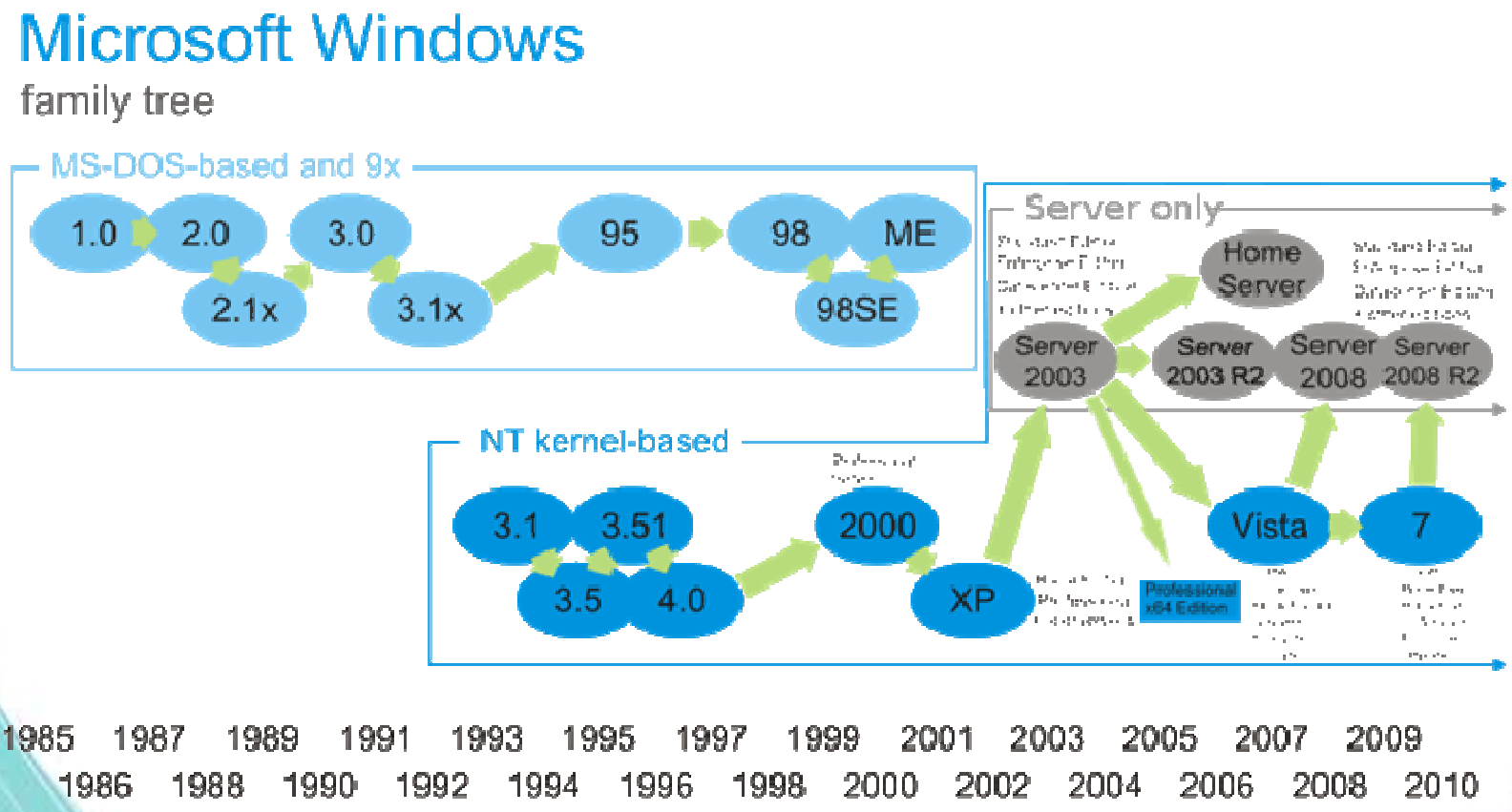
HISTORIQUE DE WINDOWS

Windows NT

- La première version de Windows NT (New Technology) est lancée en 1993 et ne repose plus sur MS-DOS
- Caractéristiques :
  - Multi-tâche préemptif (partage du temps d'exécution)
  - Multi-utilisateur
  - Multi-processeur
  - Multi-architecture (ia-32, MIPS, PowerPC, Itanium, x86-64,…)
  - Mode protégé avec des niveaux de privilèges (Kernel/User)
- Windows XP (NT 5.1) est la première version grand public
- La dernière version, Windows 10 (NT 10.0) a été lancée le 29/07/2015

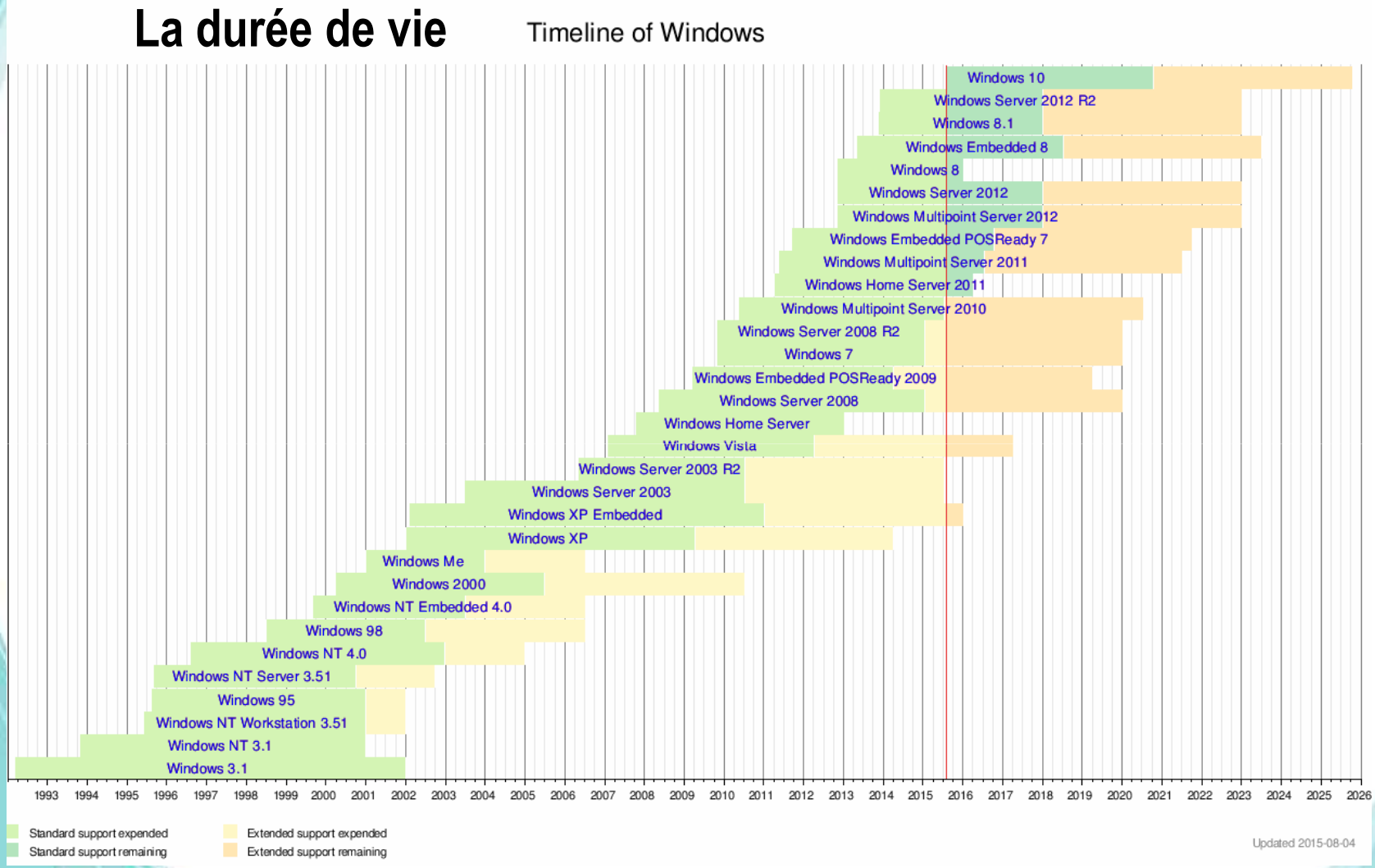
HISTORIQUE DE WINDOWS

Les différentes versions de Windows



HISTORIQUE DE WINDOWS

La durée de vie

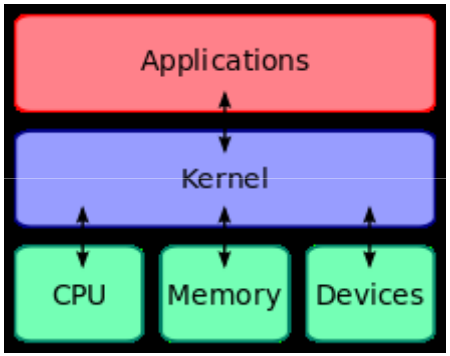


ARCHITECTURE INTERNE

ARCHITECTURE INTERNE

(Rappel) Les Noyaux

- Le noyau permet de gérer les ressources de l'ordinateur ainsi que les communications des matériels et des applications



- Le noyau permet l'accès aux ressources qu'il gère au travers d'appels système
- Il réalise une abstraction des ressources

ARCHITECTURE INTERNE

(Rappel) Les Modes ou Espaces d'un OS

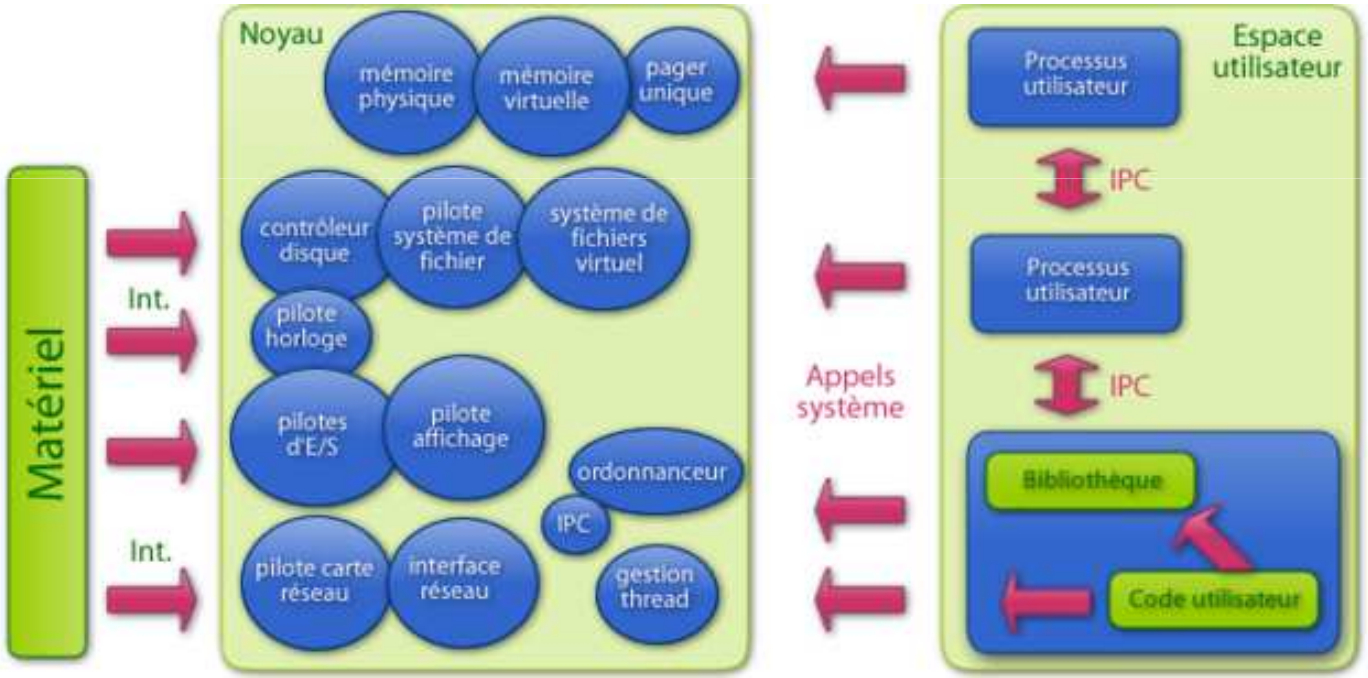
- **Les espaces permettent de protéger les données et les fonctionnalités en s'appuyant sur les modes « privilégiés » des CPUs**

	Noyau (Ring 0)	Utilisateur (Ring 3)
Instructions CPUs	Sans restriction	Réduit
Mémoire	Adressage et accès complet	Adressage Virtuel réduit et droits d'accès limités
Temps d'exécution	Sans limite	Période limitée
Entrée / Sortie	Accès complet	Pas d'accès direct
Crash lors de l'exécution	« Kernel Panic » ou « BSOD »	Le noyau tue le process

ARCHITECTURE INTERNE

(Rappel) Différents types de noyaux

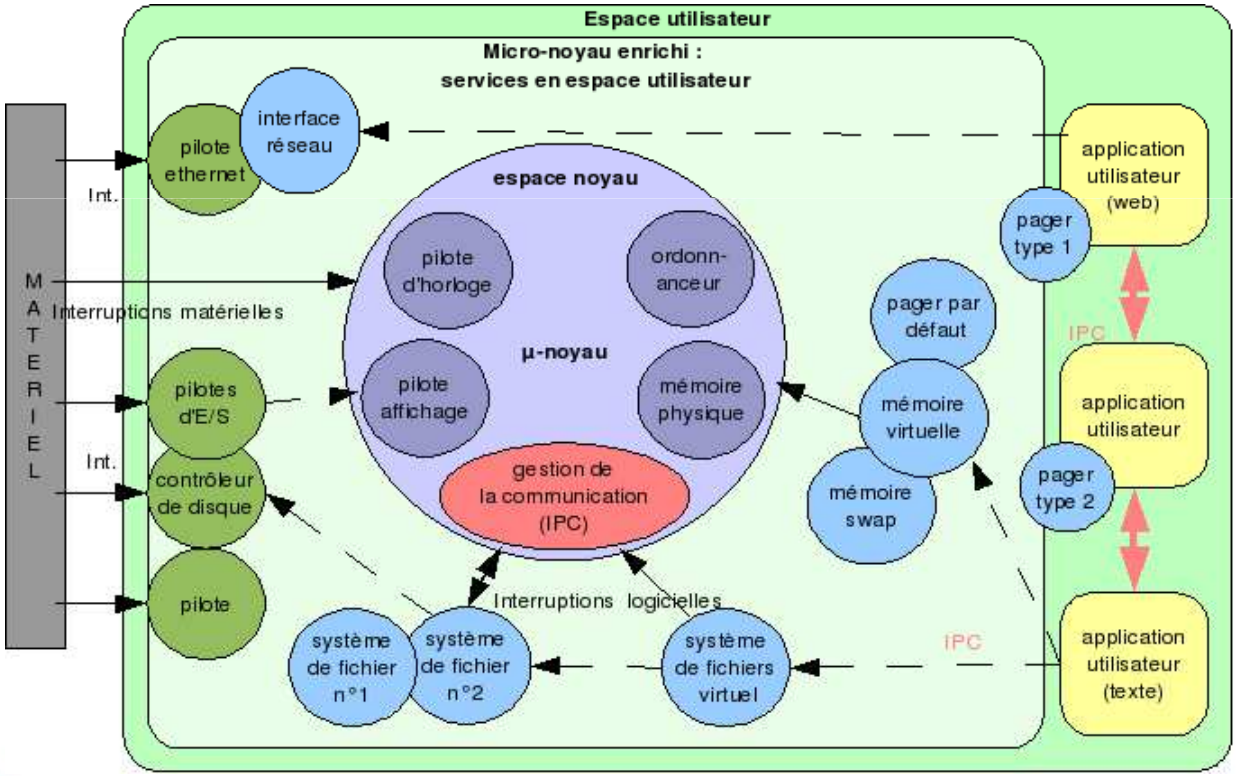
- **Noyau monolithique : centralise dans le noyau l'ensemble des fonctionnalités et des pilotes. (ex : Linux)**



ARCHITECTURE INTERNE

(Rappel) Différents types de noyaux

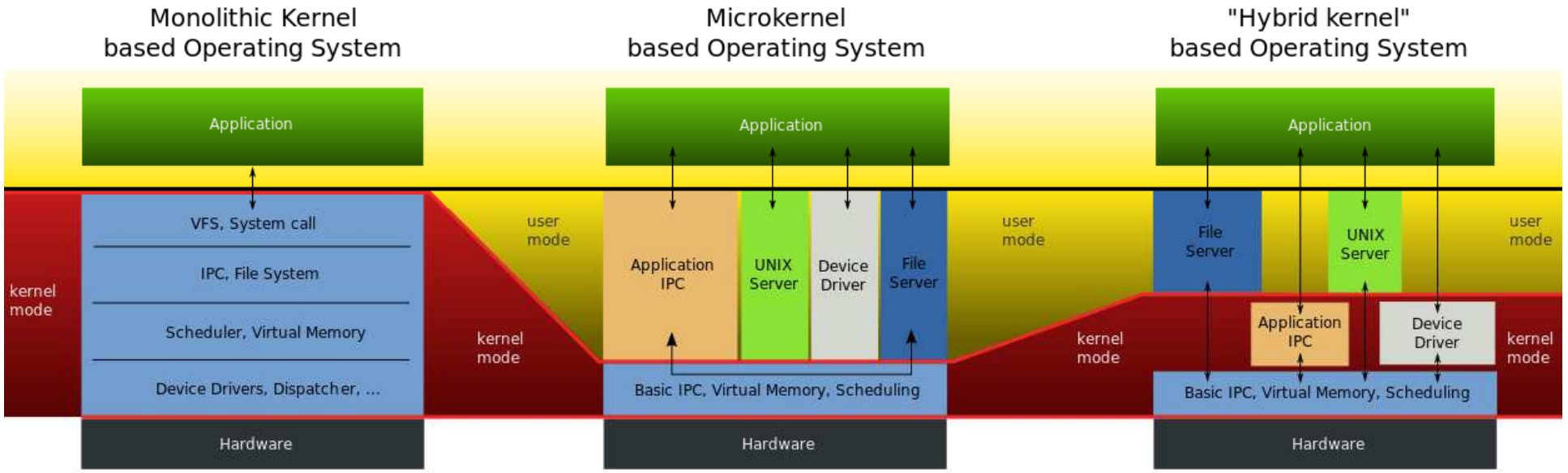
- **Micronoyau : Nombre minimaliste de fonctions, le reste est réalisé par des services en espace utilisateur**



ARCHITECTURE INTERNE

(Rappel) Différents types de noyaux

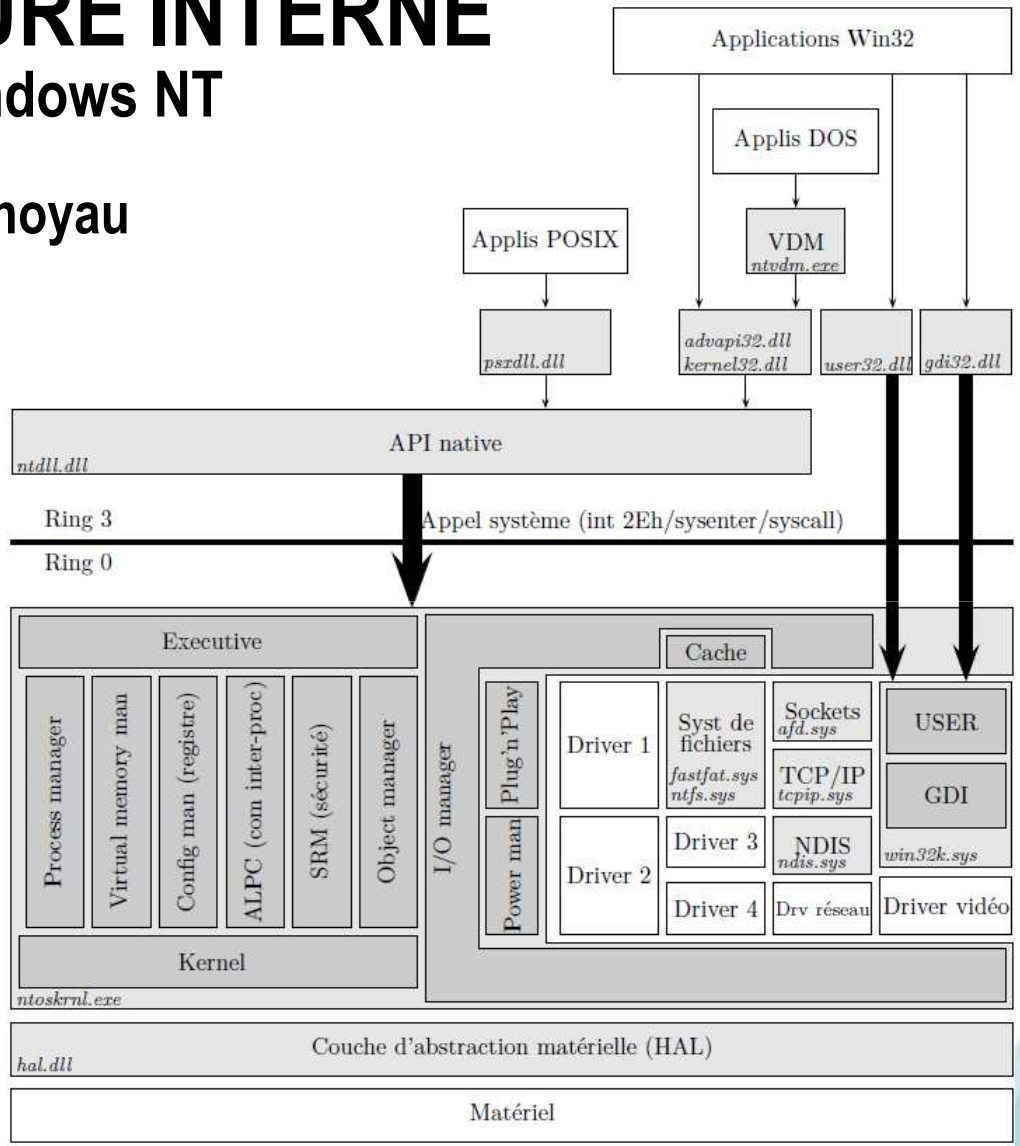
- **Noyau hybride : savant mélange des deux approches**



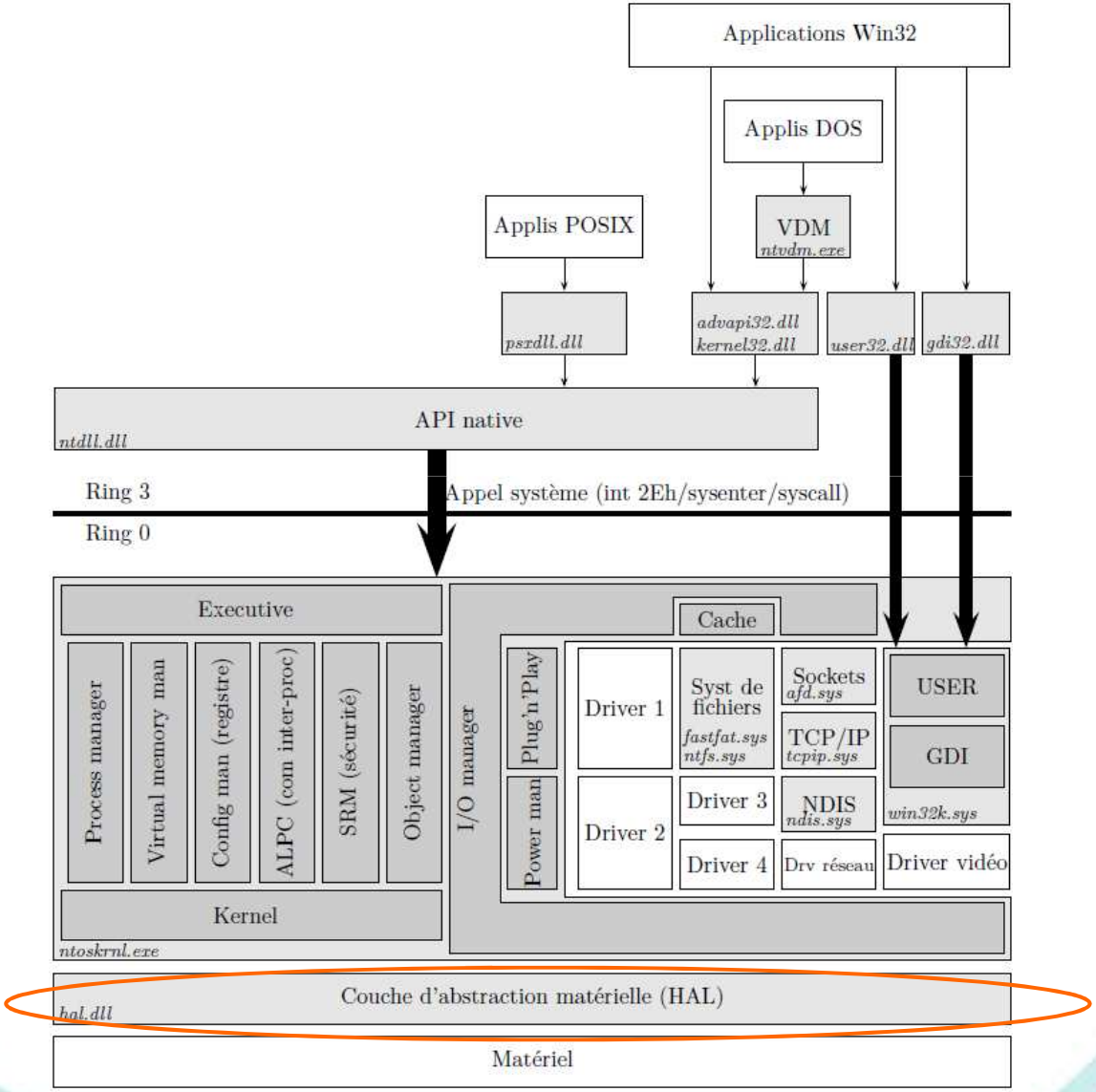
ARCHITECTURE INTERNE

Architecture de Windows NT

- Windows NT est un noyau hybride (ou enrichi)
- Il est découpé en plusieurs fonctions :
  - HAL
  - Micronoyau
  - Executive Service
  - Drivers WDM
  - Des APIs (Application Programming Interface) de communication pour l'espace utilisateur



ARCHITECTURE INTERNE
HAL

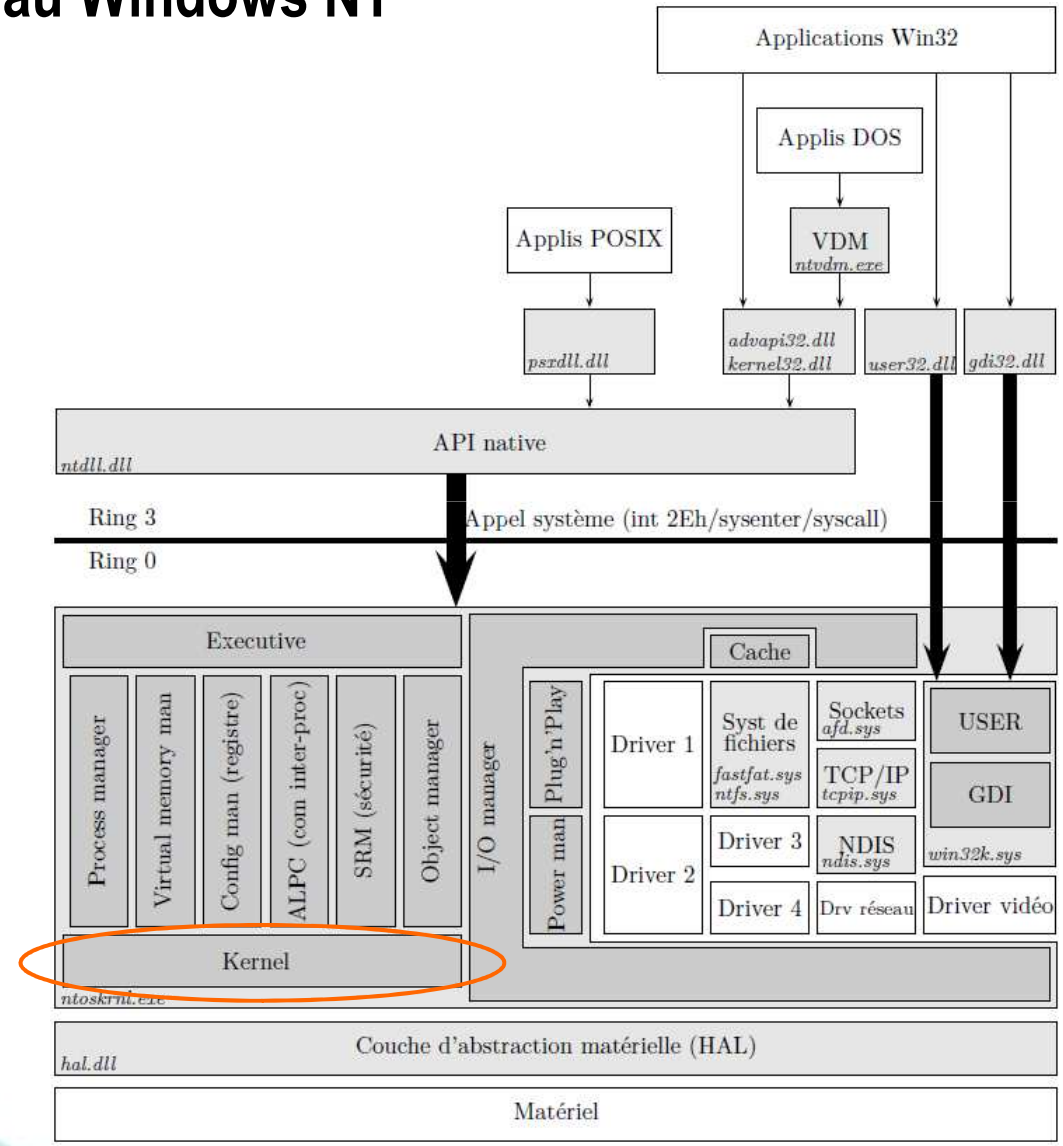


ARCHITECTURE INTERNE
Hardware Abstraction Layer

- Couche d'abstraction permettant de standardiser l'accès au matériel en cachant les spécificités du matériel
- Cela permet de faire tourner Windows NT sur une architecture x86 ou ARM (ex : Windows Mobile 8)
- Fonctionnalités fournies par HAL:
  - API générique
  - Commutation de contexte et synchronisation
  - Manipulation des interruptions et de l'horloge système
  - Gestion de l'ordre des octets (*big-endian* & little-endian)
  - Gestion de la MMU (memory management unit)

ARCHITECTURE INTERNE

Micronoyau Windows NT



ARCHITECTURE INTERNE

Micronoyau Windows NT

- Ecrit en assembleur, ne peut pas être « Swappé » ni préempté
- Réalise l'ordonnancement des « threads », gère les interruptions et surtout les exceptions

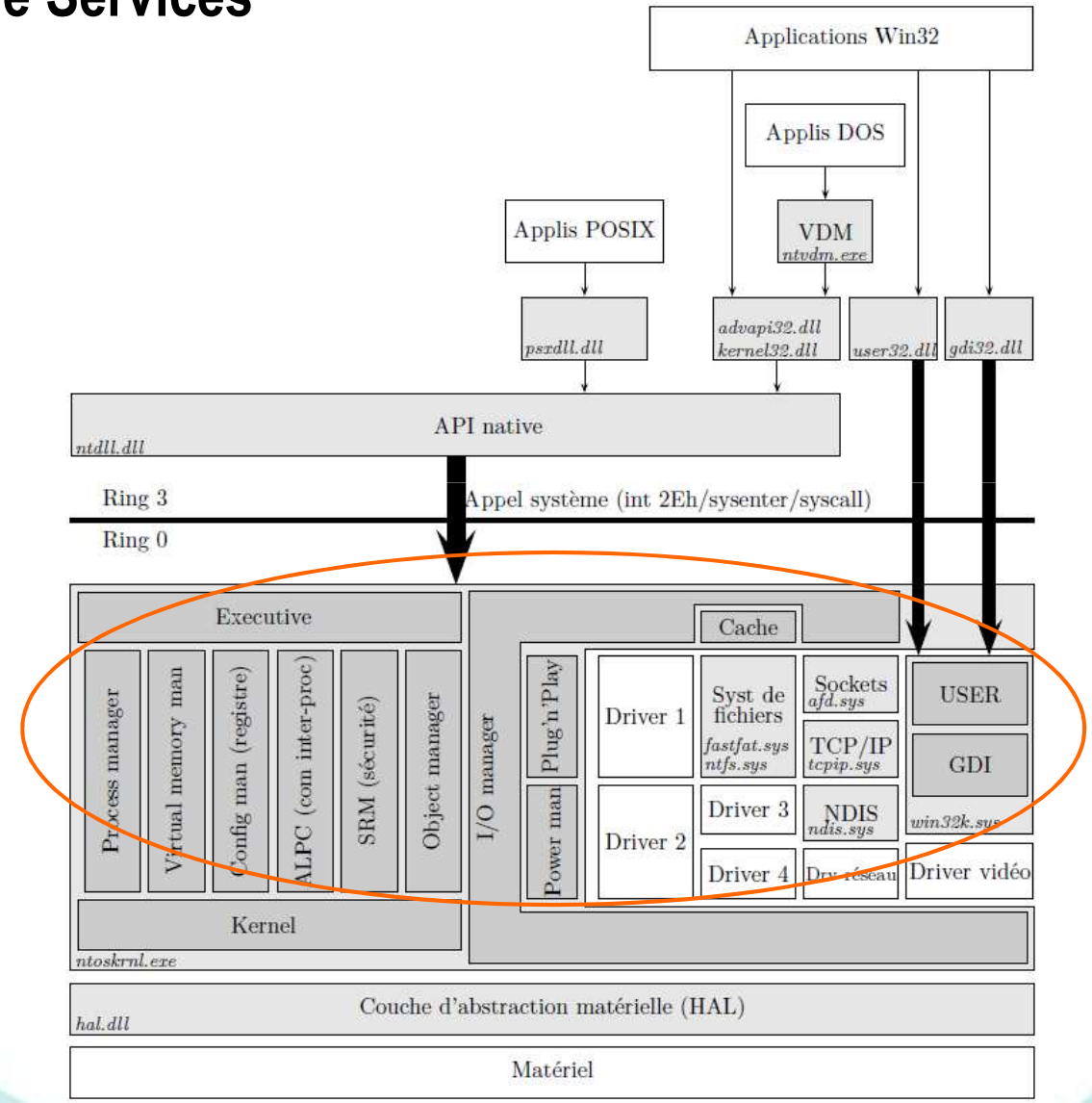

Un problème a été détecté et Windows a été arrêté afin de prévenir tout dommage sur votre ordinateur.
Si vous voyez cet écran d'erreur d'arrêt pour la première fois, redémarrez votre ordinateur. Si cet écran apparaît encore, suivez ces étapes :
Assurez-vous de disposer de suffisamment d'espace disque. Si un pilote est identifié dans le message d'arrêt, désactivez le pilote ou contactez le fabricant pour obtenir les mises à jour du pilote. Essayez de remplacer la carte vidéo.
Consultez votre revendeur de matériel pour obtenir toutes mises à jour du BIOS. Désactivez les options de mémoire du BIOS telles que la mise en cache ou l'ombrage. Si vou êtes obligé d'utiliser le Mode sans échec pour supprimer ou désactiver des composants, redémarrez votre ordinateur, appuyez sur F8 pour sélectionner les options de dé arrage avancées, puis sélectionnez le Mode sans échec.
Informations techniques :
*** STOP: 0x0000008E (0xC0000005,0x804EF15A,0xBA503578,0x00000000)
Début du vidage de la mémoire physique.
vidage de la mémoire physique vers le disque : 42

ARCHITECTURE INTERNE
Micronoyau Windows NT

- Ecrit en assembleur, ne peut pas être « Swappé » ni préempté
- Réalise l'ordonnancement des « threads », gère les interruptions et surtout les exceptions (BSOD)
- Distribue la charge sur une architecture multi-cpu afin d'occuper chaque processeur constamment
  - Priorisation des threads
  - Préemption et changement de contexte du code réentrant
- Synchronise le fonctionnement des « Windows NT Executive Services » : programmes en mode noyau qui fournissent des services de base au système

ARCHITECTURE INTERNE

Executive Services

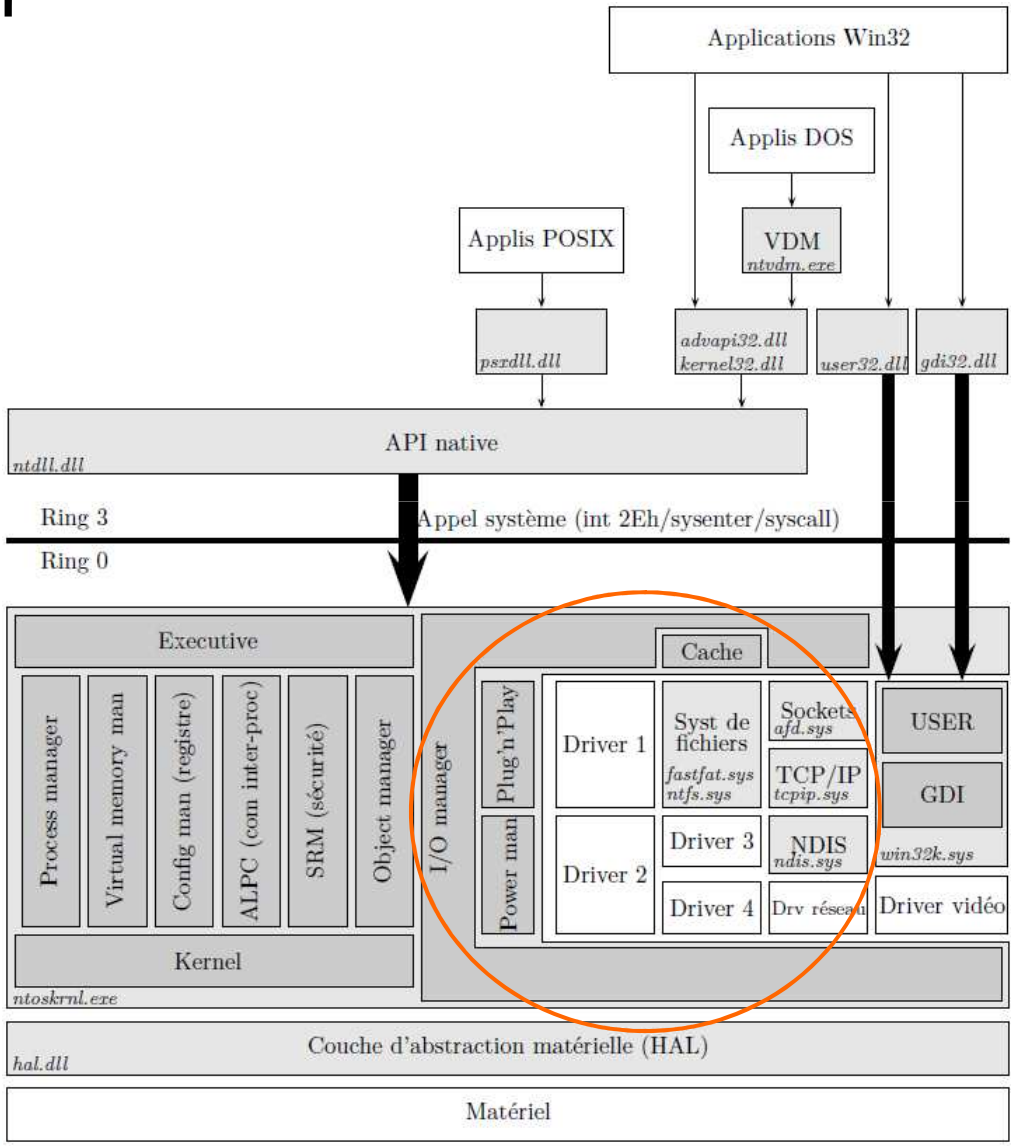


ARCHITECTURE INTERNE
Windows NT Executive Services

- Programmes en mode noyau
- Fournit des services de base au système :
  - I/O Manager
  - Object Manager
  - Security Ressource Manager
  - Process Manager
  - Local Procedure Call
  - Virtual Memory Manager
  - Graphic Manager (USER & GDI)

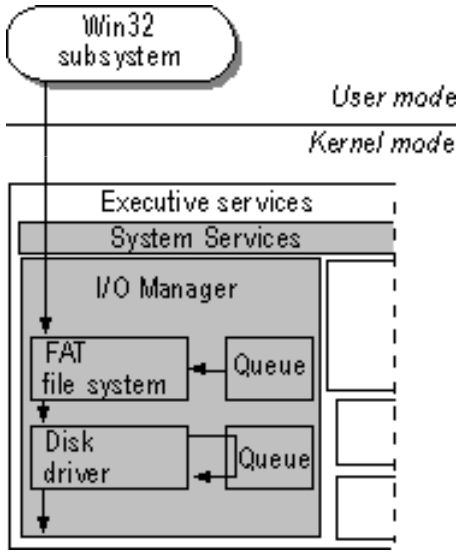
ARCHITECTURE INTERNE

I/O Manager



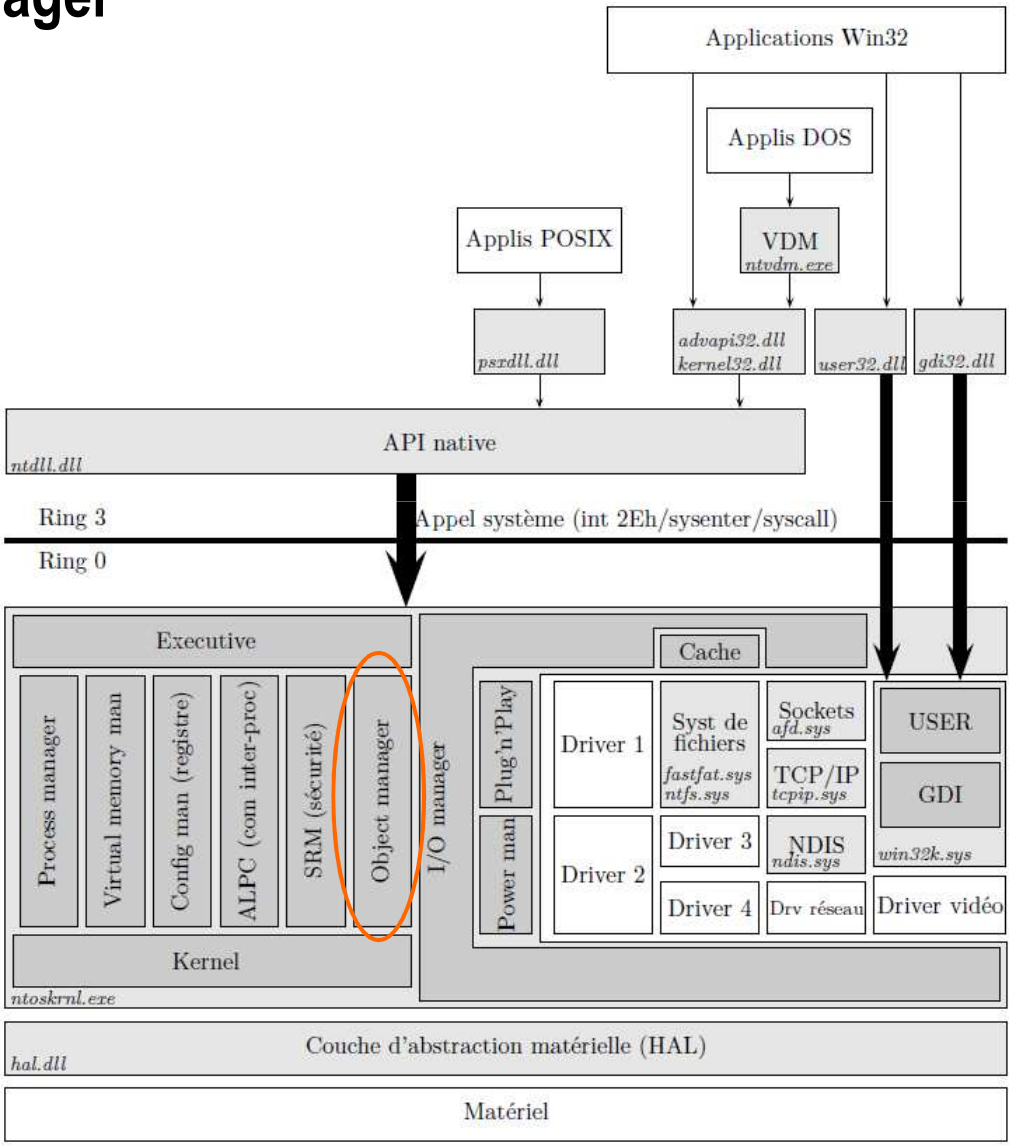
ARCHITECTURE INTERNE
I/O Manager

- Gère les entrées/sorties en s'appuyant sur des sous-couches fonctionnelles
- Permet de gérer différentes fonctions :
  - Système de fichiers
  - Cache disque
  - Redirecteurs réseau
  - Communication entre les drivers
- Communique par des messages de type IRP (I/O Request Packets)



ARCHITECTURE INTERNE

Object Manager

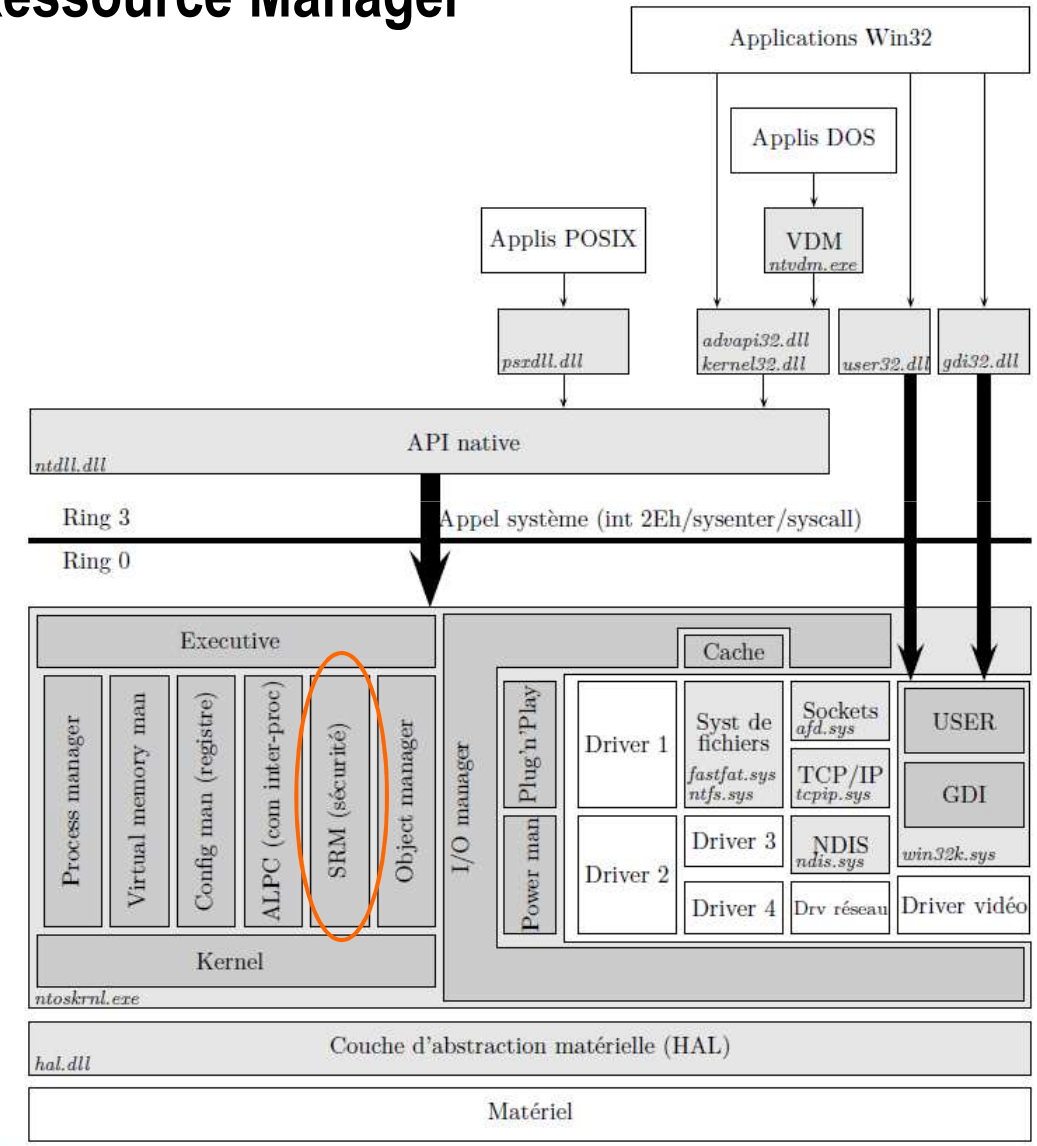


ARCHITECTURE INTERNE
Object Manager

- Gère les objets (ressources) de l'OS
- Un objet peut être de types différents : un fichier, une clé de registre, un évènement, un processus, une section de mémoire partagée … (différent de l'approche : « tout est fichier » dans l'univers Unix)
- Les objets sont identifiés par un nom et des droits leur sont associés (ACL)
- Un « Handle » est une référence à un objet
- Réalise les tâches de création, modification et suppression en fournissant des Handles

ARCHITECTURE INTERNE

Security Ressource Manager



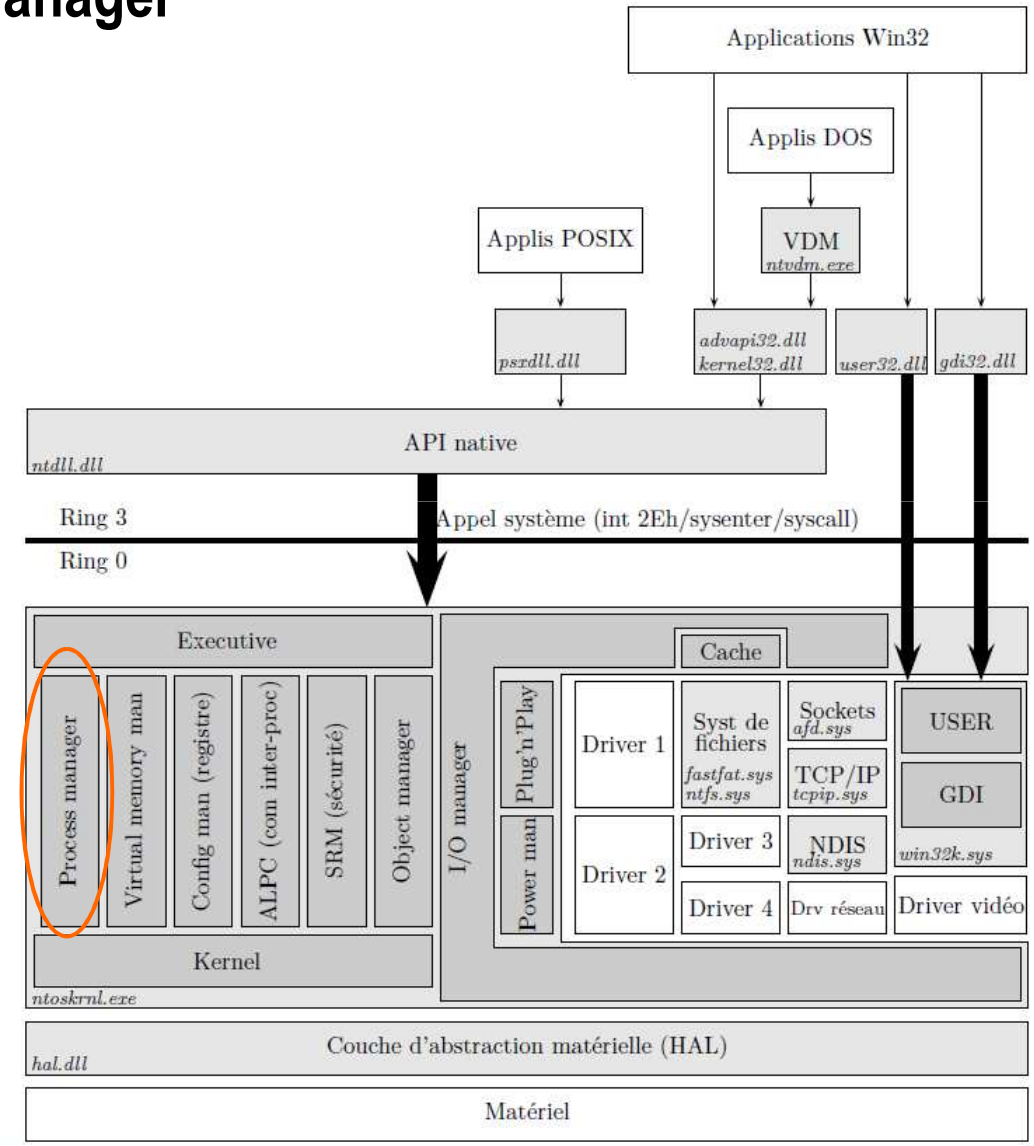
ARCHITECTURE INTERNE

Security Ressource Manager

- Gère la sécurité des objets
- Compare les droits de l'utilisateur avec les droits de l'objet et ajuste les droits du handle
- Génère des messages d'audit (activités liées à la sécurité)
- Le processus de connexion « Windows NT logon » communique directement avec SRM

ARCHITECTURE INTERNE

Process Manager

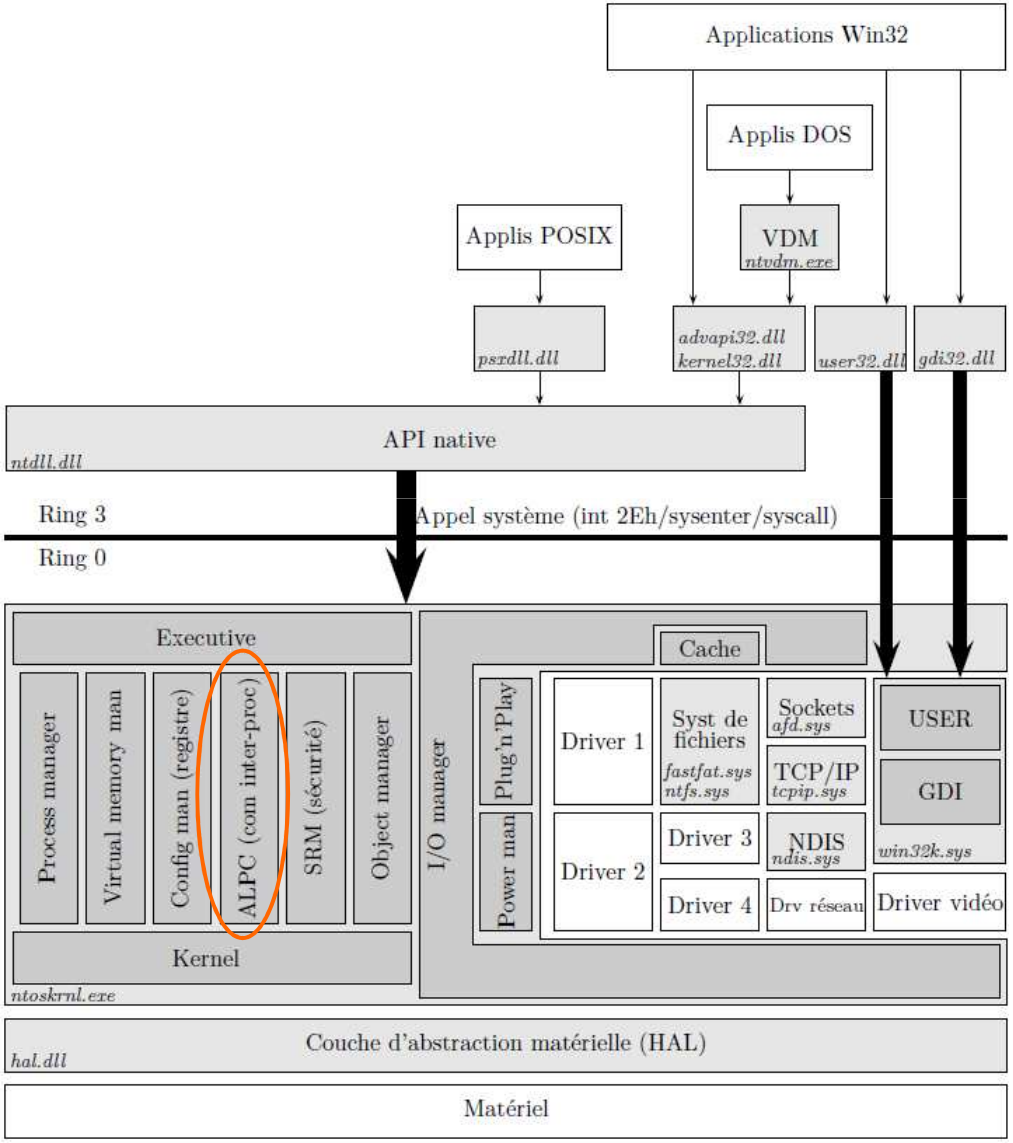


ARCHITECTURE INTERNE

Process Manager

- Gère les processus et les threads : création, modification et suppression
- Fournit des informations sur l'état :
  - Pointeur d'adresse du processus
  - Liste des threads du processus
  - Statistique sur le temps d'exécution de chaque thread
  - Information sur la priorité et l'affinité du processus
- Rappel : n'ordonnance pas (c'est le rôle du micro-noyau)

ARCHITECTURE INTERNE
ALPC

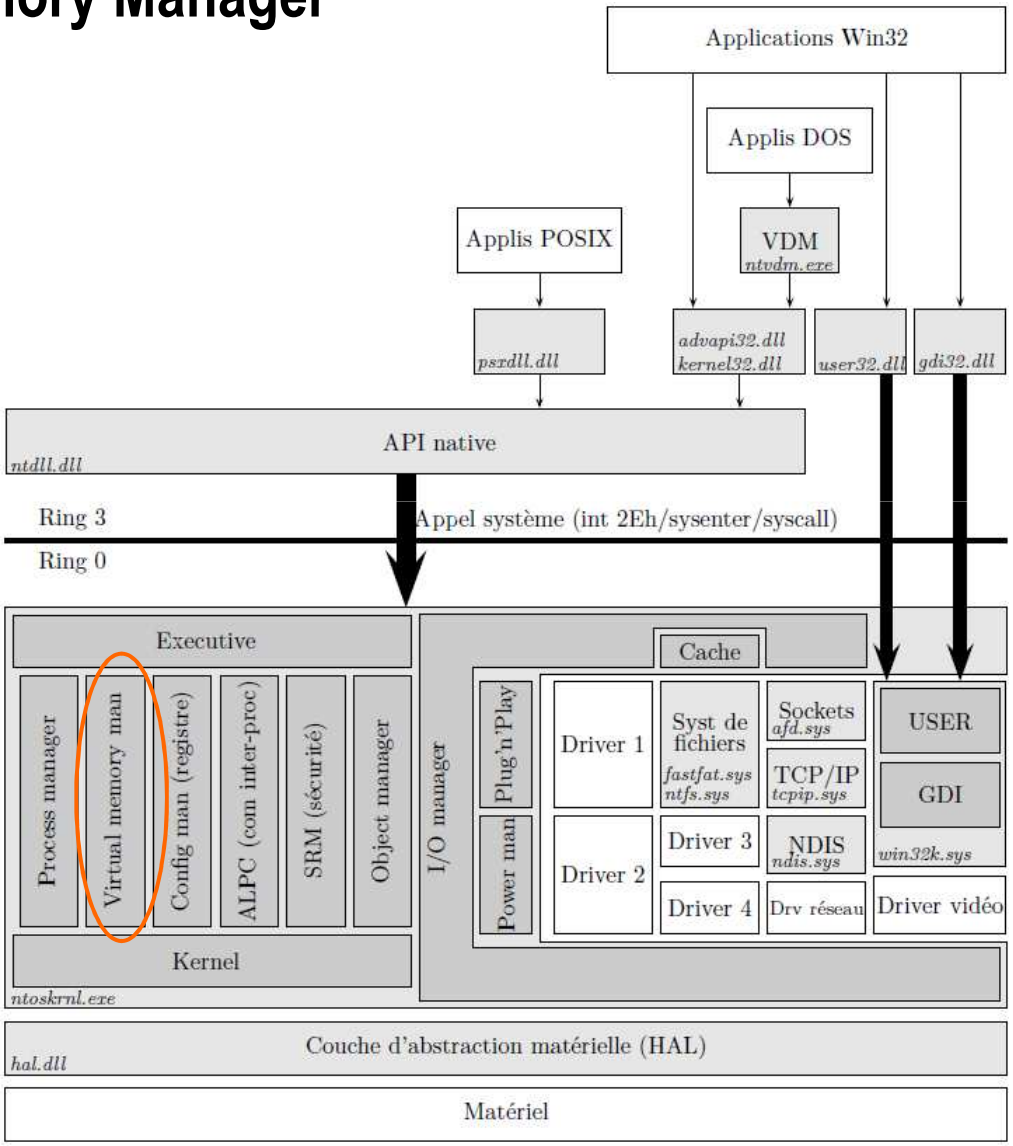


ARCHITECTURE INTERNE
Local Procedure Call

- Permet la communication entre des threads de processus différents
- Fonctionnement en mode Client / Serveur
- Renommé et réecrit à partir de Windows Vista « Advanced Local Procedure Call » (ALPC) afin d'améliorer les performances

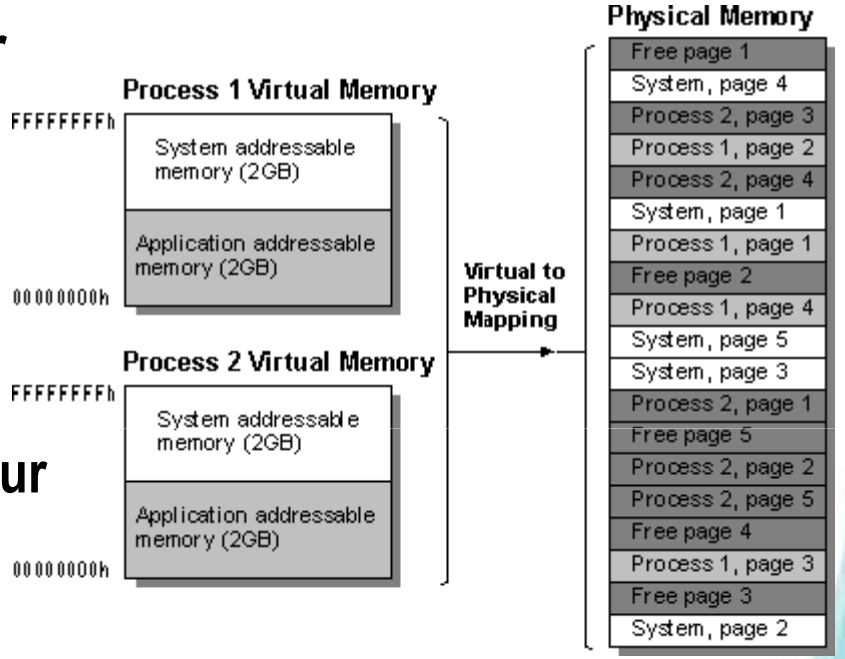
ARCHITECTURE INTERNE

Virtual Memory Manager



ARCHITECTURE INTERNE
Virtual Memory Manager

- Gère la mémoire virtuelle pour les processus en 32bits
  - Abstraction de la mémoire physique en présentant à chaque processus un espace d'adressage dédié de 4Go : 2Go pour le système + 2Go pour l'application
  - Allocation, libération et protection de la mémoire



- Gère le fichier d'échange (Swap) qui permet de libérer de la mémoire vive en stockant les données sur un support plus lent (Disque dur par exemple)

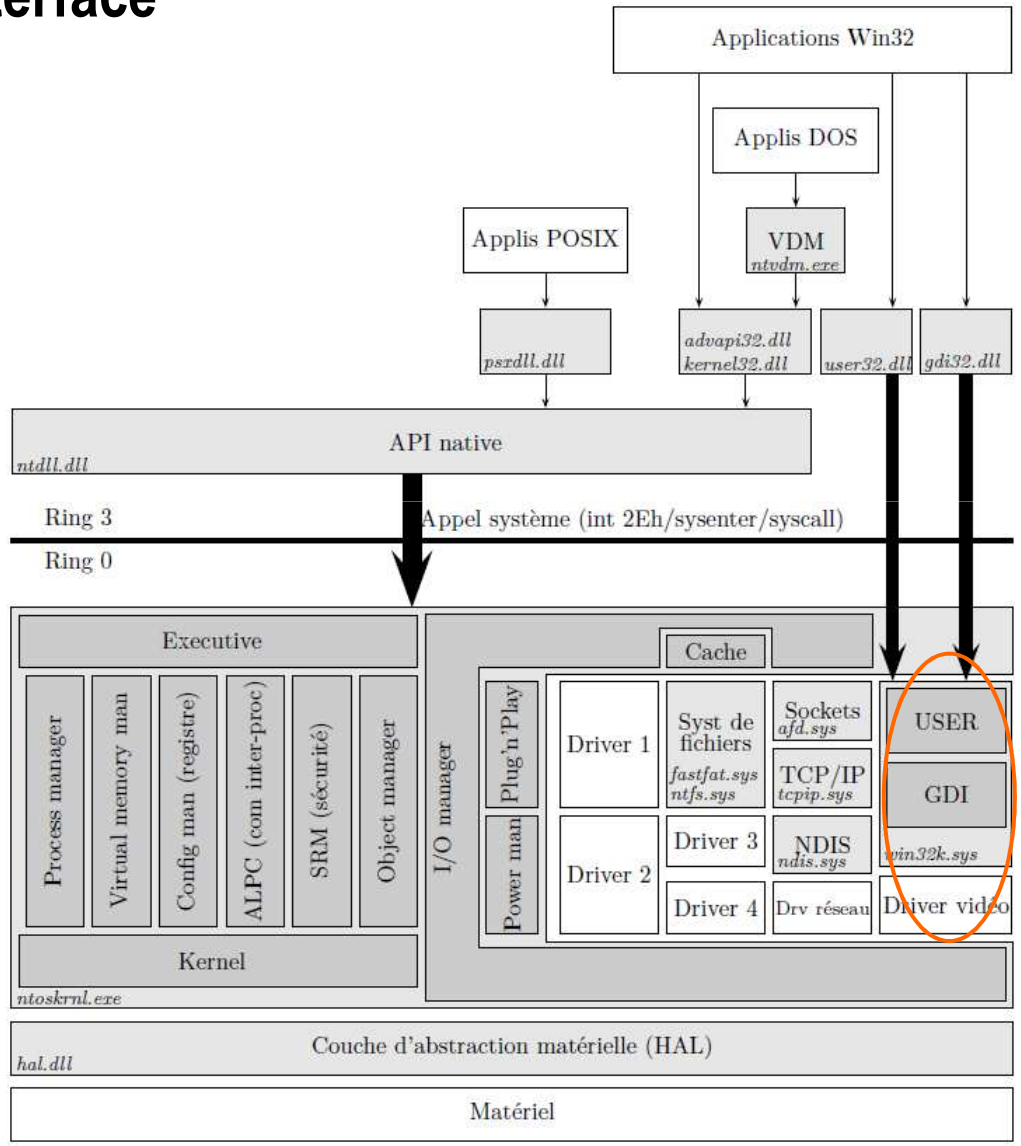
ARCHITECTURE INTERNE

Adressage mémoire en 64 bits

- Les processeurs 64 bits permettent d'adresser jusqu'à 16 Exabytes (2^64)
- Windows ne divise pas comme en 32Bits les deux espaces d'adressage
- Une application ne peut utiliser que 8 Terabytes
- L'espace réservé pour le noyau est limité à 128 Gigabytes et il est positionné en fin d'adressage

ARCHITECTURE INTERNE

Graphic Interface

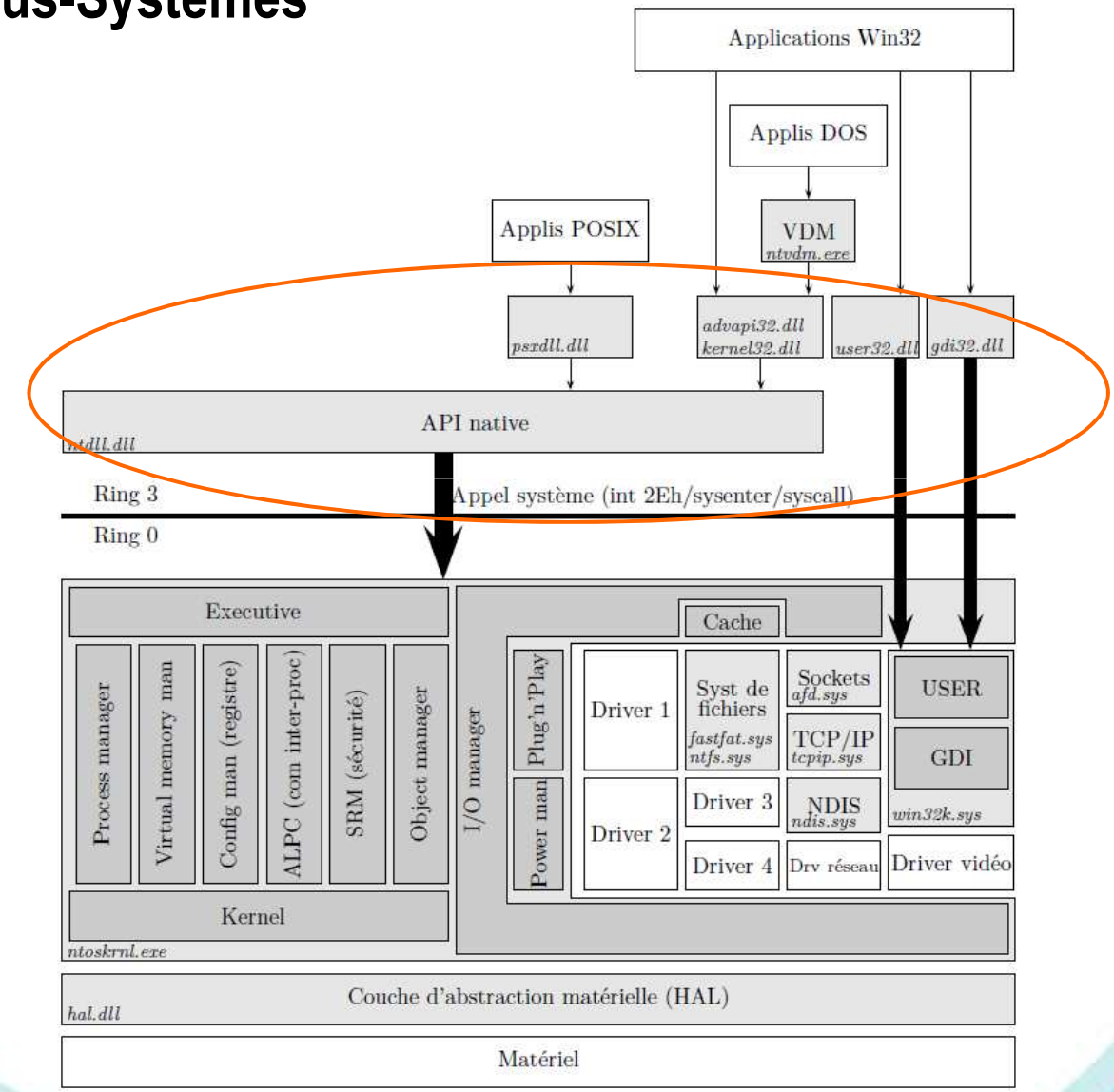


ARCHITECTURE INTERNE
Graphic Interface

- **Deux fonctions réalisent l'affichage :**
  - **L'UI (User Interface) ou « Windows Manager » réalise la gestion :**
    - des fenêtres, des menus, des boutons, etc …
    - du clavier et de la souris
    - des files d'attente des messages
  - **Le GDI (Graphic Device interface) réalise l'affichage des lignes, courbes, rendu des polices et gestion des palettes**
    - Abstraction du matériel (carte graphique)
    - Multi affichage (multi-écran)
    - N'affiche pas la 3D des applications (réalisé par DirectX / OpenGL)
- **Ajout de fonctions 3D (moteur Aero) à partir de Vista grâce à des drivers compatibles WDDM (Windows Display Driver Model)**

ARCHITECTURE INTERNE

API & Sous-Systèmes



ARCHITECTURE INTERNE
API & Sous-Systèmes

- Pour permettre la communication entre des applications en mode utilisateur et le noyau, plusieurs API existent et son organisées en sous-systèmes
- Historiquement il existait les sous-systèmes suivants :
  - Posix : compatible avec les applications Unix
  - OS/2 : compatible avec les applications OS/2 d'IBM
  - MSDOS : compatible avec les applications MS-DOS
  - Win16 : compatible avec les applications Windows 16bits
  - Win32 : sous-système natif de Windows NT compatible avec les applications Windows 32bits

ARCHITECTURE INTERNE

Les sous-systèmes de Windows NT

- Depuis l'arrivée des versions 64bits de Windows NT, deux sous-systèmes sont actuellement disponibles :
  - Win32 est le sous-système Natif de Windows NT en 32bits
  - Win64 est l'équivalent pour le 64bits
- Afin de permettre une rétro-compatibilité sur les nouvelles architectures 64bits, le pseudo sous-système WoW64 permet l'exécution d'applications, développées pour Win32, sur un sous-système Win64
- Les librairies de ces APIs sont regroupées par fonctionnalités en 8 catégories

ARCHITECTURE INTERNE
APIs Windows

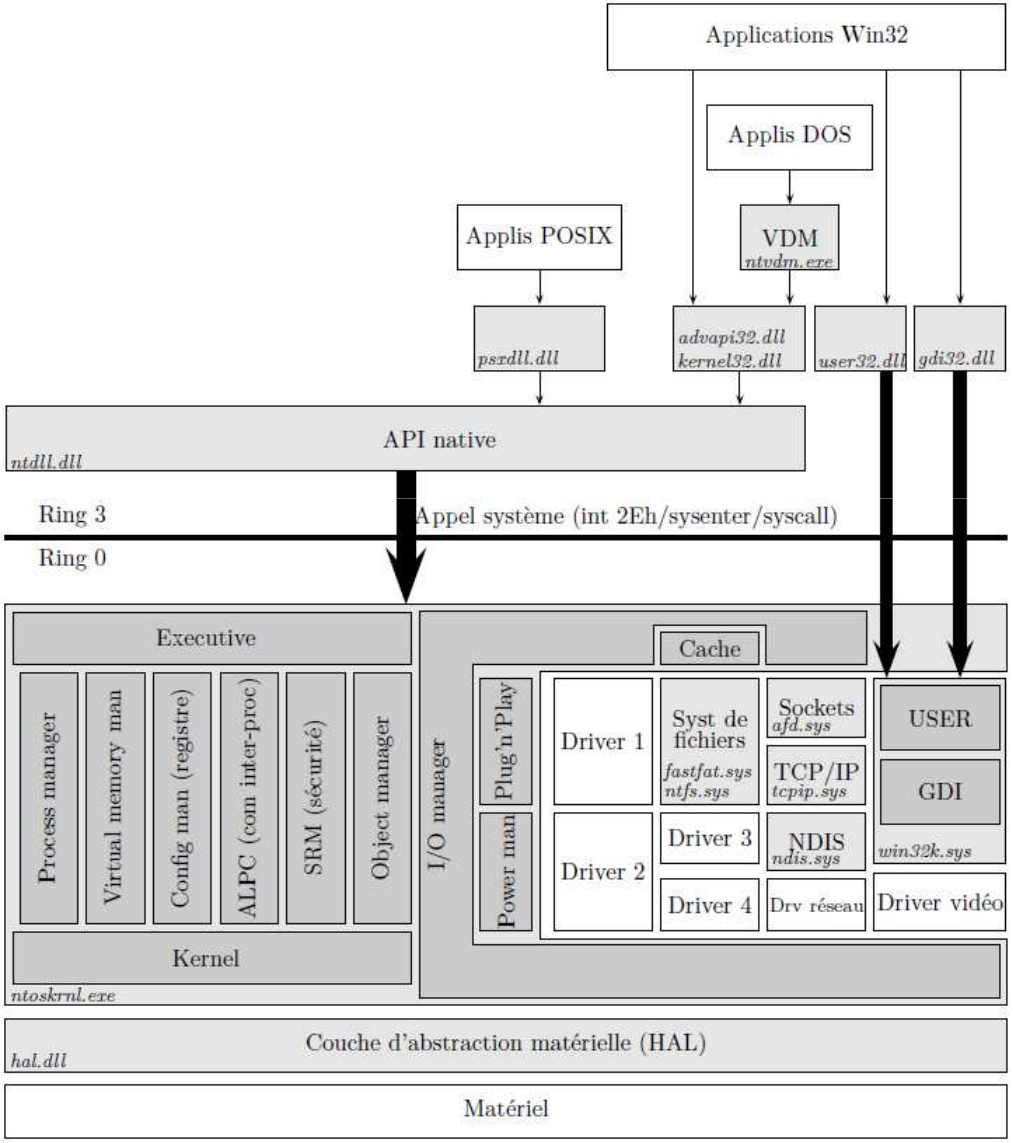
Nom	Description	Librairie (Win32)
Services de base	Accès au système de fichiers, périphériques, processus, registre système et système de gestion d'exceptions	kernel32.dll, advapi32.dll
Services avancés	Accès aux fonctions additionnelles du noyau et de la base de registre, arrêt/redémarrage de services, gestion des utilisateurs	advapi32.dll
Interface graphique	Accès à l'affichage sur les moniteurs, imprimantes	gdi32.exe
Interface utilisateur	Affiche et gère les contrôles de base comme les boutons et barres de défilement, la communication avec le clavier et la souris et des fonctionnalités associées comme l'environnement graphique	comctl32.dll, user32.dll

ARCHITECTURE INTERNE
APIs Windows - suite

Nom	Description	Librairie (Win32)
Boîtes de dialogue communes	Affiche les boîtes de dialogue pour ouvrir et enregistrer des fichiers, choisir la couleur et la police	comdlg32.dll
Bibliothèque de contrôles communs	Accès à des fonctions avancées du système d'exploitation comme des barres de statut (situées au bas des fenêtres), barres de progression, barres d'outils et onglets	comctl32.dll
Shell Windows	Accès aux fonctionnalités fournies par le shell du système d'exploitation	shell32.dll
Services réseau	Gestion de réseau du système d'exploitation. Ses sous-composants incluent NetBIOS, Winsock, RPC, etc	netapi32.dll

ARCHITECTURE INTERNE

Synthèse



ARCHITECTURE INTERNE

Ce qu'il faut retenir pour la suite

- Noyau hybride
- Architecture lourde et complexe
- Communication entre les applications et le noyau au travers d'un nombre important d'APIs
- Pas de protection lors de l'exécution de code dans le noyau (Drivers => BSOD)