Univerzita Hradec Králové
Fakulta informatiky a managementu

Architektura rodiny operačních systémů Windows NT

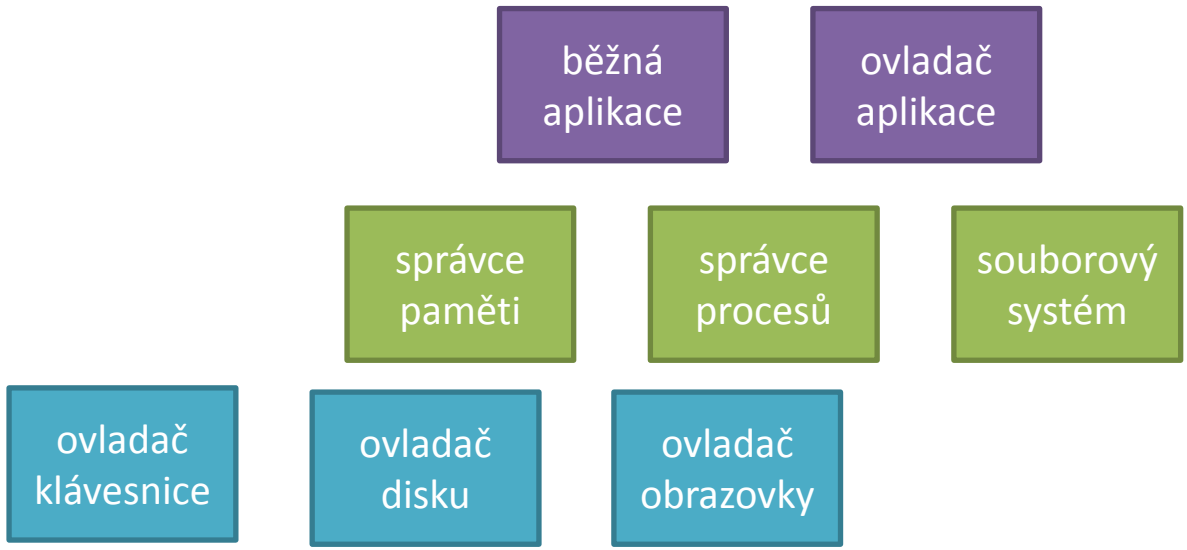
Mgr. Josef Horálek

Mikrojádro

- Velmi malé jádro
  - implementuje jen vybrané základní mechanismy:
    - virtuální paměť;
    - plánování vláken;
    - obsluha výjimek;
    - zasílání zpráv mezi procesy;
  - ostatní komponenty běží v uživatelském režimu;
    - zajištěna větší stabilita;
    - méně kritického kódu;
  - všechny pokročilé funkce v uživatelském režimu
    - časté přepínání mezi režimem jádra a uživatelským
      - může vést ke zpomalení systémů;

FIM UHK

Mikrojádro



režim uživatelský

---

režim jádra

Jádro (obsluha přerušení, zasílání zpráv mezi procesy, časování)

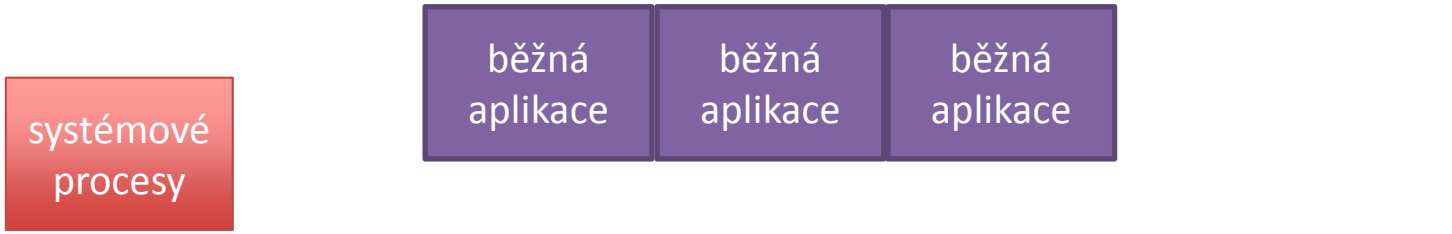
FIM UHK

Monolitické jádro

- Přesný opak mikrokernelů
  - velké jádro obsahuje většinu komponent:
    - souborové systémy;
    - správa procesů;
    - síťová komunikace;
    - bezpečnostní model;
  - sdílejí jeden virtuální adresový prostor;
    - zrychlení vzájemné komunikace;
      - možnost nechtěného ovlivnění a poškození datové struktury;
    - teoreticky nižší stabilita a bezpečnost;
    - teoreticky vyšší výkon;

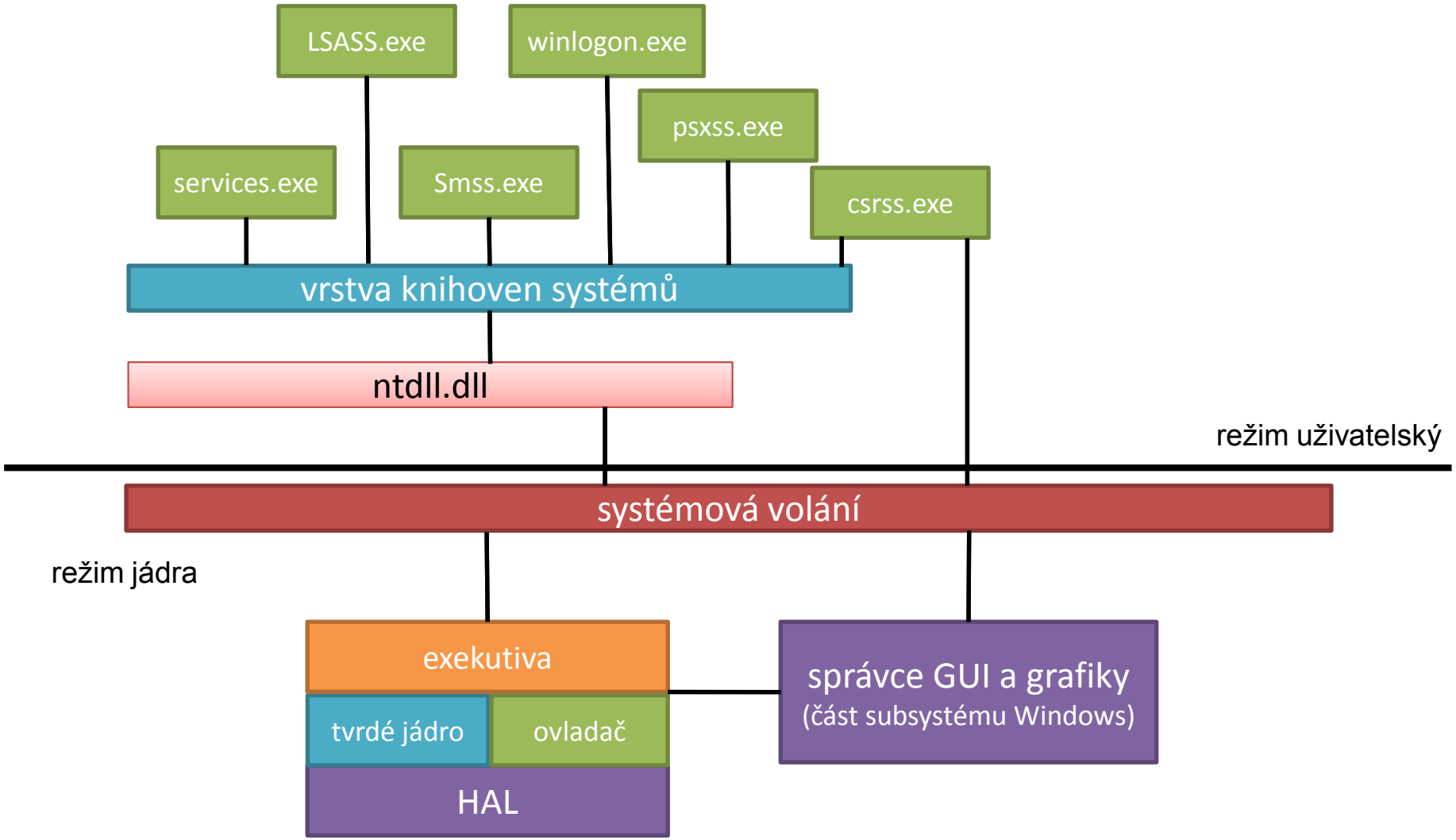
FIM UHK

Monolitické jádro



Windows a jeho součásti

= Jádro Windows NT řadíme spíše k monolitickému jádru



FIM UHK

HAL & tvrdé jádro

- Hardware Abstraction Layer
  - nejnižší úroveň jádra;
  - úkol:
    - odstínění součástí OS a aplikací od specifik hardware;
    - poskytovat rutiny pro komunikaci periferií a vyšších vrstev;
    - kód HAL uložen v hal.dll;
- Tvrdé jádro
  - implementace mechanismů pro vyšší vrstvy:
    - algoritmus plánování vláken na procesoru;
    - odložené volání procedur (DPC);
    - základní synchronizační metody;
    - práce s hardwarovým přerušením;
    - část obsluhy systémových volání;

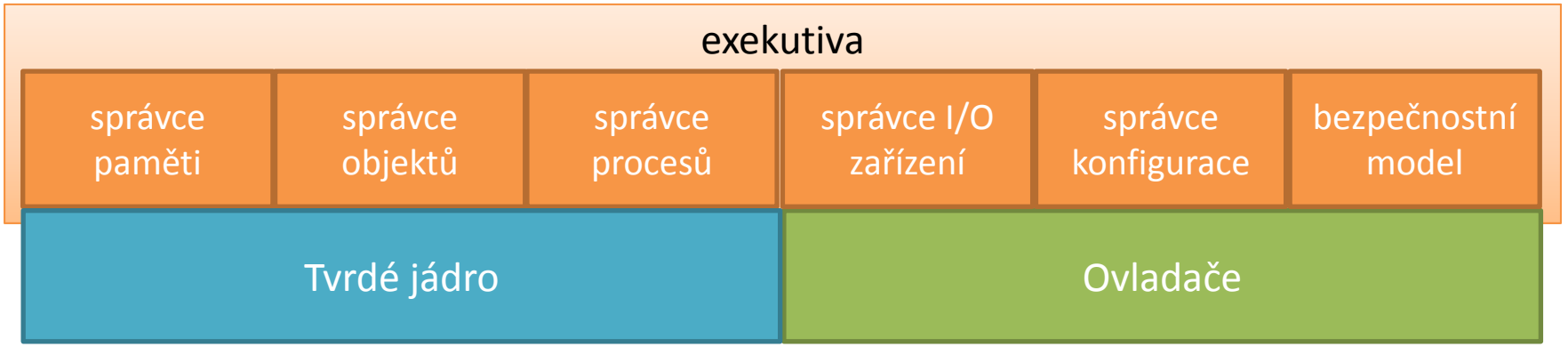
FIM UHK

Ovladače & exekutiva

- Ovladač
  - umožňuje vrstvě exekutiva komunikovat s různými typy hardware;
  - spustitelné soubory *.sys;
- Executiva
  - I/O zařízení a další komponenty;
  - využívá tvrdé jádro;
    - realizuje složitější mechanismy, které jsou přes systémová volání nepřímo využívána obyčejnými aplikacemi v uživatelském režimu;
  - implementována v hlavním modulu jádra;
    - ntoskrln.exe nebo ntkrnlpa.exe;

Exekutiva

- Executiva
  - složena z rozdílných rutin;
    - všechny ve stejném adresovém prostoru;
  - každá komponenta poskytuje speciální sadu rutin
    - každá může volat libovolný kód běžící v jádře;



Objekty exekutivy

- Správce objektů
  - umožňuje psát kód jádra;
  - umožňuje jednotným způsobem vytvářet a odstraňovat objekty;
    - např. otevřené soubory, klíče registru, paměťové mapové soubory;
- Správce paměti
  - řídí činnost virtuální a fyzické paměti;
    - přiděluje volné rámce fyzické paměti;
    - mapování mezi fyzickou a virtuální pamětí;
    - obsluha výpadku stránek;
  - vyřizuje požadavky na přidělování a uvolňování bloků virtuální paměti o proměnlivé velikosti;

Objekty exekutivy

- Správce I/O zařízení
  - zajištění funkcí ovladačů jádra a zařízení;
    - jádro může načítat a uvolňovat ovladače za běhu;
    - komunikace ovladačů mezi sebou;
- Správce procesů
  - spouštění, běh a ukončení procesů a vláken;
  - zjištění informací o běžících procesech;
  - měnit prioritu procesů
  - násilně ukončovat běžící procesy;

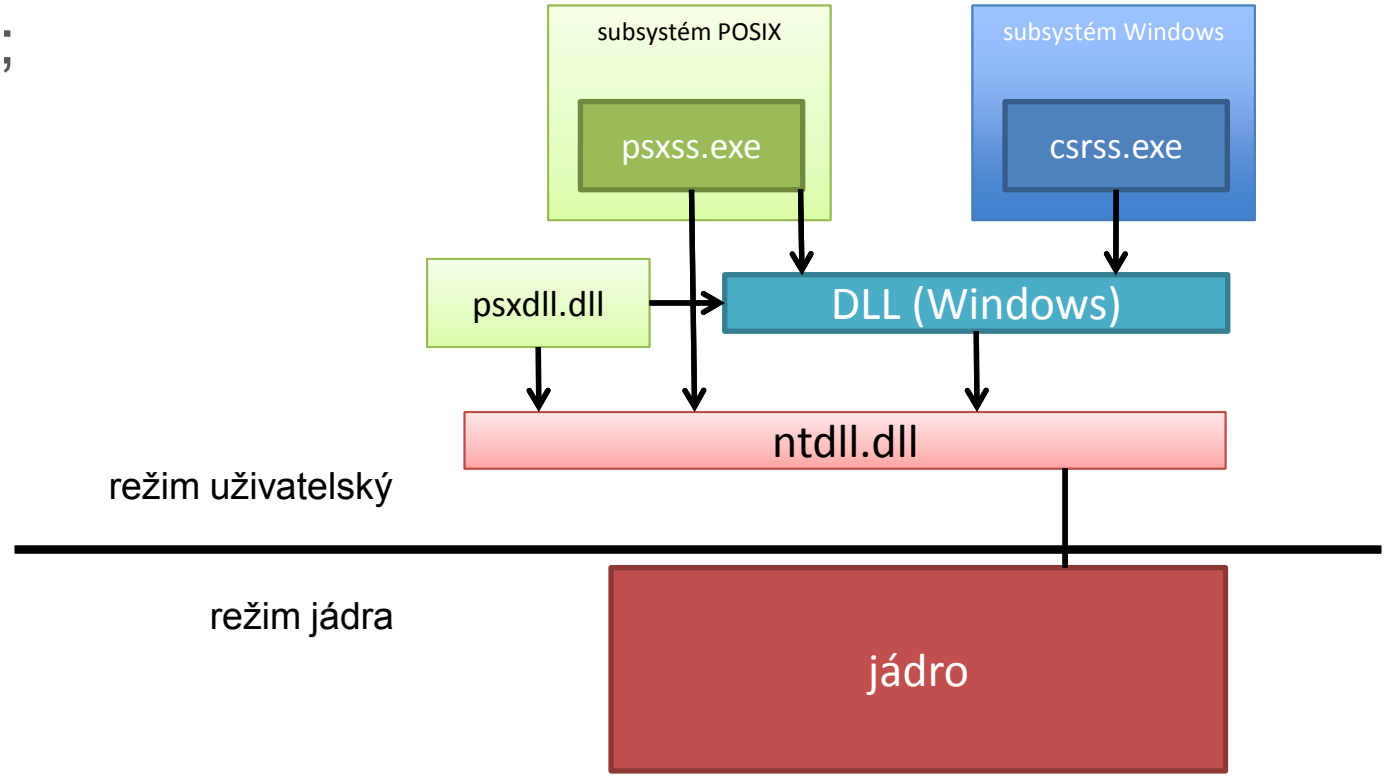
Objekty exekutivy

- Správce konfigurace
  - umožňuje přizpůsobení OS různým požadavkům
    - konfigurace ukládá v binární podobě do registru;
      - Unix ukládá do textových souborů;
    - registr
      - malá a velmi rychlá databáze;
      - obsahuje adresářovou strukturu – klíčů a hodnot;
- Bezpečnostní model
  - umožňuje nastavení práv pro každého uživatele;
  - lze určit přístup k objektům;

FIM UHK

Subsystémy

- Součást prostředí pro obyčejné aplikace
  - obecně dobře dokumentováno;
- Jsou obsaženy dva:
  - Windows;
  - POSIX;



FIM UHK

Subsystém POSIX

- Portable operating systém interface based on Unix
  - sada mezinárodních standardů;
  - popisuje aplikační rozhraní v OS založených na Unix;
  - od Windows Server 2008 implementace v podobě SUA;
    - Subsystem for Unix-based Application;
  - spouští se jen v případě potřeby;
  - hlavním procesem – psxss.exe;
    - komponenta subsystému běžící v režimu jádra – win32k.sys;

FIM UHK

Subsystém Windows

- Základní komponenty:
  - hlavní proces subsystému csrss.exe
    - knihovny DLL, které používá;
  - ovladač jádra win32k.sys
    - drivery grafické karty a videa;
  - vrstva knihoven DLL
    - zajišťují překlad volání dokumentovaných funkcí Windows API a nativní volání rutin z knihovny ntdll.dll odpovědná za volání jádra;
      - kernel32.dll, user32.dll, gid32.dll, advapi32.dll;
      - csrss.exe v sobě uchovává vlastní kopii seznamu běžících procesů a vláken;
      - bránu k ovladači win32k.sys tvoří knihovny:
        - gdig32.dll - kreslení grafických útvarů;
        - user32.dll – exportuje funkce pro práci s prvky uživatelského rozhraní;
        - kernel32.dll – exportuje vybrané části exekutivy
          - procesy, vlákna, správa paměti, synchronizace;
        - advapi32.dll – rozhraní pro práci se službami a bezpečnostním modelem;

FIM UHK

Systémové procesy

- Windows patří mezi monolitické OS
  - velké a složité jádro;
  - kritické procesy = systémové procesy;
    - správce úloh nedovolí jejich násilné ukončení;
  - nečinné procesy
    - pouze pseudoproces;
    - nevykonává žádnou činnost v uživatelském režimu;
    - úkol – spotřebovávat čas procesoru, pokud žádná součást OS ani aplikace nemá co dělat;
      - proces vytvořen jádrem OS v raných fázích inicializace syystému;
      - PID = 0;

Proces System

- Proces Systém
  - nevykonává řádný kód v uživatelském režimu;
    - nepoužívá žádné knihovny DLL;
    - neprezentuje žádný soubor *.exe;
  - v jeho kontextu běží skupina vláken
    - tzv. pracovní vlákna;
    - vytvořena během bootovacího procesu;
    - vykonávají činnost, kterou dostanou zadánu z venku;
      - většinu času čekají na zadání od jádra OS;
      - využívány jádrem pro časově náročné úkoly;
      - obvykle dokončují zpracování požadavků hardware jež nebylo možné provést při obsluze přerušení;
      - využívány při zapisování „špinavých“ stránek z vyrovnávací paměti na disk;
  - PID=4;

Správce realcí

- Session manager = smss.exe
  - spouštěn v poslední fázi startu systému
    - jedná se o první proces vykonávající kód v uživatelském režimu;
    - provádí poslední inicializaci systému;
      - pak je systém připraven k přihlášení uživatele;
    - hlavní úkol – vytvářet realce;
      - relace se využívají pro oddělení prostoru jednotlivých uživatelů;
    - smss.exe vytvoří relaci 0 tzv. konzolovou relaci;
      - v ní běží systémové procesy;
      - služby;
      - všechny procesy prvního přihlášeného uživatele;
        - každý další uživatel má svoji relaci;
        - pro každou novou relaci správce spustí kopii winlogon.exe;
    - smss.exe zodpovědný za inicializaci hlavního procesu sybsystému Windows – csrss.exe;
      - pro relaci 0 spouštěn wininit.exe místo Winlogon;

FIM UHK

winlogon.exe & LSASS.exe

- Procesy podílející se na přihlašování uživatele
  - winlogon.exe umožňuje uživateli přihlášení pomocí grafického uživatelského rozhraní;
    - zabudovaná jednoduchá ochrana proti zachycení přihlašovacích údajů;
    - po zadání jména a hesla údaje odeslány lsass.exe;
      - zajišťuje ověření;
      - zjistí oprávnění uživatele;
      - vytváří token, kterým se uživatel dále prokazuje při provádění operací;
    - obdrží-li winlogon token od LSASS zahajuje inicializaci pracovního prostředí;
      - spuštění startovacích skriptů;
      - předání řízení userinit.exe;
    - winlogon.exe zajišťují odhlášení uživatele;

FIM UHK

services.exe & svchost.exe

- Procesy pro podporu služeb
  - ve Windows mnoho součástí jako služby;
    - programy na pozadí nevyžadující interakci s uživatelem;
    - mezi služby řazeny i ovladače jádra;
    - služby mohou sdílet virtuální adresový prostor jednoho procesu;
    - služby bez vlastního procesu vykonávány v kontextu instancí procesu svchost.exe;
      - kontrola a správa services.msc;

Univerzita Hradec Králové
Fakulta informatiky a managementu

Děkuji za pozornost…