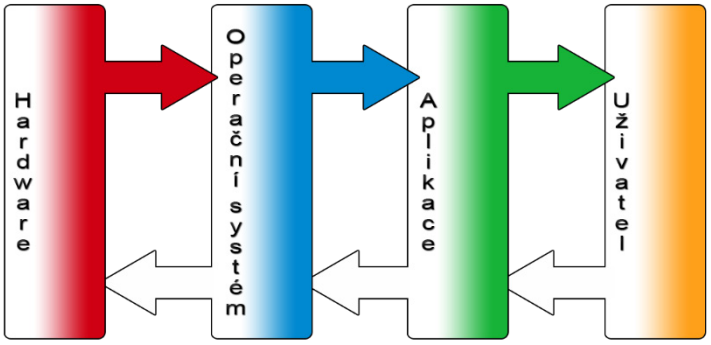
09. Operační systém

Program, který zabezpečuje komunikaci mezi technickým vybavením počítače a ve zjednodušené formě uživatelem.



Hlavní Úkoly OS

- Zajišťovat komunikaci mezi uživatelem a počítačem
- Vytvořit stabilní aplikační rozhraní (**API**) pro procesory
- Přidělovat procesorům systémové zdroje
- Provádět správu dat
- Provádět správu HW zdrojů (paměť, I/O zařízení…)

Vlastnosti OS

- Prostředí
- Kooperativní Multitasking
- Preemptivní multitasking

Služby OS

Procesy důležité pro běh operačního systému, které běží nezávisle na uživateli.

- Správa procesorů
- Správa procesů
- Správa paměti
- Správa souborů
- Správa vstupně/výstupního systému
- Sítě
- Systém ochran
- Interpret příkazů

Rozdělení OS

Podle prostředí

- Graphical User Interface (**GUI**)
- Text User Interface (**TUI**)
- Shell

Podle uživatelů

- **MonoUser**
  - Jednouživatelský systém
  - Předpokládá se, že s počítačem bude pracovat pouze jeden uživatel
  - Tento systém neobsahuje téměř žádný systém pro ochranu neoprávněného přístupu
- **MultiUser**
  - Víceuživatelský systém
  - Umožňuje uživatelům jak sdílet, tak ochraňovat svoje data
  - Umožňuje současně používat programy
  - Vhodný zejména pro síťově prostředí
  - Každý uživatel takového systému má svoje uživatelské jméno a heslo
  - Seznam uživatelů, kteří mají k počítači přístup, sestavuje administrátor (superuživatel)

Podle zpracování procesů

- **MonoTask**
- **MultiTask**
  - Schopnost operačního systému provádět několik procesů současně
  - Jádro operačního systému velmi rychle střídá na procesoru běžící procesy, takže uživatel počítače má dojem, že běží současně
- **Kooperativní Multitasking**
  - Procesor je vždy přidělen právě jedné aplikaci.
  - Jednotlivé aplikace jsou zavedeny do paměti.
  - Aplikace pracuje do doby, než sama uvolní procesor pro jinou aplikaci.
  - Pád aplikace v tomto systému může vážné narušit chod jiných aplikací i operačního systému
  - Výhodou je menší hardwarová náročnost než u preemptivního multitaskingu
- **Preemptivní Multitasking**
  - Pád jednoho programu nemůže ovlivnit chod jiných
  - To jak dlouho bude daný program pracovat, záleží pouze na operačním systému
  - Nevýhodou je větší hardwarová náročnost
- **Multithreading**
  - Jednotlivé procesy jsou rozděleny na vlákna
  - Jedna aplikace mívá hlavní řídící vlákno, z kterého se pak děli další
  - Procesorový čas je přidělován podle priorit jednotlivým vláknům

Registr příznaků

Velikost registru příznaků, počet, pozice i význam jednotlivých bitů závisí na typu procesoru (jeho architektuře). Architektura x86 měla původně registr příznaku **16bitový** a u procesorů typu **8086** byly ještě některé bity nevyužívané, ale od procesorů **80386** výš už byl **32bitový**.

Zero Flag

- Příznak vynulování
- Nastavován, je-li výsledkem operace nula

Carry Flag

- Příznak přenosu
- Nastavován například operacemi sčítání a odčítání, dojde-li k výpůjčce nebo k přenosu z nejvýznamnějšího bitu
- Také jej mohou nastavovat bitové operace

Overflow Flag

- Příznak přetečení
- Nastavován, pokud se výsledek operace nevejde do registru při počítání ve dvojkovém doplňku

Sign Flag

- Příznak znaménka
- Nastavován, je-li výsledek matematické operace záporný

Parity Flag

- Příznak parity
- Nastavován podle toho, je-li počet nastavených bitů výsledku poslední operace sudý či lichý

Vztahy OS a CPU

Vlastnosti operačního systému určují vlastnosti CPU

8086

- 16bit; x86 mikroprocesor
- 1978
- 1 MB adresovatelné paměti
- Reálný režim
- Dělí se na 2 jednotky:
    - Bus Interface Unit (Sběrnicová)
        - Zajišťuje styk procesoru se sběrnicí a výpočet adres
    - Execution Unit (Vykonávací)
        - Vykonává vlastní instrukce

80286

- 1982
- 16 MB adresovatelné paměti
- Přinesl chráněný režim
  - Oddělení jednotlivých procesů
  - Předpoklad pro bezpečný multitasking

80386

- 1986
- Rozšířil chráněný režim
- Stránkování
  - 4kB
  - Odkládání operační paměti na výměnné medium
- V86
  - Virtuální izolované 8086
  - Vytvoření chráněné oblasti → v ní se vytvoří reálný režim

80486

- 1989
- Obsahuje interní cache
- Interní matematický koprocesor (verze DX)
- Zvýšen vnitřní kmitočet (interní násobič; až 2x)

PENTIUM

- 1993
- Superskalární architektura
  - Zvyšování výkonu CPU
  - Více výpočetních jednotek (ALU)
  - Během jednoho strojového taktu zvládal provést 2 instrukce

PENTIUM 4

- 2000
- 2 vlákna
- Hyper-Threading
  - Vlastnost, která umožňovala procesoru tvářit se jako dva logické procesory

Windows

MS–DOS

- 1981

Windows 3.11

- 1993
- Nadstavba MS-DOS
- Adresace paměti nad 64kB

Windows NT 3.5

- 1994
- Souborový systém NTFS (možnost udělovat práva)
- Nové jádro OS
- Workstation | NT Server

Windows 95

- 1995
- 32bit
- Dlouhé názvy souborů, drag & drop, zařízení PnP
- Podpora práce v síti

Windows NT 4

- 1996
- Workstation | NT Server
- Nepodporuje FAT32 (lze doinstalovat)

Windows 98

- 1998
- Vylepšení 95
- Více monitorů, integrovaný browser
- Grafické vylepšení
- DVD, USB, FireWire

Windows 2000 (Windows NT 5.0)

- 2000
- Workstation | NT Server
- Důraz na bezpečnost

Windows Me

- 2000
- Lepší podpora multimedií
- Vylepšení 98

Windows XP

- 2001
- Home | Professional
- Technologie NT
- Nové UI
- Integrovaný firewall
- I 64bit
- Nutná aktivace

Windows Vista

- 2006
- Starter | Home | Business | Enterprise | Ultimate
- Aero, IPv6, podpora RSS
- Malá kompatibilita

Windows 7

- 2009
- Plná kompatibilita se vším (prakticky)
- Starter | Home | Professional | Enterprise | Ultimate
- Více jádrové CPU, gadgety

Windows 8

- 2012
- Core | Pro | Enterprise |RT
- Metro, žádný start, správce úloh (nový)
- Nativní podpora USB 3.0

Windows 10

- 2015
- Home | Pro | Enterprise | Education | LTSB
- Sjednocení všech zařízení

10. Zavedení OS, Více OS na jednom pevném disku, Bootovací manažer, Vlastnosti oddílů HDD

Zavedení operačního systému

Bootování

- Proces zavedení jádra operačního systému při zapnutí nebo restartování počítače.
- Proces inicializace jednotlivých komponent PC, zavedení části systému do operační paměti a vytvoření podmínek pro komunikaci PC s uživatelem.

Zavedení:

- Z flash paměti se zavede úvodní inicializační kód (**BIOS**)
- Provede se kontrola HW (přítomnost HW…)
- Hledá se zařízení, ze kterého lze „nabootovat“
- BIOS našel zařízení, kde je zavaděč OS k dispozici a začne zavádět operační systém
- Na začátku datové oblasti zařízení je obvykle záznam s pevnou strukturou (MBR, GPT)
    - **MBR** obsahuje krátký kód který:
        - Jeden OS
            - Nalezne aktivní oblast zvoleného disku
            - Načte do paměti a spustí kód v boot recordu
        - Více OS
            - V MBR je kód, který spustí okno výběru systému (GRUB…)
            - Podle volby zvolí správnou oblast a načte boot record
- V boot sektoru je kód, který načte a spustí zavaděč (**bootloader**) OS
- Zavaděč postupně aktivuje služby OS

Média, která lze použít pro zavedení:

- CD-ROM
- FLOPPY
- USB
- HDD
- NETWORK
- PXE BOOT (obvykle přes LAN)

Více OS na jednom pevném disku

Zavedení více OS na jeden pevný disk lze provést 2 způsoby:

Virtuálně (viz. OPS 14)

Jednodušší a lepší na testování softwaru a jiných záležitostí. Není třeba formátovat oblast HDD.
Je zapotřebí výkonnější HW. (CPU, RAM)

- Emulace
  - Emuluje HW platformu aplikace, která se má spustit v emulátoru.
- Paravirtualizace
  - Využívá prostředky hosta.
- Plná virtualizace
  - OS neví, že je virtuální
  - Virtualizuje veškeré HW prostředky, které potřebuje pro běh.

Fyzicky

HDD se nejprve musí rozdělit na více primárních oddílů. Každý OS vyžaduje svůj oddíl, kde je nainstalován. Počet primárních oddílů je omezen na 4 (MBR; extended se považuje za primární)

Při instalaci Windows Multibootu se musí instalovat systémy od nejstarších

- Pomocí správce disků (gparted; parted magic; minitool partition wizard) se rozdělí HDD na požadované oddíly a velikosti
- Instalace OS
- (popřípadě obnova grubu; pokud je zapotřebí)
- Který systém se má spouštět se určuje podle „flagů“
  - Oddílu, který se má spouštět se nastaví „BOOT FLAG“.
    - Dělat to takhle pokaždé by bylo zbytečné a nepraktické → používají se boot manažery

Bootovací manažer

Zavaděč, který nahrazuje MBR, když se na disku nachází více OS.

GRUB

- Nejpoužívanější z linux boot managerů
- Zavaděč pravomocí a specifikací multibootu

Vlastnosti oddílů HDD

Typ; souborový systém; Kapacita…

11. Práce s oprávněními a s registry OS WXP (W7) a dalších OS Microsoftu, Windows – příkazový řádek (základní příkazy OS) práce se soubory

Oprávnění

Pravidla, která se vztahují k objektům v počítači nebo síti (soubory; složky). Určují, zda má daný uživatel přístup k danému souboru / složce. Mohou být přidělovány **uživatelům**, **skupinám** a zabudovaným bezpečnostním objektům.

`Složka/Soubor → Vlastnosti → Zabezpečení`

Úroveň oprávnění	Popis
Úplné řízení Full control	Uživatelé mohou zobrazit obsah souboru nebo složky, změnit existující soubory a složky, vytvořit nové soubory a složky a spouštět programy ve složce.
Měnit Modify	Uživatelé mohou měnit existující soubory a složky, ale nemohou vytvářet nové.
Číst a spouštět Read & Execute	Uživatelé mohou zobrazit obsah existujících souborů a složek a mohou spouštět aplikace ve složce.
Číst Read	Uživatelé mohou zobrazit obsah složky a otevírat soubory a složky.
Zapisovat Write	Uživatelé mohou vytvářet nové soubory a složky a provádět změny v existujících souborech a složkách.

Skupiny oprávnění

- Administrators
- Power Users
- Users
- Guests

Poznatky

- Oprávnění lze dědit
  - Složka má určitá práva → soubory a podsložky v dané složce mají stejná práva
- Pokud není stanoveno oprávnění pro určitého uživatele → použije se oprávnění skupiny
- Práva může nastavovat pouze vlastník daného souboru/složky, nebo člověk s právem na změnu
- Vlastnictví nemůže být odebráno → lze pouze předat vlastnictví někomu jinému
- Administrátor nemůže měnit práva (není vlastník) → Administrátor se může nastavit vlastníkem

Registry

Souborová databáze, do které Windows ukládá veškerá nastavení (HW, SW, vzhled, uživatelé…). Uspořádána hierarchickou strukturou. Nachází se v „config“ složce (**%systemroot%\system32\config**). Z těchto souborů se při startu operačního systému zavádí do paměti.

Poprvé se registry objevily ve **Windows 3.11**. Měly nahradit konfigurační soubory (.ini) starších Windows OS. Registry jsou uspořádány do stromu.

Obsahují **Kořenové klíče** (**Handle Keys; HKEY**), které obsahují klíče a podklíče, které obsahují hodnoty (String, Binary, DWORD, QWORD).

Základní větve registrů

- **HKEY_CLASSES_ROOT**
  - Informace týkající se asociace názvů souborů, tříd souborů
  - Informace nezbytné pro běh softwaru
- **HKEY_CURRENT_USER**
  - Aktivní profil uživatele, který je právě přihlášen do systému (vzhled…)
  - Mapuje se z _USERS
- **HKEY_LOCAL_MACHINE**
  - Obsahuje hardwarové profily
  - Nastavení pro všechny uživatele a nastavení systému
- **HKEY_USERS**
  - Všechny aktuální profily uživatelů
- **HKEY_CURRENT_CONFIG**
  - Konfigurační data aktuálního HW profilu (z _LOCAL_MACHINE)
- **HKEY_PERFORMANCE_DATA**
  - Skrytý klíč
  - Obsahuje data kernelu
- **HKEY_DYN_DATA**
  - Pouze u Win 95, 98, ME
  - Informace o HW

Klíče HKLM

„Hives“; Klíče a podklíče slouží k snadnému organizování dat v registru, stejně jako složky a podsložky k organizování souborů.

- **HKLM**
  - Vytváří se při každém spuštění počítače pomocí programu ntdetect.com
- **SAM**
  - Security Account Manager
  - Obsahuje uživatelskou databázi
- **SECURITY**
  - Obsahuje bezpečnostní informace
- **SOFTWARE**
  - Nastavení programů instalovaných na počítači
- **SYSTEM**
  - Nastavení zařízení a služeb v systému

Hodnoty

Každá hodnota je složená z 3 částí:

- Jméno hodnoty
- Typ hodnoty
- Číselná nebo textová hodnota.

Hodnot existuje víc, ale toto jsou hodnoty, které umožňuje přidat editor registru.

- **REG_BINARY** (Binary Value)
  - Binární data obvykle v hexadecimální podobě (00 00 0a 03)
- **REG_DWORD**
  - Data představovaná číslem o délce 4 bajty (32bit)
  - Mohou být v binárním, hexadecimálním, nebo decimálním formátu (0x278d00)
- **REG_EXPAND_SZ**
  - Expandovatelný řetězec %hodnota nahrazená aplikací %.. (%SystemRoot%\system32\ntvdm.exe)
- **REG_MULTI_SZ**
  - Vícenásobné řetězce oddělované parametrem null. (System Bus Extender SCSI miniport)
- **REG_SZ**
  - Textový řetězec. (True, False,...)
- **REG_QWORD**
  - Nová hodnota ve Windows Vista pro data představovaná číslem o délce 8 bajtů (64bit).

Práce s oprávněními a s registry OS Windows

Práce s registry jsou velice nebezpečné → Nesprávné nastavení registrů může způsobit vážně chyby systému. Existuje několik programů pro práci s registry (defragmentace, editace…). Integrovaný REGEDIT, Register Crawler, Advanced Registry Tracer…

Zakázání editace registrů

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` → `DWORD DisableRegistryTools` → `1` → `Restart`

Windows příkazová řádka (cmd)

Uživatelské rozhraní, ve kterém uživatel s programy nebo operačním systémem komunikuje zapisováním příkazů do příkazového řádku. Umožňuje ovládat počítač pomocí textových příkazů (bez použití myši).

Výhody

- Nižší HW nároky
- Historie příkazů
- Tvorba skriptů (baťáků)

Nevýhody

- Znalosti syntaxe
- Nevhodné pro začátečníky

Syntaxe

```
prikaz [prepinace] [parametry]
```

Dávkové soubory

- Textové soubory s příponou .bat
- Posloupnost příkazů
- Spuštěny a vykonány cmd
- Mohou obsahovat podmínky, cykly…

Základní příkazy

- **Interní**
  - Součástí kódu příkazové řádky
  - COPY
  - REN
  - DIR
  - MD
  - CLS – clear screen
- **Externí**
  - Programy jako ostatní
  - Komunikují prostřednictvím cmd
  - MOVE
  - XCOPY – kopíruje adresářové struktury
  - FORMAT

12. Zálohování struktur na pevném disku

Zálohování

Proces, při němž vzniká kopie zdrojových dat za účelem ochrany při ztrátě a poškození dat.

Záloha dat

- **Komprimovaná**
- **Nekomprimovaná**

Archivace dat

- Dlouhodobé uchovávání dat, které již nejsou potřeba pro každodenní využití, obvykle za použití komprimace

Typy zálohování

Plná záloha

Obsahuje všechna data na disku v době jejího vytvoření. Tvoří základ pro budoucí přírůstkové a rozdílové zálohy nebo slouží jako samostatná záloha. Plná záloha vyžaduje ve srovnání s přírůstkovou nebo rozdílovou zálohou nejkratší dobu obnovení.

Rozdílové zálohování

Vytvoří se nezávislý soubor, obsahující všechny změny od vytvoření původní plné zálohy. Obecně by se měla rozdílová záloha obnovit rychleji než přírůstková, protože nemusí zpracovávat dlouhý řetězec předchozích záloh.

Přírůstkové zálohování

Přírůstkové zálohování zálohuje pouze soubory vytvořené nebo změněné od posledního normálního nebo přírůstkového zálohování. Zálohované soubory jsou označeny (jinými slovy, zaškrtnutí atributu Archivovat bude zrušeno).

Sektor po sektoru

Lze vytvořit přesný obraz disku sektor po sektoru.

Tato funkce je užitečná v případě, když je zapotřebí zálohovat poškozené diskové jednotky nebo vytvořit obraz diskového oddílu, ze kterého byl smazán důležitý soubor. Tato volba umožňuje kopírovat využité i nevyužité sektory disku.

Zásady zálohování

- Postupy zálohování se volí v závislosti na konkrétní situaci (interval změn dat, denní objem nových dat, důsledky ztráty dat aj.)
- Kontrola záloh – většina programů (kompresní, vypalovací atd.) následně umožňuje kontrolu archivu
- Popis zálohy – co obsahují, datum vytvoření
- Z instalačních médií by měla být pořízena alespoň jedna kopie, originální média by měla být ihned po pořízení kopií uložena na bezpečném místě (včetně instalačních hesel a čísel!), vlastní instalace probíhá z pořízených kopií
- Ukládání záloh na fyzicky různá místa – důležité zálohy by neměly být uloženy u počítače (požár atd.)
- Zajištění důvěrnosti dat (fyzicky, zaheslování zálohy)

- Volba média (CD, DVD, Flash…) – médium se volí podle:
  - Rychlosti zálohování (čtení)
  - Pořizovací a provozní náklady
  - Spolehlivosti média
  - Spolehlivost obnovení, doby uchovávání dat, kompatibility
  - Zálohovat jen důležitá a protříděná data, popřípadě celý operační systém
  - Využívání automatického zálohování, pomůže předejít lidskému selhání

13. Základní práce s OS Linux – terminál (základní příkazy OS)

LINUX

Linuxové jádro (otevřený standard). Linux je šířen v podobě distribucí.

- Víceuživatelský; Víceúlohový
- Podpora různých platforem
- Svobodný a otevřený software

Části Linux OS

- **Jádro** – **KERNEL** – komunikuje přímo s HW; správa operační paměti; procesů a souborů. Linux je samotné jádro
- **Knihovny** – klíčová součást systému
- **Moduly** – programy pro jednotlivé funkce
- **Distribuce** – obsahují jádro a další programy potřebné pro spuštění, správu OS a další utility.
  - SuSe
  - RedHat
  - BSD
  - Caldera
  - Ubuntu
  - …

Terminál

Obalový program, který spouští shell.

Shell

- Příkazový interpret; Základní prostředek pro komunikaci uživatele se systémem
- Shell může pracovat ve dvou režimech:
  - Interaktivní režim – postupné zadávání příkazů z příkazové řádky
  - Neinteraktivní režim – vstup příkazů je realizován ze souborů (skriptů)
- Case-sensitive
- Mohou obsahovat programátorské prvky (cykly, podmínky, proměnné…)
- Bourne shell; Bourne-again Shell; C shell; Korn Shell

Základní příkazy

pwd

Vypíše absolutní cestu k aktuálnímu pracovnímu adresáři

cd

Změna pracovního adresáře

- **Použití**:
  - *cd ..* – přechod do nadřazeného adresáře
  - *cd /* – přechod do kořenového adresáře
  - *cd ~* – přechod do domovského adresáře
  - *cd /bin* – přechod do adresáře bin v kořenovém adresáři

ls

Výpis obsahu adresáře

- **Použití**:
  - *ls*
  - *ls –al* – dlouhý výpis aktuálního adresáře včetně skrytých souborů
  - *ls -l /etc/sysconfig* – dlouhý výpis adresáře /etc/sysconfig
  - *ls -l | more* – odstránkování výpisu
  - Místo příkazu more, lze pro odstránkování použít i příkaz less

mkdir

Vytvoření adresáře

- **Použití:**
  - *mkdir cosi* – vytvoří v aktuálním adresáři podadresář
  - *mkdir ./home/student1* – vytvoří nový podadresář *student1* v adresáři *home*

rmdir

Rušení adresáře (musí být prázdný)

- **Použití:**
  - *rmdir pokus* – odstraní prázdný adresář pokus z aktuálního adresáře
  - *rmdir /home/student1* – odstraní adresář student1
  - *rm –r adresář* – odstraní neprázdný adresář

cp

Kopírování souborů a adresářů

- **Použití:**
  - *cp zdroj cíl* – lze kopírovat i více souborů najednou
  - *cp –R zdroj cíl* – kopíruje adresáře i s obsahem
  - *cp –a zdroj cíl* – při kopírování zachová strukturu a atributy objektů

touch

Vytvoření souboru nebo jeho aktualizace (pokud soubor existuje)

- **Použití:**
  - *touch pokus.txt*

rm

Odstranění souboru

- **Použití:**
  - *rm soubor1 soubor2 soubor3* – smaže všechny vypsané soubory
  - *rm –r adresar* – smaže plný adresář¨

mv

Přejmenování či přesun souboru nebo adresáře

- **Použití:**
  - *mv /cesta1/stare_jmeno_souboru /cesta2/nove_jmeno_souboru* – přesune a současně přejmenuje soubor
    - Je-li v cílové cestě jako poslední jméno adresáře, soubor se pouze přesune

Práce s textovými soubory

- Všechny konfigurační soubory a skripty v Linuxu jsou textové
- K úpravám textových souborů slouží textové editory:
  - vi
  - nano
  - joe
  - …

grep

Prohledává uvedené soubory a hledá zadanou část textu

- **Použití**:
  - grep hledany_text soubor – prohledání souboru a vypsání řádků, na kterých se nachází zadaný text
  - grep ´hledany retezec´ soubor – pokud obsahuj mezery, musí být omezen apostrofy
  - grep –i hledany_text soubor – nerozlišování velikosti písmen
  - grep – l hledany_text * – zobrazí, ve kterých souborech se nachází hledaný text
  - grep –v hledany_text soubor – vypíše řádky, které neobsahují hledaný text
  - grep –n hledany_text soubor – vypíše jméno souboru a číslo nalezeného řádku

Midnight commander

- Správce souborů
- Vlastní integrovaný editor (F4; mcedit)

Systém uživatelů

- Každý program běží pod určitým uživatelem, každý soubor je vlastněn některým uživatelem
- Každý uživatel má svoje jedinečné identifikační číslo UID
- Pro snazší přiřazování práv uživatelům jsou zavedeny skupiny, uživatel může být členem více skupin, ale jednu má vždy nastavenu jako základní
- Uživatel s UID 0 – root
- Uživatel s UID 1 – 500 – systémový uživatel
- Uživatel s UID > 500 – uživatelský účet

Příkazy

- Whoami – vypíše aktuální identifikaci (login) uživatele
- who – vypíše seznam všech uživatelů na systému
- w – vypíše seznam všech uživatelů a jejich spuštěné procesy
- finger uživatel – vypíše informace o uživateli
- su uživatel – nastaví aktuálního uživatele (žádá heslo)
- passwd uživatel – změna hesla

14. Virtualizace a virtuální PC

Virtualizace

Označení postupů, technik a prostředků, které umožňují v počítači přistupovat k dostupným zdrojům jiným způsobem, než fyzicky. Virtualizované prostředí může být mnohem snáze přizpůsobeno potřebám uživatelů, snáze se používat, případně před uživateli zakrývat pro ně nepodstatné detaily (jako např. rozmístění hardwarových prostředků). Virtualizovat lze na různých úrovních, od celého počítače, po jeho jednotlivé hardwarové komponenty (CPU, RAM…), případně pouze softwarové prostředí (OS).

Emulace

Emulátory se všeobecně odkazují na schopnost počítačového programu nebo konkrétního zařízení napodobit, emulovat jiný program či zařízení. Typický příklad lze najít ve světě tiskáren. Mnoho tiskáren je navrženo tak, aby dokázaly napodobit tiskárny společnosti Hewllet-Packard, protože jsou popsané ve velkém počtu programů. Pokud tiskárny jiných výrobců dokáží emulovat tiskárny HP, jsou schopné tisknout z programů, které by s těmito tiskárnami normálně nepracovaly.

Emulátor nemusí vystupovat jen jako software, který napodobuje, emuluje jiné prostředí, ale také jako hardwarový emulátor. Jedná se například o DOS kompatibilní karty, které se vyskytly v dřívějších verzích Macintoshů pod názvem Centris 610 nebo Performa 630. Díky tomu byly majitelé takového počítače schopni spouštět programy známé z PC.

Výhody

Emulátory zachovávají celkový vzhled i chování původní aplikace. To je stejně důležité jako samotná data takovýmto způsobem zobrazená.

Počáteční náklady na vývoj nebo pořízení emulátoru mohou být vyšší, ale s postupem času se taková investice rychle vrátí (nákup nových verzí aplikací …).

Emulátory zároveň snižují počet hodin strávených na migraci starších souborů do nových aplikací. Jakmile je emulátor naimplementován, využívá se pro všechny soubory a uživatel s nimi pracuje rovnocenně.

Mnoho emulátorů bylo vydáno pod GNU General Public License jako open source prostředí, což umožňuje významným způsobem minimalizovat náklady na pořízení, ale zároveň umožňuje využití ve velkém.

V zábavním průmyslu umožňují emulátory spouštění videoher, které jsou určeny pro konkrétní typy platforem, spouštět například na PC.

Nevýhody

Největší překážkou emulace se často uvádí duševní vlastnictví. Mnoho dodavatelů technologií se snaží při vývoji programu rozšířit své místo na trhu a současně s tím stávající programy rozšiřovat a vylepšovat tak, aby zůstaly konkurenceschopné. Tito dodavatelé často vydávají takzvaný proprietární software, který jim zaručí výsadní postavení na trhu. Díky tomu je ale schopnost pozdější emulace jejich produktu znemožněna, protože produkt je chráněn licencí.

Autorské zákony ještě nepokročily do té podoby, aby emulaci proprietárního software dostatečně popsaly.

Paravirtualizace

Samozřejmě plná virtualizace má svou cenu. Dochází k úplnému oddělení fyzické a programové vrstvy, je při plné virtualizaci prakticky nemožné dosáhnout plného výkonu i v tom případě, že virtuální počítač je víceméně přesným obrazem hardware, na kterém běží (především nabízí identický procesor a další periferie). Virtuální monitor totiž musí kompletně odstínit virtuální počítač od jakékoliv možné změny hardware. Toho dosáhne tak, že emuluje fyzické vybavení a většinu operací (včetně řady instrukcí procesoru, práce s pamětí, operace přístupu na disk a další) provádí ve vlastním software namísto, aby je přímo vykonával hardware. Nemá-li dojít k výraznému zpomalení virtuálního počítače, je virtualizace omezena pouze na virtuální prostředí, které se maximálně podobá tomu fyzickému.

Za předpokladu, že se alespoň některé komponenty virtuálního a fyzického počítače shodují, pak se hovoří o paravirtualizaci. Ta se vyznačuje tím, že provádí jen částečnou abstrakci na úrovni virtuálního počítače, tj. nabízí virtuální prostředí, které je podobné tomu fyzickému, na kterém se virtuální počítač provozuje. Virtualizace v tomto případě není úplná, některé vlastnosti např. procesoru mohou být omezeny a operační systém může rozpoznat, že běží ve virtuálním prostředí. Na druhou stranu skutečnost, že virtuální a fyzický hardware se příliš neliší, umožňuje, aby virtuální počítač v maximální míře využíval vlastnosti základního fyzického prostředí (nemusí emulovat všechny komponenty virtuálního počítače).

Paravirtualizace je široce využívána při tvorbě virtuálních prostředí nad procesory Intel (AMD). VMWare workstation a Xen patří mezi neznámější systémy, které jsou postaveny na paravirtualizaci. Základní principy paravirtualizace si lze představit na (zjednodušeném) modelu, který používá právě prostředí Xen.

Prvním problémem, který je třeba vyřešit, je virtualizace procesoru. Každý procesor pracuje alespoň ve dvou různých režimech – privilegovaném, který je přístupný pouze jádru operačního systému, a uživatelském, ve kterém běží všechny programy. Úkolem privilegovaného režimu je zajistit, že uživatelé mají kontrolovaný přístup k hardware a nemohou přímo provádět operace, které by mohly ohrozit jiné programy či integritu dat (přímý přístup na disk, složitější operace s virtuální pamětí…). Pokud se ale počítač virtualizuje, je zapotřebí ještě jedna úroveň, na které poběží virtuální monitor. V případě plné virtualizace to není problém, při tomto přístupu se emuluje celý procesor se všemi úrovněmi ochrany, v případě paravirtualizace je to však mnohem složitější.

Virtuální monitor musí běžet na nejvyšším stupni ochrany. Na stejné úrovni však nemůže automaticky běžet operační systém, protože by mohl ovlivnit stav virtuálního monitoru. Jednou z možností je pozměnit kód operačního systému tak, že nebude provádět žádnou operaci, pro jejíž provedení je třeba oprávnění té nejvyšší úrovně. Provedení instrukce se změní ve volání příslušné funkce virtuálního monitoru, který nejprve zkontroluje, zda je operace povolena a následně ji provede tak, aby změnila stav virtuálního, nikoliv fyzického počítače. Nemalý problém však budou v tomto přístupu dělat instrukce čtení paměti. Jádro operačního systému předpokládá, že má přímý přístup k libovolné části fyzické paměti, to však samozřejmě v případě virtuálního počítače není možné. Protože nelze předem poznat, zda konkrétní operace čtení z paměti bude přistupovat k privilegovaným údajům, musely by se nahradit v operačním systému všechny instrukce čtení – tím se ale začne velmi nepříjemně přibližovat k plné virtualizaci. Další problém spočívá v ochraně operačního systému před běžícími uživatelskými programy. Pokud by existovaly jen dvě úrovně ochrany (privilegované a neprivilegované), musel by operační systém virtuálního počítače pracovat neprivilegovaně, tím by však byl vystaven ohrožení ze strany aplikací.

Paravirtualizace je možná jen díky tomu, že konkrétní procesory podporují více úrovní ochrany. Procesory Intel mají definovány **4** úrovně ochrany (okruhy; **rings**). Na nejvyšším stupni ochrany (ring 0) běží operační systém, uživatelské programy běží s nejnižším stupněm ochrany (ring 3). Ostatní stupně se běžně nevyužívají. Pokud se použije paravirtualizace, pak virtuální monitor pracuje na nejvyšším stupni ochrany (okruhu 0). Operační systém virtuálního počítače se posune o jeden stupeň (do okruhu 1), aplikační programy běží stále s nejmenší ochranou. Operační systém má tak stále vyšší úroveň ochrany než aplikační programy, na druhé straně už nemůže provádět operace, které vyžadují plně privilegovaný přístup. Úrovně ochrany však lze využít i místo výše zvýšené modifikace privilegovaných instrukcí – operační systém bude ve virtuálním počítači provádět všechny instrukce, pokud však bude chtít provést "zakázanou" operaci (takovou, na kterou teď nemá dostatečná oprávnění), pak dojde k přerušení a řízení převezme virtuální monitor. Ten operaci zkontroluje a provede ji tak, aby správně změnila stav virtuálního počítače. Není v principu třeba měnit operační systém, většina instrukcí běží přímo, pouze privilegované instrukce jsou výrazně pomalejší, protože je musí provést virtuální monitor. Operační systém však může zjistit, že běží ve virtuálním prostředí, protože může mít i na úrovni 1 možnost číst některé části paměti, které jsou ve virtuálním počítači jiné než ve fyzickém. Pro paravirtualizaci je proto třeba modifikovat některé součásti operačního systému, změny jsou však malé a dobře lokalizovatelné (zvlášť dobře je pak možné provést tyto změny u operačních systémů, k nimž jsou k dispozici zdrojové kódy; i proto začala být tak oblíbená (para)virtualizace v prostředí Linuxu).

Přístup k hardware je v prostředí Xen zajišťován vrstvou virtuálního monitoru (Virtual Machine Monitor, VMM). Nad touto vrstvou jsou pak vytvářeny virtuální počítače (Virtual Machines, VM). Jeden z těchto virtuálních počítačů má speciální postavení – v terminologii Xenu se nazývá Doménou 0 (Dom 0). Operační systém, který běží v tomto virtuálním počítači, má přímý přístup k rozhraní virtuálního monitoru, může tedy definovaným způsobem měnit jeho stav a může vytvářet a rušit ostatní virtuální počítače běžící nad VMM. Další zajímavou vlastností Xenu (opět související s paravirtualizací) je to, že může konkrétnímu virtuálnímu počítači přímo zpřístupnit konkrétní rozhraní.

V jednom z virtuálních počítačů běží uživatelský program, který intenzivně komunikuje s jiným počítačem prostřednictvím počítačové sítě. Pokud používá virtuální síťovou kartu, pak její propustnost je omezena a velmi zatěžuje procesor. Pokud ale příslušnému virtuálnímu počítači po dobu běhu tohoto uživatelského programu se přímo exportuje rozhraní na fyzickou kartu, pak může síťová komunikace probíhat plnou rychlostí, kterou podporuje příslušný hardware. Samozřejmě v takovém případě kartu může používat pouze tento virtuální počítač, to ale nemusí být na závadu (fyzický počítač může mít více síťových rozhraní, ostatní virtuální počítače pak sdílí ta ostatní).

Přestože má paravirtualizace řadu výhod proti plné virtualizaci, potřebuje určité modifikace operačních systémů, což komplikuje její nasazení (zejména u proprietárních operačních systémů) a vede k určité neefektivnosti. Intel proto v poslední době zavedl další systém podpory virtualizace v podobě Intel Virtualization Technology (IVT). Jedná se o rozšíření možností procesorů tak, že přibývá další úroveň ochrany (ring -1) pro VMM a přibývají speciální instrukce na této úrovni. Virtuální monitor tak může obsluhovat několik virtuálních počítačů, které již pracují v prostředí, které se neliší od toho, které je k dispozici ve standardních procesorech bez podpory virtualizace. Operační systémy ve virtuálních počítačích není třeba modifikovat, přitom zůstávají základní výhody paravirtualizace (přímé vykonávání instrukcí virtuálního počítače fyzickým procesorem).

Plná virtualizace

Pokud se postupuje tímto způsobem, virtualizují se důsledně všechny součásti počítače. V takovémto případě se nabízí prostředí, v němž běžící operační systém nemůže žádným způsobem poznat, že nemá přístup k fyzickému technickému vybavení. Operační systém ani aplikační programy nepotřebují žádné modifikace. Jedná se v podstatě o ideální stav, kdy dochází k plnému oddělení fyzické vrstvy, veškeré programy běží pouze na virtuálním hardware a přístup k fyzickému vybavení je vždy zprostředkován. To má samozřejmě řadu výhod – lze virtuální prostředí navrhnout tak, aby vyhovovalo požadavkům (velikost paměti, typ procesoru, typ, kapacita disku…). Programy jsou rovněž nezávislé na konkrétním technickém vybavení, jeho změna nemá na virtuální prostředí vliv (samozřejmě kromě výkonnostních charakteristik).

U plné virtualizace nemusí existovat žádná jednoduchá vazba mezi virtuálním prostředím a konkrétním hardware, na němž je virtuální počítač provozován. To umožňuje plnou přenositelnost. A následně je lze přenést na počítače vybavené jiným procesorem, aniž by bylo nutné provést jedinou úpravu na úrovni virtuálního počítače. Podobně lze vytvořit virtuální počítač vybavený procesorem, který je teprve ve vývoji – návrh a ladění operačního systému a aplikací tak může probíhat paralelně s vývojem vlastního hardware.

Mezi profesionální systémy, které nabízí plnou virtualizaci počítačů s procesorem Intel, patří Microsoft Virtual Server a VMWare ESX ServerTM.

15. Windows server 2008 / 2012, DNS princip, AD

Windows 2008

Vychází ze stejného kódu jako Windows Vista (Windows NT 6.0 kernel), se kterou sdílí mnoho ze své funkcionality a architektury. Automaticky tak těží z výhod nových technologií spojených s vývojem Windows Vista, jako je přebudovaný síťový modul (IPv6, nativní podpora bezdrátových sítí nebo zvýšení rychlosti a bezpečnosti), lepší podpora instalačních obrazů, spouštění a zálohování, širší možnosti diagnostiky, monitoringu a záznamu událostí serveru, lepší bezpečností prvky (Bitlocker, ASLR, RODC, vylepšený Windows Firewall), .NET Framework 3.0, vylepšení jádra a správy paměti a procesů.

Server Core

Snad nejvýraznější novinkou Windows Server 2008 je nová verze instalace označená jako Server Core. Je to zjednodušená instalace, ve které chybí Windows Explorer a veškerá nastavení se provádějí pomocí příkazového řádku nebo vzdáleně pomocí Microsoft Management Console (MMC). Server Core dále postrádá .NET Framework a další prvky. Server Core stroj může být konfigurován pro několik základních rolí: Doménový řadič/Active Directory doména, ADLDS (ADAM), DNS server, DHCP server, souborový server, tiskový server, Windows Media Server, Terminal Services Easy Print, TS Remote Programs a TS Gateway, IIS 7 web server a Windows Server Virtualization virtual server.

Windows 2012

Byly přidány různé funkce (s velkým důrazem na cloud), jako aktualizovaná verze Hyper-V, která se používá na správu IP adres, nová verze Správce úloh systému Windows a nový souborový systém.

DNS; Domain Name System

Systém, který překládá doménové názvy na IP adresy. Počítače mezi sebou komunikují pomocí IP adres. Ty jsou však pro člověka špatně zapamatovatelné a tak se vymyslely domény a vznikl systém DNS. Běžnému uživateli pak stačí zapamatovat si doménové jméno a DNS zařídí, že se prohlížeč spojí se správným serverem a zobrazí Vám požadované stránky.

Struktura

DNS systém tvoří hierarchickou stromovou strukturu. Každý uzel tohoto stromu obsahuje informace o části jména (doméně), které je mu přiděleno a odkazy na své podřízené domény. Kořen tohoto stromu, nultou úroveň, tvoří tečka. Na první úrovni se nacházejí Top Level Domains (TLD), které lze rozdělit do dvou základních tříd:

- **gTLD**
  - Generické TLD domény
    - .com, .net…
- **ccTLD**
  - Country-code TLD
    - .cz
  - Národní domény států
    - …

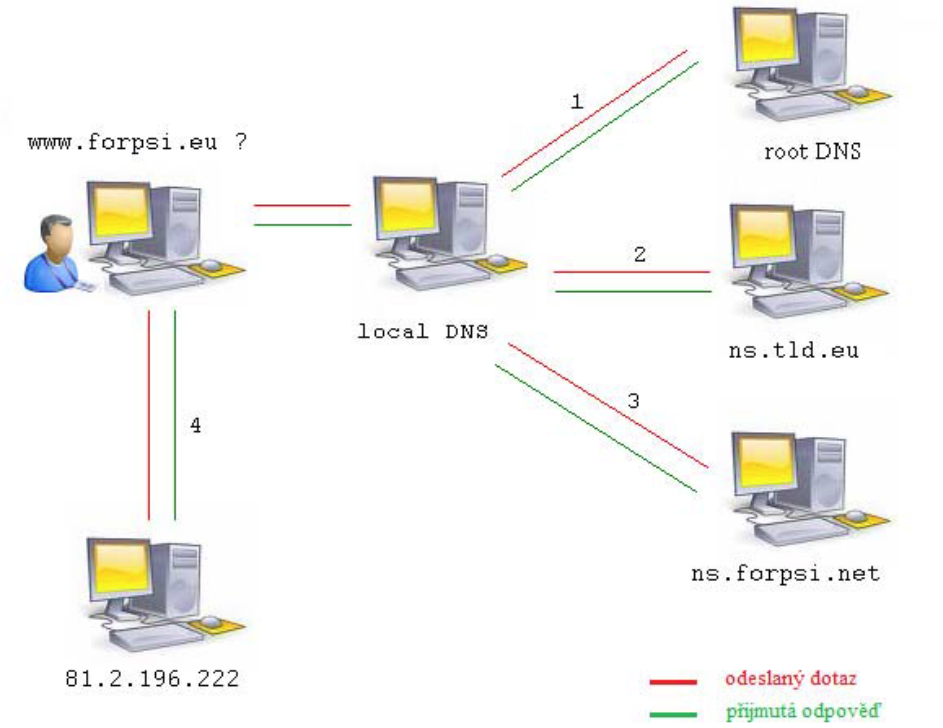
Každá doména může mít maximálně 127 úrovní. Jednotlivé subdomény mohou mít až 63 znaků (v praxi bývají zavedeny tvrdší limity) a celé doménové jméno z nich složené, může mít maximálně 255 ASCII znaků.

Typy DNS serverů

- **Primární**
  - Stará se o záznamy ve své zóně
  - Každá doména musí mít primární server
- **Sekundární**
  - Automatická kopie primární serveru pro případ jeho poruchy
  - Sám si průběžně kopíruje data z primárního serveru
- **Cachovací**
  - Slouží jako vyrovnávací paměť systému pro snížení zátěže a zrychlení odezvy
  - Uchovává výsledky a mezivýsledky dotazů dokud nevyprší jejich platnost
- **Root**
  - Kořenový server, který zná adresy autoritativních serverů všech domén TLD

Princip DNS

Každá doména má uvedeny autoritativní DNS servery, na kterých jsou uloženy konkrétní DNS záznamy ukazující na nějakou IP adresu. Autoritativní DNS servery jsou uvedeny také ve Whois databázi.



Každý má od poskytovatele internetu přiděleny lokální DNS servery (Cachovací). Prohlížeč se jich zeptá, zda znají IP adresu pro hledanou doménu (www.forpsi.eu). Server prohledá svou cache paměť, kde si data o IP adresách vždy na určitou dobu uchovává a pokud ji nenajde, ptá se dále.

- Zeptá se kořenových DNS serverů, zda znají IP adresu pro doménu www.forpsi.eu
  - Kořenový DNS server odpoví, že doménu nezná, ale ví, kdo spravuje DNS záznamy pro doménu EU
  - Pošle tento údaj
- Server informaci použije a zeptá se jednoho ze serverů pro doménu EU. Zda nezná IP adresu domény
  - Tento server pak odpoví, že doménu nezná, ale ví, které servery jsou autoritativní pro doménu forpsi.eu. a ty serveru pošle
- Server opět použije získanou informaci a zeptá se jednoho z autoritativních DNS serverů na doménu
  - Tento server již zná konkrétní IP adresu a tu lokálnímu serveru vrátí
  - Ten pak předá tuto IP adresu zpět prohlížeči → splnil svůj úkol.
- Prohlížeč pak kontaktuje přímo server pod danou IP adresou s požadavkem na zaslání webové stránky a ty zobrazí v počítači.

AD; Active Directory

Adresářové služby LDAP implementované firmou Microsoft pro řadu systémů Windows NT. Umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Active Directory ukládá své informace a nastavení v centrální organizované databázi.

- Vyžaduje instalaci služby DNS
- Založena na standardních internetových protokolech
- Jednoznačně definuje strukturu sítě
- Organizuje skupiny počítačů a domén

Výhody

- Redukce celkových nákladů na vlastnictví
- Úspora času
- Zjednodušená administrace
  - Sdružení dat do jednoho místa (informace o uživatelích, různých zdrojích, aplikacích…)
- Flexibilita
- Škálovatelnost
  - Navrženo tak, že spolehlivě pracuje v jakékoliv velikosti
- Managment Console
  - Jednoduše lze vytvořit administrativní konzolu s takovými nástroji, které jsou potřeba, což umožní pracovat na jednom místě přehledně a efektivně
- Computer Managnemt
  - Nástroj, kterým se konfigurují počítače uživatelů z vlastního počítače

Vnější struktura Active Directory

- Služba Active Directory obsahuje logické i fyzické struktury součástí sítě
- Logická struktura Active Directory je tvořena doménami (domain), organizačními jednotkami (organizational unit), stromem (tree) a lesem (forest).

Doména

Skupina počítačů sdílejících společnou adresářovou databázi.

- Základní jednotka AD, tvoří ji min. 1 DC
- Bezpečnostní hranice ve struktuře Active Directory
- Reprezentuje replikační hranici
- Má jednoznačné označení
- Má vlastní zásady zabezpečení
- Vytváří vztahy důvěry s ostatními doménami

Lesy a stromy domén

- Každá doména služby Active Directory má název DNS (vsps.cz)
- V případě, kdy jedna nebo více domén sdílejí stejná adresářová data, nazývají se LES

Group Policy

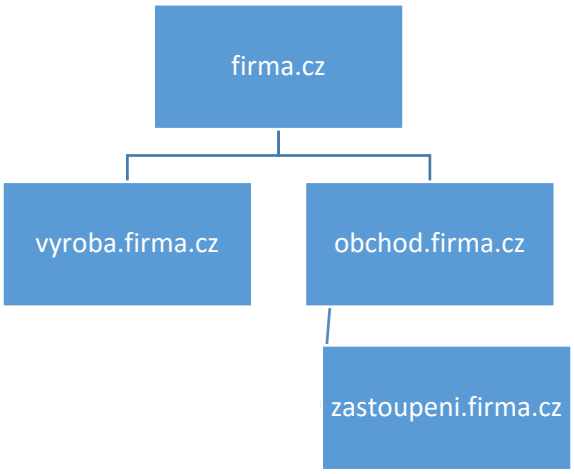
Skupiny zásad (Group Policy) je nástroj pro hromadnou správu oprávnění a nastavení, aplikovaných jak na celý počítač, tak na přihlášeného uživatele. Ve skupinách zásad je možné vytvářet kolekce nastavení, kterým se říká Object GPO, které dokáží měnit konkrétní parametry chování počítače nebo uživatele. Samotné nastavení GPO se pak "linkuje" na jednotlivé organizační jednotku OU v AD, čímž se zajistí aplikování nastavení jen na vybrané počítače nebo uživatele. Tímto způsobem tedy můžeme spravovat potenciálně tisíce počítačů nebo uživatelů změnou jednoho GPO.

Použití

- Aplikování firemních standardů (skrytí ovládacích panelů, síťové tiskárny, spuštění scriptů…)
- Aplikování zabezpečení (změna oprávnění na určitých složkách, složitost hesla, skupiny s možností se lokálně přihlásit…)
- Hromadná instalace aplikací (Office, Adobe Reader, atd.)

Policy "Politiky"

- Politiky se dělí na Lokální a Doménové
- **Lokální**
  - Každý počítač od Windows 2000 má lokální politiky (local Group Policy), které ovlivňují lokální počítač a přihlášené uživatele
  - Pokud počítač není připojen do domény, tak právě lokální politiky jsou jako jediné použity



16. Bezpečnost v OS

Chráněné objekty

- Paměť
- Procesor
- Spustitelné programy
- Sdílená zařízení typu disky
- Znovupoužitelná zařízení (tiskárny, pásky)
- Sdílená dat

Metody ochrany objektů v operačních systémech

- *Fyzická separace* – Procesy pro vykonávání operací různého stupně utajení používají oddělená zařízení
- *Časová separace* – Procesy prováděny v různém čase
- *Logická separace* – Oddělení procesů, že pro každý vytváří iluzi, že má celý počítač pro sebe
- *Kryptografická separace* – Díky kryptografickým metodám ukrytí svých dat
    - Možnost kombinace několika metod separace
    - Ty jsou seřazeny dle rostoucí složitosti a klesající spolehlivosti

Autentizace

- Proces, při kterém je ověřována identita určitého subjektu (uživatele nebo i aplikací, procesů)
- Nejjednodušší autentizace pomocí přihlašovacího jména a hesla (lehce napadnutelná) – **jedno faktorová** (jeden tajný parametr)

Autorizace

- Proces ověřování oprávnění subjektu k provedení akce
- Navazuje obvykle na autentizaci
- Základní informace pro autorizaci v datových strukturách **přístupový záznam** a **deskriptor zabezpečení objektu**
- Oprávnění, která záznam definuje, dědí všechny procesy a aplikace v relaci přihlášení

Interaktivní přihlašování ne Windows

- Základní autentizační úroveň ve Windows
- Údaje pro přihlášení porovnávány s parametrem místního nebo doménového účtu
- Proces zajištěn systémovým procesem Winlogon (winlogon.exe)
- Realizován pomocí balíčků, které provedou analýzu autentizačních údajů a pomocí určitého protokolu provedou ověření
- Pokud autentizace úspěšná, vzniká nová relace

Neinteraktivní přihlašování ve Windows

- Nastává po úspěšné interaktivní autentizaci

Správa hesel ve Windows

- Hesla jsou uložena pomocí šifrovacích obrazů (použití kryptografických algoritmů)
- **Hash** je nejslabší formou zabezpečení hesel ve Windows
- Pro větší bezpečnost nutnost využívat co nejrozmanitější hesla
- Potlačení zpětné kompatibility při ukládání LM hesel, použití více bezpečného algoritmu šifrování než DES a neukládání hesel v otevření podobě

Zabezpečení OS

- Aktualizace operačního systému
  - Pravidelně stahovat aktualizace
- Ochrana proti napadení z internetu
  - Firewall
- Antivirus
  - Avast
  - AVG
  - CA Antivirus
  - McAfee
  - BitDefender
  - TrustPort Workstation
  - …
- Ochrana proti spyware, addware
  - Ad Aware, SpyBot…
- Aktualizace veškerého software
- Zálohovat
- Přechod na jiný os (Linux)
  - Samotný Linux je sám o sobě na rozdíl od Windows bezpečnější OS
  - Škodlivý vir pro Linux prakticky neexistuje (i z důvodu menšího rozšíření a především není možná šířitelnost)
  - Binární spustitelné soubory (kde viry jsou) nejsou přenášeny, ale je přenášen pouze jejich zdrojový kód, který je na stroji přeložen do cílového tvaru
  - Mnohdy stačí aktivovat pouze Firewall, který je navíc zabudován v jádře a nezobrazuje se proto v systémové oblasti

Virus

Škodlivý program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Viry jsou jen jedním z druhů zákeřného softwaru. V obecném smyslu se jako viry (nesprávně) označují červi a jiné druhy malwaru.

Virus nemusí infikovat pouze spustitelné EXE soubory, ale může klidně nakazit i soubory s příponou .DAT, to je možné proto, že jejich vnitřní struktura je podobná .EXE souborům. Minimální pravděpodobností je, že se infikuje nějaký datový soubor (.JPEG, .MP3), protože jeho šíření by potom nebylo z hlediska viru optimální.

Rezidentní / Nerezidentní virus

Nerezidentní vir se ve chvíli spuštění hostitele (ve chvíli, kdy se při spouštění hostitele spustí kód viru) rozšíří do nalezených nenakažených souborů

Rezidentní vir se pouze uloží do operační paměti počítače, ve které zůstane až do doby vypnutí počítače, a mezitím infikuje soubory (nebo např. diskety), se kterými uživatel pracuje.

Stealth viry

- Chrání se před detekcí antivirovým programem použitím tzv. stealth technik
  - Pokud je takový virus v paměti, pokouší se přebrat kontrolu nad některými funkcemi operačního systému a při pokusu o čtení infikovaných objektů vrací hodnoty odpovídající původnímu stavu

Polymorfní viry

- Pokouší se znesnadnit svou detekci tím, že mění vlastní kód. V napadeném souboru není možné najít typické sekvence stejného kódu.

Worms (Červy)

Mnoho lidí zaměňuje viry za červy. Ale jsou zde drobné rozdíly. Dnes už viry skoro vymizely a nahradily je červy. Červ je vlastně nezávislý program, kdežto vir potřebuje nějaký kus kódu, kde by mohl přežívat. Rozdílný je i způsob šíření, kdy vir byl spíše na nějakém médiu, a červ se šíří pomocí internetu, dnes už to tak zcela není. Červy dokáží poměrně snadno přepisovat svůj kód, a tím se stávají velkým problémem pro antiviry.

Trojan horse (trojský kůň)

Tento druh malware se moc neliší od unikátní taktické strategie Římanů v řecké Tróji ve 12. století před naším letopočtem. Stejně jako tehdy se i dnes trojské koně vydávají za neškodný, ba i důležitý software. Stalo se, že se trojský kůň vydával i za antivirový program, Winrar, nebo jen obyčejnou hru. Po nainstalování tohoto „neškodného“ programu se začnou ztrácet data na počítači, nebo vytvářet díry pro napadení další havětí. Instalace nemá ale vždy takovýto průběh. Je možné, že jakmile se dostane do systému, nainstaluje se sám a nahradí nějaké potřebné soubor v používaném programu.

Backdoor

„Zadní vrátka“, ale nemusí být vždy nutně nelegální. Spousta komerčních programů na vzdálenou správu využívá tohoto systému.

Logic bomb (logická bomba)

Podle Erica Filiola: logická bomba je samostatně se nereprodukující malware, který se nainstaluje do systému a čeká na nějakou spouštěcí událost, než začne provádět ničivou nebo jinou ofenzivní funkci.

Bombou může být klidně i kód od třetích stan, ve kterém se vás autoři ptají na licenční číslo produktu. Pokud ho nezadáte do určitého limitu, program přestane pracovat.

Exploit

Druh malware, který dokáže využít slabiny v operačním systému a získat tak přístupová práva. Jak se ve své knize zmiňuje Jirovský: exploity nemají příliš dlouhou životnost. To je způsobeno zejména tím, že ve chvíli, kdy se začne exploit široce využívat, si ho velmi rychle všimnou autoři daného programu a využívanou slabinu opraví.

Keylogger

Zaznamenávání kláves v určitých situacích (hesla, čísla kreditních karet…). Keylogger se hodně špatně hledá, jelikož není vždy aktivní.

Rootkit

Jednoúčelový program pro zamaskování při vniknuti hackera do počítače. Velmi těžko se nalézá. Téměř většinou to znamená reinstall počítače.

Dialer

Tento malware se už moc nepoužívá. Měl totiž v oblibě (u vytáčeného připojení) připojovat počítač třeba přes ústřednu v Asii nebo Tichomoří (60Kč/min).

URL injection

Tento druh je poměrně neškodný, změní třeba přesměrování webových adres. Může z uživatelů tak dostat různé osobní údaje (kódy, hesla k bankovním účtům…).

Spyware

Jde o programy většinou třetích stran, vytvářející statiku pro cílenou reklamu. Spyware nelze úplně označit, jako malware-nejedná se totiž o bezprostřední ohrožení, ani zde není možnost sebeaplikace. Ale nikdo neví, kdo, jak, na co, použije vaše údaje (jména uložená v registrech, seznam otevíraných souborů, informace o softwarech), k jejichž sběru nikdo nedostal žádný souhlas.

Adware

ADvertisement a softWARE (reklamní software). I tento typ nelze přesně označit jako malware. Opět nemá možnost sebeaplikace, uživatel musí souhlasit s instalací a potvrdit licenci. Bývá velmi často součástí programů. Jeho vedlejším účinkem může být i změna domovské stránky v internetovém prohlížeči, nebo vyskakující Pop-up okna.

Hoax

Poplašné zprávy, které si uživatelé posílají mezi sebou. Ve zprávách je napsáno smyšlené nebezpečí (útěk myši ze stolu, roztočení HDD opačným směrem apod.). Na konci bývá připojeno IBM (Microsoft, Apple…) varuje atd.

Phishing

Jsou to e-maily, třeba z fiktivní banky, ve kterých jsou přiloženy formuláře k vyplnění, které pobízejí uživatele vložit citlivé údaje.

Detekce viru

- Antivirový test využívá databázi známých počítačových virů
- Zahájí se logická analýza podezřelého testovaného kódu a porovnává se s kódem virů
- Velmi častým cílem jsou různé generátory klíčů, patche, cracky…

Heuristická metoda

- Vykonává v podstatě dva kroky
  - Pomocí virové databáze hledá známé viry
    - Porovnání dekompilovaného kódu s databází
  - Pokud vir nenajde
    - Zahájí se analýza kódu, testování objektu a posuzuje se, co kód znamená v praxi a jestli dělá něco neobvyklého oproti normálnímu chování kódu
- Podle rozhodujících pravidel nebo vážících metod

Většina antivirových programů, které používají heuristickou analýzu, vykonávají tuto funkci spouštěním programovacích příkazů podezřelého programu nebo spouštěním skriptu v rámci specializovaného virtuálního stroje, a tím umožňují antivirovému programu vnitřně simulovat, co se stane v případě, když podezřelý soubor bude spuštěn při zachování podezřelého kódu, izolovaného od reálného stroje. Ten pak analyzuje příkazy, tak jak jsou prováděny, monitoruje typické virové chování, jako je replikování, přepisování souborů a snaha o utajení existence podezřelého souboru. Jestliže je detekováno jedno nebo více virového chování, je podezřelý soubor označen jako potencionální virus a uživatel je upozorněn.

17. Souborové systémy, oprávnění v různých OS

Všechny datové soubory a programy musí být někde uloženy (HDD, CD…). Nejsou tam uloženy chaoticky, ale podle pevného řádu. Tento řád určuje, jak se mají soubory ukládat a přístupová práva k nim, jak se mají jmenovat, jak jednotlivé soubory hledat, jak se pozná, komu patří… Většina OS podporuje několik různých souborových systémů.

Pevné disky jsou obvykle logicky rozděleny na oddíly, takže souborový systém se rozkládá jen na konkrétním oddílu a ne na celém disku. To umožňuje mít na pevném disku více nezávislých souborových systémů, které mohou být různého typu. Informace uložené v systému souborů se dělí na **metadata** a data.

Metadata popisují strukturu systému souborů a nesou další služební a doplňující informace (velikost souboru…) Pojmem data se pak míní vlastní obsah souboru, který lze přečíst, když se soubor otevře.

Žurnálování

Zápis dat a metadat do systému souborů probíhá v několika krocích. Proto nejsou data a metadata v každém okamžiku konzistentní. Dojde-li v takové chvíli k havárii počítače, zůstane systém souborů v nekonzistentním stavu. Z tohoto důvodu je při dalším startu operačního systému vhodné, aby byla provedena kontrola a nekonzistentní data byla opravena. K tomu může dojít Linuxu nebo ve Windows od W95, nebo je nutné spustit kontrolu ručně. Celková kontrola systému souborů a všech vazeb mezi daty a metadaty je časově velmi náročná operace, při které navíc může dojít ke zbytečné ztrátě částečně zapsaných informací. Proto jsou moderní systémy souborů rozšířeny o žurnálování, které umožňuje po havárii rychlou opravu eventuálních nekonzistencí. Principem techniky je uchovávání chronologického záznamu prováděných operací, do kterého se zapisují všechny prováděné činnosti. Pokud dojde k výpadku napájení, je po restartu nekonzistence opravena návratem do předchozího zaznamenaného stavu za pomoci záznamů z žurnálu. Žurnál je pro ochranu prováděné transakce využíván následujícím způsobem:

- Do žurnálu je zapsáno, co a kde se bude měnit
- Provede se vlastní změna
- Do žurnálu je zapsáno, že operace byla úspěšně dokončena
- Zrušení záznamu v žurnálu

Pokud dojde v kterémkoliv okamžiku k přerušení je možné pomocí dat uvedených v žurnálu uvést systém souborů do konzistentního stavu buď návratem zpět ke stavu před započetím transakce, nebo dokončením přerušené transakce.

Žurnálovací systémy

- NTFS
- HFS+
- ext3, ext4
- XFS
- ReiserFS.
- …

Omezení souborového systému

Různé souborové systémy mohou mít různá omezení.

- Velikost paměťového média, kterou je daný Systém schopen pokrýt
- Délka souboru
- Délka jména souboru
- Počet zanořených podadresářů
- Podporovaná znaková sad

Kvóty

Limity nastavené správcem systému, které určitým, způsobem omezují použití souborového systému. Nejčastěji se kvóty používají na omezení následujících věcí:

- Velikost využitého místa (usage nebo block quota)
- Počet souborů (file nebo inode quota)

Alokační blok

Základní fyzickou (adresovatelnou) jednotkou pevného disku je **sektor** – elementární jednotka diskové kapacity o velikosti 512 bajtů.

Sektory jsou dále slučovány do větších jednotek alokačních bloků/jednotek (nejmenších přidělitelných logických jednotek), se kterými pracuje operační systém

Fragmentace

Stav, kdy jsou data na datovém médiu uložena nesouvisle po částech. Fragmentace může způsobovat neefektivnost práce s uloženými daty (nižší rychlost a/nebo snížení kapacity), případně že část kapacity datového média nelze využít. Novější souborové systémy (ext3…) se snaží zabránit fragmentaci už při zápisu.

Interní fragmentace

Fragmentace uvnitř alokovaných oblastí. Souborový systém vyhradí pro uložení souboru větší prostor než je velikost souboru → Plýtvání přiděleným prostorem

Externí fragmentace

Fragmentace mezi alokovanými oblastmi. Volné místo paměti je obsazováno nesouvislými bloky souborů a prostor mezi nimi lze pak následně zaplnit pouze jednotlivými bloky fragmentovaných souborů. V souborovém systému způsobuje ukládání souborů do fragmentovaných částí zpomalení přístupu → Soubor je rozmístěn na mnoha místech disku, které neleží u sebe.

Defragmentace

Proces zpětného skládání celku z dílčích částí (fragmentů). Pomocí defragmentace se zamezuje externí fragmentaci počítačových dat.

Souborové systémy

FATY

- Tabulku obsahující informace o obsazení disku v souborovém systému.
- Jednoduchý
- **FAT12**
  - Doplněna podpora podadresářů
- **FAT16**
  - Velikost disku podle velikosti clusteru 32MB až 4GB
- **exFAT**
  - Velikost svazku až 128EiB (ExbiByte 1024^6)
  - Nepoužívá žurnál
- Vytvořen 1980
- Velikost disku 2MB
- Neumí podadresáře
- **VFAT**
  - Dlouhá jména souborů
- **FAT32**
  - Velikost disku až 8TB
- Velikost souboru max. 4GB

NTFS

Souborový systém vyvinutý společnostmi IBM a Microsoft, který jej poprvé zavedl ve svém operačním systému Windows NT. Rozšiřitelný souborový systém, který je možné přizpůsobit novým požadavkům.

Vlastnosti:

- Žurnálování
- ACL
- Komprese na úrovni souborového systému
- Šifrování EFS- Encrypting FileSystem)
- Diskové kvóty
- Dlouhá jména souborů
- Pevné a symbolické linky

ext2

Data jsou uložena ve stejně dlouhých blocích. Základní prvek **i-node** – systém identifikuje soubory podle čísla i-node, nikoli podle jejich jména. Bloky jsou rozděleny na skupiny bloků. Adresáře jsou z pohledu ext2 zvláštní soubory, které slouží k vytváření a ukládání přístupových cest k souborům.

Charakteristika:

- Nepoužívá žurnálování!!!
- Lze vytvářet adresáře
- Lze vytvářet různé typy souborů
  - Obyčejný soubor
  - Speciální soubor (reprezentuje zařízení; je typu blokový a znakový)
  - Pojmenované roury
  - Sockety
- Umožňuje používat pevné odkazy, symbolické odkazy…
- Pro každý soubor a adresář se ukládají práva UGO – vlastníka (user), skupiny (group), ostatních (other) a rozšířené atributy

ext3

- Založen na ext2 a je obousměrně kompatibilní s ext2.
- Výchozí souborový systém pro mnoho distribucí.

Výhody oproti ext2

- Žurnálování
- Indexy souborů v adresáři

Nevýhody

- Žádný nástroj pro defragmentaci
- Neobnovitelnost smazaných souborů

ext4

- Podpora svazků o velikosti 1 EiB (1024 PiB – Pibibytů; 10^{18} bajtů)
- Maximální velikost souboru 16TiB (ext pouze 2TiB)
- Oproti ext3 zvýšení možných podadresářů v adresáři z 32 000 na 64 000

Oprávnění Linux

Jelikož jsou unixové systémy víceuživatelské, je zde nutnost nějakého systému přístupových práv, aby uživatelé nemohli přistupovat k citlivým datům jiných uživatelů, páchat škodu na systému a tak podobně. Standard POSIX definuje systém oprávnění, který používají všechny unixové systémy.

Základní unixová přístupová práva

Každý soubor či adresář má svá základní oprávnění. To zahrnuje vlastníka (UID) a skupinu (GID), a dále oprávnění ke čtení (**read**), zápisu (**write**) a spuštění (**execute**) pro vlastníka (user), skupinu (group) a ostatní uživatele (others).

Právo	Význam u souboru	Význam u adresáře
r	Čtení souboru.	Čtení názvů obsažených položek.
w	Zápis do souboru.	Vytváření souborů a adresářů.
x	Spuštění souboru.	Vstup do adresáře.

Výpis LS v adresáři:

```
-rw------- 1 dave home      16 2009-11-08 14:34 muj_tajny_soubor.txt
prw-r--r-- 1 dave home       0 2009-11-08 14:43 pojmenovana_roura|
drwxr-xr-x 1 dave home       0 2009-11-08 14:37 prazdny_adresar/
-rwxr-xr-x 1 dave home 5558272 2009-11-08 14:37 spustitelny_soubor*
lrwxrwxrwx 1 root root      20 2009-11-08 14:35 cosi.txt
```

První sloupec obsahuje znaky r, w, x (vlastník, skupina, ostatní). Vlastník může s adresářem manipulovat, jak chce (rwx), zatímco skupina a ostatní do něj mohou jen vstoupit a vypsat si jeho obsah (r-x).

Další důležitá věc je vyjádření práv v osmičkové číselné soustavě.

Právo	Hodnota
r--	4
-w-	2
--x	1

Znak	Význam	Čeho je znak zkratkou
-	obyčejný soubor	-
b	soubor blokového zařízení	block device
c	soubor znakového zařízení	character device
d	adresář	directory
l	symbolický odkaz	symbolic link
p	pojmenovaná roura	named pipe
s	unixový socket	unix socket

Základní oprávnění souboru či adresáře lze tedy vyjádřit trojciferným číslem, přičemž první číslo udává práva vlastníka, druhé skupiny a třetí ostatních uživatelů.

chmod

Příkaz sloužící pro změnu práv souboru/složky.

```
chmod 755 skript.sh
chmod u+x soubor.run
chmod g+rwx soubor.txt              //skupina RWX
chmod u-x,g-wx,o-rwx "soubor s mezerami v nazvu"
chmod u=rwx,g=rw,o=r filename.ext
```

```
chmod -R 755 adresar/    //přepínač R – rekurzivně; pro složky
```

chown

Příkaz sloužící ke změně vlastníka a skupiny souborů a adresářů.

```
chown jmeno_uzivatele soubor.txt
chown uživatel:skupina "soubor.txt"
```

chgrp

Příkaz sloužící ke změně vlastnické skupiny souborů a adresářů.

```
chgrp home x //stejné jako chown :home x
```