Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

ŠTÁTNY PEDAGOGICKÝ ÚSTAV
NATIONAL INSTITUTE FOR EDUCATION

Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

Operačné systémy 3

Predmet: Operačné systémy

Línia: Vlastný odborový kontext informatiky a informatickej výchovy

Operačný program VZDELÁVANIE

EURÓPSKA ÚNIA
Európsky sociálny fond

Európska únia
Európsky sociálny fond

Moderné vzdelávanie pre vedomostnú spoločnosť/Projekt je spolufinancovaný zo zdrojov ES

Operačné systémy 3

Identifikácia modulu

Aktivita projektu:	1.2 Vzdelávanie nekvalifikovaných učiteľov informatiky na 2. stupni ZŠ a na SŠ
Línia aktivity:	Vlastný odborový kontext informatiky a informatickej výchovy
Predmet:	Operačné systémy

Garant predmetu:

PaedDr. RNDr. Ladislav Huraj, PhD.
KAI FPV UCM
ladislav.huraj@ucm.sk

Autori:

PaedDr. RNDr. Ladislav Huraj, PhD.
prof. Ing. Miloš Šrámek, PhD.
Mgr. Miroslav Wagner

Zaradenie modulu

Modul Operačné systémy 3 je tretím a posledným modulom predmetu Operačné systémy vzdelávania v rámci aktivity 1.2 projektu ĎVUi; modul štvrtého semestra.

Abstrakt modulu

Modul je tretím modulom, ktorý dopĺňa predchádzajúce moduly zamerané na dva z najpoužívanejších operačných systémov (MS Windows a Linux). Rovnako ako predchádzajúce moduly aj tento modul je postavený na prezentovaní nástrojov operačných systémov.

V module sme sa zámerne vyhli problematike sietí a sieťových nastavení, keďže na túto tému existujú v DVUI vzdelávaní pre druhú cieľovú skupinu špeciálne moduly Internet: princípy a tvorba webu 1, Počítačové systémy 5: Počítačové siete.

Poznamenajme, že cieľom nie je zachádzať do detailov, ale oboznámiť účastníkov zo základmi jednotlivých celkov. Modul je delený na nasledovné štyri hlavné celky:

- Bezpečnosť OS
- Virtualizácia
- Štruktúra OS
- História OS

Obsah

Úvod

Operačný systém sa stará o správu jednotlivých prostriedkov, ktoré sa nachádzajú v počítači. Používatelia počítača si málokedy uvedomujú, ako často operačný systém zasahuje pri spúšťaní jednotlivých programov. Operačný systém okrem iného zaisťuje efektívne využívanie univerzálneho procesora, operačnej pamäte, diskov a ostatných zariadení počítača. V neposlednej miere sa používateľovi snaží zabezpečiť príjemné prostredie pre prácu i zábavu. K úplnému pochopeniu činnosti operačného systému je potrebné pozrieť sa pod jeho povrch.

Už v predchádzajúcich moduloch Operačné systémy 1 a 2, sme sa zoznámili s dvomi zo základných predstaviteľov operačných systémov OS Windows a OS Linux. Úlohou tohto modulu je pozrieť sa na OS z pohľadu bezpečnosti, virtualizácie a historického vývoja. Modul rozoberá aj vnútornú štruktúru OS a aktivity OS vo všeobecnej rovine. V module zámerne nie je rozoberaná problematika sietí a sieťových nastavení v OS, keďže na túto tému existujú v DVUI vzdelávaní pre druhú cieľovú skupinu špeciálne moduly *Internet: princípy a tvorba webu 1, Počítačové systémy 5: Počítačové siete*.

Výučba modulu bude v počítačovej učebni s nainštalovaným OS Windows XP.
Výučba virtualizácie je zameraná na systém VirtualBox. Ten možno použiť buď na počítačoch v učebni alebo na notebookoch účastníkov. Ako hosťujúci systém možno použiť predinštalovaný systém Ubuntu podľa inštrukcií na stránke modulu 2OS3, alebo aj LiveCD/DVD podľa vlastného výberu.

Cieľ modulu

Modul je záverečným modulom predmetu Operačné systémy a nadväzuje na moduly OS1 a OS2. V rámci tohto modulu získajú účastníci vzdelávania príležitosť nadobudnúť rozširujúce vedomosti a zručnosti s problematikou bezpečnosti, virtualizácie a histórie operačných systémov. Navyše sa uchádzači čiastočne oboznámia s teoretickým modelom operačného systému. Cieľom modulu je, *prehĺbiť* si pomocou vhodných nástrojov operačného systému vedomosti a zručnosti z princípov daných systémov. Úroveň získaných vedomostí účastníkov je stanovená tak, aby boli dostačujúce pre vyučovací proces, prípadne tvorili dobrý základ pre ďalšie individuálne štúdium.

Vzhľadom na profil absolventa vzdelávania v rámci aktivity 1.2 je tento modul súčasťou línie Informatika.

Vstupné vedomosti

Požadované prerekvizity

Absolvovanie modulu Operačné systémy I., Operačné systémy II. a modulu Internet: princípy a tvorba webu 1.

Predpokladané vstupné vedomosti, skúsenosti a zručnosti

Účastník vzdelávania má základné zručnosti pri práci s operačným systémom a webovým prehliadačom, pozná prostredia OS Windows XP a OS Ubuntu.

1 Bezpečnosť OS

Bezpečnosť patrí ku kritickým bodom operačných systémov. Niektoré prvky bezpečnosti OS z používateľského hľadiska, ako napr. prístupové práva, tvorba skupín a pod., už boli preberané v predchádzajúcich moduloch. Ďalšie sú zaradené práve do tohto celku.

Časť Bezpečnosť OS oboznamuje so základnými zásadami tvorby hesiel, ako aj s rizikami spojenými so správou hesiel a útokmi na heslá. Popisuje spôsoby zálohovania a obnovy systému ako jedného zo základných prvkov bezpečnosti dát. Pomocou existujúcich stránok poukazuje na to, aké informácie unikajú o OS cez webový prehliadač. Detailnejšie popisuje problém počítačových infiltrácii a spôsoby ochrany operačného systému proti infiltrácií. Vysvetlený je pojem izolované prostredie používané na otestovanie softvéru z nedôveryhodného zdroja, ako aj ukážka takéhoto prostredia. Navyše je pri preberaní bezpečného softvéru zopakovaná myšlienka digitálneho podpisu z modulu Internet: princípy a tvorba webu 1.

Hoci podkapitoly tejto časti sú zamerané predovšetkým na OS Windows, princípy a techniky v nich preberané sa dajú zovšeobecniť pre všetky operačné systémy. Bezpečnosti z pohľadu OS Linux je venovaná samostatná podkapitola.

1.1 Prihlasovanie do systému – tvorba hesla

Biometria je jednoznačná identifikácia/autentifikácia osôb na základe jedinečných fyziologických znakov človeka.

Existujú dva typy fyzických charakteristík človeka:

- jeho fyziológia (odtlačky, tvár, časti jeho tela...)
- chovanie (reč, podpis, dynamika stláčania kláves, chôdza...).

Biometrické systémy identifikujú/autentifikujú priamo človeka, nie predmety, kódy alebo heslá.

V súčasnosti sa biometrické údaje zaznamenávajú aj napr. v slovenských cestovných pasoch.

Prihlásenie sa do systému, či už ako bežný používateľ alebo ako správca systému, patrí medzi kľúčové bezpečnostné prvky súčasných operačných systémov.

S prihlasovaním sú spojené predovšetkým dva pojmy: identifikácia a autentifikácia.

Identifikácia – neoverené prehlásenie (osoby, počítača, programu,…) o svojej identite, napr. prihlásenie používateľa do počítača, do lokálnej siete alebo programu menom, skratkou a pod., meno za výzvou login, vloženie platobnej karty do bankomatu, …

Autentifikácia - je proces overenia, že prihlásený používateľ je naozaj tým, za koho sa prehlasuje.

Autentifikácia niečím:

- čo poznáme: heslo, šifrovací kľúč
- čo máme: mechanický kľúč, magnetická karta, čipová karta, …
- čím sme: odtlačok prstu, dlane, obraz očného pozadia, …
- čím sa prejavujeme: dynamika podpisu, určitá akcia, …

Najbežnejším spôsobom prihlasovania do systému je spôsobom „čo poznáme“ a to použitím prihlasovacieho mena a hesla.

Každý systém má vlastnú bezpečnostnú politiku, ako zaobchádzať s heslami. Vo všeobecnosti však platia nasledovné zásady narábania s heslom:

- dĺžka hesla najmenej 8 znakov (znaky vyberať z celej typovej ponuky, t.j. využívať veľké a malé písmena, číslice, špeciálne znaky)

- heslo má byť ľahko zapamätateľné, má sa dať ľahko a rýchlo zadať, ale nie je možné ho nepovolanou osobou uhádnuť

- heslo nikdy neprezrádzať

- heslo nikdy nikam nezapisovať a neukladať

- pre rôzne systémy používať rôzne heslá

- heslo pravidelne meniť [1].

Existuje veľa odporučení a návodov, ako vytvárať vhodné heslá. Uvedieme aspoň jeden z nich:

Ako základ je vybraná kľúčová veta, napr. „Prsi prsi len sa leje nezatvaraj mila dvere“. Kľúčová veta nesmie obsahovať akúkoľvek permutácii používateľského mena. Následne je veta obohatená o modifikáciu, ktorá je čo najviac neštruktúrovaná, nesystematická, nezmyselná, unikátna, jednoducho nepredikovateľná. Najlepšie je kľúčovú vetu rozbiť aspoň dvoma rôznymi metódami. Nap. miesto medzery vložíme posledné písmeno slova, ale s veľkým písmenom „PrsilprsillenNsaAlejeEnezatvarajJmilaAdvereE“. Druhým rozbitím môže byť modifikácia „dvere - door“, čiže „PrsilprsillenNsaAlejeEnezatvarajJmilaAdoorR“. Ďalšie zaujímavé spôsoby rozbitia kľúčovej vety je možné nájsť v [2].

Problém pri návodoch tvorby hesiel je v tom, že každý kto vymyslí nejaký systém tvorby hesiel vie, že ak ho prezradí, budú všetky jeho heslá oslabené. To je dané samotným princípom takého systému.

Hrozby spojené s heslami:

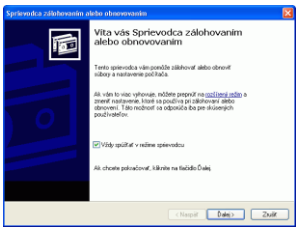
- Útok hrubou silou (brute-force attack) – pri tomto pokuse o prelomenie ochrany heslom sú automaticky skúšané všetky možné kombinácie znakov z vybranej abecedy (písmená, číslice, zvláštne symboly a pod.), danej dĺžky. Zvláštnym variantom sú tzv. masky, kde útočník pozná určité časti hesla na vybraných pozíciách, takže testuje iba zostávajúce znaky hesla (napr. pri odpozorovaní niektorých znakov pri písaní na klávesnici). Takýto útok je často značne časovo náročný.
- Slovníkový útok (dictionary attack) – snaží sa eliminovať najväčšiu slabinu útoku hrubou silou – časová náročnosť. Skúša tak slová z preddefinovaného slovníka, dokáže s nimi vykonávať niektoré základne operácie, ako napríklad jednoduchá permutácia, doplnenie číslic, mínusok, zámena veľkosti písmen a pod.

Existuje množstvo softvérových nástrojov, ktoré uľahčujú útočníkom prelomenie hesiel, prípadne zjednodušujú hľadanie a následné zneužitie slabých miest v systéme. Niektoré z nich je možné nájsť napr. na:

http://www.hackersenigma.com/hacking-tools/

Zadanie 1	Na stránke DVUI kurzu si otvorte súbor hesla.txt používaný na slovníkový útok. Nachádza sa v ňom aj vaše heslo? Pozrite si aj český a anglický slovník.
Zadanie 2	Prehliadače ponúkajú možnosť uloženia hesla pre ďalšie použitie. Otvorte v internetovom prehliadači zoznam uložených internetových hesiel. Pre Firefox: Nástroje – Možnosti – Bezpečnosť – Uložené heslá – Zobraziť heslá Pre MS Internet Explorer je potrebný špeciálny (malý) softvér, napr. IE PassView (stiahnite a spustite si ho zo stránky kurzu). Kedy je/nie je bezpečné heslá uvedeným spôsobom ukladať?
Zadanie 3	Koľko možných hesiel existuje, ak je heslo dĺžky 12 a obsahuje iba veľké písmená? Ak počítač otestuje milión hesiel za sekundu, ako dlho mu bude trvať otestovať všetky heslá? Ako sa čas zmení, keď do hesla pridáme možnosť malých písmen a cifier? Ako sa zmení, ak dĺžka hesla je len 8 znakov?

1.2 Záloha a obnova systému



Sprievodca zálohovaním a obnovením v OS Windows XP.

Program sa spúšťa cez *Štart -> Programy -> Príslušenstvo -> Systémové nástroje -> Zálohovanie*.

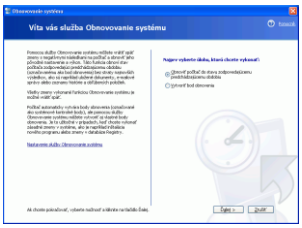
Dáta sú zvyčajne tým najcennejším, čo sa v počítači nachádza, preto je vhodné ich zálohovať. Tento fakt je však veľakrát docenený až keď sú cenné dáta nenávratne stratené. Na zálohovanie je možné využiť niektorý zo špecializovaných zálohovacích programov, avšak súčasťou OS Windows XP je už zálohovací program *Sprievodca zálohovaním a obnovením*.

Program je možné použiť v jednoduchom režime sprievodcu alebo v rozšírenom režime, ktorý je voliteľný hneď po spustení programu. Po kliknutí na tlačidlo Ďalej je na výber voľba *Zálohovať súbory a nastavenie* a voľba *Obnoviť súbory a nastavenie*. Na zálohovanie je niekoľko možností:

- *Moje dokumenty a nastavenia* – zálohuje sa adresár Moje dokumenty, obľúbené položky a adresár s cookies aktuálne prihláseného používateľa.
- *Dokumenty a nastavenia všetkých používateľov* - zálohuje sa adresár Moje dokumenty, obľúbené položky a adresár s cookies všetkých používateľov.
- *Všetky informácie v tomto počítači* – zálohujú sa všetky údaje na pevných diskoch počítač a vytvorí sa možnosť jednoduchej obnovy systému.
- *Manuálne vybrať položky*, ktoré sa budú zálohovať

Pri výbere niektorej z prvých troch možností sa program opýta na umiestenie a názov súboru so zálohou. Zaujímavá je najmä voľba *Prírastkové zálohovanie*, ktorá spôsobí zálohovanie len tých súborov, ktoré sa od posledného zálohovania zmenili. Pri možnosti *Manuálne vybrať položky*, sa navyše zobrazí dialógové okno, v ktorom je potrebné zvoliť adresáre a súbory, ktoré sa majú zálohovať.

Obnoviť súbory zo zálohy je možné pomocou voľby *Obnoviť súbory a nastavenie* v druhom kroku sprievodcu vybraním súbor so zálohou.



Nástroj Obnovenie systému

Rovnako ako používateľské dáta je možné zálohovať a obnoviť aj konfiguráciu operačného systému. OS Windows XP pre tento účel ponúka nástroj *Obnovenie systému*. Operačný systém automaticky vytvára systémové kontrolné body, tzv. body obnovenia, v pravidelných intervaloch, pri rozsiahlych zmenách konfigurácie alebo pri inštalácií kritického softvéru alebo ovládačov. Body obnovenia je možné vytvoriť aj ručne. Pomocou služby *Obnovenie systému* je potom možné z vybraných bodov obnoviť pôvodné nastavenia operačného systému a tak vrátiť späť zmeny s negatívnymi následkami na OS, alebo na celkový chod počítača.

Po spustení programu Obnovenie systému sú na výber dve položky: *Obnoviť počítač do stavu zodpovedajúcemu predchádzajúcemu obdobiu* alebo *Vytvoriť bod obnovenia*. Možná je aj konfigurácia programu voľbou *Nastavenie služby obnovenie systému* (množstvo voľného miesta pre body obnovenia na diskoch, príp. vytváranie bodov obnovenia úplne vypnúť). Nový bod obnovenia sa vytvára voľbou *Vytvoriť bod obnovenia* a pre lepšiu orientáciu je vhodné zadať adekvátny názov vytváraného bodu obnovenia. Na vrátenie systému do stavu z určitého predchádzajúceho obdobia je potrebné po voľbe *Obnoviť počítač do stavu zodpovedajúcemu predchádzajúcemu obdobiu* vybrať v kalendári bod obnovy zobrazený hrubým písmom pri označení dňa, pričom sa pri kliknutí na daný deň v pravej časti zobrazí zoznam bodov obnovenia pripadajúcich na daný deň reprezentovaný ich popismi. Po výber je nutný reštart systému.

Zadanie 4	Pomocou nástroja Zálohovanie a obnova OS Windows XP vytvorte zálohovací bod s dnešným dátumom. Obnovte systém z vytvoreného zálohovacieho súboru.

1.3 Čo sa dá dozvedieť o našom OS cez web

Činnosti ako prehliadanie internetových stránok. vyhľadávanie, zbieranie, odovzdávanie informácií, prispievanie do diskusných fór, elektronická pošta, chat sú bežnými aktivitami používateľov operačného systému. Mnohí sa však mylne domnievajú, že keď nevidia konkrétne osoby, ktoré stoja za internetovými službami

(poskytovatelia internetových služieb, prevádzkovatelia serverov), nikto nemôže vystopovať ich činnosť. Ľudia sa cítia rovnako anonymne aj voči ostatným používateľom internetu, keďže celá komunikácia sa zdanlivo odohráva len na obrazovke monitora. Môže z toho plynúť pocit bezpečia a neohroziteľnosti, ktorý je veľkým lákadlom pre mnohých používateľov internetovej siete. Z uvedených faktov však vyplýva pár otázok na zamyslenie. Je skutočne naša činnosť anonymná a nepozorovateľná? Dokážu nepovolané subjekty vypátrať, pozmeniť alebo nejakým spôsobom zneužiť dáta? Ak áno, ako sa môžeme brániť voči narušiteľom?

Kto pozná IP adresu nášho počítača, dokáže zistiť veľa informácií, napríklad:

- navštívené webové stránky
- poskytovateľa služieb internetu
- používané programy, verzie programov...

Ľahko odhaliteľná je IP adresa, hostname, DNS server, používaný operačný systém, verzia prehliadača. Uvedené a ďalšie údaje o sebe môžeme vidieť aj na nasledujúcich stránkach:

http://ip-address.domaintools.com/

http://www.ipaddresslocation.org/

http://private.dnsstuff.com/tools/aboutyou.ch

http://www.leader.ru/secure/who.html

Z viacerých dôvodov je vhodné sa chrániť a neposkytovať možným útočníkom veľa informácií. Existuje viacero prostriedkov na ochranu pred nechcenými pozorovateľmi. Niektoré z nich sú bezplatné a on-line, na druhej strane sú aj menej spoľahlivé. Väčší stupeň ochrany poskytujú platené anonymizéry. Jedná sa o programy, ktoré je potrebné stiahnuť a nainštalovať. K dispozícii sú časovo aj funkčne obmedzené verzie spomenutých programov.

Naopak, v prípade, že je potrebné, aby boli všetky informácie (história, dočasné súbory, obrázky, cookies, ...) bezpečne po skončení prezerania v prehliadači odstránené z počítača je vhodné v prehliadači zapnúť službu Súkromné prehliadanie. Napr. pre prehliadač Mozilla Firefox je to cez menu *Nástroje - Spustiť službu Súkromné prehliadanie*, pre Internet Explorer cez *Nástroje - Prehľadávanie so službou InPrivate*.

Zadanie 5	Pomocou stránky http://aruljohn.com/details.php vyšetrite, aké informácie je možné o vašom systéme zistiť cez web.
Zadanie 6	Zopakujte predchádzajúcu aktivitu s tým, že na stránku pristupujete cez stránku anonymizéra, napr. http://anonymouse.org. Aké zmeny nastali vo výpise?

1.4 Ako sa brániť napadnutiu

Počítačová infiltrácia – vírusy, červy, trójske kone ...

Pojem škodlivý softvér vznikol z anglického slova MALWARE – MALicious softWARE a vo všeobecnosti si pod týmto pojmom môžeme predstaviť počítačovú infiltráciu, teda akýkoľvek neoprávnený vstup do počítačového systému. Škodlivý softvér môžeme rozdeliť nasledovne:

- **Vírus** je program, ktorý pripája svoje kópie k vykonávateľným súborom a zabezpečuje ich aktiváciu. Jeho názov je odvodený od podobnosti s vírusmi v biológii. V súčasnosti sa vírus do počítača môže dostať najmä z internetu. Ďalšími

Anonymizér

Jednou z možností ako čiastočne skryť osobné informácie cez web je využitie nástroja anonymizér (anonymný proxy server), pomocou ktorého používateľ pristupuje ďalej do internetu, pričom sú však zobrazované identifikačné údaje anonymizéra.

Príkladom takéhoto plnohodnotného nástroja na vytváranie anonymity pre prehliadanie webu je napr. JAP anonymizér.

JAP anonymizér používa a premiešanie požiadaviek od používateľa viacero serverov, čím dosahuje vysokú mieru anonymity.

Na druhej strane prechod viacerými servermi spomaľuje prenos prenášaných dát.

možnosťami jeho šírenia je napríklad prenos v rámci lokálnej siete, či kopírovanie z dátového média ako USB zariadenie, CD, DVD, a podobne. Existujú súborové vírusy, čiže samostatné škodlivé programy, boot vírusy, ktoré napádajú zavádzací sektor disku a zabezpečia tak svoj štart už pri spustení (bootovaní) počítača a makrovírusy, ktoré sú najčastejšie súčasťou dokumentov s príponou „.doc“ a „.xls“. Ďalšie delenie vyplýva zo spôsobu vykonania škodlivej činnosti. Zatiaľ čo vírusy priamej akcie vykonajú svoju aktivitu v okamihu spustenia zavíreného objektu, rezidentné vírusy zostanú v pamäti počítača a vykonávajú škodlivú činnosť.

- **Trójsky kôň** je škodlivý program, ktorý na rozdiel od vírusov alebo červov nemá schopnosť samostatne sa kopírovať a tým infikovať súbory. Súbor v zásade neobsahuje nič iné okrem samotného škodlivého kódu. Trójsky kôň sa môže vydávať za užitočný program, ktorého činnosť však vôbec nemusí vykonávať, ale na pozadí realizuje záškodnícku činnosť. Trójsky kôň je pomerne univerzálny a môže mať rozličné funkcie, od zasielania stlačených kláves (keylogger) až po mazanie súborov (napr. sformátovaním disku), alebo tiež špeciálnu funkciu akou je inštalovanie tzv. backdooru.
- **Backdoor** je aplikácia typu klient - server, ktorá umožní autorovi vzdialený prístup na počítač. Hlavný rozdiel oproti legálnym aplikáciám s podobnou funkciou je, že proces inštalácie prebieha bez vedomia klienta. Takýto počítač sa väčšinou stáva súčasťou väčšej siete infikovaných počítačov tzv. botnetu, ktorú možno automatizovane riadiť prostredníctvom nástrojov vzdialenej správy pre spustenie koordinovaného útoku.
- **Červ** je samostatný program, ktorý rozširuje svoje kópie pomocou internetu alebo lokálnej siete. Na rozdiel od klasického vírusu, ktorý je pasívny a na rozšírenie potrebuje kopírovanie nakazeného súboru, červ sa rozširuje aktívne, rozosielaním kópií po lokálnej sieti alebo internete využívajúc e-mailovú komunikáciu, prípadne na nižšej úrovni bezpečnostné diery operačného systému. Červ môže so sebou niesť aj ďalší škodlivý program, ktorý môže vykonať rozličné činnosti, ako napr. inštalovať tzv. backdoor. Aj bez ďalších škodlivých programov môže červ spôsobiť veľké škody vplyvom zahltenia komunikačných kanálov. Dôsledkom rozšírenosti internetu je červ schopný rozdistribuovať sa po celom svete v priebehu niekoľkých hodín. Vedľajším efektom môže byť kompletné zahltenie LAN siete.
- **Spyware** je program, ktorý využíva internet na posielanie rozličných údajov o používateľovi bez jeho vedomia. Spyware programy zväčša odosielajú štatistické údaje, ako napr. informácie o nainštalovaných programoch, navštívených stránkach, odchytene prístupové mená a heslá, čísla kreditných kariet zadaných pri nákupe cez web a pod. Získané informácie bývajú v zásade zneužité na cielenú reklamu.

Firewall

S programom Brána firewall systému Windows sme sa už stretli v predchádzajúcom module *Základy hardvérového a softvérového vybavenia počítača (2DG3)*.

Firewall ako zariadenie, ktoré je súčasťou počítačového systému, slúži na riadenie a zabezpečovanie sieťovej prevádzky medzi sieťou a počítačom (príp. aj celou inou sieťou), tzn. jeho úlohou je zablokovať neoprávnený prístup a povolenú komunikáciu umožniť. Zjednodušene sa dá povedať, že slúži ako kontrolný bod, ktorý definuje pravidlá pre komunikáciu medzi počítačom a sieťou.

Firewall môže byť realizovaný buď ako hardvér alebo ako softvér, alebo ako kombinácia oboch. Moderné operačné systémy majú už priamo zabudovaný softvérový firewall.

Firewall predstavuje prvú obrannú líniu. Jeho úlohou je podľa definovaných pravidiel riadiť prevádzku.

OS Windows XP tiež využíva softvérový firewall. Keď je Brána firewall systému Windows zapnutá, komunikácia väčšiny programov prostredníctvom brány firewall je zablokovaná. Na odblokovanie programu je potrebné program pridať do zoznamu výnimiek. Každým povolením výnimky na umožnenie komunikácie programu cez bránu Windows Firewall sa však stáva počítač zraniteľnejším. Povolenie výnimky je ako prederavenie brány firewall. Ak je takýchto dier veľa, brána firewall nemôže plniť svoju funkciu. Počítačoví piráti používajú často softvér prehľadávajúci internet a vyhľadávajú pri tom počítače s nechránenými pripojeniami.

Na zníženie rizík ohrozenia platí niekoľko zásad: (i) výnimky sa udeľujú iba v nutnom prípade, (ii) výnimka sa nikdy neudeľuje programu, o ktorého dôveryhodnosti nie je nič známe, (iii) ak už výnimka nie je potrebná, treba ju odstrániť.

Zadanie 7	Pomocou voľby *Štart -> Nastavenie -> Ovládací panel -> Brána Firewall* skontrolujte, či je na vašom počítači firewall zapnutý. Ktoré programy sa nachádzajú vo výnimkách?

Antivírus

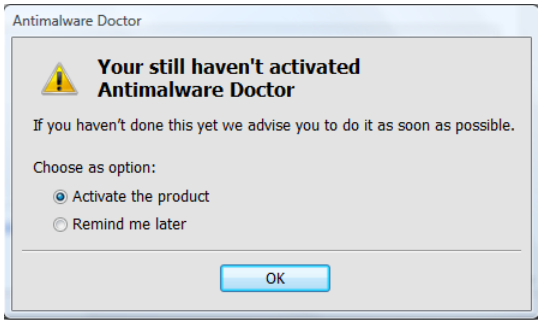
Programy typu antivírus, anti-spyware a anti-spam boli rovnako už rozobrané v predchádzajúcich moduloch. Navyše súčasné antivírusové programy už v sebe zahŕňajú všetky z uvedených podtypov softvéru. Táto podkapitola sa snaží upozorniť na nový fenomén v tejto oblasti, a to falošné antivírusové programy.

Príklad výpisu fiktívnych hrozieb falošného antivírusu

Priebeh infiltrácie falošným antivírusovým programom je zvyčaje nasledovný: plocha OS Windows sčernie, na obrazovke sa objavia blikajúce okná vírusov, a neznámy antivírus ponúka riešenie tohto problému. Neznámym "dobrodincom" je však tzv. *falošný antivírus*, často tiež označovaný ako "rogueware" alebo "fake AV". Zaujímavé je aj to, že kým v minulosti boli takéto podvodné programy "ponúkané" zadarmo a útočníci zarábali predovšetkým na ovládnutí PC a odcudzení dát, teraz si v celej rade prípadov ešte nechajú zaplatiť nákup ďalších služieb alebo softvéru. Pre tento účel využívajú rôzne sofistikované spôsoby, ako napr. nepravdivo upozorňuje používateľa na detekciu malwaru, zobrazí animáciu signalizujúcu zrútenie systému a reštartuje počítač, zámerné naruší systém alebo nahrá ďalší malware, ktorý detekuje ozajstný antivírusový softvér, či dokonca autori vytvoria skutočnú on-line podporu, na ktorú sa používateľ môže obrátiť. Vzhľad programov útočníci doviedli do takej dokonalosti, že s odlíšením falošných a pravých antivírusov majú problém aj odborníci.

Príklad úvodnej obrazovky falošného antivírusu

Platí zásada, že si treba dobre premyslieť skôr, ako na obrazovke niečo potvrdíme.



Obrázok 1 Ukážka vyskakovacieho okna pre falošný anti-malware vyzývajúca používateľa nainštalovať škodlivý program

Skontrolovanie počítača pomocou bezplatného on-line antivírusového programu OneCare spoločnosti Microsoft: http://onecare.live.com/site/sk-sk/default.htm

Zadanie 8	Na internete nájdite on-line antivírusový program. Vedeli by ste ho spustiť?
Zadanie 9	Akým spôsobom by ste odstránili falošný antivírus?

Iné nebezpečenstvá – rootkit, keylogger

Rootkit je špeciálny typ infiltrácie, ktorý má schopnosť skryť svoju prítomnosť v napadnutom systéme, a tak uniknúť detekcii. Zväčša ide o balík škodlivého kódu, ktorý umožňuje útočníkovi zneužiť zraniteľné miesta v systéme a získať tak plnú kontrolu nad napadnutým počítačom. Pri rootkitoch je najdôležitejšia prevencia, čiže schopnosť proaktívne zastaviť infiltráciu už pri pokuse preniknúť do systému skôr, ako sa stihne aktivovať jej činnosť. Rootkit sa dokáže v systéme po svojej aktivácii zamaskovať, a tým sa stať neviditeľný pre používateľa aj antivírusové programy. Napadnutý používateľ tak môže získať falošný pocit bezpečia.

Na stránke DVUI kurzu nájdete aj video, ktoré ukazuje činnosť keyloggera, jeho aktiváciu, odchytávanie údajov, ako aj samotné zobrazenie všetkých odchytených údajov a hesiel v počítači.

Keylogger je program, ktorého úlohou je zachytávať všetko čo používateľ zadá na klávesnici. Potenciálneho útočníka zaujímajú najmä zachytené prihlasovacie mená a heslá, ale môže sa dozvedieť aj iné dôverné informácie. Keylogger môže byť súčasťou trójskeho koňa, ale môže byť aj úmyselne nainštalovaný vlastníkom počítača, aby monitoroval jednotlivých používateľov, napr. v internetovej kaviarni alebo doma.

Zadanie 10	Zo stránky kurzu si prehrajte video, ktoré demonštruje činnosť rootkitu po inštalácii. Čím sa líši oproti obyčajnému vírusu?

1.5 Sandbox – ako spúšťať neznámy softvér

V počítačovej terminológii je všeobecne používaným pojmom pre **izolované prostredie** anglické slovo „sandbox“, ktoré v doslovnom preklade znamená „pieskovisko“. Môžeme teda predpokladať, že sa jedná o prostredie, v ktorom je možné „hrať sa“ určitým spôsobom bezpečne. V literatúre, príp. na internete je možné stretnúť sa tiež s pojmami „sandboxing“ alebo „secure isolation“.

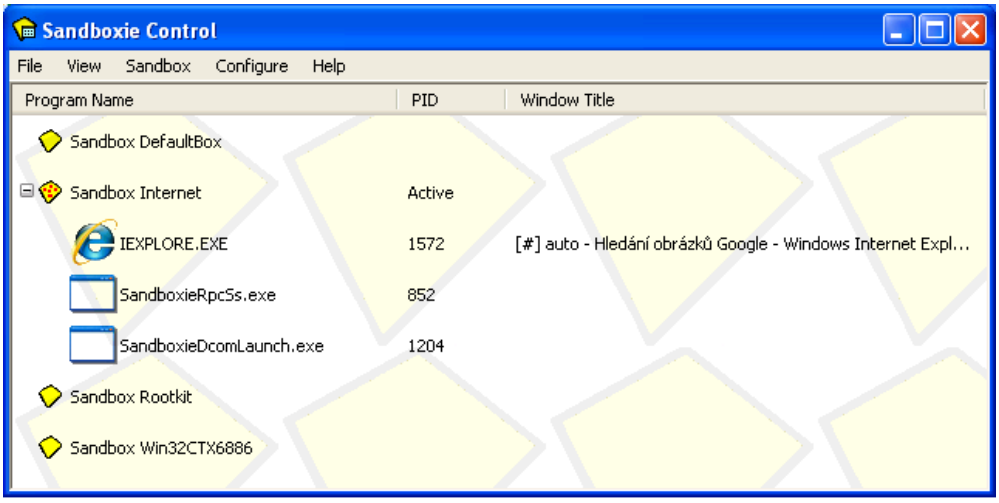
Izolované prostredie môžeme tiež definovať ako malé, uzavreté prostredie ponúkajúce minimálny súbor služieb používané ako testovacia oblasť. Akcie vykonávané v rámci izolovaného prostredia sú bezpečne obsiahnuté v tejto izolovanej oblasti bez možnosti uniknúť von a tým ovplyvňovať ďalšie dôležité súčasti systému.

Izolované prostredie je bezpečnostné prostredie okolo systému či programu, ktoré je väčšinou postavené na tom, že sú potenciálne nebezpečné činnosti (prístup k súborom atď.) jednoducho zakázané.

Jedným z programov, ktorý predstavuje konkrétne izolované prostredie, a prostredníctvom ktorého je možné testovať odolnosť voči reálnym hrozbám, je program Sandboxie. Po nainštalovaní programu Sandboxie je spustenie testovaného programu jednoduché. Stačí ikonu programu pretiahnuť myšou do okna Sandboxu, alebo kliknúť na ikonu testovaného programu pravým tlačidlom myši a vybrať ponuku „Spustit v Sandboxu“.

Príkladom takéhoto izolovaného prostredia je program Sandboxie.

Program Sandboxie je možné bezplatne stiahnuť z adresy http://www.sandboxie.com



Obrázok 2 Okno programu Sandboxie v náhľade "Programy"

Obrázok 3 Bežne spustené okno a označenie okna spusteného v Sandboxie

Izolácia programov funguje ako vsuvka medzi programom a operačným systémom, a tak zabraňuje konfliktom s inými programami. Prostredie izolácie si je možné predstaviť ako izolačnú komoru, v ktorej je možné inštalovať a spúšťať „neposlušné“ programy. V tejto izolačnej komore je možné jeden alebo viac problémových programov prinútiť k tomu, aby sa spúšťali bez ovplyvňovania zvyšku systému. Prostredie izolácie programov v podstate funguje ako virtuálny ochranný obal oddeľujúci prepojenie medzi programom a príslušnými zdrojmi operačného systému. Izolačné prostredie poskytuje virtuálny prehľad o zdrojoch systému a namapuje ich s príslušnými fyzickými zdrojmi operačného systému. Izolovaný program je však potrebné spúšťať iba pomocou menu Sandboxie.

Zadanie 11	V programe Sandboxie vytvorte nové izolované prostredie s názvom SandboxKeyLogger. Vo vytvorenom izolovanom prostredí spustite súbor – Family Key Logger, ktorý nájdete na stránke kurzu. Spustite v senboxe napr. program Notepad a niečo napíšte. Zistite, či program Family Key Logger naozaj zaznamenáva stlačené klávesy (pomocou malej ikony v spodnej liste).

1.6 Bezpečný SW – podpísaný softvér

Aby výrobcovia zvýšili bezpečnosť a dôveryhodnosť svojich softvérových produktov, digitálne ich podpisujú. Digitálnym podpisom potvrdzujú, kto je autorom produktu a že softvér nebol nijak škodlivo modifikovaný. Takýto spôsob je bežný napríklad pri ovládačoch zariadení pre OS Windows XP.

Ak je ovládač podpísaný vydavateľom, ktorý potvrdil svoju totožnosť certifikačnej autorite, používateľ má istotu, že ovládač naozaj pochádza od tohto vydavateľa a nebol pozmenený. Ak ovládač nie je podpísaný, alebo ak bol podpísaný vydavateľom, ktorý nepotvrdil svoju totožnosť certifikačnej autorite, alebo ak bol od svojho vydania pozmenený, OS Windows XP na to upozorní.

Pri upozornení môže ísť o niektorý z nasledovných problémov:

- Systém Windows nemôže overiť vydavateľa tohto softvéru ovládača.

Tento ovládač nemá digitálny podpis alebo bol podpísaný digitálnym podpisom, ktorý nebol overený certifikačnou autoritou. Tento ovládač by sa mal inštalovať iba v prípade, že bol na disku pôvodného výrobcu.

- Tento ovládač bol pozmenený.

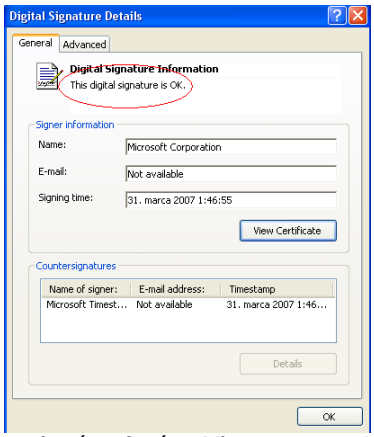
Tento ovládač bol pozmenený po digitálnom podpísaní overeným vydavateľom. Balík mohol upraviť škodlivý softvér, ktorý môže poškodiť počítač alebo odcudziť údaje. Pozmenený ovládač by sa mal inštalovať iba v prípade, že bol na disku pôvodného výrobcu.

Ak sa pri pokuse o nainštalovanie ovládača zobrazí niektoré z týchto hlásení, je vhodné navštíviť webovú lokalitu technickej podpory výrobcu a získať tam digitálne podpísaný ovládač pre svoje zariadenie. V OS Windows XP je možné Inštaláciu ovládačov zariadení, ktoré neobsahujú digitálny podpis zablokovať.

Digitálny podpis ako technológia, ktorá v súčasnosti ako jediná realizuje algoritmus pre zákon o elektronickom podpise, je často braný ako ekvivalent elektronického podpisu.

Jeho tromi hlavnými vlastnosťami sú: autentifikácia, integrita a nepopierateľnosť.

Bližší opis princípu elektronického podpisu realizovaného cez digitálny podpis bol vysvetlený v module *2Inter1: Internet: princípy a tvorba webu 1*

Zadanie 12	Zo stránky spoločnosti Microsoft stiahnite ľubovoľný softvér (napr. Movie Maker) a skontrolujte jeho digitálny podpis.  Pravé tlačidlo na daný softvér->Vlastnosti -> Digitálny podpis

1.7 Bezpečnosť v OS Linux

Pre Linux v oblasti bezpečnosti platia v zásade rovnaké pravidlá ako pre všetky ostatné operačné systémy. Základnými bezpečnostnými prvkami Linuxu sú:

- Zásada práce so základnými a nie administrátorskými právami. Nielenže nás to ochráni pred nechceným zmazaním dát v oblasti, ktorá nám nepatrí, ale v prípade naozajstného problému po chybe používateľa (napr. spustenie škodlivého skriptu z webovej stránky) to ochráni systém pred poškodením.
- Inštalácia softvéru z dôveryhodných zdrojov. Softvér sa dnes v Linuxe prakticky vždy inštaluje z webového úložiska, v ktorom sú jednotlivé balíky podpísané a podpis sa po stiahnutí automaticky overuje.
- Rýchle odstraňovanie chýb a aktualizácia softvéru. V každom softvéri sa vyskytujú chyby. V prípade Linuxu medzi okamihom odhalenia chyby a vytvorením aktualizovaného softvérového balíka častokrát uplynie len niekoľko hodín. Tu je preto dôležité nevypínať štandardne zapnutý aktualizačný systém a aktualizácie robiť vždy, keď sme na to vyzvaní.

Dodržiavanie týchto zásad, ale aj ďalšie opatrenia, robia Linux veľmi odolným (ale nie imúnnym) voči škodlivému softvéru. Vtedy nie je nevyhnutné inštalovať antivírusové programy a, pokiaľ nemáme nainštalované serverové aplikácie, tiež nie je potrebný firewall.

Antivírusové programy pre Linux existujú, ale slúžia na kontrolu súborov prichádzajúcich z iných systémov – napr. pri preposielaní pošty aj s prílohami alebo na kontrolu prenosných médií, ktoré mohli byť infikované v inom systéme. Linuxu windowsovské vírusy síce neuškodia, ale takéto médium môže infikovať ďalšie systémy s OS Windows.

Považujeme za dôležité upozorniť, že počítač s Linuxom obvykle nie je nijako chránený pred útočníkom, ktorý k nemu má fyzický prístup – keď už nič iné, tak ho môže ukradnúť celý alebo aspoň jeho disk. Linux takéto zabezpečenie ani nepredstiera – po reštarte systému možno vojsť do „záchranného“ módu, v ktorom má používateľ administrátorské práva bez zadania hesla. Inou možnosťou, ako sa dá k dátam v počítači bez obmedzení dostať, je spustenie operačného systému z prenosného média (CD, USB kľúč). Takýto nežiaduci prístup možno sťažiť vhodnými nastaveniami v BIOSe počítača. Citlivé dáta je preto vhodné chrániť šifrovaním – buď jednotlivých súborov, alebo celých diskových oddielov.

Záverom treba upozorniť na pravidlo, ktoré hovorí, že systém je taký bezpečný, ako je bezpečná jeho najslabšia časť, ktorou obvykle býva používateľ. Sofistikovane nastavený firewall je zrejme zbytočný, ak máme slabé heslo, ak pre maximalizáciu používateľského pohodlia vykonávame bežnú činnosť so zapnutými administrátorskými právami a navyše bezhlavo spúšťame všetko, čo nám na počítač príde.

Zadanie 13	Nainštalujte si rozšírenie NoScript pre Firefox, alebo obdobný pre váš prehliadač. Zabránite tak spúšťaniu programov v Jave, Javascripte a ďalších, ktoré môžu obsahovať škodlivý kód a v prípade chyby vo Firefoxe môžu spôsobiť problémy. Rozšírenie umožňuje udeľovanie výnimiek pre dôveryhodné stránky.
Riešenie	Rozšírenie získame na stránke https://addons.mozilla.org/sk/firefox/addon/722/

Čo sme sa naučili

Ukázali sme základné bezpečnostné prvky používané v OS (heslá, firewall, problém infiltrácie, anonymita, izolované prostredie, podpísaný SW) a oblasť bezpečnosti z pohľadu OS Linux.

2 Virtualizácia

Virtualizáciou v prostredí počítačov sa označujú postupy a techniky, ktoré umožňujú nahradiť fyzické zariadenie (prostriedok) softvérovým riešením. Virtualizovať je možné od jednotlivých hardvérových komponentov (pamäť, CD mechanika, tlačiareň...) až po celý počítač, tzv. virtuálny stroj. Virtualizovaním teda môžeme využívať možnosti zariadení, ktorými náš počítač nedisponuje, alebo ich nemáme v potrebnom množstve. Virtualizácia nám umožňuje emulovať aj hardvérovú platformu, ktorá sa už nevyrába, a tak používať programy, ktoré boli vytvorené pre napríklad 8bitové počítače ZX Spectrum, Atari, Commodore a pod.

2.1 Virtualizácia zariadení

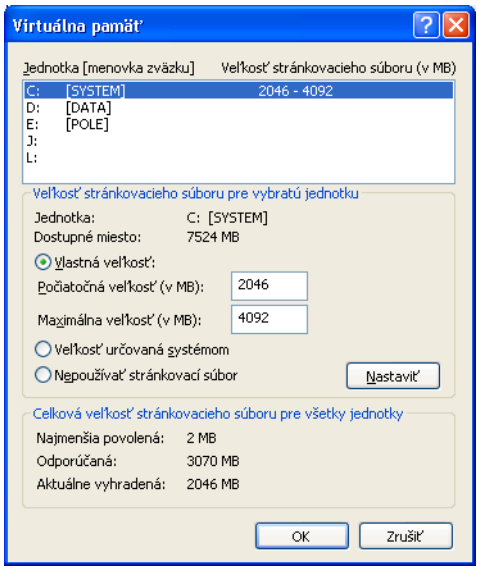
Pri súčasných možnostiach, ktoré nám počítače dokážu poskytnúť, sa nám môže stať, že nebudeme mať dostatok požadovaných zdrojov. Napríklad dostatočná kapacita operačnej pamäte, možnosť pracovať s viacerými CD alebo DVD médiami súčasne a pod.

Virtuálna pamäť

Virtuálna pamäť kombinuje operačnú pamäť (RAM) s dočasným priestorom na inom fyzickom médiu, zvyčajne na pevnom disku. Keď je kapacita pamäte RAM pre činnosť spustených programov nedostatočná, používanie virtuálnej pamäte umožňuje presunúť niektoré údaje z RAM do dočasného priestoru, ktorý označujeme ako **stránkovací súbor**. Presúvaním údajov do stránkovacieho súboru OS dokáže uvoľniť potrebný priestor v pamäti RAM pre umiestnenie práve vykonávaného kódu programu a jeho údajov. V OS Windows stránkovací súbor predstavuje súbor pagefile.sys v koreni systémového disku (zvyčajne disk C:). V OS Linux sa pre stránkovacie súbory používa rezervovaná časť disku – partícia, ktorá je vytvorená pri inštalácii OS.

S princípmi správy pamäte operačným systémom sa oboznámime v kapitole *Štruktúra OS* tohto materiálu.

Zadanie 1	Zistite aktuálnu veľkosť stránkovacieho súboru v OS Windows XP vo vašom počítači.
Riešenie	Prístup k informáciám a nastaveniam stránkovacieho súboru získame cez voľbu *Systém* v *Ovládacom panely* záložka *Spresnenie* -> v sekcii *Výkon* tlačidlo *Nastavenie* -> záložka *Spresnenie* -> v sekcii *Virtuálna pamäť* tlačidlo *Zmeniť*.

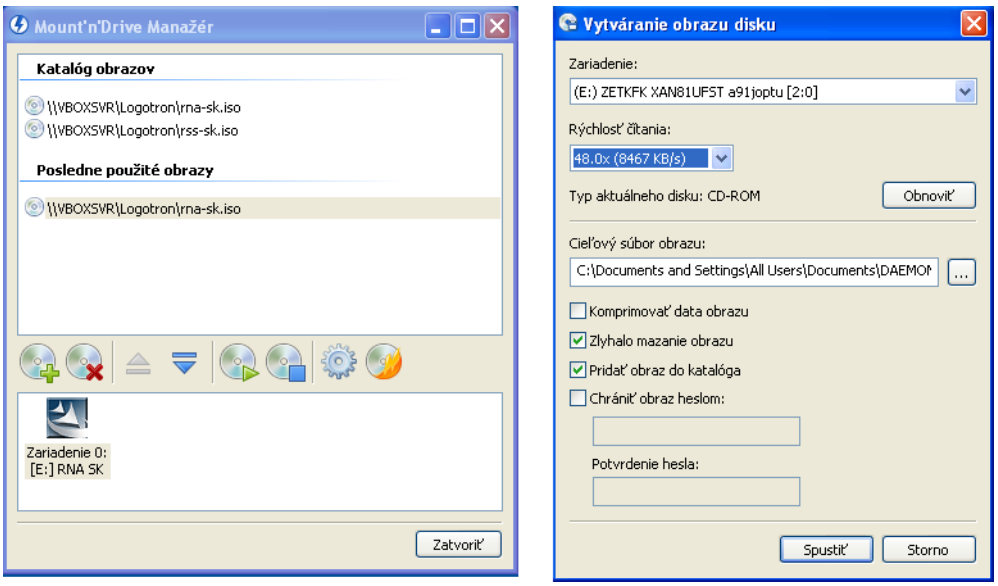


Nastavenie stránkovacieho súboru

Virtuálna CD/DVD mechanika

Medzi najznámejšie programy poskytujúce virtuálne CD/DVD mechaniky pre OS Windows patrí DAEMON Tools http://www.daemon-tools.cc

Princíp virtuálnej CD/DVD mechaniky spočíva v tom, že na pevný disk počítača uložíme obraz originálneho CD/DVD média a potom môžeme tento obraz používať ako pôvodné médium vo forme virtuálnej mechaniky. Takto môžeme ochrániť originálne médium pred náhodným poškodením pri jeho častom používaní, počúvať napríklad hudobné CD a zároveň pracovať s iným CD médiom, pracovať s obsahom CD/DVD médií aj v počítačoch bez fyzickej mechaniky, ako napríklad v mini notebookoch a podobne.



Obrázok 4: Vytvorenie virtuálnej CD mechaniky z obrazu CD média a vytvorenie obrazu CD média

V prostredí OS Linux nie je potrebné inštalovať softvér pre virtuálnu CD/DVD mechaniku. Tento OS natívne podporuje pripojenie obrazu CD/DVD média.

Virtuálna tlačiareň

Virtuálnu tlačiareň pre OS Windows poskytuje program PDFCreator http://www.pdfforge.org/pdfcreator

V OS Ubuntu virtuálnu tlačiareň nainštalujeme príkazom "`sudo apt-get install cups-pdf`"

Ďalším často virtualizovaným zariadením je tlačiareň. Virtuálna tlačiareň je nainštalovaná v OS Windows ako ďalšia tlačiareň, ktorá však pri odoslaní tlače netlačí na žiadnej fyzickej tlačiarni, ale výsledok tlače uloží zvyčajne ako súbor vo formáte PDF. Keďže formát PDF je v súčasnosti bežným štandardom, tak s takýmto súborom je možné ďalej pracovať aj na inom počítači a s iným OS.

2.2 Virtualizácia operačného systému

Pokiaľ sa stretneme so slovom virtualizácia, ktoré nie je doplnené žiadnym prívlastkom, rozumie sa virtualizácia celého počítača. Je to usporiadanie, v ktorom *hosťujúci operačný systém* využíva hardvérové prostriedky *hostiteľského počítača* nepriamo, sprostredkovane prostredníctvom programu, tzv. *správcu virtuálnych počítačov,* ktorý sa nazýva aj *hypervízor.* Hypervízor môže na jednom počítači spravovať aj viacero virtuálnych počítačov, na ktorých môžu byť spustené rôzne hosťujúce operačné systémy. Hosťujúci systém môže mať prístup k reálnym komponentom hostiteľa, rovnako ako aj k virtuálnym komponentom, ktoré sú implementované výlučne softvérovo. Virtuálne komponenty pritom môžu emulovať konkrétne hardvérové zariadenie (napr. konkrétny sieťový adaptér konkrétneho výrobcu) alebo to môžu byť špeciálne zariadenia, ktoré sa v hardvérovej podobe nevyrábajú. Tu môže ako príklad slúžiť disk virtuálneho počítača, ktorý je v skutočnosti len súborom na reálnom disku.

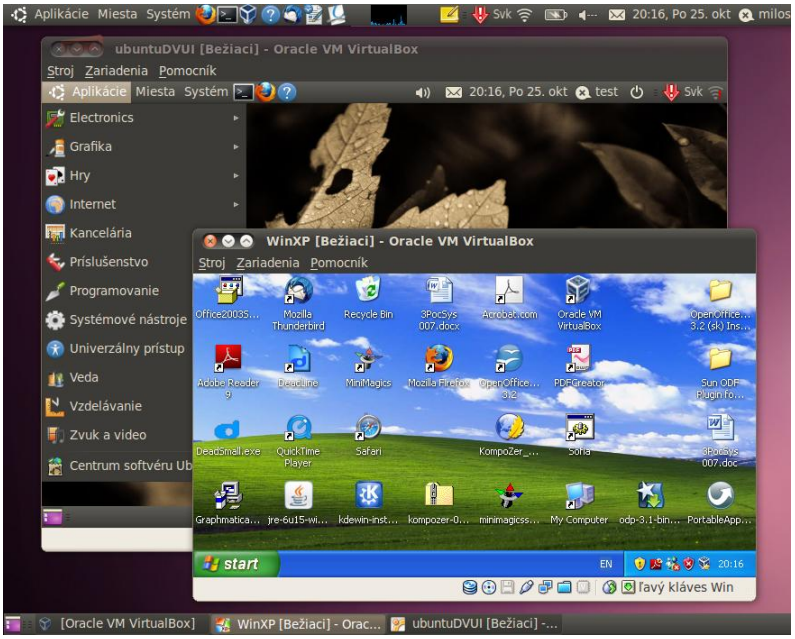
Technológia virtuálnych počítačov nie je nová – využívala sa už v 80-rokoch v sálových počítačoch IBM. Dnes je virtualizácia veľmi populárna v oblasti profesionálnych aplikácií rovnako ako aj v „domácom“ použití.

Použitie virtuálneho počítača na prevádzku dvoch systémov je jednoduchšie a praktickejšie ako dual-boot (inštaláciu dvoch operačných systémov na počítači s možnosťou výberu OS pri bootovaní počítača).

Profesionálne sa virtualizácia nasadzuje z viacerých dôvodov:

- ekonomickejšie využitie hardvéru: dnešné počítače sú také rýchle, že v mnohých aplikáciách procesor vlastne len čaká. V prípade viacerých paralelne bežiacich počítačov na jednom hardvéri sa tento využije lepšie, čo vedie k zníženiu prevádzkových nákladov.
- bezpečnosť: pokiaľ v operačnom systéme beží naraz viacero služieb (web server, poštový server, správa používateľov), tak problém s jednou z nich (napadnutie útočníkom) ovplyvňuje aj ostatné. Preto sa vytvárajú virtuálne počítače s jednou bežiacou službou.
- administrácia: virtuálny počítač (presnejšie, jeho virtuálny disk) možno ľahko prenášať z jedného reálneho počítača na iný alebo ho ľahko možno zálohovať.

Mnohé predinštalované virtuálne počítače s jednou bežiacou službou sú dostupné na internete ako „virtuálne zariadenia“



Obrázok 5: Dva virtuálne počítače (OS Windows XP a OS Ubuntu) bežiace na hostiteľskom počítači s OS Ubuntu.

Mimo firemného sveta majú virtuálne počítače uplatnenie hlavne v tom, že umožňujú súčasný prístup k aplikáciám dvoch rozdielnych operačných systémov (Obr. 5). Napríklad, používateľ Linuxu získa takto jednoduchý prístup k programu MS Word, pokiaľ potrebuje otvoriť súbor v niektorom z jeho formátov. Virtuálny počítač sa dá výhodne použiť aj vtedy, ak si chceme vyskúšať nový operačný systém alebo aspoň jeho novú verziu. Rovnako výhodný je na experimentovanie – možno si vyskúšať inštalovanie systému, operácie s diskovými oddielmi, zapájanie počítačov do siete, terminálovú sieť a mnoho ďalších. Všetko pritom bez obáv zo straty dát zo skutočného počítača, alebo z narušenia systému.

2.3 Systémy na virtualizáciu počítačov

Počas relatívne dlhej histórie virtualizácie boli vyvinuté rôzne prístupy. V tomto texte sa budeme venovať len jednej kategórii virtuálnych počítačov, a to tým, ktorých hypervízor beží ako aplikácia v hostiteľskom systéme. Tu rozlišujeme *emulačné* systémy, ktoré dokážu na hostiteľskom počítači spúšťať aj operačný systém určený pre inú architektúru a *natívne* systémy, ktoré spolupracujú s hosťujúcim systémom určeným pre ten istý typ procesora, ako má hostiteľ.

Podrobnejší úvod do problematiky virtualizácie možno nájsť napr. na http://cs.wikipedia.org/wiki/Virtualizace

Emulačné systémy

V emulačných systémoch sú inštrukcie hosťujúceho počítača prekladané na inštrukcie hostiteľa. Je zrejmé, že takýto virtuálny počítač je pomalší ako reálny počítač s rovnakými parametrami. Na druhej strane však umožňuje spúšťať operačný systém určený pre iný procesor. Príkladom takéhoto systému je program **qemu**, ktorý podporuje procesory ARM, CRIS, i386, M68k, MIPS, PowerPC, SH4, SPARca x86-64. Program si na Ubuntu môžeme nainštalovať jednoducho príkazom

Virtuálny počítač obvykle zachytí myš a klávesnicu. Pritom, pokiaľ hosťujúci systém nemá kurzor, tak ten môže aj celkom zmiznúť a myš prestane reagovať. Uvoľníme ju stlačení magickej kombinácie na klávesnici: pre Qemu/KVM je to CTRL-ALT-SHIFT, pre DosBox to je CTRL-F10 a pre VirtualBox pravý kláves CTRL.

sudo apt-get install qemu-kvm

qemu sa spúšťa z príkazového riadka. Napríklad, systém z ISO obrazu CD/DVD môžeme spustiť príkazom

qemu -m 512 -boot d -cdrom ubuntu-10.04-DVUI.iso

kde prepínač -m 512 určuje veľkosť pamäte virtuálneho počítača, -boot d hovorí o tom, že systém treba zaviesť z CD mechaniky a -cdrom definuje, že treba použiť virtuálnu CD mechaniku – súbor ubuntu-10.04-DVUI.iso s obrazom CD disku. Po zadaní tohto príkazu sa otvorí okno, ktoré hrá rolu štandardného monitoru počítača. Po kliknutí na toto okno si hosťujúci systém „privlastní“ klávesnicu a myš.

Zatiaľ čo qemu je určený skôr na profesionálne použitie, počítačového nadšenca možno zaujmú emulátory starých počítačov, s ktorými sa inak stretneme už len v múzeách. Xspect je emulátor 8-bitového počítača Sinclair ZX-Spectrum, ktorý si v druhej polovici 80-rokov do Československa priviezli desaťtisíce nadšencov. Nainštalujeme ho príkazom

sudo apt-get install spectemu-x11

Programy nájdeme na viacerých stránkach. Emulátor spustíme príkazom

xspect -tzx Hungry\ Horace.tzx

Po ZX-Spectovskom príkaze *load “”* (pre tých, ktorí už zabudli: stlačiť *j a dvakrát úvodzovku*) a spustení magnetofónu s páskou (stlačiť F6) sa program načíta a spustí (Obr. 6). Nezabudnite si zapnúť zvuk!

Zadanie 2

V Ubuntu si nainštalujte emulátor počítača ZX Spectrum (Atari...) alebo pohľadajte jeho verziu pre Windows a vyskúšajte si svoje obľúbené hry. Samotné Ubuntu pritom tiež môže byť spustené ako virtuálny počítač.

Obrázok 6: Hra pre ZX spectrum, spustená v emulátore xspect

Emulátory existujú aj pre ďalšie systémy. DosBox emuluje PC a je vybavený aj opensource implementáciou operačného systému MS DOS. V Ubuntu ho nainštalujeme príkazom

sudo apt-get install dosbox

Pracuje sa s ním ako s DOSom, z príkazového riadka. DOSBOX je dnes vhodný na spúšťanie klasických dosovských hier (Obr. 7).

Obrázok 7: Dosovská hra Quake, spustená v DosBoxe.

Zadanie 3	Nainštalujete si DosBox a vyskúšajte si hry alebo aj iné programy, ktoré nájdete na internete.

Natívne systémy

Použitie emulačného virtuálneho počítača je opodstatnené najmä vtedy, ak nám ide o spúšťanie operačného systému alebo programov, ktoré sú určené pre iný procesor, alebo ide o staré programy, kde spomalenie emuláciou nehrá rolu. Pri bežnej práci sa treba obrátiť na natívne systémy, ktoré umožňujú vykonávanie inštrukcií hosťujúceho systému priamo bez prekladu, a tak sú podstatne rýchlejšie. Existujú viaceré, medzi známe patria Vmware, XEN, KVM, MS VirtualPC, VirtualBox a ďalšie.

Z nich je KVM vlastne len doplnkom k už spomínanému qemu – pridáva modul, ktorý umožní spustenie priamo bez emulácie. Spustíme ho teda rovnako:

kvm -m 512 -boot d -cdrom ubuntu-10.04-DVUI.iso

beží však citeľne rýchlejšie.

2.4 VirtualBox

V ďalšom texte si podrobne predstavíme virtualizačný systém VirtualBox (VB), ktorý pracuje v operačných systémoch Windows, Linux, MacOs a OpenSolaris. Navyše VB má aj grafické používateľské prostredie, ktoré jeho používanie môže zjednodušiť. Budeme predpokladať prácu v prostredí OS Windows. V ostatných systémoch sa VB používa identicky a iná je len inštalácia.

Dostupnosť a inštalácia

VB je otvorený softvér, ktorého vývoj podporuje spoločnosť Oracle. Program si môžeme stiahnuť zo stránky http://www.virtualbox.org/wiki/Downloads, pričom binárna verzia je spoločná pre 32 a 64 bitové verzie Windows. Na stránke je dostupná dokumentácia, a ako sa na otvorený softvér patrí, aj zdrojový kód.

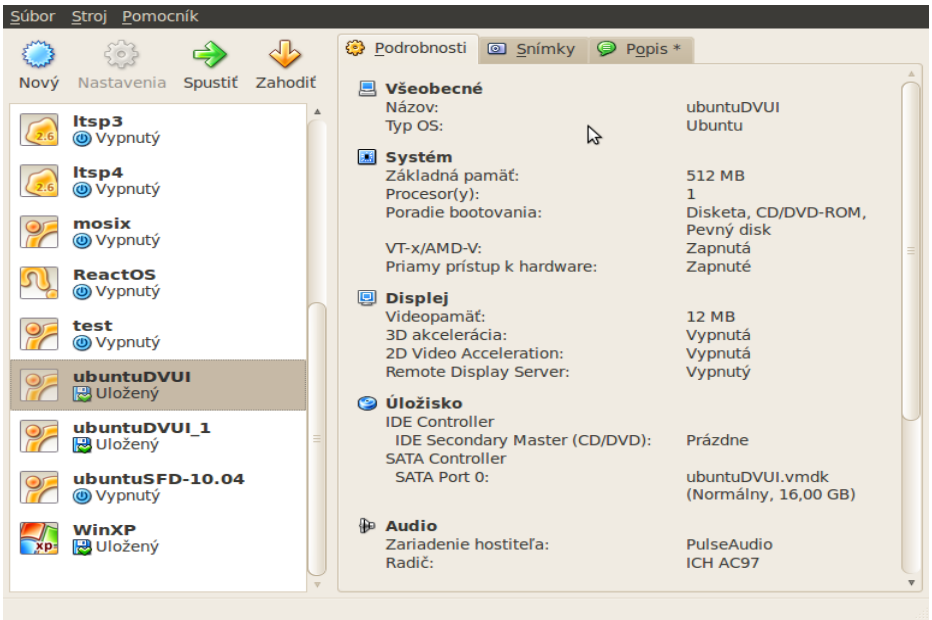
Zadanie 4	Nainštalujte si VirtualBox.
Riešenie	Inštalácia VB sa robí obvyklým spôsobom: stiahneme súbor, spustíme ho a odpovedáme na otázky, ktorých je dosť. Našťastie, postačujú predvolené odpovede, takže klikáme len na Next, OK a podobne. Následne VB spustíme (pokiaľ sa nespustil sám) a nastavíme slovenčinu v menu File-> Preferences. Podrobný opis inštalácie je uvedený na stránke http://sospreskoly.org/diskusia/predinstalovane-ubuntu-1004-pre-virtualny-pocitac

Logo virtualizačného nástroja VirtualBox

Používateľské prostredie VirtualBoxu

Používateľské prostredie (Obr. 8) VB slúži na vytváranie (konfigurácia hardvéru) a správu (zapínanie, import, export) virtuálnych počítačov a na spravovanie virtuálnych médií (napr. CD diskov). Na ľavej strane jeho okna je zoznam existujúcich počítačov (spočiatku prázdny), pričom vpravo je uvedená konfigurácia jedného z nich. Počítač môže byť v troch stavoch – *vypnutý*, *bežiaci* a *uložený*. Stav „uložený“ je podobný ako „hibernate“ v reálnom počítači. Pri prechode do tohto stavu si VB zapamätá všetko potrebné a počítač sa vypne. Po opätovnom spustení pokračuje vykonávanie programov bez zmeny ďalej – namiesto vypínania teda môžeme virtuálny počítač len takto uspávať, čím si šetríme čas pri jeho štarte.

Okno spusteného virtuálneho počítača má svoje vlastné menu, v ktorom sú voľby špecifické pre konkrétny počítač. Toto menu je odlišné od menu hlavného okna VB.



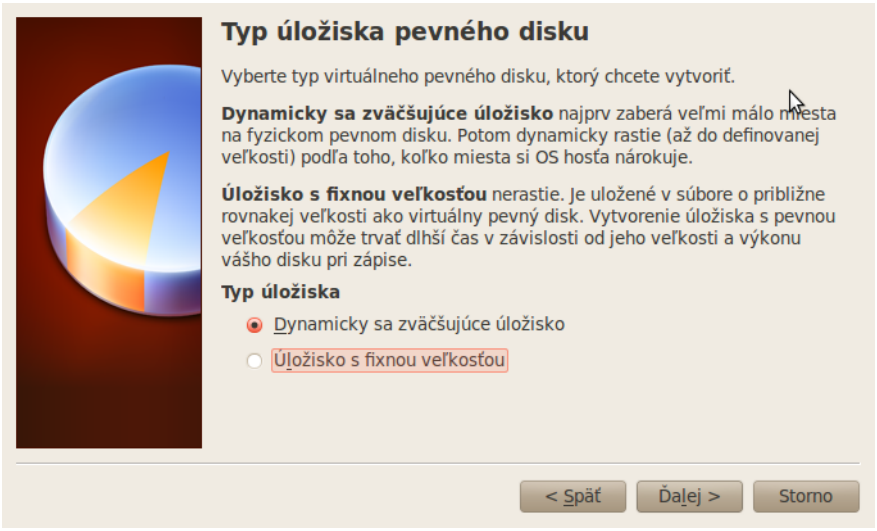
Obrázok 8: Okno programu VB.

Vytvárame virtuálny počítač

Pri vytváraní nového počítača je potrebné špecifikovať jeho konfiguráciu. Avšak tak, ako nám aj v obchode s počítačmi prichystajú predkonfigurované modely, tak aj tu sa môžeme spoľahnúť na štandardné nastavenia. VB si pritom pomôže otázkou, ktorý

systém ideme inštalovať a podľa toho nastaví parametre. Jediné, o čom treba rozhodnúť, je veľkosť disku.

Zadanie 5	Vo VirtualBox-e si vytvorte nový počítač.
Riešenie	Nový počítač vytvoríme kliknutím na „Nový“. Po niekoľkých jednoduchých otázkach sa dostaneme k vytváraniu disku. Tu dostaneme na výber disk s pevnou veľkosťou alebo dynamicky rastúci disk (obr. 9). Výhodnejšia je druhá možnosť, lebo disk zaberá len toľko miesta, koľko naozaj treba – nie však viac, ako bolo zadané. Tak ako v prípade reálneho disku, jeho veľkosť sa nedá neskôr meniť, a tak v prípade potreby je potrebné prekopírovať jeho obsah na väčší disk.



Obrázok 9: Voľba typu disku.

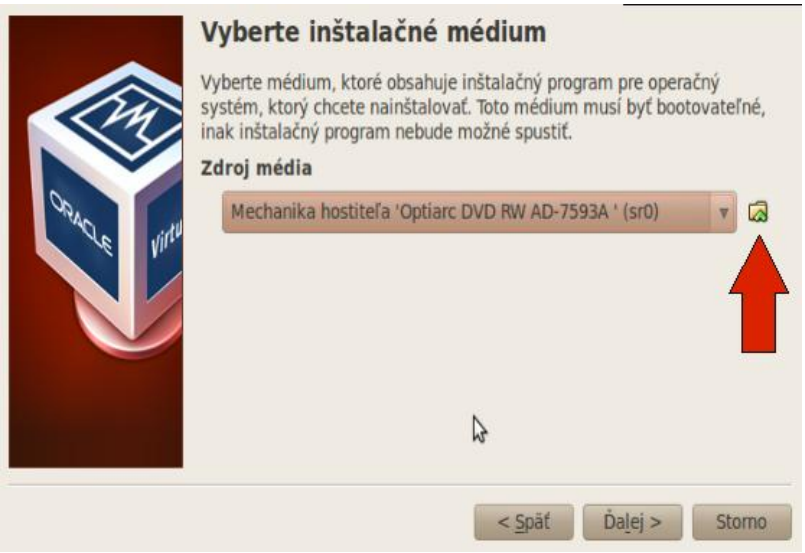
Po ukončení konfigurácie sa nový počítač objaví v ľavom menu. Pokiaľ je vypnutý, môžeme jeho konfiguráciu meniť – pridať pamäť, vymeniť sieťový adaptér, zmeniť počet procesorov a podobne.

Zadanie 6	Zoznámte sa s možnosťami nastavení virtuálneho počítača.

Počítač môžeme nakonfigurovať aj bez disku. Takýto počítač je vhodný na spúšťanie z Live CD/DVD, alebo na zavádzanie systému cez sieť zo servera – z počítača sa tak stáva terminál – tenký klient. Technológia tenkých klientov je populárna práve na školách, lebo znižuje nároky na hardvér a administráciu (namiesto o 15 počítačov v učebni sa staráme len o jeden – server počítačovej siete).

Prvé spustenie a inštalácia

Po vytvorení máme počítač bez softvéru – tak ako z obchodu (pokiaľ sme si nezaplatili inštaláciu). V prípade reálneho počítača by sme vložili do CD mechaniky štartovacie médium a nainštalovali by sme systém. VB nám so zakladaním média pomôže. Pri prvom štarte nového počítača sa otvorí Sprievodca prvým spustením, ktorý nám umožní výber inštalačného média. Môže ním byť reálne CD/DVD, alebo súbor s jeho obrazom. V druhom prípade klikneme na ikonku Manažéra virtuálnych médií (obr. 10), ktorý zatiaľ žiadne médiá nespravuje. Preto klikneme na „Pridať“, vyberieme si ISO súbor s obrazom zavádzateľného média a pridáme ho do správcu. Následne si ISO súbor vyberieme. Po čase tu budeme možno mať takýchto súborov viac.



Obrázok 10: Voľba inštalačného média. Šípka ukazuje na ikonku, ktorá vedie k Manažéru virtuálnych médií.

Po výbere média klikneme na „Dokončiť“ a zavádzanie systému z média sa spustí. Nasledujúce akcie závisia na tom, aké médium sme založili – či ide o Live CD/DVD na jednorazové spustenie systému, alebo či ide o inštalačné médium. Pokiaľ ide o inštaláciu, nemusíme mať obavy z porušenia hosťujúceho počítača – tak ako sa nemusíme báť o poškodenie počítača, ktorý stojí na inom stole ako ten, na ktorom inštalujeme systém.

Zadanie 7	Vytvorte virtuálny počítač a spustite si v ňom systém z Live CD/DVD.

Kde získať zavádzateľné médiá

Pokiaľ chceme vo virtuálnom počítači inštalovať OS Windows, je potrebné sa zoznámiť s jeho licenčnými podmienkami. OEM verzie OS Windows sú viazané na hardvér, s ktorým boli kupované, ale v prípade tzv. krabicovej verzie môžeme OS Windows, napríklad po vyradení starého počítača, nainštalovať na nový, a teda aj na virtuálny počítač. Licenčné podmienky operačného systému MacOS nepovoľujú jeho inštaláciu na hardvér od iného výrobcu ako je spoločnosť Apple – teda ani na virtuálny počítač.

Linux a ďalšie otvorené operačné systémy sa obvykle sťahujú zo siete. Inštalačné alebo Live médium je dostupné ako tzv. ISO súbor. Je to obraz CD alebo DVD disku, ktorý možno na médium napáliť, alebo z neho môžeme virtuálny počítač naštartovať priamo.

Virtuálny počítač je vynikajúcou možnosťou, ako sa zoznámiť s novým operačným systémom. Väčšina známejších distribúcií Linuxu dnes ponúka Live CD/DVD, z ktorého možno systém priamo zaviesť na vyskúšanie a prípadne aj nainštalovať. Niekoľko odkazov na distribúcie vhodné pre menej skúsených používateľov alebo začiatočníkov:

- OpenSuse: http://software.opensuse.org/113/sk
- Fedora: http://fedoraproject.org/get-fedora
- Ubuntu: http://www.ubuntulinux.org/desktop/get-ubuntu/download
- Knoppix: http://www.knoppix.net

Knoppix je distribúcia, ktorá spopularizovala použitie Live médií. Nie je určená na inštaláciu a obsahuje veľké množstvo programov.

Pre Virtuálny počítač je vhodná 32-bitová verzia. Na stránkach Fedory, OpenSuse a

Ubuntu sú uvedené viaceré verzie, ktoré sa líšia prostredím pracovnej plochy – ide tu o voľbu najmä medzi:

- *KDE* - charakterizuje ho veľký rozsah používateľských volieb,
- *Gnome* –je zamerané na jednoduchosť,
- *XFCE* –má nízke nároky na hardvér.

Okrem univerzálnych distribúcií a Live CD existujú aj špecializované. Napríklad, nasledujúce boli vytvorené pre školstvo a edukačné účely:

- Edubuntu – verzia Ubuntu s edukačným softvérom a na administráciu školy.
- openSUSE Li-f-e: Linux for Education – softvér pre žiakov, učiteľov a aj rodičov.
- Debian Education / Skolelinux – kompletné riešenie pre školy. Pochádza z Nórska, kde sa aj široko používa.
- Abuledu – francúzska edukačná distribúcia.
- Edulinux – projekt podporovaný vládou Čile.
- Guadalinex-edu – španielska školská distribúcia – má viac ako 500,000 inštalácií.
- Qimo – Edukačný softvér pre deti predškolského veku.

Vyberať si je teda z čoho.

Obrázok 11: Live CD Qimo určené pre najmenšie deti.

Import predinštalovaného počítača

Jednoduchšou cestou, ako je naozajstná inštalácia virtuálneho počítača, je jeho import z tzv. virtuálneho zariadenia (virtual appliance), ktoré bolo vytvorené exportovaním nainštalovaného a nakonfigurovaného systému. Takto sa často distribuujú jednoúčelové „zariadenia“ určené na nejakú špeciálnu činnosť. Obvykle ide o zip archív s niekoľkými súbormi, ktorý treba rozbaliť. Takto sme postupovali aj pri príprave Ubuntu 10.04, ktoré bolo modifikované pre účely vzdelávania ĎVUI.

Súbory virtuálneho zariadenia môžu byť vo viacerých formátoch. Najrozšírenejší z nich, OVF (Open Virtualization Format), je podporovaný viacerými správcami virtuálnych počítačov. Virtuálne zariadenia možno stiahnuť z rôznych stránok, napríklad z http://virtualboximages.com/.

Zadanie 8	Importujte virtuálne zariadenie s Ubuntu 10.04, ktoré bolo pripravené pre kurzy ĎVUI.
Riešenie	1. Stiahneme predinštalovaný systém z adresy 2. Ide o archív, ktorý rozbalíme. Súbory sa nachádzajú v priečinku, ktorý sa rozbalením vytvorí 3. Import zariadenia je dostupný v menu VB *Súbor -> Import appliance*.

Práca s programom VirtualBox

Zachytenie kurzora a kláves Host

Jednou z vlastností virtuálnych počítačov a emulátorov je, že ich okno zachytáva kurzor, ktorý možno uvoľniť stlačením istej kombinácie kláves. V prípade VB je to štandardne pravý kláves CTRL. Toto nastavenie možno zmeniť v *Súbor->Nastavenia-> Vstup*. V menu VB sa tento kláves uvádza ako „Host“. Napríklad, v prípade Host+F (prechod do režimu celej obrazovky) súčasne stlačíme pravý kláves CTRL a kláves F.

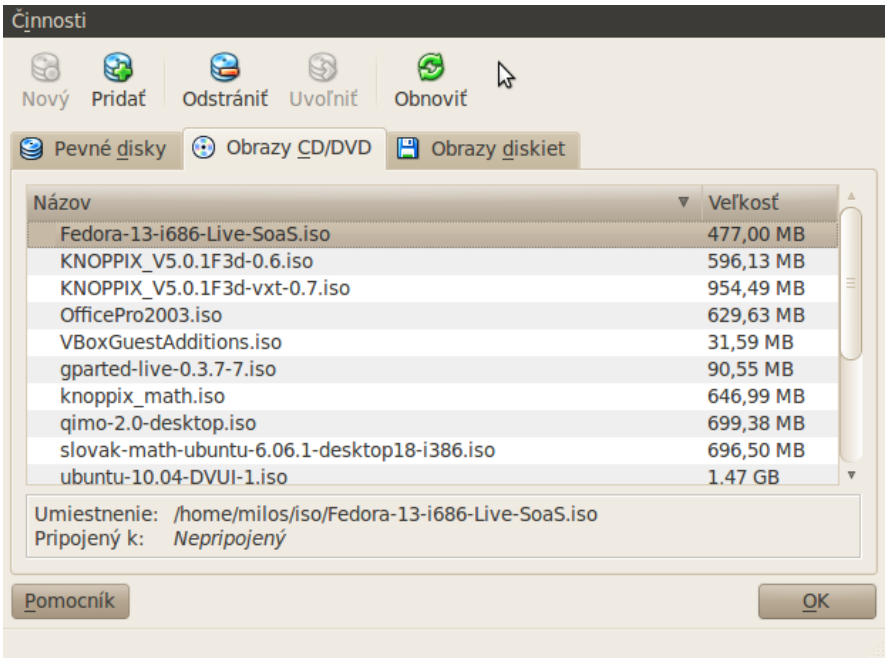
Či sa kurzor v okne VB naozaj zachytáva, to závisí aj na hostiteľskom operačnom systéme a na tom, či sú v hosťujúcom systéme nainštalované tzv. Hostiteľské doplnky.

Pripájanie médií

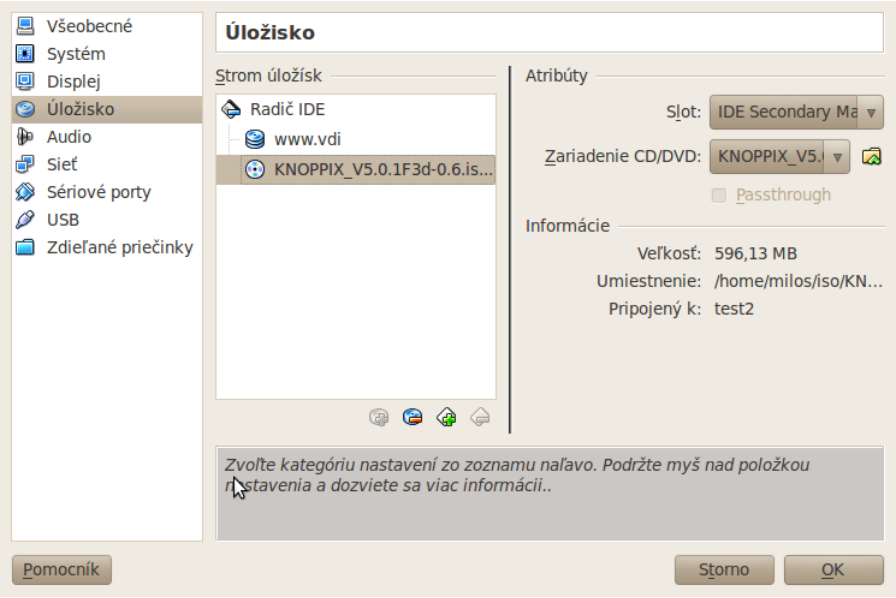
ISO súbory CD a DVD médií a diskiet, alebo virtuálne disky možno pripájať k virtuálnemu počítaču až po tom, ako ich sprístupníme pre manažér virtuálnych médií. Ten je dostupný v menu VB *Súbor -> Manažér virtuálnych médií*. V ňom si vyberieme typ a nové médium pridáme kliknutím na tlačidlo „Pridať“ (obr. 12).

V bežiacom virtuálnom počítači možno takéto médium pripojiť (vložiť do virtuálnej mechaniky) cez menu *Zariadenia* jeho okna. Operačný systém na takéto „vloženie“ zareaguje obvyklým spôsobom, tak akoby bolo vložené reálne médium do reálnej mechaniky. V tomto menu možno vybrať aj reálnu mechaniku.

ISO súbor môžeme pripojiť aj priamo do virtuálnej mechaniky, a to cez voľbu VB *Nastavenia*. Otvorí sa okno, kde vyberieme voľbu *Úložisko* (obr. 13). Tu vidíme ikonku CD disku, ktorý je pripojený na IDE radič počítača – teda rovnako, ako v reálnom počítači. Súbor pripájame opäť cez *Manažéra virtuálnych médií*.



Obrázok 12: Okno manažéra virtuálnych médií



Obrázok 13: Okno Nastavenia. Vo virtuálnej mechanike je založené médium (ISO súbor) KNOPPIX...

Poznámka k verzii:
Zdá sa, že vo verzii VirtualBox 3.2.10, ktorá bola aktuálna v čase písania tohto textu, je chyba, ktorá spôsobuje problémy pri práci s USB diskami v hostiteľskom OS Windows. Táto chyba sa dá obísť tak, že po prvom pripojení USB k virtuálnemu počítaču a inštalácii ovládačov v hostiteľskom systéme reštartujeme reálny a aj virtuálny počítač. Neskôr, pokiaľ chceme USB disk použiť vo virtuálnom počítači, tak naň po zasunutí do počítača nič v hostiteľskom systéme nezapisujeme.

Práca s USB zariadeniami

USB zariadenia taktiež pripájame cez menu *Zariadenia* okna virtuálneho počítača. Tu vidno všetky USB zariadenia (aj klávesnicu, čítačku odtlačkov a podobne). Ak chceme pripojiť USB disk, treba si správne vybrať. Po výbere USB disku sa tento odpojí z hostiteľského počítača a pripojí sa k virtuálnemu.

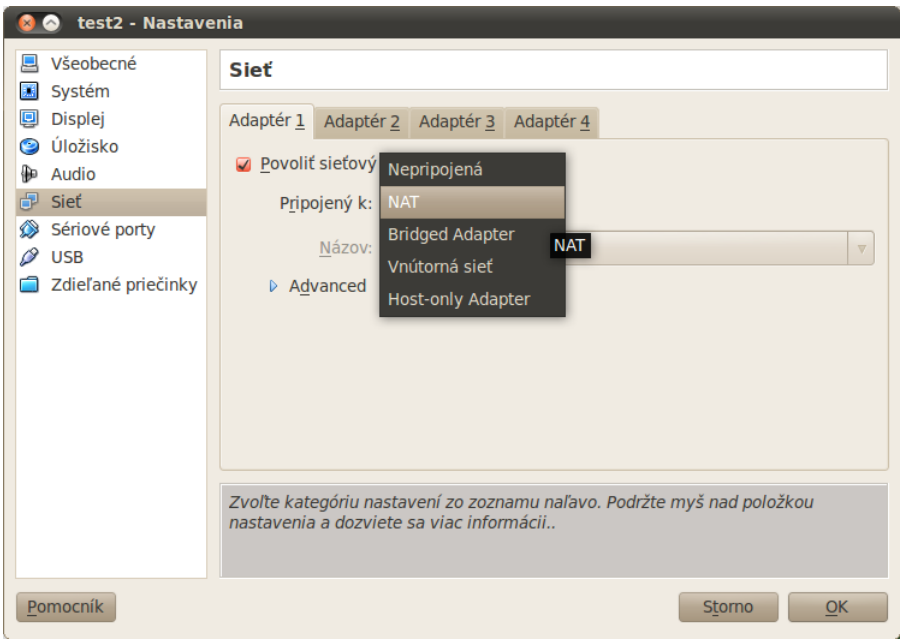
Konfigurácia siete

Virtuálny počítač môže mať priradené až štyri sieťové adaptéry, a tak si možno vytvárať virtuálne počítačové siete rôznych konfigurácií. Každý adaptér pritom môže byť v jednej zo štyroch konfigurácií (obr. 14).

NAT (Network Address Translation) je štandardná voľba, v ktorej je virtuálny počítač k sieti pripojený cez hostiteľa – konfigurácia zodpovedá takej, keď je reálny počítač priamo káblom spojený s iným počítačom. Virtuálny počítač má plný prístup k sieti, avšak z iných počítačov nie je dostupný, lebo má neverejnú IP adresu. Ak máme spustených viacero virtuálnych počítačov, tak sa navzájom nevidia.

Bridged Adapter je voľba, ktorá zodpovedá nezávislému pripojeniu počítača do lokálnej siete. Je teda akoby celkom nezávislý na svojom hostiteľovi a vyžaduje si konfiguráciu siete podľa údajov administrátora. Takto konfigurovaný počítač je viditeľný v lokálnej sieti, tak ako všetky ostatné reálne počítače.

Vnútorná sieť definuje lokálnu sieť vytvorenú z virtuálnych počítačov – zodpovedá vzájomnému prepojeniu viacerých reálnych počítačov káblami. Takejto sieti je potrebné zadať meno, aby sme ju odlíšili od inej podobnej siete. V prípade reálnych počítačov meno siete nepotrebujeme, lebo vidíme odkiaľ kam idú káble. Pokiaľ z takejto siete chceme mať prístup do internetu, tak aspoň jeden z počítačov musí ma nakonfigurované dva sieťové adaptéry.



Obrázok 14: Výber typu sieťového pripojenia

Vypnutie virtuálneho počítača

Virtuálny počítač sa vypína obdobne, ako reálny počítač (teda nie vytiahnutím šnúry zo zástrčky). Ak klikneme na tlačidlo zatvorenia okna virtuálneho počítača, objaví sa okno s tromi ponukami. V prvom prípade sa uchová stav – počítač prejde do stavu „uložený“. Druhý zodpovedá štandardnému vypínaciemu postupu a tretí je spomínaným vytiahnutím šnúry so zástrčky.

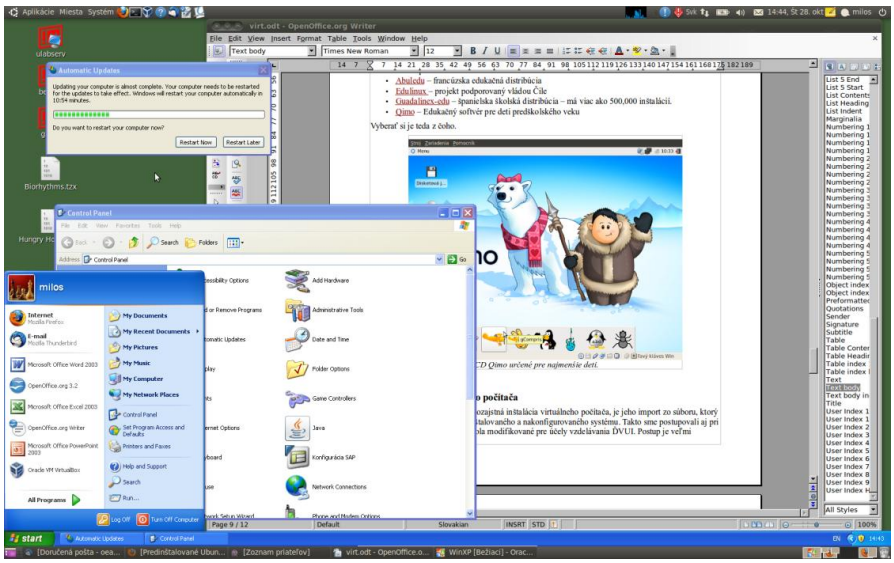
Spolupráca s hosťujúcim systémom

Virtuálny počítač, aj keď beží v prostredí svojho hostiteľa, je na ňom nezávislý – je to akoby iný počítač na stole. Hosťovské doplnky sú programy, ktoré po inštalácii vo virtuálnom počítači sprístupnia niektoré ďalšie možnosti na spoluprácu s hostiteľom. Je to najmä priamy prístup k súborom hostiteľa, možnosť meniť veľkosť okna virtuálneho počítača, režim celej obrazovky a režim integrácie okien virtuálneho počítača priamo na plochu hostiteľa (seamless mode, obr. 15).

Hosťovské doplnky sa dodávajú ako ISO obraz disku, ktorý môžeme pripojiť cez menu *Zariadenia->Nainštalovať hosťovské doplnky*. V prípade Virtuálneho počítača s Windows sa automaticky spustí príslušný program, v prípade Linuxu ho treba spustiť ručne s administrátorskými právami:

1. zvolíme *Zariadenia->Nainštalovať hosťovské doplnky.*
2. v menu *Miesta* klikneme na VBOXADDITIONS…
3. pravým tlačidlom otvoríme kontextové menu súboru VBoxLinuxAdditions-x86.run, v ktorom zvolíme *Otvoriť pomocou -> Otvoriť inou aplikáciou* a klikneme na *Použiť vlastný príkaz*.
4. do riadka, ktorý sa objaví, napíšeme „gksu“ a klikneme na *Otvoriť*. Otvorí sa okno, do ktorého sa vypisujú informácie o postupe. Inštalácia doplnkov je ukončená výpisom *Press Return…*
5. po ukončení inštalácie virtuálny počítač reštartujeme. Úspech je dokumentovaný možnosťou ľubovoľne meniť veľkosť okna virtuálneho počítača.

Po inštalácii novej verzie VB treba tento postup opakovať. Niekedy ho treba opakovať aj po aktualizácii operačného systému virtuálneho počítača.



Obrázok 15: Integrácia okien virtuálneho počítača s OS Windows XP do plochy hostiteľa s OS Ubuntu.

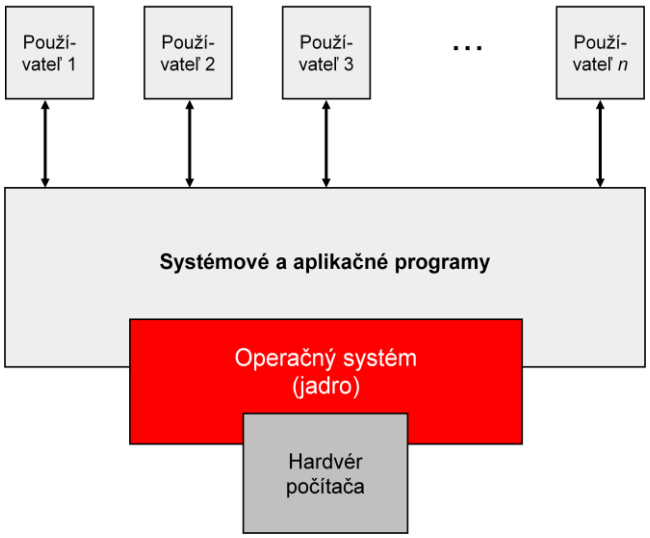
Čo sme sa naučili

V tejto časti textu sme sa zoznámili s virtualizáciou zariadení a celého počítača. Uviedli sme si dve varianty a to emuláciu počítača a plnú virtualizáciu. Uviedli sme príklady a podrobnejšie sme sa zoznámili s hypervízorom VirtualBox a možnosťami, ktoré poskytuje pre bežného používateľa.

3 Štruktúra OS

Pod názvom OS Linux alebo OS Windows si bežne používateľ najskôr predstaví jeho vzhľad, spôsob používania a aplikácie, ktoré v ňom má k dispozícii. Otázky, ktoré skutočne súvisia s vlastným operačným systémom, teda s tým, ako „to“ vo vnútri vlastne pracuje, sa však objavujú oveľa neskôr a väčšina používateľov si snáď žiadnu z tých otázok ani nikdy nepoloží.

V šesťdesiatych rokoch minulého storočia sa zaužívala definícia operačného systému ako softvéru, ktorý riadi hardvér. Avšak v súčasnosti je jeho úlohou oveľa viac a operačný systém sa stáva **správcom** celého počítača, nielen jeho hardvérovej časti, ale aj všetkých ostatných komponentov, ako sú iné procesy, používatelia v systéme, periférne zariadenia, sieťové pripojenie, …. Operačný systém rozhoduje, ktorý proces práve pobeží na procesore a aké prostriedky má k dispozícii. Operačných systémov existuje veľké množstvo, okrem spomínaných OS Linux a OS Windows, sú to napr. operačné systémy UNIX, Mach, MS-DOS, OS/2, MacOS, VMS, MVS, VM, a ďalšie.



Obr. 16 Model počítačového systému

Vo všeobecnosti môžeme počítačový systém rozdeliť na hardvér, operačný systém, systémové a aplikačné programy, ktoré sú využívané používateľmi, obr. 16. Operačný systém zahŕňa softvér na niekoľkých úrovniach. Budeme rozlišovať služby jadra operačného systému (tiež označované ako kernel) a systémové služby operačného systému na úrovni aplikácií. Základom operačného systému je jadro, kontrolný program, ktorý funguje v privilegovanom stave (režim, ktorý umožňuje vykonávať všetky hardvérové inštrukcie bez obmedzení), reaguje na prerušenia od externých zariadení a požiadavky od procesov. Všeobecne platí, že jadro je trvalo zavedené v pamäti počítača. Vytvára a ukončuje procesy a reaguje na ich žiadosť na jednotlivé služby.

Operačný systém je správcom prostriedkov. Hlavnými hardvérovými prostriedkami sú procesor/procesory, diskový priestor, vstupno-výstupné zariadenia, komunikačné zariadenia. Niektoré z hlavných činností operačného systému sú: implementácia používateľského rozhrania; zdieľanie hardvéru medzi používateľmi; zdieľanie dát používateľov medzi sebou; zabraňovanie používateľom v zasahovaní si navzájom do svojho pracovného priestoru; plánovanie prostriedkov medzi používateľmi; uľahčenie vstupu/výstupu; zotavovanie sa z chýb; účtovanie využitia prostriedkov; uľahčenie paralelných operácií; organizovanie dát pre bezpečný prístup a manipuláciu sieťovej komunikácie.

Správu vykonávanú operačným systémom môžeme vo všeobecnosti rozdeliť na niekoľko častí:

- Správa procesov

- Správa zariadení
- Správa pamäte
- Správa súborov

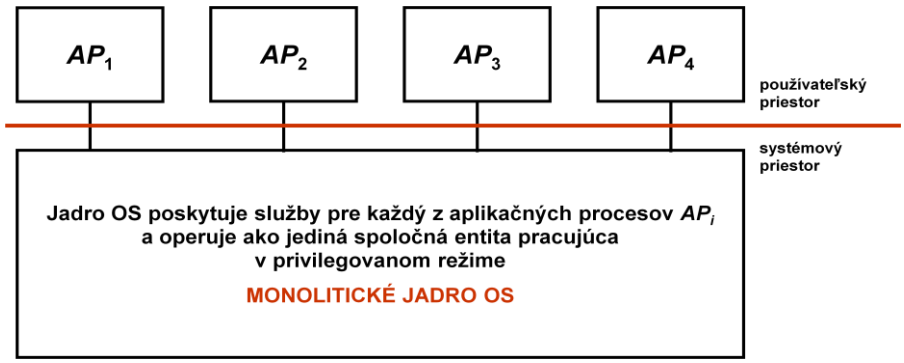
Zadanie 1	Skúste pomocou internetu nájsť, aký OS používajú počítače Macintosh spoločnosti Apple Computer. Aký názov má jeho najnovšia verzia?
Zadanie 2	Zahrajte sa hru, ktorá prezentuje činnosť OS pri prideľovaní zdrojov procesom. Čo sa vám javilo ako najťažšie pri manažovaní zdrojov pre jednotlivé procesy? Adresa hry: http://courses.cs.vt.edu/csonline/OS/Lessons/Resources/Lesson.html

3.1 Jadro OS

Jadro je základom operačného systému. Zavádza sa do operačnej pamäte počítača pri štarte a zostáva v činnosti po celú dobu behu operačného systému. Jadro môže byť naprogramované rôznymi spôsobmi a podľa toho jadrá OS delíme na:

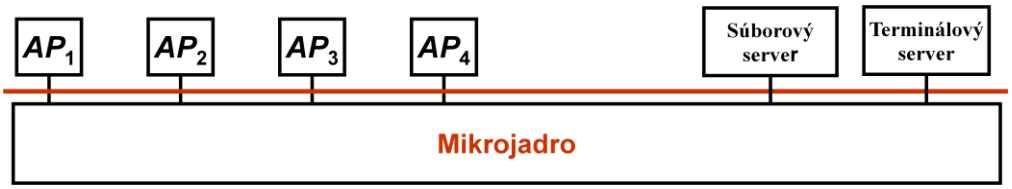
- Monolitické jadro
- Mikrojadro
- Hybridné jadro

Kód operačného systému s **monolitickým jadrom** je spustený v rovnakom jadrovom pamäťovom priestore (kernel space). Preto sú jednotlivé služby v jadre veľmi silno previazané, čo zvyšuje efektívnosť a rýchlosť jadra. Na druhej strane, chyba v jednom subsystéme jadra môže zablokovať iný, alebo dokonca zhodiť celé jadro. Monolitické jadro majú napr. MS-DOS, Windows 9x, Unix, Solaris, Linux.



Obr. 17 Monolitické jadro OS

Pri **mikrojadre** samotné jadro poskytuje len základnú funkčnosť potrebnú pre vykonávanie služieb. Jadro obsahuje len najzákladnejšie funkcie (typicky správu pamäte a podporu pre plánovanie procesov a medziprocesorovej komunikácie), ostatné potrebné časti jadra sú riešené v používateľskom priestore ako bežné procesy (označované ako servery).



Obr. 18 Mikrojadro

Hybridné jadrá sa snažia skombinovať rýchlosť a jednoduchosť dizajnu monolitického jadra s bezpečnostnými výhodami mikrojadier. Časť kódu je priamo súčasťou jadra a zdieľa jadrový pamäťový priestor (ako monolitické jadro), zatiaľ čo iná časť je riešená formou samostatných procesov (ako mikrojadro). Na rozdiel od mikrojadra, všetky (alebo skoro všetky) služby bežia v jadrovom pamäťovom priestore. Hybridné jadro majú napr. OS Windows s NT jadrom (Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7), rodina Windows CE (Windows Mobile...), Mac OS X a ďalšie.

V nasledujúcich podkapitolách budú vo všeobecnosti vysvetlené jednotlivé správy operačných systémov, pričom prakticky budú ilustrované na OS Windows XP. Správam v OS Linux je venovaná zvláštna kapitola.

3.2 Správa prostriedkov

Nasledujúca kapitola podrobnejšie rozoberá jednotlivé správy, za ktoré je OS zodpovedný.

Správa procesov

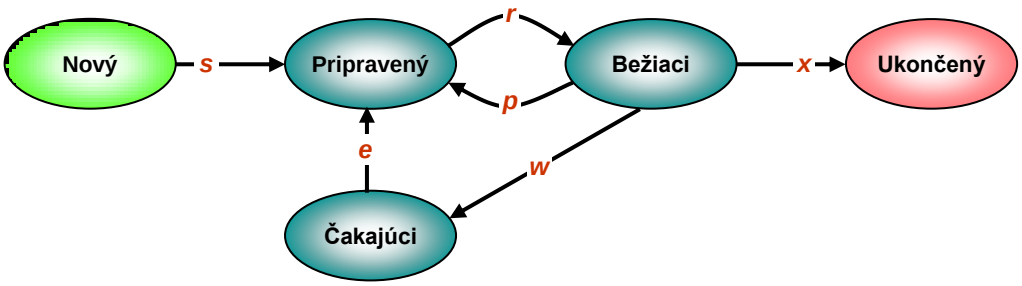
Proces je spustený počítačový program. Je umiesený v operačnej pamäti počítača v podobe postupností strojových inštrukcií vykonávaných procesorom. Jeden program môže v počítači bežať ako viac procesov s rôznymi údajmi (napríklad viackrát spustený webový prehliadač zobrazujúci rôzne stránky). Operačný systém zaisťuje oddelený beh procesov, prideľuje im systémové prostriedky počítača a umožňuje používateľovi procesy spravovať (spúšťať, ukončovať...).

V texte pri použití procesora berieme do úvahy jednojadrový procesor, resp. pri použití viacjadrového procesora, uvažujeme každé jadro ako samostatný procesor.

Moderné operačné systémy umožňujú spustiť zároveň viac procesov (textový editor, tabuľkový kalkulátor, e-mailový klient a pod.). Pokiaľ je v počítači menej procesorov, ako je bežiacich procesov, musia sa procesy na procesoroch striedať, čo označujeme ako zmena kontextu. Multitasking (multi = mnoho, task = úloha) označuje schopnosť operačného systému vykonávať (zdanlivo) niekoľko procesov súčasne. Jadro operačného systému veľmi rýchlo strieda na procesore bežiace procesy, takže používateľ počítača má dojem, že bežia súčasne.

Životný cyklus procesu prebieha podľa diagramu stavových prechodov, obr. 19.

Proces je vytvorený buď príkazom používateľa, alebo na žiadosť operačného systému o vykonaní služby, či na žiadosť iného procesu (rodiča). Vytvorený proces je v stave „pripravený“ – pripravený k vykonaniu a čaká iba na pridelenie procesora. Spustením procesu, na základe plánovacieho algoritmu, prechádza proces do stavu „bežiaci“. „Bežiaci“ proces môže byť ukončený normálne, t.j. bol celý vykonaný, alebo násilne zastavený používateľom, vykonaním chybnej inštrukcie, chybou vstupno-výstupného zariadenia, porušením ochrany pamäti, alebo na žiadosť rodiča a pod. „Bežiaci“ proces môže byť po vypršaní časového limitu pre jeho beh (uplynutie maximálneho časového kvanta) presunutý do stavu „pripravený“. „Bežiaci“ proces môže byť len jeden, ak je k dispozícii len jeden procesor, ale v stave „pripravený“ môže byť viacej procesov zaradených do radu alebo inej dátovej štruktúry, ktorú využíva plánovací algoritmus.

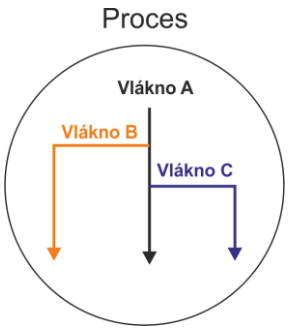


Prechod	Význam
s	Proces vzniká – *start*

r	Procesu je pridelený procesor (môže pracovať) – ***run***
w	Proces žiada o službu, na ktorej dokončenie musí čakať – ***wait***
e	Vznikla udalosť, ktorá spôsobila, že sa proces „dočkal“ – ***event***
x	Proces ukončil svoji existenciu (sám nebo „násilne“) – ***exit***
p	Procesu bol odňatý procesor, hoci je proces ďalej schopený behu, tzv. **preempcia** (napr. vyčerpaní časového kvanta) – ***preemption***.

Obr. 19 Stavový diagram životného cyklu procesu

Proces môže byť vnútorne rozdelený na niekoľko nezávisle, príp. paralelne bežiacich úloh, tzv. vlákien. **Vlákno** (thread) je objekt vytváraný v rámci procesu a viditeľný vo vnútri procesu. Tradičný proces je proces tvorený jediným vláknom. Vlákna podliehajú plánovaniu a prideľuje sa im strojový čas aj procesory. Vlákno sa nachádza rovnako ako proces v stavoch: beží, pripravené, čakajúci… Vlákna majú niekoľko výhod. Napríklad: Keďže vlákna môžu zdieľať spoločné dáta, nemusí sa používať medziprocesorová komunikácia, čím sa zrýchli vykonávanie výpočtu. K zrýchleniu výpočtu vedie aj fakt, že vlákna sa môžu vykonávať paralelne na viacerých procesoroch (príp. jadrách procesoru) počítača. Nevýhodou vlákien je zložitejšie vytváranie programu pre programátora, kde treba brať do úvahy synchronizáciu vlákien, príp. možnosť uviaznutia (deadlock) celého procesu, ak dve vlákna z nejakého dôvodu na seba vzájomne čakajú. Takmer každý profesionálny softvér však vlákna používa.



Proces pozostávajúci z troch vlákien

Zadanie 3

Prečo je v operačnom systéme dovolené spúšťať viac procesov? Nestačilo by, ak by bežal len jeden proces?

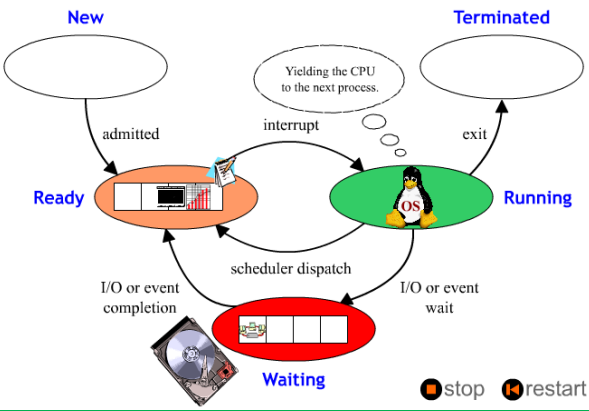
Zadanie 4

Pozrite si animovaný stavový diagram procesov pre jednoprocesorový OS zo stránky:

http://courses.cs.vt.edu/csonline/OS/Lessons/Processes/ProcessStateDiagram.swf

Priebeh zastavte a krokujte po jednotlivých fázach.

Čo pre beh procesu znamená, keď proces potrebuje získať dáta zo vstupno-výstupného (I/O) zariadenia?



Zadanie 5

Zo stránky
http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

si stiahnite softvér Process Explorer, ktorý umožňuje zobraziť detailné informácie o počte vlákien v procese. Spustite program Kalkulačka a Maľovanie. Koľko vlákien majú programy? Čo sa zmení po otvorení nápovede v programoch?

Správa zariadení

Ovládač (driver) je program, ktorý preberá od programovej vrstvy nezávislej od zariadenia požiadavky na vykonanie určitých operácií a odovzdáva ich zariadeniu vo forme jemu zrozumiteľných príkazov.

Jedine v ovládači sú zabudované konkrétne údaje o zariadení, napr. koľko a akých registrov má radič zariadenia, aké príkazy rešpektuje a ešte celý rad údajov, ktoré sú iné pre každý typ zariadenia. Preto je potrebné pre neznáme zariadenia ovládač stiahnuť a nainštalovať.

Radič periferného zariadenia je elektronický komponent zariadenia. Ide väčšinou o dosku v počítači a OS pomocou ovládača skoro vždy komunikuje práve s radičom.

Procesy potrebujú často pristupovať k periférnym zariadeniam pripojeným k počítaču, ktoré sú ovládané jadrom OS cez ovládače zariadení. OS sa stará o odstránenie technických detailov a poskytuje procesu využitie zariadenia na vyššom stupni abstrakcie. Napríklad pre zobrazenie niečoho na obrazovke musí proces vytvoriť požiadavku pre jadro, ktoré ho odovzdá radiču displeja, ktorý je potom zodpovedný za skutočné vykreslenie znakov alebo pixelov.

Jadro OS musí udržiavať zoznam dostupných zariadení. Tento zoznam môže byť známy vopred (napríklad vo vloženom systéme, kde jadro je prepísané keď sa dostupný hardvér zmení), nastavený používateľom alebo zistený operačným systémom za behu (Plug-and-play).

Úlohou správy zariadení je aj prideľovanie zariadení, t.j. ak zariadenie (napr. tlačiareň, kde nemôžu naraz tlačiť dva procesy) môže používať v jednej chvíli len jeden proces, operačný systém musí situáciu vyriešiť. Navyše kontroluje, či proces má oprávnenie zariadenie používať.

Periférne zariadenia v OS Windows XP je možné skontrolovať pomocou Správcu zariadení, kde je možné spravovať aj ovládače zariadení.

Správa pamäte

Operačný systém zodpovedá aj za správu systémovej pamäte (anglicky memory management), ktorú používajú procesy v systéme a zabezpečuje, že proces nepoužije pamäť už obsadenú iným procesom. OS môže zabezpečovať aj následné uvoľňovanie pamäte (keď už proces pamäť nepotrebuje), nastavovať ochranu pamäte a eventuálne aj správu adresácie pamäte. Existujú rôzne metódy ochrany pamäte, ako napr. segmentácia a stránkovanie pamäte.

Operačný systém zvyčajne rieši problém obmedzenia veľkosti fyzickej pamäte (fyzicky pripojená operačná pamäť RAM) používaním **virtuálnej pamäte**. Každý proces má ilúziu vlastnej virtuálnej pamäte, do ktorej adresuje pomocou tzv. virtuálnych adries a nezaujíma sa, kde a aká je skutočná adresa vo fyzickej pamäti. Prevod medzi virtuálnou a fyzickou adresou je podporovaný priamo procesorom.

V súčasných bežných operačných systémoch je virtuálna pamäť implementovaná pomocou **stránkovania pamäte** spolu so stránkovaním na disk, ktoré rozširuje operačnú pamäť o priestor na pevnom disku a tým umožňuje, aby mohla byť virtuálna pamäť väčšia ako fyzická pamäť. Stránkovanie je adresovacia technika, pri ktorej sa virtuálna pamäť rozdelí na úseky pevnej dĺžky tzv. stránky a na rovnaké úseky je rozdelená aj fyzická pamäť, na tzv. rámce. Potrebná stránka virtuálnej pamäte je potom mapovaná do príslušného rámca vo fyzickej pamäti. Stránky, ktoré nie sú potrebné, alebo sa do fyzickej pamäte nezmestili, sú odložené na disk. V prípade, že je stránka potrebná (t.j. požaduje sa adresa z tejto stránky), musí byť z disku opäť načítaná do fyzickej pamäte. Ak vo fyzickej pamäti nie je voľné miesto, vyberie sa vhodná stránka na základe určitých kritérií, tzv. „obeť“, ktorá je následne odložená na disk a tak uvoľní miesto vo fyzickej pamäti. Transformácia virtuálnej adresy na fyzickú sa vykonáva na základe tabuľky stránok (page table).

Zadanie 6

OS Windows pre ukladanie virtuálnej pamäte na disku využíva súbor `pagefile.sys`, ktorý je zväčša uložený priamo v priečinku `C:` ako skrytý súbor.

Nájdite súbor `pagefile.sys` na disku a zistite jeho veľkosť. Zistite nastavenie veľkosti virtuálnej pamäte v systéme. Porovnajte veľkosti.

Nezabudnite nastaviť *Zobrazovanie skrytých súborov a priečinkov* pomocou programu Prieskumník.

Správa súborov

Operačný systém poskytuje služby pre správu a prácu so súbormi. Najzákladnejšie operáciami sú:

- vytvorenie súboru s daným menom,
- nastavenie príznakov (atribútov) súboru,
- otvorenie súboru pre čítanie, alebo modifikáciu,
- čítanie a modifikáciu otvoreného súboru,
- uloženie zmien na pamäťové médium,
- zatvorenie súboru a uloženie prípadných vykonaných zmien na pamäťové médium.

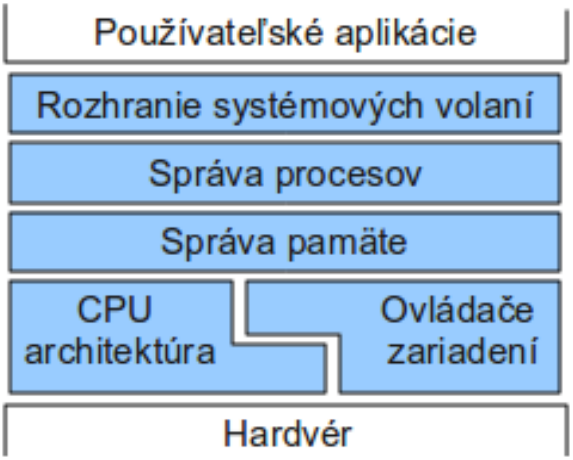
Spôsob, akým počítač organizuje a manipuluje s priečinkami a súbormi, sa vo všeobecnosti označuje ako *súborový systém*. Väčšina počítačov má aspoň jeden súborový systém. Niektoré OS umožňujú použitie niekoľkých rôznych súborových systémov. Napríklad OS Windows XP podporuje aj starší súborový systém typu FAT pôvodne vytvorený pre OS MS DOS a navyše podporuje nový súborový systém NTFS. Každý súborový systém má svoje výhody a nevýhody. OS Linux má vlastné súborové systémy (ext3, ReiserFS,…), avšak podporuje aj súborové systémy OS Windows.

Porovnanie vlastnosti jednotlivých súborových systémov OS Windows FAT a NTFS môžeme nájsť napr. na stránke http://www.ntfs.com/ntfs_vs_fat.htm

Program, ktorého hlavnou úlohou je zjednodušenie práce pre používateľa s počítačovými súbormi a adresármi, najmä prehliadanie, vykonávanie, kopírovanie, mazanie, premenovanie, sa nazýva Správca súborov. Každý operačný systém poskytuje aspoň jedeného správcu súborov. Pre OS Windows je najpoužívanejším súborovým manažérom program Windows Explorer.

3.3 Operačný systém GNU/Linux

V tejto kapitole sa chceme pozrieť dovnútra OS Linux a práve preto je dôležité používať presnejší názov GNU/Linux. Súvisí to s tým, že softvér, ktorý je na linuxovom počítači nainštalovaný, môžeme rozdeliť zhruba na dve časti – na jadro a na aplikačný softvér. Tieto dve časti majú rôznu funkciu, sú navzájom značne nezávislé a majú aj rôzny pôvod.



Obrázok 20: Zjednodušená štruktúra jadra Linux

Základom operačného systému GNU/Linux je jeho jadro (Obr. 20). Jeho tvorcom je Linus Torvalds a nazýva sa Linux. Jadro sprostredkováva spojenie medzi hardvérom počítača (pamäť a vstupno-výstupné zariadenia) a používateľskými programami. Tými sú bežné aplikácie, s ktorými sa stretáva používateľ – nástroje na spracovanie textu, kreslenie, prehrávanie hudby a videa – ale aj obslužné a iné špeciálne programy, s ktorými sa používateľ stretáva už menej (napríklad kompilátor). Väčšina nástrojov z tejto druhej kategórie vznikla v rámci projektu GNU (Gnu is not Unix), ktorý viedol Richard M. Stallman a jeho nadácia FSF (Free Software Foundation) od

začiatku 80-tych rokov. Tieto nástroje sú neoddeliteľnou súčasťou operačného systému, bez nich by jadro nemalo ako plniť svoju úlohu. Z tohto dôvodu budeme v texte odlišovať GNU/Linux ako operačný systém pozostávajúci z jadra a používateľských programov od samotného jadra Linux.

Rozlišovanie jadra a aplikácií je dôležité aj preto, lebo kombinácia GNU + Linux nie je jedinou možnosťou. Existujú aj GNU/Hurd (Hurd je jadro, ktoré vyvíja FSF) alebo GNU/Solaris (Solaris je zase jadro, ktoré pôvodne vyvíjala spoločnosť SUN), teda kombinácie nástrojov GNU s iným jadrom, ako je Linux. Naopak, Linux je bez GNU nástrojov použitý v operačnom systéme Android, ktorý spoločnosť Google vyvíja pre mobilné telefóny a iné podobné zariadenia, alebo v moderných televízoroch a inej konzumnej elektronike.

Zadanie 7	Na stránke www.kernel.org v časti *What is Linux* zistite, ktoré počítačové architektúry Linux podporuje.

Jadro Linux

Jadro operačného systému je správcom hardvérových prostriedkov počítača, ktoré sprístupňuje používateľským programom. Veľmi zjednodušená schéma Linuxu je na Obr. 20. Podrobnejšiu schému možno nájsť na stránke http://www.makelinux.net/kernel_map.

Na najnižšej logickej úrovni jadra sa nachádza kód, ktorý priamo spolupracuje s hardvérom (napr. prostredníctvom jeho registrov). Táto časť na jednej strane súvisí s procesorom a jeho architektúrou a na druhej s prídavnými zariadeniami (disky, sieťové adaptéry a mnohé ďalšie. Jadro je napísané v jazyku C, pričom len malá časť, súvisiaca s architektúrou, musí byť napísaná v zodpovedajúcom assembleri. Vďaka tomu je Linux veľmi dobre prenositeľný – dnes ho možno rovnako dobre použiť na mobilných telefónoch, ale aj na najväčších superpočítačoch (http://en.wikipedia.org/wiki/List_of_Linux_supported_architectures).

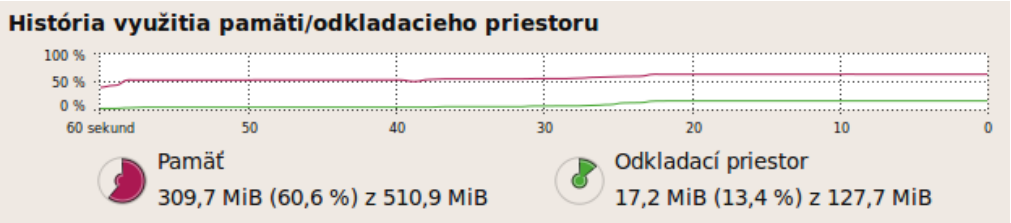
Ovládače zariadení

Najväčšiu časť kódu Linuxu predstavujú ovládače zariadení – Linux dnes podporuje najviac zariadení zo všetkých operačných systémov [5]. Tieto ovládače sú pritom priamo zaradené do jadra, takže používateľ si ich nemusí sám doinštalovávať. Samozrejme, že toto pravidlo má aj výnimky. Napríklad, viaceré ovládače grafických adaptérov nie sú otvoreným softvérom a preto ich treba doinštalovať. V prípade OS Ubuntu systém na dostupnosť takýchto ovládačov sám upozorní alebo si ju možno overiť v menu Systém -> Správa -> Ovládače hardvéru. Samotná inštalácia je otázkou niekoľkých kliknutí myšou.

Správa pamäte

Jednou z úloh jadra je mapovanie virtuálneho adresného priestoru do fyzickej operačnej pamäte počítača alebo dokonca aj do pamäťového priestoru na diskovom zariadení. V druhom prípade ide o odkladanie pamäťových stránok na disk do odkladacieho priestoru a začne k nemu dochádzať v prípade, keď sa sumárne požiadavky všetkých bežiacich programov začnú blížiť k veľkosti operačnej pamäte počítača. Tento odkladací priestor sa vytvára pri inštalácii Linuxu, keď sa na tento účel vyčleňuje jeden diskový oddiel. Celkový stav pamäťových požiadaviek bežiacich programov zistíme pomocou programu *Systém -> Správa -> Monitor* systému v záložke *Zdroje* (Obr. 21).

Odkladací priestor má ešte jedno použitie. Pri hibernácii systému (teda pri takom vypnutí počítača, keď sa zachová aktuálny stav bežiacich programov) sa do odkladacieho priestoru uloží obsah celej operačnej pamäte. Odtiaľ sa pri opätovnom zapnutí počítača opäť načíta a programy pokračujú v práci tam, kde sa pred hibernáciou zastavili. Z tohto využitia aj vyplýva odporúčaná veľkosť odkladacieho priestoru – priestor má byť väčší ako operačná pamäť. Inak môže byť aj menší.



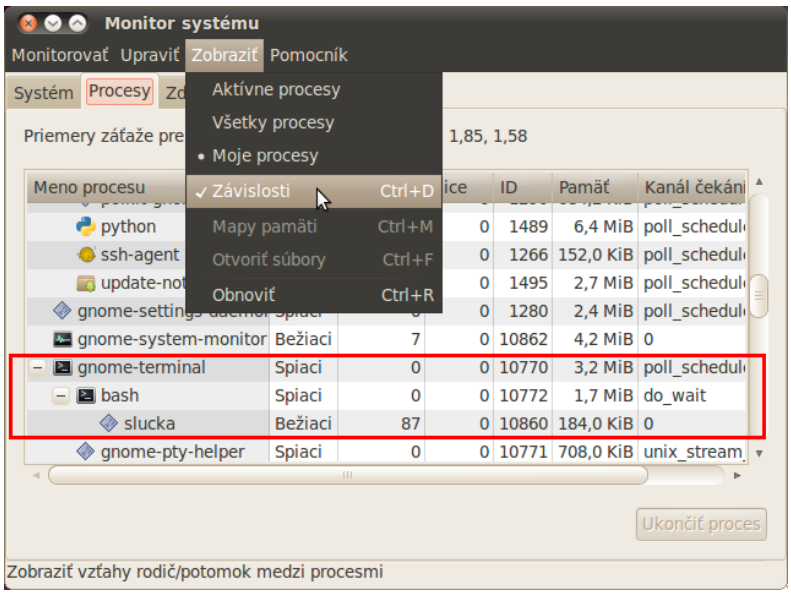
Obrázok 21: Grafické znázornenie spotreby operačnej pamäte a odkladacieho priestoru v programe Monitor systému.

Virtualizácia pamäte umožňuje obmedzenie práv používateľského programu. Vďaka nej program môže pristupovať len do „svojej“ pamäte a nie do pamäťového priestoru iných programov alebo dokonca do priestoru, ktoré využíva samotné jadro. Jadro samozrejme nepracuje s virtuálnou pamäťou – do operačnej pamäte pristupuje priamo. Tu častokrát na odlíšenie používame termíny kernelový a používateľský priestor.

Oddelenie používateľského a kernelového pamäťového priestoru má zásadný vplyv na stabilitu systému. Závažná chyba v používateľskej aplikácii, spočívajúca v zápise na pamäťové miesto, kam sa zapisovať nesmie, totiž nemôže viesť k ohrozeniu celého systému – abnormálne sa ukončí len chybná aplikácia. Iné je to, samozrejme v kernelovom priestore, kde taká chyba vedie k zrúteniu celého operačného systému, k tzv. kernel panic.

Spúšťanie programov a procesy

Jednou z hlavných úloh jadra je vytváranie nových procesov, zavádzanie programov zo súboru do pamäte a prideľovanie procesorového času jednotlivým procesom. So spúšťaním programov a procesmi sme sa z pohľadu používateľa už zoznámili v module 2OS2. Tu si ukážeme, ako pri spúšťaní procesov používateľské programy využívajú služby jadra.



Obrázok 22: Vzájomná závislosť programov gnome-terminal, bash a slucka

Najskôr sa však pozrime na to, čo nám ukáže Monitor systému ešte o bežiacom programe. Spusťme program slucka na pozadí, otvorme si *Monitor systému* a v položke *Zobraziť* zaškrtnime *Závislosti*. Zobrazenie procesov sa zmení – vidíme, že náš proces vykonávajúci program slucka je akoby podradený procesu bash a ten je podradený procesu gnome-terminal (obr. 22). Je to naozaj tak: program gnome-terminal spustil interpreter príkazov bash a ten spustil náš program slucka. Takéto spúšťanie sa robí to pomocou dvoch volaní (funkcií) jadra – *fork* a *exec*. Takto vznikne hierarchia procesov na vrchole ktorej je proces init. Má identifikátor 1 a je predkom všetkých procesov v spustenom systéme.

Volanie *fork* zduplikuje bežiaci proces. Následne oba procesy, pôvodný aj nový pokračujú ďalej vo vykonávaní toho istého programu. Nový proces je pritom potomkom pôvodného procesu (rodiča). Najskôr sa však pozrime na program fork.pas. Podstatná časť programu je zobrazená na Obr. 23. Vidíme tu funkciu fpFork, ktorá volanie *fork* sprostredkováva. Podstatné je, že vracia rôzne hodnoty v rodičovi a potomkovi. Na základe toho teda môžeme odlíšiť, v ktorom procese sa nachádzame.

```
t := fpFork;      {vetvenie volaním funkcie FpFork}
if t = 0 then     {v potomkovi fpFork vracia 0}
        begin     {vykoná sa v potomkovi}
                  writeln('Potomok, proces č. ', fpGetPid);
        end
else              {v rodicovi fpFork vracia ID potomka}
        begin     {Vykoná sa v pôvodnom procese}
                  writeln('Rodic, proces č. ', fpGetPid);
        end;
```

Obrázok 23: Ukážka vetvenia procesor v jazyku Pascal.

Program pstree, ktorý zadáme v termináli, nám ukáže dva bežiace procesy fork, pričom jeden je potomkom druhého (Obr. 24). Tie sú potomkom procesu programu bash a ten je ďalej potomkom terminálu gnome-terminal, ktorý je potomkom procesu init (na obrázku nie je viditeľné).

```
├─gnome-terminal─┬─bash───fork───fork
│                ├─bash───pstree
│                ├─gnome-pty-helpe
│                └─{gnome-terminal}
```

Obrázok 24: Stromové usporiadanie procesov.

Zadanie 8

Z príkazového riadka spustite textový editor gedit. Pomocou programu pstree alebo *Monitor systému* si pozrite, kde v hierarchii súborov je umiestnený. Následne gedit *spustite z menu Aplikácie->Príslušenstvo->Textový editor* a opäť si pozrite jeho umiestnenie.

Jednoduchý interpreter príkazov

Vieme už, ako vytvoriť nový proces. Teraz si na príklade jednoduchého interpretera príkazov ukážeme, ako v tomto novom procese spúšťať programy. Základom interpretera (vykonaj.pas) je slučka, v ktorej sa opakovane načíta a vykoná príkaz (Obr.25). Program najskôr vytvorí volaním fpFork nový proces a v ňom volaním fpExecLP spustí zadaný príkaz (ten je uložený v reťazci mstr). Ak na konci podpríkazu nedáme znak &, hlavný proces čaká na dokončenie vytvoreného procesu volaním fpWait.

Program vykonaj skončíme vložením znaku CTRL-D, ktorý predstavuje koniec súboru (test na eof v programe vykonaj.pas).

```
write('Zadaj príkaz: ');
while not eof do
begin
        Readln(istr);
        mstr := DelChars(istr, '&');    {najdi a odstran znak &}
        t := fpFork;                     {vetvenie}
        if t = 0 then                {v potomkovi}
                fpExecLP(mstr, []);      {vykonaj zadany prikaz}
        if istr = mstr then      {v rodicovi, ak nebol znak &}
                fpWait(stat);    {cakaj na ukoncenie potomka}
        write('Zadaj príkaz: ');
end
```

Obrázok 25: Základná slučka interpretera príkazov.

Zadanie 9	Vyskúšajte si program `vykonaj` a spustite v ňom program `gedit` na pozadí (so znakom `&`) a tiež aj v popredí. Pozorujte, ako sa správa hlavný program.

Čo sme sa naučili

Ukázali sme, z čoho sa OS skladá, aké správy OS poskytuje (správa procesov, zariadení, pamäte, súborov), detailnejší opis ich činnosti a príklady pre OS Linux.

4 História OS

Moorov zákon je empirické pravidlo v ktorom platí, že zložitosť integrovaných obvodov sa zdvojnásobuje každých 24 mesiacov, pričom cena ostáva konštantná.

Zo začiatku počítače vôbec operačný systém nemali a programátor musel s počítačom rozprávať v jeho reči, teda zadávať presne jednotky a nuly, a pritom vedieť, kde sa v počítači čo nachádza, kde je aké zariadenie. S rozvojom výpočtovej techniky sa ale takáto metóda stávala neúnosnou. Z toho dôvodu vznikli programovacie jazyky. Miesto nekonečných radov čísel v dvojkovej sústave sa tak zadávali príkazy v podobe čísel osmičkovej alebo šestnástkovej sústavy a neskôr aj skutočné slová z písmen. Programovacie jazyky môžu byť buď viazané na konkrétny hardvér (napr. assembler), alebo sú na hardvér nezávislé (tzv. vyššie programovacie jazyky). Najstarším vyšším programovacím jazykom bol Short Code z roku 1949. Neskôr vznikol jazyk Fortran (1956, vyvinutý IBM), COBOL (1959), BASIC (1965, neskôr štandardný jazyk pre PC), Pascal (1971), C (1972), atď.

Aj vývoj OS neustále prebieha a požiadavky na OS sa menia spolu so zdokonaľovaním a možnosťami hardvéru, na ktorom sú spúšťané.

V 60. rokoch šiel vývoj ešte ďalej. Vznikla potreba programu, ktorý by základné funkcie systému obstarával sám a uľahčil tak programátorovi prácu. Programátor totiž stále ešte musel presne poznať hardvér počítača, napr. pri disketách alebo pevných diskov musel kódom zadávať, na aké miesto sa môžu nahrať dáta. Ak sa pomýlil a zadal úsek už obsadený, počítač mu nedal žiadnou správou najavo, čo sa stalo a dáta prepísal. Preto vznikli prvé operačné systémy pre sálové počítače (mainframe). So vznikom minipočítačov v polovici 60. rokov, ktoré nevyžadovali natoľko špecializovanú obsluhu ako mainframe, vyvstala potreba operačných systémov tak, ako ich poznáme dnes.

Mac OS od Apple Computers sa stal prvým rozšíreným OS využívajúci grafické používateľské rozhranie. Mnohé z jeho čŕt, ako sú okná a ikony sa neskôr stali samozrejmosťou pre všetky GUI.

V 70. rokoch došlo k vzniku dvoch operačných systémov – VMS a Unix a od neho odvodená varianta BSD. Od Unixu a BSD boli odvodené ďalšie verzie ako napr. IBM AIX, HP-UX, SGI IRIX, Cray Unicos, Sun Solaris a ďalšie. Všetko to však boli operačné systémy pre sálové počítače alebo minipočítače.

Všetky PC sa do roku 1981 ovládali nie pomocou dnes známych operačných systémov, ale prostredníctvom programovacieho jazyka Basic. Neskôr sa však objavil OS CP/M ako zjednodušenie Unixu (ako prvý zavádzal osemznakové mená súborov a trojznakové prípony a označenie diskových jednotiek písmenami). V roku 1981 firma IBM predstavila svoje PC s OS MS-DOS od firmy Microsoft. Podobne svoje „DOSy“ vyvíjali aj iné firmy, asi najslávnejším sa stal DR-DOS.

V tej istej dobe pripravovala firma Apple prvý operačný systém s grafickým používateľským rozhraním s myšou ovládanými okienkami namiesto príkazového riadku, navyše bol celý operačný systém 32-bitový, oproti 16-bitovým u PC. Počítač Macintosh z roku 1984 sa stal legendou. Umožňoval multitasking, mal multimédiá a vďaka ovládaniu myšou sa s ním mohol naučiť pracovať ktokoľvek. Ďalšími odlišnými variantmi oproti PC boli napr. počítače Atari alebo Commodore Amiga, ale ich podiel na trhu v priebehu rokov klesal. Firma IBM v spolupráci s Microsoftom v roku 1987 vytvorila nový operačný systém pre PC OS/2. Spolupráca oboch firiem sa však rozpadla a každá z nich vyvíjala svoju vlastnú verziu OS/2. Firma Microsoft tú svoju čoskoro premenovala na Windows NT. V tejto dobe pridáva Unix grafické používateľské rozhranie nazývané X Window System (1984).

Na prelome 80. a 90. rokov došlo k rozmachu siete internet, a záujem o Unix sa zvýšil. Od systému BSD bolo odvodených množstvo verzií pre PC, napr. FreeBSD, OpenBSD alebo NetBSD a najsľubnejší klon Unixu pre PC – Linux, výtvor fínskeho študenta Linusa Torvaldsa. Na prelome tisícročia sa objavila nová verzia OS od spoločnosti Apple MacOS X, zameraná na multimediálne aplikácie [4].

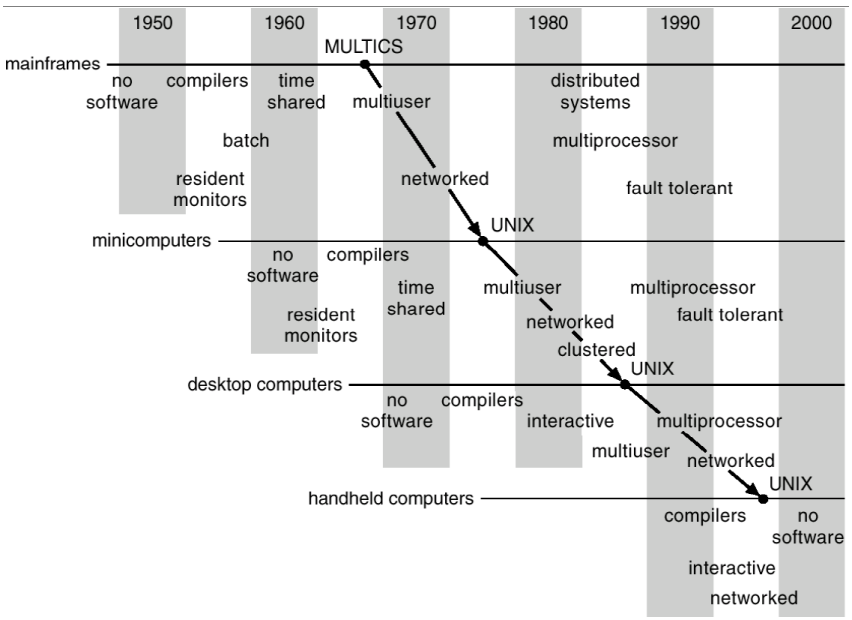
Nastane teda za päť, desať rokov situácia, kedy bude na stole len terminál s gigabitovým pripojením do internetu a všetka činnosť bude prebiehať na vzdialenom serveri kdesi za morom?
Tu vyvstáva otázka a obavy voči zverovaniu všetkých svojich dát a údajov nejakej tretej "osobe", ktorá by k nim teoreticky mohla mať voľný prístup.

V súčasnosti okrem nových verzii známych operačných systémov sa dostáva do popredia iný fenomén a to virtualizácia. Operačné systémy boli pôvodne navrhnuté tak, aby bežali priamo na hardvéri počítača a poskytovali služby aplikáciám. Pri virtualizácii operačného systému OS nebeží priamo na hardvéri, ale vo virtuálnom stroji, pričom takto môže byť spustených viac operačných systémov. V mnohých ohľadoch virtuálny stroj dnes plní úlohu, ktorú predtým vykonával operačný systém, vrátane riadenia hardvérových prostriedkov (procesor, pamäť, I/O zariadenia), používania plánovacích politík, či možnosti administrátorovi spravovať systém. O virtualizácii a aj o virtualizácii OS sme sa dozvedeli v kapitole Virtualizácia.

Nové smerovanie v OS môže predznamenať aj príchod operačného systém Google

Chrome OS spoločnosti Google, ktorý je zameraný na prácu s webom a využíva Cloud Computing, kde na počítači je spustený len prehliadač a všetko ostatné sa odohráva v „internetovom mraku“.

Zaujímavým je aj náhľad na históriu OS z pohľadu nových zariadení, kde sa zdá, že každý nový druh (mainframe, minipočítač, osobný počítač, embedded počítače, čipové karty, atď.) prechádza podobnými vývojovými etapami ako jeho predchodcovia, čo je vidno aj z nasledujúceho obrázka.



Obrázok 26 Historická genéza OS

Zadanie 1	Pomocou internetu zistite aký OS používajú v súčasnosti počítače Macintosh. Aké grafické používateľské rozhranie využíva?
Zadanie 2	Zistite chronologicky všetky verzie OS Windows, od predchodcu OS MS DOS až po súčasnú verziu OS Windows 7.
Zadanie 3	Na stránke http://www.levenez.com/unix/ si pozrite, ako sa vyvíjali unixové operačné systémy a nájdite tam OS Linux a MacOs X.

Čo sme sa naučili

Oboznámili sme sa s históriou operačných systémov z pohľadu ich chronologického vývoja a vzájomného ovplyvňovania. Navyše sme sa zamysleli nad možnými trendmi do budúcnosti.

Čo sme sa naučili v tomto module

Zhrnutie

V tomto module sme nadobudli vedomosti a zručnosti s bezpečnosťou OS, problematikou virtualizácie, prvotnými teoretickými znalosťami o štruktúre OS a poznatkami z histórie OS. Aktivity sa týkali narábania s heslami, vytvárania záloh a obnovy OS, firewallu, bezpečného spúšťania neznámeho softvéru, vytvárania virtuálnej CD/DVD mechaniky, virtualizácie OS cez nástroj VirtualBox. Navyše sme sa oboznámili s historickým pozadím OS a rozumieme pojmom ako jadro OS a správa zdrojov v OS.

Preverenie výstupných vedomostí

Účastník vzdelávania by mal vytvoriť počas tohto modulu v praktických cvičeniach minimálne nasledovné výstupné úlohy a prezentovať ich lektorovi pomocou zosnímaných obrazoviek:

- vytvoriť zálohovací bod, zistiť svoju IP adresu a ďalšie informácie, ktoré poskytuje počítač cez web, spustiť program Sandboxie a do v ňom program Family Key Logger, ukázať overenie digitálneho podpisu SW, spustiť softvér Process Explorer a detekovať viacero vlákien v programoch, zistiť veľkosť súboru `pagefile.sys` pre ukladanie virtuálnej pamäte, nainštalovať emulátor počítača ZX Spectrum, vytvoriť virtuálny počítač a spustiť v ňom systém z Live CD/DVD.

Hodnotenie účastníkov: absolvoval/neabsolvoval.

Literatúra a použité zdroje

[1] Vondruška, P.: Klíče a hesla (doporučení pro začátečníky), Crypto-World 3/2006, str.2-6, http://crypto-world.info/casop8/crypto03_06.pdf

[2] Klíma, V., Rosa, T.: Kryptologie pro praxi (39) – Ro-z-rušte heslo!, Sdělovací technika, 11/2006, str. 17, http://crypto-world.info/2006/ST_2006_11_17_17.pdf

[3] Oracle (2010) VirtualBox Documentation. Dostupné na internete: http://www.virtualbox.org/wiki/Documentation

[4] Koudelka, P.: Historie operačních systémů, http://airborn.webz.cz/histos.html

[5] Greg Kroah-Hartman: How Linux Supports More Devices Than Any Other OS, Ever. November 2010, Dostupné na internete: http://broadcast.oreilly.com/2008/10/how-linux-supports-more-device.html

[6] Portál projektu ĎVUi: *Slobodný a otvorený softvér a operačný systém Linux*. 2009. Dostupné na internete: http://dvui.ccv.upjs.sk/

[7] Ivan Bíbr a kolektív: *Ubuntu 10.04 CZ Praktická příručka uživatele Linuxu*. Computer Press, Brno, 2010

[8] *Documentation for Ubuntu 10.04*. August 2010. Dostupné na internete: https://help.ubuntu.com/10.04/

[9] Windows XP Professional: Ako na to [online], Dostupné na internete: http://www.microsoft.com/slovakia/windows/xp/pro/using/howto/default.mspx

Tento študijný materiál vznikol ako súčasť národného projektu Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika v rámci Aktivity „Vzdelávanie nekvalifikovaných učiteľov informatiky na 2. stupni ZŠ a na SŠ“.

Autori © PaedDr. RNDr. Ladislav Huraj, PhD.
prof. Ing. Miloš Šrámek, PhD.
Mgr. Miroslav Wagner

Názov Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

Podnázov Operačné systémy 3

Študijný materiál prešiel recenzným pokračovaním.

Recenzenti doc. Ing. Matilda Drozdová, CSc.
RNDr. Peter Gurský, PhD.

Počet strán 40

Náklad 300 ks

Prvé vydanie, Bratislava 2010

Vydal Štátny pedagogický ústav, Pluhová 8, 830 00 Bratislava, v súčinnosti s Univerzitou Pavla Jozefa Šafárika v Košiciach, Univerzitou Komenského v Bratislave, Univerzitou Konštantína Filozofa v Nitre, Univerzitou Mateja Bela v Banskej Bystrici a Žilinskou univerzitou v Žiline

Vytlačil BRATIA SABOVCI, s r.o., Zvolen

ISBN 978-80-8118-071-2