Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Architektúra informačných systémov

RNDr. Jaroslav Janáček, PhD.
2013

KPMG
cutting through complexity™

Obsah

- informačný systém – skladačka z komponentov
- vrstvy v informačných systémoch
- hardvér, operačný systém, databázové systémy
- virtualizácia, cloud
- klient-server model
- bezpečnostné funkcie vrstiev

Prečo?

- znalosti základov fungovania významných komponentov pomáhajú pochopiť význam a možnosti bezpečnostných opatrení
- uľahčiť komunikáciu neinformatikov s informatikmi

Informačný systém

- sa skladá z komponentov
  - všeobecných
    - napr. hardvér, operačný systém, databázový systém, rôzne všeobecné knižnice, podporné aplikácie, ...
  - špecifických
    - aplikácie vytvorené špecificky pre konkrétny informačný systém

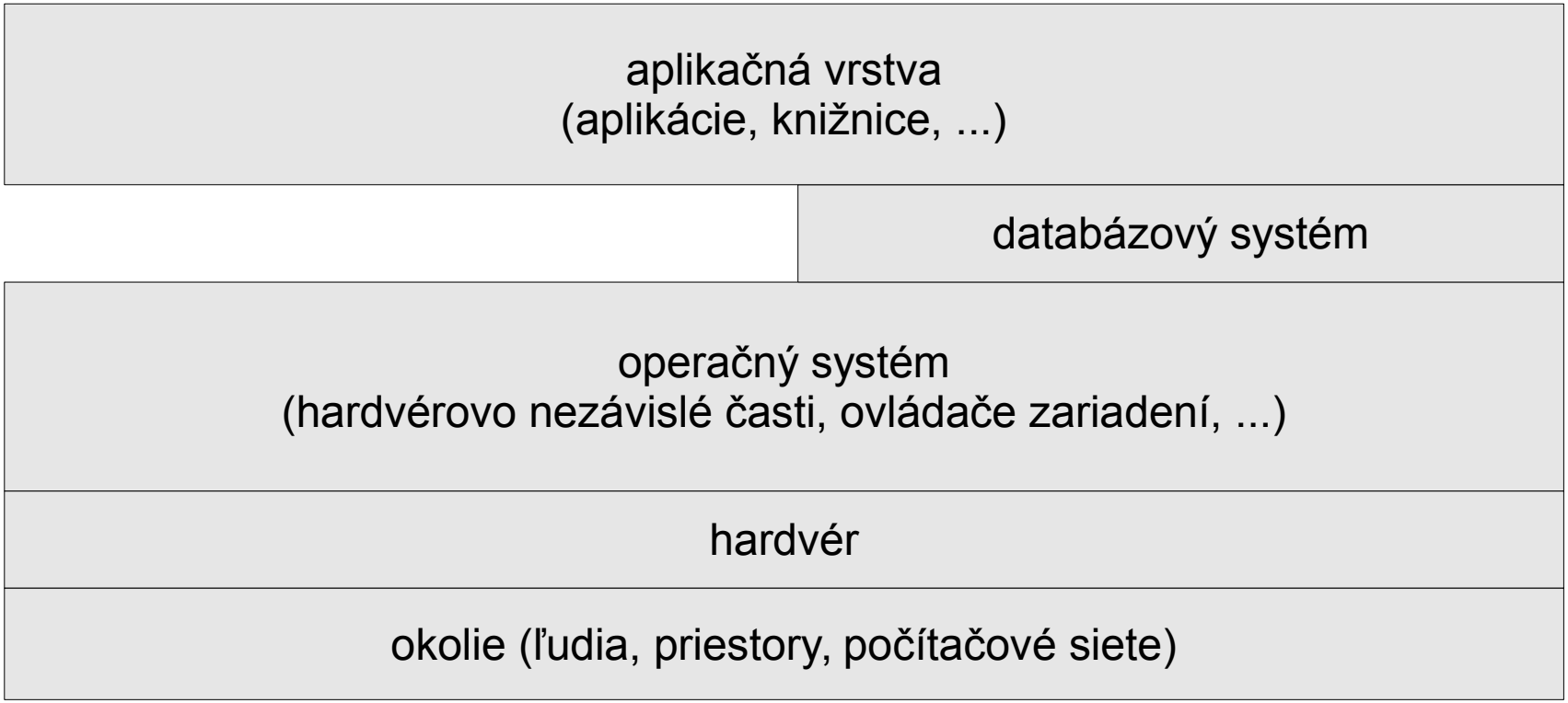
Komponent

- poskytuje definované *služby* prístupné prostredníctvom určitého *rozhrania*
  - *rozhranie* definuje spôsob, ako je možné službu využiť
- využíva služby iných komponentov
- môže sa skladať z viacerých menších komponentov

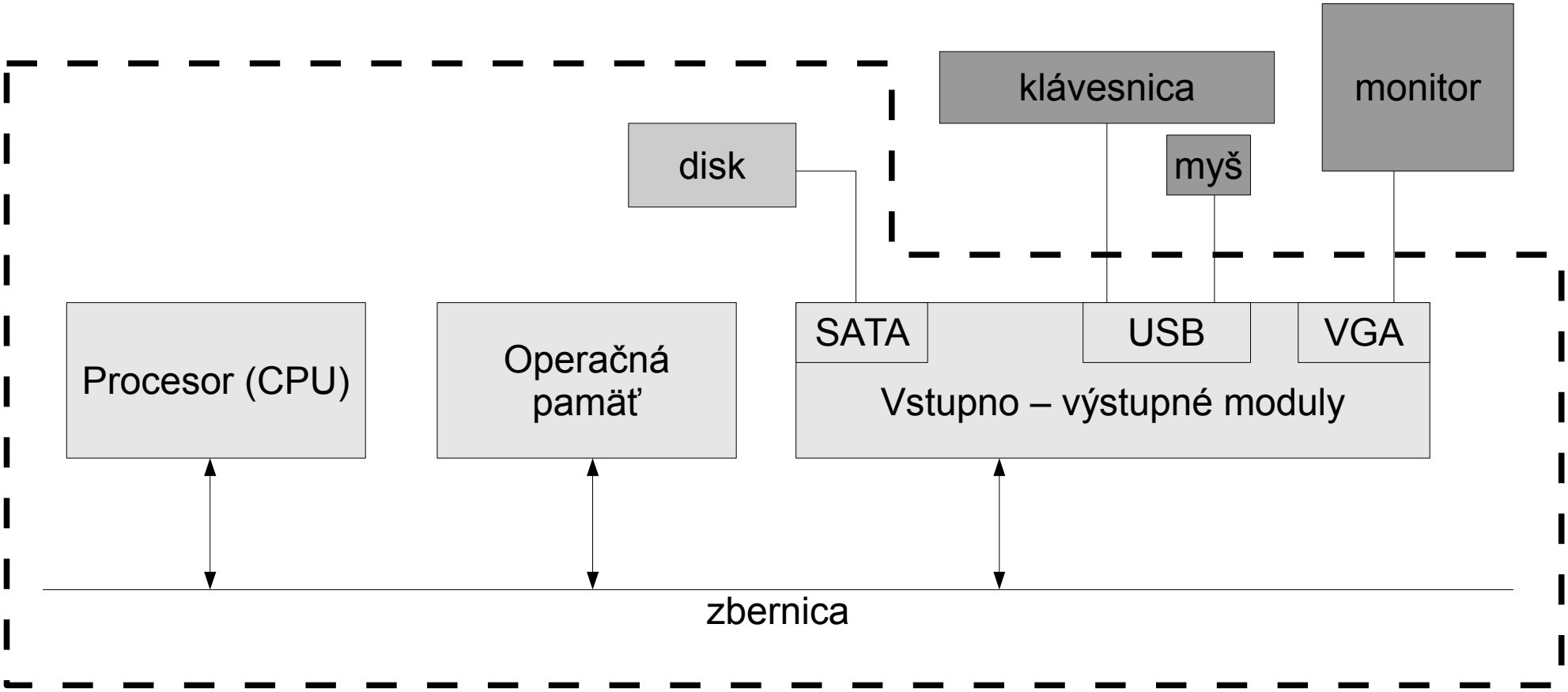
Výhody skladania z komponentov

- nie je potrebné vymýšľať vlastné riešenia pre bežné problémy
  - rýchlejší a lacnejší vývoj
  - jednoduchšia integrácia systémov
- je možné zdieľať všeobecné komponenty medzi rôznymi IS
  - šetrenie nákladov – napr. netreba samostatný hardvér
- pri zachovaní rozhrania je možné komponenty nahradiť inými
  - napr. môžeme presunúť údaje z lokálneho disku na externé diskové pole použitím iného komponentu v OS

Vrstvy v informačných systémoch



Hardvér


klávesnica
monitor
disk
myš
Procesor (CPU)
Operačná pamäť
SATA
USB
VGA
Vstupno – výstupné moduly
zbernica

HW – Základná doska

- zbernice na prepojenie jednotlivých komponentov
  - zbernica medzi CPU a pamäťou
  - PCI, PCI Express
- často integrované základné vstupno-výstupné moduly
  - radič diskov (IDE, SATA)
  - radič USB, PS/2
  - grafická karta

HW – Procesor (CPU)

- môže ich byť aj viac
- *jadrá* – v podstate samostatné procesory
- riadi činnosť počítača a vykonáva väčšinu operácií s údajmi
- základné časti
  - riadiaca jednotka
  - aritmeticko-logická jednotka
  - registre

HW – Procesor (CPU)

- riadiaca jednotka
  - načítava a dekóduje *inštrukcie programu*
  - aktivuje ďalšie obvody na vykonanie inštrukcie
- aritmeticko-logická jednotka
  - vykonáva základné aritmetické a logické operácie
- registre
  - slúžia na uloženie práve spracovávaných údajov
    - malá, rýchla pamäť priamo v procesore

HW – Procesor (CPU)

- inštrukcia
  - elementárny príkaz vykonateľný procesorom
    - načítanie údajov z operačnej pamäte do registra
    - zápis údajov z registra do operačnej pamäte
    - sčítanie/odčítanie/porovnanie/násobenie/delenie 2 čísel
    - „skok“ - presun na inú časť programu
    - ...

HW – Procesor (CPU)

- program
  - zdrojový text vo *vyššom programovacom jazyku*
    - vyššia úroveň abstrakcie, nezávislá od procesora
    - C/C++, Java, ...
  - preklad do *strojového kódu*
    - postupnosť inštrukcií konkrétneho procesora
    - alebo virtuálneho procesora (napr. Java Virtual Machine)
      - vykonáva sa pomocou *interpretera*

HW – Operačná pamäť

- dočasná pamäť s náhodným prístupom (RAM)
  - procesor môže pristupovať k ľubovoľnému miestu v pamäti
- uloženie vykonávaného programu a spracovávaných údajov
- veľkosti v rozsahu niekoľkých gigabyte-ov (GB)
  - v serveroch aj desiatky GB

HW – Operačná pamäť

- po vypnutí napájania stráca obsah
- ale nejaký čas to trvá
  - pri izbovej teplote sekundy až minúty
  - pri nízkych teplotách aj hodiny
- preto vypnutie nie je z bezpečnostného hľadiska postačujúce na okamžité zničenie obsahu pamäte

HW – Ďalšie pamäte

- „nezabúdajúce“ pamäte
  - EEPROM, Flash, ...
  - obsahujú program pre inicializáciu hardvéru (BIOS) a na načítanie a spustenie operačného systému
  - ich obsah je možné vymazať a nanovo nahrať
    - riziko zmeny škodlivým kódom
- cache pamäť
  - obsahuje kópiu používaných údajov z oper. pamäte
  - na preklenutie rozdielu v rýchlosti oper. pamäte a CPU

HW – Vstupno – výstupné moduly

- rozširujúce karty pripojené na zbernicu
  - prípadne integrované priamo na základnej doske
- príklady:
  - grafická karta – zobrazovanie na monitore
    - VGA, DVI, HDMI, DP
  - sieťová karta – pre pripojenie k poč. sieti
  - radič diskov SCSI/SAS

HW – Pevné disky

- trvalejšie ukladanie údajov a programov
- veľkosti v rozsahu desiatok GB až niekoľko TB
- obsahujú mechanicky citlivé prvky
  - čítacie a zapisovacie hlavy, platne (5-15 tisíc ot./min.)
  - časom sa opotrebujú a pokazia – strata údajov
- aj po prepísaní je možné rekonštruovať predchádzajúci obsah

HW – Pevné disky

- rozhrania
  - IDE, SATA – v stolných počítačoch a notebook-och
  - SCSI, SAS, FC – v serveroch
- rozhrania pre externé disky
  - USB, eSATA
- SSD
  - náhrada za pevné disky bez pohyblivých častí
  - rýchle, ale malá kapacita, obmedzený počet zápisov

HW – Komunikácia s V/V modulmi

- pomocou špeciálnych inštrukcií CPU
  - používané najmä pre komunikácie bez potreby prenosu väčších objemov údajov
- pamäťovo-mapované zariadenia
  - zariadenie sa pre CPU „tvári“ ako pamäť
- priamy prístup do pamäte (DMA)
  - prenos priamo medzi operačnou pamäťou a zariadením bez účasti CPU

HW – Prerušenia

- systém potrebuje reagovať na rôzne externé údalosti
  - napr. prijatie údajov zo siete, dokončenie DMA prenosu, ...
- zariadenia môžu generovať tzv. *prerušenie*
- riadiaca jednotka CPU medzi inštrukciami kontroluje, či nedostala žiadosť o prerušenie
  - ak áno, začne vykonávať inštrukcie programu na obsluhu prerušenia a až potom bude pokračovať v pôvodnom programe

Operačný systém

- odbremeňuje vyššie vrstvy od detailov hardvéru
  - poskytuje celý rad abstrakcií rôznych zariadení
- základné úlohy
  - správa procesov a procesora
  - správa pamäte
  - správa súborov
  - správa zariadení
- príklady: Windows, Linux, ...

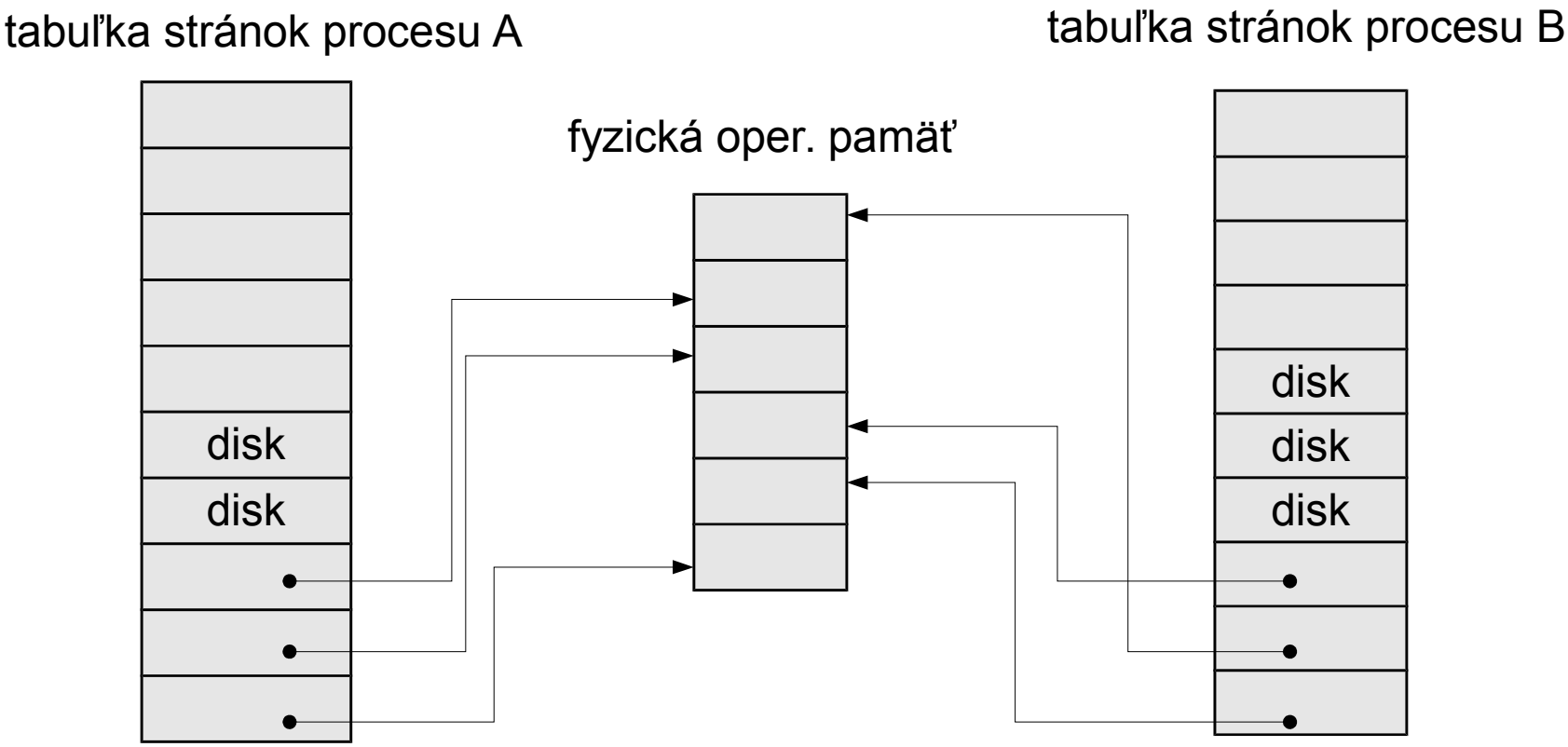
OS – Správa procesov

- *proces* – vykonávaný program
  - má pridelenú pamäť a iné zdroje v systéme
- multitasking
  - zdanlivo súčasný beh viacerých procesov
  - v skutočnosti striedanie procesov
  - správa procesov prideľuje a odoberá procesor jednotlivým procesom
- multithreading

OS – Správa pamäte

- prideľovanie a odoberanie blokov pamäte procesom
- virtuálna pamäť
  - OS „predstiera“, že má viac pamäte
  - procesom prideľuje bloky (*stránky*) virtuálnej pamäte
  - obsah stránky je buď niekde vo fyzickej pamäti, alebo je odložený na disku

OS – Správa pamäte



OS – Správa pamäte

- keď potrebná stránka nie je vo fyzickej pamäti
  - vznikne prerušenie – *výpadok stránky*
  - OS nájde voľný blok fyzickej pamäte
    - ak neexistuje, vyberie nejaký obsadený, uloží jeho obsah na disk a uvoľní ho
  - načíta doň obsah požadovanej stránky z disku
  - upraví tabuľku stránok
  - vráti sa k vykonávaniu prerušeného programu

OS – Správa súborov

- poskytuje abstrakciu pre ukladanie údajov
  - súbory, adresáre (priečinky)
  - poskytuje vyšším vrstvám štandardné rozhranie bez ohľadu na konkrétne detaily súborového systému
- súborový systém
  - definuje spôsob uloženia súborov na disku (alebo inom médiu)
    - rieši správu priestoru na disku – prideľovanie blokov jednotlivým súborom

OS – Správa súborov

- súborové systémy
  - lokálne
    - ukladajú údaje na pevných diskoch, CD/DVD, USB kľúčoch a pod.
    - napr. FAT16/32, NTFS, EXT2/3/4, XFS, JFS, ISO 9660, UDF, ...
  - sieťové
    - sprístupňujú súbory uložené na vzdialených systémoch
    - napr. CIFS, NFS, AFS, ...

OS – Správa zariadení

- poskytuje abstrakciu rôznych zariadení
  - odbremeňuje vyššie vrstvy od technických detailov
- rieši vylúčenia súčasného prístupu viacerých procesov k zariadeniu
  - napr. virtualizáciou zariadenia a riadeným prenosom údajov medzi virtuálnym a skutočným zariadením
    - napr. obrazovka, tlačiareň

OS – Vnútorné komponenty

- OS sa skladá z mnohých komponentov
  - nezávislé od hardvéru
    - napr. správa súborov, časť správy pamäte, sieťový subsystém, ...
  - závislé od hardvéru
    - ovládače zariadení
    - časť správy pamäte (manipulácia s tabuľkou stránok)
    - časti využívajúce špeciálne inštrukcie procesora
    - ...

OS – Bezpečnostné funkcie

- vzájomná izolácia procesov
  - vzájomná interakcia len cez definované a kontrolované rozhrania
- čiastočná izolácia procesov od hardvéru
  - prístup len pomocou služieb OS
  - priamy prístup len k „neškodným“ častiam hardvéru
    - napr. bežné inštrukcie procesora

OS – Bezpečnostné funkcie

- riadenie prístupu
  - procesy sú vykonávané v mene určitého používateľa
  - OS vyhodnocuje, či daný proces môže vykonať požadovanú operáciu s príslušným objektom
- identifikácia a autentifikácia
- vymazávanie zvyškovej informácie
  - napr. z bloku pamäte prideleného procesu

Databázový systém

- poskytuje aplikačnej vrstve služby na ukladanie a vyhľadávanie vo veľkých objemoch štruktúrovaných údajov – v databázach
- aplikačná vrstva nemusí riešiť problém s efektívnou manipuláciou s údajmi
  - len formuluje svoje požiadavky vo vyššom jazyku – napr. SQL
- spôsob uloženia údajov a efektívny prístup k nim rieši databázový systém

Databázový systém

- riadenie prístupu
  - na úrovni databázy, tabuľky, stĺpca
  - identifikácia a autentifikácia
- transakčné spracovanie
  - zabezpečuje konzistenciu použitých a uložených údajov
  - umožňuje návrat do konzistentného stavu v prípade zlyhania transakcie

Databázový systém

- príklad transakčného spracovania
  - proces na potvrdenie objednávky
    - zistí, či je na sklade požadované množstvo tovaru
    - ak áno, zníži stav skladu a potvrdí objednávku, ak nie, zamietne ju
  - 2 rovnaké procesy A a B bez transakcií:
    - A zistí stav (1ks), B zistí stav (1ks)
    - A zníži stav na 0 ks a potvrdí objednávku
    - B zníži stav na 0 ks (alebo -1 ks) a potvrdí objednávku

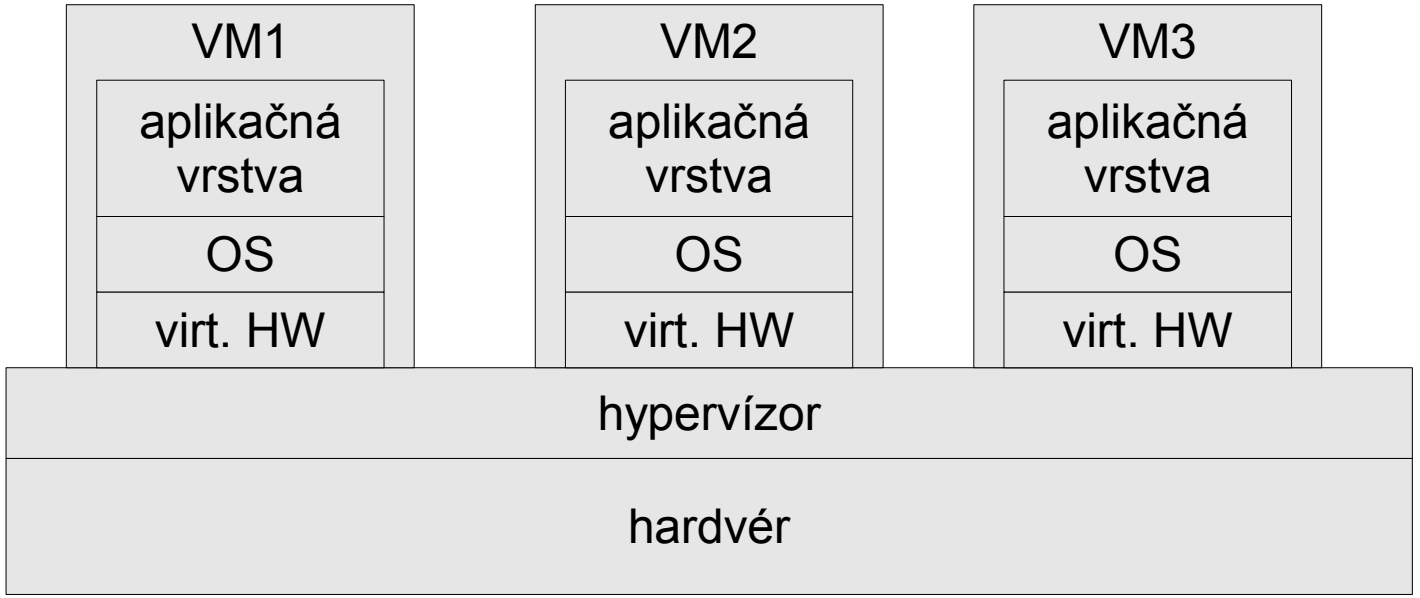
Databázový systém

- pri správnom použití transakčného spracovania:
  - A zistí stav (1 ks), B zistí stav (1 ks)
  - A zníži stav na 0 ks a potvrdí objednávku
  - pri pokuse B o modifikáciu stavu systém deteguje modifikáciu údaja, ktorý bol po čítaní zmenený inou transakciou a transakciu zruší pre možné narušenie konzistencie
  - B môže transakciu skúsiť zopakovať (pričom objednávku zamietne)
  - výsledkom bude úspešne potvrdená jedna objednávka, no zamietnutá druhá

Virtualizácia

- výkonné servery sú často využité len na zlomok svojej kapacity
  - neefektívne využitie priestoru, energie, financií
- virtualizácia
  - viac fyzických serverov sa nahradí jedným
    - lacnejší
    - energeticky a priestorovo úspornejší
  - medzi hardvér a OS pribudne *hypervízor*

Virtualizácia



Virtualizácia

- paravirtualizácia
  - OS virtuálnych počítačov musí byť prispôsobený na spoluprácu s hypervízorom
  - virtualizácia môže byť efektívnejšia
- plná virtualizácia
  - hypervízor emuluje nejaké bežné hardvérové zariadenia, OS virt. počítačov je bez zmeny
- hybridné riešenie
  - plná virtualizácia s výnimkami
    - napr. disky, sieťové karty, grafické karty použijú špeciálne ovládače špecifické pre hypervízor

Cloud

- poskytovateľ služieb
  - poskytuje cloudové služby (softvér, platforma, virtuálna infraštruktúra)
    - na požiadanie
    - zvyčajne samoobslužným spôsobom
  - zabezpečuje údržbu a prevádzku infraštruktúry
- používateľ služieb nepotrebuje vlastnú infraštruktúru
  - môže ušetriť na niektorých prevádzkových nákladoch

Cloud

- softvér ako služba (Software as a Service – SaaS)
  - poskytovateľ klientom poskytuje príslušnú aplikáciu
- platforma ako služba (Platform as a Service – PaaS)
  - poskytovateľ poskytuje platformu – OS + DB + web server + prostredie pre beh aplikácií (napr. PHP)
- infraštruktúra ako služba (Infrastructure as a Service – IaaS)
  - poskytovateľ poskytuje virtuálnu infraštruktúru – virtuálne počítače, úložisko údajov, virtuálne siete, ...

Cloud

- bezpečnosť
  - údaje sú uložené mimo dosah organizácie – v cloude
    - môže byť problém s dôverou, niekedy aj s legislatívou
  - poskytovateľ služieb môže efektívnejšie investovať do niektorých bezpečnostných riešení
    - môže byť výhoda pre menšie organizácie
  - nové hrozby
    - získanie kontroly nad systémom pre správu cloudu
    - objavenie a zneužitie slabiny v hypervízore

Model klient – server

- najčastejší model pre väčšie viacpoužívateľské informačné systémy
- údaje sú spracovávané na *serveri*
- používatelia pristupujú k systému pomocou *klienta*
  - hrubý klient
    - špecifická aplikácia inštalovaná na počítači používateľa
    - môže vykonávať predspracovanie vstupov a dospracovanie výstupov
  - tenký klient
    - malá aplikácia, zvyčajne univerzálna – napr. webový prehliadač
    - menšie možnosti predspracovania a dospracovania údajov a interakcie s používateľom

Model klient – server

- bezpečnosť
  - ochrana komunikácie medzi klientom a serverom
    - identifikácia a autentifikácia oboch strán
    - kryptografická ochrana dôvernosti a integrity pri prenose
  - riadenie prístupu zásadne na serveri
    - na klientovi môže mať len podpornú funkciu
      - napr. zneprístupnenie položiek menu
    - ale nie je možné sa naň spoliehať
      - útočník použije vlastného klienta bez obmedzení

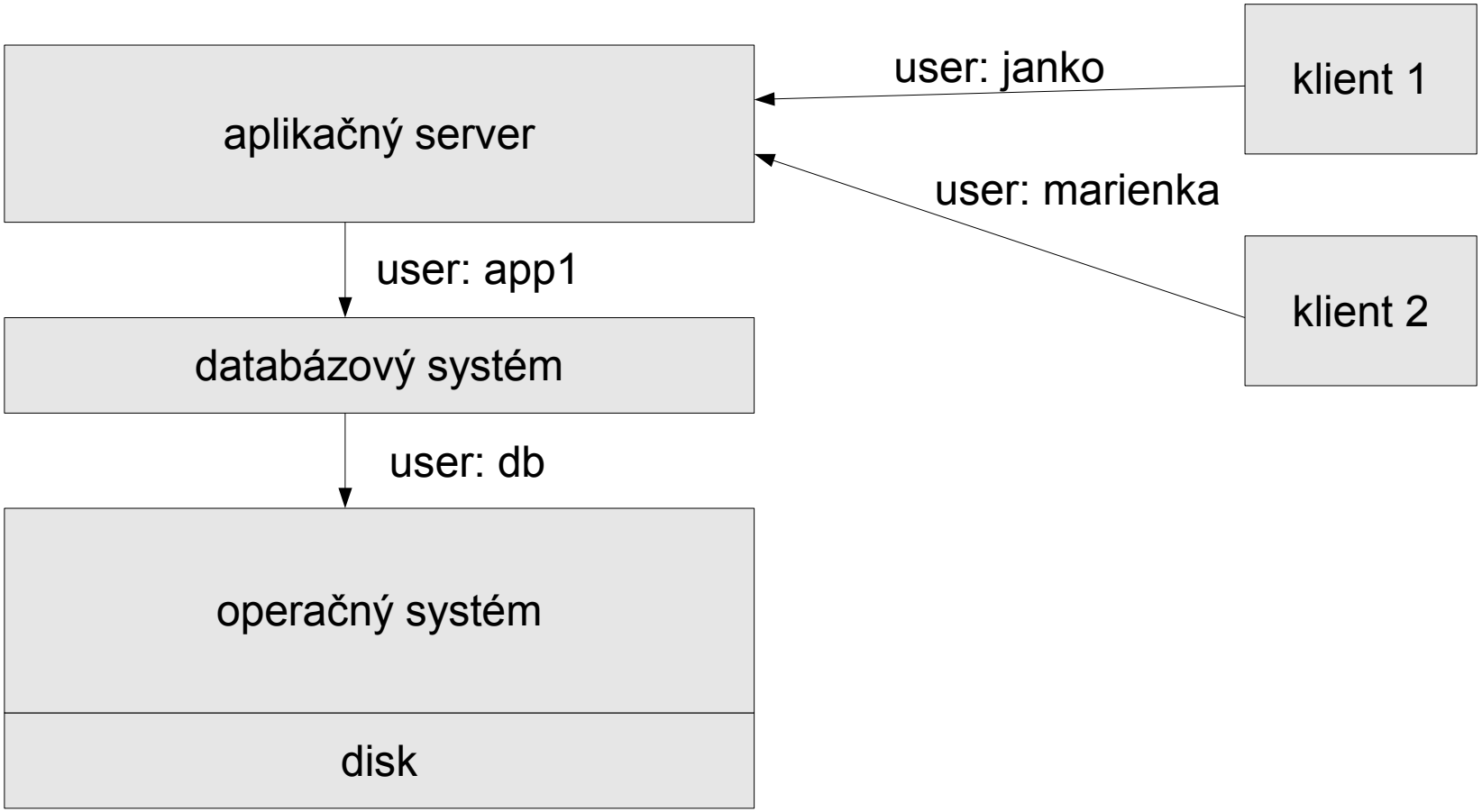
Bezpečnostné funkcie vrstiev

- Nevyhnutné predpoklady účinnosti bezp. funkcie
  - neobíditeľnosť
  - ochrana implementácie proti neoprávnenej zmene
  - ochrana bezpečnostných údajov proti neoprávnenej zmene
  - ochrana dôverných bezpečnostných údajov proti prezradeniu

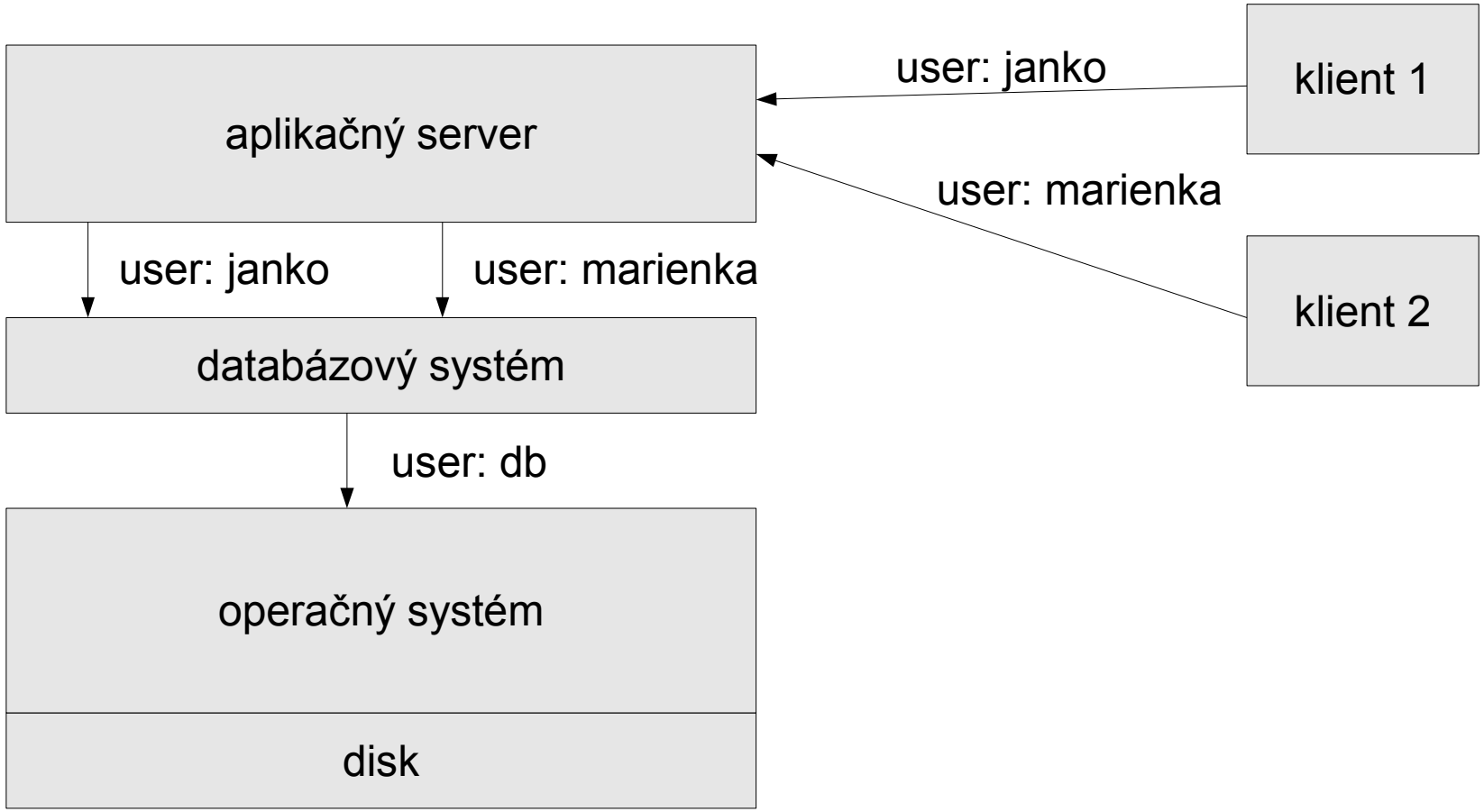
Bezpečnostné funkcie vrstiev

- Na ktorej vrstve implementovať bezpečnostné funkcie?
  - Bezp. funkcie realizované na určitej vrstve môžu brániť len útokom vedeným na tejto alebo prípadne vyššej vrstve.
    - výnimka – kryptografia
  - Čím vyššia vrstva, tým viac informácie o význame údajov a teda možnosť lepšie zohľadniť potreby.
    - údaje z pohľadu procesora sú len údaje, pre aplikáciu majú význam

Bezpečnostné funkcie vrstiev



Bezpečnostné funkcie vrstiev



Bezpečnostné funkcie vrstiev

- A teda na ktorej vrstve?

Bezpečnostné funkcie vrstiev

- A teda na ktorej vrstve?
- Na každej
  - primerane podľa možností
  - na nižších najmä vytvoriť vhodné predpoklady pre vyššie
  - na vyšších využiť lepšiu rozlíšiteľnosť (údajov, používateľov, ...) a vhodne využiť funkcie nižších vrstiev

Bezpečnostné funkcie vrstiev

- aplikačná vrstva
  - riadenie prístupu k aplikačným funkciám
  - pri klient – server modeli
    - izolácia útočníka na aplikačnej vrstve od prístupu k službám nižších vrstiev
- databázový systém
  - riadenie prístupu k údajom v databáze

Bezpečnostné funkcie vrstiev

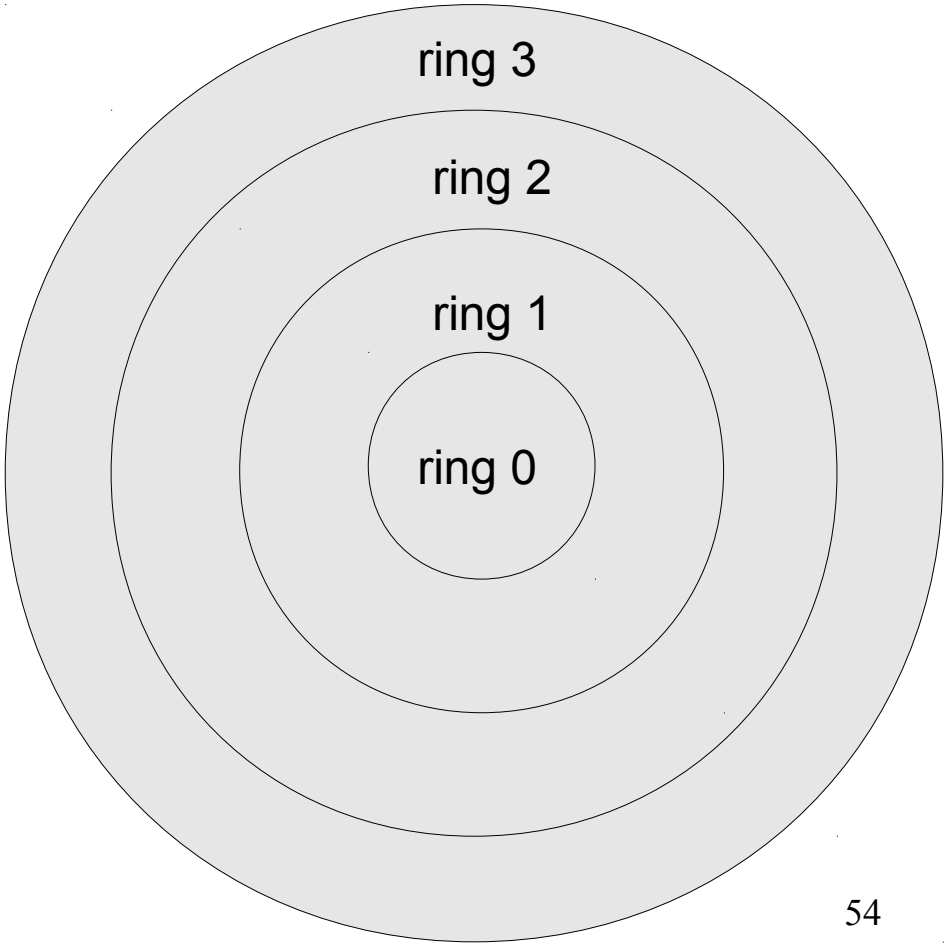
- operačný systém
  - ochrana vlastnej implementácie a bezpečnostných údajov
  - ochrana implementácie a údajov vyšších vrstiev
  - pomocou
    - riadenia prístupu
    - izolácie procesov navzájom
    - izolácie procesov od prístupu k hardvéru
  - kryptografická ochrana údajov na diskoch

Bezpečnostné funkcie vrstiev

- hardvér
  - podpora pre OS, aby mohol zabezpečiť izoláciu
  - riadenie prístupu do pamäte
    - umožňuje OS určiť, ku ktorým častiam pamäte má konkrétny proces prístup
  - riadenie prístupu k zariadeniam
  - obmedzenie prístupu k *privilegovaným* inštrukciám
    - vyhradzuje inštrukcie s globálnym dopadom len pre OS

Bezpečnostné mechanizmy HW

- bezpečnostné okruhy
  - vnútorný – jadro OS
    - bez obmedzení
  - vonkajší – aplikácie
    - nemôžu používať privilegované inštrukcie
    - môžu pristupovať len k určeným častiam pamäte
    - nemajú prístup k zariadeniam



Bezpečnostné mechanizmy HW

- riadenie prístupu k pamäti
  - využitím bezpečnostných okruhov
  - stránkovaním
    - proces má prístup len k tým častiam pamäte, ktoré mu určuje tabuľka stránok
- riadenie prístupu k zariadeniam
  - využitím bezpečnostných okruhov (napr. od ring 1)
  - a/alebo špecifikáciou konkrétnych *portov* pre proces

Bezpečnostné funkcie okolia

- bezpečnosť sietí
  - umožňuje (čiastočne) izolovať útočníka od prístupu k službám OS, DB aj aplikačnej vrstvy
- fyzická ochrana
  - vyššie vrstvy neochránia proti fyzickým útokom
- organizačné opatrenia
  - nie všetko sa dá zabezpečiť technicky

Známe „zrady“

- zvonku prístupné zbernice
  - CardBus, ExpressCard na notebook-och
  - FireWire (IEEE 1394)
  - v oboch prípadoch môže útočník bez otvárania počítača získať prístup k zbernici a pomocou DMA napr. získať kópiu operačnej pamäte

Otázky?

Ďakujem za pozornosť.