DIDAKTICKÉ TECHNOLOGIE 2

Mgr. Petr Vybíral, Ph.D.

4.4.2020

Témata k distančnímu studiu

(odkazová prezentace)

- Informační společnost
- Operační systém a internet
- Sítě a internet
- Multimédia – zvuk a video
- Grafika – rastrová X vektorová
- Kryptografie a bezpečnost 1
- Kryptografie a bezpečnost 2
- Zásady tvorby prezentace PPT
- Prezentace jako učební pomůcka

Informační společnost

Informační společnost

- Význam sběru informací, jejich zpracování a distribuce
- Šíření informací je dnes oproti době před nástupem IT velmi snadné
- Cena šíření je nezávislá a zpravidla zanedbatelná vzhledem k hodnotě informace
- Pojem znalosti zpracovaného souboru informací, který v přináší v nové ekonomice přidanou hodnotu

Co to jsou informace?

Informace

- Něco co má pro nás informační hodnotu (na rozdíl od náhodného šumu)
- Něco co je ukládáno v podobně kódovaných dat
- Informace lze ukládat, vysílat, přijímat, komprimovat, šifrovat, kódovat
- Na počítačích jsou v dnešní době informace ukládány v podobě 0 a 1 – binárně, digitálně, …
- Velikost dat (ve kterých jsou informace) udáváme v bitech/Bytech (b, B) a jejich násobcích…
- Měříme velikost informací i rychlost jejich přenosu

Ekonomika a informační společnost

- Nárůst podílu služeb na celkové ekonomické produkci → významnost technologií zefektivňující kancelářskou práci
- Systémy pro zpracování pošty, textů, databází a informační systémy → **redukce počtu pracovníků**?
- Přesunem znalostí a informace do centra pozornosti vzniklo celé nové odvětví zabývající se jejich akumulací a zpracováním → **nárůst počtu pracovníků**!
- Snadnost a rychlost výměny informací, porovnávání nabídek, prodej, distribuce, komunikace, globální trh a ekonomika

e-Government

- Účast IT na demokratických volbách – infrastrukturní a mobilizační
- Elektronické volby – čipové občanské průkazy – zajištění bezpečnosti
- Náhrady vertikálního toku informací za horizontální – nová média pro komunikaci a šíření informací
- Digitální ověřování identity, elektronický podpis a uznávané elektronické značky (právnické osoby) (zákon č. 227/2000 Sb.)→zákon 297/2016 Sb. (zákon o službách vytvářejících důvěru pro elektronické transakce)

Duševní vlastnictví

- Majetek nehmotné povahy – výsledek tvůrčí činnosti lidí a jejich intelektu (díla literární, umělecká, vědecká, …)

Autorské právo

- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským, a o změně některých zákonů (AZ)
  - Několik novelizací:
    - 228/2014 Sb., 496/2012 Sb., 168/2008 Sb., 216/2006 Sb…
    - http://business.center.cz/business/pravo/zakony/autorsky/
- Co není upraveno v AZ, řeší obecné úpravy v občanském zákoníku (OZ)
- Mezinárodní smlouvy (nadřazené dle ústavy před zákony ČR)
- Právní předpisy Evropských společenství

Autorské dílo

- Dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam.
  - Zákon (§ 2) uvádí demonstrativní výčet, co je a není považováno za autorské dílo z hlediska zákona
- Předmětem ochrany je duševní vlastnictví - ne hmotná věc (např. DVD)

Licenční smlouva

- Je třeba k užití díla – souhlas autora
- Mimo volného využití díla pro osobní potřebu a tzv. zákonných licencí
- Zákonná opatření platí tehdy, není-li smluvními stranami sjednáno jinak

Volné užití

- **Pro osobní nekomerční potřebu fyzické osoby**
  - Využití v rámci jejího vlastního soukromí
  - (zahrnující rodinu a osoby blízké)
  - Podmínky blíže vymezeny v AZ § 30
  - Vztahuje se jen na díla zveřejněná
  - Není nadřazeno k právu autora na opatření technickými prostředky k ochraně práv
    - Nemůže dojít k prolomení ochrany (i pro zhotovení kopie pro vlastní potřebu) – DRM – Digital Rights Management
- Nevztahuje se na (§ 30):
  - **Počítačový program**, el. databázi, arch. stavbu, záznam z kina, …

Ale…

- V § 29 AZ existuje „bernský třístupňový test“ pro volné použití díla (splnění všech podmínek):
  - Jen ve zvláštních případech stanovených autorským zákonem
  - Užití není v rozporu s běžným užitím díla
  - Nejsou nepřiměřeně dotčeny oprávněné zájmy autora

- Výklad bodů je poměrně sporný!
  - Soudy v ČR rozhodly u trestní odpovědnosti, že uživatel nemusí zkoumat zdroj odkud film pochází (tj. jak se na internet dostal) -> lze stahovat i z nelegálního zdroje?

- Konečný výrok má případný soud!
- Žalobce musí prokazovat!

Bezúplatné zákonné licence

- Neporušení AZ v případě specifických užití definovaných zákonem v § 30 a dále..
  - Rozmnožování na papír
  - Předvedení či oprava přístroje zákazníkovi
  - **Citace – „odůvodněná míra“, vyučování, vědecký výzkum, … (nutnost uvedení autora)**
  - Propagace výstavy uměleckých děl
  - Užití díla umístěného na veřejném prostranství
  - Úřední a zpravodajská licence
  - Občanské, náboženské obřady, úřední akce, školní představení, …
  - Dílo souborné
  - Knihovní licence
  - Licence pro zdravotně postižené
  - Dočasné rozmnoženiny
  - Fotografická podobizna
  - … a dále

Porušování autorského práva

- Jakýkoliv neoprávněný zásah do autorských práv nebo vědomé jednání toto umožňující
- Využití pojmu „pirátství“
  - Vznik z rozhlasového vysílání z lodí kotvících v mezinárodních vodách (rádio Merkur – 1958 – vysílání hudební autorská díla z lodí kotvících v mezinárodních vodách, aby se tak vyhnuly povinnostem vyplývajícím z právních předpisů dané země).
  - Filmové, hudební, softwarové, …
- Vypalování, kopírování, internetové pirátství

Internetové pirátství

- Zisk většinou jen provozovatelé pirátských serverů (reklama)

- Peer-to-peer sítě (BitTorrent)
- Upload – download služby (filehosting, např. uloz.to)
- Soukromé ftp servery
- Streaming online
- Linky na nelegální obsah
  - Rozlišení aktivních a neaktivních a embedded
  - „Spoluodpovědnost“ za škodu
- Prodej na nosičích, …

Upload a sdílení na internetu

- Protiprávní bez souhlasu autora díla (veřejně přístupné)
- Zveřejňování odkazů také protiprávní
- P2P (peer to peer) sdílení je také protiprávní
  - BitTorrent (a podobné) sítě, nezávislé servery s „trackery“ (piratebay, isohunt, …). .torrent soubory stažené do klienta (např. uTorrent a umožňující přímé stahování a sdílení s dalšími uživateli.
  - Jsou využívány i k legálnímu šíření (GNU software, apod.)

Download z internetu

- Není nutně protiprávní – vztahuje se na něj volné využití pro osobní potřebu a bezúplatné zákonné licence
- Záleží tedy na konkrétním využití

Počítačové programy - software

- Legální je takové využívání, které je v souladu s licencí programu

- Komerční licence – individuální pro konkrétní firmu/produkt
  - EULA – End User Licence Agreement
- Distribuce
  - Freeware
  - Demo, Shareware, trial verze, …
  - Open source licence a licence pro svobodný software
    - GNU GPL (General Public Licence)

Protipirátská legislativní opatření - návrhy

- HADOPI (Fr.) – „Zákon na ochranu tvůrčí práce na internetu" třikrát a dost
- ACTA – „Obchodní dohoda proti padělatelství"
- Zatčení „Kim Dotcoma" – Megaupload (byl obviněn za způsobení škody ve výši 500 miliónů dolarů zábavnímu průmyslu kvůli souborům nahrávaným na jeho stránky Megaupload, které měly přes 150 milionů registrovaných uživatelů).

Ochrana osobních údajů

- informace, které lze využít k úplné, či částečné identifikaci, kontaktování nebo lokaci fyzické osoby – citlivost
- jméno, bydliště, čísla kreditních karet a dokladů, data narození a dalších je dnes nutné uvažovat i o emailu, IP adrese, historii webové aktivity, záznamu polohy mobilního telefonu a jiných technologických údajích
- Získané osobní údaje lze v dnešní technologické realitě buď přímo zpeněžit (např. cílená reklama, prodej emailových adres), či využít k vyvíjení nátlaku.

Sociální média a sítě

- Dynamický web (web 2.0) – tvorba obsahu uživateli
- Blogy, fóra, diskuze, chaty, mikroblogy, komunitní weby, sociální sítě, ….
- navazování a udržování kontaktů a vytváření prostoru k vyjádření a vytváření konverzací
- Problémy s kontrolou obsahu – rasová nesnášenlivost, pornografie, kyberšikana, falešná identita → moderování, cenzura, …
- Ztráta kontroly nad informacemi online → zneužití

Vyhledávání informací

- Klíčová dovednost → mnoho nástrojů
  - Odborné databáze – licencovaný, omezený obsah, úzce zaměřené, neviditelné z fulltextového vyhledavače…
    - http://ezdroje.muni.cz/prehled/abecedne.php
    - http://www.ped.muni.cz/wlib/neweb/index.php?sekce=3
  - Automatické vyhledavače – většinou fulltextové
    - Google – PageRank
    - Složení ze 3 částí:
      - automatického robota (software) procházejícího webový obsah (cestuje po odkazech),
      - indexování (extrakce klíčových slov, nadpisů, ...) a
      - vyhledávání (nalezení nejvíce relevantní stránky vůči zadanému dotazu)
- vyhledávače snaží na základě dalších informacích o uživateli (geologické polohy, historie vyhledávání, rozkliknutých výsledků atp.) vybírat co nejvhodnější sadu výsledků tak, aby uživatel dostal odpověď na svůj dotaz.
  - https://history.google.com/history/
  - RIZIKA?

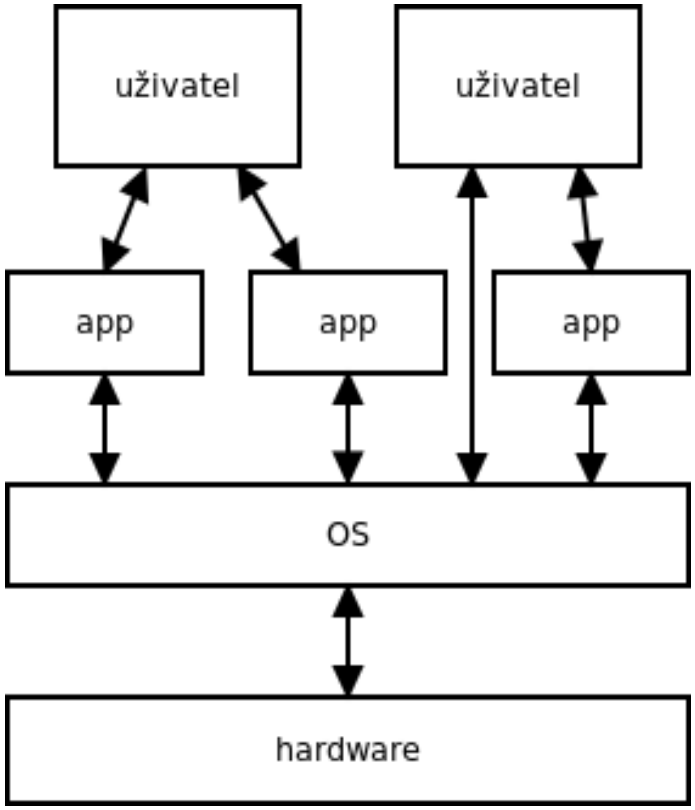
Data vs. služby

- Množství **cloudových** služeb je v dnešní době nabízeno pro osobní využití zdarma. Ačkoliv uživatel neplatí přímo penězi, provoz služeb není levný a poskytovatel této služby musí přijít se způsobem monetarizace. Kromě variant prémiových předplatných (např. více funkcí) a placených variant pro firemní a korporátní uživatele získávají poskytovatelé kontrolu nad uživatelskými daty. Je často velmi těžké službu opustit a přejít ke konkurenci, málokterý poskytovatel umožňuje přenést snadno uživatelská data jinam. Je třeba mít na paměti, že libovolná služba může být kompromitována a útočník může získat přístup k uloženým datům. Je tedy například třeba uvažovat, jaké dokumenty uchovávat v online dostupné emailové schránce, nebo na cloudových úložištích (např. Dropbox).

Operační systémy a počítačové sítě

OS – operační systém

- Základní programové vybavení počítače
- Poskytuje:
  - Správu paměti
  - Správu procesů
  - Správu hw a periferií
  - Správu souborů
  - Správu uživatelů a oprávnění
  - UI
  - …

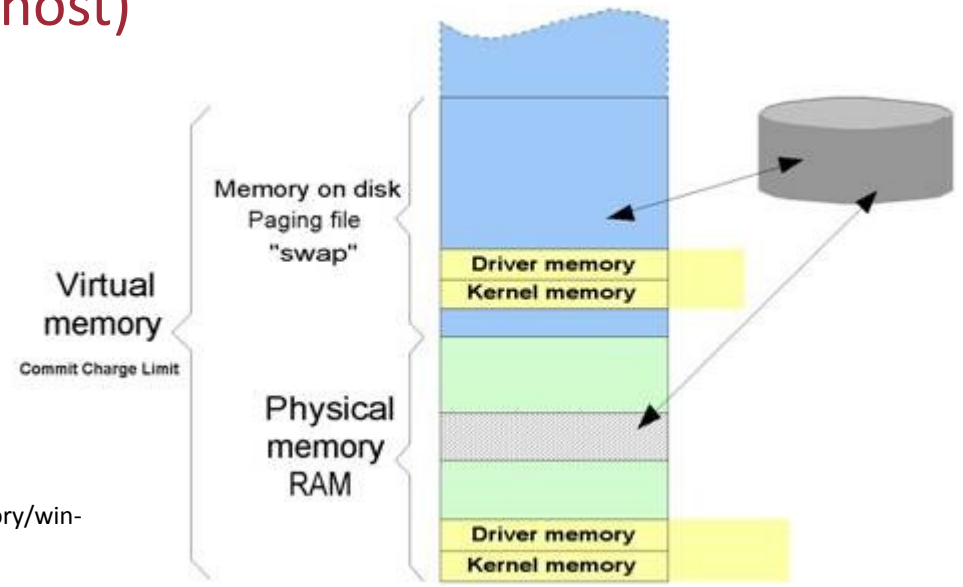


Proces

- Je realizace programu (průchod sledem instrukcí)
- Při spuštění je uložen v OP
- OS vytváří při spuštění programu proces a procesy spravuje (task manager)
- OS přepíná procesy a realizuje tak spuštění více programů „současně“ - **multitasking**

Paměť

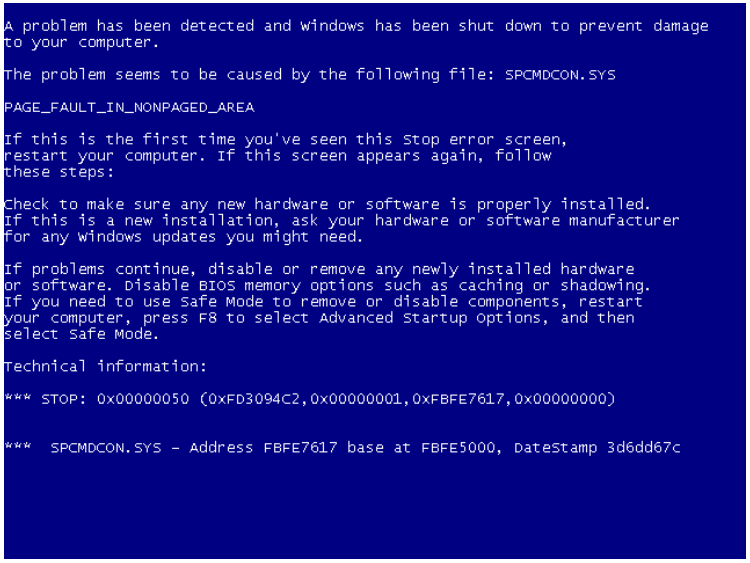
- OS realizuje přidělování fyzické OP (RAM)
- Přímou fyzickou paměť OS mapuje na logickou – **virtuální** paměť a tu přiděluje procesům
  - Souvislé bloky pro procesy a fragmentace do fyzické
  - Více virtuální než je fyzické s využitím odkládání na pevný disk
  - Oddělení paměťového prostoru mezi procesy (jednoduchost a bezpečnost)



http://pctuning.tyden.cz/ilustrace3/zombux/vista_memory/win-memory.jpg

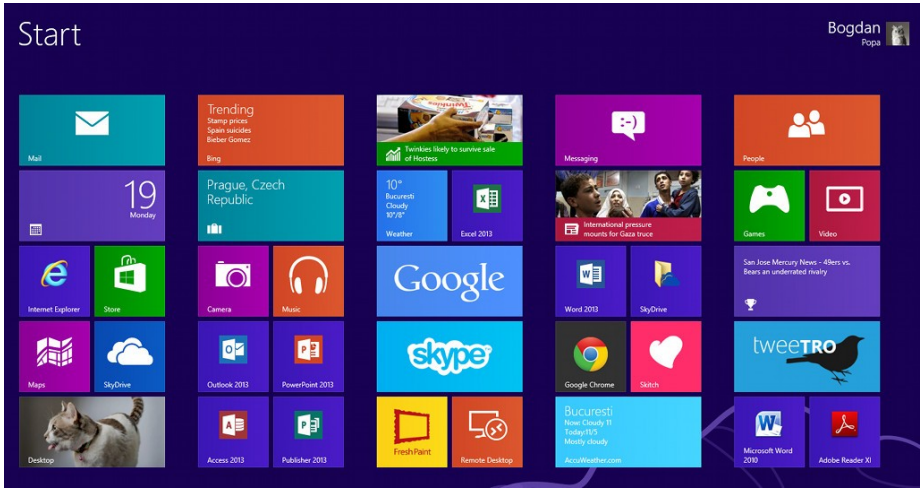
Periferie

- Z pohledu OS vše mimo hlavní komponenty (P, OP, MB)
- OS komunikuje prostřednictvím ovladačů a pracuje s periferiemi
- Vyřizuje žádosti od periferií a od aplikací – řadí požadavky
- BSOD



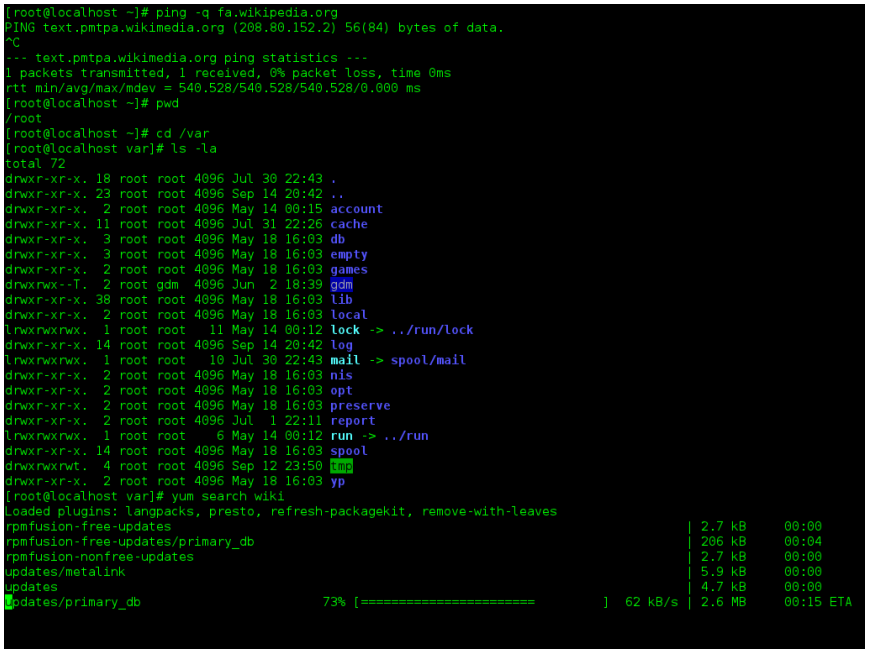
Uživatelské rozhraní

GUI – grafické uživatelské rozhraní



http://i1-news.softpedia-static.com/images/news2/Windows-8-Is-a-Monster-that-Terrorizes-Workers-Design-Expert-2.jpg?1353335086

CLI – příkazový řádek



http://upload.wikimedia.org/wikipedia/commons/2/29/Linux_command-line._Bash._GNOME_Terminal._screenshot.png

Systém souborů – File system

- Soubor = abstrakce dat + metadat
- FS řeší primárně organizaci souborů (složky, ..) a jejich fyzické ukládání
- Cesta k souboru: C:\WINDOWS\...
- Běžné FS:
  - FAT – starý, jednoduchý, limity velikosti souboru 4 GB, další limity a nezabezpečení
  - NTFS – novější windows fs, větší limity, řízení přístupu k souborům – práva, žurnálování, podpora EFS
  - Ext4 – linuxový FS (linux podporuje celou řadu FS)

Pozn: disk management a formátování disku

Uživatelé a bezpečnost

- OS zajišťuje správu uživatelů a jejich práva (skupiny uživatelů)
- OS s FS zajišťuje přístup k souborům a složkám
- Víceuživatelský OS

Správa aplikací a aktualizace

- Instalace aplikací a jejich správa v OS
- Centralizovaná distribuce (jedno místo ze kterého se instaluje a kterou spravuje výrobce OS) – Android, iOS, …
- Decentralizovaná (běžně windows) – problémy

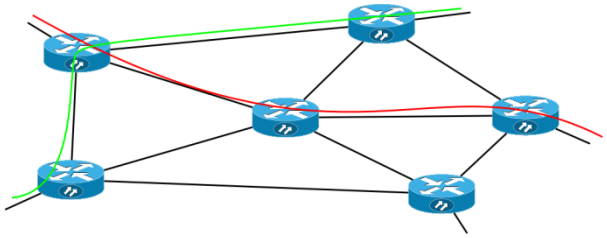
- Aktualizace OS
- Aktualizace software

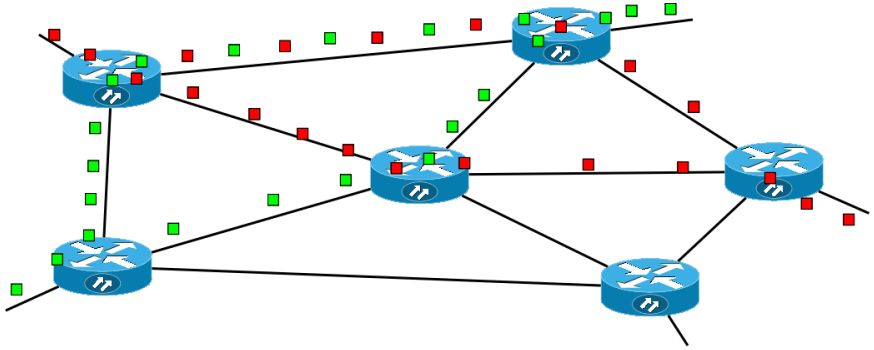
Počítačové sítě a internet

Spojované a nespojované sítě

- Běžné datové sítě (ethernet, internet tcp/ip) jsou **nespojované** – není vytvořeno spojení
- Data jsou rozdělena na malé části (pakety)

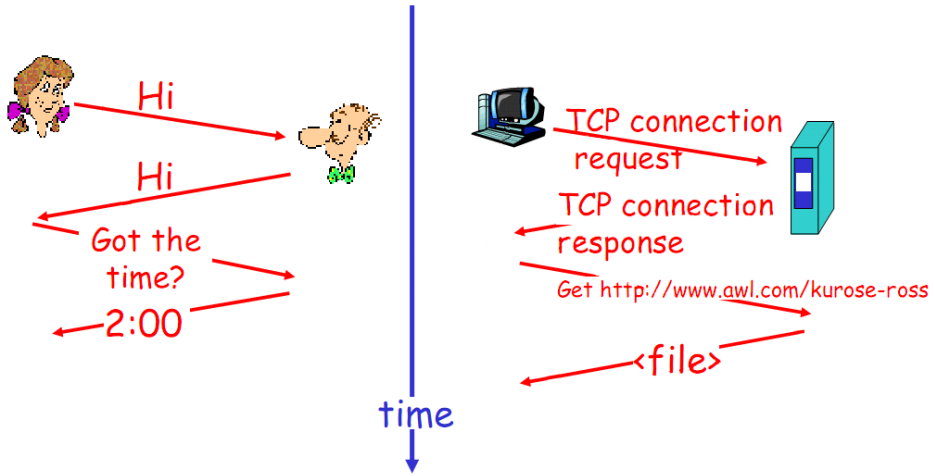
- Lepší využití dostupné přenosové kapacity
- Lepší odolnost vůči výpadkům
- Horší garance přenosové kapacity
- Složitější řízení toku dat (směrování)





Komunikační protokoly

- Definují způsob a pravidla komunikace dvou uzlů v síti
  - kdo, kdy, jak, s kým, jakým jazykem, v jakém pořadí, jak zabezpečeno, jak se kontrolují chyby, …
- Běžné aplikační protokoly:
  - HTTP, HTTPS, FTP, POP3, SMTP, IMAP, …



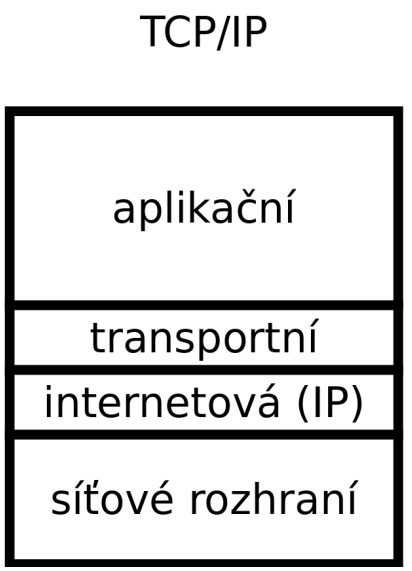
LAN – lokální sítě, WAN – rozlehlé sítě

- Geograficky blízké uzly
- Počítače, přenosová média a propojovací prvky (switch, bridge, hub, router)
- Různé topologie (způsoby zapojení) – hvězda, kruh, sběrnice, …
- Různé technologie – nejběžněji **Ethernet** a jeho varianty

- WAN – rozlehlé sítě, **Internet** – propojení lokálních sítí, Internet využívá TCP/IP protokolů

TCP/IP

- Model komunikace – 4 vrstvy podle abstrakce
- Každá vrstva samostatná činnost a zajištění návaznosti na další vrstvy – jednodušší implementace
- Transmission control protocol / Internet protocol
- Vrstvy:
  - Aplikační (aplikace a aplikační protokoly)
  - Transportní (porty, spojovaný a spolehlivý přenos) – TCP
  - Internetová – IP – IP adresace uzlů, tvorba paketů
  - Síťové rozhraní – adresace lokálních sítí, fyzické prostředky sítí



IP adresace

- Každý uzel v TCP/IP má svoji adresu
- IPv4 – 32b adresa (např. 192.168.1.0)
- Zleva hierarchická
- Vyhrazené adresy pro privátní sítě (192.168.x.x, 172.16.x.x – 172.31.255.255, 10.x.x.x)

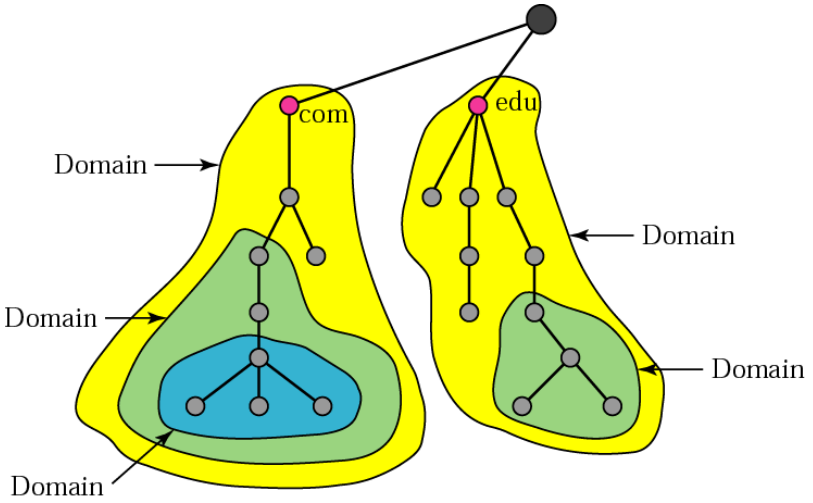
- Přechod na IPv6 – 128b – více adres
  - 2^{32} -> 2^{128}

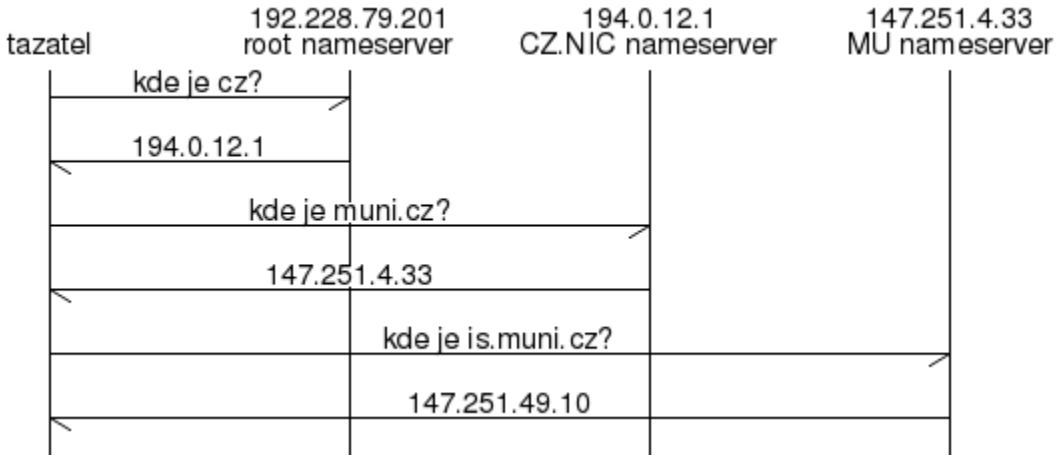
Internet

- Vznik v 60. letech z ARPANET – decentralizovaný a distribuovaný systém
- Data jsou přenášení mezi propojenými lokálními sítěmi poskytovateli připojení a směrovány (router) od odesílatele k příjemci na základě IP adres

Domény - DNS

- Jmenná služba adres – převod mezi IP a doménovou adresou (DNS)
- Hierarchický prostor adres
  - Např.: wrack.ped.muni.cz
- Převoditelnosti (DNS servery)
  - Muni.cz -> 147.251.5.231





Registrace domén – registrátoři – správa: www.nic.cz

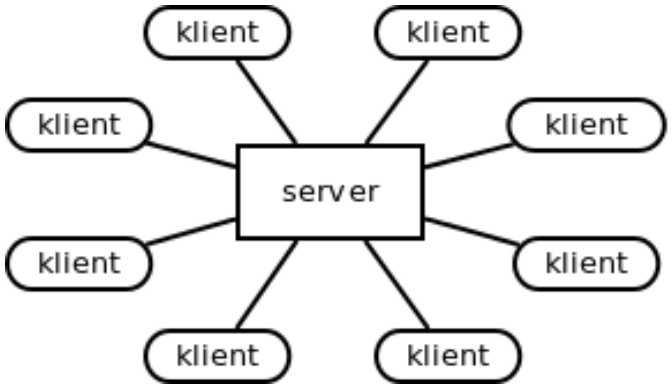
Pozn. webhosting

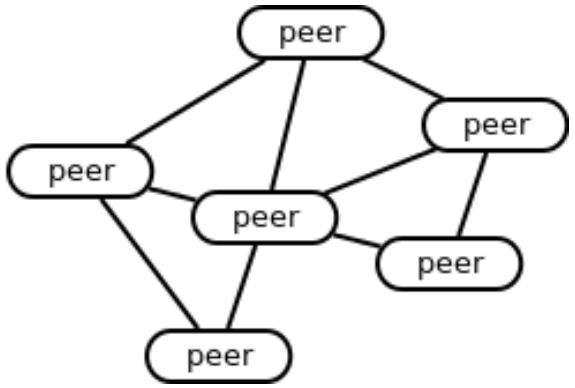
Služby internetu I

- **www** – world wide web (http, https, 90. léta), HTML jazyk
- **Email** – základní služba internetu, SMTP protokol, 70.léta, webmail, MIME rozšíření
- **Ebanking** – vícestupňové zabezpečení, https. (+ další zprostředkovatelské služby – např. PayPal)
- **Cloud** – služby online, přístup k datům i aplikacím odkudkoliv. Např. webmail, ms office 365, …
- **Hlas** – nutnost zajištění malého zpoždění a kolísání rychlosti – problém nespojované sítě, QoS pro upřednostňování hlasových dat, VoIP, Skype, …

Služby internetu II

- **FTP** – přenos souborů, nezabezpečený, ftps
- **Peer to peer –** decentralizované služby (klasické služby jsou *klient-server*). Distribuovaná data, absence centrálního serveru, např. torrent, skype, …





Konfigurace

- **WIFI** - Nutnost lepšího zabezpečení oproti LAN na kabeláži – skrýt SSID, MAC filtry, šifrování, WEP, WPA, WPA2
- **DHCP –** dynamické přidělování IP serverem, snazší správa IP
- **VPN** – virtuální privátní sítě - http://vpn.muni.cz
- **Eduroam** - http://eduroam.muni.cz
- **Firewall** – sw (hw) prvek zajišťující inspekci spojení, paketový filtr, IDS, …

Sítě a internet

Počítačová síť

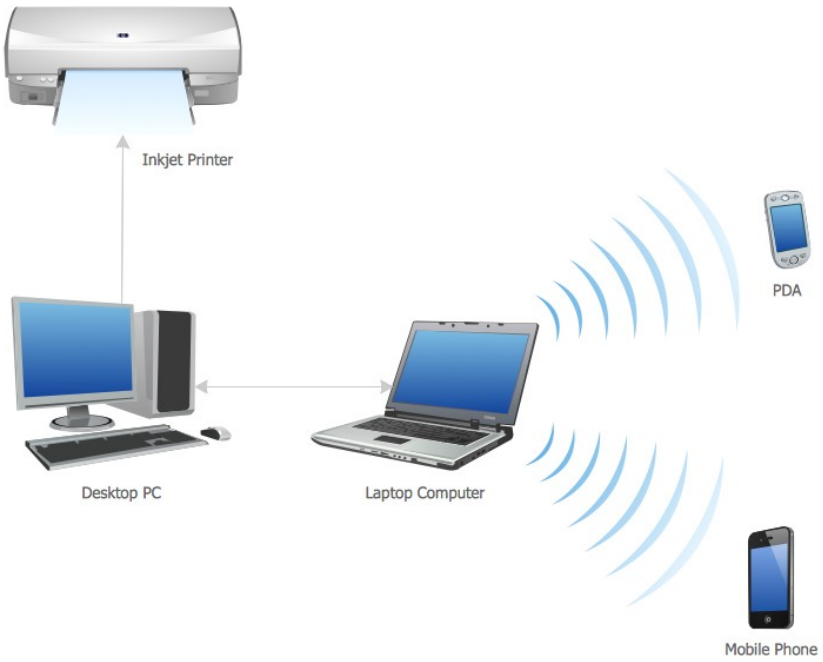
„Počítačová síť je vzájemné propojení dvou a více počítačů“

Počítačová síť

- Síť je založena na splnění 2 základních podmínek:
- 1) síťový hardware - umožňuje fyzické propojení počítačů:
  - kabeláž, síťová karta, aktivní síťové prvky (switche, routery…)
- 2) síťový software - postará se o vlastní přesuny dat od navázání spojení přes zabezpečení, kontrolu apod. Jedná se o ovladače, firmware, ovládací SW, aplikace apod.

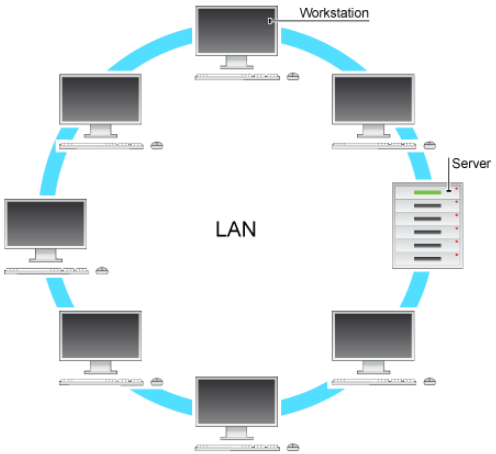
Dělení počítačových sítí

- PAN - Personal Area Network
  - Osobní síť
  - Velice malá, několik metrů okolo jednotlivce
  - Příklad: propojení mobilu s notebookem přes bluetooth



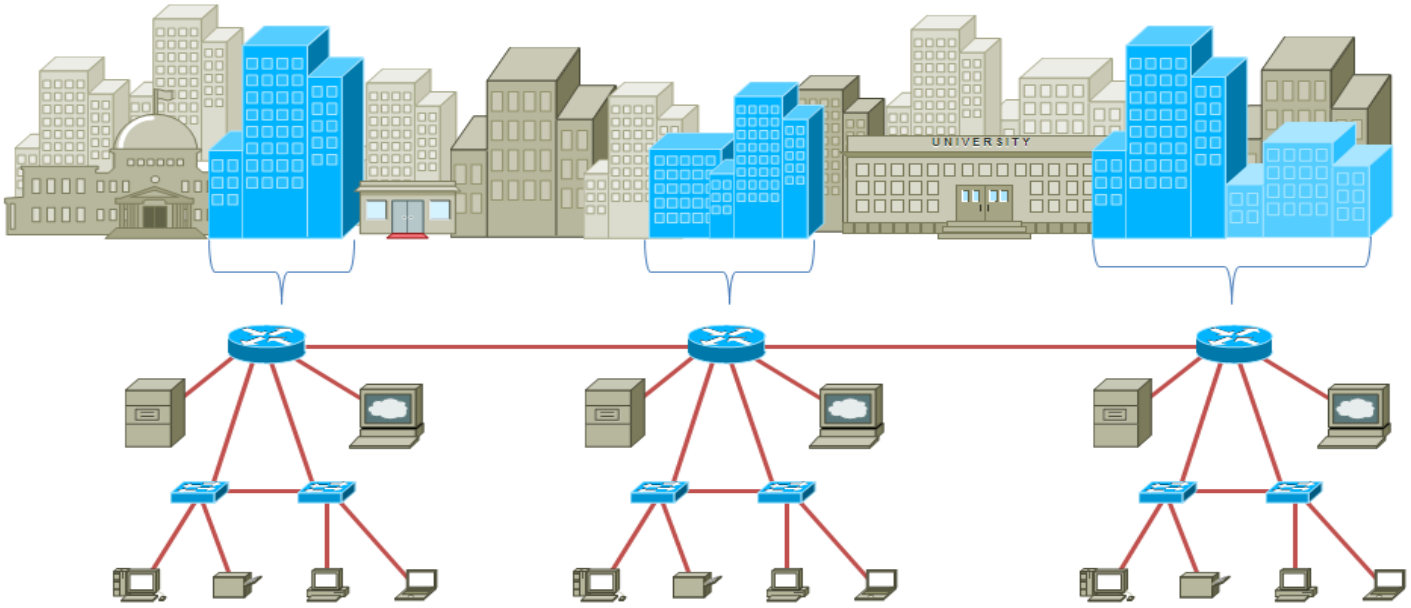
Dělení počítačových sítí

- LAN – Local Area Network
  - Menší síť propojující zařízení (PC, tiskárny…) v jedné domácnosti, budově, nebo několika přilehlých budovách.
  - Do několik stovek metrů maximálně, nejčastěji se však setkáváme s malými LAN sítěmi v domácnostech
  - Nejčastěji propojeny přes routery a switche



Dělení počítačových sítí

- MAN – Metropolitian Area Network
  - Velká síť na úrovni města
  - Síť propojující lokální sítě v městské zástavbě, spojuje vzdálenosti řádově jednotek až desítek kilometrů



Dělení počítačových sítí

- WAN – Wide Area Network
  - Velké sítě, spojujích mnoho LAN sítí do jednoho celku
  - Sítě zahrnující několik kontinentů, celosvětové sítě
  - Nejvýznačnější WAN síť - INTERNET

Přenos dat v síti

- Data se v síti přenáší za využití:
  - Paketů
  - Nespojované komunikace
  - Síťových protokolů (TCP/IP)
  - IP adresace

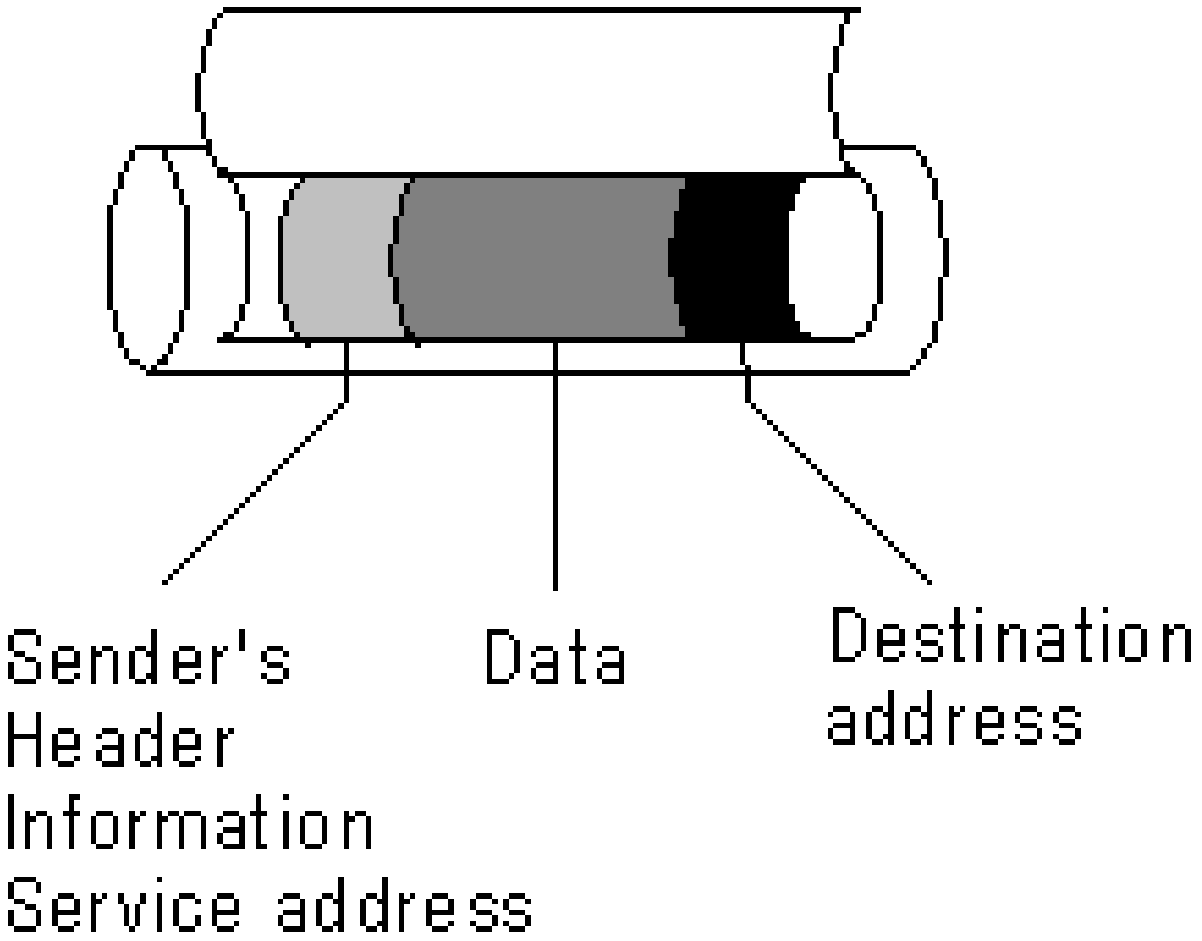
Paket

- základní přenosová jednotka (alespoň v sítích TCP/IP). Skládá se z dat a metadat.

- Obsahuje záhlaví informace k přenosu a případně zápatí.

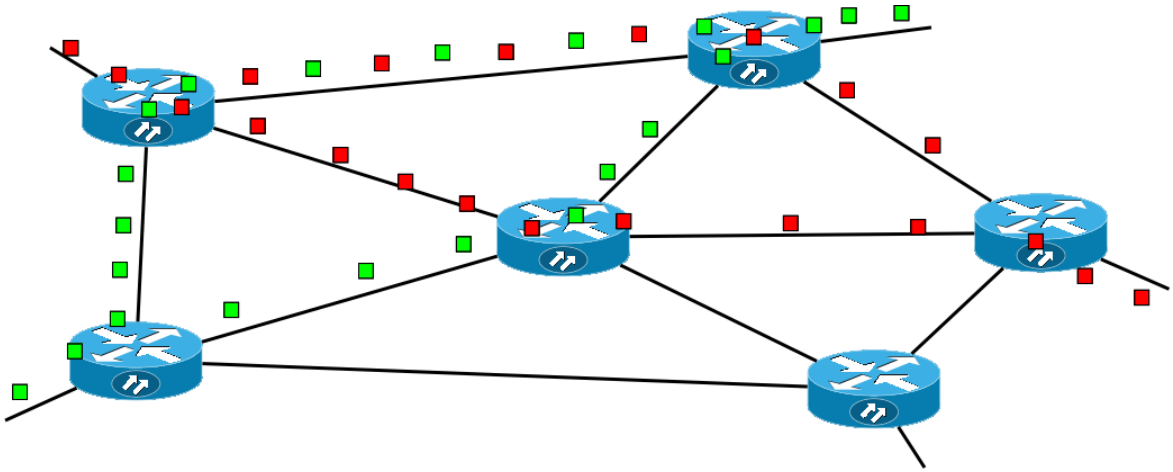
- ***Metadata** - jsou strukturovaná data o datech. Příkladem je katalogizační lístek v knihovně, obsahující data o původu a umístění knihy: jsou to data o datech v knize, uložená na katalogizačním lístku.

Packet

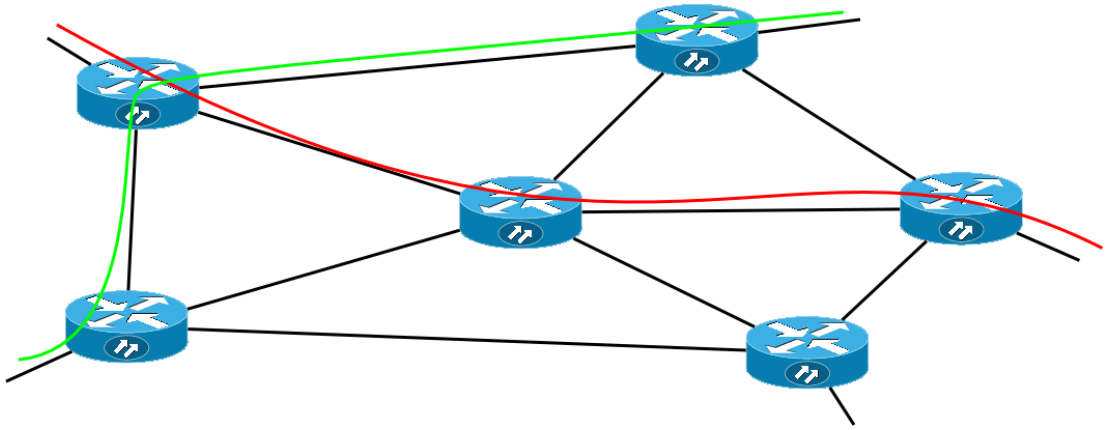

Sender's
Header
Information
Service address
Data
Destination
address

Nespojovaná komunikace

- Komunikaci mezi dvěma entitami není vytvářený rezervovaný okruh (spoj), ale data jsou rozdělena na malé části — tzv. pakety,
- Pakety jsou přenášené sítí nezávisle na sobě
- Takovýto transport dat je také odolnější vůči výpadkům, v případě poškození, či přetížení jedné cesty lze dynamicky přesměrovat pakety jinudy aniž by se narušila vlastní komunikace.
- Nevýhodou je komplikovanější řízení provozu takovéto sítě — je nutné řešit směrování **každého paketu v síti k jeho cíli**.



Nespojovaná komunikace



Spojovaná komunikace

Komunikační protokoly

- Přesně definují způsob, jakým probíhá komunikace realizující konkrétní funkci a to na všech úrovních.

- Máme protokoly pro zasílání dat, navazování zabezpečených kanálů, vyhledání síťové adresy odpovídající doménovému jménu, doručení emailu atd.
- Protokol je známý oběma komunikujícím stranám a popisuje přesně *jaký obsah, v jakém pořadí a s jakým časováním* je předáván. Odklon od takto strukturované komunikace je možné interpretovat jako chybu.

TCP/IP

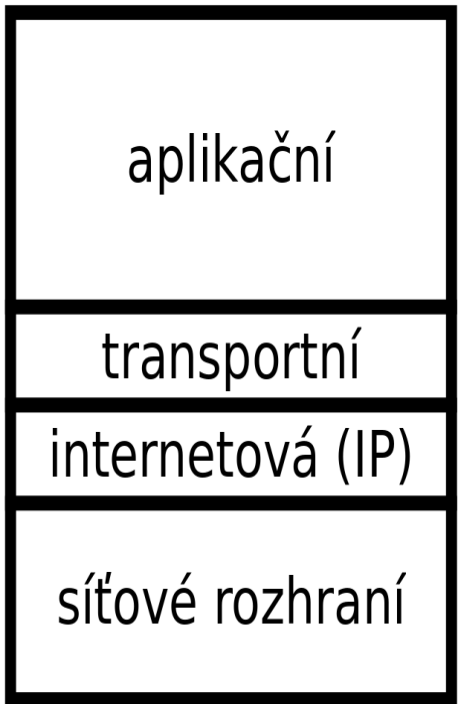
- Základním principem prostupujícím architekturu počítačových sítí je rozdělení komunikace do vrstev podle abstrakce. Každá vrstva je zodpovědná za popis přenosu od úrovně aplikace až po komunikaci po fyzických spojích. Síťový model TCP/IP je základním kamenem všech dnešních sítí a i celého internetu a je pojmenován podle dvou hlavních protokolů zajišťujících směrování a transport dat mezi uzly.

TCP/IP

- Rodina protokolů TCP/IP předpokládá existenci čtyř vrstev:
  - - aplikační vrstvy
  - - transportní vrstvy
  - - síťové vrstvy
  - - vrstvy síťového rozraní

TCP/IP

Vrstvy:



- **Aplikační** - zahrnuje protokoly síťových aplikací: elektronické pošty, HTTP, www, ftp…
- **Transportní** - tato vrstva zajistí spolehlivost a celistvost dat
- **Síťová (internetová, IP vrstva)** - Protokol IP popisuje adresaci uzlů, rozklad dat na pakety a jejich směrování uvnitř sítě.
- **Síťové rozhraní** – zajišťuje komunikaci po fyzickém médiu (kabelu) a přenos dat mezi dvěma přímo spojenými stanicemi

Jak to začalo jak to funguje…

- https://www.youtube.com/watch?v=vDrUUqHsy0k

IP adresace

- **IP adresa určuje jednoznačně počítač v síti**

- Adresa je zleva hierarchická, to znamená, že adresné prostory jsou přidělovány fixací čísel od leva: například Masarykova Univerzita má k dispozici rozsah
  147.251.0.0 - 147.251.255.255.
- Některé adresní rozsahy jsou vyhrazené speciálním účelům, například pro privátní podsítě, které nejsou adresovatelné zvenčí jsou vyhrazené následující rozsahy:

- Vzhledem k rostoucímu počtu připojených zařízení došlo v roce 2011 k vyčerpání adresného prostoru 32 bitů. Z toho důvodu je zaváděn nástupný protokol IPv6, který k adresaci využívá 128 bitů a zapisuje se v hexadecimálních oktetech, například adresa 2001:4860:b002::68 odpovídá testovací adrese ipv6.google.com.

IP adresy vs. domény

- IP adresy používané pro adresaci strojů v síti nejsou vhodné pro koncové uživatele — špatně se pamatují, lze je snadno zaměnit a mohou se měnit. Proto se používá jmenná služba, která popisuje stroje pomocí textových jmen rozdělených do domén.

IP vs. domény

.cz	=	1. řád (koncovka)
example.cz	=	2. řád
blog.example.cz	=	3. řád (subdoména)
www.blog.example.cz	=	4. řád

- Domény nejvíce vpravo označujeme jako domény nejvyššího řádu: jedná se o národní domény a obecné domény jako .net, .com, .org a další. Jejich registrace a delegace správy spadá pod mezinárodní organizaci ICANN.

- Například českou doménu .cz spravuje sdružení CZ.NIC (nic.cz), které mimo jiné prostřednictvím tzv. registrátorů registruje domény nižšího řádu — například muni.cz. Vlastník určité domény může libovolně vytvářet a spravovat domény nižších řádů, v kompetenci MU je tedy správa domén jako is.muni.cz, phil.muni.cz…

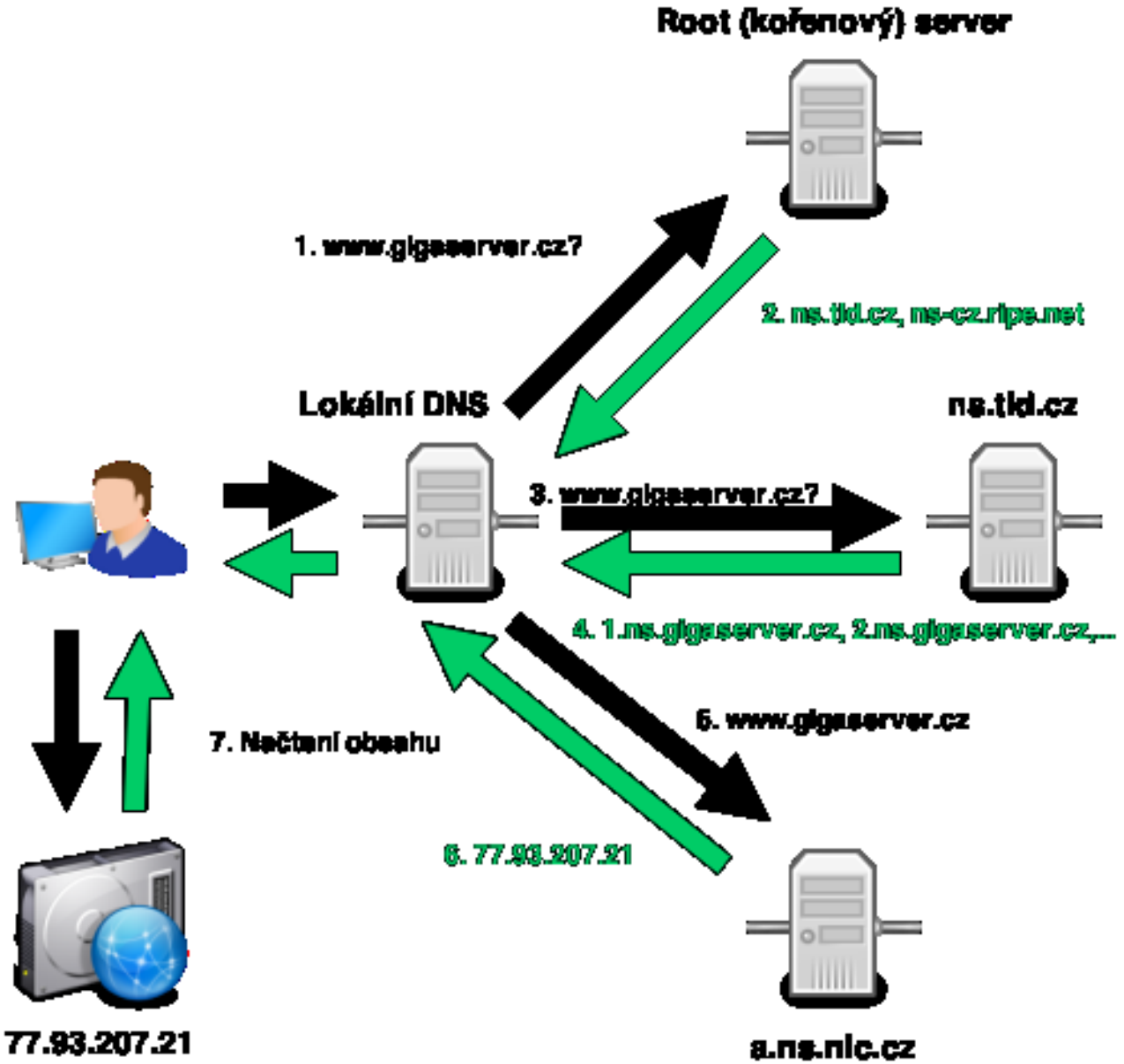
IP vs. domény

- Pro překlad z doménových jmen na IP adresy se používá Domain Name System (DNS). Například:

- muni.cz. -> 147.251.5.231 Tento protokol postupuje od domény nejvyššího řádu a dotazuje se příslušných DNS serverů na adresy zodpovědné za domény nižšího řádu tak dlouho, než dostane informaci o stroji, na který směřuje doména nejnižšího řádu přítomná v názvu.

Jak domény fungují ?

- 1. Uživatel zadá název domény do prohlížeče a lokální DNS server se obrátí na některý kořenový server a zeptá jestli nezná IP adresu domény www.gigaserver.cz.
- 2. Kořenový DNS server nezná IP adresy konkrétních domén, ale ví na kterých serverech se nachází záznamy .CZ domény a pošle lokálnímu DNS seznam těchto serverů.
- 3. Lokální DNS se tak obrátí na servery, které záznamy o .CZ doménách obsahují (ns.tld.cz, ns-cz.ripe.net,…).
- 4. Tyto servery však stále konkrétní IP adresu neznají, ale mají informace o všech .CZ doménách II. řádu a tak lokálnímu DNS odpoví názvy serverů, které informaci o IP adrese budou mít.
- 5. Lokální DNS se tak obrátí na tyto servery (1.ns.gigaserver.cz, 2.ns.gigaserver.cz, 3.ns.gigaserver.cz, 4.ns.gigaserver.cz).
- 6. DNS server konktrení IP adresu požadované domény zná, je to 77.93.207.21 a pošle ji zpět lokálnímu DNS.
- 7. Lokální DNS pak předá IP adresu počítači uživatele, ten se spojí s daným server a zobrazí obsah požadované domény.



- Zdroj: https://kb.gigaserver.cz/co-je-to-ip-adresa-jak-funguje-dns/

Služby sítě internet

- Hlavní služby poskytované sítí internet:
  - WWW
  - E-mail
  - E-banking
  - Cloudové služby
  - VoIP (hlasové služby)
  - FTP
  - Peer-to-peer (P2P)

WWW (Word Wide We

- Multimediální obsah, poskytovaný uživatelům pomocí protokolu HTTP -> primárně webové stránky
- Uživatelé tento obsah konzumují pomocí webových prohlížečů a v podstatě se stal synonymem pro internet jako takový.

E-mail

- Již od raných dob internetu je k dispozici zasílání textových zpráv mezi jednotlivými uživateli, dodnes je zajišťován pomocí protokolu SMTP, který byl vyvinut v 70. letech.

- Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy)

- Alternativou ke stahování pošty je využití některého z webmailů, což jsou v podstatě webové aplikace umožňující vzdálenou manipulaci s emailovou schránkou. Služba jako taková negarantuje pravdivost údajů o odesílateli, ani žádné další bezpečnostní prvky (šifrování), ty je nutné zajistit použitím příslušného software na obou komunikujících stranách.

E-banking

- Internetové bankovnictví umožňuje provádět pomocí síťové infrastruktury finanční transakce. Jedná se v jádru o zprostředkování zabezpečené komunikace mezi uživatelem a jeho bankou, při které je ověřena uživatelova identita a přijat příkaz k provedení dané operace.

- K zajištění dostatečného zabezpečení se kromě obvyklého https spojení a uživatelského jména a hesla užívá i tzv. vícestupňového ověření — např zaslání potvrzujícího kódu pomocí SMS. Zvyšuje se tak obtížnost zneužití ukradených přístupových údajů případným útočníkem. Pro usnadnění mezinárodních transakcí a zvýšení důvěry na straně prodejců i nakupujících vznikly tzv. zprostředkovatelské služby — jako například PayPal — tyto zjednodušují provádění online transakcí a zvyšují jejich bezpečnost (obchodník například nepřijde do styku s číslem platební karty zákazníka a pod.).

Cloud

- Poskytování služeb či programů uložených na serverech na Internetu s tím, že uživatelé k nim mohou přistupovat například pomocí webového prohlížeče a používat je prakticky odkudkoliv.

- Uživatelé neplatí (za předpokladu, že je služba placená) za vlastní software, ale za jeho užití. Nabídka aplikací se pohybuje od kancelářských aplikací, přes systémy pro distribuované výpočty, až po operační systémy provozované v prohlížečích, jako je například eyeOS či iCloud.

- Příklady: Google docs, dropbox, google drive…

Cloud

VoIP (hlasové služby)

- technologie, umožňující přenos digitalizovaného hlasu v těle paketů rodiny protokolů TCP/IP prostřednictvím počítačové sítě
- Využívá se pro telefonování prostřednictvím Internetu nebo intranetu
- Nutnou podmínkou pro srozumitelné a spolehlivé VoIP telefonní spojení je zajištění tzv. kvality služby, zkráceně označované QoS.

- **QoS** - nastavení aktivních prvků (např. routeru) sítě tak, aby upřednostňovaly hlasová data před ostatním provozem. Na většině domácích routerů lze nastavit prioritu hlasového (nebo videokonferenčního) datového toku tak, aby ostatní uživatelé sdílející tutéž linku nemohli nezahltit její kapacitu například stahováním objemných dat.

- **Příklady:** Skype, Google hangouts

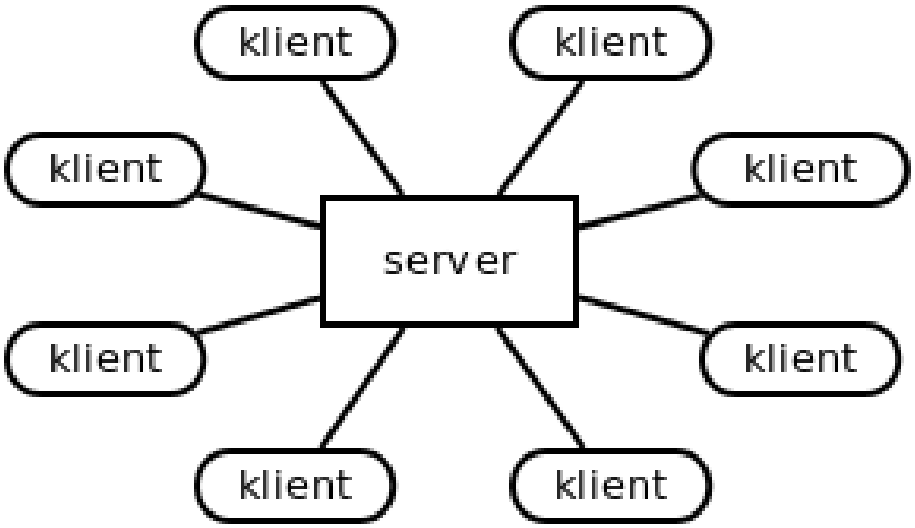
FTP- File Transfer Protocol

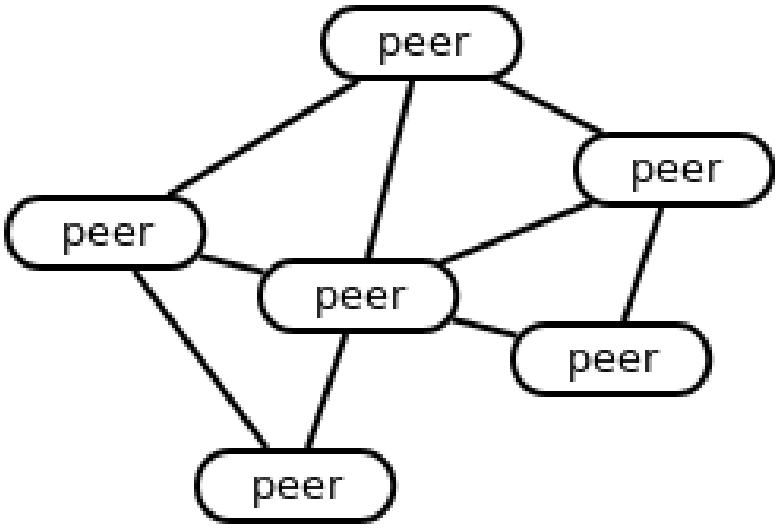
- Klasický protokol pro přenos souborů po síti
- Umožňuje navázat spojení se vzdáleným počítačem, procházet danou adresářovou strukturu **(složky)** a přenášet soubory oběma směry.
- Zpravidla chráněn uživatelským jménem a heslem. Provoz po FTP není nijak šifrován, proto pokud je to možné je vhodné používat zabezpečenou variantu FTPS (obdoba HTTPS). V dnešní době se s tímto protokolem uživatel setká nejčastěji při přístupu na webhostingové diskové prostory, případně na vnitřní firemní sdílená datová úložiště.

- **Vhodné programy:** Total Commander, FileZilla….

Peer-to-peer (P2P)

- Většina služeb funguje na bázi **klient-server**





- U klient-server dochází k distribuci obsahu uloženého na serveru ke klientům, klienti navzájem si data nepředávají. => Velká zátěž na serveru, data pouze na něm
- Pokud server selže, žádný klient svá data neobdrží

P2P

- P2P odstraňují výsadní pozici serveru a jsou založené na decentralizované a distribuované architektuře.
- Každý peer je tak zároveň klientem i serverem: poskytuje služby ostatním peerům a zároveň využívá jejich služeb

P2P

- **Výhody:** rozložení zátěže mezi peery (oproti její koncentraci na straně serveru), zvýšené odolnosti vůči výpadku a dobrou škálovatelnost (lze libovolně navyšovat počet peerů, aniž by se přetížil centrální server).
- **Nevýhody:** náročné vystavění p2p sítě (složitější modely komunikace) a nepřehlednost správy takovéto sítě.
- **Příklady**: Skype, bitttorent

Konfigurace síťových služeb

- Vybrané konfigurační prvky:
  - Zabezpečená wifi
  - DHCP, statická IP
  - VPN
  - Eduroam
  - Firewall

Zabezpečená Wifi – viz přednáška o kryptografii

- Při konfiguraci bezdrátového připojení je nezbytné dbát na co největší míru zabezpečení.
- Bezdrátový přenos je možné odposlouchávat a následně zneužít.
- K šifrování nabízí většina přípojných bodů pro domácnosti dvojí volbu: **WEP a WPA**. WEP protokol je od roku 2004 považován za **zastaralý** a lze jej běžně dostupnými prostředky prolomit. WPA (a jeho novější varianta WPA2) používají pro silnější algoritmy s dynamicky měněným klíčem, což zamezuje získání klíče dlouhodobým odposlechem.

DHCP a statická IP

- Každé zařízení připojené do počítačové sítě musí mít přidělenu jednoznačnou IP adresu.
- **Je v podstatě dvojí možnost, jak adresy v síti rozdělovat:**

- 1) Staticky-zde je třeba o novou adresu požádat správce sítě a následně ji na příslušných místech v nastavení systému zadat.

- 2) DHCP - adresa je přidělována automaticky DHCP serverem přítomným v síti (např. v domácnostech součástí routeru) bez dalších zásahů uživatele. Takto přidělená adresa se navíc může měnit při každém připojení do sítě.

VPN – Virtuální privátní síť

- Slouží k vytvoření zabezpečeného propojení fyzicky vzdálených počítačů tak, jakoby byly propojeny lokální sítí.
- Umožňuje tak například vzdálené připojení do firemní sítě, nebo propojení vzdálených poboček do jedné sítě při zachování vysoké úrovně zabezpečení.
- V rámci univerzity je VPN také k dispozici a umožňuje například přístup do elektronických zdrojů (placené články…) tak jako by se stroj připojoval z univerzitní sítě (jako by byl třeba zde v učebně).
- Podrobné návody k navázání připojení jsou dostupné zde: http://vpn.muni.cz

Eduroam

- Eduroam je mezinárodní projekt umožňující studentům a zaměstnancům univerzit připojení do bezdrátových sítí všech zúčastněných institucí.

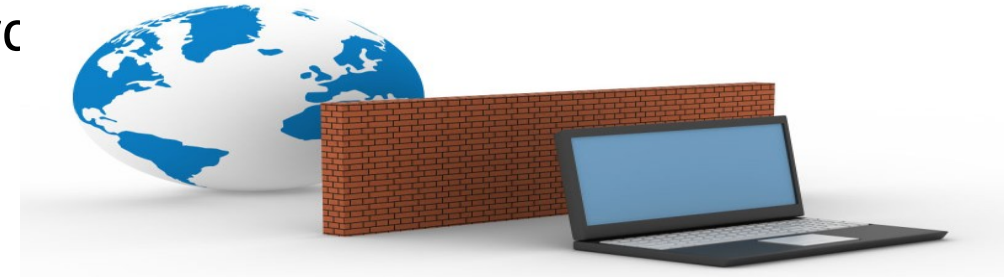
- Jedná se o příklad federativního autentizačního mechanizmu, kdy je uživateli umožněno se přihlašování do libovolné zapojené sítě prokazovat přihlašovacími údaji své domovské instituce (UČO, sekundární heslo).

- Tato služba velmi usnadňuje připojení nejen na Masarykově univerzitě (na všech fakultách stejné nastavení), ale především při návštěvách jiných institucí — zapojené jsou nejen univerzity, ale například i veřejné knihovny, instituty AV a další. Návody jsou opět k dispozici na http://eduroam.muni.cz

Firewall

- **Firewall** je virtuální nástroj oddělující provoz mezi sítí (internetem) a počítačem, tak že propouští jedním nebo druhým směrem informace podle předem definovaných pravidel. Brání tak zejména před neoprávněným vniknutím do sítě a odesílání dat bez vědomí a souhlasu uživatele či oprávněné osoby. Ve virtuálním prostředí domácností i firem je instalace brány firewall nejefektivnějším a nejdůležitějším krokem při ochraně a zabezpečení počítače.

- Firewall definuje pravidla, podle kterých může probíhat komunikace mezi počítači či sítěmi, resp. povolí se podmínky a služby, které jsou nutné pro provoz a ostatní jsou zakázány. Firewall nepřetržitě kontroluje dění v domácí či firemní síti a podrobně jej monitoruje. Informuje i o legálních procesech, vzniklých použitím některý
povolit či zablokovat.



Multimédia – zvuk a video

Multimédia

Souhrnný pojem pro různé (kombinované) formy obsahu

Multimédia

Statické prvky
- text, schémata, grafy, prezentace

Dynamické prvky
- animace, interaktivita, **video**sekvence, **zvuk** a hudba, online aplikace, verifikační a validační aparát

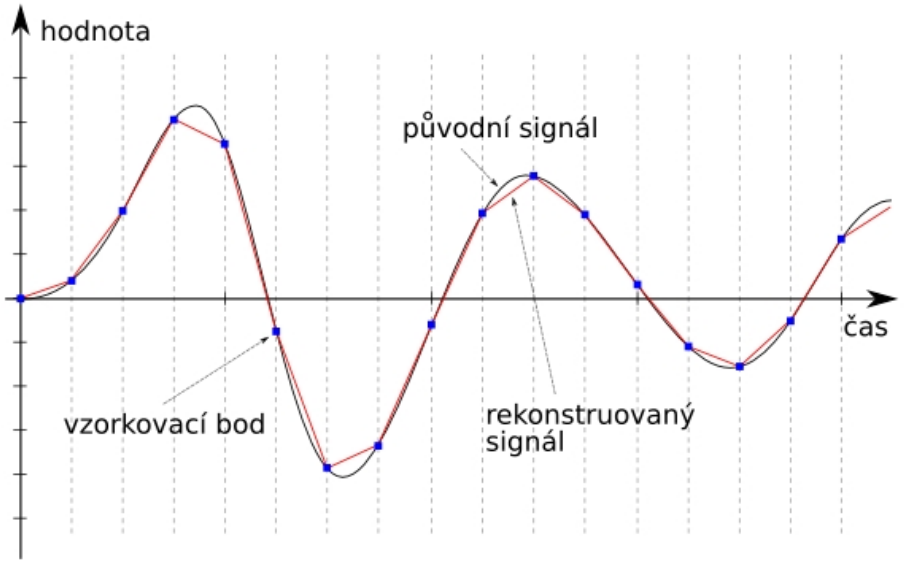
Asi 80 % informací a podnětů vnímají lidé zrakem, asi 12 % sluchem

Zvuk a video

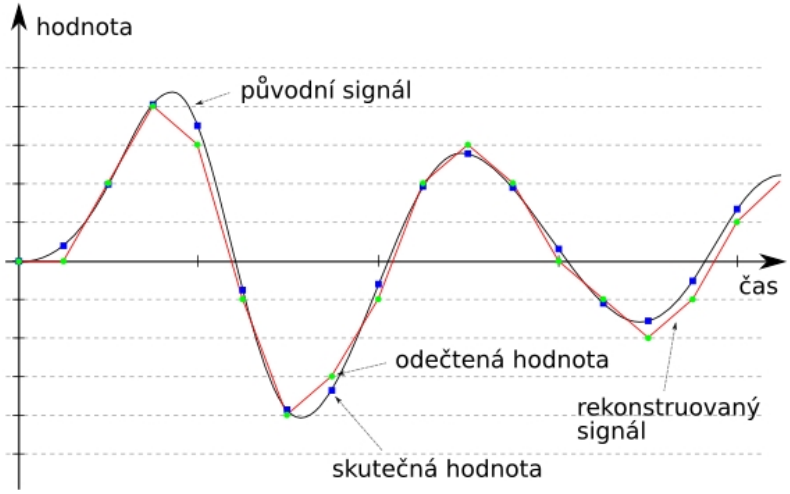
http://www.elearn.vsb.cz/archivcd/FS/Zaut/Animace/VzorkovaniKvantovani/VzorkovaniKvantovani.html

- Zvuk – mechanické vlnění ve vzduchu (nebo jiném médiu)
- Video – zpracování viditelné složky světla dopadajícího na sítnici oka
- Obojí dále zpracovávané v mozku

Zvuk i obraz jsou spojité vjemy – v případě zpracování na PC je třeba je reprezentovat pomocí **diskrétních** hodnot v čase (vzorků)



Přesnost nabírání informací určuje **kvantování** – čím více informace v bodě vzorku zachytíme tím bude výsledek přesnější



Základní termíny

- **Kódování dat** - Hrubý signál je vzorkován, kvantován, komprimován a v ukládán v daném formátu. Tomuto procesu se říká kódování, zpětné rekonstrukci pak dekódování. Dvojice algoritmů kodér-dekodér se pak dohromady označuje jako **kodek** (např. standard MPEG 1 Layer 3 = mp3).

- **Komprese –** cíl? Snížení objemu dat.
  - **Ztrátové –** odstraňují část dat (znalost lidských smyslů, psychoakustika, …), snižování bitrate, apod. (větší komprese)
  - **Bezeztrátové –** využívají inherentní struktury dat (opakující se data, předvídatelnost, apod.)

- **Metadata –** popisný charakter dat – čím, kdy, jak, autor, o kodeku, …

Základní termíny II

- **Formáty** – určují jakým způsobem jsou data uložena. Formáty úzce souvisí s použitým kodekem (např. mp3). Obálkové formáty definují jen strukturu souboru a ponechávají volnost pro různé kodeky (např. avi které může obsahovat DivX, xvid, mpeg4, mp3, h.263, flac, atd…).

- **Stream –** distribuce multimediálního obsahu současně s jeho prezentací uživateli

- **DRM –** Digital Rights Management – techniky k chránění práv souvisejících s využíváním multimediálního obsahu …

Práce v Audacity

- Získání audia z CD
  - https://www.youtube.com/watch?v=KlLCCU6ZthM
- Získání audia/videa z Youtube
  - https://www.youtube.com/watch?v=hTsKlPCqgW4Sav efrom.net (ss)
  - http://www.youtube-mp3.org/
- Zaznamenání a úprava audia v Audacity
  - https://www.youtube.com/watch?v=8fSlhfdSdqo
- Zpracování videa ve Windows Live Movie Maker
  - https://www.youtube.com/watch?v=Ky3yQypb-QM

- 1) stáhněte z YouTube hudbu dle Vašeho výběru (doporučuje se kolem 2 minut z důvodu délky stahování).

  2) Výsledný formát videa bude **WMV** a u hudby to bude formát **MP3 nebo WAV**.

  3) uložte na plochu do složky s Vaším **příjmením**.

  4) Pomocí softwaru **Audacity** otevřete hudbu, kterou jste si právě uložili do složky.

  5) Nyní hudbu upravte dle následujících pokynů:

  - písničku upravte na délku **dvou minut**
  - začátek písničky bude upraven pomocí nástroje **Postupný náběh**
  - konec písničky bude upraven pomocí nástroje **Do ztracena**
  - přibližně uprostřed písničky použijte nástroj **Kvákadlo**

- 6) Hudbu uložte ve formátu **WAV**.

- 1) Stáhněte z Youtube libovolné video (vhodná délka je cca 2 minuty) do formátu **WMV** (nebo jiný vhodný formát) a uložte do PC

- 2) Stáhněte z Youtube libovolnou hudbu, která bude později vložena do videa (nebo využijte hudbu z minulé hodiny)

- 7) Pomocí Windows Movie Maker Live otevřete video, které máte uloženo ve složce

  8) Nyní video upravte dle následujících pokynů:

  - úvodní titulky budou obsahovat Vaše **jméno** a barva písma bude **žlutá**
  - přibližně **do středu videa vložte obrázek** z knihovny obrázků nebo internetu
  - u tohoto obrázku bude **titulek** s názvem obrázku (třeba Koala), který bude **animován** dle Vašeho výběru (např. posun ze strany na stranu ...)
  - zvolte odpovídající **přechod** dle Vašeho výběru při změně z videa na obrázek (má se na mysli úsek ...video - VÁŠ ZVOLENÝ přechod - obrázek - video...)
  - video bude po celou dobu doprovázeno Vámi staženou **písničkou** z Youtube
  - na konci videa budou **závěrečné titulky**, kde bude slogan "Děkujeme za Váš čas", pozadí těchto titulků bude **v barvě červené**

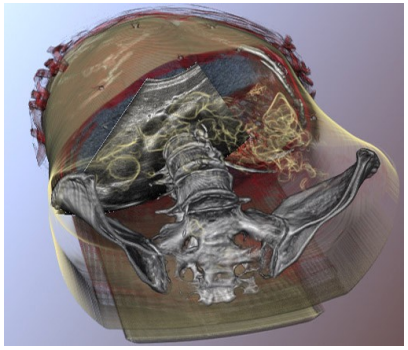
- 9) Nyní video uložte ve formátu **WMV**

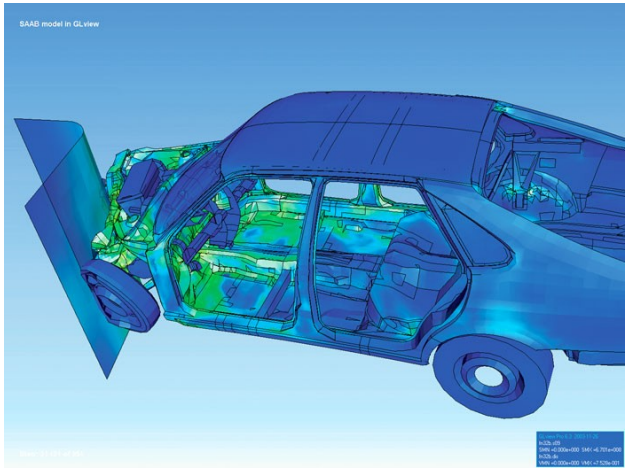
  10) Zkontrolujte

Počítačová grafika – rastrová x vektorová

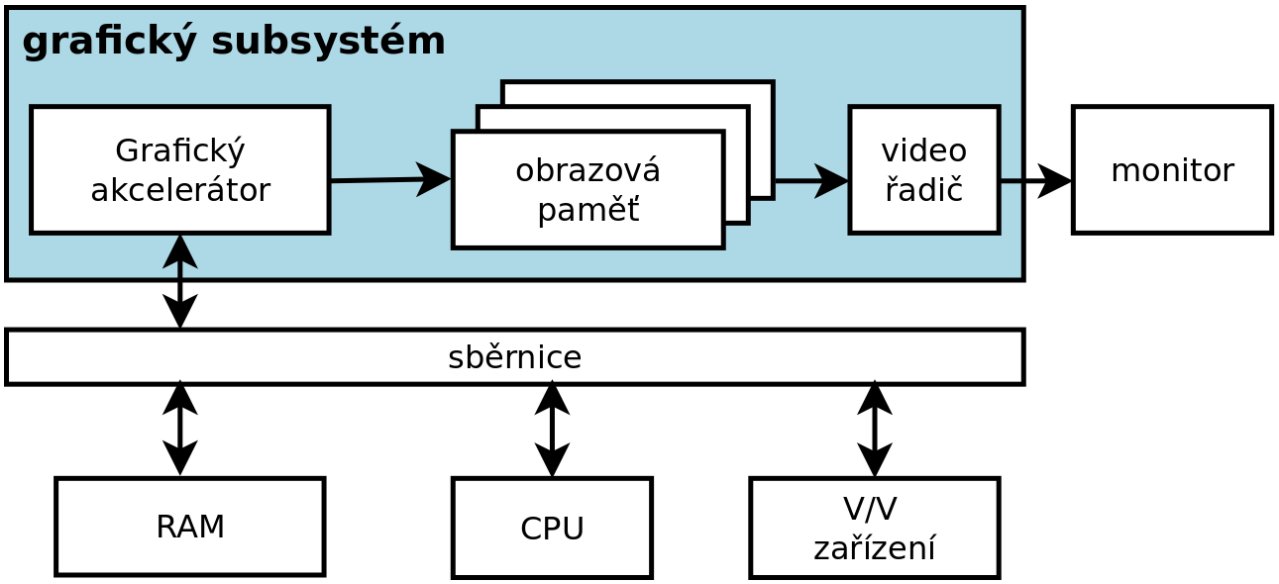
Obor počítačové grafiky

- Zabývá se zobrazením, manipulací a ukládáním vizuálního obrazu.
- Zahrnuje množství aplikací, s některými se setkáváme každý den:
  - grafická uživatelská rozhraní
  - zábavní průmysl (TV, poč. hry, ...)
  - vizualizace ve vědě (simulace, analýza signálů, ...)
  - vizualizace medicínských dat (EKG, EEG, MRI, ...)
  - 3D modelování (architektura, strojírenství, ...)
  - zpracování digitální fotografie a další.





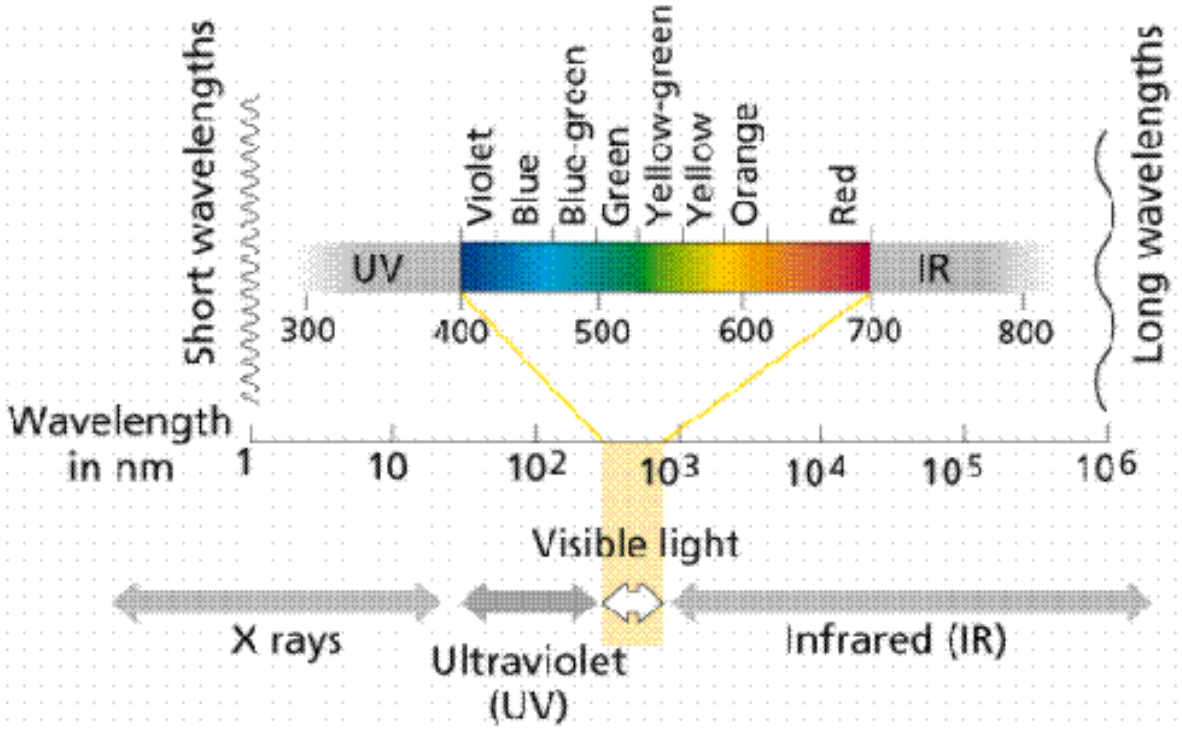
Grafický subsystém



- Grafická karta komunikuje s PC systémem přes sběrnici (např. PCIex.) a zpracovaný obraz zasílá přes výstup (DVI, HDMI, …) na monitor (LCD, CRT, …)

Světlo

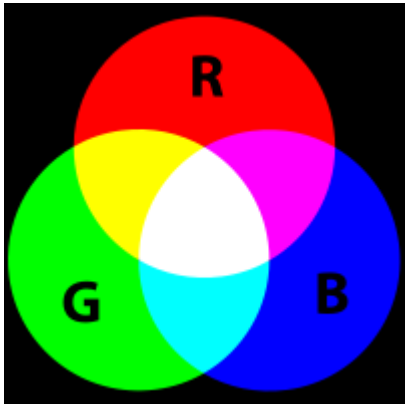
- je elektromagnetické vlnění charakterizované vlnovou délkou a intenzitou. Lidské oko je schopné vnímat pouze úzký výsek možných vlnových délek — tzv. viditelné spektrum (400 nm fialová – 700 nm červená).



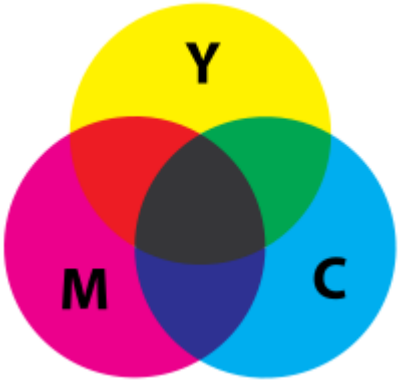
http://www.mazar.cz/files/2.gif

Barva

- Vnímání barvy lidským okem jako mix vlnových délek a interpretace mozkem
- V PC reprezentovány různými barevnými modely



Aditivní – RGB (monitory a další zařízení pracující se světlem)



Subtraktivní – CMY(K) (tiskárny, …)

Pozn.: existují i další modely využitelné spíše pro grafiky…

Barevná hloubka – počet bitů pro reprezentaci barvy jednoho **pixelu**
- např.: 24b barevná hloubka = 8b na kanál (R, G, B) = 2^8 = 256 úrovní jedné složky barvy ➔ celkový počet barev = 256*256*256 tedy 16,7 Mbarev

Pixel

- Reálný obraz je v PC prezentován nespojitě (diskrétně) rozložený do obrazových bodů = pixelů.
- Pixely tvoří pole (rastr)
- Počet bodů v obraze udává jeho rozlišení
  - Např.: monitor fullHD 1920x1080, digitální fotoaparát 12MPx = 4000x3000, ….

- Rozlišení se udává také v DPI (dots per inch)
  - 1 palec – 2,54cm
  - Obrázek o rozměrech 100x100px o velikosti 2,54cm x 2,54cm má DPI 100
  - Při foto-tisku na 300DPI 9x13 tedy potřebujeme 1063x1536 bodů
  - Atd…

Antialiasing, hinting, …

- Převod reálného obrazu (rasterizace) může přinášet ztráty a nežádoucí artefakty - alias - (zubaté okraje, méně detailů, …)
- Antialiasing – techniky kompenzující chyby

sample

sample

Antialiasing:

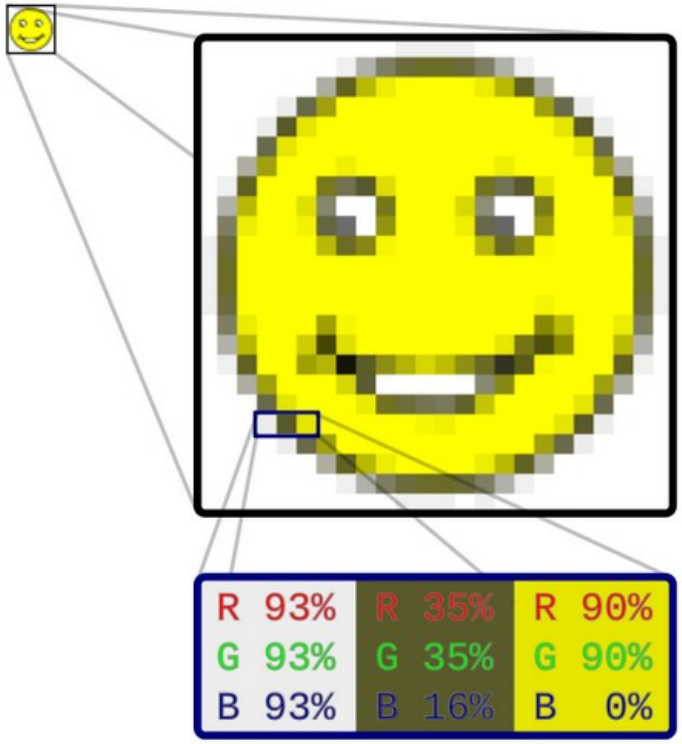
sample

sample

Hinting:

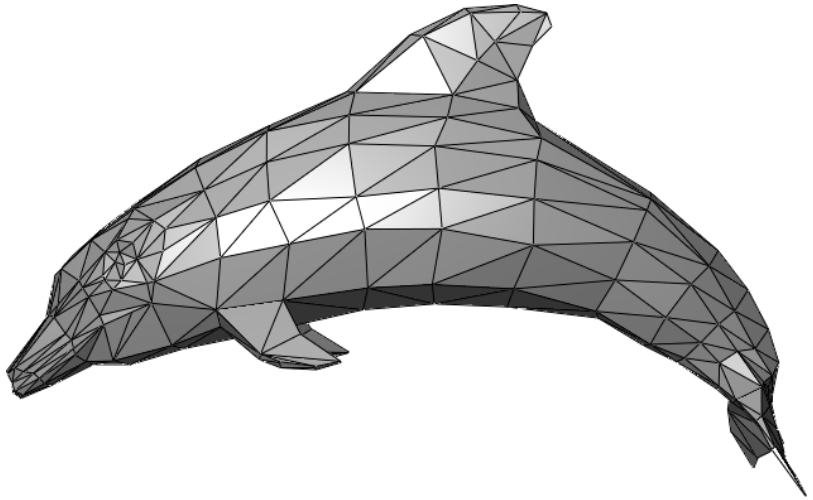
sample

sample



3D

- **3D** model popisuje tvar objektů ve scéně, vlastnosti jejich povrchu a zdroje světla
- Objekty 3D scény jsou **modelovány** jen pomocí svého **povrchu**
- Ten je popsán jako síť mnohoúhelníků (tzv**. polygonů**, nejčastěji trojúhelníků) a jeho optické vlastnosti, jako barva, rozptyl a odraz světla a struktura, se definují pomocí **textur** — obrázků "natažených" na plochý povrch polygonů.
- Proces vytvoření výsledného obrazu z 3D modelu scény se nazývá **renderování**. (tento proces může být velmi výpočetně náročný v závislosti na složitosti a realističnosti)



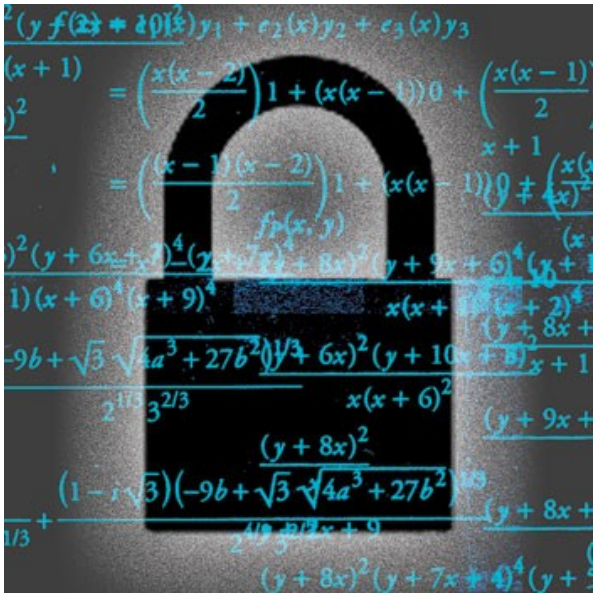
Vektorová grafika

- Obraz který není reprezentovaný rastrem bodů, ale pomocí matematických primitiv a jejich vlastností
  - Body, úsečky, křivky, n-úhelníky, …
- Lze ji libovolně zvětšovat a transformovat beze ztráty detailů
- Nevhodná pro fotorealistickou grafiku
- Paměťová náročnost závislá na složitosti a ne rozlišení
- Vhodná pro:
  - Loga, písma, návrhy plakátů, apod.

Kryptografie a bezpečnost 1

Kryptografie

- věda zabývající se zajištěním utajené a důvěryhodné komunikace – tedy tvorbou šifer pro lepší zabezpečení nás na síti



Proč kryptografie?

- Stále větší část našich dat je na síti
- Prostřednictvím internetu děláme i důležité úkony (el. Podpis, žádosti o práci, platby…)
- Kryptografie na síti je stejně logická jako to, že zamykáme svoje domy nebo auta
- S kryptografií se setkáváme každý den, i když si to ani neuvědomujeme -> třeba při přihlašování do IS MU

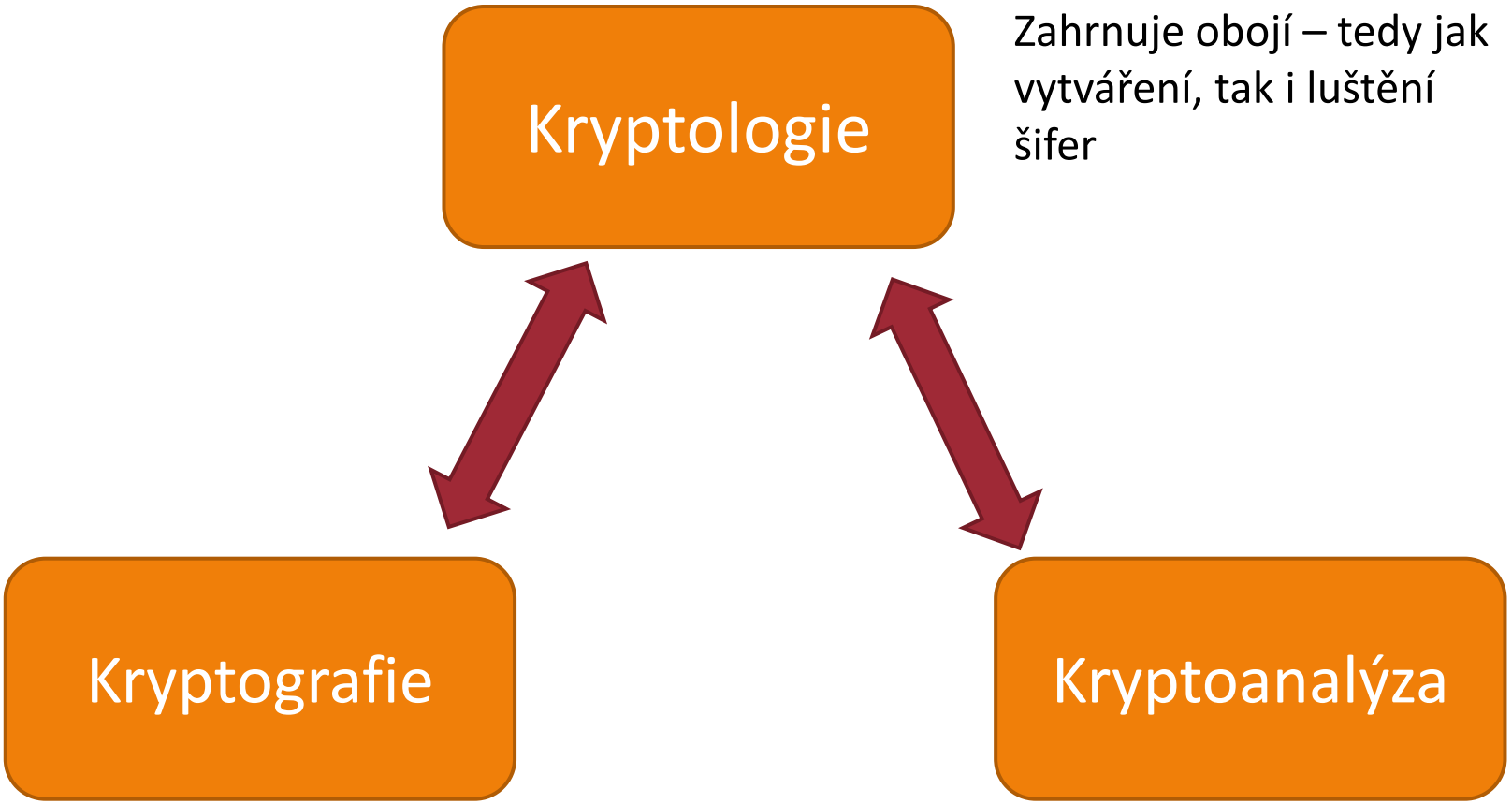
Něco z historie

- Lidé šifrovali svoji komunikaci již od starověku
- Šifrovali se rozkazy pro vojska, deníky politiků, depeše diplomatů…
- Kryptografie nebyla tedy vědou spojenou s IT, ale obecně s šifrováním zpráv

Skytalé - šifrování, který se skládá z válce a na něm navinutém pergamenu na kterém je napsaný vzkaz. Používali je Řekové, kteří ji využívali během válek.

Enigma - šifrovací stroj používaný za války německou armádou

Kryptografie vs. Kryptoanalýza



Cíle kryptografie

- zabezpečit komunikaci citlivých dat mezi uživatelem a internetovou službou
- zajistit důvěryhodnost komunikace mezi uživateli (např. email)
- autorizace závažných úkolů (ebanking, el. obchody, ...)
- omezit přístup k určitým službám jen pro určené jedince (zabezpečená wi-fi)

Časté omyly uživatelů

- „V tom e-mailu stejně nemám nic co by stálo za to ukrást.“ – chyba. Stačí i to, že znají vaše e-mailové heslo, které může být stejné/podobné jako heslo k e-bankingu, pracovním datům a podobně
- „Jaká je pravděpodobnost, že se to stane zrovna mě?“ – docela slušná. Data o uživatelích dnes kradou často autonomní programy. Pokud odhalí že máte slabé zabezpečení zaměří se na vás.
- I když vy sami nejste pro hackera zajímavý, může z vašich dat získat informace třeba o vašem zaměstnavateli

Co tedy napomáhá k naší ochraně?

- Dobré heslo
- Certifikační systém
- Šifrované spojení
- Zdravá paranoia ☺

Autentizace

- … je ověření identity uživatele, který se pokouší přihlásit do služby, systému apod. (od slova autentický)

Autentizace – jak se provádí?

❖podle toho, co uživatel zná (zná správnou kombinaci uživatelského označení a hesla nebo PIN)

❖podle toho, co uživatel má (nějaký technický prostředek, který uživatel vlastní – hardwarový klíč, smart card, privátní klíč apod.)

❖podle toho, čím uživatel je (uživatel má biometrické vlastnosti, které lze prověřit – otisk prstu, snímek oční duhovky či sítnice apod.)

❖podle toho, co uživatel umí (umí správně odpovědět na náhodně vygenerovaný kontrolní dotaz)

Heslo – vaše osobní šifra

Co je to „dobré heslo“

- …je takové, co půjde špatně odhalit ☺
- 1) Heslo by se neměl tvořit nějaký snadno dohádatelný údaj o uživateli. – tedy ne vaše jméno, jména vašich dětí apod.
- 2) Mělo by být dostatečně dlouhé – čím delší tím déle trvá jeho odhalení. S každým dalším znakem se násobí časová délka nutná k jeho odhalení
- 3) Mělo by obsahovat velká a malá písmena, čísla a speciální znaky (@, ?). Nejdůležitější je ale jeho délka

Jak s heslem zacházet

- hesla k důležitým službám (ebanking, IS, email, ...) nesmí být stejná
- heslo nikdy nikomu nesdělujte
- důležitá hesla neukládejte v prohlížeči, ani je nikam nezapisujte
- po zadání hesla na nedůvěryhodném stroji (např. na cestách) jej při nejbližší příležitosti změňte

Klikni zde

Něco více o heslech

Útoky na hesla

- **Sociální inženýrství** - patří mezi nejúčinnější metody útoků . Útočník se snaží zjistit buď přímo zjistit heslo, nebo informace, které ho k heslu dovedou. Prostě se vás zeptá. Druhá varianta je zjistit si základní informace o daném člověku a potom zkusit zmiňované jméno partnera, dětí, dalších rodinných příslušníků, nebo domácích zvířat.

- **Odchycení hesla-** používají se například keyloggery (programy pro snímání stisknutých kláves na klávesnici).

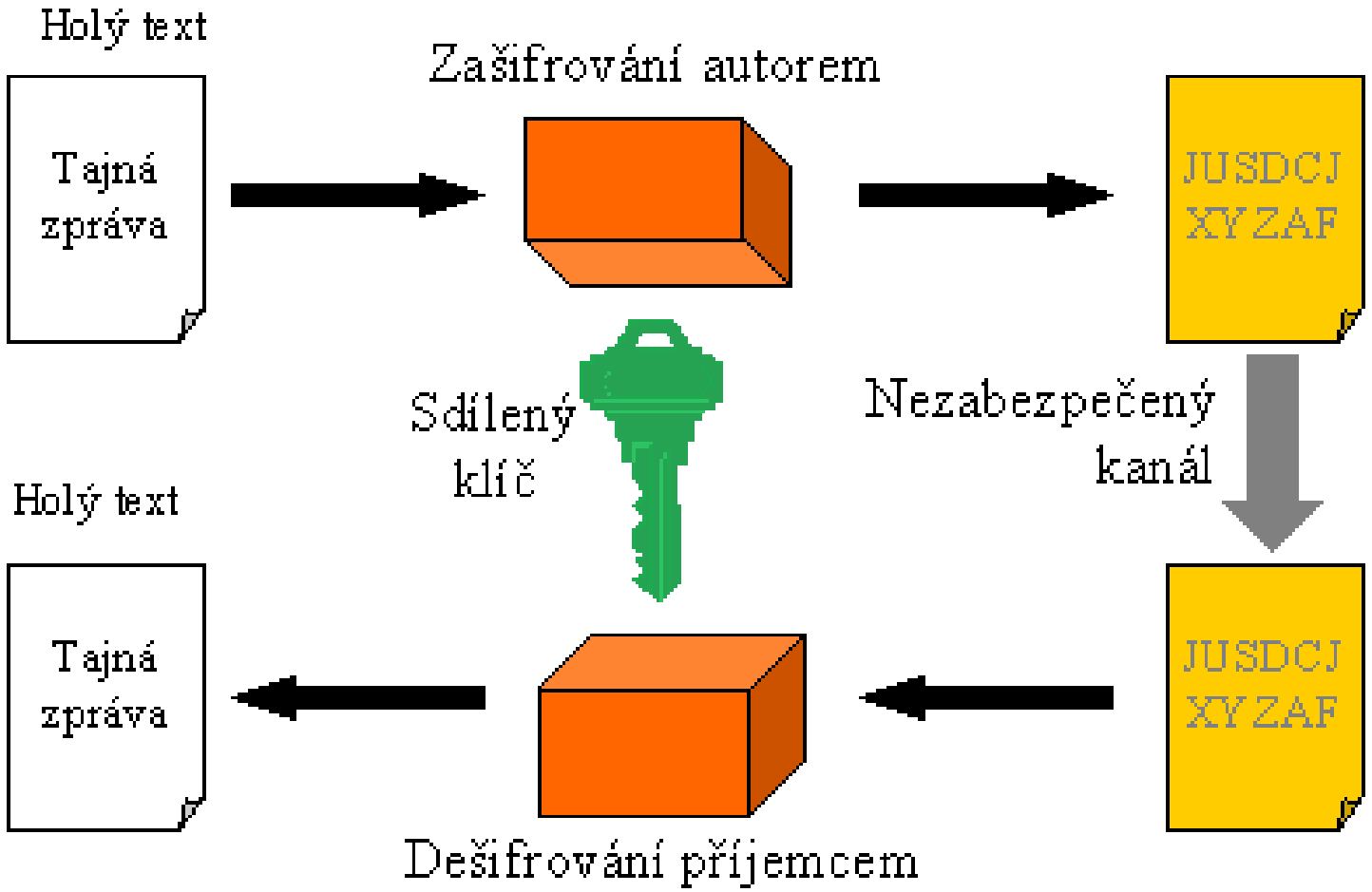
- **Slovníkový útok -** Útočník má slovník slov daného jazyka a zkouší zadat jako heslo jednotlivá slova z tohoto slovníku. Nezadává ručně, ale automaticky pomocí počítačového programu. Takovým způsobem pak může vyzkoušet mnoho hesel za sekundu.

- **Útok hrubou silou -** Nejprimitivnější varianta útoku, útočník zkouší postupně zadávat všechny kombinace, například: aaa, aab, aac, aad,...

Symetrická kryptografie

- Funguje na jednodušším principu než asymetrická
- Odesilatel i příjemce zprávy mají ten stejný klíč k zašifrování i rozšifrování – typicky heslo
- **Příklad:** Posíláte symetricky zašifrovaná data vašemu známému. Jako heslo si určíte „heslo123“ , které mu předtím řeknete. Vy toto heslo použijete na zašifrování dat on toto stejné heslo použije na rozšifrování dat a převedení zašifrovaných dat zpět do podoby běžného textu. Je to v principu stejné jako když má více lidí stejný klíč k jedněm dveřím

Symetrické šifrování



Symetrická kryptografie

- Výhody:
- Jednodušší na výpočetní výkon – symetrická šifra je vytvořena velice rychle
- Nevýhody:
- Nutnost předání soukromého klíče druhé straně

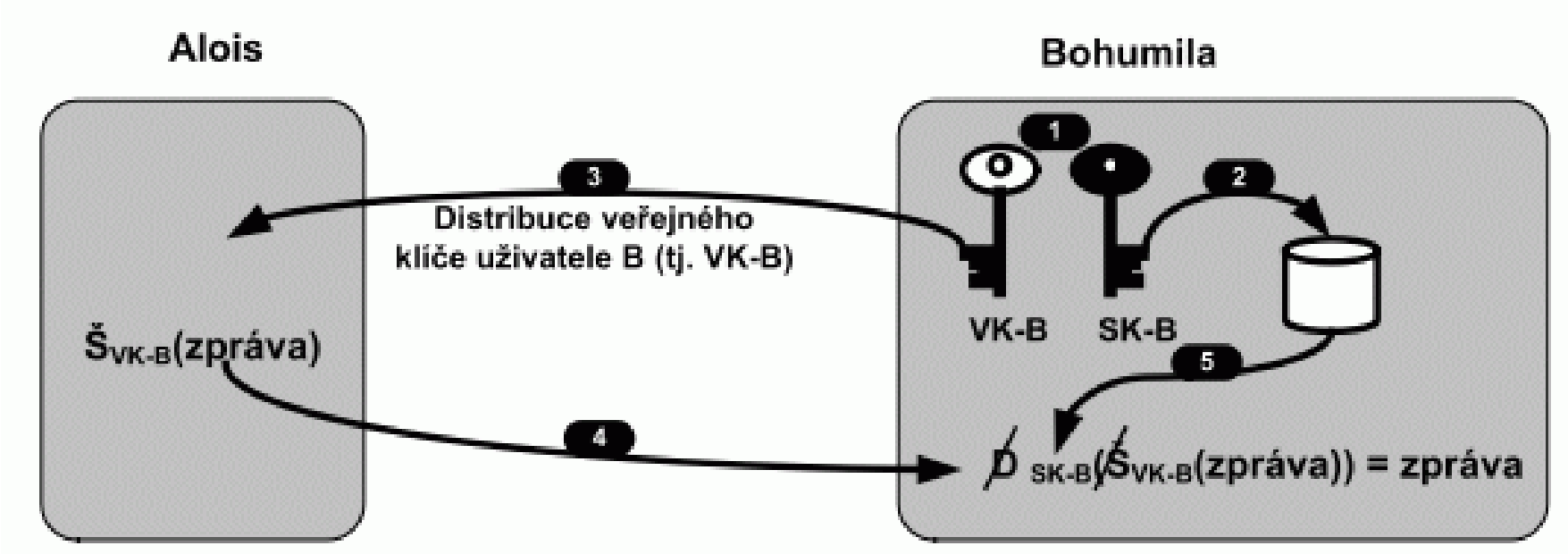
Asymetrická kryptografie

- Tyto šifry nepoužívají jeden tajný šifrovací klíč sdílený mezi odesilatelem a příjemcem, ale vždy se používá **pár šifrovacích klíčů**. Jeden klíč **pro šifrování** a **druhý pro dešifrování**. U digitálního podpisu pak uvedeme, že operace šifrování a dešifrování jsou u některých šifer zaměnitelné, proto u asymetrických šifer nemluvíme o šifrovacím a dešifrovacím klíči, ale o **veřejném a soukromém klíči**.

Asymetrická kryptografie

- Bohumila, tj. příjemce zprávy, si musí vygenerovat dvojici klíčů: **veřejný klíč** (VK-B) a **soukromý klíč** (SK-B).
- Bohumila si uloží svůj soukromý klíč do důvěryhodného úložiště klíčů. Např. na disk, na čipovou kartu atd. **Soukromý klíč je aktivem Bohumily, které si musí střežit.**
- Bohumila distribuuje svůj veřejný klíč (VK-B) **do celého světa**. Klidně může svůj veřejný klíč poslat Aloisovi po slídivém Cyrilovi.
- Alois po obdržení veřejného klíče Bohumily šifruje zprávu Bohumile jejím veřejným klíčem (VK-B).
- Bohumila (příjemce) dešifruje přijatou šifrovanou zprávu svým soukromým klíčem (SK-B) a získá původní zprávu.

Asymetrická kryptografie



- Základní vlastností šifrování na bázi asymetrických algoritmů je skutečnost, že je relativně jednoduché za využití veřejného klíče šifrovat text, ale na základě znalosti veřejného klíče a veřejným klíčem šifrované zprávy je velice obtížné získat původní zprávu.

Elektronický podpis

- Vychází z principů asymetrického šifrování

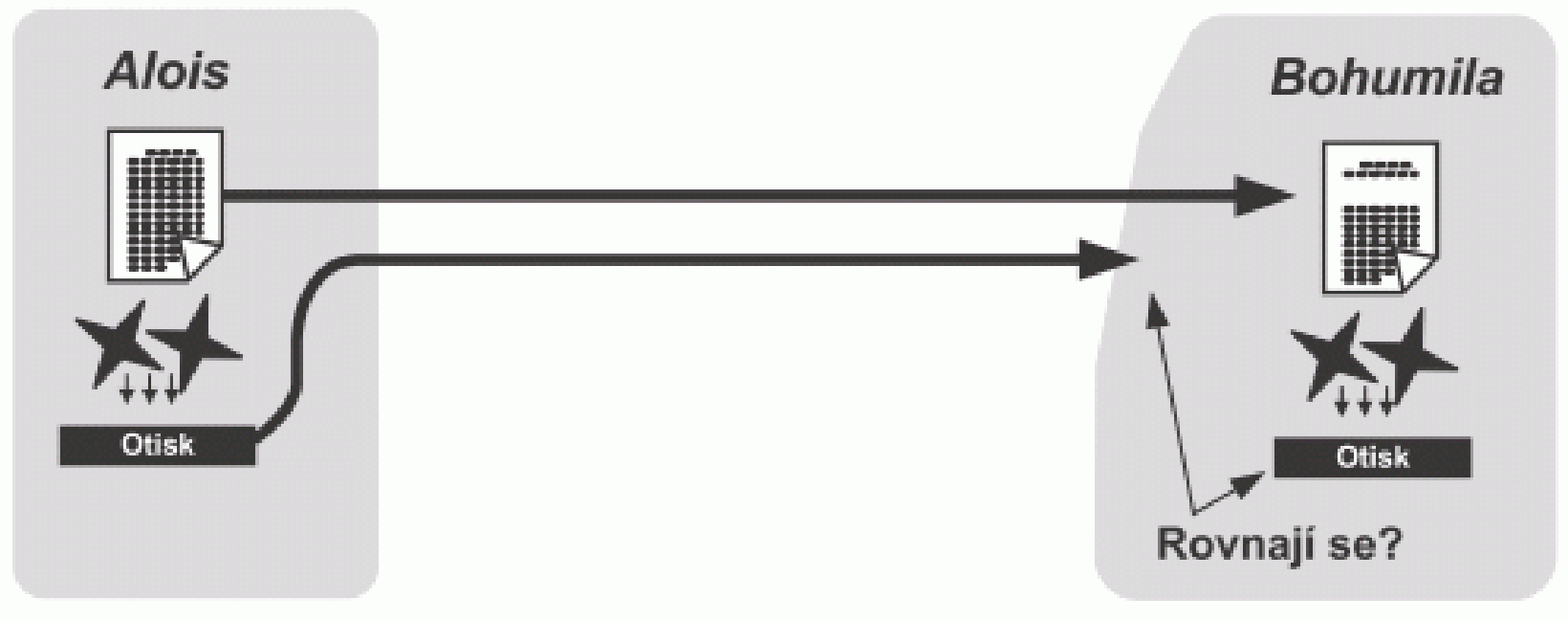
- El. podpis je potvrzení, že zpráva byla vytvořena daným autorem
- realizován pomocí asymetrické kryptografie:
  - pomocí soukromého klíče je k dané zprávě vytvořen podpis
  - příslušný veřejný klíč umožňuje ověřit pravost podpisu

Hash – kontrolní výpočet

- Krátký **otisk** textu (zprávy, hesla) vytvořený jednocestnou funkcí. Pro daný text je hash jednoznačně daný, nelze z něj ale zrekonstruovat žádné informace o původním textu

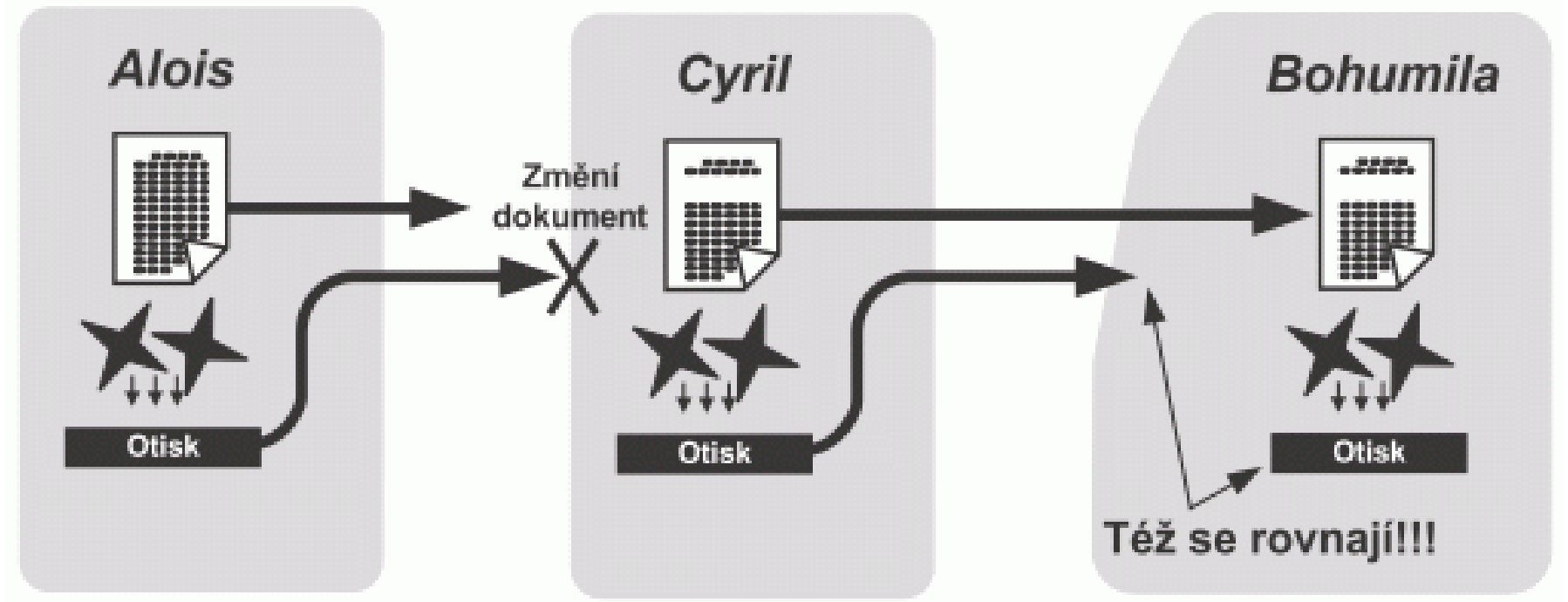
- …. ale lze jej použít pro kontrolu přijaté zprávy, že nebyla cestou změněna

Hash – jak funguje?



- Alois posílá zprávu Bohumile. Spolu s ní odešle hash. Bohumila, poté co přijme zprávu, spočte otisk (hash) z přijaté zprávy a porovná svůj výsledek s otiskem ze zápatí přijaté zprávy (tj. s otiskem spočteným Aloisem). Pokud jsou oba otisky shodné, zpráva nebyla cestou změněna.

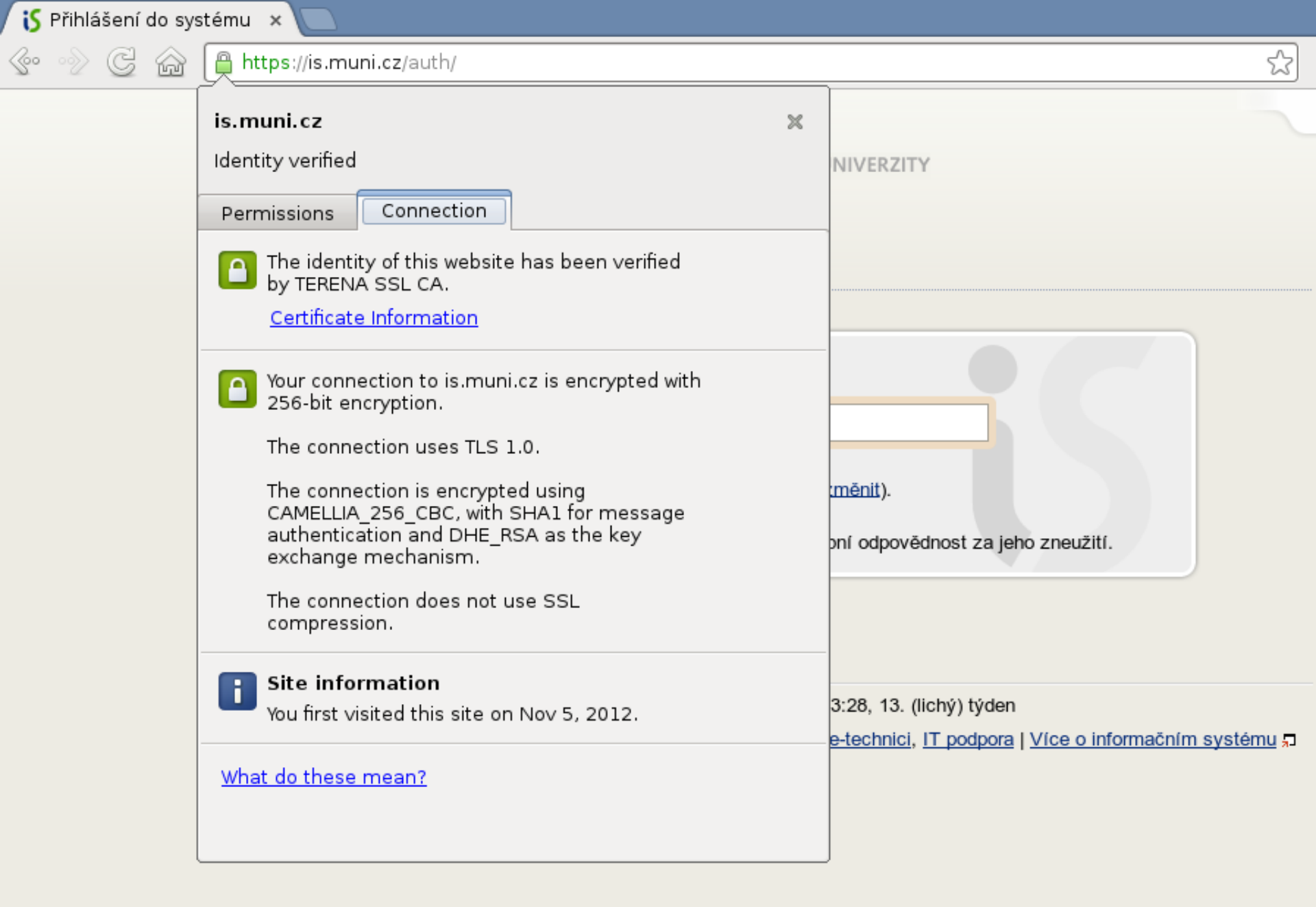
Hash – jak funguje?



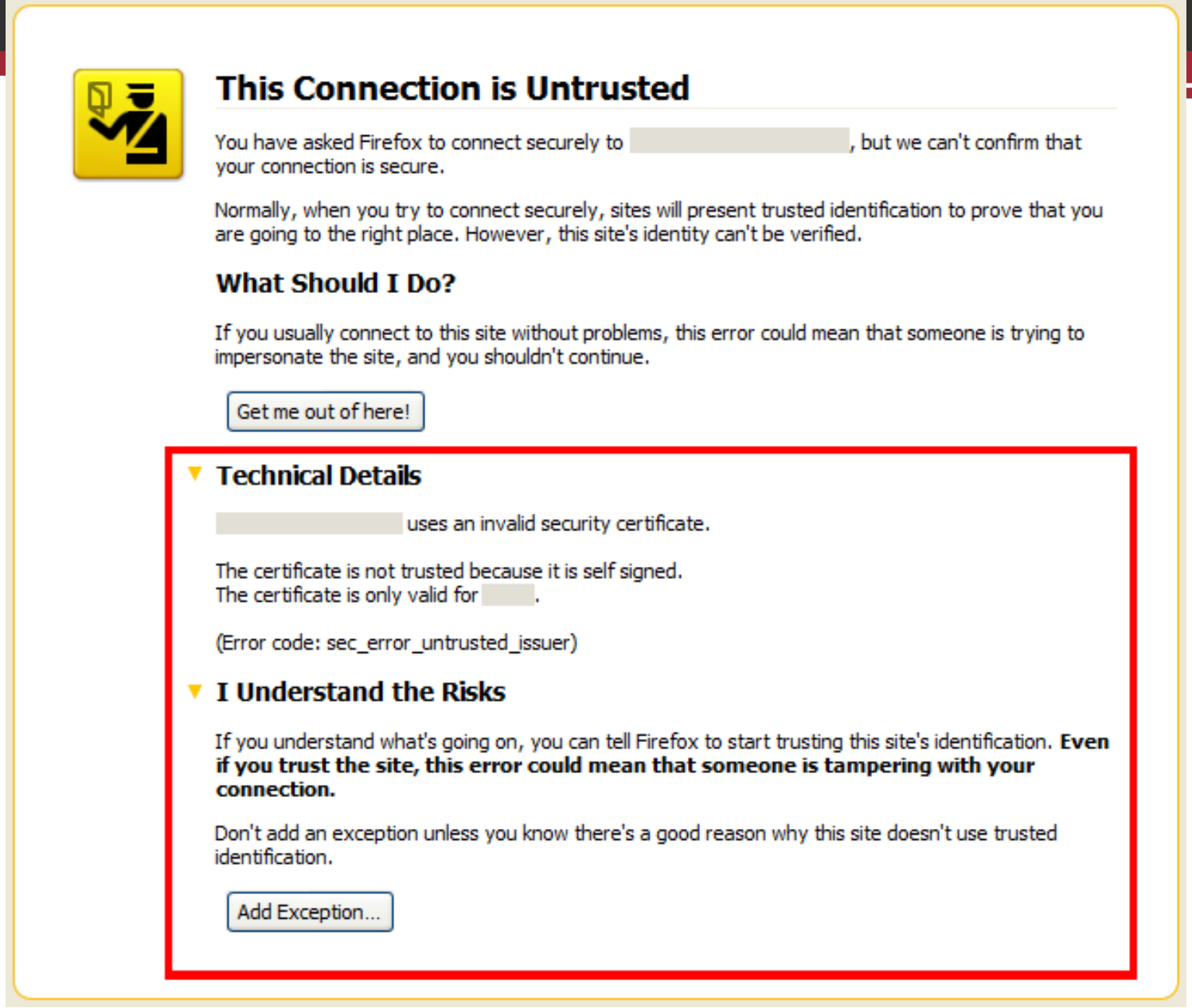
- Zprávu odchytí (a tím pozmění) slídil Cyril. Zpráva dojde (pozměněná) Bohumile. Tím že došlo ke změně zprávy, tak už nejde zpětně dopočítat hash, Bohumila tedy ví, že zpráva byla po cestě změněna.

Certifikace pomocí https

- Nástavba běžného http protokolu, který není šifrován
- U https jsou využívány certifikáty důvěryhodnosti, které vydává nějaká velká certifikační autorita
- Dnešní prohlížeče s certifikáty umí běžně pracovat a pokud web žádnou certifikaci nemá (nebo ji jen předstírá) snaží se vás většinou varovat



- Certifikát v Google Chrome



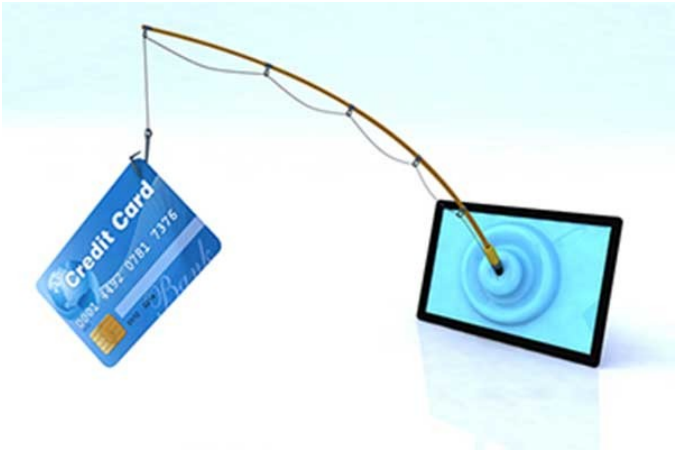
- Odhalení nedůvěryhodného certifikátu

Některé formy útoku

- **Phising** – podvržené stránky a zahrávání si s psychologií uživatele
- **Útoky na hesla** – různé metody jak odhalit vaše heslo. Viz. kapitola o heslech
- **Odposlech bezdrátové komunikace**
- **Malware** – různé druhy škodlivého softwaru, které mohou získat vaše hesla, nebo přímo data

Psychologie v útoku - phishing

- *Only amateurs attack machines; professionals target people.*
  - *— Bruce Schneier*



Phishing

- Pro útočníka je jednodušší využít neopatrnosti cíle (vás) a jeho oklamání, než složitě nabourávat šifrované stroje

- Evolučně jsme si vytvořili poznávací mechanismy, proti podvodům z očí do očí, teď se musíme naučit mechanismy pro odhalení podvodů skrze monitor.

Phishing – jak funguje

- Vytvoření návnady (falešná stránka vaší banky)
- Rozeslání e-mailů uživatelům (výzva ke změně hesla, kontrole údajů…)
- Uložení vašich údajů u útočníka
- …poté proběhne standardní přihlášení do běžné služby, aby se nevytvořilo podezření


THE NIGERIAN PRINCE NEEDS MY HELP?
I'LL GET MOM'S CREDIT CARD!

Šifrování wifi vs. odposlech

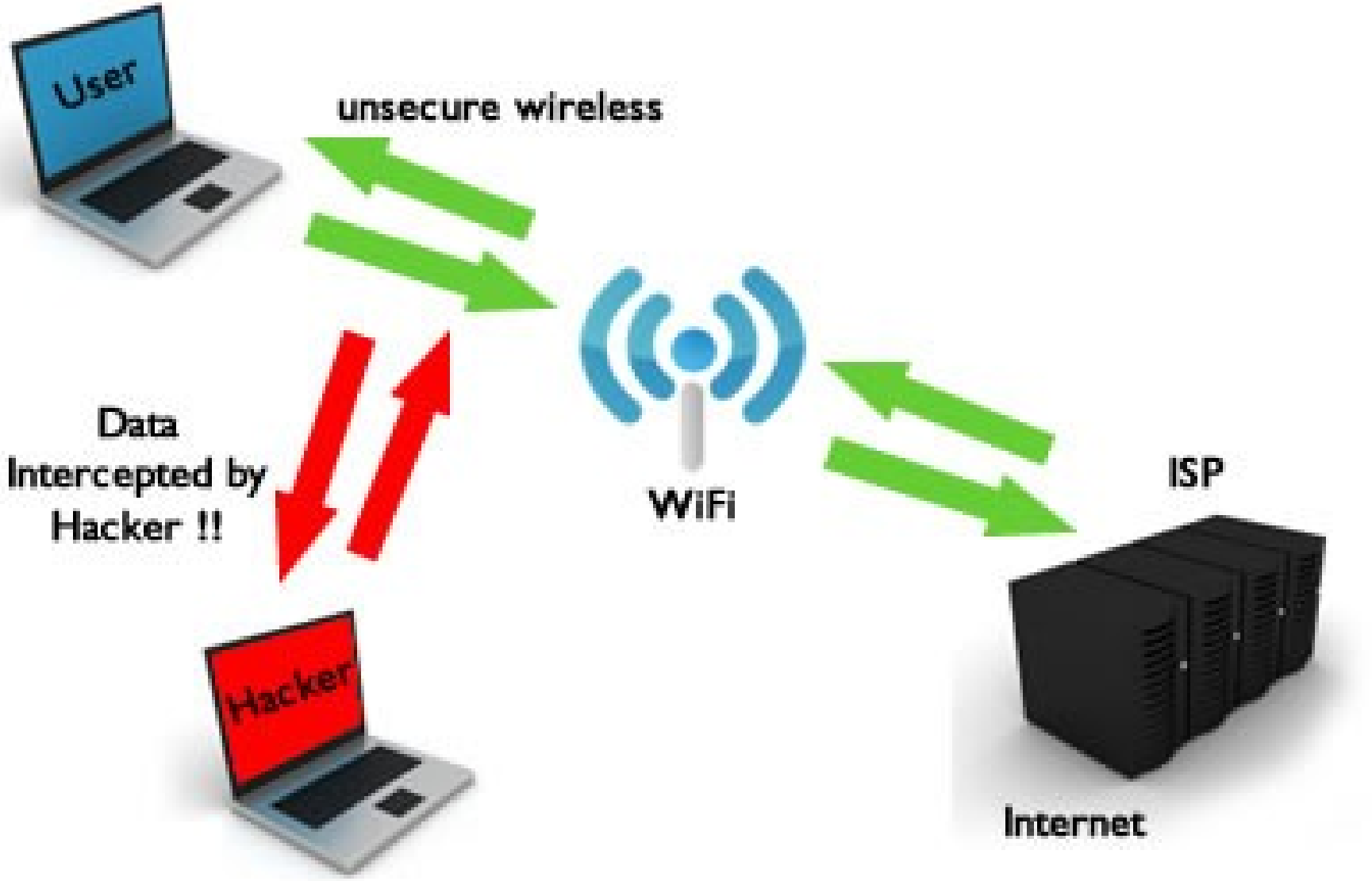
- Na rozdíl od pevné (drátové) sítě nelze fyzicky omezit přístup k bezdrátové síti. U wifi není možné zjistit, zda probíhající komunikaci někdo nesleduje (a nenahrává). Z těchto důvodů se zavádí autentizace (přihlašování) při připojení síti a šifrování provozu přihlášených uživatelů

- Pozor tedy na wifi zdarma! ☺

Útok na wifi

- **Odposlech**
- není možné jeho aktivitu zjistit
- v případě nešifrované (nebo slabě šifrované — WEP) vidí veškerou komunikaci vedenou mimo zabezpečené protokoly (např. https)
- může sledovat například osobní údaje, stahované dokumenty a další data putující sítí, které mu umožní vést přímé útoky: vydávání se za uživatele (krádež identity), získání přístupu přes fingovanou ztrátu hesla a pod.

- **Ofenzivní útočník**
- v případě slabého šifrování může získat klíč pro vstup do sítě (WEP)
- může získat přístup k nastavení přípojného bodu (a využít jej např. ke sledování aktivity na síti)
- po získání přístupu do sítě útočit na jednotlivé počítače (i tak jednoduše, jako vyhledávání nevědomky sdílených složek)
- vytvořit volně přístupný přípojný bod, na kterém bude sledovat veškerou komunikaci


User
unsecure wireless
Data
Intercepted by
Hacker !!
WiFi
ISP
Hacker
Internet

Jak se tedy bránit?

- **jako uživatel**
  - nepřipojujte se k nedůvěryhodným přípojným bodům
  - používejte zabezpečený protokol https
  - mějte zapnutý firewall
- **při nastavení domácí sítě**
  - změňte výchozí hodnoty pro název sítě a heslo pro administraci
  - vyberte šifrování provozu pomocí WPA (WPA-2), **WEP varianta je dnes již považována za slabou**
  - zvolte dostatečně silné heslo (viz výše)

Malware

- = škodlivý software, jehož účelem je poškození, nebo infiltrace počítačového systému
- Řadí se sem různé viry, trojské koně, keylogery, atp.
- Pomocí malwaru je možné:
  - Získávat data a údaje z postiženého PC (třeba hesla, soukromá data…)
  - Použít ovládnutý počítač k nelegální aktivitě (rozesílání dalších virů, útokům na velké cíle…)

Některé druhy malwaru

- Trojský kůň – vydává se za užitečný SW, po instalaci uživatelem provádí svoji pravou funkci
- Keylogger – program který snímá stisknuté klávesy (odposlech hesel)
- Adware – méně škodlivý, způsobuje časté zahlcování reklamou

Rady na závěr

- Buďte paranoidní ! Pomáhá to ☺
- Nepodceňujte svoji významnost !
- Když nevíte nechte si poradit od vašeho správce sítě!
- Vždycky někdo někde poslouchá !

Zdroje

- http://prf-czv.osu.cz/nabidka/seminar/data/Kryptografie.pdf
- http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c05.pdf
- http://mi21.vsb.cz/sites/mi21.vsb.cz/files/unit/mzka.png
- http://frakira.fi.muni.cz/~izaak/PBIT/Kryptografie_a_bezpe%C4%8Dnost.html
- http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf
- http://www.flops.cz/zaklady-sifrovani-symetricka-a-asymetricka-kryptografie
- http://cs.wikipedia.org/wiki/Autentizace
- http://www.guardmyip.com/images/wireless_security1.jpg

- DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-80-251-2619-6.

Kryptografie a bezpečnost 2

Osnova

1. Základní pojmy
2. Bezpečnost sítí
3. Kryptografie
4. Autentizace
5. Zálohování dat

Pomocné materiály

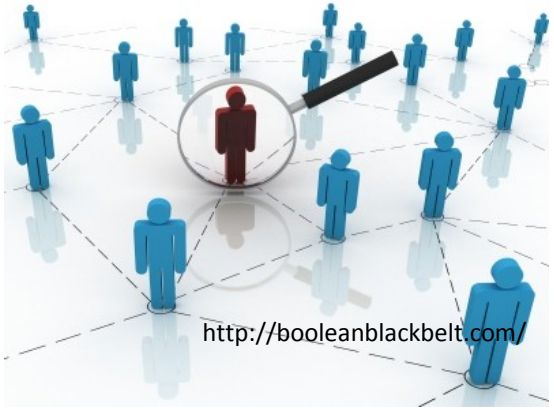
- http://www.fi.muni.cz/~xstehl2/SITMU/Home.html.
  - Rozpracované materiály v rámci projektu SITMU.
- http://frakira.fi.muni.cz/~izaak/PBIT/Kryptografie_a_bezpe%C4%8Dnost.html.
  - Kapitola o bezpečnosti IT a kryptografii v rámci materiálů „Základy IT gramotnosti“.

Základní pojmy

- Informační soukromí
  - Možnost kontroly informací osobních dat a jiných citlivých informací.
- Funkce zajišťující informační soukromí
  - *Anonymita* - vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému.
  - *Pseudonymita* - vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému tak, že uživatel je stále zodpovědný za toto použití.
  - *Nespojitelnost* - vlastnost systému, který zajišťuje možnost opakovaného použití zdrojů nebo služeb s tím, že ostatní si tato použití nebudou schopni spojit.
  - *Nepozorovatelnost* - vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb tak, že ostatní nemohou zpozorovat používání daného zdroje nebo služeb.

Další bezpečnostní vlastnosti

- Identita
- Autentizace
- Identifikace
- Autorizace
- Důvěrnost
- Integrita
- Dostupnost
- Nepopiratelnost
- Účtování
- …



http://www.123rf.com/

Bezpečnost sítí

- Většina hrozeb přichází z Internetu.
- Většina počítačů je připojena do Internetu.
- Žádný počítač připojený do Internetu není 100% bezpečný!
- Je nuté zajistit alespoň *relativně* bezpečné připojení do Internetu.

Základní předpoklady

- Použití těchto nástrojů:
  - Antivir.
  - Antispyware.
  - Firewall.
  - Udržování operačního systému a dalších programů v aktuálním stavu.
  - Použití běžných uživatelských účtu – nikoli správcovských.
- Důležité je správné a odpovědné chování při prohlížení webu či používání e-mailu.

Viry

- Počítačový program, který se šíří tím, že vytváří kopie sebe sama.
- Sofistikované viry umí mutovat a tím znesnadnit svoji detekci antivirovým programem.
- Druhy virů
  - Viry.
  - Červy.
  - Trojští koně.

Antiviry I

- Detekují a pomáhají odstranit počítačové viry.
- Útočníci jsou vždy o krok napřed, přesto je **pravidelně aktualizovaný** antivirový program základním předpokladem počítačové bezpečnosti.

Antiviry II

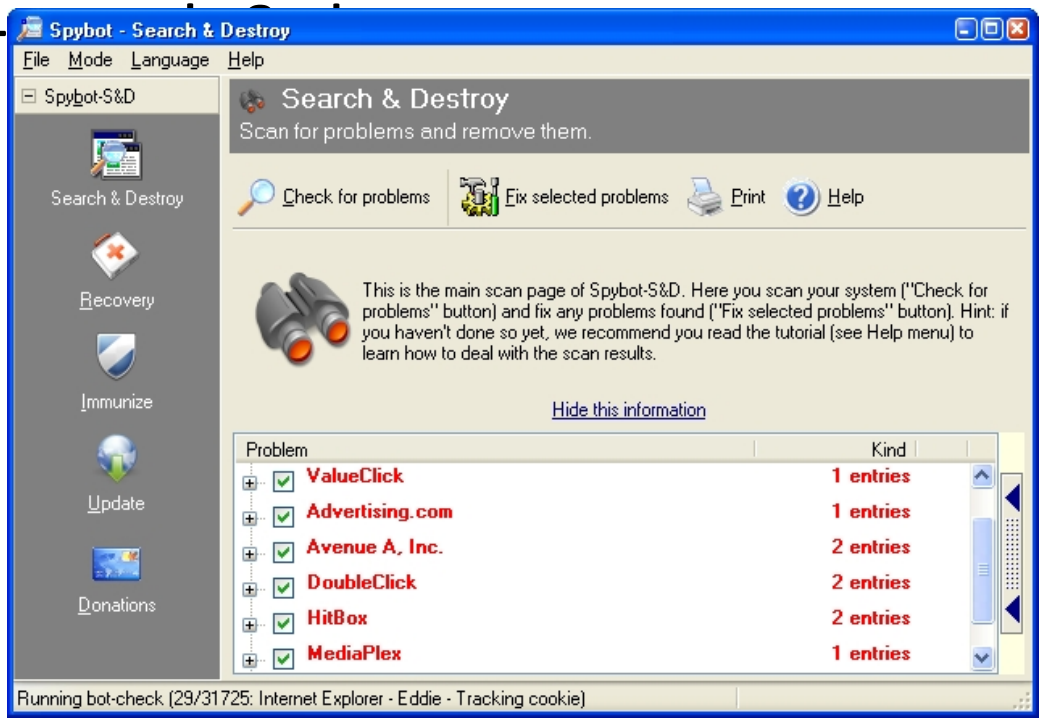
- Antivirový program je nutné udržovat **aktuální**.
- Volně dostupné antiviry:
  - Avast Home Edition.
  - AVG Antivirus Free.
  - …

Spyware

- Sleduje online chování a sbírá informace.
- Mění nastavení počítače.
- Odesílá data z počítače bez vědomí uživatele.
- Adware
  - Cílem je stahovat a zobrazovat uživateli reklamy.
  - Ne vždy je škodlivý – např. alternativa k placení.

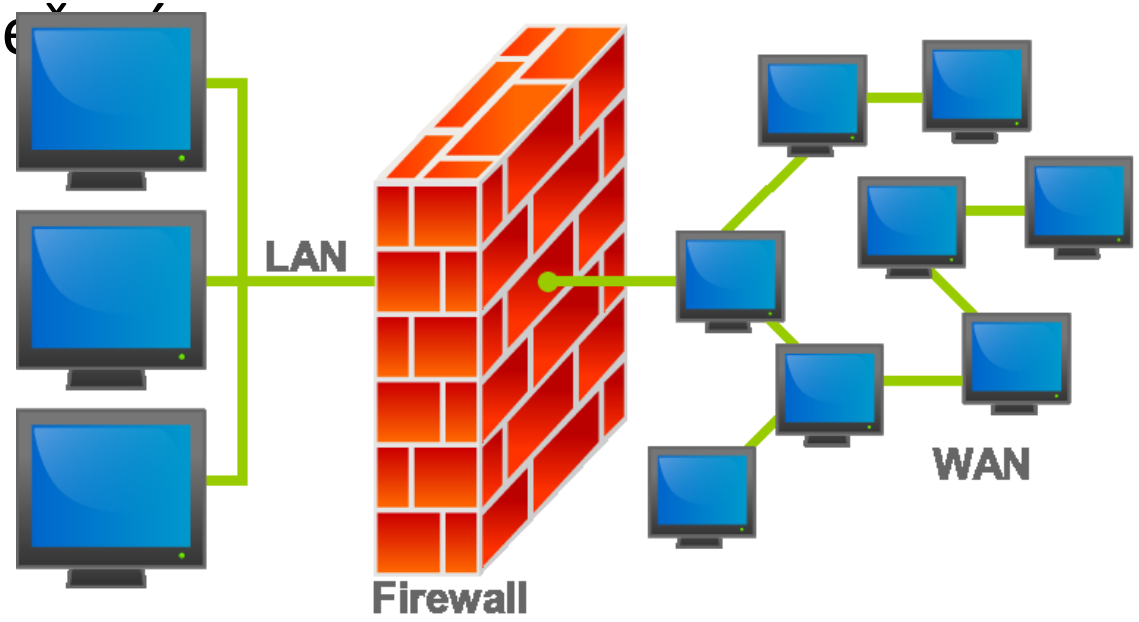
Antispyware

- Blokuje nebo odstraňuje spyware stažený do počítače bez vědomí uživatele.
- Spybot –

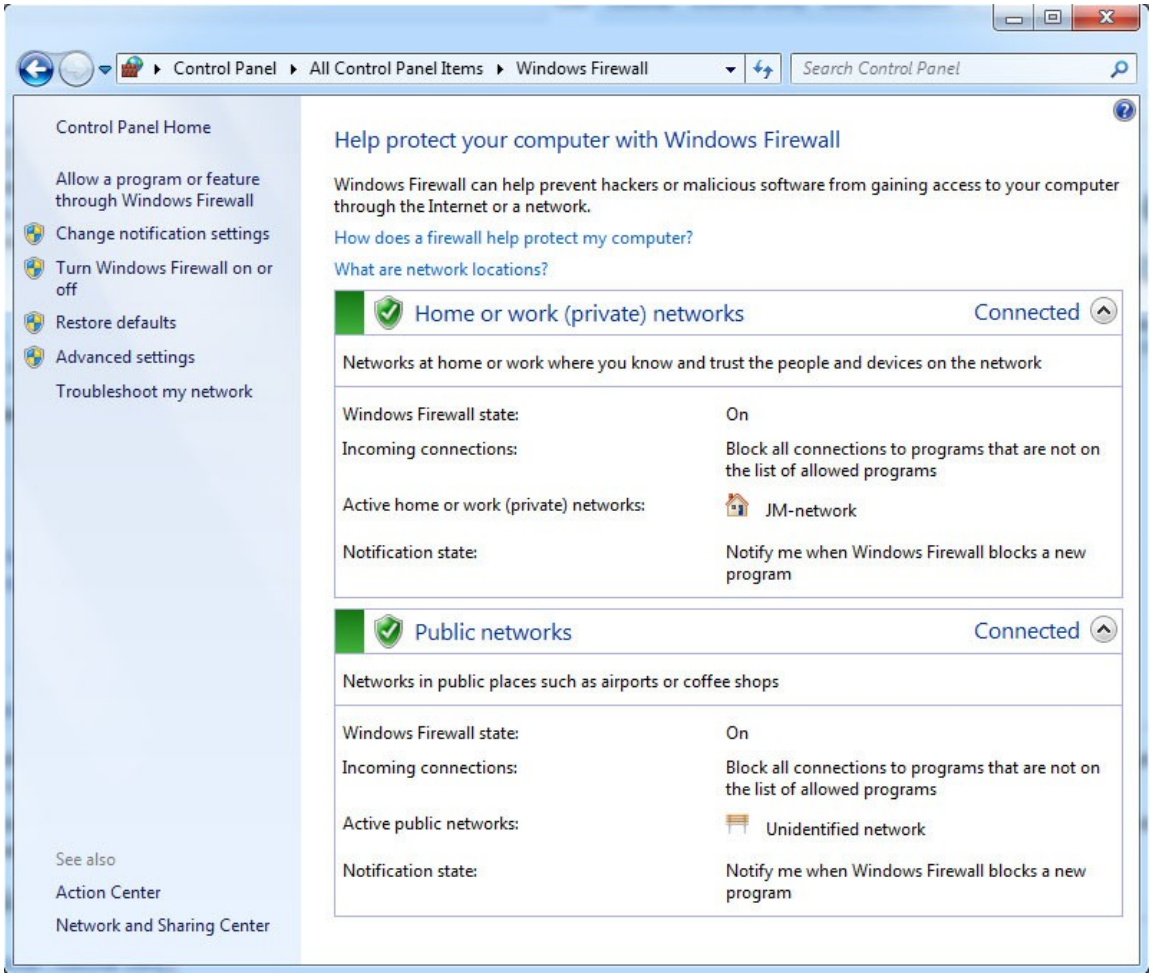


Firewall

- Slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpe



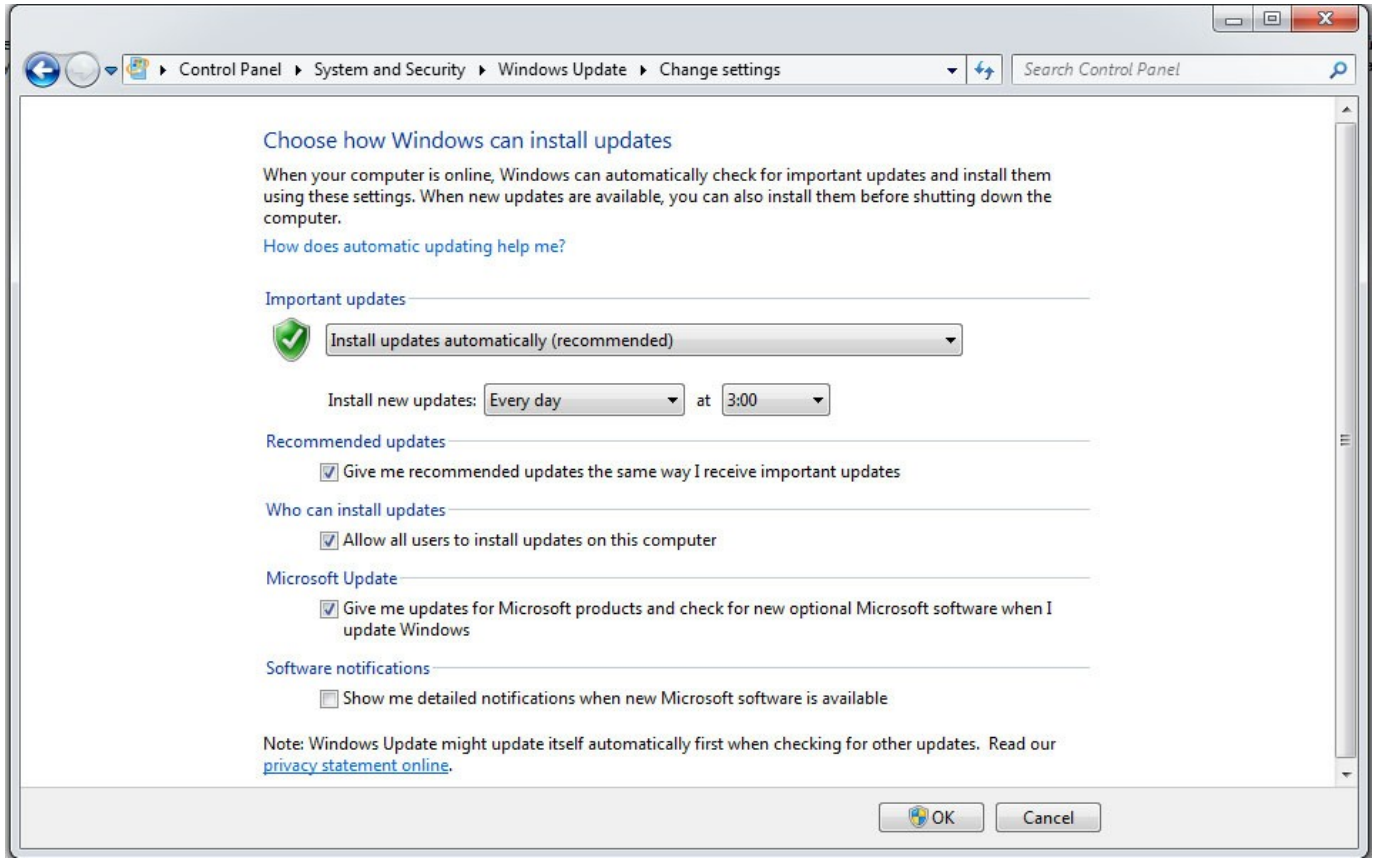
Firewall ve Windows 7



Aktualizace operačního systému a software

- Bezpečnostní díry jsou často terčem pro počítačové viry a hackery.
- Udržujte Vaše programy **aktuální**!
  - Operační systém.
  - Internetový prohlížeč.
  - Další software.
- Aktualizujte pravidelně.
  - Je vhodné nechat software aktualizovat automaticky.

Automatické aktualizace ve Windows 7



Použití běžných uživatelských účtů

- Zabraňuje provádět změny, které mají vliv na všechny uživatele počítače.

ALE navíc:

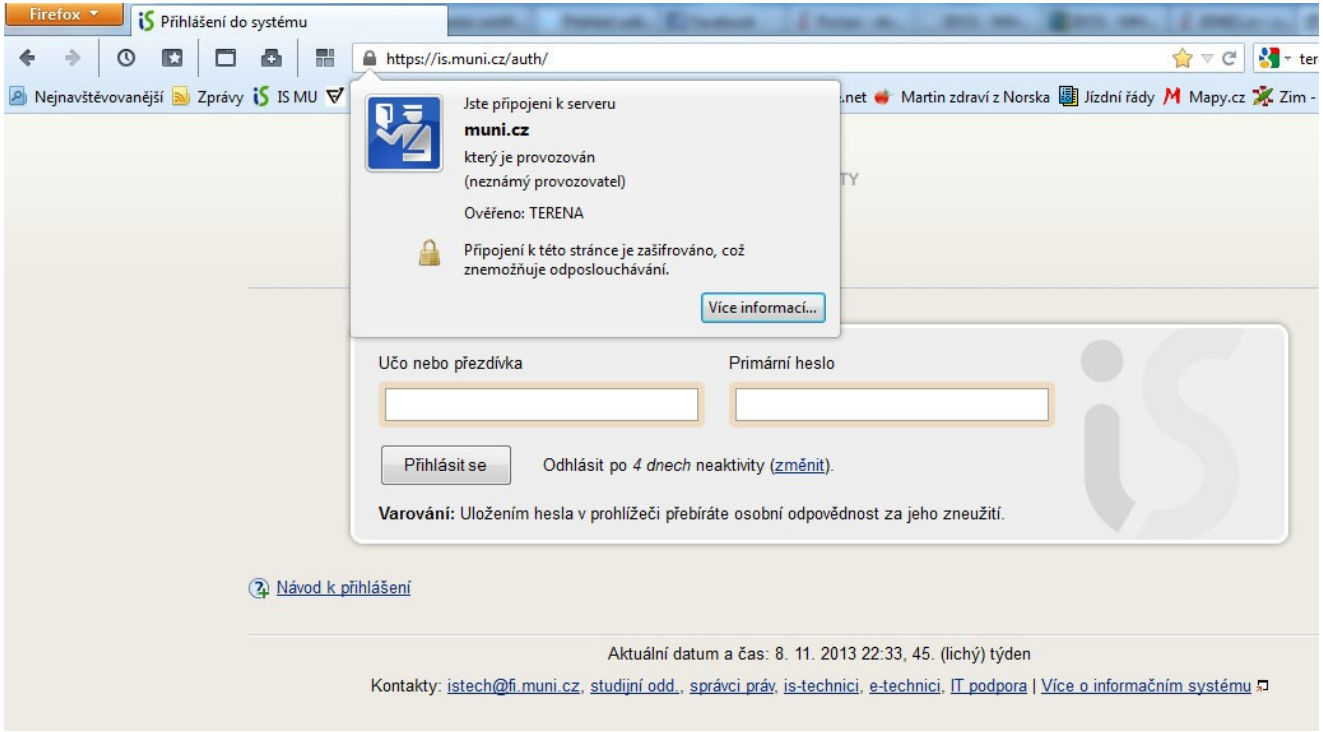
- Zabraňuje či omezuje provádět změny škodlivému software.

Ztráta soukromí na Internetu

- Co jednou dáme Internetu k dispozici již „nejde smazat“.
- Uživatelé si neuvědomují, kolik informací je o nich na Internetu dostupných.
- Profilování pomocí Googlu.
- Veřejně dostupné fotografie.
- Informace v profilech Skype, ICQ, Facebook…
- Falešné profily na Facebooku.

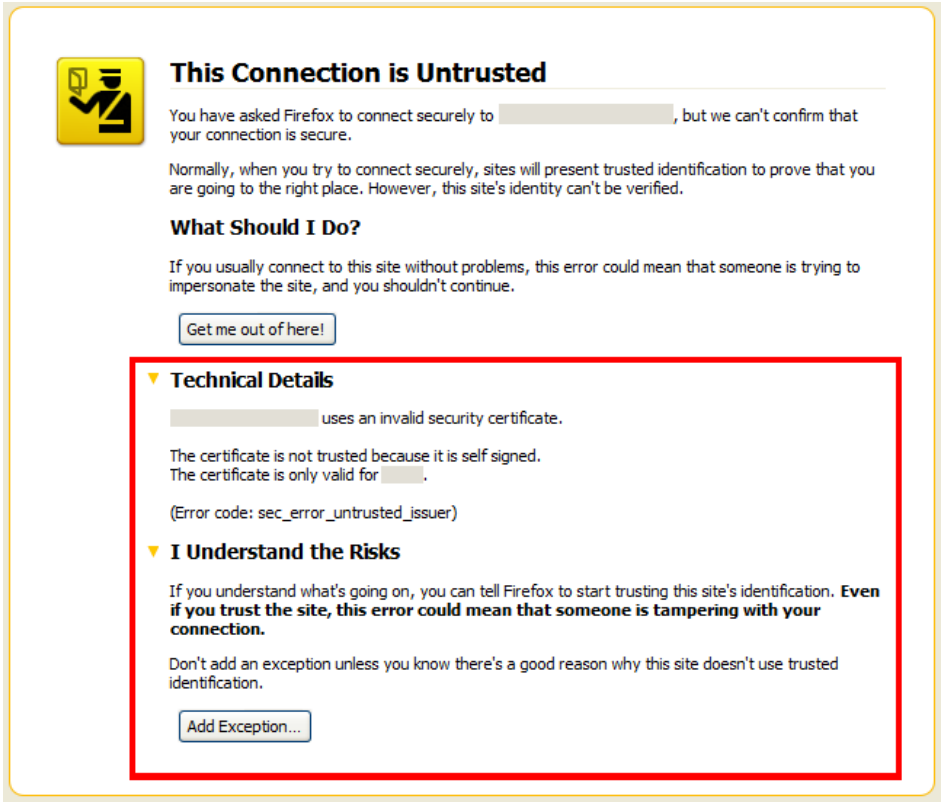
Bezpečné prohlížení webu I

- HTTPS – zajišťuje šifrování obsahu.



Bezpečné prohlížení webu II

- HTTPS – bez důvěryhodného certifikátu.



Bezpečnost e-mailu I

- E-mail využívá protokol, který nezajišťuje nezpochybnitelnou identifikaci odesílatele.
  - Je velice jednoduché se vydávat za někoho jiného.
- Jedině digitálně podepsaný e-mail může zajistit, že:
  - Odesílatelem je skutečně uvedená osoba.
  - Nikdo obsah e-mailu nezměnil.
- Digitální podpis není elektronický podpis!

Bezpečnost e-mailu II

- E-mail využívá protokol, který nezajišťuje důvěrnost na cestě mezi odesílatelem a příjemcem.
- Jedině šifrovaný e-mail může zajistit, že:
  - Obsah e-mailu nečetl nikdo, kdo má přístup k síti.

Bezpečnost e-mailu III

- Pro šifrování a digitální podpis e-mailu existují dvě základní služby.
- Certifikáty podepsané certifikační autoritou
  - První certifikační autorita, a. s.
  - Česká pošta, s. p.
  - eIdentity a. s.
- Certifikáty založené na důvěře („web of trust“).
  - PGP/GPG.
  - Lze integrovat do e-mailového klienta.

PGP

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-2
Version: GnuPG v2.0.17 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

hQEMA+lUtPdWSZi1AQf/WJXb/8Xu2aowCnrvWQ3VZlTU20zMr8PVL2mbqHa7sdkw
4GUNMThcTVv1/l5s5nBBA+P9+3bteuT3Mghr7aF4VFtAQ4pdCsyRQpvA735BEr9Z
Lo/dFCTBrNrBbeF/y0G6e51m62/pzHOPFWzZSZPfAZoiyhlXA3e0ED35fd0p3HHC
lKo647GU+s28KVdaxPJKoG6wDOMq80YA6r9gr1iDtdVcUjrnA1PwWP7gi4hx3qCF
9jQniaMgjS0+s8OsVXW+1O3RnG6s3nWfXIEXcnNoUzqUN+PuBTX/vUjvKmm7uKDx
qUsvBpNK0e6mOP9T2q5ULoZC3Mkx0YrOArxPoCM/wtLAvwGX9yIm8ySJGAmJZlxz
6f8VWt8d6fNlT2a1lmUH4Zvn59KZhQzbyERK9U1LBSBD4x1I3qBEy8AE3t7Q2V+U
znGBrq97rFVgIhCtjwi+5aQ5xtUZfV8LYtweCm5C+dzGcwQrLmZjHepZ8u61gXBG
z2GpbMqPng46YZUbljBkDkFL7Qfcaza52llTLzc+KxEjZXLfNSAJ59LPzt6R2KYX
/kTiFoYdvQx0svx0tM9EalQymwxcmgnXkl9TcG9cBTkhYq5otMOEz7a9UJwOL0Sy
8lK85Ytyj6rZ7uidaUKtVsUF8YCWYwy0nt7Da/lRQ6uFurSMO8Dxx+K2a4EHEM+j
kOMp+eQeUx7b+lZApRycclqXms6NHlq8gZxutGRrD8DJtfaXYbvv9qNN9CW7Xivl
D2NTl41faFD1a5d5jcgvOUzpedWTZsQxfnnEWb1VdBIEN3kGFO6hfiX3TGyz9aGm
pvHMubJdcShTzKDXGufccACBLDo3z3p7vxqGTc7l69ek =rDt2
-----END PGP MESSAGE-----

Internetové bankovnictví

- Používejte ideálně jen ze svého nebo jiného důvěryhodného počítače s aktualizovaným prohlížečem a operačním systémem.
- Kontrolujte zašifrované spojení (HTTPS) a přistupujte jen pokud je certifikát důvěryhodný.
- Používejte dostatečně silná hesla a PINy.
- Neposílejte nikdy svoje hesla, PINy či jiné osobní údaje e-mailem.
- Při zadávání kontrolujte adresní řádek prohlížeče.

Phishing

- Cílem útočníka je vylákat z uživatele citilivé informace.
- Útočník se vydává za cizí identitu a např. rozesílá e-maily obětem pod hlavičkou dobře známé autority (banka, …).
- V e-mailu je umístěn odkaz, který ale ve skutečnosti vede na server útočníka.
- Zadané údaje jsou zaslány útočnikovi namísto bance.

Phishing na Českou spořitelnu I

Předmět: Ceska sporitelna – Pozor! Nove bezpecnostni standardy.
Od: „Ceska sporitelna“ <servise@csas.cz>
Datum: Wed, 11 Oct 2006 14:45:52 –0500

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci. Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku. Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.

S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem. Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu. Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

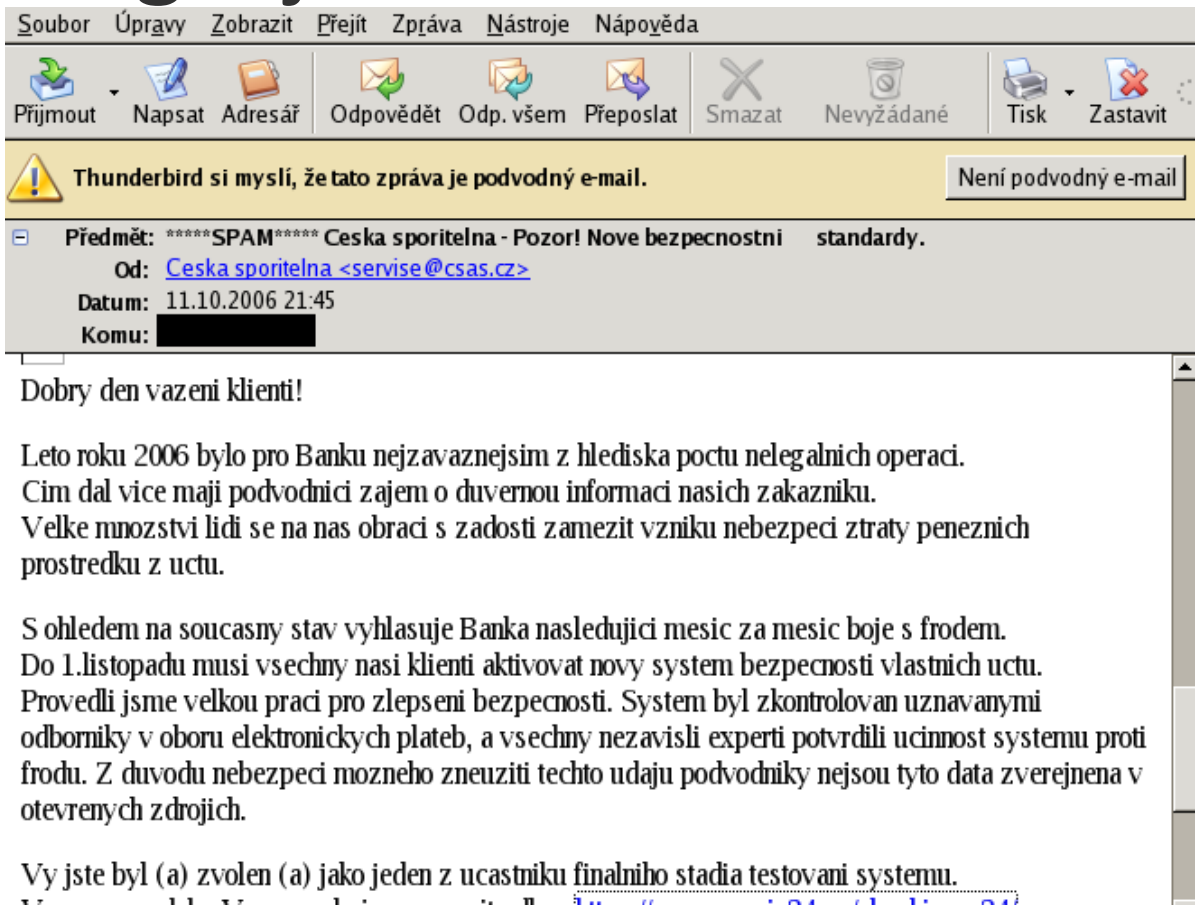
Vy jste byl(a) zvolen(a) jako jeden z ucastniku finalniho stadia testovani systemu. V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.ser-vis24.cz/eban-king-s24/ a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system. V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti. Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.

Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablokovany do okamziku uplne identifikace Vasi osoby. Proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.

S pozdravem, Oddeleni Banky pro ochranu pred frodem.

http://www.root.cz/clanky/cesky-phishing-v-akci/

Phishing – jak se bránit?



Soubor Úpravy Zobrazit Přejít Zpráva Nástroje Nápověda

Přijmout Napsat Adresář Odpovědět Odp. všem Přeposlat Smazat Nevyžádané Tisk Zastavit

Thunderbird si myslí, že tato zpráva je podvodný e-mail. Není podvodný e-mail

Předmět: *****SPAM***** Ceska sporitelna - Pozor! Nove bezpecnostni standardy.
Od: Ceska sporitelna <servise@csas.cz>
Datum: 11.10.2006 21:45
Komu: [redacted]

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci.
Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku.
Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.

S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem.
Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu.
Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci moznehо zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl (a) zvolen (a) jako jeden z ucastniku finalniho stadia testovani systemu.

http://www.root.cz/clanky/cesky-phishing-v-akci/

Phishing na Českou spořitelnu II

http://www.root.cz/clanky/cesky-phishing-v-akci/

Phishing – jak se bránit?

http://www.root.cz/clanky/cesky-phishing-v-akci/

Připojení přes Wi-Fi I

- Při připojení počítače přes veřejnou nezabezpečenou Wi-Fi síť:
  - Může kdokoli ve Vašem dosahu jednoduše odposlouchávat Vaši komunikaci.
  - Pokud není prohlížená stránka zabezpečena protokolem HTTPS, jednoduše mohou být odposlechnuta např. vkládaná hesla a jiná citlivá data.

Připojení přes Wi-Fi II

- Zabezpečení:
  - Pro domácí sítě zásadně používat šifrování pomocí WPA se silným heslem!
  - Pro veřejné sítě – pokud možno, používat protokol HTTPS.
  - Možné využít virtuálních privátních sítí (VPN) – studenti MU mají k dispozici, více informací zde: http://vpn.muni.cz/doku.php.

Kryptografie

- Smysl kryptografie
  - Utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí (znalost klíče).
  - Kryptografie se využívá pro šifrování dat a digitální podpis.
- Důvěrnost dat.
- Integrita dat.
- Autenticita dat.
- Nepopiratelnost.
- Autentizace a autorizace uživatelů a strojů.

Autentizace

- „Něco, co uživatel zná“
  - Hesla, PINy.
- „Něco, co uživatel má“
  - Tokeny, čipové karty.
- „Něco, co uživatel je“
  - Biometriky (otisky prstů, dynamika podpisu, vzor oční duhovky či sítnice, …).

Hesla

- Hesla by měly mít dostatečnou délku a složitost:
  - 8-10 znaků je naprosté minimum.
  - Kombinace velkých a malých písmen, číslic a nealfabetických znaků.
- Je vhodné volit hesla, která jsou:
  - Těžce *uhodnutelná.*
  - Lehce *zapamatovatelná.*
- Náhodně vybraná hesla se obtížně pamatují.
- Doporučuje se používat hesla založená na frázích:
  - Polámal Se Mraveneček, Ví To Celá Obora, O Půlnoci Zavolali
  - **=> psmVTCOo24Z**

PINy

- Nepoužívejte jednoduché, lehce uhodnutelné PINy.
- Pravděpodobnost uhodnutí PINu by měla být: 0,01 %.
- Analýza PINů:
  - http://www.datagenetics.com/blog/september32012/.

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

Čipové karty

- Často ve spolupráci s PINy.
  - Pozor na odpozorování při zadávání.
- Mít kartu při platbách stále na očích.
- Čipové karty
  - Kontaktní.
  - Bezkontaktní.
- ISIC lze zkopírovat!

Biometriky

- Otisk prstu.
- Vzor oční duhovky.
- Vzor oční sítnice.
- Srovnání obličeje.
- Geometrie ruky.
- Verifikace hlasu.
- Dynamika podpisu.
- Dynamika psaní na klávesnici (zadání hesla, …).

Jak můžeme přijít o data?

- Vlivem lidského faktoru:
  - Neúmyslné smazání.
  - Nesprávné používání nebo manipulace.
  - Nedbalost.
- Selháním systému:
  - Výpadky elektrického proudu, přepětí, podpětí.
  - Výpadek operačního systému.
  - Selhání pevných disků.
  - Softwarová chyba.

Jak můžeme přijít o data?

- Úmyslné poškození:
  - Virová nákaza.
  - Krádež.
- Fyzikální a přírodní vlivy:
  - Požár.
  - Voda.
  - Zásah blesku.

Zálohování dat

- Data jen v jedné kopii nikdy nejsou bezpečná.
- Záloha je kopie dat uložená na *jiném* datovém nosiči.
- Existují různá zálohovací software či software pro synchronizaci dat.

Zálohovací média

- Optické disky – CD a DVD.
  - Výhodou je cena.
  - Vypalujeme na kvalitní produkty nízkou vypalovací rychlostí.
  - Zálohy je potřeba obnovovat či duplikovat.
  - Dnes se od CD a DVD pomalu ustupuje.

Zálohovací média

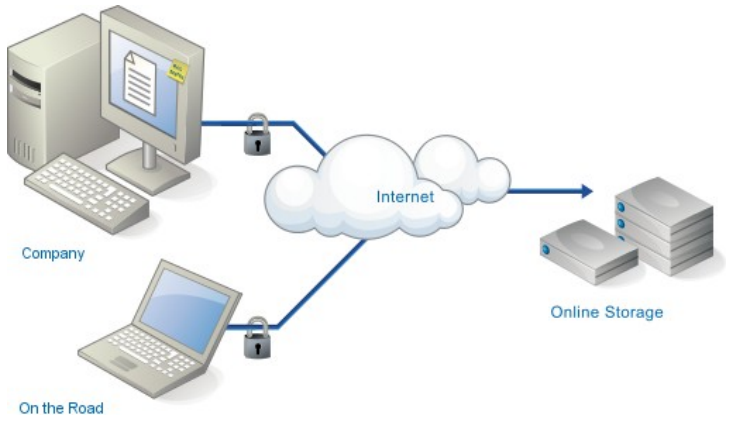
- Pevné disky
  - Zřejmě nejvhodnější zálohování pro domácnosti a jednotlivé uživatele.
  - Uložení velkého množství dat za rozumnou cenu.
  - Rychlý přesun dat.
  - Externí vs. interní disky.
  - Je vhodnější použít externí disky (zejména pro přenosné počítače).

Zálohovací média

- Síťové disky
  - Pevný disk připojený do sítě síťovým kabelem, bezdrátově, přes USB, …
  - Výhodou je umožnění přístupu více uživatelům sítě.
  - Důležité je zabezpečení komunikace a přístup jen autorizovaným uživatelům.
  - Vhodné jako alternativní záloha.

Zálohovací média

- Online zálohování
  - Služba poskytovaná třetí stranou.
  - Možnost si data kdykoliv (při přístupu k Internetu) nahrát na server a zase stáhnout zpět.
  - Nevýhodou je možná nedůvěryhodnost k poskytovateli.
  - Rychlost připojení.



Zálohovací média

- Nevhodné média
  - USB Flash paměti a paměťové karty.
  - Vysoké riziko ztráty dat.
  - Omezený počet zápisů.

Kerchhofův princip

- Síla algoritmu nezávisí na utajení *algoritmu*, ale na utajení a síle tajného *klíče*.
- Algoritmus je veřejně známý.

Literatura

- Zálohování dat
  - http://www.swmag.cz/150/zalohovani-dat/

Zásady tvorby prezentace

Co je a není prezentace?

- Prezentace není PowerPoint!
  - Prezentace nejsou samotné snímky, neměly by říkat vše co chcete říct
- Prezentace není PowerPoint!
  - Software nevytváří prezentaci, prezentaci vyvářite VY
- Prezentace není VÝUKOVÝ MATERIÁL!
  - Prezentace slouží k prezentování, výukový/studijní materiál k (samo)studiu

Prezentace jste VY

- VY vytváříte prezentaci
- VY vedete a řídíte posluchače
- VY určujete téma
- VY vymezujete čas
- VY prezentujete

Rozvržení prezentace

(tradiční i moderní)

- Úvod
- jádro
- ověření
- závěr

Max 10% času, obsahuje představení, obsah, rozvržení cílů, dle typu i hlavní pointu

Asi 70% času (v případě diskuze během prezentace 30-40% času), obsahuje hlavní myšlenky a jejich podložení, struktura dle typu prezentace

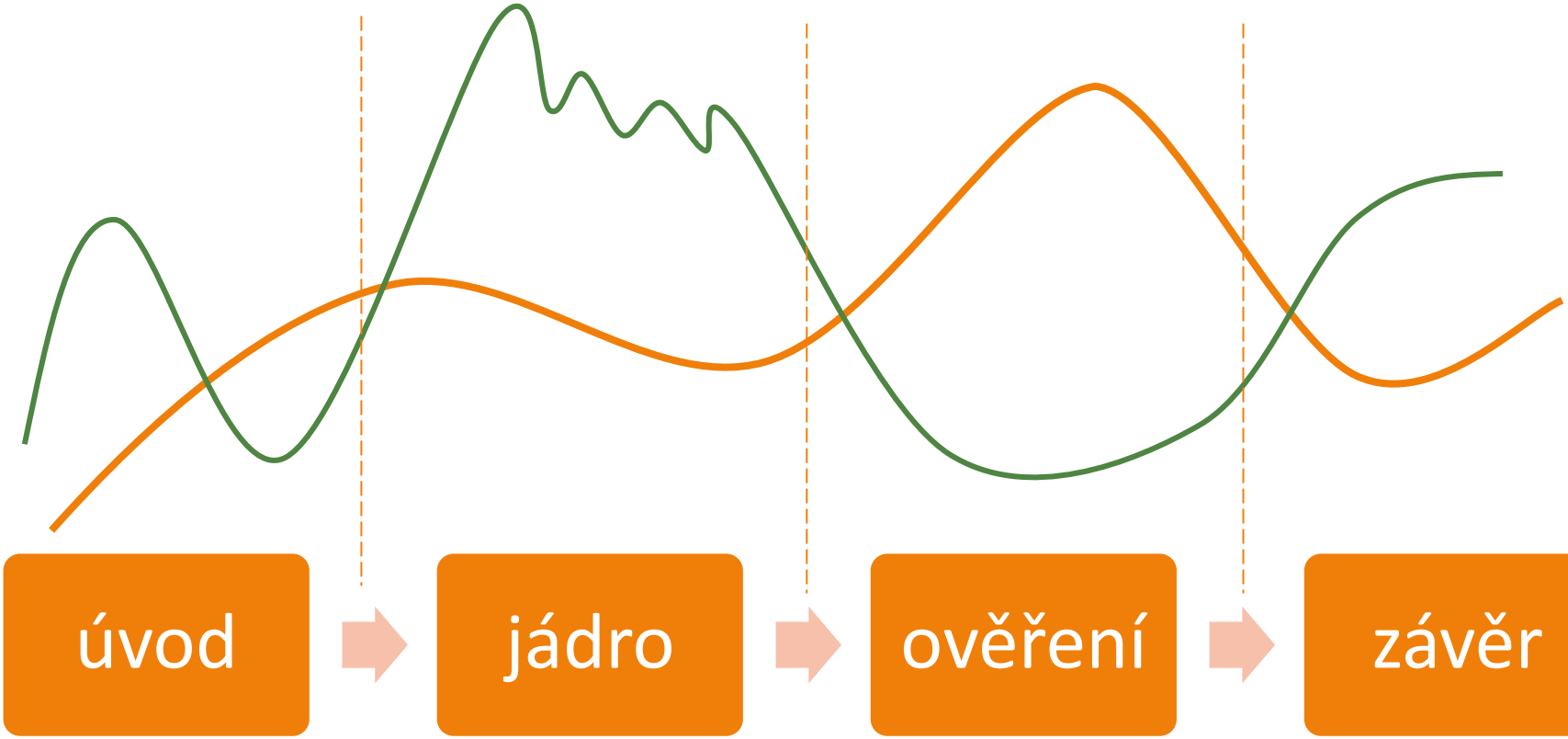
Přibližně 15% času (35-40% času v případě diskuze během prezentace), obsahuje ověření znalostí, úkoly, otázky, shrnutí, apod.

Přibližně 5% času prezentace, závěr je tvořen rozloučením poděkováním, případně připomenutím myšlenky a plány do budoucna

Rytmus prezentace na základě rozvržení

Míra překvapení posluchačů, sdělování nových poznatků a myšlenek (jádro prezentace, popř. „bomba na úvod“)

Míra zapojení účastníků na prezentaci (je závislá na povolení diskuze během prezentace), kulminuje při ověření



Úvod (a představení)

1

Představení se a úvodní projev z velké míry ovlivňuje další vnímání prezentujícího posluchači. **Pokazit první dojem se nevyplácí**.

- Představení se a přivítání
  - Dobrý den. Zdravím. Vítám vás tu.
  - Já jsem. Mé jméno je. Zastupuji zde.
  - Dnes si povíme. Budu hovořit. Moje přednáška.
  - Cestou sem jsem. Chtěl bych vám povědět.

Jak je možné se představit s ohledem na druh prezentace a jak se nepředstavovat?

- Úvodní slovo
  - Připravuje půdu pro hlavní sdělení, které je součástí jádra
  - Vylaďuje publikum pro vnímání tématu a hlavně prezentujícího pro hladký průběh prezentace, navozuje pozornost posluchačů a jejich zájem
  - Vtip, historka, šoková informace k tématu, úvodní otázky k upoutání zájmu a přitáhnutí pozornosti, aktuální informace k tématu
  - **Být vtipný se vyplatí a získá posluchače**

Jádro prezentace

②

Jádro je tvořeno **hlavním sdělením** (informací, vyučovací látkou, představením produktu, …). Hlavní sdělení by mělo vycházet z jasného **cíle prezentace** (naučit, představit, přesvědčit, předvést, …), který je možné podpořit několika dílčími body.

Jedná se typicky o nejdelší část prezentace a obsahuje informace, které by měli posluchači pochytit. Tvrzení je nutné ve většině případů dále potvrdit a podpořit (důkaz, ukázka, příklady, praxe, …)

Dodržujte zásadu **„od obecného ke specifickému“**

- Rétorické postupy
  - „Bomba“ na úvod, která bude dále osvětlena – výhodou je přitáhnutí pozornosti posluchačů
  - Tvrzení
  - Emocionální důkaz (příběh, zkušenost, zážitek)
  - Logický důkaz (statistika, rovnice, …)
  - Opakování pointy (pravidlo tří – třikrát opakovat jinými slovy)
  - Otázky

Ověření

③

Po jádru prezentace by mělo následovat její ověření (jak posluchači rozumí, mají zájem, co je třeba sdělit jinak a lépe)

- Využíváme
  - Diskuze
  - Otázek od prezentujícího  *Jak a kdy klást otázky?*
  - Dotazů od posluchačů
  - Ověření úrovně informovanosti a znalostí
  - (úkoly)

Závěr (a ukončení) ④

Poslední částí prezentace je její závěr a ukončení. Jeho součástí by už neměly být žádné nové informace k tématu, ale kromě rozloučení je možné zařadit i další prvky:

- Stručný odkaz hlavních bodů, zopakování hlavní myšlenky, tvrzení
- Otázka na závěr i k zamyšlení
- Informace do budoucna (další přednáška, více informací)
- Odkazy na přednášejícího, zdroje a literaturu
- Poděkování za pozornost
- Organizační záležitosti
- Rozloučení

3. Příprava prezentace

Kdybych měl osm hodin na pokácení stromu, strávil bych šest hodin broušením sekery (A. Lincoln)

Příprava na prezentaci a její tvorbu

Proč chci něco říct? Jaký je můj záměr a cíl?
Nejpodstatnější bod pro urovnání si myšlenek, důvody a téma prezentace, co je cílem samotné prezentace

- **Kde** bude prezentace probíhat?
  - Načasování začátku, místnost a prostor, prostředí, uvnitř nebo venku, …

- **Co** má být vše sděleno? Co řeknu?
  - Hlavní body a myšlenky sdělení, tvrzení

- **Ke komu** budu hovořit? Kdo jsou posluchači prezentace?
  - Vztah k posluchačům – podřízený, nadřízený, učitel.
  - Znalosti posluchačů vztahující se k témat prezentace
  - Jaká je motivace posluchačů
  - Jaká jsou jejich očekávání

- **Jak** informace sdělím, aby druzí přijali cíl mé prezentace?
  - Podpoření tvrzení, úroveň detailů sdělení, způsob komunikace, ověření a vysvětlení

- **S kým** a **čím** bude prezentace prováděna?
  - Závislost na materiálních prvcích a osobách
  - Prezentace ve více lidech
  - Technické vybavení, pomůcky
  - Forma podkladů na prezentaci (PowerPoint, Multimédia, …)

- **Kdy** bude prezentace probíhat a **Jak** bude dlouho trvat?
  - Přizpůsobení se době a délce určeného času
  - Délka možné přípravy

V čem připravit a přinést podklady na prezentaci

V závislosti na vybavení z předchozího snímku je možné (a většinou vhodné) připravit si podklady pro prezentaci na PC (např. PowerPoint). V případě, že nebude na místě PC je nutné přizpůsobit formu podkladů dostupnému vybavení

Možnosti

- PowerPoint
- Word, PDF
- Webová prezentace
- Videoprezentace
- Papírové podklady
- Podklady pro posluchače
- Průsvitky
- …

Doporučujeme přinést elektronické podklady pro prezentaci alespoň 2x (různé formáty, média)

Multimédia

Cílem využití multimédií je zapojení co nejvíce smyslů posluchačů:

- Uši, Oči, Ruce, Ústa druhých

Multimédia

Statické prvky
- text, schémata, grafy, prezentace

Dynamické prvky
- animace, interaktivita, videosekvence, zvuk a hudba, online aplikace, verifikační a validační aparát

Asi 80 % informací a podnětů vnímají lidé zrakem, asi 12 % sluchem -> disproporce s tradičním vzděláváním, tu je možné odstraňovat zapojením prezentací s multimédii

Jakým způsobem můžeme zapojit více smyslů?

5. Zásady prezentace v PowerPointu

Jak by měla vypadat prezentace?

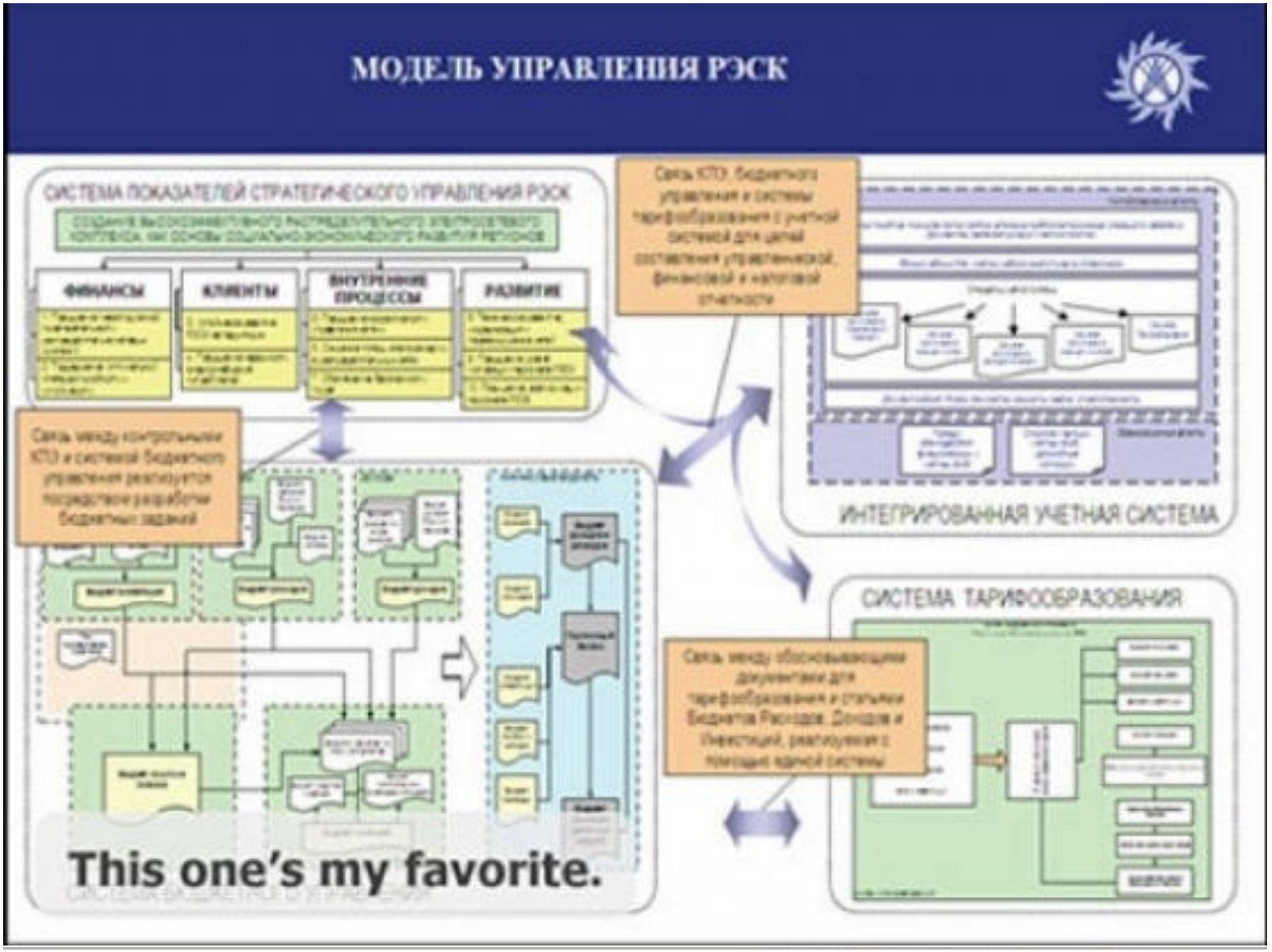
Doporučení pro tvorbu prezentací I

- **Jednotný vzhled prezentace** –jednotný styl celé prezentace, upravenost a ucelenost (výjimkou může být první a poslední snímek nebo vložené prvky, např. videa, odkazy)
- **Srozumitelné efekty** – umístění efektů „tam, kde mají smysl“ a vhodného typu
- **Vytvářejte jednoduchou stránku** (ne chaos). Celá stránka (snímek) musí být přehledný – méně je někdy více
- **Omezte přechody** pro ozvláštnění prezentace (jen na důležité snímky)

Co umístit do zápatí snímků?

- Používejte **předlohu** (šablonu) a **zápatí** snímků
- **Pozadí** volte tak, aby se text neztrácel, nevhodné jsou různobarevná pozadí, obrázková pozadí i výrazné přechody

Jak by prezentace vypadat neměla… I



Doporučení pro tvorbu prezentací II

- Raději volte **pastelové barvy** (ne příliš ostré či šedivé).
- Používejte **kontrastní barvy** pro text a pozadí a vhodné **barevné kombinace** (uvědomte si, že zobrazení na projektoru bude vypadat jinak, než při tvorbě na monitoru – jas, kontrast, světlo v místnosti, …)
- Obvyklá vhodná velikost textu je **24 bodů** a větší (v závislosti na místnosti a plátně)

Jaký je rozdíl mezi prezentací a distančním studijním materiálem?

- Pro sdělení zprávy **používejte krátké věty nebo odstavce –** prezentace v PowerPointu je „jen“ podporou pro samotné prezentování
- Do prezentace můžete přidat **hypertextové odkazy mezi snímky**, možnost nelineární prezentace působí zajímavěji a umožňuje interaktivitu!
- Na konci prezentace **shrňte celou problematiku, otázky (oboustranně), poděkování**
- **Vyzkoušejte si předvádění „nanečisto“ !**

Jak by prezentace vypadat neměla… II

US Wireless Market – Q2 2010 Update

Executive Summary

The US wireless data market grew 6% Q/Q and 22% Y/Y to exceed $13.2B in mobile data service revenues in Q2 2010 - on track so far to meet our initial estimate of $54B for the year.

Having narrowly edged NTT DoCoMo last quarter for the first time, Verizon Wireless continued to maintain its number one ranking for the 1H 2010 in terms of the operator with the most mobile data revenues (though the difference was thinner than the amoeba membrane). The total wireless connections for Verizon were almost 100M with 92.1M being the traditional subscriber base. Rest of the 3 top US operators also maintained leading positions amongst the top 10 global mobile data operators.

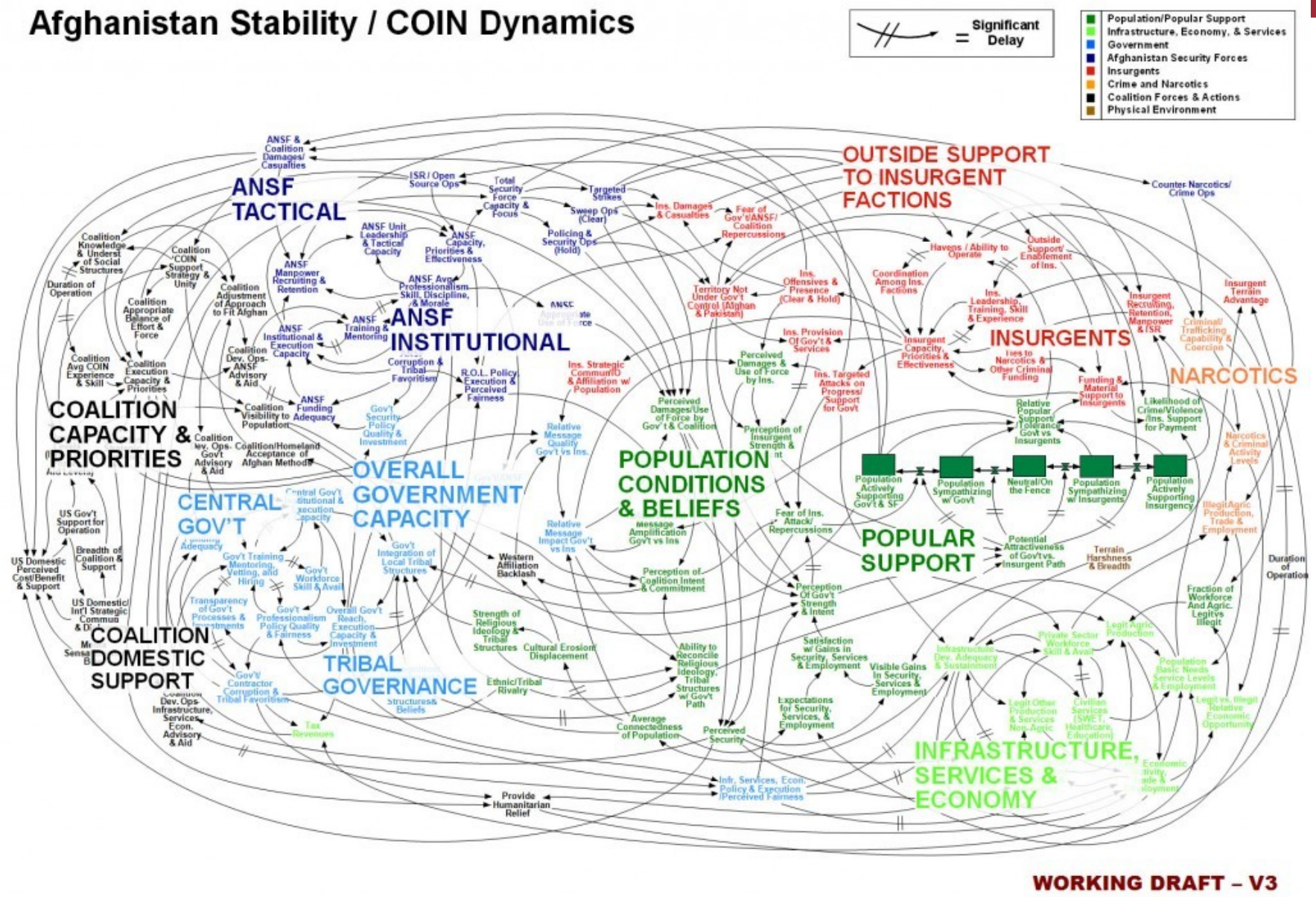
Sprint had the first positive netadd quarter in 3 years and has been slowly and steadily turning the ship around. T-Mobile did better on the postpaid netadds but overall additions declined again. The larger question for the market is if 4 large players can stay competitive. Generally, the answer is no. But these are different times and there are a number of permutations and combinations that are possible.

The US subscription penetration crossed 95% at the end of Q2 2010. If we take out the demographics of 5 yrs and younger, the mobile penetration is now past 100%. While the traditional net-adds have been slowing, the "connected device" segment is picking up so much that both AT&T and Verizon added more connected devices than postpaid subs in Q2 2010. Given the slow postpaid growth, operators are fiercely competing in prepaid, enterprise, connected devices, and M2M segments.

Data traffic continued to increase across all networks. By 1H 2010, the average US consumer was consuming approximately 230 MB/mo up 50% in 6 months. US has become ground zero for mobile broadband consumption and data traffic management evolution. While it lags Japan and Korea in 3G penetration by a distance, due to higher penetration of smartphones and datacards, the consumption is much higher than its Asian counterparts. Given that it is also becoming the largest deployment base for HSPA+ and LTE, most of the cutting edge research in areas of data management and experimentation with policy, regulations, strategy, and business models is taking place in the networks of the US operators and keenly watched by players across the global ecosystem.

As we had forecasted, the tiered pricing structure for mobile broadband touched the US shores with AT&T becoming the [illegible]jor operator to change its pricing plan based on consumer consumption. We will see the pricing evolve over the [illegible] quarters as the US mobile ecosystem adjusts to the new realities and strategies for mobile data consumption.

Afghanistan Stability / COIN Dynamics



WORKING DRAFT – V3

Text v prezentaci

- Velké – doporučuje se používat velikost 24, nevhodná je velikost menší než 16
  - 32b 24b 16b
- Několik bodů, definice, důležité texty,
- Výstižně, jasně a stručně
- Maximálně 3 úrovně osnovy
- Jednotný font i barva pro nadpisy, a text stejného významu
- Hypertext
- Číslování stránek
- Na vhodných místech nahrazovat text grafickými prvky. Ty podporují lépe zapamatovatelnost i poutají pozornost

Pozadí

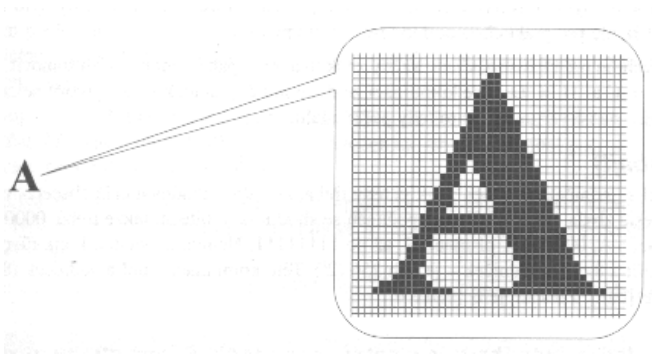
- Nechaotické – pozadí by nemělo narušovat čitelnost informací, pozor na vzory, přechody, výrazné obrázky
- Vhodná je jedna barva
- Grafické prvky nenarušující vzhled prezentace

Odrážky

- Různé úrovně – odlišení odrážek
- Přiměřené velikostí i barvou
- Číslování vs. odrážky

Obrázky a diagramy

- Přehledné a jasně čitelné, jednoznačného významu (popř. opatřit vhodným komentářem)
- Postupné načítání diagramů pro přehlednost
- Rozlišení
- Komprese



Animace

- Ne po písmenech či slovech, ale po bodech nebo logických blocích (výjimky?)
- Vhodný efekt
- Vhodné využití

Následky špatné prezentace

Jak tedy ANO?

Stručné shrnutí základních zásad

Garr Reynolds. Presentation Zen: Simple ideas on Presentation Design and Delivery

Buďte vypravěčem příběhu

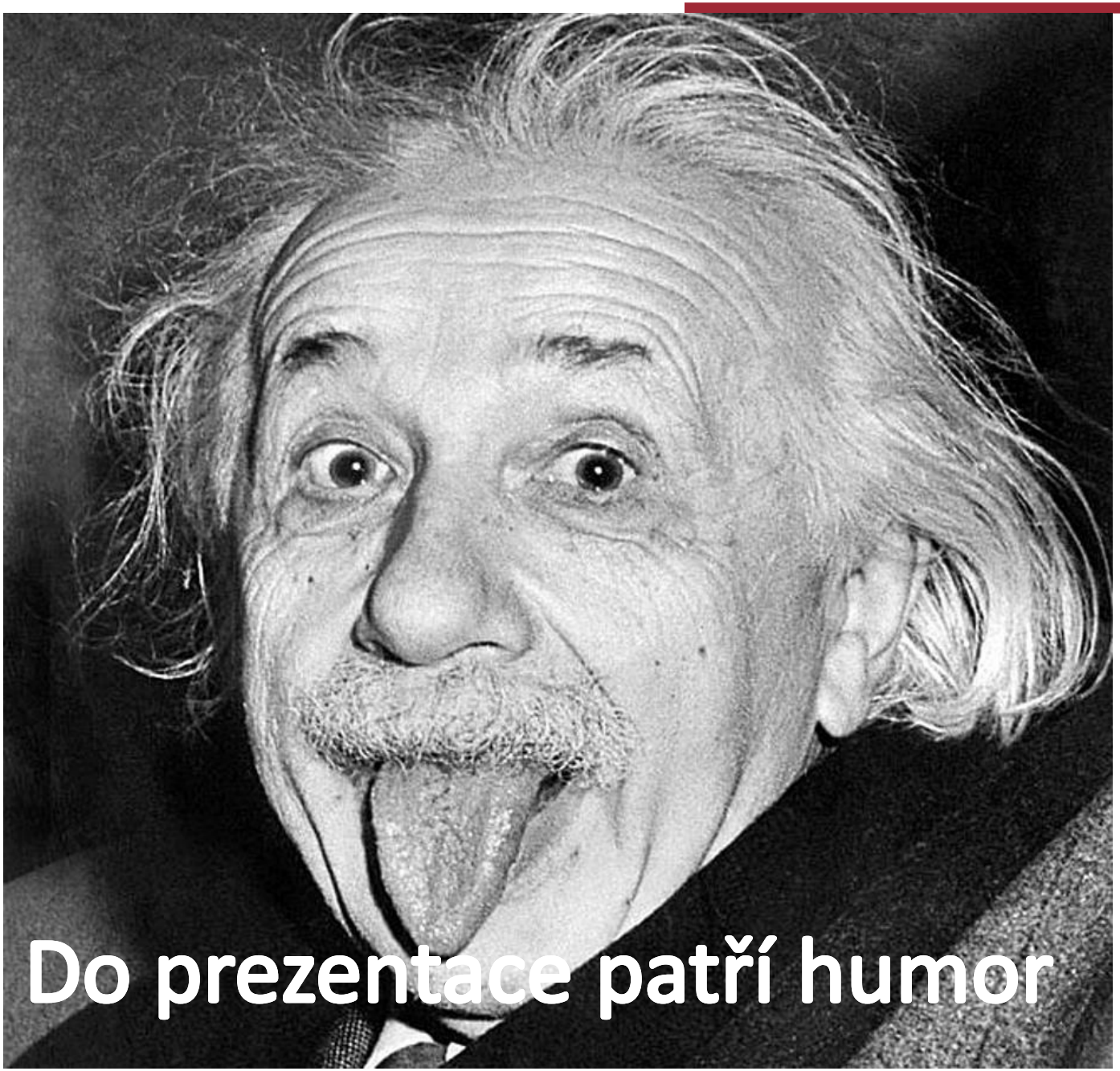
Nechte obrázky vyprávět příběh

Využívejte vizualizací a obrázků

Méně než 7 slov na snímku

Prázdná místa zesilují vizuální vjem

Používejte celosnímkové obrázky, ale NE na úkor čitelnosti


Do prezentace patří humor

Vyhněte se odrážkám

(bullet points)

Dejte pozor na sladění barev textů a pozadí

Dejte pozor na sladění barev textů a pozadí

Dejte pozor na sladění barev textů a pozadí

Dejte pozor na sladění barev textů a pozadí


Používejte jednoduché fonty
Arial
Impact
Calibri
Gill Sans
Vyhněte se ozdobným a obtížně čitelným fontům

Nebuďte nuceni
číst body ze snímků

Procvičujte a trénujte před samotnou prezentací

A co všechny detaily?

Výuková prezentace má svá specifika a většinou obsahuje více informací

Prezentace může odkazovat na příklady, cvičení, pracovní sešity, skripta, apod…


Inspirujte se a učte se od profesionálů…

Trocha čísel…

95 % prezentací je nudných

Ukažte snímek

14 – 21 sekund

předtím, než o něm budete hovořit

Jeden snímek by měl trvat

40 – 90 sekund

maximálně

Každé **3 – 4 minuty**

zvyšte pozornost posluchačů vhodnou technikou

Přímé náhrady PowerPointu

- **Impress (OpenOffice.org, LibreOffice)**
- **Google Presentation (Google Docs)**
  - **http://docs.google.com**
- **MS PowerPoint Web App**
  - **http://skydrive.live.com**
- **Prezi**
  - **http://prezi.com/**
  - **Prezentace je vytvářena na jediné ploše a při prezentování se přelétá mezi prvky**
- **SlideRocket**
  - **http://www.sliderocket.com/**
  - **Webová obdoba Powerpointu**
- **ZOHO Show**
  - **http://www.zoho.com/show/**
  - **Online tvorba prezentací i jejich export (po registraci)**

Alternativy

- **Apple iWork Keynote**
  - http://www.apple.com/cz/iwork/keynote/
  - **Kompatibilita s ppt, pdf, …**
- **Proshow Gold**
  - http://www.photodex.com/proshow/gold
- **Adobe Captivate**
  - **Tvorba interaktivních prezentací a e-learning obsahu, včetně sw simulací a testování znalostí**
  - http://www.adobe.com/cz/products/captivate.html
- **Screenr, Wink**
  - **Online záznam činnosti na obrazovce, tentýž princip jako desktop aplikace**
  - http://www.screenr.com/
  - http://www.debugmode.com/wink/

Hardcore alternativy

Některé vybrané profesionální programy pro tvorbu prezentace formou profesionálních animací a videa

- **Adobe After Effects**
  - **video, 3D, fota, střih, zvuk, efekty, …**
- **3D studio MAX, Cinema 4D, …**
  - **3D aplikace**
- **Nuke, Final Cut, Shake, …**

Sdílení prezentací

- **Present.me**
  - **Sdílení PowerPoint a PDF prezentací**
  - **Import + video/audio komentáře**
  - **http://present.me/**

- **Slideshare**
  - **Sdílení prezentací, dokumentů a videí**
  - **http://www.slideshare.net/**
  - **Velký výběr prezentací**

Výukové LMS/CMS systémy

- **Drupal**
  - Content management system
  - http://www.drupal.cz/
  - http://drupal.org/
- **Joomla**
  - CMS
  - http://www.joomlaportal.cz/
  - http://www.joomla.org/
- **WordPress**
  - CMS, blog, RS, …
  - http://wordpress.org/
- **Open Journal Systém (OJS)**
  - Publikační systém a řízení časopisů
  - http://pkp.sfu.ca/?q=ojs
- **Moodle**
  - Rozšířený LMS systém
  - http://moodle.cz/
- **Survs**
  - Online tvorba výzkumů a průzkumů
  - http://www.survs.com/
  - Obdoba např. vyplnto.cz
- **Basecamp**
  - Project management software
  - http://basecamp.com/

Literatura a zdroje

Hospodářová, Ivana. Prezentační dovednosti. Alfa Publishing, Praha 2004. isbn 80-9039-629-6

Hierhold, Emil. Rétorika a prezentace -- Jak s jistotou prezentovat a působivě přednášet - 7., aktualizované vydání, Grada 2008, isbn 978-80-247-2423-2

Harvey, Christine. Jak vystupovat na veřejnosti a získávat důvěru posluchačů. Management Press, 1994. isbn 80-85603-69-1

Černý, Vojtěch. Rétorika pro obchodníky i běžný život. Edika, 2011. isbn 9788025130520

Bradbury, Andrew. Jak úspěšně prezentovat a přesvědčit. Bizbooks 2007. isbn 9788025116227

Bělohlávková, Věra. 33 rad jak úspěšně prezentovat. Computer Press, Brno 2004, isbn 80-251-0326-9

Nöllke Claudia. Umění prezentace – Jak přesvědčivě, srozumitelně a působivě prezentovat. Grada Publishing, Praha 2004, isbn 80-247-9057-2

Měchurová Albína. Jak dobře mluvit a úspěšně jednat – Základy rétoriky a komunikace. Univerzita Jana Amose Komenského, Praha 2008, isbn 978-80-86723-32-7

MotivP. Kurz Prezentační dovednosti. Agentura MotivP, 2009.

Programový tým projektu EQUAL 0076. Celoživotní vzdělávání v komunitním plánování. Modul 11 Komunikace, řešení konfliktů a mediace. EQUAL 0076, Centrum komunitní práce Ústí nad Labem

Zdroje

- **Použité webové zdroje:**
- http://www.uloz.to/x9UwsRm/2010-04-14-prezentacni-dovednosti-doc
- http://www.uloz.to/xnB6jmW/modul-c-2-prezentacni-a-komunikacni-dovednosti-pdf
- http://rossrightangle.files.wordpress.com/2011/07/bomb01.jpg
- http://3.bp.blogspot.com/_9gn6KLa5xtY/RrimkRTnubI/AAAAAAAAAss/YeUVMfwZ_gA/s400/BatBoy3.jpg
- http://www.ljcreate.com/products/img/st80sci_srs.jpg
- http://technet.idnes.cz/bezec-oscar-pistorius-s-protezou-dq9-/tec_technika.aspx?c=A120803_131005_tec_technika_mla
- http://technet.idnes.cz/rusky-proton-nedoletel-0v9-/tec_vesmir.aspx?c=A120807_181717_tec_vesmir_vse
- http://ilgresults.com/wp-content/uploads/2010/02/Question-mark-in-blue.jpg
- http://cs.wikipedia.org/wiki/Multim%C3%A9dia
- NOCAR, David. *E-learning v distančním vzdělávání.* 1. Vyd. Olomouc : Univerzita Palackého, 2004. 77 s. ISBN 80-244-0802-3
- MOORE, Michael. G. Editorial: three types of interaction. *The American Journal of Distance Education*, 1989 3, 1–6.
- WAGNER, J. *Nebojme se eLearningu* [online] Česká škola, 2005 [cit. 2011-06-04]
- MASON, Robin a Frank RENNIE. *Elearning: The Key Concepts.* Vyd. 1. Abington: Routledge, 2006. 158 s. ISBN 0-415-37307-7
- http://www.eamos.cz/amos/zsrudolfovska/externi/zsrudolfovska_783/dpi.png
- http://www.johnhpanos.com/jpeg.jpg
- http://randomoverload.net/wp-content/uploads/2009/11/ba49498c6drpoint.jpg.jpg
- http://lh6.ggpht.com/-pzCwVtRAJLo/T16-yZJ-aPI/AAAAAAAAA-8/ls5kRH1uezs/death-by-powerpoint%25255B8%25255D.jpg
- http://cs.wikipedia.org/wiki/Neverb%C3%A1ln%C3%AD_komunikace
- http://attachments.conceptart.org/forums/attachment.php?attachmentid=529915&stc=1&d=1227942979
- http://f00.inventorspot.com/images/printedhug.img_assist_custom.jpg
- Birdwhistell, R. 1970. *Kinesics and Context.* University of Pennsylvania Press, Philadelphia.
- http://intercommwinter11.blogspot.cz/2011/02/kinesics-jandt-119.html
- http://stallonezone.com/imgs/news/2007/011507sly_gestures.jpg
- http://img.ibtimes.com/www/data/images/full/2010/05/06/7925-u-s-president-barack-obama-gestures-as-he-speaks.jpg
- http://www.gesture.com/body_language.jpg
- http://www.dgps.de/fachgruppen/methoden/mpr-online/issue4/art3/img4.gif
- http://images.sciencedaily.com/2009/08/090813142131-large.jpg
- http://citelighter-cards.s3.amazonaws.com/p1730clni11hdg5alid1u1qd5a0_42685.png
- http://www.lepsi-firma.cz/neverbalni-komunikace-prezentace
- http://nonv2ttu.files.wordpress.com/2011/12/personal-space.jpg
- http://www.tiesncuffs.com.au/blog/wp-content/uploads/man-dressed-for-black-tie-event.jpg
- http://media.novinky.cz/161/221617-original1-e9xgn.jpg
- http://www.ikoss.cz/images/thb_view/22-shutterstock_55310137.jpg
- http://www.uspesnaprezentace.cz/vystupovani-a-forma/
- http://www.flickr.com/photos/janettowbin/3472292148/sizes/l/in/photostream/
- http://www.flickr.com/photos/rockersdelight/6285751053/sizes/l/in/photostream/
- http://harryneelam.com/photoblog/wp-content/uploads/2012/04/Einstein.jpg
- http://www.wallchan.com/images/sandbox/14934-colt-python-gun-bullet.png
- http://www.charlesrussell.co.uk/UserFiles/image/blackboard-with-chalk.jpg
- http://www.flickr.com/photos/43659079@N03/5569862071/sizes/l/in/photostream/
- http://www.vzdelavacifilmy.cz/userdata/products/16/steve-jobs.jpg
- http://i.lagardere.cz/evropa2/img/content/blog/pavelc/nuda.jpg
- http://obrazky.superia.cz/nahled-velky/presypaci_hodiny.png
- http://sranda.kdecoje.cz/obrazek/student.jpg
- http://www.globalwarmingisreal.com/wp-content/uploads/2010/09/No-button.jpg
- http://www.uspesnaprezentace.cz/vystupovani-a-forma/

Prezentace jako učební pomůcka

Tvorba učebních pomůcek

Tvorba a využití učebních pomůcek prostřednictvím didaktických technologií:

- ve školní výuce
- při zájmových výukových činnostech
- v době mimo vyučování.

Co je učební pomůcka

- Učební pomůckou rozumíme takový materiální didaktický prostředek, který má při použití ve výuce přímý a bezprostřední **vztah k učivu** a zejména k výukovým cílům, k jejichž dosažení má učební pomůcka napomoci.

K čemu slouží učební pomůcka?

Učební pomůcky jsou využívány ve výuce jako:

- zdroje informací,
- prostředky řízení výuky,
- prostředky kontroly výuky,
- prostředky pro rozvoj dovedností i schopností žáků,
- prostředky motivační.

Forma využití učební pomůcky?

- Učební pomůcky jsou nepostradatelnou skupinou pomůcek, které umožňují vykonávání různých činností ve výukovém procesu :
- hry,
- učební činnosti,
- práce a činnosti ve volném čase

Co musí obsahovat?

- Popis a úplnou fotografickou dokumentaci učební pomůcky (je dáno povahou pomůcky),
- informace, pro který studijní nebo učební obor,
- pro který ročník je určena,
- pro který tematický celek učiva je učební pomůcka určena.

Výukový cíl

- Dále musí být uveden **výukový cíl**, k jehož dosažení je pomůcka vytvořena,
- navrhovaná výuková metoda a
- předpokládaný nebo ověřený výsledek výuky s nově vytvořenou učební pomůckou.

Zadání seminární práce

- Vytvořte učební pomůcku v programu **powerpoint** v rozsahu **minimálně 12 slidů.**
- Tematicky bude prezentace zaměřena na některý z předmětů 1. nebo 2. stupně ZŠ, který koresponduje s RVP.
- Prezentace bude obsahovat obrázky, fotografie a text a bude uvedeno pro který ročník a předmět je tato učební pomůcka určena.

Forma a termín odevzdání

- Prezentace bude odevzdána elektronicky do odevzdávárny IS jaro 2020 v IS MU
- Termín odevzdání do 15.6. 2020