Uživatel v síti

- Internet je globální, podléhá ale lokálním vlivům
  - zákony
  - regulační opatření
  - etika
  - kulturní zvyklosti
  - jazyková specifika
  - kupní síla
- vzniká řada problémů dříve nebývalých

Netiketa (1)

- pravidla slušného chování pro uživatele (e-mail, diskuse, blogy apod.)
  - adresátem Vašeho sdělení je člověk, nikoli stroj
  - berte na něj ohled
- technika odlidšťuje, adresát sdělení je nepřímý, svádí k agresivitě a vulgaritě
- obecné pravidlo:
  - **nepište do mailu apod. něco, co byste adresátovi nebyli ochotni říci do očí**

Netiketa (2)

- dodržuje v elektronické komunikaci stejná pravidla, jako v běžném životě
- nebuďte zbytečně útoční či agresivní
- ostatní mají své názory a povinnosti, nečekejte, že s vámi každý bude souhlasit a okamžitě reagovat na vaše podněty či požadavky
- ve sporu argumentujte k věci, nepoužívejte osobní invektivy

Netiketa (3)

- šetřete ostatním čas
  - buďte struční, pište k věci a omezujte balast
  - snažte se jasně vyznačit téma svého příspěvku
  - pokud odpovídáte, ponechte z původní zprávy jen relevantní části
  - než pošlete velký objem dat, ověřte si, že adresátovi nezpůsobíte problém
  - komprimujte data
  - nepřeposílejte nesmysly

Netiketa (4)

- než se zeptáte, zkuste se porozhlédnout po odpovědi (máme Google a další) – opakované dotazy zkušené uživatele dráždí
- naopak poraďte, pokud můžete
- nezneužívejte svou moc (nadstandardní přístupová práva) či vědomosti
- respektujte soukromí ostatních
- snažte se být tolerantní

Anonymita v Internetu

- uživatelé jsou do značné míry anonymní
- pseudoanonymita
  - diskusní příspěvky bez registrace
  - účty na veřejných mailových službách (Seznam, Google apod.) získané bez prokázání totožnosti
  - totožnost diskutujícího lze vysledovat (IP adresy a další indicie)
- anonymizační služby
  - cílem je naprostá nezjistitelnost uživatele
  - pro e-mail, web a další služby

Klady a zápory anonymity

- **klady**
  - svobodné vyjádření bez obavy z postihu
  - ochrana soukromí
- **zápory**
  - beztrestnost svádí k vulgaritě, agresivitě
  - usnadňuje nelegální aktivity

Na hraně – k zamyšlení

Jaký je váš názor na dotaz

„Je Václav Klaus žid?“

v diskusi pod článkem k prezidentské volbě?

Diskuse a anonymové

- anonymní příspěvky často diskusi znehodnocují (viz libovolná diskuse k prezidentské volbě)
- možná řešení:
  - **nechat být**, případně doporučení vhodného chování (kodex diskutujícího)
  - umožnit diskutovat **jen registrovaným** – pseudoanonymita, uživatelé si udržují identitu
  - **moderovaná diskuse** – mazání nevhodných příspěvků, zákazy uživatelů porušujících pravidla
  - **zrušení diskuse**

Ochrana soukromí

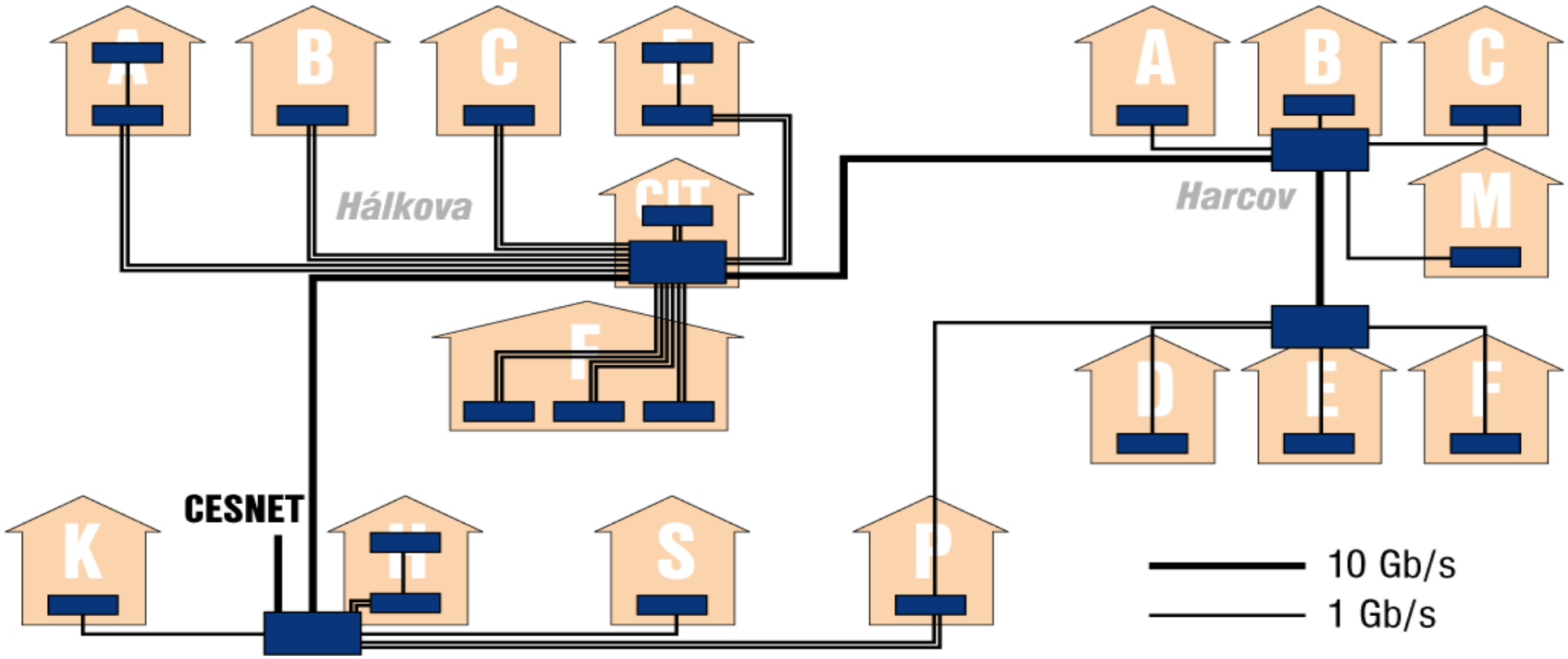
- **přímé hrozby**
  - **spyware** – sleduje uživatelovy aktivity, zjišťuje využitelné (zneužitelné) informace
  - **phishing** – podvodné předstírání reálné služby (např. „aktualizace uživatelských účtů v bance“) na falešném serveru s cílem získat přístup (heslo) ke službě (internetové bankovnictví)
- **potenciální hrozby**
  - často se pod jednou střechou nabízí řada služeb zdarma (např. Google: pošta, kalendář, dokumenty, fotografie, RSS čtečka, mapy,...); poskytovatel získává informace o uživatelích

vytvořeno s podporou
projektu ESF

LIANE – síť TU v Liberci

- LIberec Academical NEtwork
- připojena do sítě CESNET2 (česká akademická síť), do GÉANT2 (evropská akademická páteř) a samozřejmě do Internetu
- dosah:
  - areál univerzity (všechny budovy)
  - koleje (Harcov, Vesec, Hanychov)
  - budovy mimo Liberec (Jablonec n. N., Prostějov)
- http://liane.tul.cz/

Topologie LIANE (2008)

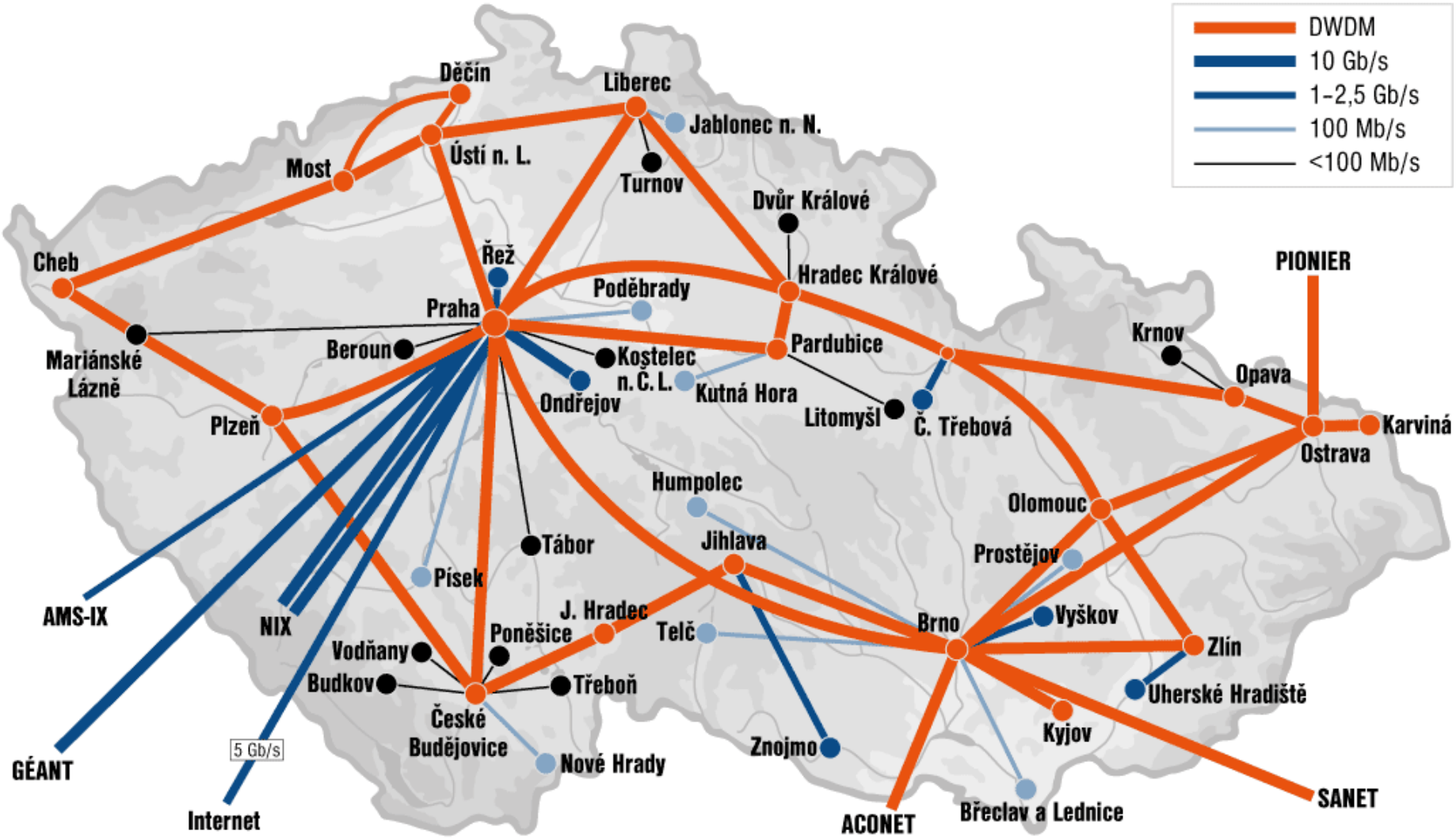


- CIT – centrum většiny klíčových spojů
- H – druhá serverovna, připojení k CESNETu

Páteřní trasy

- většinou vlastní optická vlákna
  - položená na zakázku
  - 2008: položení trasy Harcov–P, uzavření kruhu Hálkova–Harcov–P–H–Hálkova (redundance)
- spolupráce na pořádání MS 2009 – optická trasa do Vesce
- vzdálené lokality (Hanychov) připojeny mikrovlnnými spoji
- meziměstské spoje – CESNET2

Topologie CESNET2 (2011)



Síť CESNET2

- páteř používá DWDM
  - vlnový multiplex (jedno vlákno, různé vlnové délky)
  - optická vlákna přenášející několik nezávislých kanálů (n × 10 Gb/s)
  - umožňuje flexibilně propojovat fyzické trasy mezi libovolnými koncovými body; tzv. end-to-end služby
  - stejně napojena i na evropskou páteř GÉANT2; snaha o end-to-end služby v globálním měřítku (problém: heterogenní systémy i řízení)
- podporuje protokoly IP verze 4 (současná) i verze 6 (budoucí)

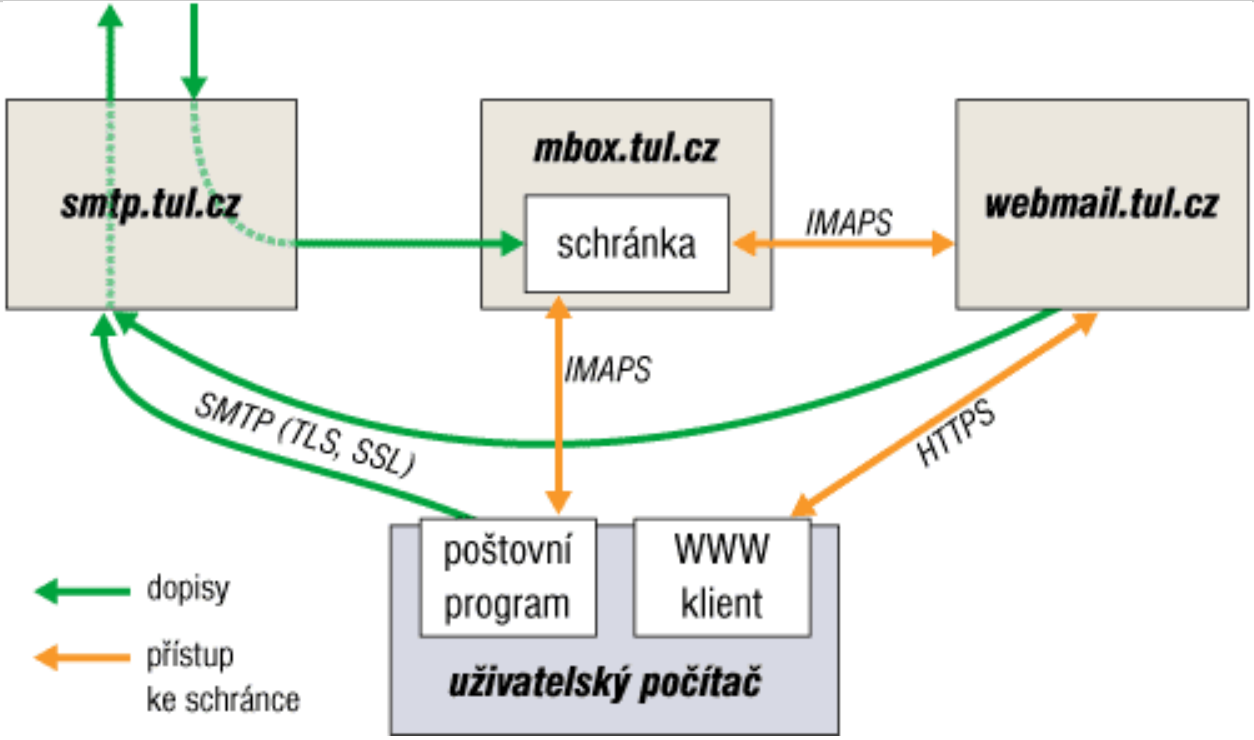
Služby LIANE

- rychlé připojení do Internetu a akademických sítí (jednotky až desítky Gb/s)
- elektronická pošta pro uživatele
- centrální autentizace uživatelů (LDAP)
  - nevyužívá ji STAG (dočasně)
- WWW servery pro univerzitu, její části i uživatele
- domácí adresář dostupný po síti
  - při velikosti a cenách flash pamětí ztrácí smysl

Významné servery LIANE

- **uživatelské**
  - www.tul.cz, fakulty, katedry, knihovna,...
  - menza.tul.cz, koleje.tul.cz
  - webmail.tul.cz – WWW přístup k e-poště
  - mbox.tul.cz – poštovní schránky (přístup: IMAP)
- **servisní**
  - sfinx.tul.cz – konfigurace pro uživatele
  - bubo.tul.cz – přeprava pošty, primární DNS, DHCP
  - tyto.tul.cz – NetWare server, LDAP

Elektronická pošta (1)

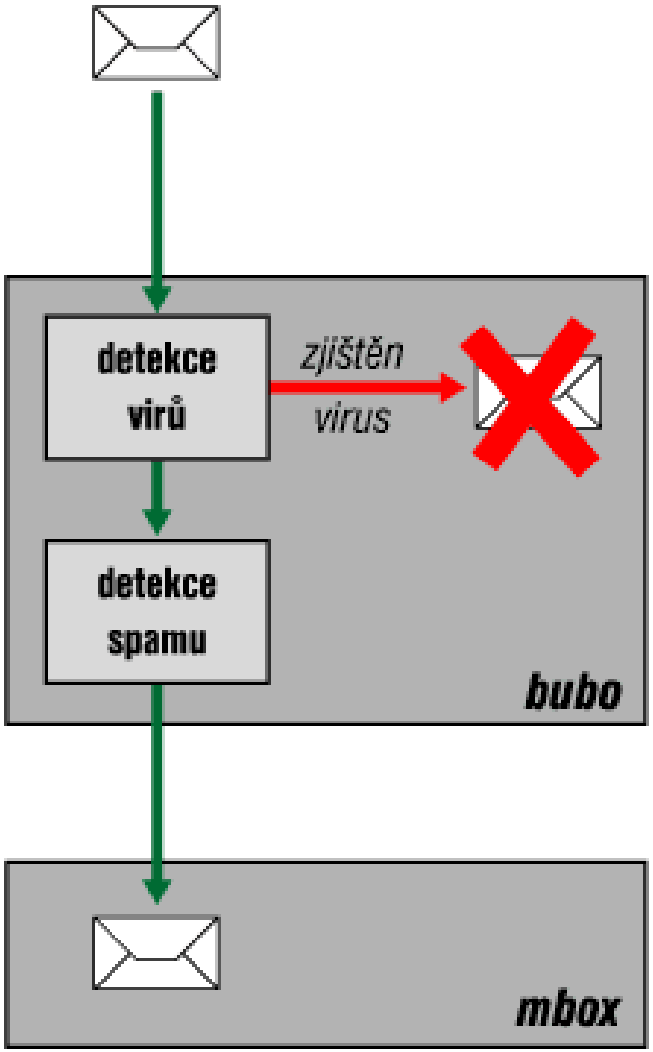


- adresa: jmeno.prijmeni@tul.cz
- přístup: IMAPS (mbox), WWW (webmail)
- konfigurace: sfinx.tul.cz

Elektronická pošta (2)

- vstupem zvenčí je bubo.tul.cz, záložní je tul.cesnet.cz (v Praze)
- předává na mbox.tul.cz
  - zde jsou uživatelské schránky
  - mbox.tul.cz přijímá poštu jen od bubo.tul.cz
- bubo.tul.cz zajišťuje ochranu přicházející pošty

Elektronická pošta (3)



- **viry**
  - Clam AntiVirus (www.clamav.net)
  - otevřený (GPL), aktualizován každou hodinu
  - zavirovaný dopis je smazán bez upozornění odesilateli (adresa bývá padělaná)
  - poštovních virů v poslední době výrazně ubylo (desítky denně do celé TU)

Elektronická pošta (4)

- **spam**
  - **graylisting**
    - první pokud o doručení dopisu server odmítne
    - opakovaný přijme
    - programy distribuující spam a viry většinou neopakují
    - adresáty a odesilatele si ukládá, příště jejich poštu propouští
  - **blacklisting**
    - nepřijímá dopisy od známých distributorů spamu
    - on-line kontrola dopisů
    - razor.sourceforge.net

Elektronická pošta (5)

- **spam**
  - **SpamAssassin** (spamassassin.apache.org)
    - heuristická analýza obsahu dopisů, výsledek není jistý
    - podle nalezených příznaků přidělí dopisu bodové hodnocení, při překročení limitu označí za spam
    - dopisy v předmětu označeny ***SPAM*** plus hlavičky X-Spam-...
    - dopis je doručen, zpracování ponecháno na uživateli (možnost automatických filtrů v poštovních klientech)

Bezdrátová síť (Wi-Fi)

- pokrývá většinu budov, zejména významné „veřejné“ prostory (menza, knihovna), rozšiřuje se
- dostupné standardy
  - IEEE 802.11b/g – pásmo 2,4 GHz, rychlost 11/54 Mb/s
  - IEEE 802.11a – pásmo 5 GHz, rychlost 54 Mb/s
- centrální řízení přístupových bodů (AP)
  - homogenní konfigurace
  - koordinace vysílacích výkonů apod.
  - umožňuje přechod uživatelů mezi AP

eduroam

- akademický roaming, umožňuje připojení uživatelů v účastnických sítích
  - autentizace se provádí „doma“
  - netřeba nic nastavovat, prostě to funguje
- dva typy autentizace:
  - **eduroam** – bezpečné, veškerá komunikace šifrována, umožňuje roaming, autentizace protokolu IEEE 802.1X
  - **liane** – bez zabezpečení, omezené služby, jen lokálně, autentizace webovým formulářem

Autentizace uživatelů (1)

- centrální autentizační server tyto.tul.cz, Novell NetWare + LDAP server
- uživatelská jména **jmeno.prijmeni@tul.cz** nebo **jmeno_prijmeni** (pro služby nepodporující LDAP)
- autentizace prostřednictvím LDAP se používá pro:
  - elektronickou poštu
  - menzu
  - konfigurační formuláře na sfinx.tul.cz
  - některé učebny

Autentizace uživatelů (2)

- Shibboleth – SSO (Single Sign On)
  - webové stránky na TUL
  - partnerské organizace (eduID.cz)
- jiná autentizace (vlastní hesla):
  - STAG
- účet v LIANE je automaticky zakládán a prodlužován podle údajů studijního oddělení
- heslo platí po celou dobu studia, je vhodné je jednou ročně měnit

LDAP (1)

- Lightweight Directory Access Protocol
- zjednodušená verze X.500 DAP
- RFC 2251–2255, TCP port 389
- umožňuje autorizaci (tzv. bind) a většinu operací pro správu uživatelů – přidávání, mazání, vyhledávání,...
- v základním návrhu obsahuje zabezpečení připojení přenosu pomocí TLS, některé operace nelze provádět bez tohoto zabezpečení
- binární protokol, pro výměnu dat se používá formát LDIF (LDAT Data Interchange Format)

LDAP (2)

- uživatele reprezentují objekty uspořádané do stromu
- informace o objektu uloženy v atributech (položkách)
- hlavní položka **dn** (Distinguished Name) představuje jméno
- každý objekt má až desítky atributů podle složitosti stromové struktury dané instituce, která LDAP používá

LDAP – příklad

```
dn: cn=Jiri_Vrany,ou=LIANE,o=VSLIB
loginShell: /bin/bash
homeDirectory: /home/j/jiri.vrany
gecos: Jiri Vrany
workforceID: f0b74008d72d96d2800d28356f42bd37
mail: Jiri.Vrany@tul.cz
uid: jiri.vrany
givenName:: SmnFmcOt
fullName: Jiri Vrany
lockedByIntruder: FALSE
messageServer: cn=TYTO,ou=LIANE,o=VSLIB
allowUnlimitedCredit: TRUE
accountBalance: 0
sn:: VnJhbsO9
securityEquals: cn=Everyone,ou=LIANE,o=VSLIB
securityEquals: cn=Students,ou=LIANE,o=VSLIB
securityEquals: cn=Kai,ou=LIANE,o=VSLIB
passwordUniqueRequired: FALSE
passwordRequired: TRUE
passwordMinimumLength: 5
passwordExpirationTime: 20081114081639Z
passwordExpirationInterval: 31536000
passwordAllowChange: TRUE
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: Person
objectClass: Top
objectClass: ndsLoginProperties
objectClass: posixAccount
objectClass: shadowAccount
loginTime: 20060317124940Z
loginScript:: UkVNDQoA
loginIntruderAddress:: MSOT5kmR
loginGraceRemaining: 7
loginGraceLimit: 7
loginDisabled: FALSE
loginAllowedTimeMap:: //////////
ndsHomeDirectory:
    cn=TYTO_US1,ou=LIANE,o=VSLIB
groupMembership:
    cn=Everyone,ou=LIANE,o=VSLIB
groupMembership:
    cn=Kai,ou=LIANE,o=VSLIB
cn: Jiri_Vrany
```

vytvořeno s podporou
projektu ESF

Elektronická pošta

- elementární služba, výchozí pro některé další
- jedna z prvních síťových služeb vůbec
  - v Internetu: protokol SMTP
  - existují i další poštovní systémy, zpravidla propojeny s internetovou poštou
- základní principy popisují
  - RFC 2821 – protokol SMTP
  - RFC 2822 – formát dopisu (jen ASCII, omezená délka)

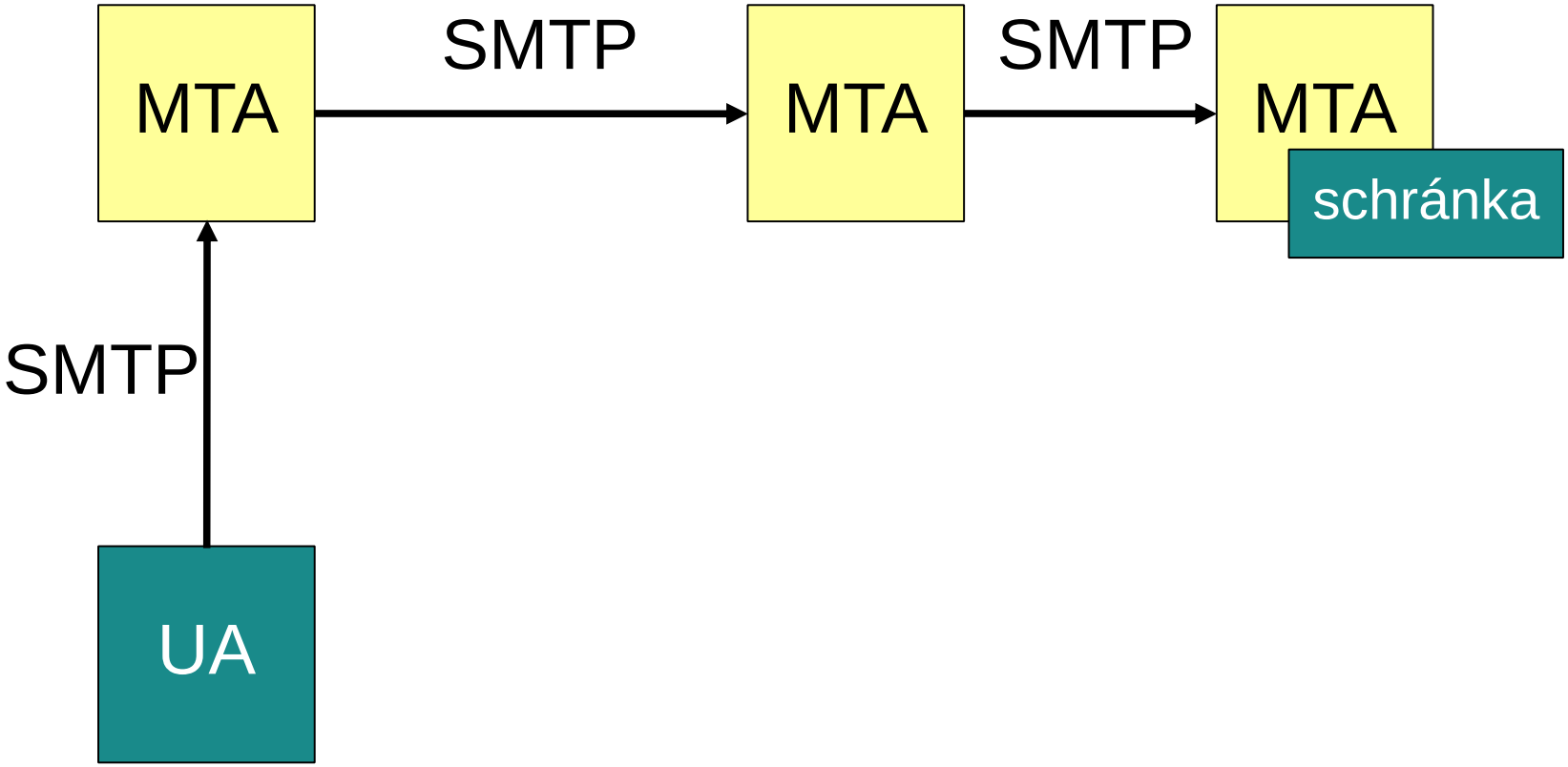
Architektura pošty

- z pohledu uživatele platí analogie s klasickou poštou – napíši dopis, odešlu a po nějaké době se objeví v adresátově schránce
- základním principem je schéma klient–server
- **klient (UA, User Agent)** – uživatelské rozhraní pro používání pošty
- **server (MTA, Message Transfer Agent)** – zajišťuje vlastní přenos zpráv, nabízí služby klientům

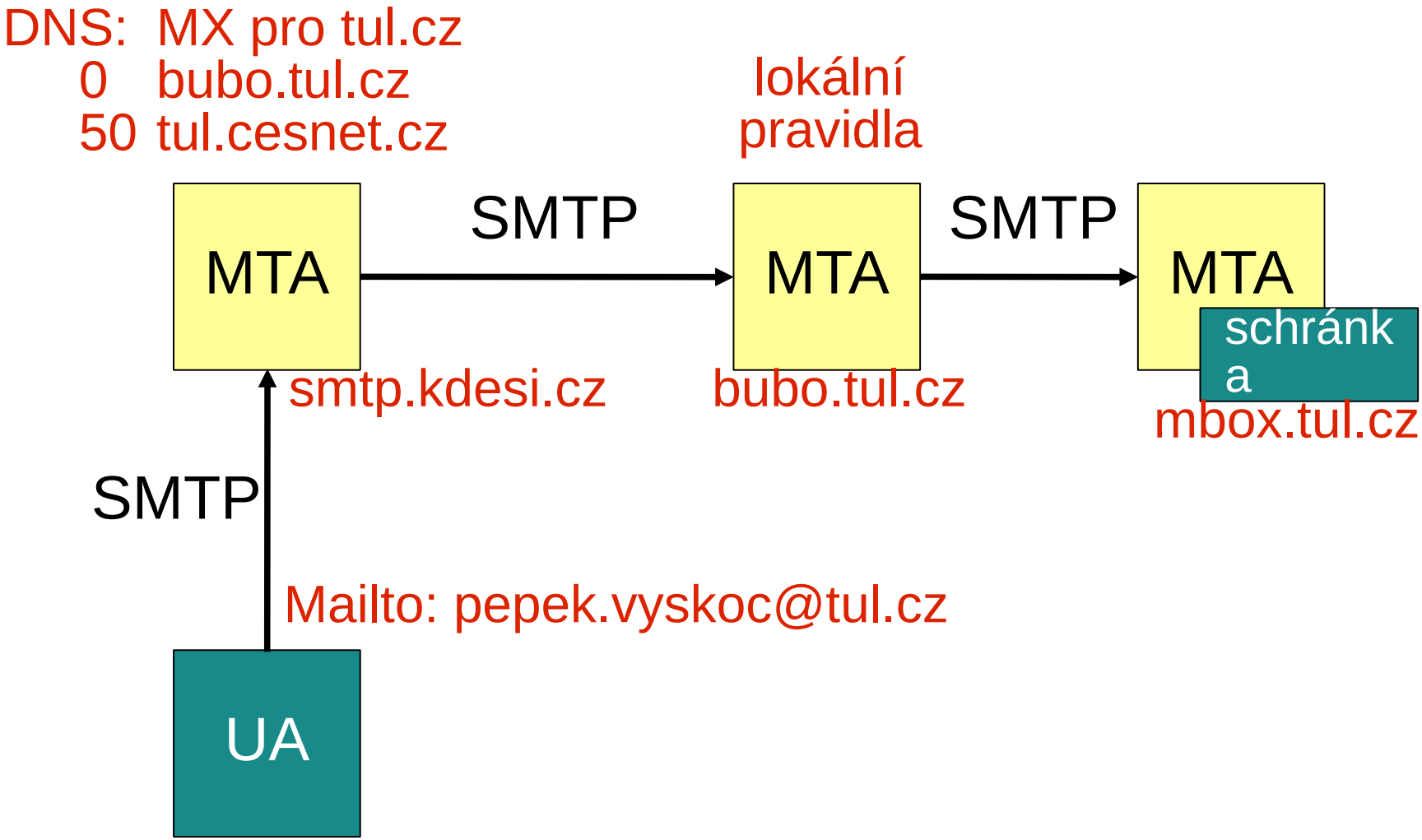
Poštovní adresy

- formát definován v RFC 2822
  franta.uzivatel@nejaka.doména
- **identifikátor příjemce** – uživatelské jméno, případně alias, podle kterého MTA určí cílovou schránku
- **doména** – podle ní se rozhoduje, kam se má doručit; konkrétní MTA se zjišťuje pomocí MX záznamů v DNS

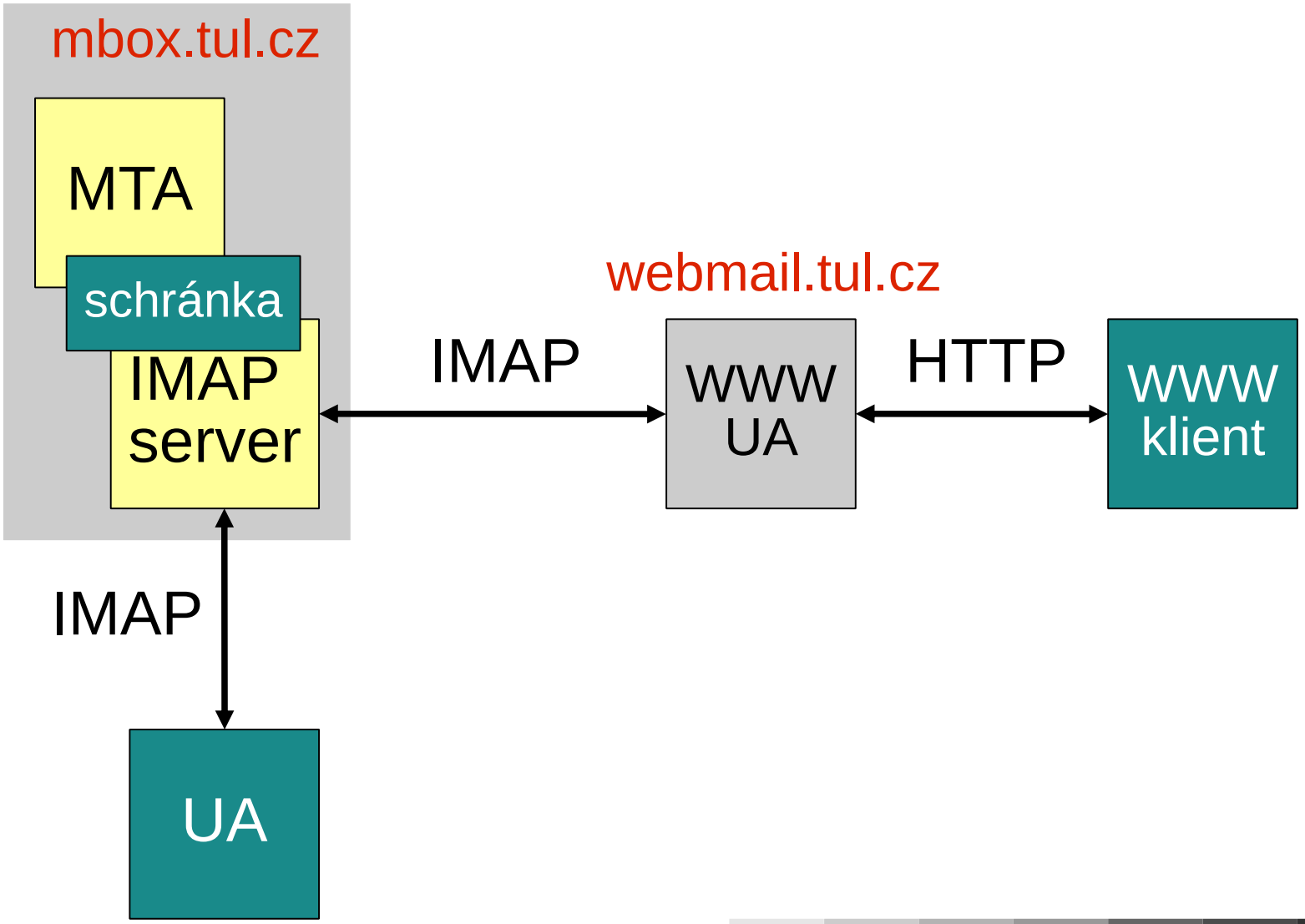
Přenos dopisu



Přenos dopisu



Přístup ke schránce



Protokol SMTP

- Simple Mail Trasfer Protocol
- základní přepravní protokol, RFC 2821
- řídí komunikaci UA–>MTA a MTA–>MTA
- jednoduchý protokol, snaha o jednoduchý spolehlivý přenos krátkých zpráv složených z ASCII znaků
- sedmibitový přenos
  - základní ASCII tabulka má 128 znaků (2^7)
  - chybí znaky s diakritikou apod.

Protokol POP3

- Post Office Protocol verze 3, RFC 1939
- pro čtení pošty ze schránky
  - typicky: připojí se k POP3 serveru, dopisy ze schránky přenese na lokální počítač a odpojí se
  - při práci s dopisy už nemusíte být on-line, vhodné pro komutovaná připojení (placená podle doby připojení)
  - se schránkou nelze rozumně pracovat z více počítačů
- neobsahuje zabezpečení, jméno a heslo se posílá otevřeně

Protokol IMAP

- Internet Message Access Protocol, RFC 3501
- vzdálená práce se schránkou
  - podporuje připojený (on-line) i nepřipojený (off-line, de facto dávkový) režim práce
  - se schránkou lze pracovat z různých počítačů, i současně
  - umožňuje stahovat části dopisů, v základu přenáší jen hlavičky
- také bez zabezpečení, zpravidla se kombinuje se SSL (resp. TLS) – označován jako IMAPS

Struktura dopisu (1)

- původní struktura definována v RFC 2822
- základní struktura:
  - **obálka** – neviditelná, vzniká a zaniká při SMTP přenosu
  - **hlavičky** – popisné informace o dopisu (kdo poslal, kdy, komu, kudy,...)
  - **tělo** – vlastní nesená zpráva
- praktické cvičení – rozeberte hlavičky dopisů ze své schránky (je třeba zobrazit neupravený zdrojový kód dopisu, Ctrl-U v Thunderbirdu)

Struktura dopisu (2)

- sedmibitové omezení
  - jak posílat znaky s diakritikou?
  - jak posílat přílohy (obrázky, dokumenty)?
- MIME (Multipurpose Internet Mail Extensions)
  - RFC 2045, 2046, 2047, 4288, 4289, 2077
  - klient dopis zakóduje tak, aby vyhovoval původním omezením; příjemcův klient dekóduje

MIME

- identifikuje, jakého typu jsou nesená data (hlavička **Content-Type**)
  - využije přijímající klient ke zpracování/prezentaci
- popíše, jak jsou kódována pro přenos (hlavička **Content-Transfer-Encoding**), hodnoty:
  - **7bit** – nekódováno, 7bitová data
  - **quoted-printable** – kódování vhodné pro texty
  - **base64** – kódování vhodné pro binární data
  - **8bit**, **binary** – nekódováno, 8bitová data, vyžaduje podporu MTA (je obvyklá)

Kódování Printed Quotable

- vhodné pro texty s národními znaky
- znaky z dolní poloviny ASCII tabulky (7bitové) nechává beze změny
- znaky z horní poloviny převede na trojice =XX kde XX je kód znaku v šestnáctkové soustavě
- Čárka převede na =C8=E1rka
- díky zachování ASCII znaků je s trochou cviku čitelné „pouh=FDm okem“

Kódování Base64

- kóduje bez rozdílu všechny bajty, vhodné pro ryze binární data, ve výstupu používá 64 znaků
- vstupní data bere jakou souvislý proud bitů, rozdělí na 6b úseky, těm přidělí znaky podle

ascii8bit	Č	á	r	k	a	
binárně	11001000	11100001	11100010	01101011	01100001	
binárně 6bit	110010	001110	000111	100010	011010	110110	000100
dekadicky	50	14	7	34	26	54	4
base64	y	O	H	i	a	2	E=

Praktický test

```
telnet smtp.tul.cz 25
Trying 147.230.16.1...
Connected to smtp.tul.cz (147.230.16.1).
Escape character is '^]'.
220 bubo.tul.cz ESMTP Postfix
HELO smtp.tul.cz
250 bubo.tul.cz
MAIL FROM:jmeno.prijmeni@tul.cz
250 Ok
RCPT TO:jmeno.prijmeni@tul.cz
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Ahoj jak se mas? Ja docela dobre.
.
250 Ok: queued as 8AB7F5F401
QUIT
221 Bye
Connection closed by foreign host.
```

samotná tečka ukončí dopis

Poštovní klienti

- dnes obvykle součástí operačního systému
- nejběžnější:
  - **MS Outlook Express** resp. **Windows Mail**
  - **Mozilla Thunderbird**
  - **Opera** (vestavěn ve WWW prohlížeči)
- webmail – poslední dobou velmi populární
  - výhody: konzistentní chování odkudkoli, není třeba instalovat a konfigurovat software
  - nevýhody: omezené funkce, svěřujete důvěrná data provozovateli (u veřejných webmailů)

Aplikace pro spolupráci

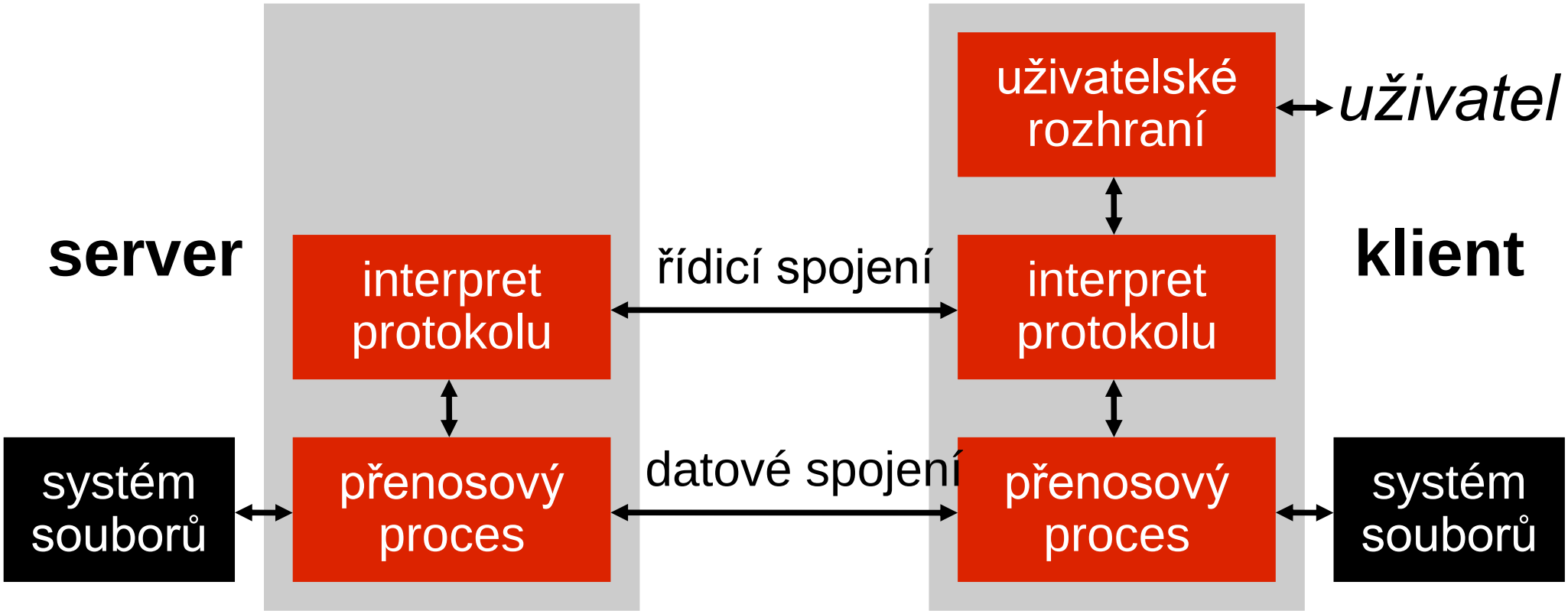
- poštovní klient plus rozšiřující služby
  - kalendář umožňující sdílení
  - toky dokumentů, připomínkování apod.
  - vyžaduje podporu na straně serveru
- příklady:
  - **MS Outlook** – součást MS Office
  - **Novell Evolution** – existuje volná i komerční verze
  - **Lotus Notes** – tradiční, častý ve velkých firmách

vytvořeno s podporou
projektu ESF

File Transfer Protocol (FTP)

- protokol pro přenos souborů, jeden z klasických
- RFC 959
  přehled specifikací na http://www.wu-ftpd.org/rfc/
- opět architektura klient-server
- navržen s ohledem na efektivní využívání prostředků – alokuje si je až v případě potřeby

Architektura FTP



FTP spojení

- **řídicí spojení**
  - vzájemná výměna příkazů a reakcí na ně
  - trvalé, navazuje klient, TCP port 21
  - server si udržuje informace o něm (aktuální adresář, režim přenosu apod.)
- **datové spojení**
  - vzniká při konkrétním požadavku, po přenesení souboru zaniká, TCP port 20
  - zahajuje odesilatel dat (zpravidla server)

Přenos dat

- FTP nesleduje obsah souborů, 3 způsoby přenosu:
  - **Stream mode:** spojitý proud dat, nejrychlejší, nejmenší nároky na klienta i server
  - **Block mode:** data rozdělena do bloků, po přerušení lze navázat a pokračovat, cenou je vyšší režie
  - **Compressed mode:** jednoduchá komprese – nahrazuje opakující se hodnoty
- při přenosu se rozlišuje typ dat:
  - **ASCII:** textový režim, konvertuje znaky mezi systémy
  - **Image:** binární, přenáší data beze změn

Komunikační jazyky

- **řídicí**
  - komunikace na řídicím spojení
  - ASCII příkazy definované protokolem FTP
- **uživatelský**
  - komunikace s uživatelem, ovládání činnosti klienta
  - klienti se liší – různé textové příkazy, GUI,...
- klient zároveň funguje jako překladač mezi těmito dvěma jazyky

FTP klienti

- **klasický textový**
  - ftp a lepší (ncftp, yafc,...)
  - dostupné všude, lze používat dávkově
- **grafický**
  - SmartFTP (Win), gftp (Lin)
  - uživatelsky příjemný, mívá nadstandardní dovednosti
- **vestavěný**
  - ve správci souborů (Total Commander, Free Commander) – FTP server se chová jako další disk
  - ve WWW prohlížeči (jednosměrný)

Uživatelský jazyk FTP klienta

- 3 hlavní skupiny příkazů
  - **přihlášení**
    open, user, close, quit, ...
  - **nastavení přenosových parametrů**
    ascii, binary, mode, ...
  - **vlastní přenosy**
    get, put, cd, dir, mget, mput, reget, ...

FTP a uživatelé

- FTP používá obvyklý koncept uživatelů, hesel a přístupových práv (hesla posílá otevřeně!)
- **anonymní přístup**
  - uživatel: ftp nebo anonymous
  - heslo: e-mailová adresa
  - nejčastěji pro distribuci volného software
- **autentizovaný přístup**
  - uživatelské jméno a heslo definuje správce serveru
  - např. pro správu WWW stránek

TFTP

- Trivial FTP, RFC 1350
- velmi jednoduchý protokol, např. pro start bezdiskových stanic, načtení konfigurace či OS
- používá UDP
- nemá uživatele a hesla, přístup řízen firewallem
- nemá aktuální adresář, režimy přenosu apod.

SCP: přenosový ideál

- Secure Copy, využívá SSH (Secure Shell)
- šifruje celou komunikaci mezi klientem a serverem
- **textová varianta: scp *co kam***
  - vzdálený cíl se zadává v podobě uživatel@server:cesta
  - scp index.html kdosi@www.kdesi.cz:/web/
    scp pepa@pc.jinde.cz:obrazy/*.jpg .
- **grafické verze**
  - např. **WinSCP** (http://winscp.net/)
  - rozhraní napodobuje průzkumníka nebo commander

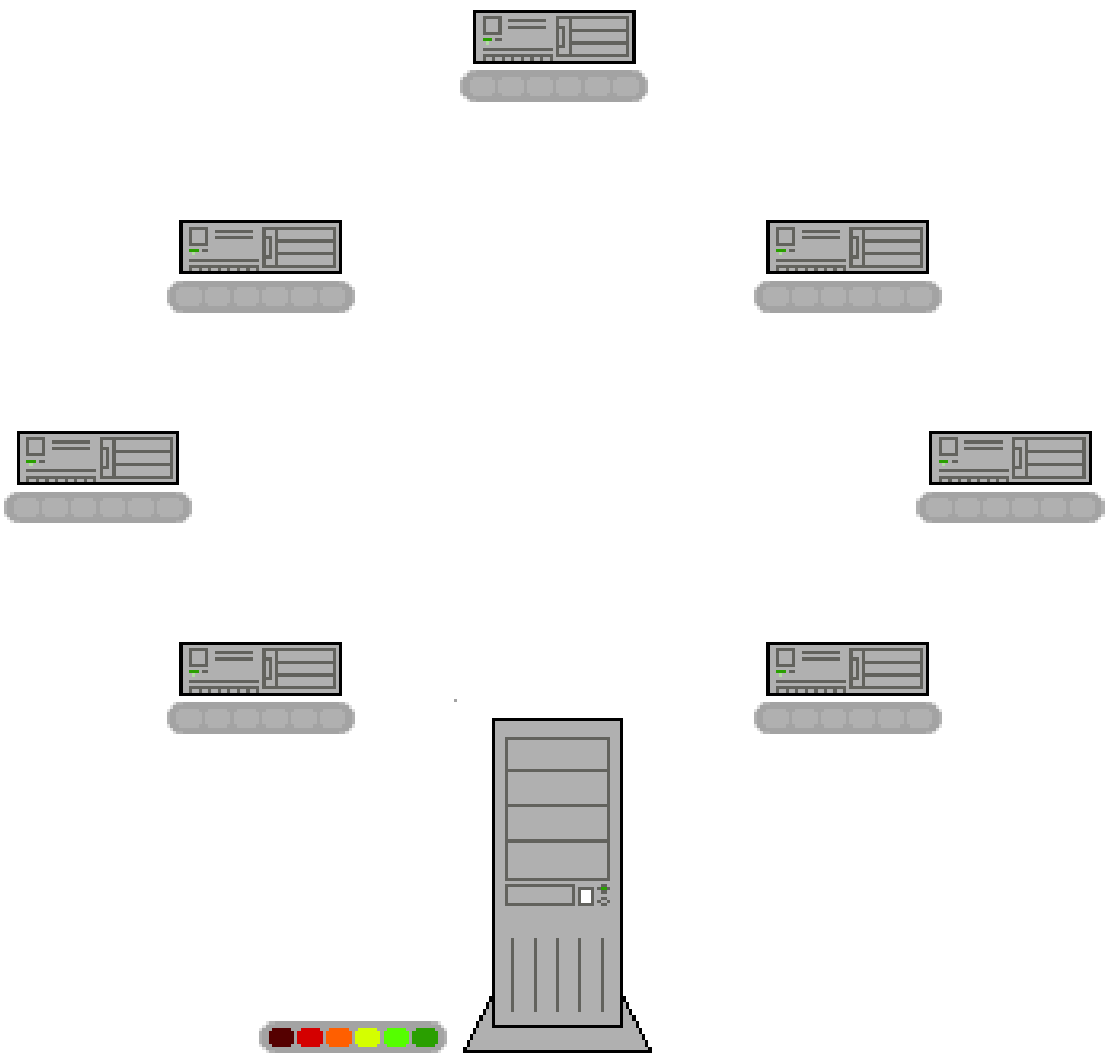
P2P sítě (1)

- peer-to-peer – klienti spolu komunikují přímo
  - přenosová kapacita roste s počtem účastníků
  - chybí centrální autorita kontrolující obsah
  - duplikace zdrojů – odolné proti výpadkům
  - struktura sítě se stále mění, klienti přicházejí a odcházejí
- použití P2P sítí:
  - sdílení souborů
  - IP telefonie (Skype)
  - audio/video streaming

P2P sítě (2)

- typy P2P sítí:
  - **decentralizovaná** – server vůbec neexistuje, např. Kazaa
  - **centralizovaná** – existuje centrální server/router, např. DirectConnect
  - **hybridní**

BitTorrent



- protokol i aplikace pro přenos souborů
- silná replikace – soubor skládá z mnoha zdrojů
- specializovaná aplikace nebo WWW klient Opera

PSP sítě a zákony

- realita
  - velká část obsahu porušuje zákony
  - vlastníci autorských práv si najímají specializované firmy vyhledávající, kdo nabízí jejich díla
- v ČR je legální stahovat hudbu a filmy pro vlastní potřebu (nikoli software!), ale ne poskytovat
- pokud používáte P2P sítě, hlídejte si, co nabízíte
  - vlastní tvorba (digitální fotografie)
  - volně šiřitelný software

vytvořeno s podporou
projektu ESF

World-Wide Web (WWW, W3)

- nejznámější internetová služba (WWW není Internet, jen jedna z jeho služeb)
- původně služba pro integraci informačních zdrojů a publikování dokumentů, dnes brána mnoha služeb i aplikací
  - e-komerce
  - vyhledávání
  - uživatelské komunity
  - on-line aplikace
  - ...

Hypertext (1)

- základní myšlenka: lidé nemyslí přímo, ale přeskakují z jednoho tématu na jiné
- hypertext je text přizpůsobený tomuto způsobu čtení/myšlení
- počátky po 2. světové válce v USA
- první realizace: systém XANADU (zahájen 1960, vyvíjel se velmi dlouho, software vydán 1998)

Hypertext (2)

- přecházení z dokumentu na dokument – browsing
- informace členěny na menší celky (stránky) propojené hypertextovou strukturou (odkazy)

- **výhody**
  - distribuovatelnost
  - libovolné propojení stránek
  - záleží jen na čtenáři, jak bude procházet
- **nevýhody**
  - nevhodné pro tisk, nutí číst na počítači
  - může rozptylovat (těkání)
  - informace propojuje autor, čtenáři nemusí vyhovovat

Historie a vývoj WWW

- první specifikace: 1989 Tim Berners-Lee v CERNu
- původně textový systém, později grafický režim (NCSA Mosaic, Netscape)
- vychází ze SGML (Standard Generalized Markup Language), HTML je definován pomocí SGML
- bouřlivý vývoj v 90. letech (válka prohlížečů, přidávání prvků do jazyka jako nástroj konkurenčního boje)
- založení WWW konsorcia pro neutrální vývoj

HTML dnes

- **HTML 4** dlouho deklarován jako poslední
- jazyk je strukturální, definuje význam jednotlivých částí stránky
- **XML** (podmnožina SGML, jednodušší pravidla, snazší implementace)
- **XHTML 1** – HTML 4 převedené do XML
- **CSS (Cascading Style Sheets)** pro definici vzhledu, oddělení obsahu (HTML, XHTML) od formy (CSS)

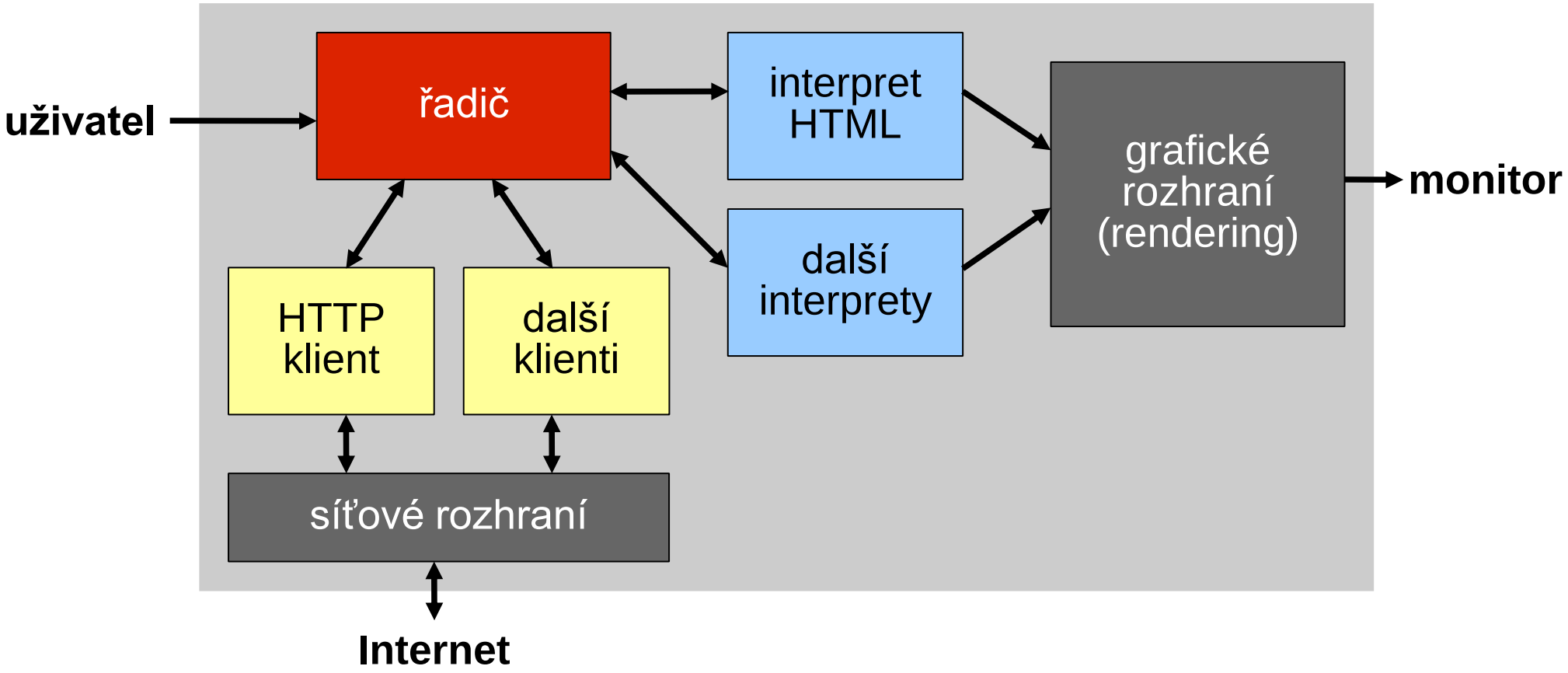
Budoucnost

- další vývoj měl probíhat jen pro XHTML
- 2007 zahájen vývoj **HTML 5** (a **XHTML 5**)
  - iniciován mimo WWW konsorcium, později jej převzalo
  - cíl: lepší podpora aplikací
  - řada kontroverzí
  - specifikace očekávána v roce 2010, první návrh vyšel v lednu 2008

Architektura WWW

- princip klient-server
- server: uchovává stránky a na žádost je poskytuje
- klient: posílá žádosti na stránky (a další materiál) a formátuje jejich podobu na monitoru
- základní specifikace:
  - HTML (HyperText Markup Language) – jazyk stránek
  - HTTP (HyperText Transfer Protocol) – protokol pro komunikaci mezi klientem a serverem

WWW klient



- základní funkce: síťová komunikace, interpretace dat, zobrazování, komunikace s uživatelem

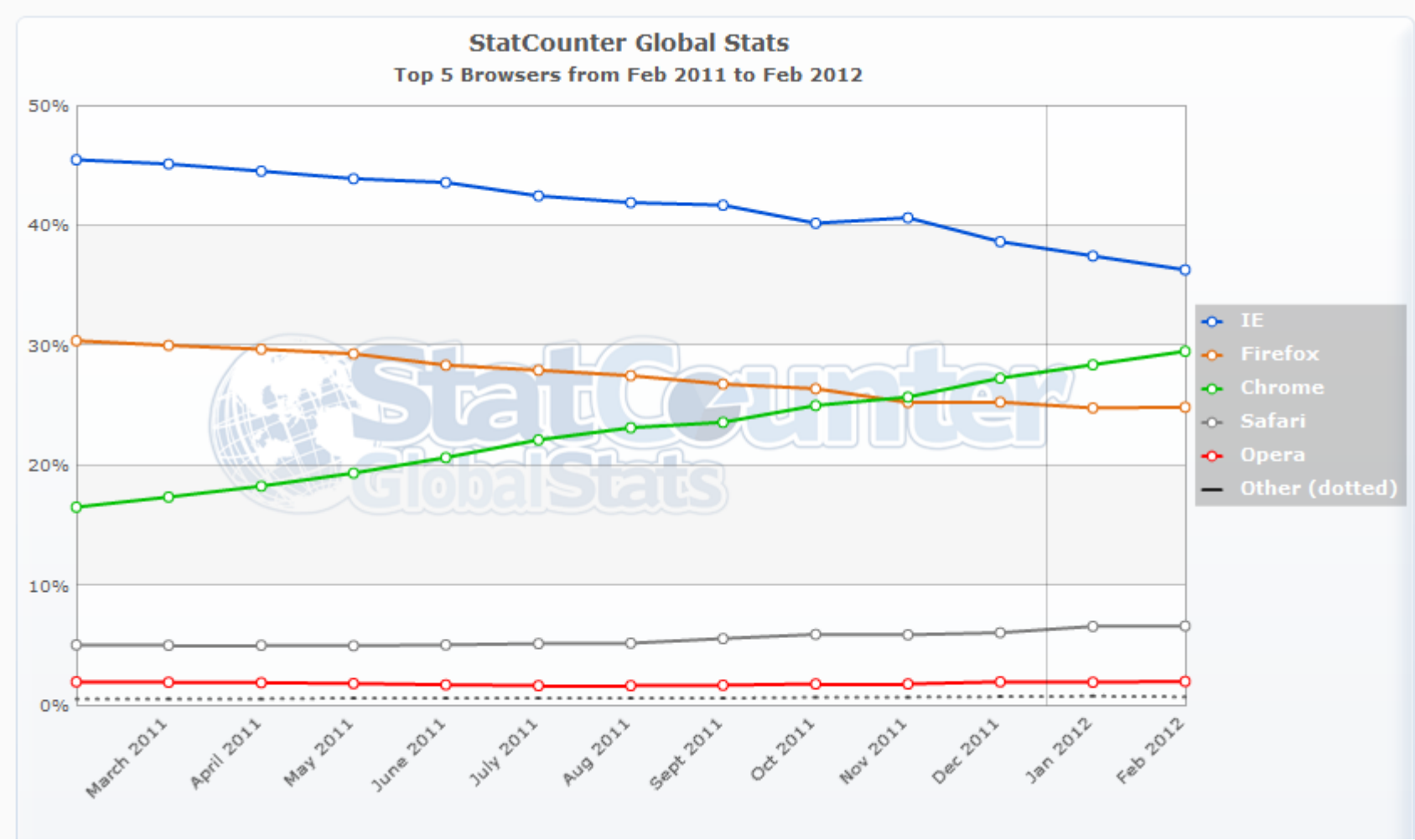
WWW klienti (1)

- **MS Internet Explorer (v. 9.0)**
  - jen MS Windows
  - problematická podpora standardů ve starších verzích
  - nejrozšířenější, ale ztrácí
- **Google Chrome (v. 17.0.963.46)**
  - multiplatformní
  - oddělené procesy pro jednotlivé záložky
  - rychlý javascript

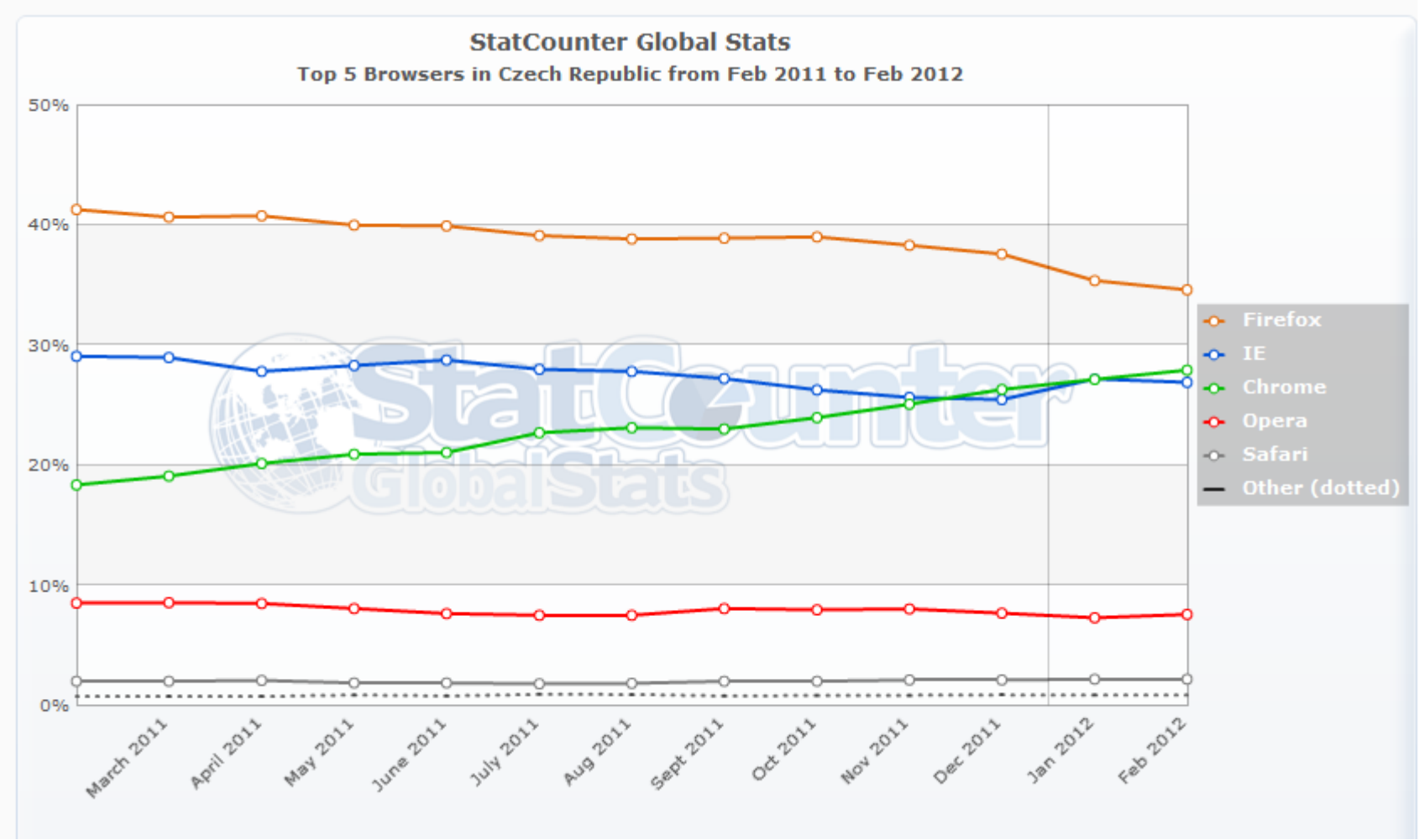
WWW klienti (2)

- **Mozilla Firefox (v. 10.0.1)**
  - multiplatformní
  - základní funkce rozšiřovány pomocí doplňků (Adblock, All-in-One Gestures, Firebug,...)
- **Opera (v. 11.61)**
  - multiplatformní, dominuje na palm-topech
  - nejvíce schopností v základní instalaci
  - rychle startuje a efektivně se ovládá
- **Safari (v. 5.1.2)**
  - standard pro MacOS, nyní i pro MSWindows

WWW prohlížeče – celosvětově



WWW prohlížeče –ČR



HTTP

- HyperText Transfer Protocol verze 1.1, RFC 2616
- **bezstavový protokol** – server neudržuje stavové informace o klientech
  - robustní
  - základní schéma **dotaz–odpověď**
  - mezi klientem a serverem mohou být proxy cache servery (ukládají stránky)

URL

- Uniform Resource Locator
- univerzální „internetová adresa“, identifikuje informace poskytované různými službami
- obecná syntaxe: schéma:specifická_část
- **schéma** určuje službu (přístupový protokol)
- **specifická část** závisí na schématu, identifikuje cíl
- alternativou je URN (Uniform Resource Name) – identifikace obsahu bez ohledu na umístění, stále spíše holub na střeše

Příklady URL

- http://liane.tul.cz/email/thunderbird/

- ftp://ftp.muni.cz/pub/linux/fedora/

- mailto:pavel.satrapa@tul.cz

HTTP dotaz (1)

- základní tvar:
  metoda cesta verze_HTTP
  hlavičky

  tělo
- nejběžnější metody:
  - **GET** – chci stránku, tělo je prázdné
  - **POST** – chci stránku, tělo neprázdné (data z formuláře)
  - **OPTIONS** – dotaz na parametry komunikace

HTTP dotaz (2)

- hlavičky nesou doplňující informace
  - **host** – povinná v HTTP/1.1, obsahuje jméno serveru, na který se klient obrací (umožňuje virtuální servery – více serverů na jedné IP adrese)
- příklad dotazu:

GET /index.html HTTP/1.1
Host: www.tul.cz
User-Agent: Mozilla/5.0 (X11; U; Linux i686;
cs-CZ; rv:1.8.1.12)
Accept: text/xml,text/html
Accept-Language: cs,en-us;q=0.7,en

HTTP odpověď (1)

- základní tvar:
  verze_HTTP kód vysvětlení
  hlavičky

  tělo
- číselný **kód** identifikuje, zda operace dopadla úspěšně, textové **vysvětlení** pak obsahuje komentář ke kódu (pro případného lidského čtenáře)
- **hlavičky** poskytují další informace, **tělo** obsahuje vlastní data

HTTP odpověď (2)

- výsledkové kódy
  - klíčová je první číslice, zbývající upřesňují
  - **1xx** – informační, žádost přijata, pokračujeme
  - **2xx** – žádost přijata a akceptována (OK)
  - **3xx** – přesměrování, je třeba jiný zdroj
  - **4xx** – chyba, špatný nebo nesplnitelný dotaz
  - **5xx** – selhání serveru při sestavení odpovědi

Příklad HTTP odpovědi

HTTP/1.1 200 OK
Date: Sun, 24 Feb 2008 10:30:06 GMT
Server: Apache/2.2.3 (Red Hat)
X-Powered-By: PHP/5.1.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 7840
Connection: close
Content-Type: text/html

<html>
...
</html>

Příklad HTTP komunikace

telnet jméno_serveru 80
Trying server...
Connected to server.
Escape character is '^]'
GET / HTTP/1.0

HTTP/1.1 200 OK
Date:.....
.....
.....

Cookies (1)

- někdy by se hodilo uchování stavu na serveru (nákupní košík, nastavení preferencí,...)
- v HTTP stav uchovává klient – musí dát najevo, že navazuje na předchozí aktivity
- 3 základní možnosti:
  - pomocí URL
  - skrytou položkou formuláře
  - cookies (nejpopulárnější)

Cookies (2)

- cookie – identifikátor vygenerovaný serverem
- server předá klientovi v hlavičce odpovědi **Set-Cookie**
- klient si uloží a když požaduje další stránku z tohoto serveru, přidá k dotazu hlavičku **Cookie** obsahující identifikátor
- server použije cookie k identifikaci klienta a využije informace, které o něm má

WWW server

- odpovídá na dotazy klientů, standardně TCP port 80
- nejrozšířenější:
  - **Apache** – multiplatformní, modulární
  - **MS Internet Information Server (MS IIS)** – pouze pro MSWindows
- koncepce a konfigurace se liší
  - často rodičovský proces odštěpuje potomky obsluhující jednotlivé dotazy

- vytvořeno s podporou projektu ESF

Vzdálený přístup k počítačům

- jedna z nejstarších služeb – vzdálený přístup k sálovým počítačům
  - nejprve vzdálené terminály
  - později terminálová emulace jako jedna ze služeb počítačové sítě
- současnost
  - využíváno pro vzdálené výpočty na výkonných systémech (superpočítače,...)
  - vzdálená správa systémů
  - ASP

ASP

- Application Service Provider – poskytování aplikačních služeb
- jeden z trendů současného internetového podnikání
- masivní rozvoj souvisí se zlevňováním a zkvalitňováním (zrychlováním) připojení k Internetu
- „půjčovna“ software – klient ASP společnosti využívá její SW (i HW) pomocí vzdáleného přístupu
- příklady: účetnictví (a další ekonomické oblasti), distribuované výpočty

Vlastnosti ASP pro klienta

- výhody
  - jednodušší správa systému
  - není třeba budovat a aktualizovat IT
  - možnost soustředit se na předmět podnikání
- nevýhody
  - vyžaduje kvalitní připojení k Internetu (rychlé, spolehlivé)
  - značná závislost na poskytovateli služby

Varianty vzdáleného přístupu

- klasický textový přístup
  - Telnet, SSH
  - vzdálená správa systému, superpočítače
- plnohodnotné grafické rozhraní
  - aplikace běží na straně vzdáleného počítače
- tenký klient (prostřednictvím WWW)
  - časté pro ASP
  - rozdělení aplikace, klient zajišťuje uživatelské rozhraní, klíčové věci probíhají na serveru

Grafická rozhraní (1)

- řada systémů s podobným principem, odlišnosti spíše v detailech (cena, efektivita, bezpečnost)
- jednotlivé systémy mají vlastní protokoly
- zpravidla uspořádání klient-server, ale neobvykle:
  - server je program obsluhující periferie (monitor, klávesnici, myš,...), tedy uživatelský počítač
  - klient je aplikace, která žádá o vykreslení věcí na obrazovku či dostává ke zpracování události typu stisk klávesy, může běžet na vzdáleném počítači

Grafická rozhraní (2)

- klient-server si vyměňují poměrně jednoduché pokyny typu „vykresli na souřadnice X, Y“, „přesuň objekt na danou pozici“
- objem přenášených dat nemusí být velký
- obecně komunikují po síti
  - mohou běžet na stejném počítači, ale i každý na jiném

Citrix Presentation Server

- dříve Citrix MetaFrame
- dlouhodobě nejrozšířenější řešení pro MS Windows (existuje verze i pro Unix)
- používá protokol ICA (Independent Computing Architecture)
  - malý objem dat
  - nad TCP/IP i jinými protokoly
- www.citrix.com

Microsoft Terminal Services

- objevilo se ve Windows NT 4, původně založeno na kódu Citrix, později přepracováno
- využívá Remote Desktop Protocol
- klienti
  - Remote Desktop Connection – oficiální MS klient ve Windows, existuje i pro Mac
  - rdesktop, tsclient – open source klienti pro Unix/Linux
- server
  - Windows Terminal Server

X Window System

- vzdálený grafický přístup pro Unix/Linux
- klient-server (server obsluhuje obrazovku, klient je aplikace)
- využívá protokol TCP/IP
- protokol označován X (aktuální verzí je X11)
- základní přenos není zabezpečen, lze řešit SSH tunely
- rozvíjen a implementován nadací X.Org

VNC (1)

- Virtual Network Computing
- multiplatformní, od počátku navrhováno nezávisle na operačním systému (oba konce se mohou lišit)
- využívá protokol Remote FrameBuffer (RFB)
  - použitelný pro všechny okenní systémy (X11, Win,...)
  - původně jednoduchý, postupně rozšířen a zahrnuje i přenosy souborů či on-line komprimaci
  - základem obdélníky rastrových dat – náročnější na přenosové objemy
  - slabé zabezpečení (lze SSH tunel)

VNC (2)

- klient
  - VNC Viewer
  - velmi nenáročná aplikace, vyžaduje jen komunikaci s přenosovým protokolem a grafickým rozhraním
- server
  - poskytuje data v grafickém formátu vyžadovaném klientem
- implementace pro většinu platforem, viz http://gentoo-wiki.com/VNC, www.realvnc.com

VNC konfigurace

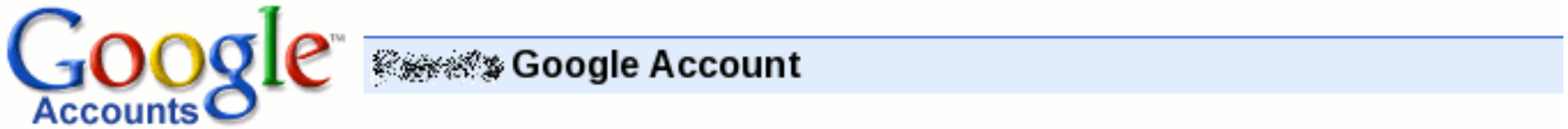
Webové aplikace (1)

- výrazný trend poslední doby
- obvyklé lokální aplikace (textový editor, tabulkový kalkulátor, pošta apod.) se přesouvají na web
  - ovládány prostřednictvím WWW klienta
  - obvyklý protokol HTTP
  - data uložena „někde na serveru“, obvykle lze exportovat a uložit lokálně (často v různých formátech)
  - navíc často umožňují sdílení a týmovou práci (některé redakce využívají Google Docs pro týmovou přípravu článků)

Webové aplikace (2)

- typickým představitelem je rodina produktů Google
  - Google Docs
  - Google Mail
  - Google Calendar
  - Google Maps
  - někdy propojení lokální aplikace (Picasa pro úpravu fotografií) s webem (Picasa Web Albums)
  - a další, vše zdarma (financováno z reklamy)
  - vyžaduje účet u Google

Google služby



Personal information - Edit

Country: Czech Republic (Česko)

Time zone: (GMT+01:00) Central European Time

Change password

Change security question

My services - Edit

- **Calendar**
- **Docs**
- **Gmail** - Settings
- **iGoogle** - Settings Add content
- **Maps** - My Maps
- **Notebook**
- **Picasa Web Albums** - Settings
- **Reader** - Settings
- **Talk**

vytvořeno s podporou
projektu ESF

Malware

- souhrnné označení pro škodlivý software, který pronikne do systému obvykle bez vědomí uživatele
- základní kategorie:
  - **infekční** – čistá destrukce – viry, červi (worms)
  - **skryté** – autor se snaží ovládnout cizí počítač – trojské koně (trojan), zadní vrátka (backdoor)
  - **ziskové** – autor se snaží je komerčně využít – špioni (spyware), roboti a jejich sítě (botnet), odposlechy, dialery

Viry (1)

- název dle jisté podobnosti s biologickými viry
- program je schopen se sám replikovat, pokud má hostitele
- při provedení hostitele se provede i kód viru – pokusí se o sebereplikaci, případně další činnosti
  - často pak virus zůstává aktivní a snaží se nakazit zpracovávaná data
  - další činnosti jsou velmi pestré – od ničeho přes žertíky až po poškozování dat

Viry (2)

- typy virů – podle hostitele:
  - **souborové** – spustitelné soubory
  - **boot viry** – systémové oblasti disku
  - **makroviry** – virus je realizován makrem v dokumentu (nejčastěji pro MS Office); částečně multiplatformní
  - **skriptové viry** – nejčastěji ve Visual Basic skriptech

Červi

- k šíření nevyužívají soubory, ale síťové komunikační služby
- infikovaný počítač rozesílá do sítě pakety hledající nedostatky pro infikování dalších strojů
- nelze zachytit klasickým antivirovým SW
- obvykle nemají žádnou další činnost, jen se množí a množí a zahlcují komunikační kanály

Trojské koně

- program, který předstírá (či vykonává) určitou užitečnou činnost, ale potají navíc vykonává škodlivé aktivity
- musí být spuštěni uživatelem, nereplikují se, nenakazí další soubory
- dělení:
  - password stealing – zachycují stisky kláves
  - destruktivní – poškozují data na disku
  - dropper – spouštějí další program, např. červa

Zadní vrátka

- otevírá tajný přístup k počítači
- speciální případ trojského koně
- v podstatě na principu klient-server umožňuje ovládat na dálku počítač
- nejčastější zneužití:
  - odposlech hesel pro další systémy
  - rozesílání spamu
  - útoky na další systémy, včetně zapojení do distribuovaných útoků

Spyware

- shromažďuje a odesílá citlivá data z uživatelského počítače
  - instalovaný software
  - soubory s hesly apod.
  - navštěvované WWW stránky
- někdy viditelná činnost (zobrazování reklamy)
- instalován často pomocí bezpečnostních děr WWW prohlížečů
- získané informace se prodávají

Botnet

- jako bot (robot) je označován program, který potají běží v cizím počítači a je schopen vykonávat příkazy svého původce
- existují sítě koordinovaných botů – botnety
- používají se např. pro distribuci spamu, distribuované útoky typu zahlcení
- botnety se pronajímají, cena závisí na atraktivitě prostředí (botnet v bankovní síti je dražší než botnet v učebně TUL)

Dialer

- speciální program pro zneužití vytáčeného připojení k Internetu
- bez vědomí uživatele zavěsí a připojí se na jiné telefonní číslo
  - obvykle zahraniční a velmi drahé
  - vlastník čísla inkasuje jako za placenou telefonní službu
- uživatel často odhalí až podle výše telefonního účtu
- vyhynou přirozeně díky přechodu na ADSL

Panika (hoax)

- poplašné zprávy varující před viry – „Neotevírejte dopisy se jménem Invitation...“
- zatím **žádné** z těchto varování nebylo reálné
- přímo neškodí, ale zahlcují schránky a otravují
- než varování přepošlete, porozhlédněte se
  - ve známých databázích hoaxů (např. www.hoax.cz)
  - případně Googlem na vhodný úryvek z textu

Sociální metody

- **profit z šedé operace**
  - model: potřebujeme převést pololegálních 50 mil. USD z Afriky do Evropy, pomozte nám a dostanete 10 %
  - cíl: přístup ke kontu, případně manipulační poplatky
  - řešení: ignorovat
- **phishing**
  - model: vaše banka instaluje nový systém, přihlaste se na (padělané) stránce a vygenerujte si nové heslo
  - cíl: získat vaše jméno a heslo, např. pro bankovnictví
  - řešení: ignorovat nebo ověřit **telefonem** do banky

Viry v elektronické poště

- spuštění díky nedostatku v poštovním klientovi, častěji ale díky naivitě uživatele
  - např. Beagle.M je v příloze zazipován, archiv je chráněn heslem, které je přiloženo k dopisu jako obrázek – uživatel musí vyvinout značné úsilí, aby si zaviroval počítač, přesto se virus úspěšně šířil
- samy si najdou adresy ve vaší poště a pošlou se dál
- svého času velké téma, dnes téměř zmizely

Antivirová ochrana

- řada různých řešení
- nejvhodnější je kombinace
  - ochrana celé sítě v bodě jejího připojení k Internetu (kontrola pošty, firewall, detekce útoků)
  - ochrana koncových stanic přímo na nich
- klíčová je pravidelná aktualizace
  - neaktuální SW může být horší než žádný (falešný pocit bezpečí)

Antivirové programy pro stanice

- **jednoúčelové**
  - detekují/odstraňují konkrétní infekce, zpravidla zdarma
- **jednoduché skenery**
  - provedou kontrolu disku
  - ne vždy dovedou nalezené viry odstranit
- **komplexní systémy**
  - kromě skenování i rezidentní ochrana – kontrola všech procházejících dat
  - nalezené viry odstraňují (je-li to možné)

Metody skenování

- **vyhledávání virových sekvencí**
  - hledá sekvence podle známé databáze virových kódů
  - viry se často kódují – spouští je ve virtuálním prostředí
- **heuristická analýza**
  - hledá v kódu operace typické pro viry
- **generická detekce**
  - zobecnění vyhledávání sekvencí, stejná sekvence se může vyskytovat v různých virech
  - použitelné i pro detekci kódu využívajícího nedostatky v zabezpečení

Kontrola integrity

- vytvoří a uloží si informace o důležitých souborech (kontrolní součty, délky, dobu změny,...)
- později ověřuje, zda nedošlo k jejich změně
- jednoduché a účinné
- informace lze využít při rekonstrukci napadeného systému
- problém se soubory, které se mění běžnou činností (např. instalací nových programů)

Monitorovací systém

- sleduje „živě“ chování programů v systému
- viry se snaží identifikovat podle podezřelých aktivit, např. zápis do systémové oblasti disku
- vychází z databáze obvyklých virových operací a postupů
- náročné na nastavení, aktualizace nemusí být příliš častá

Odkazy

- www.wildlist.org – aktuální výskyt virů
- www.messagelabs.com – analýza elektronické pošty (zastoupení virů, spamu a phishingu)
- www.hoax.cz, www.viry.cz – české servery
- software
  - antiviry: www.free-av.com, www.aec.cz, www.avg.cz, www.avast.cz, www.kaspersky.com
  - antispyware: www.superantispyware.com, www.lavasoft.de (Ad-Aware)

Jak se chránit

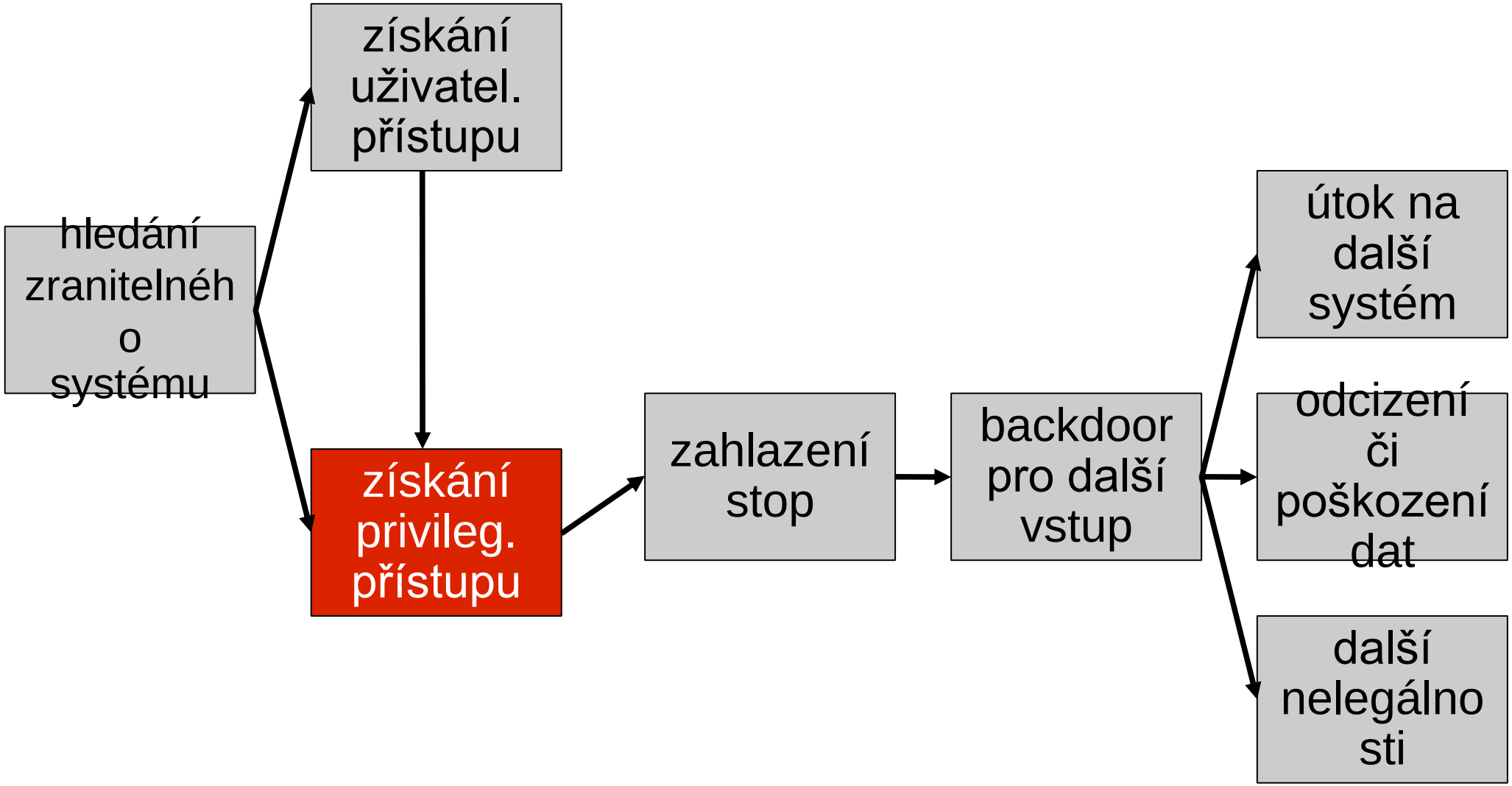
- **chovejte se rozumně**
  - čím blíže k undergroundu, tím blíže k problémům
  - čerpejte SW a data ze seriózních zdrojů
- **nejvíce malware je pro většinové programy**
  - MS Windows + IE + Outlook = největší riziko
  - raději Firefox či Operu než IE, raději Thunderbird než Outlook
  - chcete brouzdat po rizikových webech? pořiďte si na to Live CD s Linuxem (např. Ubuntu)

vytvořeno s podporou
projektu ESF

Bezpečnost sítí – útoky

- na počítač číhá mnoho rizik
  - napadení místním uživatelem (krádež/poškození dat)
  - napadení po síti
  - krádež
  - požár,...
- ochrana něco stojí (peníze, komfort, flexibilitu,...)
- je třeba chovat se rozumně – zhodnotit, jaká je pravděpodobnost a důsledky ohrožení, co stojí ochrana proti němu a zda se vyplatí

Schéma síťového útoku



Hledání cíle

- **sociální metody**
  - zmíněné již u virů, hledá se nezabezpečený systém pomocí nepočítačových metod
  - nejhorší průniky
- **scanování a OS fingerprint**
  - speciální aplikace zjišťuje, jaké porty (služby) jsou otevřené na cílovém počítači
  - části definice TCP/IP nejsou jednoznačné, pakety se liší podle systému – vytvářejí identifikační otisk systému, lze se pak zaměřit na známé slabiny daného systému

Princip scanování

- základ triviální – pokusí se navázat TCP spojení
  1. odešle paket SYN
  2. server přijme (SYN/ACK) nebo zamítne (SYN/RST)
  3. vyzyvatel spojení zahájí (ACK) nebo ukončí (RST)
- zanechá jasnou stopu k útočníkovi (žádost o spojení zaznamenána do logu)
- speciální programy obsahují metody, které dokážou tento záznam potlačit

Nmap

- jeden z nejpoužívanějších scannerů
- http://nmap.org/
- multiplatformní (Unix, Windows, MacOS,...)
- grafická nadstavba Zenmap
- obsahuje řadu scanovacích metod, nejpoužívanější
  - TCP connect
  - TCP SYN

Nmap TCP connect

- nejzákladnější forma port scanu
- systémovým voláním connect() otevře systém spojení
- pokud byl přijat (port je otevřen), skončí úspěšně, jinak chybou
- volání connect() nevyžaduje speciální oprávnění
- dojde k záznamu do logu

Nmap TCP SYN

- známé také jako half-open
- pošle SYN paket jako při otevírání spojení, čeká na odpověď
  - dorazí-li SYN/ACK, je port otevřen
  - odpověď RST znamená zavřený port
- při úspěchu spojení hned přeruší (RST) – navázání nebylo potvrzeno a nemusí se zapsat do logu
- obvykle vyžaduje administrátorská práva pro spuštění

Použití Nmap

- je rozumné pravidelně či příležitostně nechat Nmapem zkontrolovat vlastní stroj, zda nejsou otevřeny nežádoucí porty
- existují i on-line nástroje (www.auditmypc.com)
  - neumí scanovat stroj za firewallem/NATem
  - provozovatel se dozví o slabinách vašeho systému, věříte mu dostatečně?
  - lépe scanovat lokálně

HW útoky (1)

- **fyzické útoky**
  - cílem je fyzické poškození síťového HW – přerušení kabeláže, vyřazení aktivních prvků apod.
  - záležitost zejména lokálních sítí
- **rušení signálu**
  - pomocí silného elektromagnetického zářiče blízko síťových rozvodů
  - narušení mikrovlnného spoje
  - mnohdy neúmyslné, o to hůře odhalitelné

HW útoky (2)

- **odposlechy**
  - fyzické odposlechy (např. modemu nebo teoreticky i signálu v kabelu)
  - SW odposlech Ethernetu – sdílené médium doručí signál každému, kdo je připojen; postačí přepnout kartu do tzv. promiskuitního režimu (přijímá všechna data, nejen ta, která jí patří); přepínače komplikují
  - využívá se i při řešení problémů se sítí
  - program Wireshark (www.wireshark.org), bývalý Ethereal

SW útoky (1)

- pomocí chyb v programech
  - **přetečení zásobníku (stack overflow)** – aplikace zapíše do paměti, kam normálně nemá přístup; vede k provedení útočníkova programu
    ochrana: aktualizovat aplikace
  - **backdoor** – přístup, který si vytvořil autor programu pro ladění aplikace; může později posloužit útočníkovi
    ochrana: může odhalit scanování

SW útoky (2)

- **útoky proti WWW**
  - populární, jistá forma grafitti
  - díky skriptovacím jazykům typu PHP dnes pro WWW programuje téměř každý
  - řada programátorů se spokojí s dosažením požadovaných funkcí, bezpečnost neřeší – např. předávání parametrů v URL
  - volné programy někdy obsahovaly či obsahují chyby
  - nevěřit ničemu, co posílá klient (lze falšovat)

SW útoky (3)

- **podvržení identity**
  - IP spoofing – do odchozích paketů je vkládána falešná (cizí nebo podvržená) IP adresa
  - odpověď se nevrátí zpět – výsledek útoku je třeba předat jinak
  - source routing – varianta, útočník se vydává za důvěryhodný počítač, který předtím vyřadil pomocí DoS útoku

DoS útoky (1)

- **Denial of Service**
- cíl útoku je vyřazen z činnosti, často zahlcen
- někdy jako součást jiného útoku či zahlazení stop
- **DoS pomocí chyb v implementaci IP**
  - **PingOfDeath** – odeslání příliš velkého paketu pomocí ping, nekontrolující příjemce se zhroutil
  - **Teardrops** – využívá chyby při skládání fragmentovaných paketů (posílá nekorektní fragmenty)

DoS útoky (2)

- **DoS pomocí nedokonalostí TCP/IP**
  - **SYN flooding**
    - útočník zahájí navázání TCP spojení (pošle paket SYN)
    - cíl potvrdí (SYN ACK) a alokuje pro otevírané spojení zdroje
    - útočník ale nedokončí navázání spojení, místo toho zahajuje otevírání dalších a dalších spojení
    - cíl postupně vyčerpá své zdroje a přestane přijímat žádosti o spojení od regulérních klientů
    - řešení: zkrátit dobu čekání na potvrzení navázaného spojení od klienta, alokovat pro ně zdroje až po potvrzení

DoS útoky (3)

- **DoS pomocí nedokonalostí TCP/IP**
  - **Land attack** – varianta SYN útoku, v žádosti o spojení je jako adresát i odesilatel uveden cílový stroj, ten se zahltí zasíláním potvrzení sám sobě
  - **Smurf** – zahlcení cíle ICMP pakety (ping), jejich zpracování mívá někdy přednost před běžným provozem; útočník pošle žádost o ping všem (broadcast) a jako odesilatele uvede cíl útoku
  - **DNS útok** – podobný předchozímu, jen místo ICMP používá DNS dotazy a odpovědi

DoS útoky (4)

- **DDoS – Distributed Denial of Service**
  - DoS útok vedený souběžně z mnoha stanic
  - na nezabezpečené počítače je distribuován útočný program (označován jako zombie), např. virem
  - v určitý čas útočník vzbudí zombie a pošle je současně na cíl
  - mnoho různých variant, zejména v přístupu k synchronizaci zombie
  - obtížně se blokuje – zdrojů je příliš mnoho

Ochrana před útoky

- mnoho úrovní zabezpečení
  - autentizace uživatelů sítě – nepovolaným vstup zakázán
  - zabezpečení stanic – ochrana dat zbytku sítě (napadená stanice se stává nástrojem dalšího útoku)
  - zabezpečení provozu – sledování provozu sítě, vnitřní filtrování; nejnebezpečnější útoky jsou zevnitř
  - zabezpečení LAN – ochrana LAN před útoky z Internetu
  - zabezpečení na úrovni poskytovatele – neexistuje internetová bezpečnost, ale řadu věcí poskytovatelé sledují či omezují

Lapač útoků

- počítač (nejlépe vyhrazený pro tento účel), který analyzuje přicházející pakety, hledá v nich příznaky útoků a upozorňuje správce
- cenná služba při zjišťování útoků a ochraně před nimi
- vyžaduje ale soustavný dohled a rychlou reakci na zjištěné problémy
- realizuje program Snort (www.snort.org)

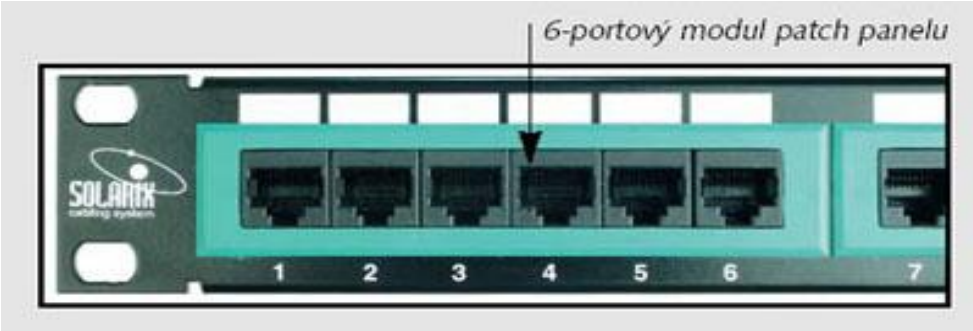
vytvořeno s podporou
projektu ESF

Strukturovaná kabeláž (1)

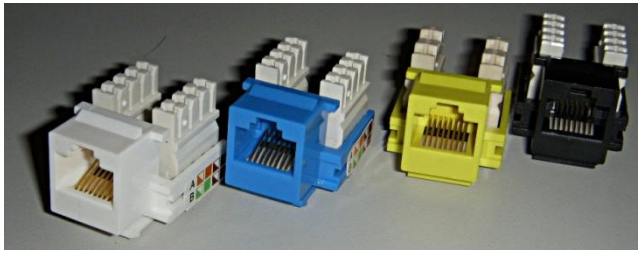
- **rack**
  - skříň, obvykle zamykatelná
  - obsahuje propojovací (patch) panely, aktivní prvky, někdy i servery a další komponenty
  - vnitřní šířka 19“
  - výška rozhoduje o kapacitě, měří se v „U“ (1 U=1,75 in=4,45 cm)

Strukturovaná kabeláž (2)

- **patch panel**
  - blok označených zásuvek
  - na rubu svorkovnice pro připojení kabelů

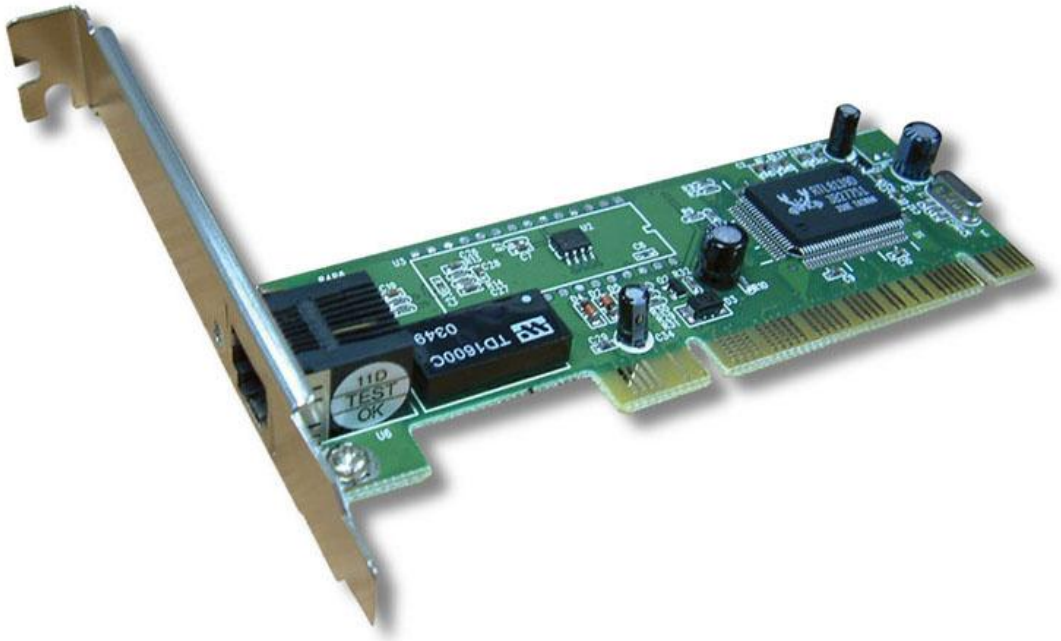


- **zásuvka**
  - různá provedení – na zeď, pod omítku, do lišt apod.
  - uvnitř obsahuje tzv keystone



Síťová karta

- propojuje počítač se sítí
- dnes obvykle na základní desce, může být ale samostatná



Aktivní prvky

- předávají pakety a rekonstruují je
- dnes prakticky výlučně **přepínače (switche)**
  - předávají paket jen na port, kde se nachází příjemce
  - zjišťují automaticky z procházejících paketů (plug&play)
  - optimalizace výkonu a propustnosti
  - dva režimy práce:
    - **store&forward** – načte celý rámec do bufferu (store) a pak jej předá (forward)
    - **cut-through** – načte pouze hlavičku a hned předává dál

Typy přepínačů

- **jednoduché koncové**
  - plug&play bez možnosti nastavení
  - laciné
- **páteřní**
  - pokročilé možnosti konfigurace
  - VLAN, bezpečnostní mechanismy, dálková správa,...
  - podstatně dražší

Potíže přepínačů

- musí zkoumat obsahy všech rámců
- musí šířit všesměrové vysílání (broadcast)
- dodržují forward-if-not-local
  - předávají, kdykoli rámec není lokální
  - nezkoumají, zda příjemce existuje – mohou předávat zbytečně
- mají problém s redundantními cestami (cykly)
  - spanning tree – dohoda na nepoužívání některých spojů

Směrovače

- pracují v síťové vrstvě (typicky s protokolem IP, mohou být i jiné)
- koncové počítače je „vidí“ a musí s nimi cíleně spolupracovat (konfigurace default gateway)
- základem práce směrovací tabulka s nejlepšími cestami ke známým cílům
- směrovač obvykle provozuje jeden či několik směrovacích protokolů aktualizujících jeho směrovací tabulku

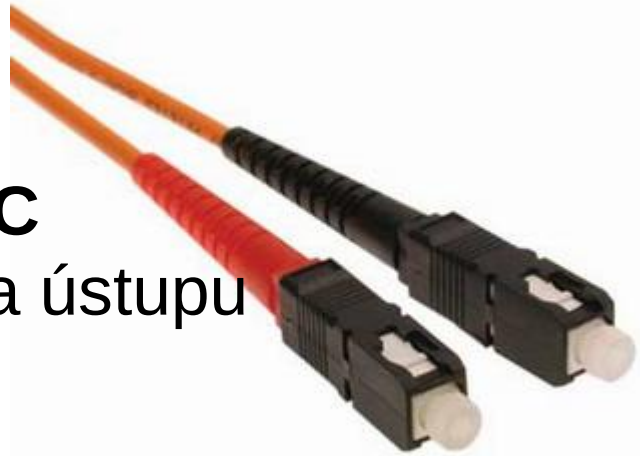
L3 přepínač (L3 switch)

- módní pojem
- kombinace ethernetového přepínače s rychlým jednoduchým směrovačem
  - známé síťové protokoly směruje, ostatní přepíná
  - konfigurací lze nastavit chování podle potřeby
  - směrování a přepínání velmi rychlé (wirespeed)
- určeny pro LAN, kde dnes představují de facto standard pro směrovače

Optické vlákno

- nejčastější typy konektorů

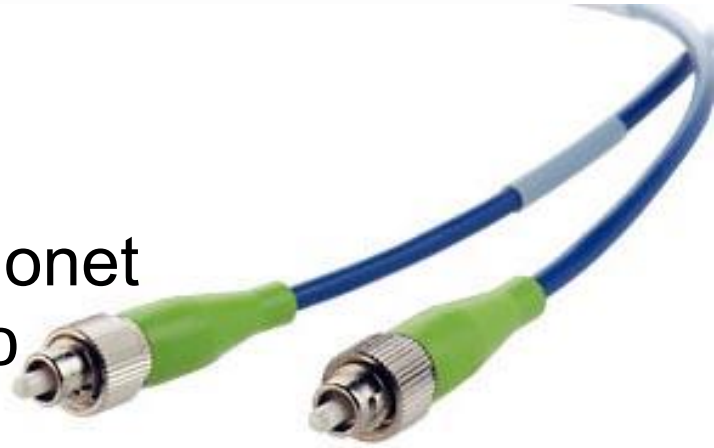
E2000
nejpřesnější, nejdražší,
používány v telekomunikacích



SC
na ústupu

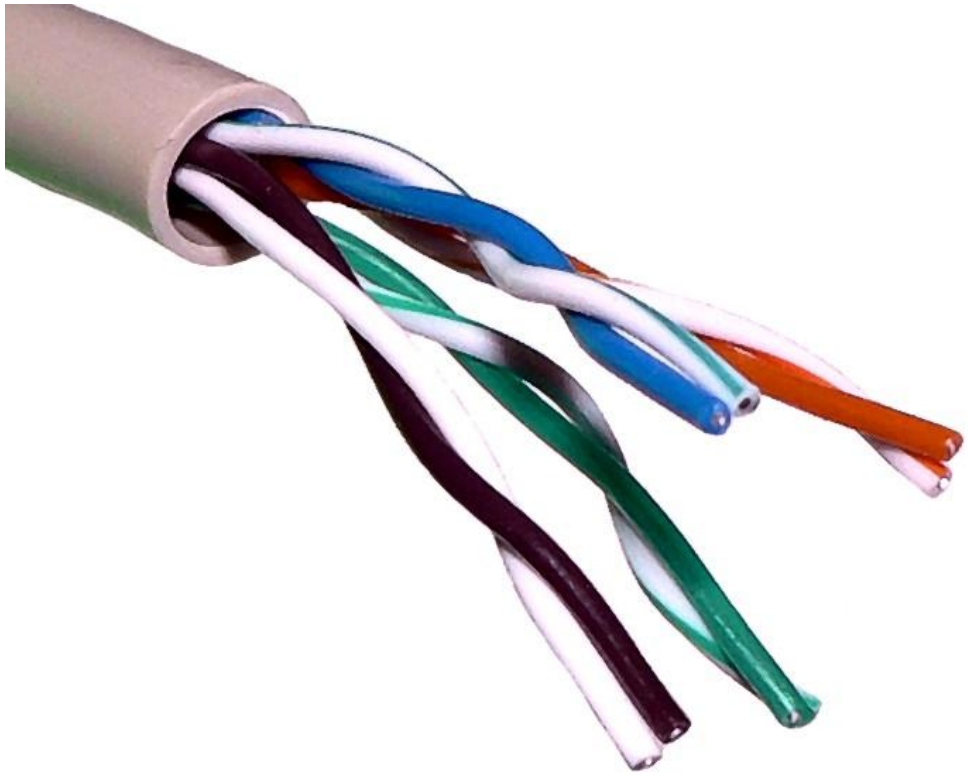
LC
moderní

ST
nejhorší, bajonet
kroutí vlákno



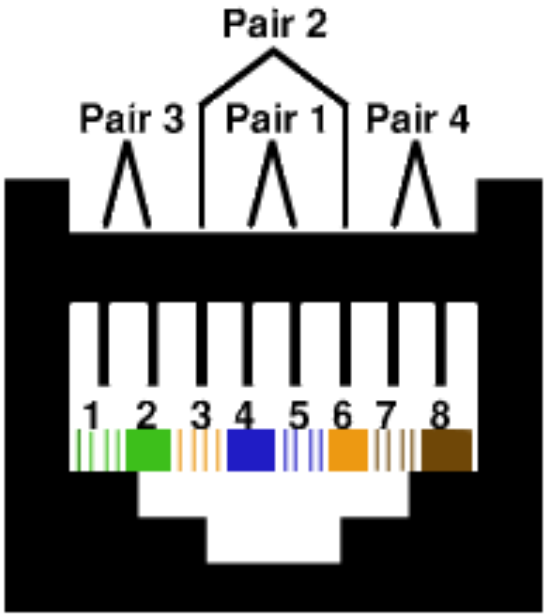
UTP – kroucená dvojlinka

- 4 páry:
  - modrý
  - oranžový
  - zelený
  - hnědý
- jeden vodič celobarevný, druhý v kombinaci bílé a barvy

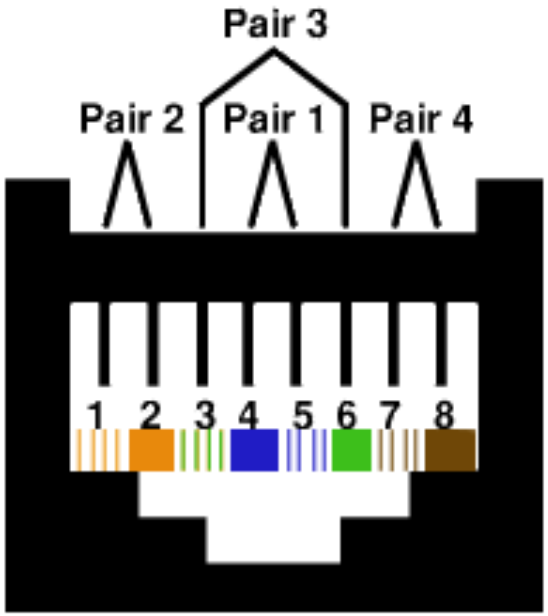


Zapojení UTP

- dva standardy: T568A a T568B, mají prohozený zelený a oranžový pár; v praxi nevadí (jen je třeba, aby oba konce jednoho kabelu byly zapojeny stejně)



T568A

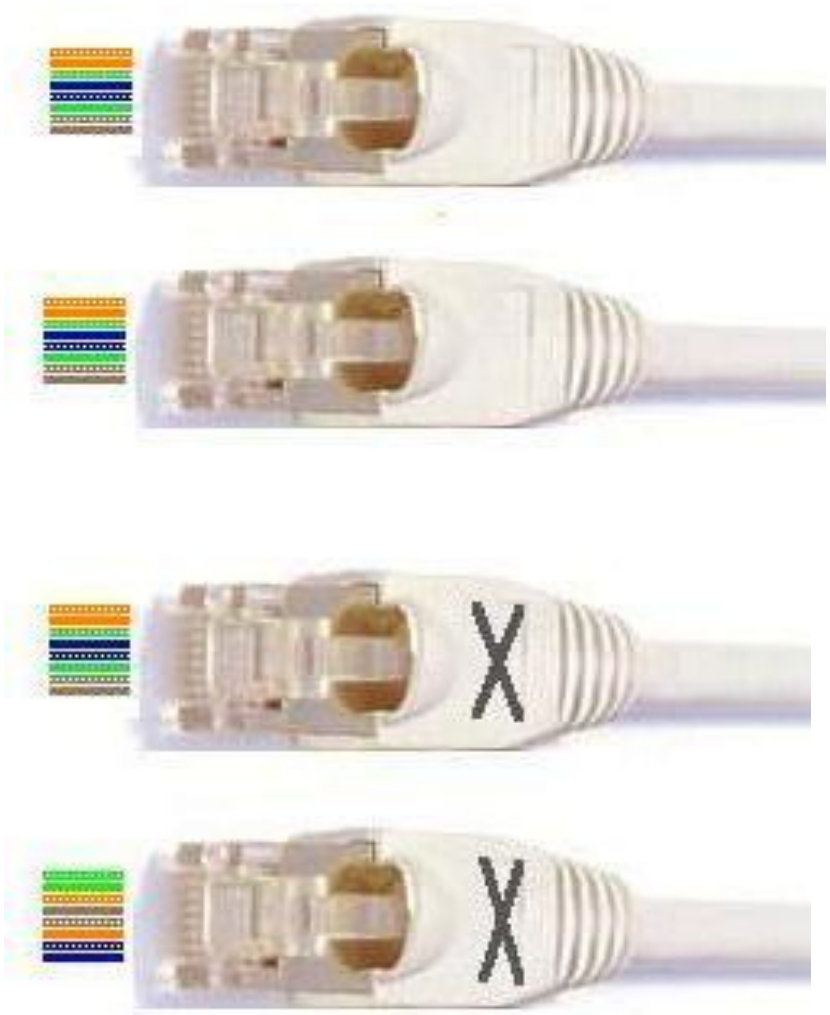


T568B

pohled zepředu na zásuvku

UTP kabel

- **standardní**
  počítač–switch
  1–1, 2–2, 3–3, 4–4,
  5–5, 6–6, 7–7, 8–8
- **křížený**
  počítač–počítač nebo
  switch–switch,
  dnes autodetekce
  1–3, 2–6, 3–1, 4–8,
  5–7, 6–2, 7–5, 8–4



vytvořeno s podporou
projektu ESF

Autentizace uživatelů

- základní prvek ochrany sítí a systémů
- kromě povolování přístupu lze uživatele členit do skupin, nastavovat různá oprávnění apod.
- nejčastěji dvojicí **jméno** a **heslo**
- další varianty:
  - jednorázová hesla
  - identifikace hardwarem – kartou, klíčem,...
  - biometrická identifikace – otisky prstů, sítnice, hlas,...

Průnik

- jednou z nejsnadnějších cest k útoku je získat heslo existujícího uživatele (nejlépe superuživatele)
- útoky na hesla
  - **hrubou silou** – program zkouší hromady hesel
  - **sociální** – ze znalosti uživatele útočník zkouší uhodnout heslo

Útoky hrubou silou

- zkouší všechny možné kombinace
- slovníkový útok – zkouší slova ze slovníku + jejich modifikace
- **obrana před online útokem**
  - zablokování účtu po několika špatných heslech
  - prodlužování časové odezvy
- **obrana před offline útokem**
  - periodická změna hesla (frekvence podle důležitosti)
  - kvalitní heslo

Sociální útoky

- útok využívá osobní informace (uživatelské jméno? obráceně? jména dětí? datum narození? SPZ auta?)
- mnohdy je horší – hesla na papírku na monitoru
- ochrana:
  - hesla by neměla vycházet z vašich osobních údajů
  - generátory hesel (http://www.converter.cz/passgen/ apod.) vytvářejí silná hesla, ale obtížně zapamatovatelná

Silná zapamatovatelná hesla

- pomocí mnemotechnické pomůcky
  - vyjděte z průpovídky, názvu knihy nebo písně, měla by obsahovat nepísmenné znaky
  - heslo z prvních znaků slov a nepísmenných znaků
  - příklad:
    - **sNdz,nl** – šla Nanynka do zelí, natrhala lupení
    - **Kz25.A:Ch** – Kurtizány z 25. Avenue: Chemie
    - **MV:Blpp,92** – Michal Viewegh: Báječná léta pod psa, 1992
  - se znalostí sloganu se snadno pamatují, bez něj působí zcela chaoticky

Autentizace v síti

- základní problém: přenos hesla sítí
  - nešifrované heslo – minulost, lze odposlechnout
  - šifrovaný přenos – řada systémů i algoritmů
  - centrální autentizace – řada systémů, často jen pro jedno prostředí (Windows Domain, Novell)
  - multiplatformní řešení – Kerberos, DCE, Sesame

Kerberos (1)

- autentizační systém původem z MIT (projekt Athena)
- řeší centrální autentizaci uživatelů a služeb
- základem centrální server s databází uživatelů a serverů
- vhodný do distribuovaného prostředí
- jeden server lze zabezpečit snadněji – jak z hlediska sítě, tak z hlediska fyzické bezpečnosti

Kerberos (2)

- základní princip: vstupenky (tickets)
  - přenos hesla (i šifrovaný) je potenciálním rizikem
  - lístek – jednorázové oprávnění pro přístup ke službě, platí pro konkrétní službu omezenou dobu – snižuje riziko zneužití
  - základem práce v systému je TGT – Ticket to Grant Ticket (vstupenka pro získání vstupenek), slouží jako identifikátor uživatele pro další autentizace

Získání TGT

- v přihlašovacím dialogu uživatel zadá jméno a heslo
- heslem se zašifruje aktuální čas (silné šifrování algoritmem 3DES) a spolu se jménem odeslán na autentizační server
- server příslušným heslem dešifruje čas a porovná se svým (ochrana proti podvržení vstupenky)
- je-li autentizace úspěšná, vygeneruje TGT a zašifrované heslem vrátí uživateli

Kerberos – použití

- po autentizaci uživatel získá od serveru klíč k sezení a dále vstupenku pro další autentizaci zašifrovanou jak klíčem sezení, tak klíčem služby pro autentizaci
- při použití síťové služby (např, souborový server) pak s použitím klíče požádá autentizační server o vstupenku opravňující k jejímu použití; její součástí je identifikace používané služby – klient má jistotu, že používá skutečně požadovaný server, nikoli jeho padělek

Kerberos – výhody

- heslo se nepřenáší sítí v žádné podobě
- vstupenky mají omezenou životnost – snižuje riziko jejich zneužití (opakování)
- klíč sezení se generuje náhodně a má omezenou životnost – není technicky možné zjistit jej hrubou silou (nestihne se)
- multiplatformní – lze autentizovat uživatele ve Windows, v Linuxu i dalších systémech

Kerberos – nevýhody

- neřeší problém sociálních útoků
- každá služba, aplikace či operační systém, které chceme použít, musí být speciálně upraveny (tzv. kerberizovány)
- dojde-li k průniku na autentizační server, má útočník hesla všech uživatelů

Šifrování

- ochrana citlivých dat
- již staří Římané...
- značný rozmach ve 20. století (telegraf, války, sítě)
- Kryptologie – věda o šifrách
- Kryptografie – část kryptologie zabývající se převedením srozumitelné zprávy do nesrozumitelné podoby a zpět (šifrování a dešifrování)
- Kryptoanalýza – část kryptologie zabývající se odhalením klíče

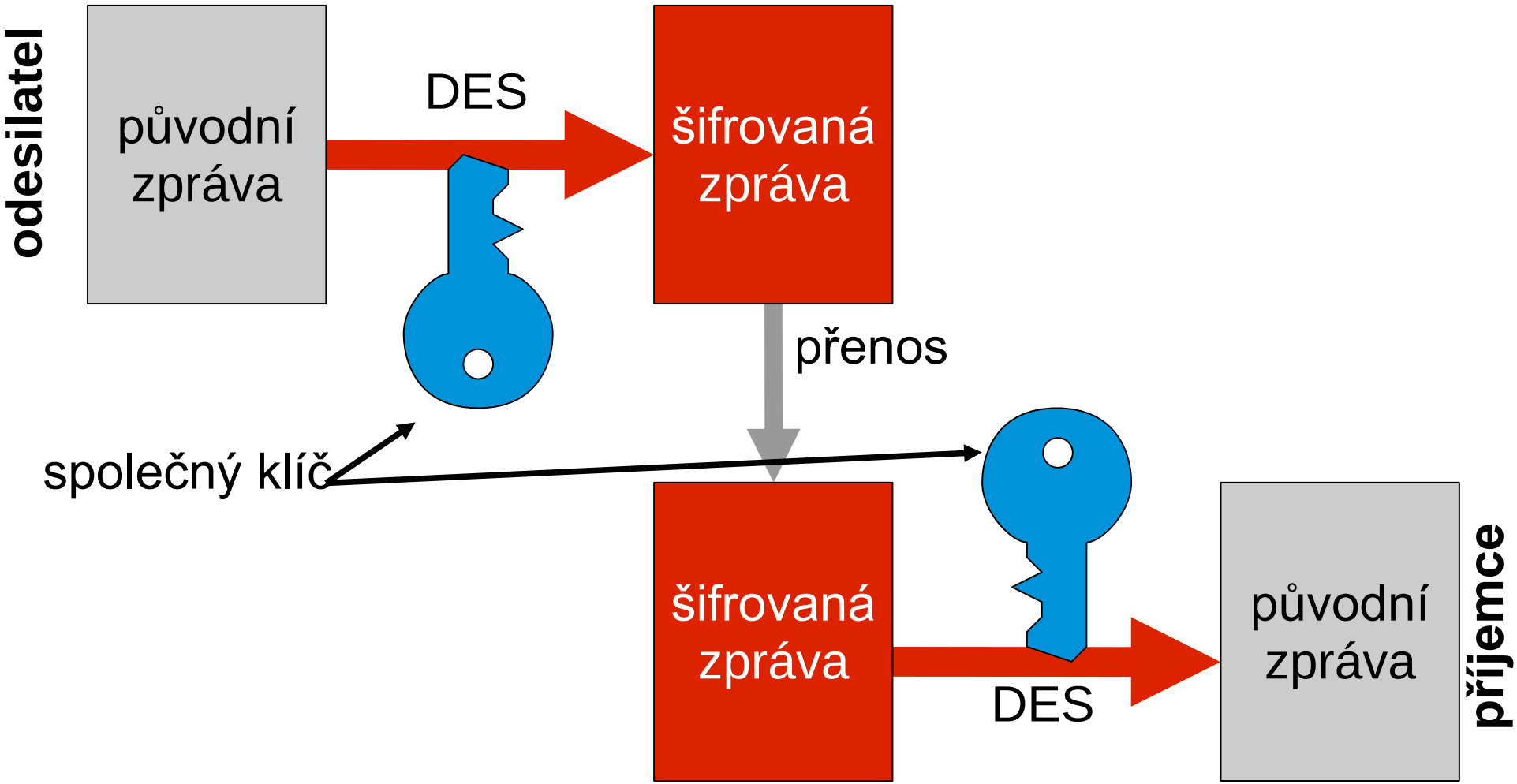
Šifrovací algoritmy

- základní dělení:
  - symetrické – obě strany používají stejný klíč
  - asymetrické – každá strana má jiný klíč

Symetrické šifrování

- stejný klíč pro šifrování i dešifrování
- algoritmy: DES, 3DES, CAST, IDEA, Blowfish
  většinou velmi rychlé
- algoritmy jsou veřejně popsány, bezpečnost vychází z jejich principů, síla šifer se vyjadřuje délkou klíče
- za bezpečné jsou považovány klíče nad 128 b
- problém: každá dvojice potřebuje svůj klíč, jak si je předávat?

Symetrické šifrování



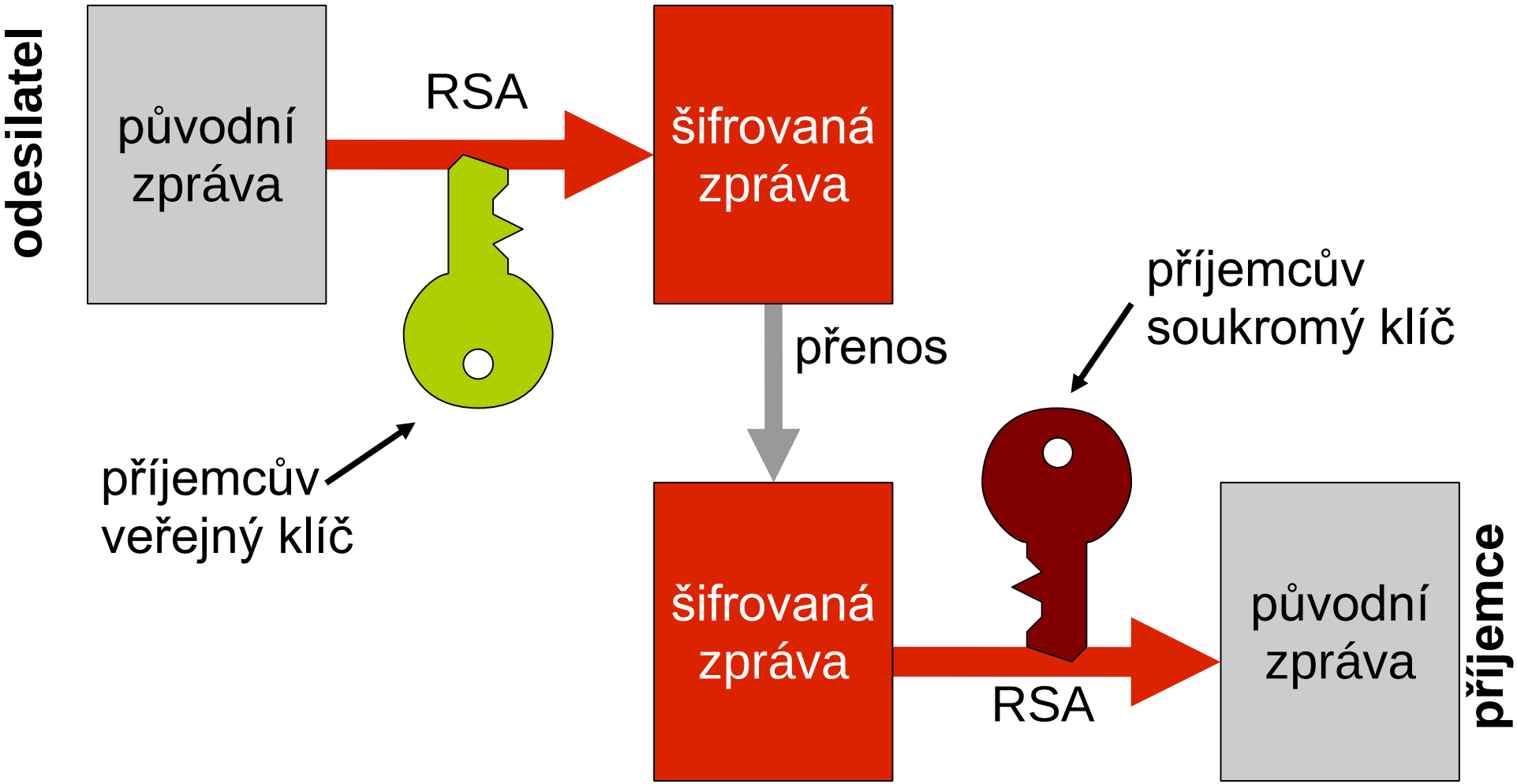
DES, 3DES

- Data Encryption Standard, navržený pro banky
- vznik: 1975 IBM, původně s klíčem 256 b (algoritmus Lucifer), později omezeno na 56 b
- DES není považován za bezpečný, HW dekodéry rozluští klíč během několika hodin
- 3DES data šifruje třikrát, stejným či několika klíči (celková délka klíče pak 168 b)
- podstatou algoritmu je 16 opakování základního permutačního kroku, implementován HW

Asymetrické šifrování

- dvojice klíčů: veřejný a soukromý
  - veřejný může použít kdokoli pro zašifrování zprávy
  - dešifrovat lze jen pomocí soukromého klíče
  - soukromý klíč neopustí vlastníka, nelze jej odvodit z veřejného
- algoritmy RSA, Diffie-Hellman, DSS
  mnohem (řádově 1000x) pomalejší než symetrické
- klíče o velikosti i několika kilobitů

Asymetrické šifrování



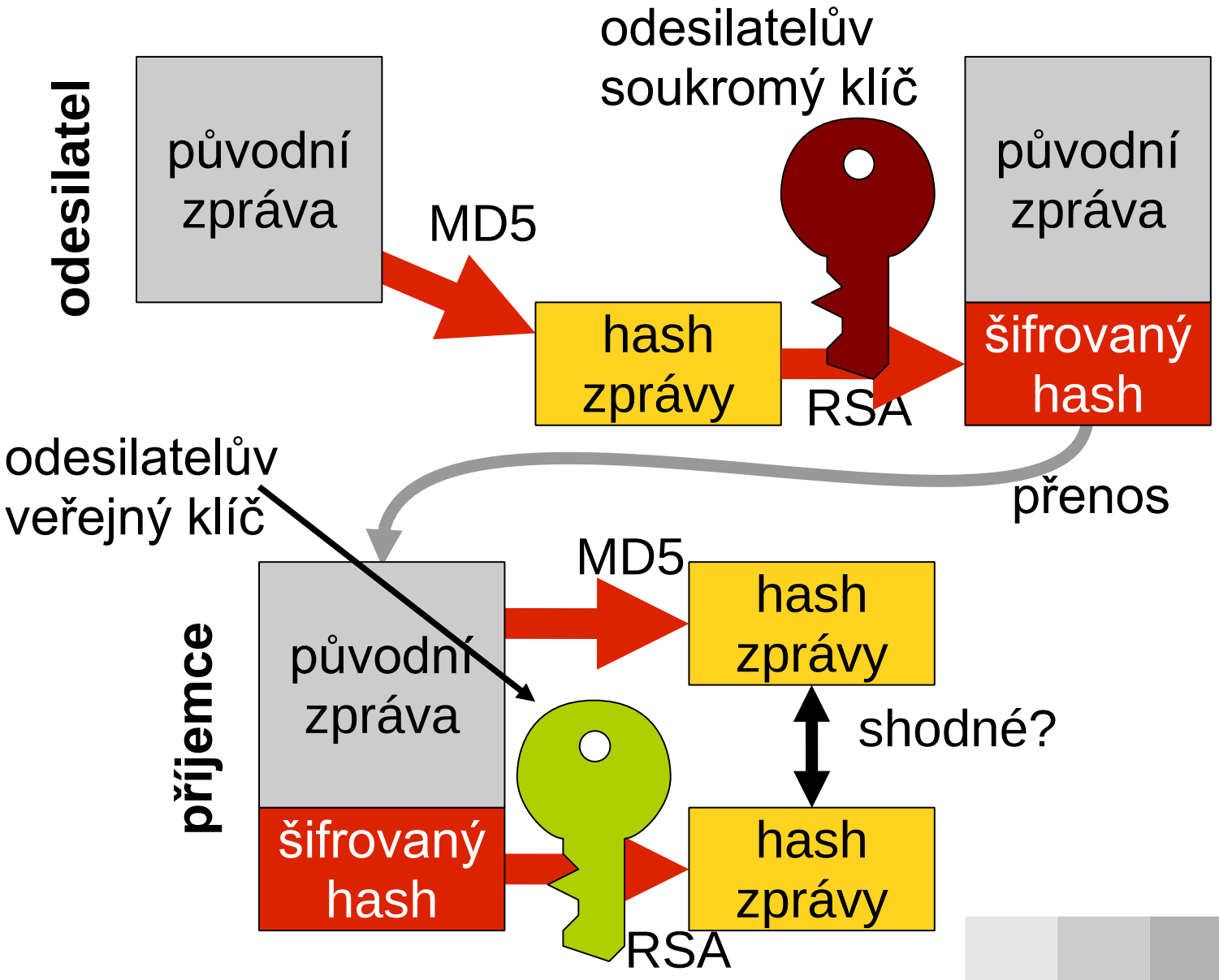
RSA

- Ron Rivest, Adi Shamir, Len Adleman (1977)
- nejznámější asymetrická šifra, základ většiny asymetricky šifrujících systémů
- založen na problému faktorizace (rozklad na součin prvočísel) velmi velkých čísel
  - velmi asymetrické: znám-li prvočísla, snadno spočítám jejich součin; znám-li součin, najít prvočísla je velmi těžké
- doporučují se klíče alespoň 2048 b

Digitální podpis

- vychází z asymetrického šifrování
- ke zprávě se vytvoří kontrolní součet (hash), např. algoritmem MD5
- tento kontrolní součet se šifruje soukromým klíčem
- příjemce dešifruje veřejným klíčem odesilatele a pokud souhlasí s kontrolním součtem došlé zprávy
  - zpráva pochází skutečně od odesilatele
  - zpráva nebyla cestou změněna

Digitální podpis



Kombinované šifrování

- žádná z metod není ideální
  - symetrické šifrování vyžaduje stejné klíče
  - asymetrické šifrování je výpočetně náročné (pomalé)
- řešení: kombinace obou metod
  - zpráva se zašifruje symetrickou šifrou
  - klíč pro symetrickou šifru se zašifruje asymetricky a přiloží ke slávě
  - asymetricky se šifrují/dešifrují jen malá data, klíč pro symetrickou šifru se přepraví bezpečně

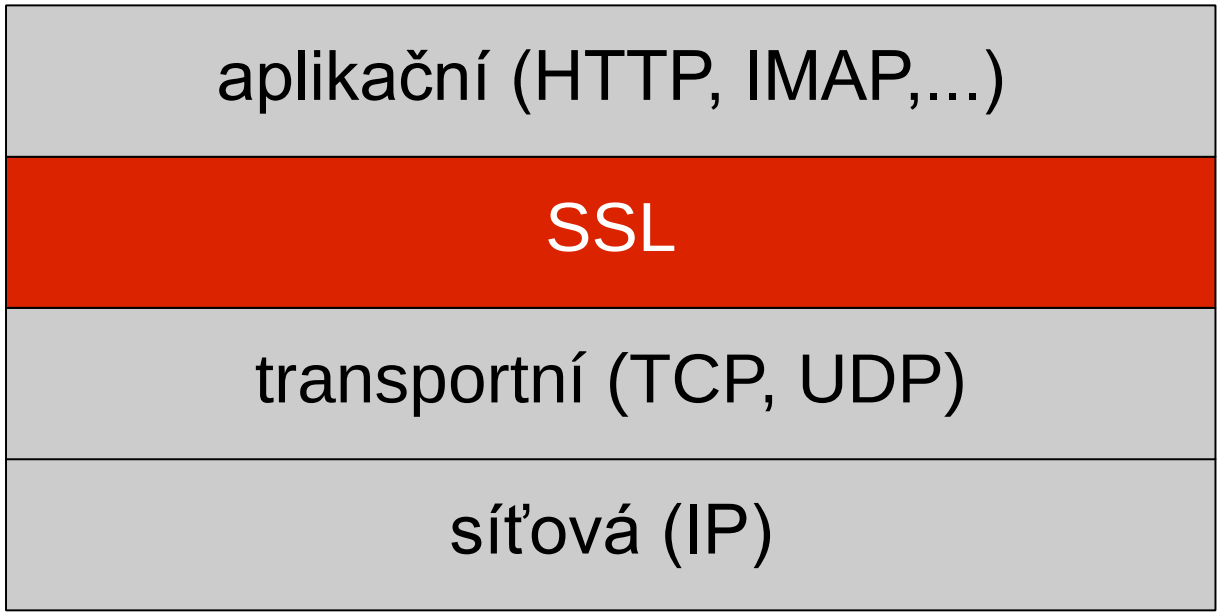
Problém distribuce klíčů

- veřejné asymetrické klíče lze volně distribuovat
- jak **důvěryhodně** získat něčí veřejný klíč?
- **certifikáty**
  - organizace (certifikační autorita, CA) potvrdí svým podpisem, že klíč patří danému uživateli či serveru
  - veřejný klíč CA potvrdí svým certifikátem vyšší CA
  - hierarchie CA – **Public Key Infrastructure (PKI)**
  - teoreticky stačí veřejný klíč kořene PKI k ověření všeho
  - těžké politické a obchodní boje o kořen – PKI nemáme

vytvořeno s podporou
projektu ESF

SSL – Secure Sockets Layer

- internetové aplikační protokoly jsou nezabezpečené
- SSL vkládá do architektury šifrující vrstvu



SSL

- poskytuje zabezpečenou komunikaci klient-server
- univerzální, mohou jej využívat různé aplikační protokoly
- využívá kombinaci šifrovacích algoritmů
  - asymetrické při navázání spojení a výměně klíčů
  - symetrické pro šifrování vlastní komunikace
  - kontrolní součty pro zajištění integrity dat

Navázání SSL komunikace

- server při oslovení pošle klientovi svůj veřejný klíč a certifikát dosvědčující jeho pravost
- klient vygeneruje náhodný blok dat a pošle (zašifrovaný) serveru
- server z něj vybere část a informuje klienta o svém výběru; vybraná data se nazývají Master Secret, z nich se vygeneruje symetrický klíč a přidávají se k přenášeným datům
- data jsou pak přenášena spojeními (connections)

SSL sezení

- základem přenosu je sezení (session), parametry:
  - Session ID – libovolná hodnota identifikující sezení
  - Peer Certificate – X.509.v3 certifikát protějšku
  - kompresní metoda
  - údaje pro šifrování (algoritmus, MAC,...)
  - Master Secret
  - a další

SSL spojení

- každé sezení může obsahovat několik spojení (connection), spojení ale patří do jediného sezení
- parametry spojení:
  - náhodné číslo generované serverem i klientem
  - SERVER-MAC-WRITE-SECRET
  - CLIENT-MAC-WRITE-SECRET
  - SERVER-WRITE-KEY
  - CLIENT-WRITE-KEY
  - a další

Činnost SSL

- **Record Layer Protocol (RLP)** představuje pro aplikační vrstvu celou SSL vrstvu, jeho pomocí se realizují jednotlivá spojení
- přenášená data procházejí následujícím procesem:
  - **fragmentace** – rozdělení do bloků
  - **komprimace** – původní obsah je komprimován
  - **vytvoření MAC** – (Message Authentication Code) kontrolní součty se vytvoří dohodnutým hash algoritmem
  - **šifrování** – opět dohodnutým algoritmem
  - příjemce postupuje opačně

Handshake Protocol (HP)

- dohaduje parametry sezení; postup:
  - ověření serveru klientem
  - vyjednání společných šifrovacích algoritmů
  - ověření klienta serverem (volitelně)
  - použití asymetrického šifrování pro výměnu sdílených hesel
  - ustavení zabezpečeného SSL spojení (connection)
- pro RLP je dalším aplikačním protokolem – zprávy HP se balí do RLP

Další protokoly SSL

- **Change Cipher Specification Protocol (CCSP)**
  - pro nastavení parametrů prostředí
  - HP dohodne parametry, CCSP zajistí jejich nastavení
- **Alert Protocol (AP)**
  - signalizace problémů druhé straně
  - podobný účel jako ICMP pro IP

TLS

- **Transport Layer Security**
- nástupce SSL, vychází ze SSL verze 3
- obsahuje několik drobných vylepšení, obecné principy jsou stejné
- zatím je rozšířenější SSL

SSH

- Secure Shell
- bezpečná varianta programů pro vzdálené připojení
- celá komunikace šifrována symetrickým algoritmem (3DES, Idea, Blowfish), navíc lze komprimovat
- pro výměnu klíče a základní autentifikace se používá RSA
- může také vytvářet bezpečná spojení (tunely) pro ostatní protokoly (POP3, X Window,...)

Transportní protokol SSH

- definuje formát paketu
- zajišťuje případnou kompresi
- ověřuje integritu – MAC z tajného sdíleného čísla, pořadí paketu a obsahu zprávy, SHA-1 nebo MD5
- symetrické šifrování dat, 3DES, Blowfish, Arcfour, Idea, data obou směrů se šifrují nezávisle
- algoritmy veřejných klíčů pro autentizaci
- algoritmy pro výměnu klíčů (RSA, Diffie-Hellman)

Autentizační protokol SSH

- využívá transportní vrstvu SSH
- **autentizace veřejným klíčem** – povinná, server může vyžadovat další
- **autentizace heslem** – server kontroluje v databázi systému; heslo se nesmí poslat, dokud není plně zajištěno šifrování a MAC
- **autentizace na hostitelském počítači** – ověření identity se provede podepsáním zprávy klíčem hostitelského počítače (nemusí brát ohled na uživatele)

Spojovací protokol SSH

- pracuje nad transportní a autentizační vrstvou
- umožňuje interaktivní přihlášení, vzdálené spouštění příkazů, přesměrování TCP/IP a X11 spojení (tunely)
- pro přenos používá tzv. kanály
  - kanálem je terminálové nebo přesměrované spojení
  - mohou vzniknout na obou stranách komunikace
  - identifikovány čísly

SSH tunely

- SSH umožňuje vytvořit bezpečný kanál pro běžné TCP spojení
  - např. POP3 tunel na server pop.kdesi.cz se vytvoří ssh -L 1110:pop.kdesi.cz:110 pop.kdesi.cz
  - vede ze zdejšího portu 1110 na port 110 na stroji pop.kdesi.cz
  - v konfiguraci poštovního programu je třeba změnit identifikaci serveru na localhost a číslo portu na 1110
  - na stroji pop.kdesi.cz musí běžet SSH server, který umožní přihlášení

SSH pod Windows

- původně jen placené implementace, dnes již řada volných
- přehled na **www.freessh.org**
- nejpoužívanější je **Putty**
  - http://www.chiark.greenend.org.uk/~sgtatham/putty/
  - jednoduchý klient
  - grafická konfigurace
  - podporuje tunely

Firewall

- původně pro oddělení LAN od Internetu
  - pustit dovnitř jen povolená data
  - nikdy nechrání 100%, nelze rezignovat na bezpečnost počítačů za firewallem
- **personální firewall**
  - běží na koncovém počítači a kontroluje/omezuje jeho síťovou komunikaci
  - dnes považován za důležitý prvek bezpečnosti počítače
  - obsažen ve Windows (XP a novější), jiné jsou lepší (Sunbelt, Comodo), pro osobní využití bývají zdarma

Typy firewallů

- **filtrování síťové vrstvy (IP adres)**
  - přístup jen z povolených adres, nedostatečné
- **filtrování transportní vrstvy**
  - povolují se jen určité služby (kombinace portů a adres)
- **stavová inspekce**
  - ukládá si informace o TCP spojeních a data kontroluje v souvislosti s předchozím provozem
- **filtrování aplikační vrstvy**
  - pro konkrétní aplikační protokol, musí být nastaven v aplikaci (proxy)

vytvořeno s podporou
projektu ESF