Základy informatiky

05 Internetové technologie

Michal Kačmařík, Daniela Szturcová

Obsah přednášky

- Internet
  - Vznik a vývoj
  - Služby
  - Princip
  - Možnosti připojení
- HTTP, URL, IP, DNS
- Kybernetická bezpečnost

Vznik Internetu

1962 – vzniká projekt počítačového výzkumu agentury DARPA

1969 – vytvořena experimentální síť ARPANET

1987 – vzniká pojem Internet

1987 – propojení 27 000 počítačů do sítě

1989 – Tim Berners-Lee, vedoucí projektu, jehož cílem bylo vytvořit infrastrukturu pro sdílení vědeckých výsledků.

- Protokol http
- Adresování objektů pomocí URL
- Jazyk HTML

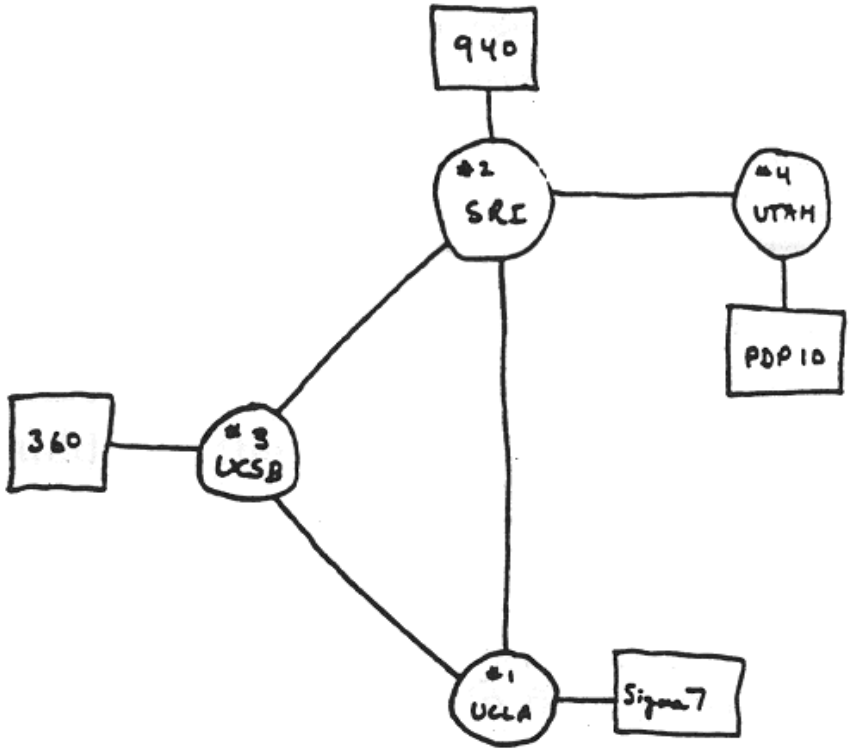
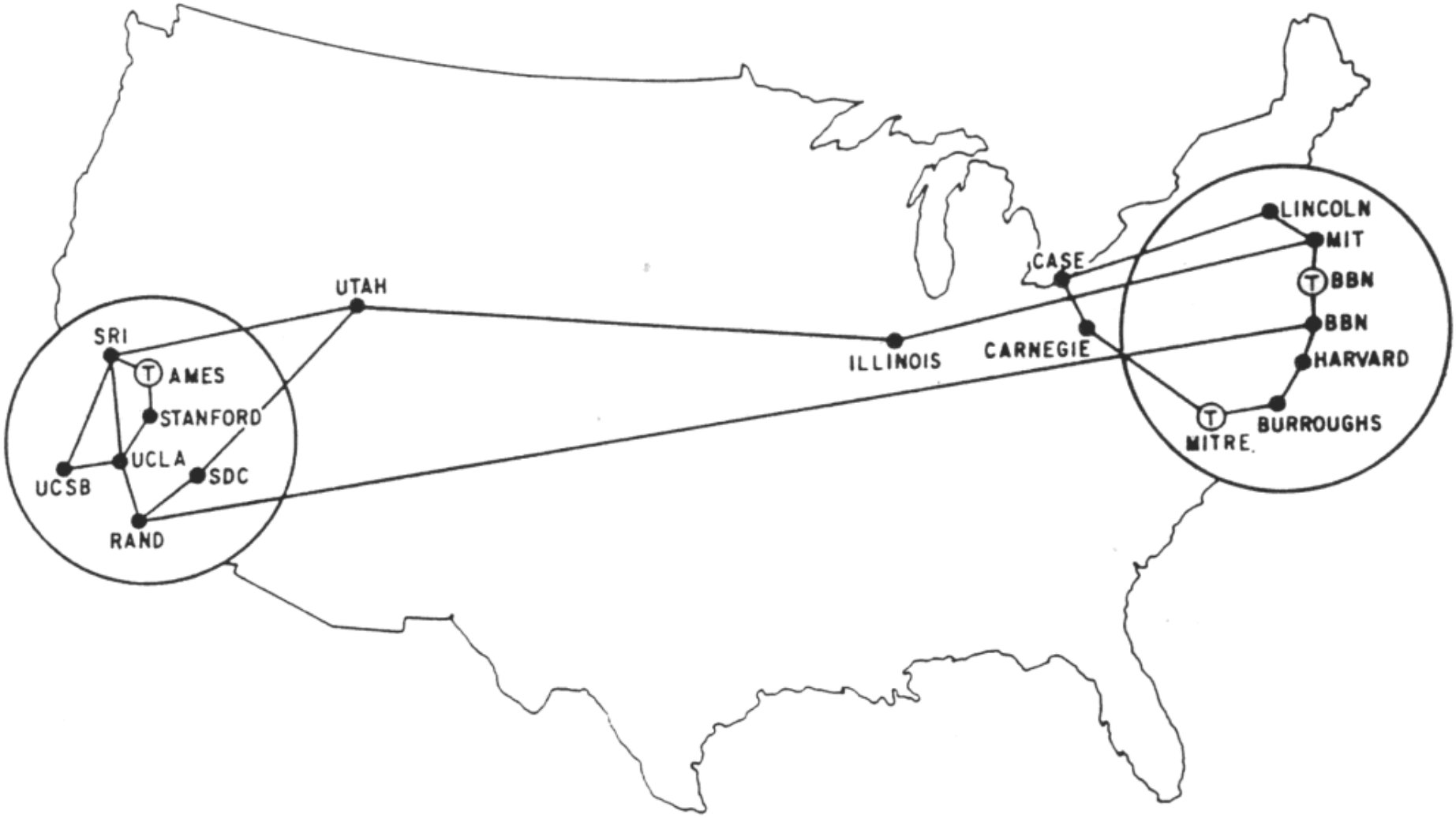
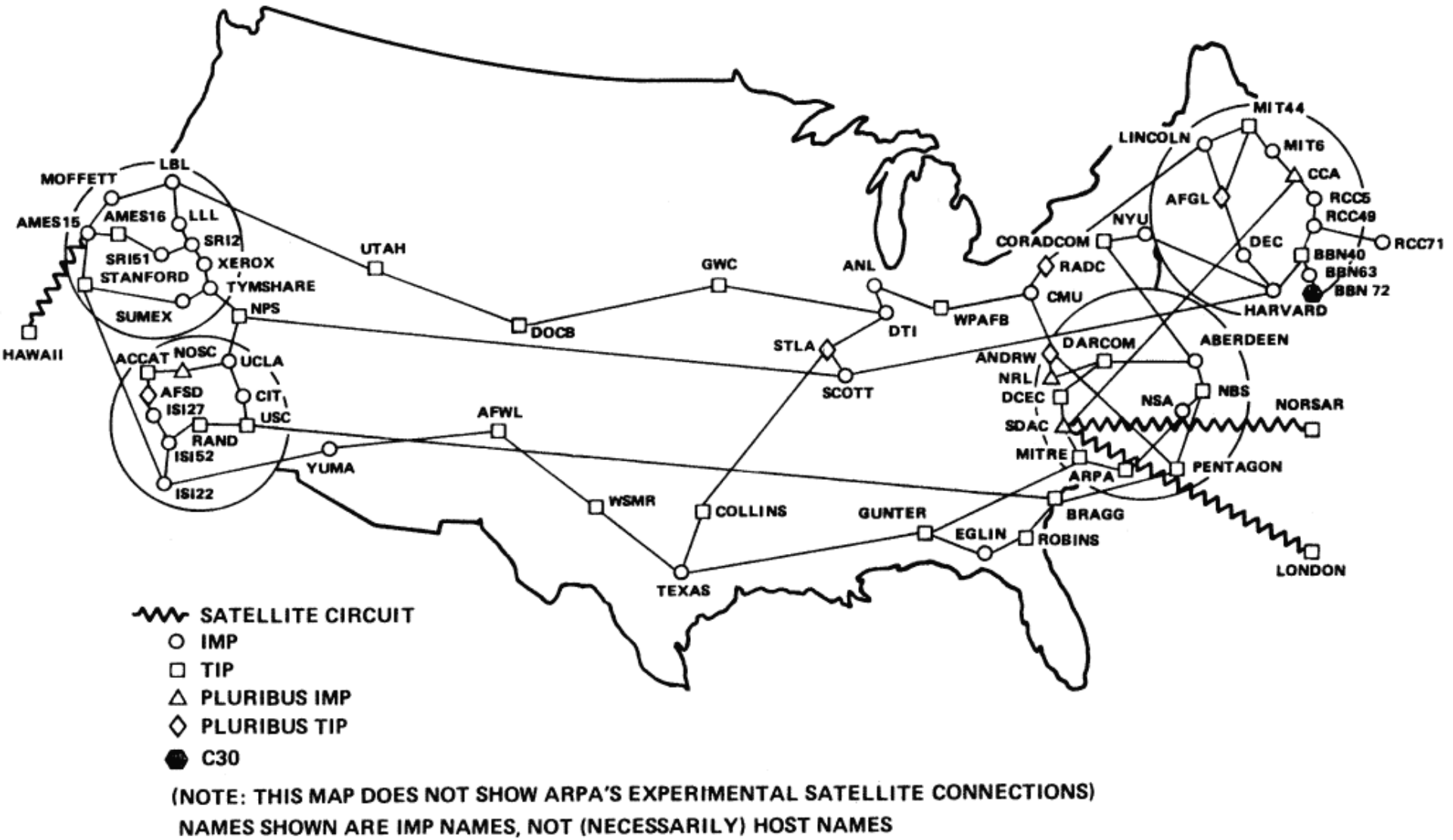


FIGURE 6.2 Drawing of 4 Node Network (Courtesy of Alex McKenzie)



MAP 4 September 1971

ARPANET GEOGRAPHIC MAP, OCTOBER 1980

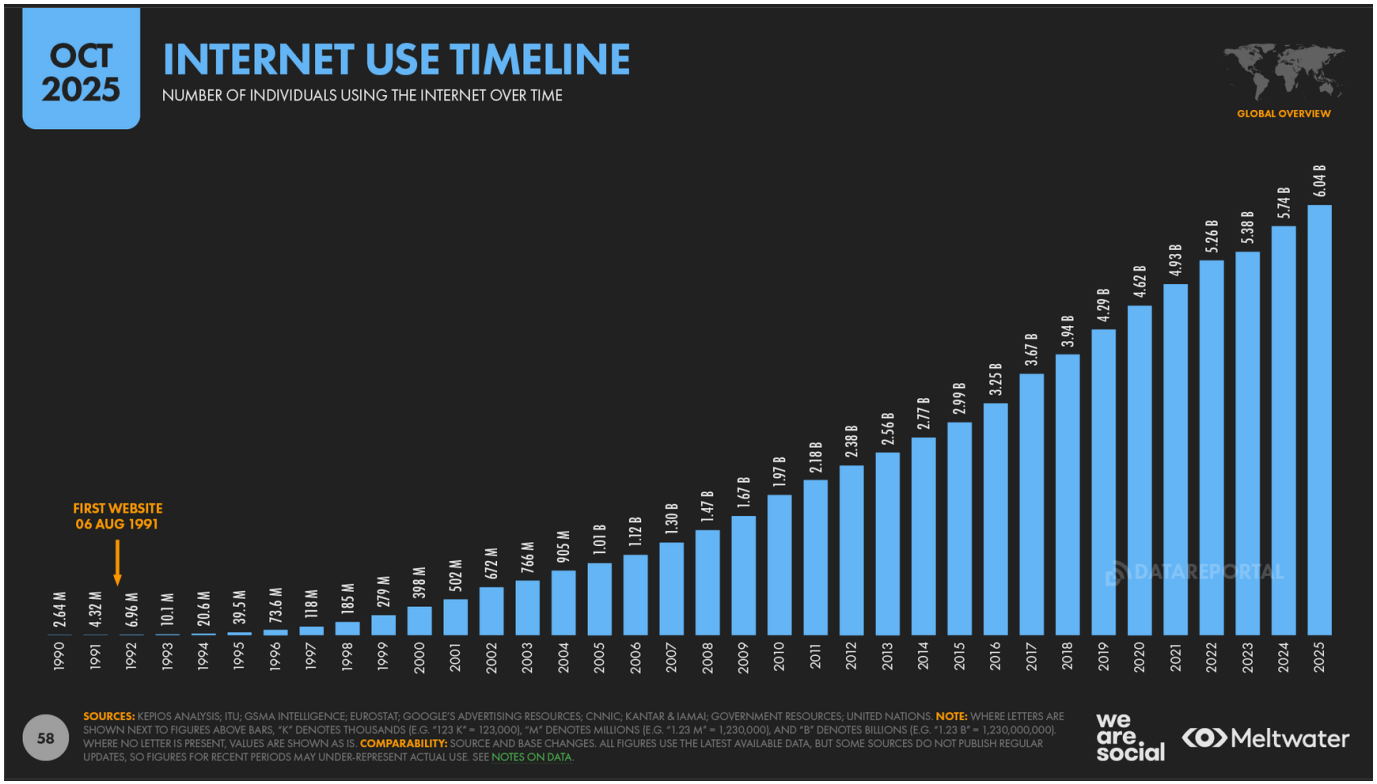


(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

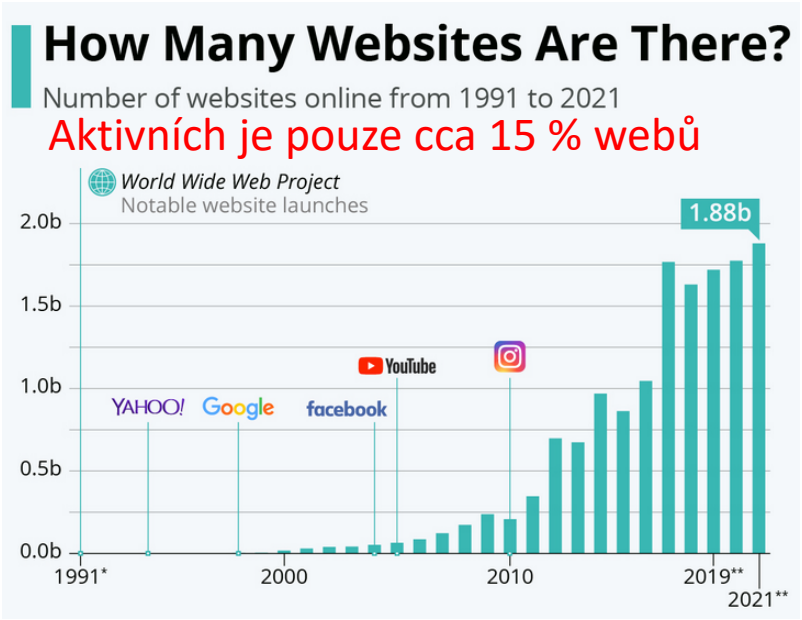
Internet

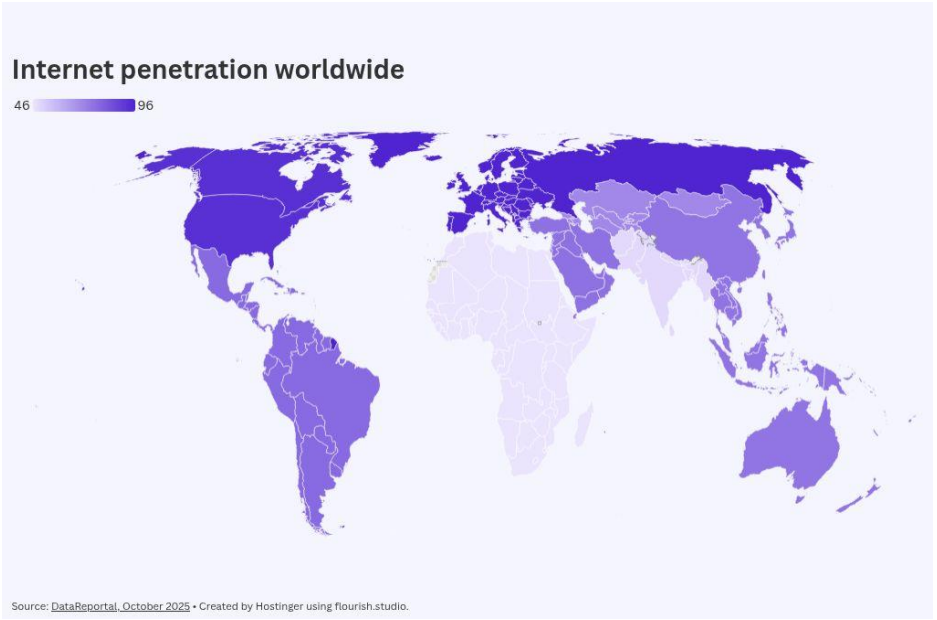
- Celosvětová veřejně přístupná počítačová síť
- Propojuje mezi sebou menší sítě
- Propojení probíhá pomocí standardního internetového protokolu IP
- Název vznikl zkomolením slova internetwork nebo internetworking
- Internet nemá žádného majitele

Něco čísel

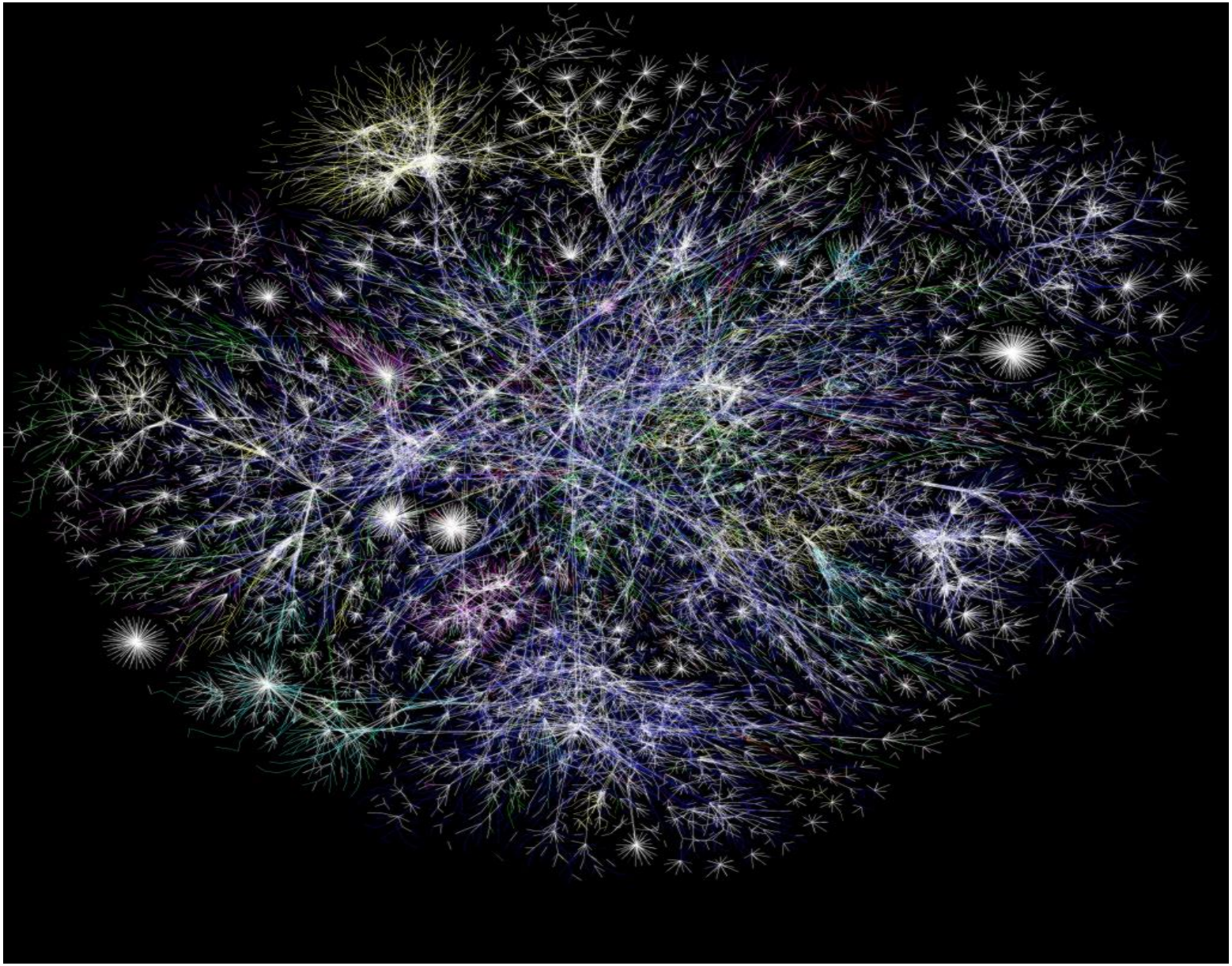


https://datareportal.com/reports/digital-2026-six-billion-internet-users

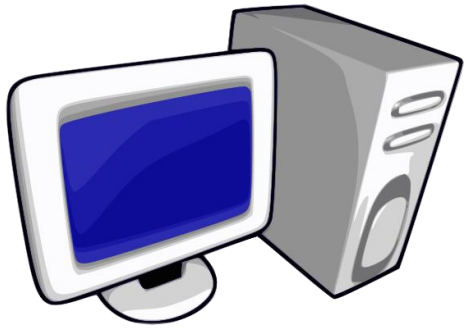




Jak vypadá Internet?



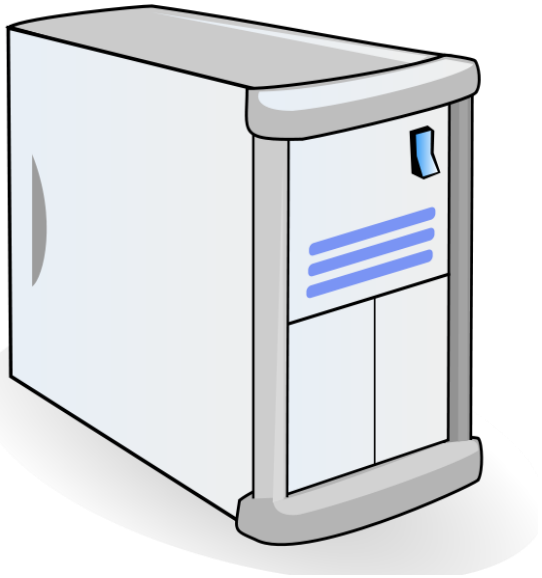
Klient - Server

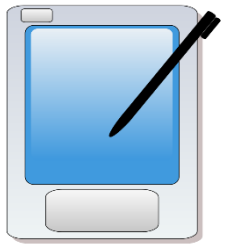


Dotaz

Odpověď

Server (apache)





Dotaz

Odpověď

Klient-Server

- Klient – vstupní bod do internetu – PC, notebook, mobil, ...
- Server – obsluhuje požadavky uživatele, zasílá požadované informace atd.
- Data a výpočetní výkon jsou distribuovány po síti.

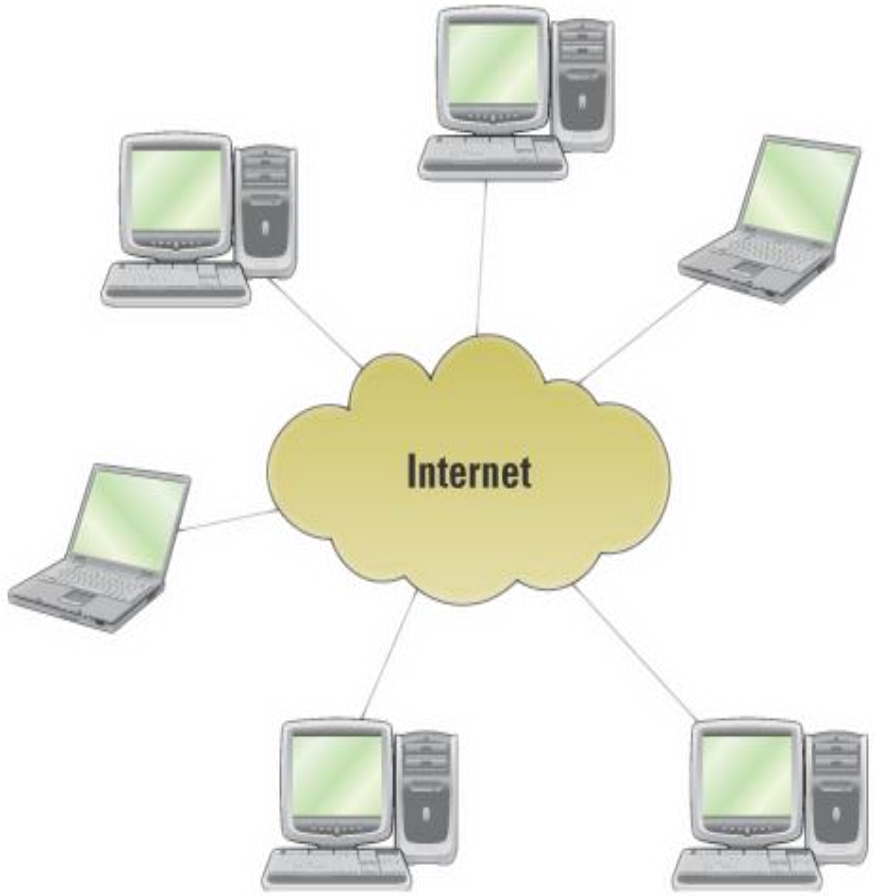
- Klient vyšle požadavek, server odpovídá.

Typy klienta

- Tlustý klient – obvykle rozsáhlá aplikace nebo softwarový balík, většina dat je umístěna lokálně. Většina výpočetního výkonu je soustředěna na straně klienta.
- Tenký klient – malá rychlá aplikace (např. browser). Většinu počítání nechává na serveru, zobrazuje pouze výsledky.

Peer-to-Peer sítě

- Spojení dvou počítačů tak, že oba fungují současně jako server i jako klient (Torrent)

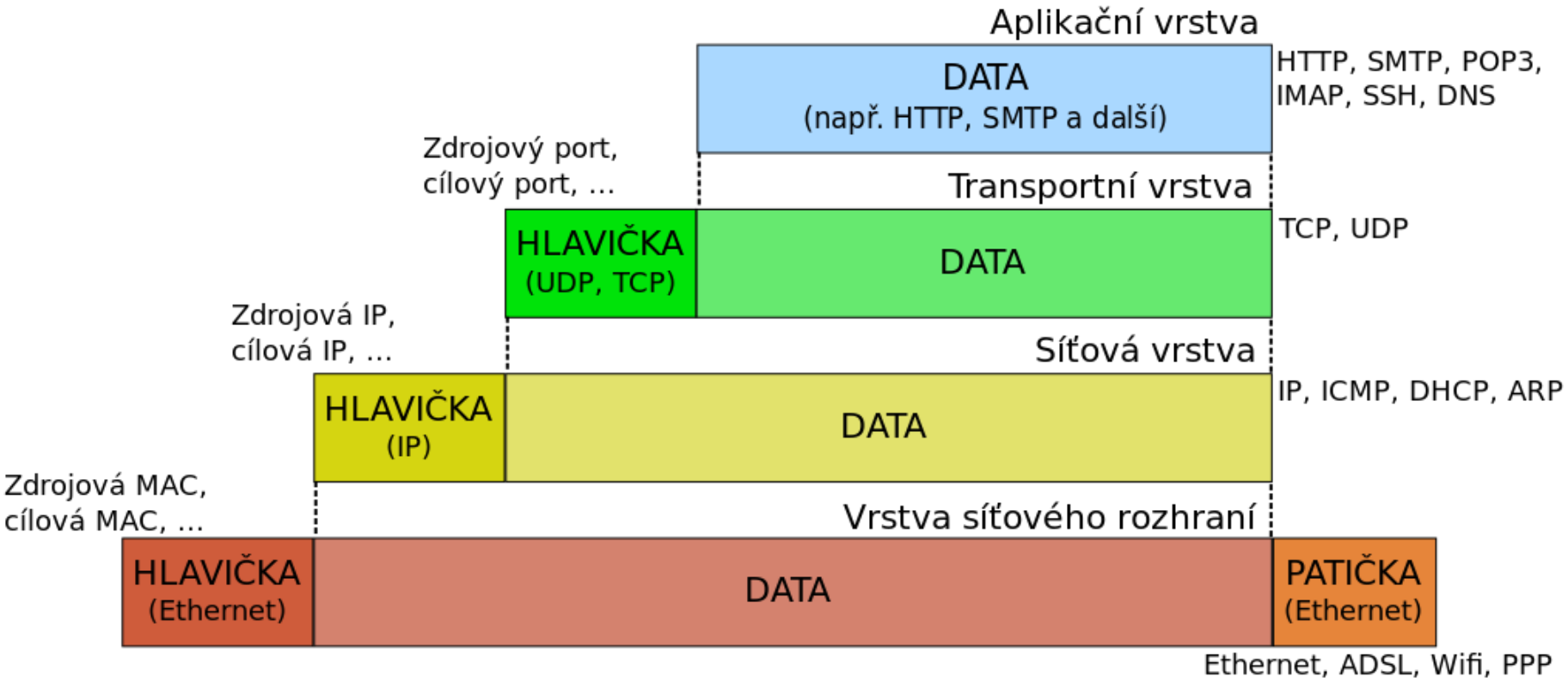


TCP/IP

- *Transmission Control Protocol/Internet Protocol* – „primární přenosový protokol/protokol síťové vrstvy“
- rodina protokolů pro komunikaci v počítačové síti (hlavní protokol internetu)
- komunikační protokol = množina pravidel, která určují syntaxi a význam jednotlivých zpráv při komunikaci
- Architektura:
  - Vrstva síťového rozhraní = nejnižší vrstva, umožňuje přístup k fyzickému přenosovému médiu (příklady sítí Ethernet, Token Ring, FDDI)
  - Síťová vrstva = zajišťuje především adresaci, směřování a předávání datagramů
  - Transportní vrstva = poskytuje transportní služby (kontrolovaný protokol TCP, nekontrolovaný UDP)
  - Aplikační vrstva = programy/procesy pro konkrétní služby (Telnet, FTP, HTTP, …)

TCP/IP

ZAPOUZDŘENÍ DAT V SÍTI TCP/IP



TCP/IP

Doporučená videa k vysvětlení problematiky

What is TCP/IP?
https://www.youtube.com/watch?v=PpsEaqJV_A0

TCP IP Model Explained | TCP IP Model Animation | TCP IP Protocol Suite | TCP IP Layers
https://www.youtube.com/watch?v=2QGgEk20RXM

IP adresa

- Jednoznačně identifikuje zařízení v počítačové síti
- IPv4:
  - doposud stále nejrozšířenější verze
  - adresou je 32bitové číslo zapisované po jednotlivých bytech (celkem 2^{32} = 4 294 967 296 možností)
  - např. 158.196.128.1
  - část adresy je vyhrazena pro identifikaci sítě, část pro identifikaci podsítě a část pro identifikaci počítače uvnitř sítě (toto rozdělení určuje maska sítě)
- IPv6:
  - nová verze řešící problémy s nedostatkem adres a bezpečností
  - adresou je 128bitové číslo zapisované jako osm skupin po čtyřech hexadecimálních číslicích
  - např. 2001:0718:1c01:0016:0214:22ff:fec9:0ca5
- Zařízení může při připojení do sítě dostávat stále stejnou IP adresu (statická IP), nebo různou (dynamická IP)

MAC adresa

- jedinečný identifikátor síťového zařízení (fyzická adresa)
- přidělen napevno zařízení samotným výrobcem
- u moderních karet je možné ji dodatečně změnit
- 48bitové číslo, zapisované dle standardu jako šestice dvojciferných hexadecimálních čísel (např. 01-23-45-67-89-ab)

- Zjištění informací o síťových připojeních zařízení
  - Windows: příkazový řádek, příkaz ipconfig –all
  - Linux: terminál, příkaz ipconfig -a

DNS

- Domain Name System (DNS)

www.wikipedia.org	< = >	145.97.39.155
www.vsb.cz	< = >	158.196.149.9
gislinb.vsb.cz	< = >	158.196.143.62

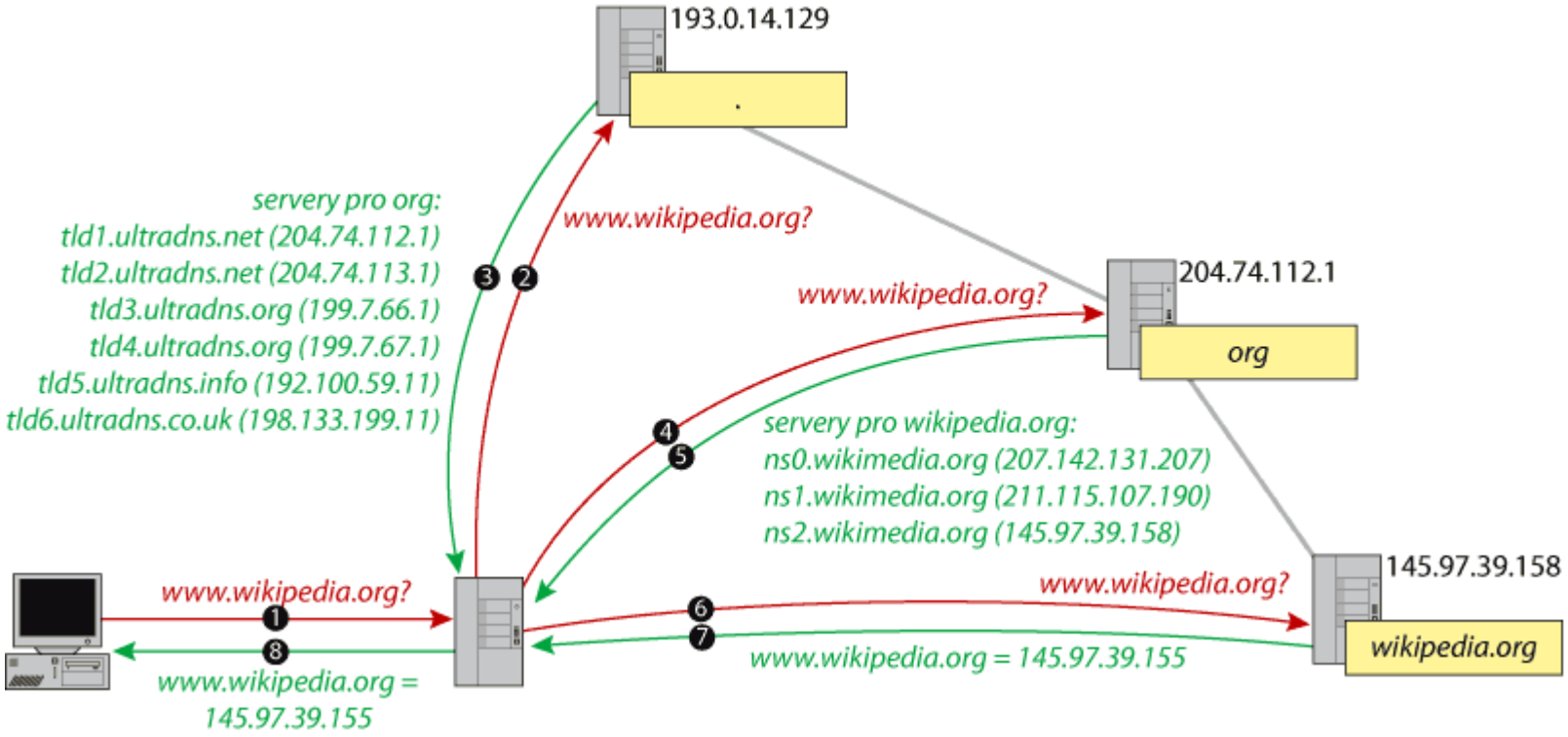
- Seznam kořenových serverů

  http://www.root-servers.org/

DNS

- Popis dotazu na adresu www.wikipedia.org

  http://cs.wikipedia.org/wiki/Soubor:Dns-wikipedia.gif



DHCP

- Dynamic Host Configuration Protocol
- Protokol z rodiny TCP/IP protokolů, který se používá pro automatické a dynamické konfigurování počítačů v počítačové síti.
- Přiděluje se
  - IP adresa,
  - maska sítě,
  - implicitní brána,
  - DNS server.
- Přidělení je omezeno na určitou dobu, na klientském počítači o prodloužení žádá DHCP client. Jinak jsou parametry přiděleny jinému stroji.

Aktivní síťová zařízení

- Repeater (opakovač) = přijímá zkreslený, zašuměný či jinak poškozený signál, opravuje jej a posílá dále, slouží pro zvýšení dosahu bez ztráty kvality
- Hub (rozbočovač) = umožňuje větvení, veškerá data, která přijme na některém z portů, rozkopíruje dále na všechny své porty = nijak neřídí signál
- Switch (přepínač) = obdoba hubu, data se vysílají jen do rozhraní, do kterých je připojen adresát. Propojuje počítače uvnitř jedné sítě.
- Router (směřovač) = přeposílá data k jejich cíli, propojuje dvě sítě

Možnosti připojení k internetu

- Telefonní linka – klasické vytáčené spojení (modem). Rychlost max. 56 Kb/s.
- ISDN – digitální telefonní linka, lze volat a zároveň pracovat na internetu. Rychlost 64-128 Kb/s.
- DSL (ADSL) – vysokorychlostní internet pomocí telefonní linky. Je potřeba modem, rychlost až 100 Mb/s.
- Kabelový internet – rychlé a kvalitní připojení, koaxiální kabel či optické vlákno (páteřní sítě), rychlost pro standardní koncové uživatele standardně desítky/první stovky Mb/s
- Mobilní telefon – pomocí sítí mobilních telefonních operátorů
- Wi-Fi – bezdrátové připojení

Mobilní internet - technologie

- Poprvé v roce 1991, různé technologie, frekvence, rychlý vývoj
- 2G (2nd Generation) - 1991
  - 2.5G – GPRS, rychlost download 56 – 115 kbit/s
  - 2.75G – EDGE, rychlost download až 237 kbit/s
- 3G (3rd Generation) - 2001
  - Různé technologie (UMTS, CDMA, EDGE-Evolution)
  - Rychlosti typicky několik Mbit/s
- 4G (4th Generation) - 2008
  - Různé technologie (HSPA+, WiMAX, LTE)
  - Rychlosti typicky desítky či stovky Mbit/s
- 5G (5th Generation) - 2020
  - cílem je max. teoretická rychlost 20 Gb/s

Wi-Fi technologie

- Wi-Fi = obchodní značka pro standardy IEEE 802.11
- využití frekvencí v pásmu:
  - 2.4 GHz – od počátku, větší dosah, nižší rychlost, menší počet kanálů, náchylnější na interference
  - 5 GHz – od standardu 802.11n z roku 2008, menší dosah, vyšší rychlost, vyšší počet kanálů
  - v nových standardech se objevuje taktéž využití 900 MHz a 6 GHz
- původně dosah cca 100 m, od standardu IEEE 802.11 ah nárůst na cca 1 000 m
- koncové zařízení se připojuje k Wi-Fi routeru (tzv. AP, Acces Point)

Wi-Fi technologie

- 1997 - první verze protokolu, 802.11-1997, max. 2 Mbit/s
- 1999 – 802.11a (max. 54 Mbit/s), 802.11b (max. 11 Mbit/s)
- 2003 – 802.11g (max. 54 Mbit/s)
- 2009 – 802.11n (max. 600 Mbit/s)
- 2013 – 802.11ac (teoreticky max. 6928 Mbit/s)
- 2019 – 802.11ax (teoreticky max. 600-9608 Mbit/s)
- 2025 - 802.11be (teoreticky max. 1376–46120 Mbit/s)

Služby poskytované na internetu

- Vyhledávání a publikování informací (HTTP, WWW stránky)
- Sdílení souborů (FTP, P2P)
- Rádiové a televizní vysílání
- Telefonování (Skype, VoIP)
- Elektronická pošta (SMTP, POP3, IMAP)
- Komunikace (Messenger)
- Vzdálené připojení (telnet, ssh)
- Cloudové služby

WWW

- World Wide Web

- Provázaná síť dokumentů na Internetu:
  - statické dokumenty (zobrazeny bez změny vždy stejně).
  - dynamické dokumenty (vytváří se podle určených parametrů a požadavků uživatele).

HTTP

- **HTTP - Hypertext Transfer Protocol** - protokol pro přenos stránek mezi webovým serverem a prohlížečem
- Průběh vyřízení požadavku
    1. navázání spojení
    2. zaslání požadavku klientem
    3. zaslání odpovědi serverem
    4. uzavření spojení
- Protokol funguje způsobem dotaz-odpověď. Uživatel (pomocí internetového prohlížeče) pošle serveru dotaz ve formě čistého textu, obsahujícího označení požadovaného dokumentu. Server následně odpoví pomocí několika řádků textu, popisujících výsledek dotazu (zda se dokument podařilo najít nebo ne apod.). Hned potom následuje tělo požadovaného dokumentu.

Ukázka komunikace

```
GET /wiki/Wikipedie HTTP/1.1
Host: cs.wikipedia.org
User-Agent: Mozilla/5.0 Gecko/20040803 Firefox/0.9.3
Accept-Charset: UTF-8,*
```

```
HTTP/1.0 200 OK
Date: Fri, 15 Oct 2004 08:20:25 GMT
Server: Apache/1.3.29 (Unix) PHP/4.3.8
X-Powered-By: PHP/4.3.8
Vary: Accept-Encoding,Cookie
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Language: cs
Content-Type: text/html; charset=utf-8
```

HTTP

- Protokol HTTP neumožňuje uchovávání stavu.
- Pokud má uživatel více dotazů na jeden server, jedná se vždy o další nezávislý dotaz a odpověď. Server nedokáže rozlišit, jestli druhý dotaz nějak souvisí s předchozím.
- Díky této vlastnosti se protokolu HTTP říká **bezstavový**.
- V praxi ale občas potřebujeme uchovávat informaci o stavu připojení uživatele (identitě uživatele apod.). K tomuto účelu byl protokol HTTP doplněn o tzv. HTTP **cookies**, které umožňují serveru uchovávat informace o stavu spojení na počítači uživatele.

HTTPS

- Zabezpečená verze protokolu HTTP
- Umožňuje přenášená data zašifrovat a tím je chránit před odposlechem či narušením
- Využívány protokoly SSL nebo TLS
- Pomocí asymetrické kryptografie je ověřena identita webového serveru, volitelně i klienta. Poté následuje dohoda na klíči pro symetrické šifrování samotné komunikace

URL

- Unified Resource Locator
  - Řetězec znaků identifikující abstraktní nebo fyzický zdroj.
  - Identifikuje zdroje na základě jejich síťové lokace.

Nejjednodušší forma:

schéma://host/cesta

http://gis.vsb.cz/kacmarik

Úplná forma:

schéma://uzivatel:heslo@host:port/cesta?parametry#odkaz

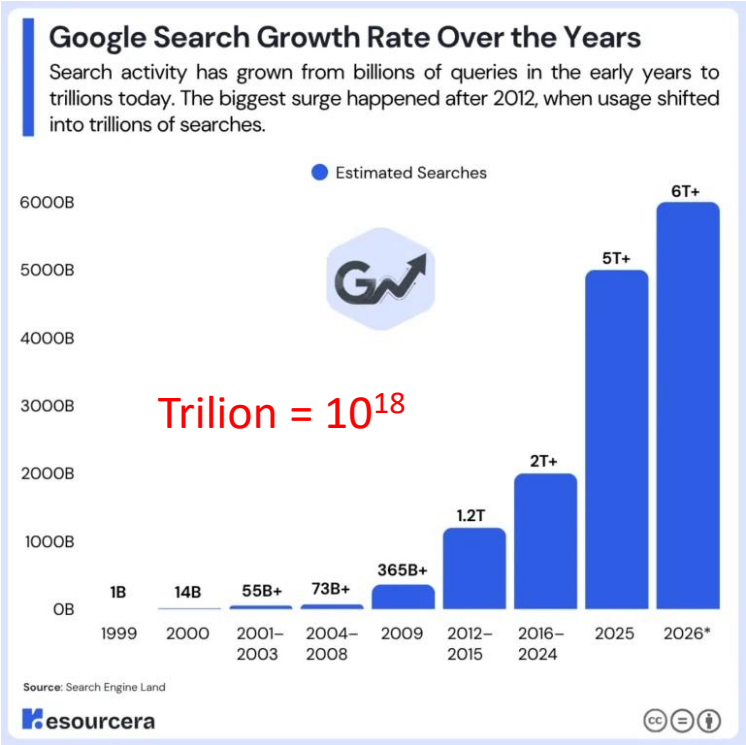
ftp://der011:heslo@gislinb.vsb.cz:21/public_html/index.html#odstavec1

Vyhledávání na webu

- Page Rank
- Hodnota přidělená každé stránce na základě „důležitosti“ a relevantnosti odkazů, které na ni ukazují.
- Popis lze najít zde:

Page, Lawrence and Brin, Sergey and Motwani, Rajeev and Winograd, Terry (1999) The PageRank Citation Ranking: Bringing Order to the Web. Technical Report. Stanford InfoLab.

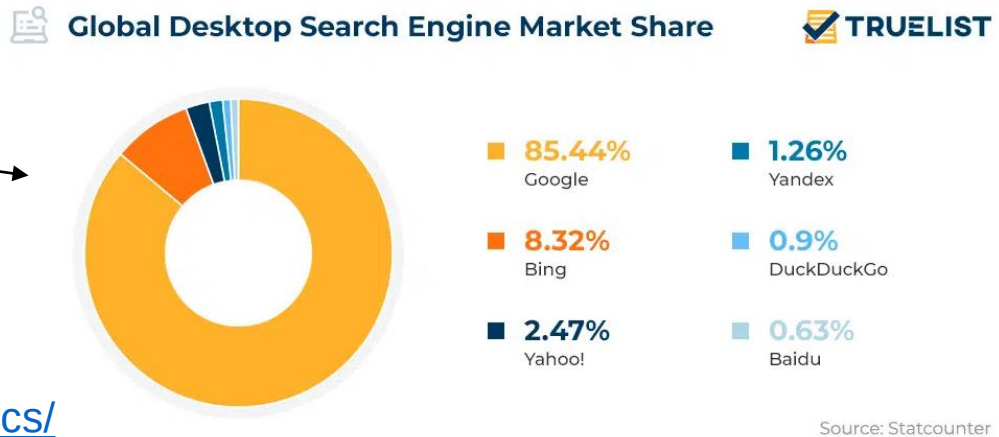
Vyhledávání



- 96.84% of the global mobile search traffic belongs to Google. (Statcounter)
- The number of searches grows by 10% every year. (InternetLiveStats)
- With 94.19%, India is the top Google-using country. (Statista)
- 77% of people use Google 3 times a day. (Moz)
- 20% of all Google searches are done by voice commands. (Google)
- Every business that will spend $1 on Google ads will earn roughly $8. (Google)
- Only 0.78% of people click something on Google's page 2. (Backlinko)
- Having a question in the meta title will raise the CTR for 14.1%. (Backlinko)
- When it went public, Google was worth about $23 billion. (CNN, CNBC)

https://earthweb.com/how-many-google-searches-per-day/

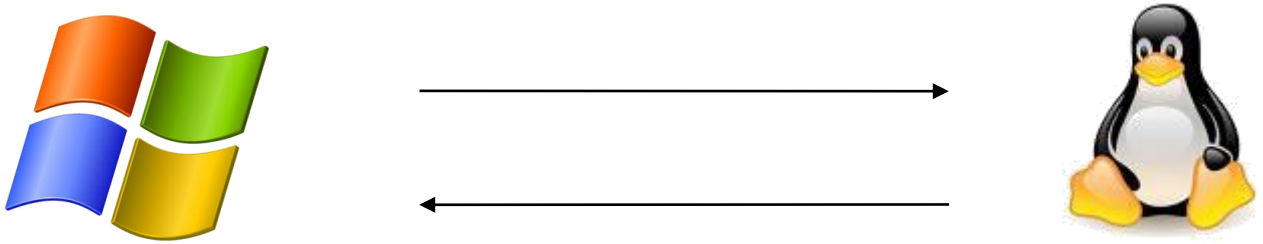
vyhledávače, 2024 →



https://truelist.co/blog/google-search-statistics/

FTP

- File Transfer Protocol
- Přenos souborů mezi zařízeními (s různými operačními systémy)
  - Port 21 – řídící, přenos příkazů FTP
  - Port 20 – přenos dat, binární a textový mód (úprava konce řádků dle OS)
- Všechna data včetně přihlašovacích údajů jsou přenášena v čitelné podobě, tedy nezabezpečeně
- Existují různé zabezpečené šifrované varianty (FTPS, FTP/SSL, apod.)
- Přenos souborů podporován i protokolem HTTPS



telnet, ssh

- Telecommunication Network
  - Slouží k ovládání vzdáleného zařízení pomocí terminálu s příkazovým řádkem.

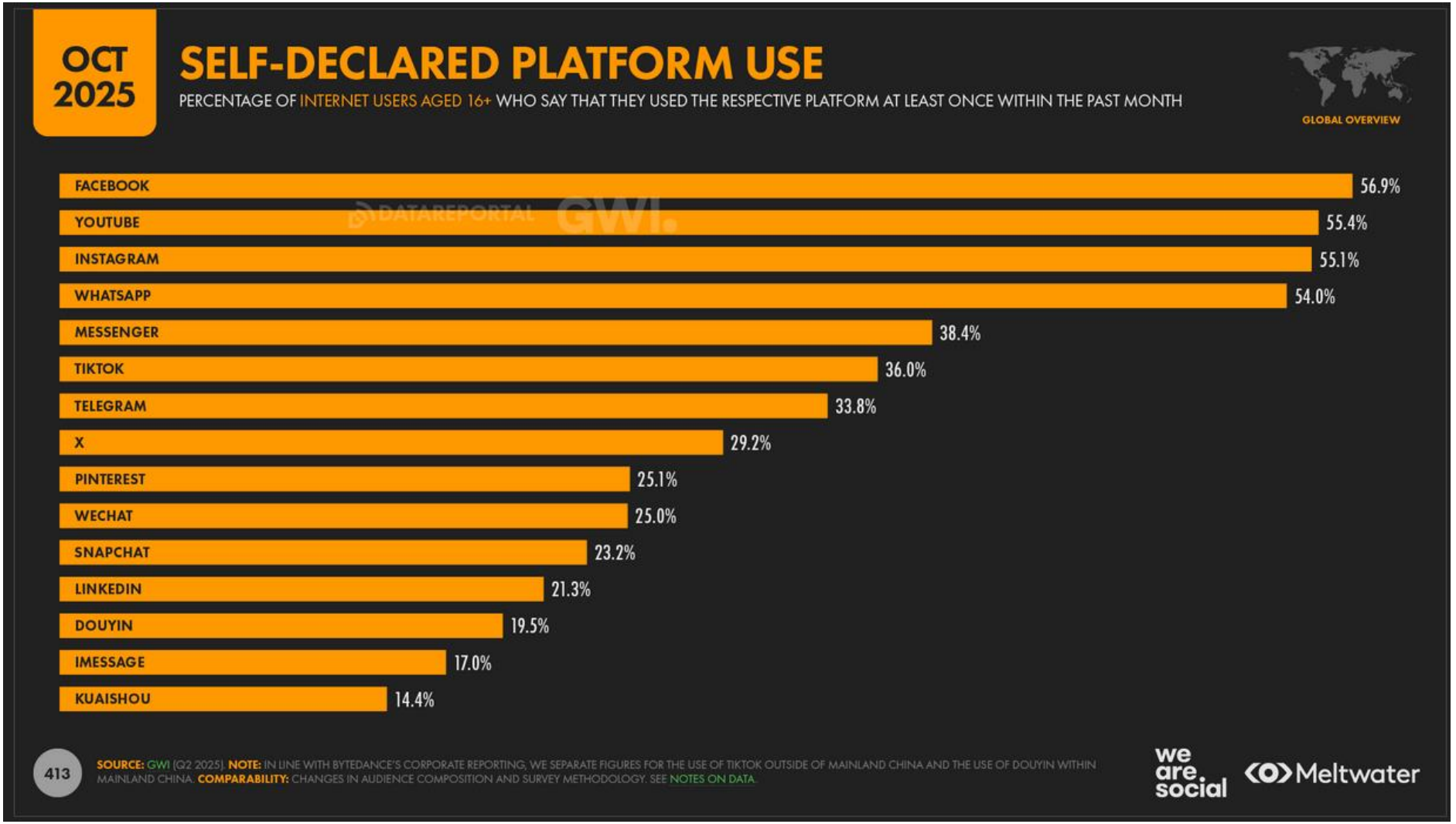
- Secure Shell
  - Označuje zabezpečený komunikační protokol v počítačových sítích, náhrada za telnet a jiné nezabezpečené vzdálené shelly.

e-mail

- POP3
  - klient se připojí na poštovní server pouze na tak dlouho, aby si stáhl novou poštu
  - dochází ke stahování zpráv ze serveru na stranu klienta, poté je připojení ukončeno

- IMAP - Internet Message Access Protocol
  - internetový protokol pro vzdálený přístup k e-mailové schránce prostřednictvím e-mailového klienta
  - používá se synchronizace zpráv vůči poštovnímu serveru (užitečné pro přístup k emailové schránce z většího množství zařízení)
  - proti jednodušší alternativě POP3 lze použít pokročilé možnosti vzdálené správy

Sociální sítě



https://datareportal.com/social-media-users

Cloudové služby

- technologie umožňující přistupovat k datům, aplikacím a výpočetnímu výkonu přes internet
- **IaaS** (Infrastructure as Service): poskytuje výpočetní zdroje – virtuální servery, úložiště jako náhradu za vlastní fyzické stroje uživatele. Např. Microsoft Azure, Amazon Web Services (AWS)
- **PaaS** (Platform as Service): nabízí vývojářské prostředí pro vývoj, správu a testování softwarových aplikací. Např. Google App Engine, Heroku
- **SaaS** (Software as Service): představuje hotový software přístupný on-line. Např. emailový klient, Office 365, Google Drive, ArcGIS Online, Google Earth Engine

Kybernetická bezpečnost

- obor chránící sítě, systémy a data před digitálními útoky
- V dnešní době, kdy vykonáváme řadu činností v on-line prostoru, je nevyhnutelné znát a řídit se alespoň základními pravidly
- Tři základní cíle bezpečnosti
  - Důvěrnost – data jsou přístupná pouze oprávněným osobám
  - Integrita – data nemohou být neoprávněně změněna
  - Dostupnost – data a služby jsou dostupné když jsou potřeba
- Příklad z geoinformatiky
  - ortofotomapa nesmí být pozměněna (integrita)
  - data katastru nesmí být veřejně modifikovatelná (důvěrnost)
  - mapový server musí být dostupný (dostupnost)

Autentizace × autorizace

Pojem	Význam
Identifikace	Kdo tvrdím, že jsem
Autentizace	Jak prokážu svou identitu
Autorizace	Co smím dělat

Příklad:

- přihlášení do univerzitního informačního systému Edison
- přihlášení do ArcGIS Online
- přístup do databáze PostgreSQL

Hesla

- Doporučení NÚKIB na délku hesla: alespoň 12 znaků pro uživatelské účty
- Nový trend = vytvářet **frázová hesla** (kombinace několika slov, pro nás snadno zapamatovatelných), např.
  JezevecZpíváNerad100Let

  trhat.fialky.B00M.dynamitem
- Neprolomitelná hesla neexistují, dvě cesty k prolomení:
  - Sociální inženýrství = útočníkovi nějakým způsobem heslo sami prozradíme
  - Útok hrubou silou = útočník zkouší zadávat naše heslo (náhodné generování znaků, slovníkové útoky, únik databází hesel)
- Možnost využívat správce hesel

Hashování hesel

- do databáze se samotná hesla neukládají
- hashování = jednosměrná kryptografická metoda převádějící uživatelské heslo na unikátní řetězec znaků (hash, český termín otisk), který slouží k bezpečnému uložení hesla v databázi
- pokud dojde k úniku dat, původní heslo nelze z otisku zpětně odvodit
- Pro maximální bezpečnost se navíc k samotnému heslu před výpočtem otisku přidává tzv. salt (sůl)

Vícefaktorové ověřování

- Kombinace dvou způsobů autentizace při přihlašování
- Nejčastěji dvoufaktorové ověřování (2FA) v podobě zadání hesla + dalšího způsobu, který je pro útočníka velmi náročné realizovat
- Rozdělení faktorů:
  - něco znám (heslo, PIN, bezpečnostní otázky)
  - něco vlastním (mobil, platební karta,)
  - něco jsem (biometrie = rozpoznání tváře, otisku prstu, …)

Šifrování

- Kódování = prostý zápis jiným způsobem (např. morseovkou, jiným jazykem, atd.)
- **Šifrování** = zápis parametrizovaný **klíčem**, tedy šifrování či dešifrování by nemělo být možné bez znalosti klíče
- **Symetrická šifra** = používá stejný klíč pro šifrování i dešifrování
  - Výhody = velice rychlé, menší velikosti šifrovaných souborů
  - Nevýhody = problematická výměna klíčů mezi oběma stranami, správa klíčů (každá dvojice komunikujících potřebuje jeden tajný klíč), omezená možnost ověřování uživatelů
  - Nejběžněji je používán šifrovací algoritmus AES (Advanced Encryption Standard)
  - Hlavní aplikace: ochrana úložiště, zabezpečení databáze, aplikace v reálném čase (platební systémy, VPN, streamovací služby)

Šifrování

- **Asymetrická šifra** = používá jeden (veřejný) klíč pro šifrování a druhý (soukromý) pro dešifrování, klíče jsou jedinečně propojeny, z jednoho nelze odvodit druhý
  - Na počátku se vygeneruje pár klíčů: soukromý klíč (máme jen my); veřejný klíč (můžeme někomu poslat či jej zveřejnit)
  - Pokud nám někdo chce poslat zprávu, data, atd., stačí, když je zašifruje veřejným klíčem. Bez našeho soukromého klíče nepůjde obsah dešifrovat
  - Výhody: není potřeba bezpečná výměna klíčů, zjednodušení správy klíčů pro více uživatelů, vyšší bezpečnost
  - Nevýhody: pomalejší šifrování, vyžaduje větší velikosti klíčů, nevhodné pro šifrování velkých objemů dat
  - Nejběžněji je používán šifrovací algoritmus RSA
  - Hlavní aplikace: digitální podpisy a ověřování, bezpečná výměna klíčů (hojně používáno pro výměnu klíčů pro symetrické šifrování = data pak stačí šifrovat symetricky, tento postup využívá např. https)

Elektronický versus digitální podpis

	Digitální podpis	Elektronický podpis
Definice	Typ elektronického podpisu, který využívá kryptografické technologie ke zvýšení bezpečnosti a zabránění manipulace s podepsaným dokumentem.	Širší pojem pro jakýkoliv elektronický proces, symbol nebo zvuk, který označuje souhlas nebo schválení obsahu daného dokumentu.
Úroveň zabezpečení	**Vysoká** (digitální certifikáty, **ověření identity** a asymetrické šifrování)	**Dostačující**
Složitost procesu	**Složitější**—vyžaduje kroky jako ověření identity a potenciálně osobní ověření s certifikačními autoritami.	**Jednodušší**—může zahrnovat napsání jména, ověření podpisu přes e-mail, kliknutí na tlačítko nebo nahrání naskenovaného podpisu.

https://autenti.com/cs/blog/digitalni-podpis-vs-elektronicky-podpis

Nejčastější útoky

- Malware
- Spyware
- Adware
- Trójský kůň
- Phishing
- Pharming
- Hoax
- Spam
- ...

Malware

- Souhrnný název pro škodlivý software
- Co může dělat:
  - Poškodit data (zašifrovat, smazat)
  - Sledovat aktivitu uživatele
  - Zobrazovat nevyžádané reklamy
  - Vniknutí do systému a převzetí kontroly nad zařízením
- Šíření malware:
  - Otevření souboru staženého z internetu, z přílohy emailu, zkopírovaného z flash disku, apod. (virus)
  - Instalace zároveň s nějakým jiným softwarem (trojský kůň)
  - Skrze díru v neaktualizovaném operačním systému/software (červ)
- Červ je typ malware, který nepotřebuje hostitelský soubor (soubor obsahuje jen červa).

Malware

- Ochrana proti malware:
  - Mít aktualizovaný operační systém i používané programy
  - Používat antivirový program (AVG, Norton, Avast, Sophos, atd.), mít jej aktualizovaný, se zapnutou ochranou v reálném čase
  - Nevypínat firewall
  - Vlastní obezřetnost uživatele a používání zdravého rozumu

Spyware

- Software, který bez vědomí uživatele odesílá z počítače důvěrné a osobní informace o uživateli (seznam navštívených stránek, nainstalované programy, atd.)
- Původní účel byl zjistit potřeby a zájmy uživatele a využít tyto informace pro cílenou reklamu
- Spyware se šíří společně s řadou sharewarových programů
- Může vést i k instalaci dalšího softwaru do počítače uživatele bez jeho vědomí (viry, trójské koně, vykradače hesel atd.)

Adware

- Produkt, který obvykle znepříjemňuje práci s PC reklamou.
- Typickým příznakem jsou různá vyskakovací reklamní okna během surfování, nebo vnucování stránek (automatická změna domovské stránky apod.)
- Adware bývá součástí některých zdarma dostupných produktů (např. DivX), které jsou v placené verzi bez reklamy.

Trójský kůň

- Škodlivý program, který se šíří pomocí emailů nebo stažení z Internetu.
- Nejedná se o virus, protože se nedokáže sám šířit.
- Sám o sobě není škodlivý, ale otevírá porty (zadní vrátka) k počítači, které jsou pak terčem útoku hackera.
- Počítač se tedy stává velmi snadno napadnutelný.

Phishing

- Jedná se o podvodnou techniku používanou na internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku.
- Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiných podobných institucí a vyzývají adresáta k zadání určitých údajů na odkazovanou stránku.
- Tato stránka může například napodobovat přihlašovací okno internetového bankovnictví a uživatel do něj zadá své přihlašovací jméno a heslo.
- Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.

Pharming

- Nebezpečnější technika než Phishing
- Jedná se o hackerský útok, jehož cílem je přesměrování síťového provozu na hackerem podstrčený server.
- Využívá se technika DNS cache poisoning (donucení DNS serveru k chybnému překladu názvu na IP adresu).

Hoax

- Poplašná zpráva, která obvykle varuje před neexistujícím nebezpečným virem nebo jinými nepříjemnými skutečnostmi.
- Šíří se přeposíláním dalším uživatelům.
- Odvolává se na důvěryhodné zdroje.
- Vždy vyžaduje rozeslání dále.

- Zjistěte na serverech zabývající se touto problematikou, zda je zpráva registrována jako hoax.

http://hoax.cz/

Spam

- Nevyžádaná pošta s reklamním obsahem.
- Neškodí, pouze obtěžuje uživatele.

Zdroje

http://www.let.leidenuniv.nl/history/ivh/frame_theorie.html

http://searchenginewatch.com/3634991

http://www.spyware.cz/

http://hoax.cz/

https://autenti.com/cs/blog/digitalni-podpis-vs-elektronicky-podpis

https://www.itnetwork.cz/bezpecnost/zakladni-pojmy-a-zasady-kyberneticke-bezpecnosti

https://www.serverion.com/cs/uncategorized/when-to-use-symmetric-or-asymmetric-encryption/

Školení IT bezpečnosti, VŠB-TUO