Dobré odpoledne

- Prezentující
- *Jiří Vejrosta* a
- *Ladislav Kavřík*

Internet – základní informační medium

- fungování
- historie
- bezpečnost
- kriminalita
- e-mail
- spam

Fungování internetu

- síť sítí
- decentralizovaná
- každý host je nezávislý
- vybere si co použije a co poskytne okolí
- přístup na internet přes ISP (Internet Service Providers)
- Internet je síť využívající protokoly TPC/IP a přepojování paketů

Komunikace na sítích

- problém nekompatibility sítí na počátku času (počítačů)
- klíčové slovo ***gateway***
- počítač tvořící rozhraní mezi oběma sítěmi. Toto rozhraní převádělo datový tok z řízení protokolů výchozí sítě na datový tok řízený protokoly cílové sítě.
- klasickým případem byl gateway pro předávání elektronické pošty. Elektronický dopis se adresoval na vhodné síťové rozhraní, které vyhodnotilo část specifikující adresu v druhé síti, provedlo potřebné transformace a dopis odeslalo na určenou adresu

TCP/IP protokol

TCP - umožňuje vytvořit mezi dvěma hostitelskými systémy oboustranné propojení garantující bezchybný přenos posloupnosti paketů v tomtéž pořadí

IP - specifikuje formáty paketů, zahrnuje internetové adresní schéma (IP adresy), dříve adresní prostor 32 bitů (4 mld. počítačů), dnes nová experimentální verze s 128 bity (opravdu hodně).

Domény

- od zavedení protokolu TCP/IP na síti ARPANETu (předchůdce internetu) byl zaveden systém domén pro lepší orientaci na netu
- 6 domén nejvyšší úrovně

  EDU (education),

  GOV (government),

  MIL (military),

  COM (commercial),

  ORG (organization),

  NET (network resources)

  doplněny o národní domény (např. cz)

Co internet poskytuje za služby

- www - world wide web
- e-mail - electronic mail
- ftp - File Transfer Protocol
- Telnet
- Gopher
- USENET

www - world wide web

- systém internetových serverů, který podporuje speciálně formátované dokumenty v jazyce nazvaném HTML (Hyper Text Markup Language)
- www využívá protokolu *HyperText Transfer Protocol* (http)

e-mail - electronic mail

- Lze definovat jako transmisi zpráv přes komunikační sítě
- E-mail je rychlý, flexibilní, spolehlivý ale mnohdy problematický v obchodním styku a z bezpečnostního hlediska (viz. dále)

ftp - File Transfer Protocol

- Je to protokol, využívaný pro výměnu souborů. FTP pracuje na stejném principu jako HTTP pro transfer *webových stránek* od serveru k uživatelově browseru
- FTP je běžně používán k stahování souborů ze serveru nebo k nahrávání souborů na server (popř. nahrání webové stránky na server).

Shrnutí historie v datech

1948 – matematická teorie komunikace

1958 – první křemíkový čip

1962 – představena počítačová síť

1964 – vynalezeno přepojování paketů

1965 – vynalezen Hypertext

1969 – vznik ARPANETu

1972 – vytvořen protokol TCP/IP

1984 – vznik názvu Internet, Internet začíná pracovat na TCP/IP

1989 – vytvořen world wide web

1993 – vznik prvního prohlížeče – Mosaic (předchůdce Netscape Communicatoru)

1995 – začíná věk eCommerce

Růstové trendy internetu

- 1971 - 111 IP počítačů
- 1987 - 10 000 IP počítačů
- 1992 - 1 000 000 IP počítačů
- 2002 - přes 200 000 000 IP počítačů

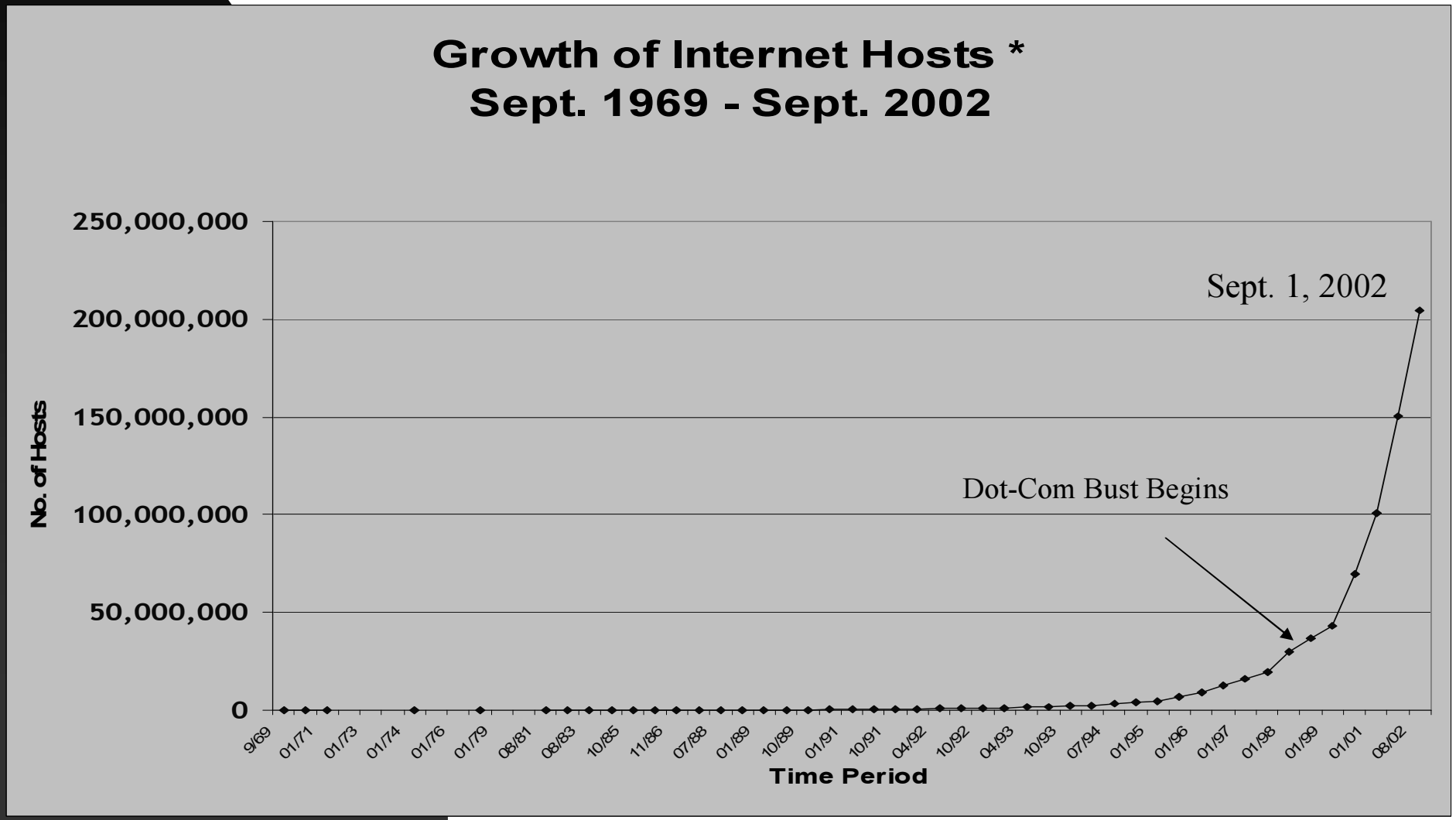
- **Přibližně v září 2002 Internet dosáhl dvou důležitých milníků:**

  200 mil. IP počítačů

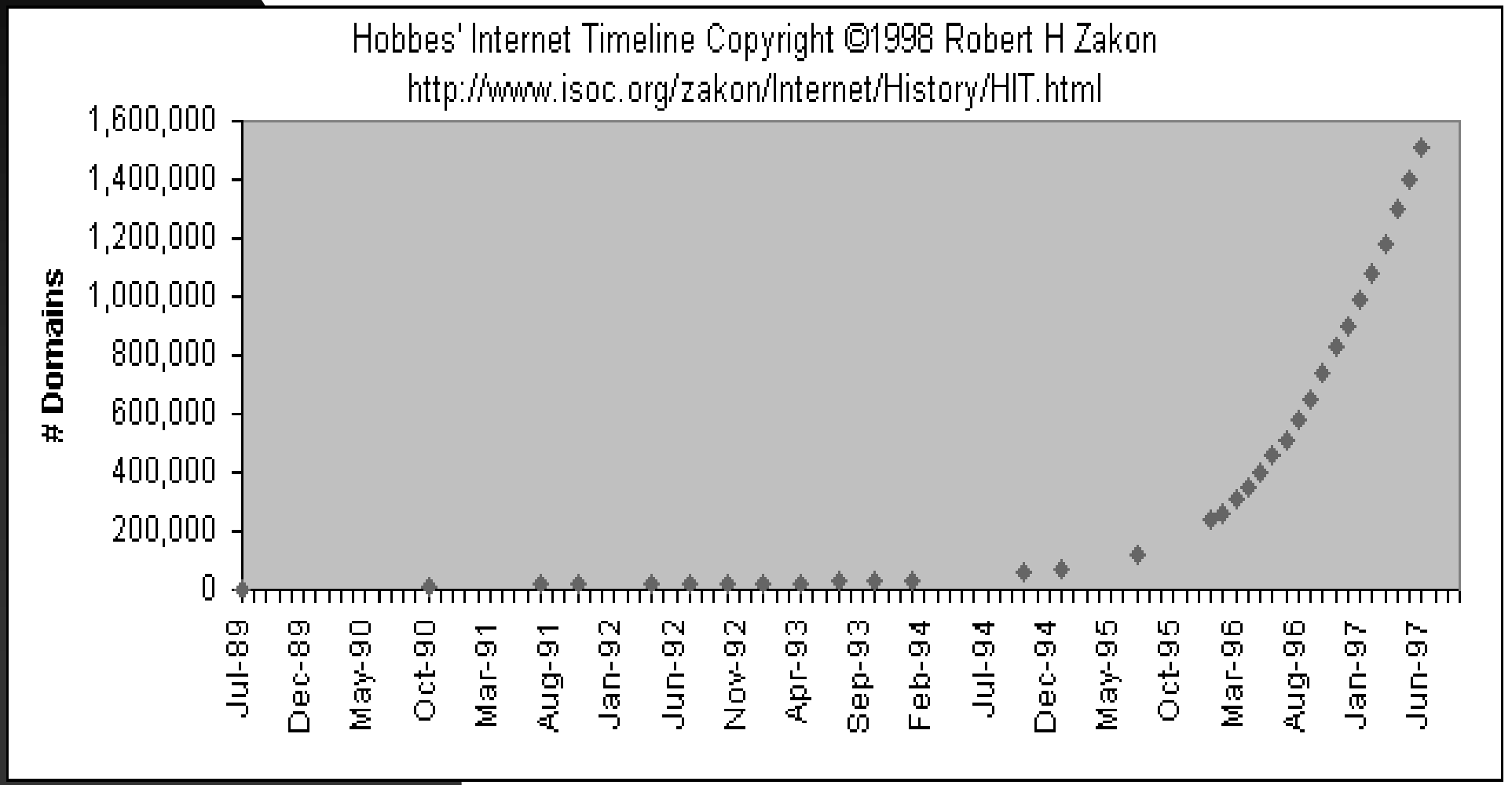
  840 mil. uživatelů

  Je zřejmé, že jen zlomek IP adres má své doménové jméno

Růst počtu počítačů na internetu



Registrace domén – leden 1989 – červenec 1997



Bezpečnost internetu

- cílem je, aby se veškerá data, dostala do rukou pouze těm, kterým jsou určena, a že všechny provedené transakce jsou směrovány vůči těm, kterým to zamýšlíme.
- Internet si můžeme představit jako řetěz, jehož síla je determinována silou jeho nejslabšího článku, takto musíme chápat schopnost Internetu bránit se náhodným i záměrným chybám.
- Největší ohrožení spolehlivosti a bezpečnosti Internetu spočívá v jeho dostupnosti a rozšíření a dále v prakticky nulové ceně přenosu informací po již vytvořené infrastruktuře

Vývoj bezpečnosti

- vojenská komunikační síť schopná přežít atomový útok => žádná centralizace a bezpečnost komunikace
- přenosové mechanismy se samy nesnaží jakkoli šifrovat, kódovat či jinak zabezpečovat přenášená data
- v roce 1990 má komerční sféra větší nároky na bezpečnost komunikace (jde o peníze)
- problém je jak zabezpečit - stanovit standard

Možnosti zabezpečení

- zabezpečit data již na úrovni aplikace, a k přenosu je předat v již zabezpečeném tvaru. Vlastní přenosové mechanismy Internetu pak mohou zůstat takové jaké jsou
- zabudovat příslušné zabezpečovací mechanismy přímo do přenosových sítí
- zabudování bezpečnostních mechanismů do přenosové infrastruktury
- uživatelé si zvolí co svěří internetu a co doručí jinak

Zabezpečení www stránek

- SSL (Secure Socket Layer) - vytváří zabezpečení pro více aplikací jednou společnou vrstvou
- S/HTTP (Secure HTTP) - rozšíření stávajícího protokolu HTTP o zabezpečovací mechanismy
- SET (Secure Electronic Transactions) - zaměřen na potřeby placení po Internetu

Bezpečnostní rizika

- útoky na hesla uživatelů
- útoky založené na předstírání IP adresy
- náhodné prohlížení přenášených paketů
- přivlastnění IP adresy
- předstírání administrátorů systému
- útok vedený pomocí neautorizovaného softwaru
- viry

Zásady ochrany počítače

- používat kvalitní a hlavně pravidelně aktualizovaný antivirový program
- **Firewall**
- Pravidelné aktualizace operačního systému

Firewall

- je systém vytvořený k prevenci před neautorizovaným vstupem do nebo ze soukromé sítě
- hardwarové a softwarové nebo kombinace obou
- Všechny zprávy procházejí firewallem, který zkoumá každou zprávu a blokuje ty, které nevyhovují specifikovaným bezpečnostním kritériím.

Počítačová (informační) kriminalita

- Definice pojmu není jednoduché
- Váže se na nejrůznější oblasti trestního práva
- Oproti hmotným produktům lze informační technologii a informace získat mnohem snadněji
- Počítačová kriminalita je mnohdy jen jinou formou různých forem standardních trestných činů.

Členění dle Rady Evropy

- Počítačové podvody,
- Počítačové falzifikace,
- Poškozování poč. dat a programů,
- Počítačová sabotáž,
- Neoprávněný přístup, průnik,
- Neoprávněné kopírování autorsky chráněného programu,
- Neoprávněné kopírování fotografie,
- Změna v datech či počítačových programech,
- Počítačová špionáž,
- Neoprávněné užívání počítače,
- Neoprávněné užívání autorsky chráněného programu,

Spam

- Spam je označení pro nevyžádaný obtěžující mail
- definice je značně subjektivní
- typy:

reklamní zprávy - texty, které mají odesílateli přinést finanční nebo jiný prospěch

Hoax - jsou řetězové dopisy obsahující zpravidla nepravdivou informaci, jež příjemce určitým způsobem nutí

řetězové dopisy - neškodné, ale mohou obtěžovat adresáta

Informační zdroje

- www.w3c.org
- http://www.webopedia.com
- http://www.isoc.org
- http://www.lupa.cz/clanek.php3?show=2467
- Bezpečnost na Internetu (Matyska L., ÚVT, a FI MU)
- http://www.earchiv.cz/a97/a711p200.php3

A to je vše, díky za pozornost

Hodně štěstí na písemce.