Internet a bezpečnosť

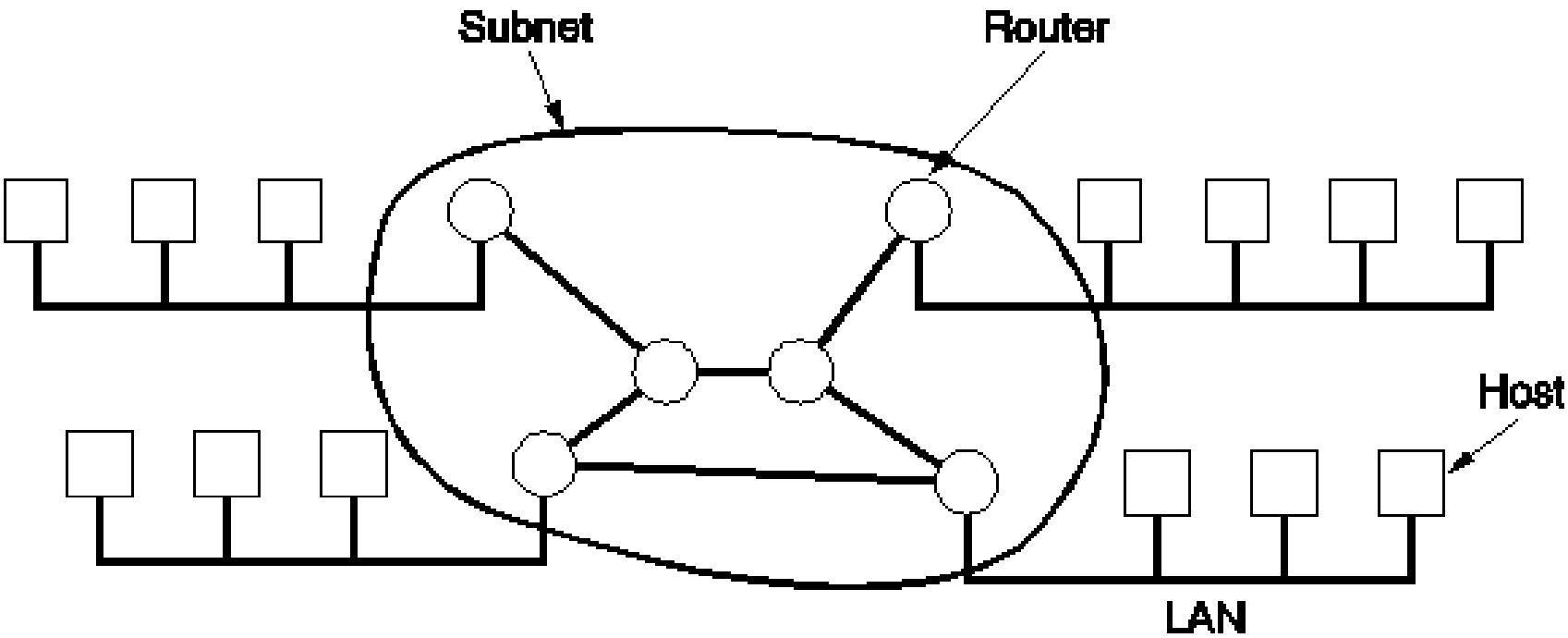
RNDr. Jaroslav Janáček, PhD.

Katedra informatiky FMFI UK

Akadémia Trojstenu, 6.12.2013

Ako funguje Internet?

- počítače alebo lokálne siete prepojené pomocou komunikačných liniek a smerovačov (routerov)



Ako funguje Internet?

- každý počítač má adresu (4B dlhé číslo)

Ako funguje Internet?

- každý počítač má adresu (4B dlhé číslo)
- prenášané údaje sa rozdelia na pakety

Ako funguje Internet?

- každý počítač má adresu (4B dlhé číslo)
- prenášané údaje sa rozdelia na pakety
- smerovač určí podľa cieľovej adresy, ktorému smerovaču paket pošle

Ako funguje Internet?

- každý počítač má adresu (4B dlhé číslo)
- prenášané údaje sa rozdelia na pakety
- smerovač určí podľa cieľovej adresy, ktorému smerovaču paket pošle
- posledný smerovač na ceste paket pošle cieľovému počítaču

Na čo používame Internet?

- zábava (filmy, mp3, chat, hry, ...)

Na čo používame Internet?

- zábava (filmy, mp3, chat, hry, ...)
- hľadanie informácií, vzdelávanie

Na čo používame Internet?

- zábava (filmy, mp3, chat, hry, ...)
- hľadanie informácií, vzdelávanie
- sťahovanie softvéru

Na čo používame Internet?

- zábava (filmy, mp3, chat, hry, ...)
- hľadanie informácií, vzdelávanie
- sťahovanie softvéru
- komunikácia (e-mail, web, ...)

Na čo používame Internet?

- zábava (filmy, mp3, chat, hry, ...)
- hľadanie informácií, vzdelávanie
- sťahovanie softvéru
- komunikácia (e-mail, web, ...)
- Internet banking (elektronický prístup do banky)

Na čo používame Internet?

- zábava (filmy, mp3, chat, hry, ...)
- hľadanie informácií, vzdelávanie
- sťahovanie softvéru
- komunikácia (e-mail, web, ...)
- Internet banking (elektronický prístup do banky)
- elektronické nakupovanie a predávanie

Na čo používame Internet?

- zábava (filmy, mp3, chat, hry, ...)
- hľadanie informácií, vzdelávanie
- sťahovanie softvéru
- komunikácia (e-mail, web, ...)
- Internet banking (elektronický prístup do banky)
- elektronické nakupovanie a predávanie
- prístup k službám úradov
- ...

Základné aspekty bezpečnosti

- dôvernosť
  - k informácii sa má dostať len oprávnený príjemca

Základné aspekty bezpečnosti

- dôvernosť
  - k informácii sa má dostať len oprávnený príjemca
- integrita
  - informácia sa nesmie neoprávnene a nepozorovane zmeniť

Základné aspekty bezpečnosti

- dôvernosť
  - k informácii sa má dostať len oprávnený príjemca
- integrita
  - informácia sa nesmie neoprávnene a nepozorovane zmeniť
- autentickosť
  - musí byť možné spoľahlivo určiť pôvodcu informácie

Základné aspekty bezpečnosti

- dôvernosť
  - k informácii sa má dostať len oprávnený príjemca
- integrita
  - informácia sa nesmie neoprávnene a nepozorovane zmeniť
- autentickosť
  - musí byť možné spoľahlivo určiť pôvodcu informácie
- dostupnosť
  - informácia musí byť dostupná vtedy, keď treba

Čo sa cez Internet prenáša?

Čo sa cez Internet prenáša?

- obsah voľne prístupných WWW stránok

Čo sa cez Internet prenáša?

- obsah voľne prístupných WWW stránok
- vyplnené políčka vo formulároch

Čo sa cez Internet prenáša?

- obsah voľne prístupných WWW stránok
- vyplnené políčka vo formulároch
- citlivé informácie z informačných systémov (napr. Internet banking)

Čo sa cez Internet prenáša?

- obsah voľne prístupných WWW stránok
- vyplnené políčka vo formulároch
- citlivé informácie z informačných systémov (napr. Internet banking)
- prihlasovacie mená a heslá

Čo sa cez Internet prenáša?

- obsah voľne prístupných WWW stránok
- vyplnené políčka vo formulároch
- citlivé informácie z informačných systémov (napr. Internet banking)
- prihlasovacie mená a heslá
- e-mailové správy

Čo sa cez Internet prenáša?

- obsah voľne prístupných WWW stránok
- vyplnené políčka vo formulároch
- citlivé informácie z informačných systémov (napr. Internet banking)
- prihlasovacie mená a heslá
- e-mailové správy
- dáta medzi informačnými systémami
- ...

Čo potrebujeme chrániť?

Čo potrebujeme chrániť?

- dôvernosť informácií, ktoré nemajú byť dostupné komukoľvek – napr.:
  - heslá
  - dôverné informácie z informačných systémov
  - dôverné informácie v e-mailoch

Čo potrebujeme chrániť?

- dôvernosť informácií, ktoré nemajú byť dostupné komukoľvek – napr.:
  - heslá
  - dôverné informácie z informačných systémov
  - dôverné informácie v e-mailoch
- integritu a autentickosť informácií, na základe ktorých sa niečo má robiť – napr.:
  - príkazy v Internet bankingu
  - dôležité oznamy (na webe, e-mailom)
  - identita informačných systémov, ktorým poskytujeme dôverné informácie

Čo je WWW?

Čo je WWW?

- systém na prístup k hypertextovým multimediálnym dokumentom

Čo je WWW?

- systém na prístup k hypertextovým multimediálnym dokumentom
- dokumenty = stránky

Čo je WWW?

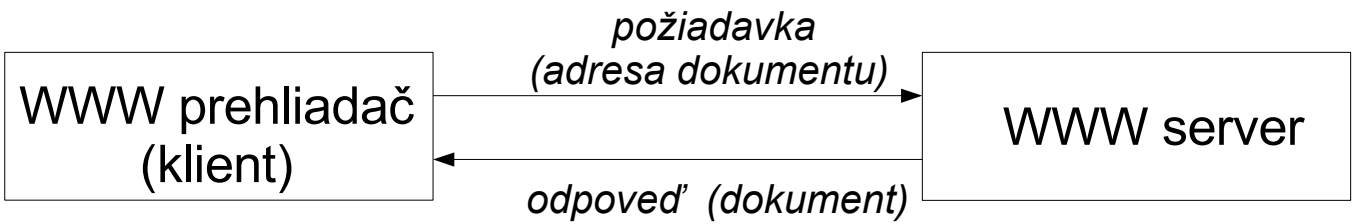
- systém na prístup k hypertextovým multimediálnym dokumentom
- dokumenty = stránky
- adresa – URL: `http://server/adresar/.../subor.html`

Čo je WWW?

- systém na prístup k hypertextovým multimediálnym dokumentom
- dokumenty = stránky
- adresa – URL: `http://server/adresar/.../subor.html`
- protokol HTTP

Čo je WWW?

- systém na prístup k hypertextovým multimediálnym dokumentom
- dokumenty = stránky
- adresa – URL: `http://server/adresar/.../subor.html`
- protokol HTTP
- klient – server architektúra



Ako vyzerá HTTP

```
GET /index.html HTTP/1.0

HTTP/1.0 200 Sending document
MIME-version: 1.0
Content-type: text/html
Content-transfer-encoding: 8bit
Last-Modified: Friday, 11-Dec-09 07:24:20 GMT
Content-length: 2965

<HTML>
<HEAD>
<TITLE>Univerzita Komenskeho Bratislava</TITLE>
...
```

Ako je to bezpečnosťou HTTP?

Ako je to bezpečnosťou HTTP?

- ktokoľvek na ceste môže odpočúvať požiadavku a odpoveď

Ako je to bezpečnosťou HTTP?

- ktokoľvek na ceste môže odpočúvať požiadavku a odpoveď
- ktokoľvek na ceste môže meniť požiadavku a odpoveď

Ako je to bezpečnosťou HTTP?

- ktokoľvek na ceste môže odpočúvať požiadavku a odpoveď
- ktokoľvek na ceste môže meniť požiadavku a odpoveď
- nie je ťažké presmerovať komunikáciu na iný server

Ako je to bezpečnosťou HTTP?

- ktokoľvek na ceste môže odpočúvať požiadavku a odpoveď
- ktokoľvek na ceste môže meniť požiadavku a odpoveď
- nie je ťažké presmerovať komunikáciu na iný server
- nie je nijak zabezpečená identita servera

Čo sa s tým dá spraviť?

Čo sa s tým dá spraviť?

- zabaliť HTTP do SSL $\Rightarrow$ HTTPS
  - ochrana dôvernosti prenášaných informácií – šifrovanie
  - ochrana integrity a autentickosti prenášaných informácií a identity servera – digitálne podpisy

Čo sa s tým dá spraviť?

- zabaliť HTTP do SSL ⇒ HTTPS
  - ochrana dôvernosti prenášaných informácií – šifrovanie
  - ochrana integrity a autentickosti prenášaných informácií a identity servera – digitálne podpisy
- zabezpečiť distribúciu verejných kľúčov – certifikáty
  - na overenie podpisu treba *spoľahlivo* poznať verejný kľúč
  - certifikát – zviazanie verejného kľúča s identitou jeho vlastníka
  - certifikáty vydávajú a elektronicky podpisujú *certifikačné autority* (CA)
  - certifikačné autority môžu vydávať certifikáty aj iným CA

Problémy pri používaní SSL

- Ignorovanie varovaní od prehliadača
  - certifikát vydaný neznámou CA – nemožno overiť podpis na certifikáte
  - certifikát vydaný na iné meno servera
- V oboch prípadoch sa môže jednať o útok a bezpečnosť je ako bez SSL.

Bezpečnostné vlastnosti e-mailu

Bezpečnostné vlastnosti e-mailu

- e-mail = pohľadnica písaná na stroji

Bezpečnostné vlastnosti e-mailu

- e-mail = pohľadnica písaná na stroji
- je triviálne poslať e-mail z ľubovoľnej adresy

Bezpečnostné vlastnosti e-mailu

- e-mail = pohľadnica písaná na stroji
- je triviálne poslať e-mail z ľubovoľnej adresy
- ktokoľvek na ceste môže odpočúvať

Bezpečnostné vlastnosti e-mailu

- e-mail = pohľadnica písaná na stroji
- je triviálne poslať e-mail z ľubovoľnej adresy
- ktokoľvek na ceste môže odpočúvať
- ktokoľvek na ceste môže meniť

Riešenia

Riešenia

- S/MIME
  - šifrovanie
  - elektronický podpis
  - používajú sa opäť certifikáty vydané CA
  - rovnaké problémy s overovaním podpisov ako pri SSL
  - podporované mnohými mailovými programami

Riešenia

- S/MIME
  - šifrovanie
  - elektronický podpis
  - používajú sa opäť certifikáty vydané CA
  - rovnaké problémy s overovaním podpisov ako pri SSL
  - podporované mnohými mailovými programami
- PGP
  - namiesto certifikačných autorít si certifikáty/kľúče podpisujú ľudia navzájom
  - existujú plugin-y pre mnohé mailové programy

Zavlečenie škodlivého softvéru

- Na webe je veľa škodlivého softvéru,

Zavlečenie škodlivého softvéru

- Na webe je veľa škodlivého softvéru,
  - často sa tvári užitočne,

Zavlečenie škodlivého softvéru

- Na webe je veľa škodlivého softvéru,
  - často sa tvári užitočne,
  - často je *pridanou hodnotou* k skutočne užitočnému softvéru,

Zavlečenie škodlivého softvéru

- Na webe je veľa škodlivého softvéru,
  - často sa tvári užitočne,
  - často je *pridanou hodnotou* k skutočne užitočnému softvéru,
  - jeho škodlivosť nemusí byť viditeľná.

Zavlečenie škodlivého softvéru

- Na webe je veľa škodlivého softvéru,
  - často sa tvári užitočne,
  - často je *pridanou hodnotou* k skutočne užitočnému softvéru,
  - jeho škodlivosť nemusí byť viditeľná.
- Škodlivý softvér sa šíri aj v e-mailoch.

Zavlečenie škodlivého softvéru

- Na webe je veľa škodlivého softvéru,
  - často sa tvári užitočne,
  - často je *pridanou hodnotou* k skutočne užitočnému softvéru,
  - jeho škodlivosť nemusí byť viditeľná.
- Škodlivý softvér sa šíri aj v e-mailoch.
- Prehliadače, mailové programy, editory, . . . obsahujú chyby,

Zavlečenie škodlivého softvéru

- Na webe je veľa škodlivého softvéru,
  - často sa tvári užitočne,
  - často je *pridanou hodnotou* k skutočne užitočnému softvéru,
  - jeho škodlivosť nemusí byť viditeľná.
- Škodlivý softvér sa šíri aj v e-mailoch.
- Prehliadače, mailové programy, editory, . . . obsahujú chyby,
  - škodlivý softvér sa môže skrývať aj v dokumentoch.

Ochrana pred škodlivým softvérom

- vyhýbať sa pochybným stránkam

Ochrana pred škodlivým softvérom

- vyhýbať sa pochybným stránkam
- nespúšťať programy z pochybných zdrojov

Ochrana pred škodlivým softvérom

- vyhýbať sa pochybným stránkam
- nespúšťať programy z pochybných zdrojov
- mať aktualizovaný operačný systém a aplikácie

Ochrana pred škodlivým softvérom

- vyhýbať sa pochybným stránkam
- nespúšťať programy z pochybných zdrojov
- mať aktualizovaný operačný systém a aplikácie
- používať antivírusový softvér

Ochrana pred škodlivým softvérom

- vyhýbať sa pochybným stránkam
- nespúšťať programy z pochybných zdrojov
- mať aktualizovaný operačný systém a aplikácie
- používať antivírusový softvér
- nepoužívať na prezeranie webu a čítanie e-mailu konto s administrátorskými právami

Priame útoky na počítač

- Operačný systém a aplikácie obsahujú chyby,
- chyby v programoch poskytujúcich sieťové služby sú často zneužiteľné.

Priame útoky na počítač

- Operačný systém a aplikácie obsahujú chyby,
- chyby v programoch poskytujúcich sieťové služby sú často zneužiteľné.
- Ochrana:

Priame útoky na počítač

- Operačný systém a aplikácie obsahujú chyby,
- chyby v programoch poskytujúcich sieťové služby sú často zneužiteľné.
- Ochrana:
  - aktualizovaný operačný systém a aplikácie,

Priame útoky na počítač

- Operačný systém a aplikácie obsahujú chyby,
- chyby v programoch poskytujúcich sieťové služby sú často zneužiteľné.
- Ochrana:
  - aktualizovaný operačný systém a aplikácie,
  - minimalizovať bežiace sieťové služby,

Priame útoky na počítač

- Operačný systém a aplikácie obsahujú chyby,
- chyby v programoch poskytujúcich sieťové služby sú často zneužiteľné.
- Ochrana:
  - aktualizovaný operačný systém a aplikácie,
  - minimalizovať bežiace sieťové služby,
  - používať firewall.

Sociálne inžinierstvo

- ľudia často naletia lákavým ponukám

Sociálne inžinierstvo

- ľudia často naletia lákavým ponukám
- ľudia často nečítajú podmienky použitia služieb

Sociálne inžinierstvo

- ľudia často naletia lákavým ponukám
- ľudia často nečítajú podmienky použitia služieb
- ľudia sú často príliš dôverčiví a nechajú sa "ukecať"

Otázky?