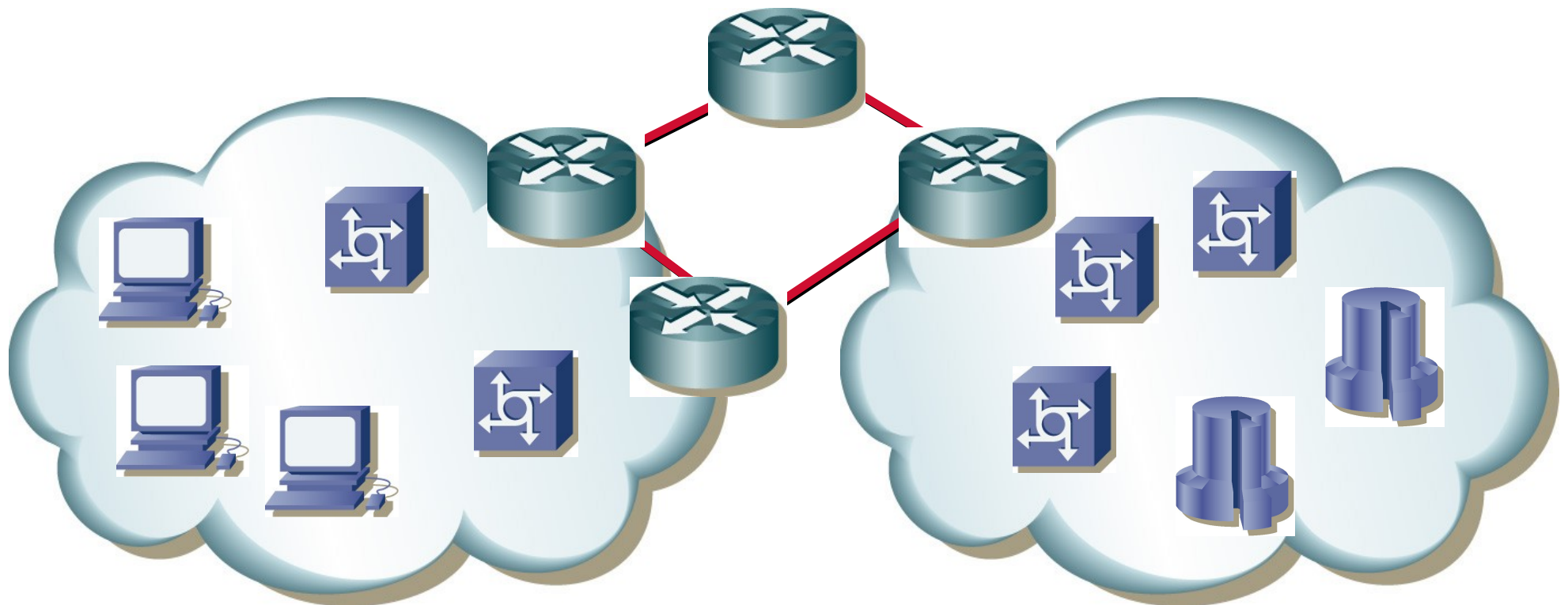


Počítačové sítě II

20. Útoky na síť a její ochrana

Miroslav Spousta, 2006

<qiq@ucw.cz>, <http://www.ucw.cz/~qiq/vsfs/>



Bezpečnost sítí

- cílem je ochránit počítačovou síť a především data/zařízení v nich před ztrátou, zneužitím, poškozením
- chceme zajistit
 - utajení a důvěrnost dat (ochrana před únikem informací)
 - autentizaci (uživatelů a služeb)
 - integritu dat (ochrana před (úmyslným/neúmyslným) poškozením dat)
- hojně se používá šifrování, podpisy, certifikáty
- ochrana může fungovat na různých vrstvách, *nikdy není absolutní*
 - fyzická: optická vlákna, kvantový přenos
 - linková: např. WEP, WPA, kontrola přístupu na základě adres
 - síťová IPSec, VPN, filtrování provozu
 - aplikační: SSL
- součástí systémové bezpečnostní politiky

Útoky na síť

- vnitřní a vnější
 - překvapivě hodně útoků se děje z vnitřní sítě
 - i částečně (útočník se nějak dostane do vnitřní sítě a tam škodí)
- útoky na propustnost sítě
- protokolové útoky (útoky na slabiny některých protokolů)
- útoky na aplikace (chyby v aplikacích, špatně ošetřené vstupy, atd.)
- falšování identity zdroje (spoofing)
- útoky na přístupová hesla
- odposlech komunikace
 - man-in-the-middle útok: změna informací po cestě
- odmítnutí služby (Denial of Service – DoS)
- unesení relace (session hijacking)

Spoofting

- změna adresy odesilatele (IP datagramu)
 - s úmyslem chovat se jako uživatel, který má přístup k určité službě
 - obcházení mechanismů pro filtrování provozu na základě adres
- pro UDP provoz může představovat velký problém
- útočník nedostane odpověď, ale to někdy nemusí vadit
- jako zdrojové adresy se používají např. adresy vnitřní sítě, loopback, ...
- obrana: filtrování podezřelých zdrojových adres na vstupním prvku (směrovači) do sítě

Přístupová hesla

- pokus zjistit přístupové heslo a tím oprávnění přístupu/nastavování zařízení
 - routery, switche, servery, tiskárny
- odposlechnutím komunikace (telnet, ftp, www)
- brute-force útok se zkoušením různých hesel
 - využití slabých hesel (slovníkových)
 - omezení některých algoritmů (crypt v UNIXu)
- obrana:
 - vynucení kvalitních hesel (už při zadávání), případně občasná kontrola hesel
 - šifrovaná komunikace (proti odposlechu)
 - omezení počtu neúspěšných přihlášení za jednotku času (brute-force)
 - hlášení pokusů o zjištění hesla

Útoky vedoucí k odmítnutí služby

- denial of service
- většinou zahlcením oběti, případně zahlcením linky k oběti
- mnoho způsobů
 - SYN flooding: generování mnoha paketů s nastaveným SYN flagem – cílový systém odešle SYN-ACK a čeká na odpověď, ale té se nedočká, časem mu přetečou tabulky pro otevřená spojení a přestane přijímat nová
 - záplava UDP datagramy: např pomocí chargen a echo (falešná adresa odesilatele)
 - ping na broadcast adresu (opět falešná adresa odesilatele), oběti se vrátí mnoho paketů (vlastně ostatní uzly v síti slouží k zesílení útoku)
 - přetížení DNS serverů
- často jsou útoky distribuované (z mnoha adres najednou)
- obrana: monitorování a filtrování provozu, omezení podezřelého provozu na směrovači, zakázání nepotřebných služeb

Unesení spojení, útoky na aplikace

- pokud probíhá komunikace (TCP), může se útočník snažit nahradit jednoho z účastníků (např. který je autorizován)
- pomocí uhodnutí následujícího sequence number
 - nebo při navazování spojení
 - obrana: při navazování spojení volit náhodné sequence number
- útoky na aplikace:
 - buffer overflow: přetečení bufferu
 - dojde k přepsání části zásobníku uživatelskými daty
 - začne se vykonávat kód, který si přeje klient (útočník)
 - obrana: pravidelně aktualizovat aplikace, speciální ochrany proti přetečení zásobníku
 - změna systému oprávnění: pouze nutná práva pro aplikaci, jemnější členění oprávnění

Útoky na DNS

- DNS je pro uživatele jedna z nejdůležitějších služeb
- útok DoS pomocí přetížení DNS serveru (např. rekurzivními dotazy)
 - dotaz je krátký, získat odpověď může být náročné
 - obrana: povolit rekurzivní dotazy jen někomu (z lokální sítě, ...)
- změna informací v cache
 - cache poisoning, úmyslně pozměním informace v cache tak, aby překlad směřoval na moji adresu – uživatelé budou myslet, že se jedná o původní server
 - např. pomocí falešné odpovědi DNS serveru (poměrně snadno: používá se UDP protokol)
- DDoS na DNS server: problém, nefunguje překlad adres => pro uživatele nepoužitelný Internet
- napadení přímo DNS serveru (a změna dat)
 - BIND míval velké bezpečnostní problémy

Firewall

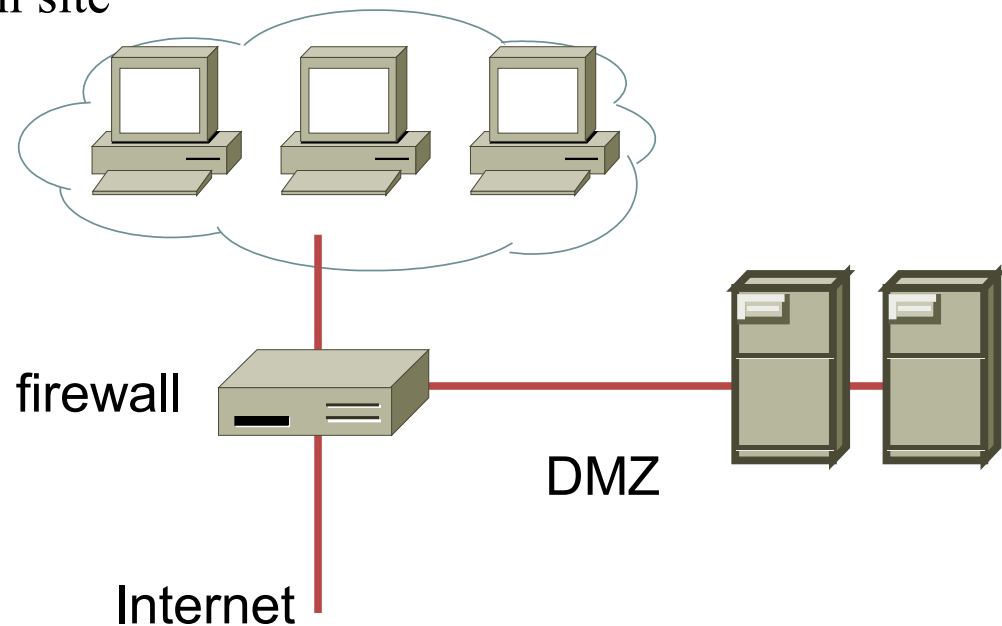
In construction, a firewall consists of a *windowless*, fireproof wall.

-- <http://wikipedia.org>

- je potřeba chránit vnitřní síť od vnějšího Internetu
- používá se označení firewall (ochranná zeď)
- filtruje provoz (především dovnitř, ale může i vně)
- většinou součástí směrovače, případně oddělené zařízení
- demilitarizovaná zóna (DMZ)
- firewall může rozhodovat podle informací z různých úrovní
 - fyzické: rozhraní
 - linkové: MAC adresa, protokol
 - síťové: IP adresy, flagy, fragmentace, ...
 - transportní: porty
 - aplikační: podle protokolu
- může provádět i např. šifrování provozu

Demilitarizovaná zóna

- neboli DMZ
- servery, které jsou přístupny ze světa není dobré umístit za firewall
 - stávají se zranitelným místem infrastruktury
- vyhradí se pro ně speciální část sítě oddělená od vnitřní sítě
 - servery (a služby na nich jsou přístupné vnějším uživatelům (v Internetu), ale nejsou fyzicky uvnitř privátní sítě



Firewall (2)

- původně: firewally byly bezstavové
 - aplikovaly se tzv. access-listy
 - pokud paket vyhovuje pravidlu, provede se daná akce (zahození, povolení, ...)
 - vše se děje jen na základě informací z hlaviček protokolů
- později: aplikační firewall: proxy server
 - analyzuje přímo aplikační protokol
 - může fungovat transparentně (není vidět) i netransparentně
 - zpomaluje komunikace (může i výrazně)
- stavová filtrace
 - firewall si pamatuje, která spojení byla navázána a přiřazuje pakety ke spojení
 - je možné např. povolit z Internetu pouze navázaná spojení
 - zatěžuje firewall, ale málo zpomaluje

Co je dobré filtrovat

- obecný přístup: vše zakázat, vybrané povolit
- na vstupu do sítě je vhodné filtrovat
 - adresy, které jsou součástí chráněné sítě
 - lokální adresy
 - datagramy, které jsou podezřelé (obsahují zdrojové směrování, příliš krátké fragmenty, ...)
 - datagramy, které nejsou součástí žádného spojení (ani nově navazovaného)
 - provoz dovnitř sítě pro služby, které nejsou explicitně povolené
 - někdy i v rámci sítě
 - ICMP zprávy: přesměrování, příliš velký ICMP provoz
- co by se nemělo filtrovat
 - většina ICMP zpráv (např. Time Exceeded zprávy, zprávy týkající se fragmentace, echo, ...)

Šifrování, autentizace

- pro utajení zpráv se používá šifrování
 - data se transformují tak, že není možné je rekonstruovat bez znalosti klíče
 - často se nejdříve data komprimují (po zašifrování to už není možné)
- používají se dva způsoby šifrování: symetrické a asymetrické
 - symetrické používá stejný klíč pro šifrování a dešifrování
 - asymetrické potřebuje pár klíčů
- pro ověření odesilatele zprávy je možné použít hash
 - pro zadanou zprávu se spočítá číslo, které odpovídá původní zprávě (ale je kratší, často má pevnou velikost)
 - pro autentizaci se používají symetrické i asymetrické šifry, kde prokázaná znalost tajného klíče umožňuje ověřit odesilatele

Symetrické šifrování

- šifrování symetrickým klíčem
- používá se stejný klíč pro šifrování i dešifrování
 - sdílí ho obě strany – tzv. sdílené tajemství (shared secret)
- používá se stejný algoritmus pro šifrování i dešifrování (jen obrácený)
- klíče mohou být poměrně krátké (128 bitů, 256 bitů)
- šifrování je velmi rychlé
- problém s distribucí klíče
 - je potřeba bezpečně doručit klíče oběma stranám
- algoritmy: DES, 3DES, AES, IDEA, Blowfish
 - liší se v délce klíče, rychlosti...

Asymetrické šifrování

- také šifrování asymetrickým klíčem
- máme pár klíčů, jeden je pro šifrování, druhý pro dešifrování
 - jsou svázané, patří k sobě
- jeden je privátní (musí být pečlivě střežen), druhý může být veřejně přístupný
- algoritmy jsou pomalé, náročné, většinou se nepoužívají pro samotné šifrování provozu, ale pouze pro počáteční inicializace
 - např. výměnu symetrických klíčů, které se pak používají pro další šifrování síťového provozu
- algoritmy:
 - Diffie-Hellman (DH): používá se pro distribuci klíčů
 - RSA: (faktorizace velkých čísel): velmi často používaný (SSL, podpisy, ...)

Otisky zprávy (hash)

- ze zprávy (libovolných dat) se vytvoří otisk
 - posloupnost (stovky) bitů
- tato posloupnost vyjadřuje šifrovací kontrolní součet
 - mělo by být velmi těžké najít dvě zprávy tak, aby měly stejný hash
 - také by mělo být těžké upravit zprávu s tím, že hash bude stejný
 - z hashe nelze rekonstruovat původní zprávu
 - ochrana proti (úmyslné) změně dat (ne tak CRC)
- používá se v zabezpečení jako doklad toho, že zpráva nebyla modifikována
 - je potřeba zajistit, aby nebyla modifikovaná zpráva i hash
 - k tomuto se ještě přidává k hashovací funkci tajné heslo (pro každé heslo vyjde jiný hash)
 - kdo nezná heslo, nemůže vypočítat hash => nemůže pozměnit zprávu
- algoritmy: MD5 (!), RC4 (!), SHA

Digitální podpis

- zpráva se uloží do speciálního formátu
- z takovéto zprávy se vytvoří hash
- výsledná hodnota se zašifruje privátním klíčem (vznikne podpis)
 - ale původní text je čitelný
- nyní se změna v původním textu (nebo v podpisu) dá snadno detekovat
 - dešifrujeme hash původní zprávy (pomocí veřejného klíče)
 - spočítáme hash aktuální zprávy – sedí-li je zpráva OK, jinak byla změněna
- k funkci digitálního podpisu je potřeba *důvěryhodná třetí strana*
 - Certifikační autorita (CA)
 - umožňuje ověřit, že daný veřejný klíč patří opravdu odesilateli
 - této třetí straně musí účastníci komunikace důvěřovat

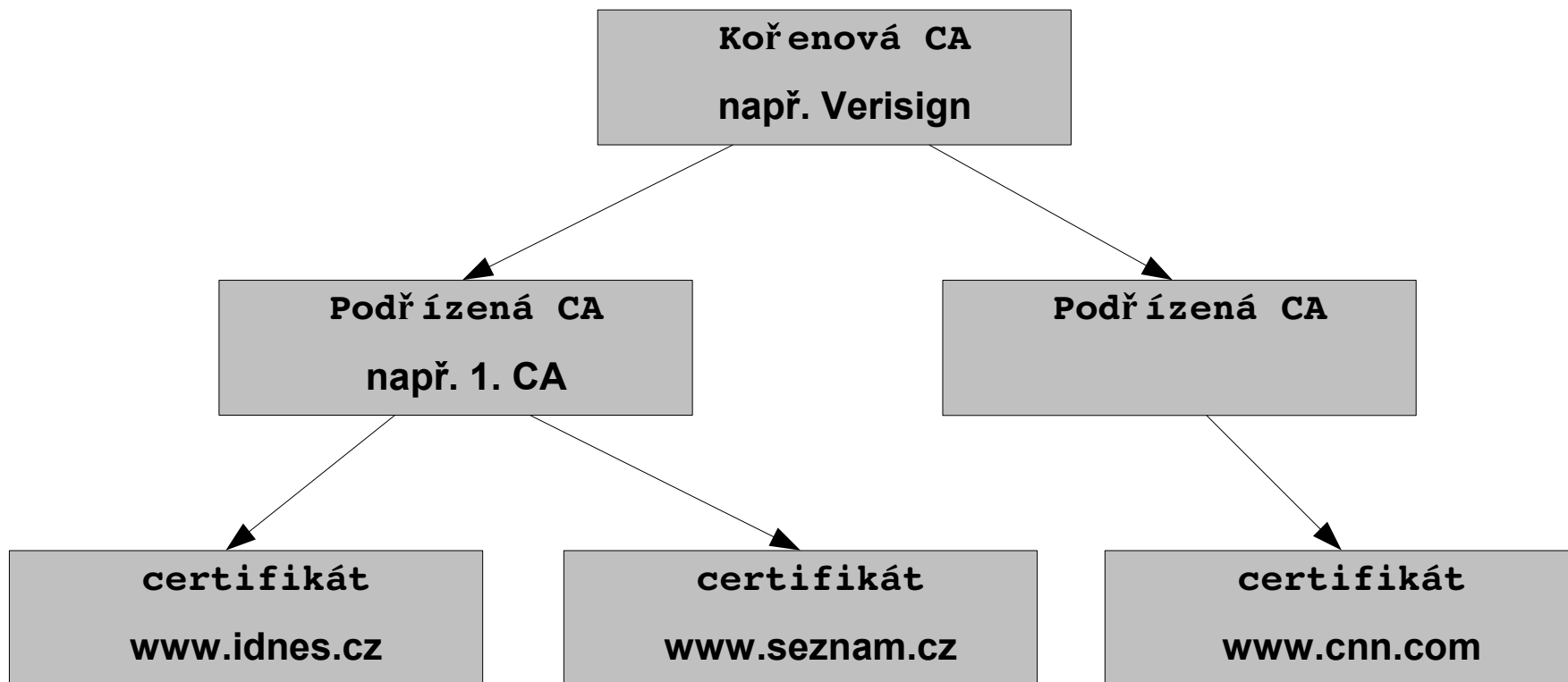
Certifikáty

- svazují osobu (nebo entitu, např. web server) se soukromým klíčem
- obsahují název entity, identifikační údaje, veřejný klíč, platnost certifikátu
- z těchto údajů je vytvořen hash (pomocí tajného klíče CA)
 - CA potvrzuje použitím svého klíče, že certifikát je platný
- Certifikační autorita (CA)
 - zodpovědná za vydávání certifikátu
 - stromová struktura (CA má svůj certifikát, ...)
 - kořenová autorita má certifikát podepsaný sama sebou (uživatelé mu musí věřit)
 - může jich být více
 - bývá důkladně zabezpečena
 - vydává certifikáty, CRL (Certificate Revocation List – neplatné certifikáty)

PKI

- Public Key Infrastructure
 - software (klient, server (CA)), hardware (smart cards, ...) a postupy
- umožňuje svázání veřejných klíčů s identitou uživatele
 - bez předchozí komunikace (!)
 - veřejné klíče bývají součástí certifikátů
 - umožňuje ověření identity protistrany
- uživatel podepisuje data svým privátním klíčem
 - protistrana si pomocí veřejného klíče, který je součástí certifikátu může ověřit, že data byla podepsána opravdu uživatelem s danou identitou
 - obdobně může uživatel data i zašifrovat
- dnes nejpoužívanější formát certifikátu: X.509
- použití:
 - podepisování/šifrování e-mailů (OpenPGP, S/MIME), autentizace (SSL), sestavení bezpečného spojení (SSL), výměna klíčů (IKE)

Certifikační authority, certifikáty

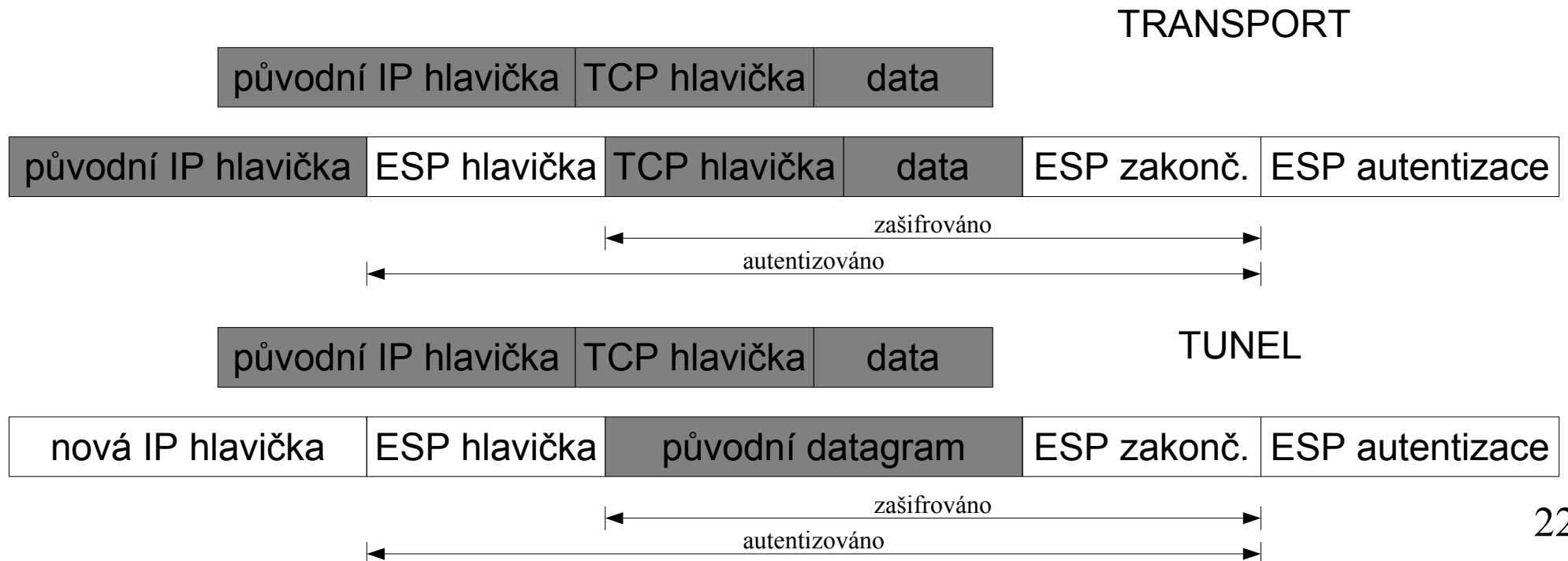


IPSec

- rozšíření Internet Protocolu o zabezpečení, šifrování datagramů
 - pracuje na síťové vrstvě (původně pro IPv6, dnes i pro IPv4)
 - koncové uzly o ní ani nemusí vědět
- využívá rozšíření hlavičky IP datagramu
- používá pojem bezpečnostní asociace (SA)
 - definuje opatření podle cíle (IP adresa) a obsahu datagramu
 - komunikující strany musí mít stejnou asociaci (váže se k ní dojednaný algoritmus pro šifrování, autentizaci...)
- IPSec podporuje dva protokoly: AH a ESP
- AH (Authentication Header) zajišťuje jen integritu (celého datagramu)
- ESP zajišťuje integritu i šifrování záhlaví a obsahu
- je potřeba zajistit distribuci symetrických klíčů: IKE (Internet Key Exchange, používá DH algoritmus), ISAKMP

IPSec

- funguje ve dvou režimech: transportu a tunelu
- transport: rozšíření IP hlavičky, jinak zůstává datagram stejný
 - menší režie
- tunel: datagram se celý zabalí do nového datagramu
 - ideální pro vytváření VPN



SSL (TLS)

- pracuje na aplikační (relační) vrstvě
- původně pro HTTP protokol (Netscape), Secure Socket Layer
- dnes se používá TLS (Transaction Level Security)
 - vychází z SSL
- používá X.509 certifikáty (většinou pro server, ale i pro klienta)
 - umožňuje ověřit, že daný server je opravdu ten, se kterým chcete komunikovat
 - brání man-in-the-middle útoku, ...
- důležité pro komerční využití
- velmi rozšířený, dnes se používá i u jiných služeb Internetu
 - POP3, IMAP, SMTP, LDAP, FTP
 - někdy se SSL domlouvá před navázáním spojení (POP3, IMAP), jindy v rámci protokolu (SMTP, FTP)