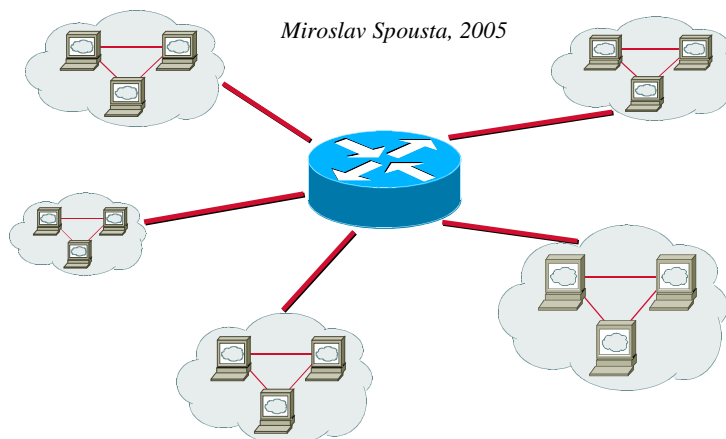


Po íta ové síť II

18. zabezpe ení síťí

Miroslav Spousta, 2005



1

Bezpe nost síťí

- cílem je ochránit po íta ovou síť a p edevším data/za ízení v nich p ed ztrátou, zneužitím, poškozením
- chceme zajistit
 - utajení a d v nost dat (uchrana p ed úníkem informací)
 - autentizaci (uživatel a služeb)
 - integritu dat (ochrana p ed (úmyslným/neúmyslným) poškozením dat)
- hojn se používá šifrování, podpisy, certifikáty
- ochrana m že fungovat na r zných vrstvách, *nikdy není absolutní*
 - fyzická: optická vlákna, kvantový p enos
 - linková: nap . WEP, kontrola p ístupu
 - síťová IPSec, VPN, filtrování provozu
 - aplika ní: SSL
- bezpe nostní politika: rozeznání autorizovaného a neautorizovaného chování²

2

Útoky na síť

- vnit ní a vn jší
 - p ekvapiv hodn útok se d je z vnit ní síť
- útoky na propustnost síť
- protokolové útoky (útoky na slabiny n kterých protokol)
- útoky na aplikace (chyby v aplikacích, špatn ošet ené vstupy, atd.)
- falšování identity zdroje (spoofing)
- útoky na p ístupová hesla
- odposlech komunikace
 - man-in-the-middle útok: zm na informací po cest
- odmítnutí služby (Denial of Service – DoS)
- unesení relace (session hijacking)

3

Spoofing

- změna adresy odesílatele (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 je to velký problém
- útočník nedostane odpověď, ale to někdy nemusí vadit
- jako zdrojové adresy se používají například adresy vnitřní sítě, loopback, ...
- obrana: filtrování podezřelých zdrojových adres na vstupu do sítě

4

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 kontrola hesel
 - šifrovaná komunikace (proti odposlechu)
 - omezení počtu neúspěšných přihlášení za jednotkovou dobu (brute-force)

5

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, a tím se mu přeteče tabulka otevřených spojení a přestane přijímat nová
 - záplava UDP datagramy: například pomocí chargen a echo (falešná adresa odesílatele)
 - ping na broadcast adresu (opět falešná adresa odesílatele), oběti se vrátí mnoho paketů (vlastně ostatní uzly v síti slouží k zesílení útoku)
 - přetížení DNS serveru
- často jsou útoky distribuované (z mnoha adres najednou)
- obrana: monitorování a filtrování provozu, omezení podezřelého provozu namířeno na konkrétní služby, zakázání nepotřebných služeb

6

Unesení spojení, aplikace a útoky

- 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 náhodné sequence number
- útoky na aplikace:
 - buffer overflow: přetečení bufferu
 - dojde k přepsání části zásobníku uživatelskými daty
 - za ně se vykonává kód, který si přejme klient (útočník)
 - obrana: pravidelně aktualizovat aplikace

7

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 navenku (z lokální sítě, ...)
- zmáknutí informací v cache
 - cache poisoning, úmyslné pozmenění informace v cache tak, aby předkládaná na moji adresu – uživatelé budou myslet, že se jedná o provozní server
 - např. pomocí falešné odpovědi DNS serveru (snadno: jedná se o UDP protokol)
- DDoS na DNS server: problém, nefunguje předkládaná adresy => pro uživatele nepoužitelný Internet
- napadení přímo DNS serveru (a zmáknutí dat)
 - BIND mával velké bezpečnostní problémy

8

Firewall

- je potřeba chránit vnitřní síť od vnějšího Internetu
- používá se označení firewall (obránná zeď)
- filtruje provoz (předešlým dovnitř, ale může i ven)
- 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 například šifrování provozu

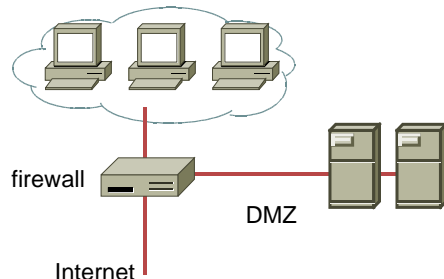
In construction, a firewall consists of a windowless, fireproof wall.

-- <http://wikipedia.org>

9

Demilitarizovaná zóna

- DMZ
- servery, které jsou přístupné ze sv. ta není dobré umislovat za firewall
 - stávají se zranitelným místem infrastruktury
- vyhradí se pro n. speciální část sítě oddělená od vnitřní sítě
 - servery (a služby na nich jsou přístupné vnějším uživat. m (v Internetu), ale nejsou fyzicky uvnitř privátní sítě



10

Firewall

- p. vodn.: 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 viditelný) i netransparentně
 - zpomaluje komunikaci (může i výrazně)
- stavová filtrace
 - firewall si pamatuje, která spojení byla navázána a paketizuje pakety ke spojení
 - je možné například povolit z Internetu pouze navázaná spojení
 - zatěžuje firewall, ale málo zpomaluje

11

Symetrické šifrování

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

12

Asymetrické šifrování

- šifrování asymetrickým klíčem
- máme pár klíčů, jeden je pro šifrování, druhý pro dešifrování
- jeden je privátní (musí být pevně uložen), druhý musí být veřejně dostupný
- algoritmy jsou pomalé, náročné, většinou se nepoužívají pro samotné šifrování provozu, ale pro počáteční inicializaci
 - například výměnu symetrických klíčů
- algoritmy:
 - Diffie-Hellman (DH): používá se pro distribuci klíče
 - RSA: (faktorizace velkých čísel): velmi používaný (SSL, podpisy, ...)

13

Otisky zprávy (hash)

- ze zprávy (libovolných dat) se vytvoří otisk – posloupnost bitů (stovky)
- tato posloupnost vyjadřuje šifrovací kontrolní součet
 - mohl by být velmi těžké najít dvě zprávy tak, aby měly stejný hash
 - z hashu 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 tomu se ještě přidává k hashovací funkci tajné heslo (pro každé heslo vyjde jiný hash)
 - kdo nezná heslo, nemůže vytvořit hash => nemůže poznamenat zprávu
- algoritmy: MD5 (!), SHA

14

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)
 - spojíme hash aktuální zprávy – sedí-li je zpráva OK, jinak byla změněna
- k funkci digitálního podpisu je potřeba *digital certificate*
 - Certifikační autorita (CA)
 - umožňuje ověřit, že daný veřejný klíč patří opravdu odesílateli
 - této třetí stranou se ujíždí účastníci komunikace

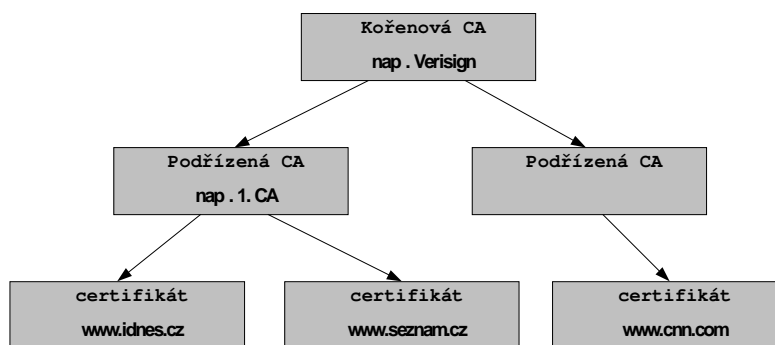
15

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 certifikátů
 - 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)

16

Certifikační autority



17

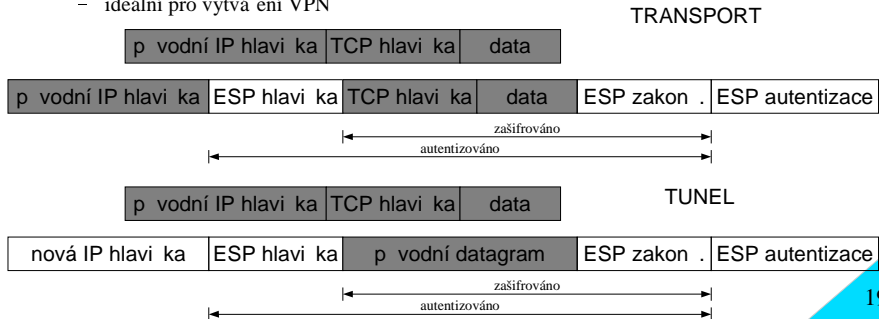
IPSec

- rozšíření Internet Protocolu o zabezpečení, šifrování datagramů
 - pracuje na síťové vrstvě (převodně 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, ISAKMP

18

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



19

SSL (TLS)

- pracuje na aplikační (relační) vrstvě
- původně pro HTTP protokol (Netscape), Secure Socket Layer
- dnes se používá TLS (Transaction Level Security)
 - vychází ze SSL
- používá X.509 certifikáty (včetně pro server)
 - umožňuje ověřit, že daný server je opravdu ten, se kterým chcete komunikovat
 - brání man-in-the-middle útoku, ...
- důležité pro komerční využití
- velmi rozšířený, používá se i u jiných služeb
 - POP3, IMAP, SMTP, LDAP, SSH

20