1. Základy zabezpečení sítí

Zabezpečení sítě

- ✓ minimalizace zranitelných míst v síti (zajišťujeme informace a data, služby přenosu a zpracování dat, zařízení, uživatele - jejich majetek a identitu)

Ohrožení komunikačního systému

- ✓ zničení, poškození, modifikace, krádež nebo ztráta informací, přerušení služeb

Bezpečnostní služby v sítích

Utajení a důvěrnost dat (Confidentiality and Privacy)

- ✓ ochrana před neautorizovaným únikem informací (pokud dojde k zachycení dat útočníkem, tato data jsou pro útočníka nesrozumitelná)

Autentizace (Authentication)

- ✓ ověření totožnosti druhé komunikující strany (druhá strana je opravdu tím, za koho se prohlašuje)

Integrita dat (Integrity)

- ✓ zajištění nedotknutelnosti přenášených dat (vyslaná a přijatá zpráva jsou shodné)

Nepopiratelnost (Nonrepudiation)

- ✓ zabránění odesilateli nebo příjemci odmítnout potvrzení o vyslání nebo přijetí zprávy (popření odpovědnosti)

Řízení přístupu (Access Control)

- ✓ na základě identifikace uživatele umožnění přístupu do systému podle přidělených práv

Útoky na bezpečnost sítě

Průzkum sítě

- ✓ slouží k neautorizovanému sběru informací a mapování zařízení, systémů, služeb a zranitelných míst v síti
- ✓ pro jeho realizaci se používá – hromadný ping (ping sweeps), odchytávání paketů (packet sniffer), skenery portů (port scanners) apod.

Hromadný ping

- ✓ zjišťuje, které, počítače jsou v síti „živé“ (odpovídají na ping)
- ✓ ochrana – zakázání odpovědi na ping na firewallu - akce DROP (systém se jeví jako neaktivní)

Odchytávání paketů

- ✓ Wireshark – původně Ethereal, zachycuje síťový provoz pro případnou analýzu dat, má uživatelsky přívětivé grafické rozhraní
- ✓ Tcpdump – předchůdce Wireshark, nemá grafické rozhraní
- ✓ Dsniff – odchytává provoz a na výstup vypisuje zachycená uživatelská jména a hesla

Skenování portů

- ✓ Zjišťování otevřených portů, cílem je zjistit, jaké služby jsou na něm spuštěny
- ✓ Nmap – multiplatformní port skener, dokáže určit operační systém, jména a verze služeb, typ zařízení, případně firewall

Internetové informace

- ✓ Lze zjistit poskytovatele serveru, adresu DNS serveru a další
- ✓ Používá se utilita whois

Získání přístupu

- ✓ Útok na heslo – útok hrubou silou, použitím trojských koní, odchycením hesla jako plain text (POP3, telnet, …)

Lámání hesel

Lámání přístupového hesla

- ✓ Útok hrubou silou – útočník zkouší všechny možné kombinace písmen a znaků, je nutná alespoň částečná povědomost například o délce hesla, časově velmi náročné
- ✓ Slovníkový útok - útočník zkouší nejpoužívanější slova daného jazyka
- ✓ Ochrana - delšími intervaly mezi chybně vloženými hesly, dočasným zamknutím účtu, volbou vhodného hesla (delší hesla s kombinací písmen, čísel a dalších znaků)

Lámání lokálně uložených hash otisků

- ✓ Při napadení databáze může útočník získat zašifrovaná hesla (obvykle v podobě hash otisku)
- ✓ Hash – jednosměrná funkce, která produkuje řetězce definované délky (MD5)

Programy pro lámání hesel

- ✓ Cain a Abel, John the Ripper, Ophcrack, Nessus

Využití důvěryhodnosti - Man in The Middle (MITM)

- ✓ Útočník se stane prostředníkem komunikace dvou stran a snaží se odposlouchávat nebo měnit přenášenou komunikaci
- ✓ Ochrana – sslstrip (při útoku přeruší SSL spojení)

DHCP spoofing

- ✓ Útočník připojí do sítě vlastní DHCP server, který přiděluje klientům správné IP adresy, ale adresa DNS a brány mají IP adresu útočníka
- ✓ Ochrana – použití funkce DHCP snooping

ARP spoofing

- ✓ Útočník pošle **oběti** ARP reply paket, ve kterém je uvedeno, že brána má MAC adresu útočníka a **bráně** pošle ARP reply paket, ve kterém je uvedeno, že oběť má MAC adresu útočníka
- ✓ Napadené stanice budou tedy při vzájemné komunikaci používat MAC adresu útočníka, který je pak přeposílá na správné MAC adresy

Přetečení zásobníku (Buffer Overflow)

- ✓ Program zapíše data na zásobník mimo alokovanou oblast (do bufferu pevné délky, jehož velikost je menší než zapisovaná data)
- ✓ Poškození obsahu jiných proměnných, pád aplikace
- ✓ Jedna z nejstarších a nejúčinnějších forem počítačového útoku

Exploit

- ✓ Program, část dat nebo posloupnost instrukcí, které využívají chyby v programu a způsobují například přetečení zásobníku
- ✓ Další část kódu pak umožní neoprávněný přístup do systému nebo spuštění DoS útoku

Phishing

- ✓ Technika založená na sociálním inženýrství
- ✓ Slouží k vylákání citlivých údajů přes internet
- ✓ Rozesílání podvodných e-mailových zpráv, které vyzývají k zadání přihlašovacích údajů a hesel
- ✓ Společné znaky podvodných zpráv – http odkazy vedou na jiné stránky, než je uvedeno v textu, zpráva obsahuje spustitelnou přílohu, je vyžadováno neprodlené sdělení osobních údajů (například pod pohrůžkou zrušení účtu), často má zpráva výrazné gramatické nedostatky nebo je v cizím jazyce

Pharming

- ✓ Slouží k získávání osobních údajů od uživatelů manipulací s DNS záznamy
- ✓ Díky upraveným DNS záznamům se podvodné stránky jeví jako originální
- ✓ Mechanismus útoku – modifikace lokálního DNS (hosts soubor), napadení DNS serveru a provedení úprav

Útoky na webové aplikace

Cross Site Scripting (XSS)

- ✓ Narušuje správnou interpretaci webových stránek, k tomu využívá bezpečnostních chyb ve skriptech obvykle podstrčením vlastního javascript kódu
- ✓ Poškození vzhledu a funkčnosti stránky, získání citlivých dat
- ✓ Nepersistentní (Reflected) útok – úprava části URL, uživatel otevře falešný link, útočník tím přesměruje citlivá data na sebe
- ✓ Persistentní (Stored) útok – škodlivý kód se spustí sám, jakmile se uživatel octne na odkloněných stránkách (například komentář k produktu)

SQL Injection

- ✓ Technika napadení databázové vrstvy přes vrstvu aplikační
- ✓ Zranitelnost je způsobena špatně vyfiltrovanými uživatelskými vstupy, které jsou vloženy přímo do SQL dotazů
- ✓ Útok je obvykle prováděn úpravou samotného URL

Denial of Service (DoS)

- ✓ Cílem je zahlcení oběti požadavky, které způsobují postupné vyčerpávání jeho zdrojů, čímž dojde ke znepřístupnění služby, počítače nebo celé sítě

Vyčerpání prostředků

- ✓ Přenosového pásma, místa na disku
- ✓ Narušení směrovacích informací, stavových informací nebo fyzických síťových komponent

IP spoofing

- ✓ falešná adresace, mění skutečnou zdrojovou adresu datagramu, která je zakázaná pro vstup do dané sítě, na adresu povolenou, útočník pak požaduje služby jako důvěryhodný uživatel
- ✓ průnik do sítě je možný v rámci různých aplikací (FTP, SMTP, Telnet, www)
- ✓ je uskutečnitelný jak zvnějšku tak i od vnitřního uživatele (bez příslušných přístupových práv)
- ✓ identifikace zdroje útoku se provádí například pomocí zdrojové MAC adresy v záhlaví linkového rámce (pokud není stanice za směrovačem)

Útoky pomocí ICMP zpráv

Ping of Death

- ✓ útočník pošle ICMP zprávu s požadavkem na odezvu, jejíž velikost je větší než maximální povolená (64kB)
- ✓ Je účinný především u starších systémů

Smurf Attack (Šmoulí útok)

- ✓ Využívá techniku podvrhnutí zdrojové IP adresy
- ✓ Útočník posílá ICMP zprávy echo request na všeobecnou adresu, avšak se zfalšovanou zdrojovou adresou (adresa oběti)
- ✓ Všechny počítače, které žádost přijmou, ji pošlou zpět na IP oběti

Ping flooding

- ✓ Útočník posílá rozsáhlé požadavky na odezvu v krátkých intervalech, aby zahltil linku oběti
- ✓ Útočník musí mít rychlejší připojení než oběť

TCP SYN Flood

- ✓ generování zpola otevřených spojení TCP, tím donutí oběť odesílat SYN-ACK, ale protože na ně žádné potvrzení neobdrží, hromadí se tyto zprávy ve vyrovnávací paměti, ta se zahltí a systém začne odmítat oprávněné žádosti o navázání spojení (cca 94% útoků)

Distributed Denial of Service (DDoS)

- ✓ využívají více toků útočného provozu, aby zahltily cílové systémy přemírou paketů, cílem je zahltit systém samotný nebo jemu příslušející komunikační spoj

Nebezpečné programy

Virus

- ✓ program, který se dokáže šířit (vytváří své vlastní kopie) bez vědomí uživatele
- ✓ pro svou aktivaci potřebuje akci ze strany uživatele (otevření infikované přílohy mailu a podobně)
- ✓ mohou být destruktivní (mazání systémů na disku, modifikace systémových registrů) nebo nepříjemné (rozeslání kontaktů z adresáře mailem, zobrazení zprávy na obrazovce)
- ✓ Nejznámější viry – Pakistani Brain (1986) , Christmas Tree (1987), Michelangelo (1991), Melissa (1999)

Červ

- ✓ Program kopírující sám sebe bez vědomí a bez zásahu uživatele
- ✓ Součástí červa je náklad (payload), který způsobuje narušení systému, mazání souborů, vyhledávání citlivých údajů, vytvoření zadních vrátek do systému pro pozdější snadný přístup
- ✓ Nejznámější červy - Worm (1988), Iloveyou (2000), Code Red (2001), Blaster (2003), Mydoom (2004)

Trojský kůň

- ✓ Trojský kůň se obvykle tváří jako užitečný program (hra, spořič obrazovky, …)
- ✓ Je to škodlivý software, který na rozdíl od virů nebo červů nemá schopnost sám sebe replikovat
- ✓ Trojský kůň může hackerovi poskytnout vzdálený přístup k cílovému počítačovému systému a využít ho (sniffer, keylogger, spam server, …)
- ✓ Některé trojské koně jsou spíš nepříjemné než nebezpečné (změna ikony na ploše)

- ✓ Jiné mohou způsobit vážná poškození odstraněním souborů a ničit informace na disku
- ✓ Například – Waterfalls.scr, Dowloader-EV, NetBus, Tagasaurus

Řízení přístupu

- ✓ **AAA** (Authentication, Authorization and Accounting) – autentizace, autorizace a účtování

Autentizace

- ✓ ověřování a potvrzování totožnosti uživatelů pro kontrolu oprávněnosti přístupu k síti (podle použitého jména a hesla, certifikátů, čipových karet a podobně)
- ✓ **identifikace** – zjištění identity uživatele
- ✓ **verifikace** – potvrzení identity uživatele

Existují tři možné způsoby autentizace

- ✓ **kdo jsou** – identifikace podle globálně jednoznačných ukazatelů jako jsou otisky prstů, hlas, struktura oční duhovky, podpis, DNA – biometrická autentizace, lze je obtížně zaměnit, avšak vyžadují nákladná zařízení pro identifikaci
- ✓ **co mají** – identifikace podle vlastnictví určitých předmětů (klíče, karty), jednodušší způsob, ale je náchylný ke ztrátám, kopiím a krádežím
- ✓ **co znají** – identifikace pomocí přístupových hesel, číselných kombinací, osobních identifikačních čísel, nejjednodušší způsob zabezpečení, je však náchylný k zapomenutí, možnost zneužití v případě záznamu na libovolném médiu, ochrana pomocí silných hesel a jejich častým změnám

autentizace může probíhat

- ✓ **jednosměrně** (one-way) – autentizuje se pouze jedna strana vůči druhé
- ✓ **obousměrně** (two-way) – autentizují se obě strany vzájemně
- ✓ za pomoci **třetí důvěryhodné strany** (trusted third party) – poskytuje informace pro autentizaci nebo ověřuje identitu uživatelů
- ✓ **IPv6** – autentizace uživatelů je zaimplementována přímo v protokolu

Autorizace a účtování

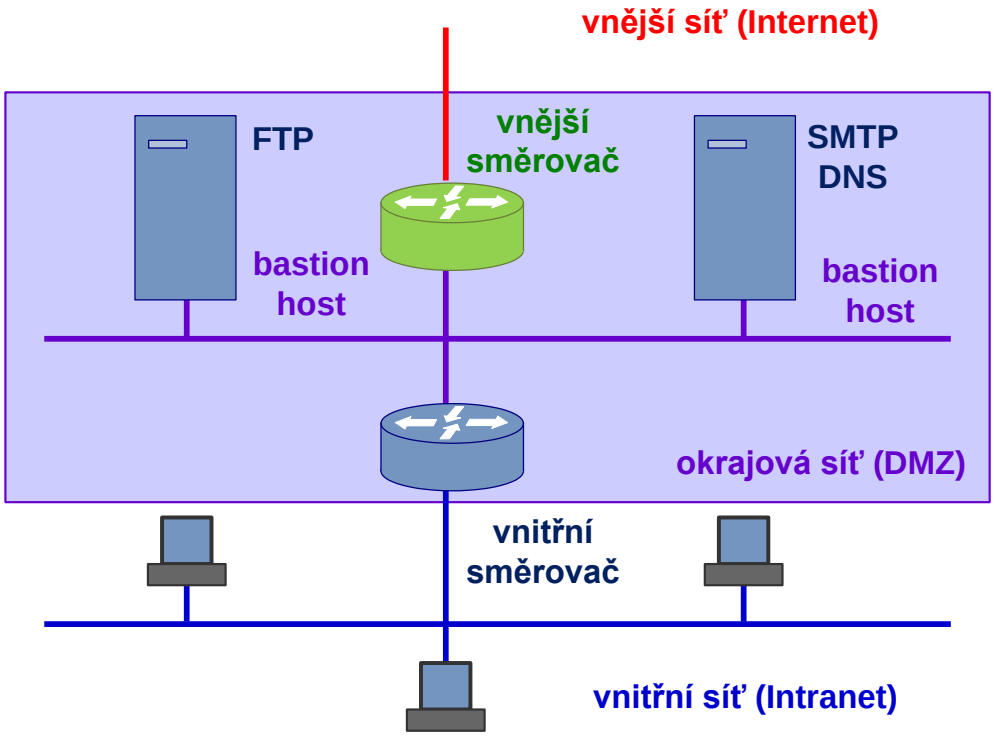
- ✓ **Autorizace** - specifikuje, jaké operace mohou uživatelé provádět v daném systému a jaká data jsou pro ně dostupná
- ✓ **Účtování** - zodpovídá za záznam všech činností uživatele v daném systému (čas přihlášení, změny na zařízení, čas odhlášení)

Centralizovaná adresářová služba pro správu uživatelů (jména, hesla, záznamy o jejich činnosti):

- ✓ **TACACS** (Terminal Access Controller Access Control System) – umožňuje ověřit každého uživatele na individuální bázi před přístupem ke směrovači nebo komunikačnímu serveru, lze ho využívat ve spolupráci se systémem Kerberos, zahrnuje všechny složky architektury AAA
- ✓ **RADIUS** (Remote Authentication Dial-In User Service) – zahrnuje všechny tři složky architektury AAA, navržen pro přístup uživatelů po vytáčeném připojení (SLIP, PPP), šifruje pouze heslo
- ✓ **TACACS+** - používá protokol TCP (garantována komunikace mezi klientem a serverem), šifruje celé spojení, podporuje různé metody AAA, umožňuje definovat příkazy, které smí uživatel použít (pevně kontrolovaný přístup pro značné množství uživatelů)

Firewall

- ✓ chrání síť před útoky zvnějšku
- ✓ nesmí nepříznivě ovlivňovat provoz v dané síti (především zpoždění v síti)
- ✓ nesmí obsahovat žádná data ani prostředky, které by mohl případný útočník zneužít pro přístup do sítě



- ✓ **směrovač** filtruje provoz mezi vnitřní a vnější sítí, aby omezil útoky zvnějšku
- ✓ **demilitarizovaná zóna** (DMZ – DeMilitarized Zone, perimeter network) - server nebo síť serverů přístupná zevnitř podnikové sítě i zvnějšku, obsahuje potřebné servery (www, SMTP, FTP, autentizační) – bastion hosts, přístupné zvnějšku přes externí směrovače i zevnitř přes vnitřní směrovače (filtrace paketů oběma směry)

Druhy firewallu

Paketový filtr

- ✓ Zpracovává pakety a rozhoduje o jejich propuštění nebo zahození
- ✓ Statické filtrování – na směrovači je nakonfigurováno filtrovací pravidlo (ACL)
- ✓ Dynamické filtrování – při odchozím provozu lze dynamicky měnit pravidla
- ✓ Stavový firewall – paketový filtr rozšířený o tabulku probíhajících spojení, je schopen řídit filtrování i pro příchozí provoz již navázaných spojení

Circuit Gateways

- ✓ Brány pracující na transportní vrstvě, provoz řídí na základě zdrojové nebo cílové IP adresy, nekontrolují obsah paketů, slouží k prevenci přímého propojení sítí

Aplikační brána

- ✓ Proxy firewall (= zástupný firewall)
- ✓ Pracuje na aplikační vrstvě (je schopna rozhodovat na základě obsahu aplikačních dat)
- ✓ zajistí nejprve autentizaci vnějšího uživatele, a teprve pak umožní komunikaci se serverem v DMZ

NAT (Network Address Translation)

- ✓ Překlad privátních adres na veřejné adresy
- ✓ Umožňuje ochranu vnitřních uživatelů sítě, jejichž adresy zůstávají pro vnější sítě neznámé, a tedy nedostupné

Filtrace paketů

- ✓ ACL (Access Control List) – přístupový seznam

Port ACLs

- ✓ Aplikují se na L2 rozhraní přepínače
- ✓ Jsou podporovány pouze pro vstupní směr filtrování na fyzických rozhraních
- ✓ **Standard IP ACLs** – filtrují pouze zdrojovou IP adresu
- ✓ **Extended IP ACLs** – používají zdrojovou i cílovou IP adresu případně typ protokolu
- ✓ **MAC extended ACLs** – používají zdrojovou a cílovou MAC adresu případně typ protokolu

Router ACLs

- ✓ Aplikují se na L3 rozhraní směrovače (nebo přepínače)
- ✓ **Standard IP ACLs** – používají zdrojovou IPv4 adresu
- ✓ **Extended IP ACLs** – používají zdrojovou i cílovou IP adresu případně typ protokolu

Šifrování

- ✓ Slouží k utajení přenášených dat nebo k autentizaci
- ✓ Šifrování – kryptografický algoritmus převádějící prostý text na šifrovaný
- ✓ Klíč – tajná informace, která slouží k šifrování/čtení zprávy
- ✓ **Soukromý klíč** (private key, symetrické) – obě strany komunikace sdílejí stejný soukromý klíč, který se používá pro šifrování i dešifrování
- ✓ **Veřejný klíč** (public key, asymetrické) – data zašifrovaná jedním klíčem lze dešifrovat klíčem druhým, přičemž oba tyto klíče tvoří jedinečný pár vzájemně korespondujících klíčů, jeden klíč je dostupný komukoli, zatímco druhý je přísně soukromý
- ✓ **Hashovací funkce** – funkce, která zpracuje celý text a vytvoří z něj krátký řetězec, který by měl se stoprocentní pravděpodobností identifikovat nezměněný text

Šifrování soukromým klíčem

- ✓ Klíč k šifrování/dešifrování musí být znám pouze uživatelům
- ✓ Při distribuci samotného klíče je třeba zajistit jeho šifrování silnou šifrou (bezpečnost)

DES (Data Encyption Standard)

- ✓ Klíč o délce 56 bitů (+ 8 bitů paritních), který se používá na blok o délce 64 bitů
- ✓ Roku 1977 zvolena za standard pro šifrování ve státních organizacích v USA
- ✓ Prolomena1997, lze ho prolomit hrubou silou za méně než 24 hodin

3DES

- ✓ Silnějšího šifrování lze dosáhnout trojitým použitím klíče
- ✓ Celková délka klíče je pak 3 x 56 = 168 bitů

AES (Advanced Encryption Standard)

- ✓ Moderní symetrická bloková šifra založena na Rijndaelovu algoritmu
- ✓ Pochází z roku 2001, ja nástupcem šifry DES
- ✓ Klíče o délkách 128, 192 nebo 256 bitů pro šifrování bloků 128, 192 nebo 256 bitů
- ✓ Je součástí zabezpečení WPA2 pro WiFi sítě

Kerberos

- ✓ Systém zabezpečeného distribuovaného výpočetního prostředí využívající šifrování soukromým klíčem založeném na DES
- ✓ Byl navržen pro autentizaci požadavků na využívání síťových zdrojů
- ✓ Slouží pro verifikaci identit jednotlivých entit v nechráněné síti využívá důvěryhodnou třetí stranu (autentizační server)

Šifrování veřejným klíčem

- ✓ K šifrování/dešifrování používá dvou klíčů – soukromého a veřejného
- ✓ Koncový systém vygeneruje **dva klíče** – jeden tajný a druhý veřejně dostupný
- ✓ Pokud **uživatel A** potřebuje zaslat šifrovanou zprávu uživateli B, použije k zašifrování **veřejný klíč**, inzerovaný uživatelem B
- ✓ **Uživatel B** pak použije jen sobě známý **soukromý klíč**
- ✓ Každé dvě stanice mohou bezpečně komunikovat bez předchozího předávání klíčů dvojím šifrováním, soukromým a veřejným klíčem, a to v libovolném pořadí
- ✓ K dešifrování zprávy **neoprávněnému uživateli** nestačí ani znalost šifrovacího klíče, algoritmu a přenášené zprávy, neboť mu chybí soukromý klíč
- ✓ Výhoda - jednoduchá správa šifrovacích klíčů (není třeba zabezpečená komunikace)
- ✓ Nevýhoda – složitost použitého algoritmu (často se používá pro zašifrování a bezpečnou distribuci symetrických klíčů)

Diffie-Hellman (DH)

- ✓ Protokol umožňující vytvořit mezi komunikujícími stranami zabezpečené spojení bez nutnosti předchozí domluvy šifrovacího klíče
- ✓ Algoritmus pro výpočet veřejného klíče pochází z roku 1976, používá se pro bezpečnou distribuci klíčů
- ✓ Náchylné na útoky man-in-the-middle (útočník může odposlechnout veřejné klíče obou stran a podsunout svoje falešné klíče)

RSA (autoři Rivest, Shamir, Adleman)

- ✓ Šifra s veřejným klíčem, je vhodný pro podepisování i šifrování
- ✓ Používají se klíče přes 100 číslic dlouhé (spolehlivost algoritmu závisí na délce použitého klíče)
- ✓ Použití – šifrování, autentizace, elektronická pošta, digitální podpisy,SSL

Elektronický podpis

- ✓ Splňuje podmínky autenticity, integrity, nepopiratelnosti a nenapodobitelnosti podpisu

Postup vytvoření elektronického podpisu

- ✓ Vyrobí se otisk zprávy
- ✓ Otisk se zašifruje pomocí soukromého klíče
- ✓ Zpráva se odešle v čitelné podobě (plain text), jako příloha se doplní šifrovaný otisk a veřejný klíč
- ✓ Příjemce rozšifruje pomocí veřejného klíče zašifrovaný otisk a porovná ho s otiskem, který si sám vytvoří z přijaté zprávy
- ✓ Pokud se otisky shodují, zpráva nebyla pozměněna (integrita) a díky veřejnému klíči je ověřen i odesílatel zprávy (nepopiratelnost)
- ✓ Nevýhoda – nejsme schopni ověřit, kdo je skutečným vlastníkem veřejného klíče (nutno zavést certifikáty)ú

PKI (Public Key Infrastructure)

- ✓ Označení HW a SW prostředků a pracovních postupů, které umožňují spravovat a distribuovat veřejné klíče
- ✓ Umožňuje používat cizí veřejné klíče a ověřovat jimi elektronické podpisy

Digitální certifikát

- ✓ Je to digitálně podepsaný veřejný šifrovací klíč, který vydává certifikační autorita
- ✓ Má formát běžného datového souboru, jehož zfalšování se zabrání tím, že ho podepíše třetí strana (certifikační autorita)
- ✓ Strukturu certifikátu jednoznačně popisuje mezinárodní norma X.509

Každý certifikát musí obsahovat:

- ✓ Sériové číslo – pro každý certifikát je jedinečné
- ✓ Dobu platnosti – závisí na délce použitého klíče (pro klíč 1024b je to 1 rok)
- ✓ Identifikační údaje subjektu – ověřuje certifikační autorita
- ✓ Veřejný klíč – nejčastěji 1024 nebo 2048b, + typ algoritmu pro elektronický podpis
- ✓ Identifikační údaje certifikační autority – identifikace klienta, podpis elektronické pošty, autorizace bankovních transakcí, omezení použití certifikátu, …

Certifikační autorita (CA – Certification Authority)

- ✓ Subjekt, který se zabývá vydáváním digitálních certifikátů pro ostatní subjekty i osoby
- ✓ Root CA – kořenová CA, nejvyšší certifikační autorita
- ✓ Abychom mohli považovat certifikát za bezpečný, musí být podepsán v hierarchii nadřazenou CA
- ✓ CRL (Certificate Revocation List) – seznam zneplatněných certifikátů (se skončenou dobou platnosti)

Registrační autorita (RA-Registration Authority)

- ✓ Slouží ke snížení zátěže CA
- ✓ Mají za úkol komunikaci s žadateli a jejich ověřování, generování klíčů pro uživatele, přeposílání žádostí na CA (nemůže certifikáty vydávat nebo publikovat CRL)

Virtuální privátní síť (VPN)

- ✓ **VPN** (Virtual Private Network)
- ✓ Umožňují bezpečný vzdálený přístup do soukromé sítě přes veřejnou síť
- ✓ Princip – tunelování provozu mezi oběma stranami

Výhody VPN

- ✓ Úspora nákladů – společnost nemusí pořizovat drahé připojení (pronajaté linky)
- ✓ Bezpečnost – šifrování, autentizace, …
- ✓ Škálovatelnost – snadné rozšíření o další uživatele
- ✓ Dostupnost – připojení přes WiFi, xDSL, 3G, …

Nevýhody VPN

- ✓ Nutnost instalace a nastavení VPN klienta
- ✓ Snížení propustnosti – šifrování, redundantní data
- ✓ HW nároky – především na směrovače a VPN koncentrátory při vyšších přenosových rychlostech

Typy VPN

- ✓ **Site-to-Site VPN** – ropojení geograficky vzdálených sítí do jednoho intranetu,
- ✓ **Remote access** – vzdálený přístup, brána VPN musí vykonávat funkce DHCP a DNS, autentizace klientů

IPSec

- ✓ poskytuje silné zabezpečení na bázi šifrování pro IPv4 a IPv6
- ✓ zajišťuje šifrování, autentizaci, integritu, a důvěryhodnost na úrovni datagramů

Režimy zabezpečení paketů

Režim transportu

- ✓ Šifruje pouze datovou část IP paketu
- ✓ Bezpečnostní záhlaví je vloženo mezi záhlaví IP datagramu a záhlaví vyšší vrstvy (TCP/UDP)
- ✓ Méně bezpečné, slouží k ochraně komunikace v rámci jedné sítě a při komunikaci s klienty

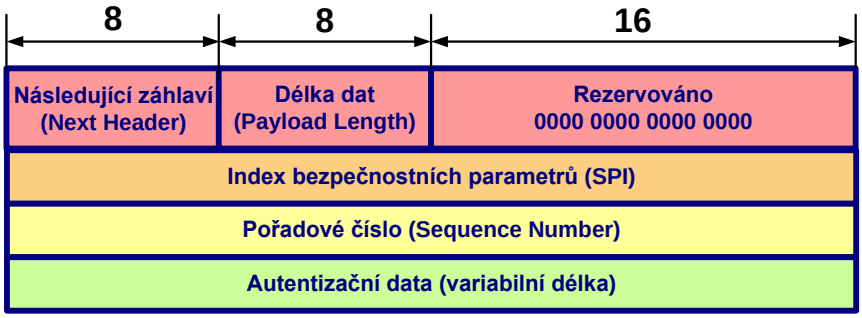
Režim tunelu

- ✓ Chrání celý IP paket – zabezpečí se a vloží do nového IP paketu
- ✓ Paket má dvě IP záhlaví – vnitřní (původní) a vnější (nové)
- ✓ Používá se mezi sítěmi s nedůvěryhodnou cestou

IPsec protokololy

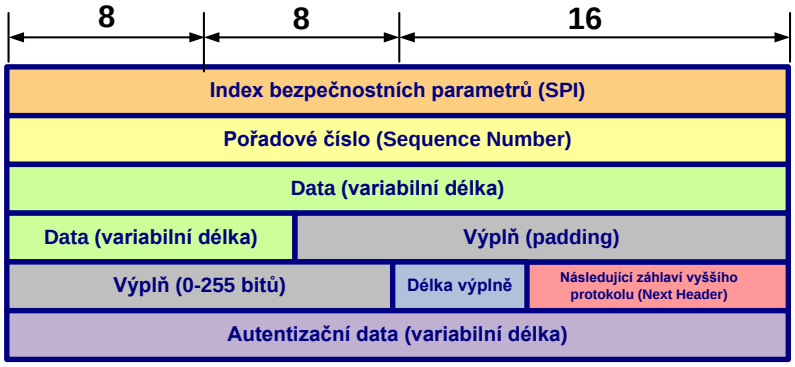
Protokol AH

- ✓ AH – Authentication Header
- ✓ IP protokol číslo 51
- ✓ Zajišťuje autentizaci a integritu dat
- ✓ Užívá se v případě, kdy není nutno data šifrovat



Protokol ESP

- ✓ **ESP** – Encapsulating Security Payload
- ✓ IP protokol číslo 50
- ✓ Zajišťuje utajení zprávy šifrováním datového obsahu i záhlaví, autentizaci a integritu dat
- ✓ Je vhodný v náročnějších případech (ochrana dat před odposlechem a zneužitím)



SPI (Security Parameter Index)

- ✓ Nachází se v záhlaví protokolu AH i ESP
- ✓ Index SPI je ukazatelem do databáze, ve které jsou uvedeny použité šifrovací klíče

SA (Security Association)

- ✓ Tvoří ji SPI, IP adresa příjemce a použitý protokol (AH nebo ESP)

IKE SA (IKE – Internet Key Exchange)

- ✓ používá se pro řízení komunikace, pro dojednání parametrů šifrování a autentizaci protistrany
- ✓ pracuje ve **třech režimech** (a dvou fázích)
- ✓ **hlavní režim** – (fáze 1) obousměrná komunikace mezi iniciátorem a příjemcem, nejprve se dohodnou algoritmy a hashe, pak se pomocí mechanismu Diffie-Hellmann dojedná sdílený klíč, nakonec se ověří identita druhé strany
- ✓ **agresivní režim** – (fáze 1) rychlejší výměna informací za použití méně paketů, nejprve navrhne iniciátor SA (algoritmus, hash a režim), veřejnou hodnotu Diffie-Hellmann a identifikační paket pro ověření totožnosti prostřednictvím třetí strany,

příjemce pošle zpět potřebné informace, iniciátor příjem zprávy potvrdí, rychlejší, méně bezpečný (komunikace před navázáním bezpečného komunikačního kanálu)

- ✓ **rychlý režim** – (fáze 2) slouží k vlastnímu dojednání bezpečnostních asociací po předem vytvořeném zabezpečeném kanále a prostřednictvím IKE

IPsec SA

- ✓ používá se pro dojednání šifrovacích algoritmů (ESP) a způsobu, jakým bude provoz chráněn (ESP i AH)

GRE (Generic Router Encapsulation)

- ✓ Výchozí tunelovací protokol na Cisco komponentech
- ✓ Protokol určený k zapouzdření paketu jednoho protokolu do paketu protokolu druhého
- ✓ Používá se – při přenosu protokolů s omezeným TTL, při propojení nespojitých sítí nebo pro tunelování IPv6 přes IPv4 sítě

SSL (Secure Sockets Layer) VPN

- ✓ Používá se na aplikační vrstvě na zabezpečení webové komunikace přes Internet, (nezabezpečuje veškerou komunikaci, ale pouze některé aplikace)
- ✓ Snaží se dojednat bezpečný přenosový kanál, a pokud se to nepodaří, data se nepřenáší
- ✓ Podporuje obousměrnou autentizaci, ale používá se obvykle pouze jednosměrně
- ✓ Zajišťuje autenticitu odesilatele, integritu a šifrování aplikačních dat při jejich přenosu přes veřejnou IP síť
- ✓ Použití – nejčastěji zabezpečený http (https), dále ftps, telnets, ...
- ✓ Vyžaduje spolehlivý transportní protokol (TCP)

VPN na bázi MPLS

- ✓ **MPLS** (MultiProtocol Label Switching)
- ✓ Vhodné pro propojení podnikových LAN, nehodí se pro vzdálený přístup
- ✓ Značka přidělená každému paketu na okraji sítě (při vstupu do MPLS sítě) obsahuje identifikátor VPN + identifikátor CoS (Class of Service) – zajišťuje pro pakety stejné třídy stejné služby
- ✓ Používá se pro mapování privátní IP sítě na veřejnou IP síť provozovatele

SSH (Secure SHell)

- ✓ metoda vzdáleného přístupu
- ✓ zašifrovaný textově orientovaný protokol, používá se místo protokolu Telnet
- ✓ VPN založená na SSH používá pro navázání síťového rozhraní na místním směrovači protokol PPP
- ✓ směrovací tabulka místního směrovače je nakonfigurovaná tak, aby veškerá data určená VPN nebo vzdálené síti odcházela rozhraním PPP, toto rozhraní používá SSH na zašifrování dat a na spojení s VPN branou