Základy počítačových sítí
Šifrování a bezpečnost

Základy počítačových sítí
Lekce 10
Ing. Jiří ledvina, CSc.

Bezpečnost

- požadavky na bezpečnost se v poslední době výrazně mění
- tradičně byla zajišťována zamezením přístupu (uzamykáním a administrativně)
- se zavedením výpočetní techniky vznikla potřeba vytvářet automatizované prostředky pro ochranu souborů a dalších informací
- použití počítačových sítí a komunikačních linek vyžaduje zajistit ochranu dat během přenosu

Definice

- **počítačová bezpečnost** – všeobecný název pro soubor prostředků, navržených k ochraně dat a maření úsilí hackerů
- **síťová bezpečnost** – opatření k ochraně dat během přenosu
- **bezpečnost Internetu** – opatření k ochraně dat během přenosu přes soubor propojených sítí
  - spočívá v opatření k odrazení, prevenci, detekci a korekci bezpečnostních hrozeb poškozujících přenos informace

Služby

- **bezpečnostní služby** – zvýšení bezpečnosti přenosu a zpracování dat
- **bezpečnostní mechanizmus** – navržen k detekci, prevenci a obnově po bezpečnostním útoku, používá šifrovacích technik
- **bezpečnostní útok** – jakákoliv akce, která naruší bezpečnost informací

Ochrana výpočetních systémů

- **ochrana zdrojů** – ochrana proti neoprávněnému použití prostředků v OS
- **bezpečná komunikace** – vlastní ochrana přenášené informace
- **ověřování uživatelů** – zabezpečení, aby zprávy přicházely od ověřeného zdroje a bez modifikace

Napadení systému

- **pasivní**
  - odposlech
  - analýza přenosu – odkud, kam, kolik, ...
- **aktivní**
  - modifikace, zadržování nebo podstrkávání zpráv
  - modifikace toku dat – změna obsahu, opakování, změna pořadí, rušení, syntéza zpráv, změna adresy, změna dat, atd.
  - Odepření služby

Cíl zabezpečení

- prevence pasivního útoku
- detekce aktivního útoku.

Prostředky pro zajištění bezpečnosti

- Bezpečnost
  - Bezpečnostní služby
    - Zajištění soukromí
    - Ověřování pravosti
    - Zajištění integrity
  - Kryptografické algoritmy
    - Symetrické šifrování (tajný klíč)
    - Asymetrické šifrování (tajný a veřejný klíč)
    - Otisk zprávy

Bezpečnostní mechanizmy

- šifrování
- digitální podpisy
- řízení přístupu
- integrita dat
- ověřování výměny dat
- vyplňování přenosu
- řízené směrování
- ověřování třetí stranou

Bezpečnostní architektura

- **authentication** – ověření pravosti – ujištění, že entita je to, za co se vydává
- **access control** – řízení přístupu – zamezení neautorizovaného využívání zdrojů
- **data confidentiality** – důvěrnost dat – ochrana dat před neautorizovaným přístupem
- **data integrity** – integrita dat – ujištění, že přijatá data byla odeslána ověřenou entitou
- **non-repudiation** – nepopiratelnost – ochrana proti popření jednou z komunikujících entit

Terminologie šifrování

- **otevřený text** (plaintext)
- **šifrovaný text** (ciphertext)
- **šifra** – algoritmus pro transformaci otevřeného textu na šifrovaný
- **klíč** – parametr šifrování
- **šifrování** – převod otevřeného textu na šifrovaný
- **dešifrování** – převod šifrovaného textu na otevřený
- **kryptografie** – studium šifrovacích principů a metod
- **kryptoanalýza** – studium principů a metod pro dešifrování bez znalosti klíče
- **kryptologie** – kryptografie a kryptoanalýza

Základní operace šifrování

- Šifrovací operace
  - Substituce – náhrada znaků za jiné
  - Transpozice – přesun znaků (bitů) na jiné místo v kódu
- Šifra
  - Bloková – šifruje se po blocích pevné délky
  - Proudová – šifruje se po bitech nebo slabikách

Základní šifrovací operace

- Substituce
  - Každé písmeno nebo skupina písmen je nahrazena jiným písmenem nebo skupinou písmen
  - Např. Caesarova šifra – použita Caesarovými vojsky
  - Jednoduše prolomitelné
- Transpozice
  - Přeuspořádání písmen, ale ne překódování
  - Sloupcové šifrování – otevřený text je šifrován po sloupcích různými klíčovými slovy
  - Ne tak jednoduché prolomení jako u substitučních šifer.

Základní šifrovací operace

- Jednorázová hesla
  - Šifrovaný text je vytvářen konverzí otevřeného textu na bitový řetězec a XOR-ován s náhodným bitovým řetězcem. Délka přenášených dat je omezena délkou řetězce (klíče)
  - Neprolomitelná šifra
  - Klíč je obtížné si pamatovat – odesílatel i příjemce musí přenášet i kopii klíče
  - Vyžaduje striktní synchronizaci mezi odesílatelem a příjemcem. Jeden chybějící bit může pomotat cokoliv

Jednoduché šifry

- Monoalfabetické šifry
  - Caesarova šifra (substituční) - posunutí abecedy o 3 pozice v abecedě
  - pouze 26 možností - řešení → útok hrubou silou
  - Vylepšení - náhodné přiřazení (prohození) písmen (klíč 26 písmen dlouhý – 26! = 4×10^{26})

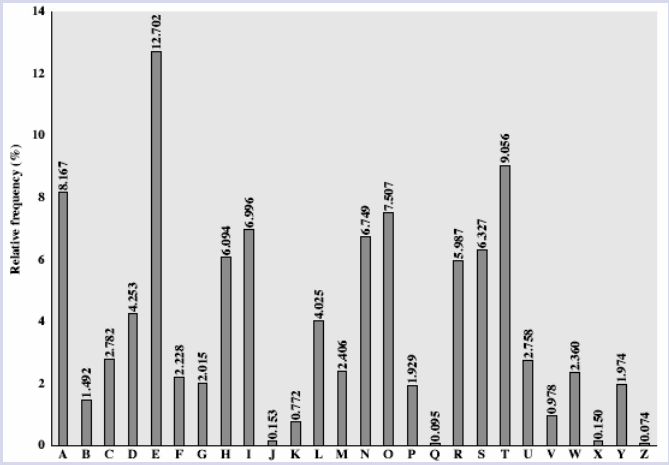
Plain:	`abcdefghijklmnopqrstuvwxyz`
Cipher:	`DKVQFIBJWPESCXHTMYAUOLRGZN`
Plaintext:	`ifwewishtoreplaceletters`
Ciphertext:	`WIRFRWAJUHYFTSDVFSFUUFYA`

Jednoduché šifry

- Polyalfabetické šifry
  - kombinace transpozice a substituce
  - šifrování na dané pozici závisí na klíči, šifrování pozic se opakuje s periodou délka klíče
  - řešením je nalézt délku klíče, a pak jde a o několik monoalfabetických šifer
- Útok hrubou silou
  - Snaha odhalit klíč metodou pokus-omyl
  - Vyzkoušení „všech“ možností – výpočetně složité
  - Nalezení postupu, který by eliminoval počet pokusů

Frekvenční analýza

- Frekvenční analýza výskytu znaků v anglické abecedě
- Frekvenční analýza skupin znaků (a, an, the, …)
- Obrana – odstranění mezer mezi slovy



Zabezpečení

- Předpoklad: Algoritmus je útočníkovi znám, není znám klíč
- Stupeň zabezpečení
  - **absolutní bezpečnost** – bez znalosti klíče nelze odhalit otevřený text
    - jednorázová hesla
    - Heslo (klíč použijeme pouze jednou)
  - **výpočetní bezpečnost** – šifra nemůže být prolomena pro nedostatečnou výpočetní výkonnost
    - Realizace specializovaných počítačů umožňujících prolomit šifru (útok hrubou silou)
    - Obrana (dočasná) prodloužením klíče

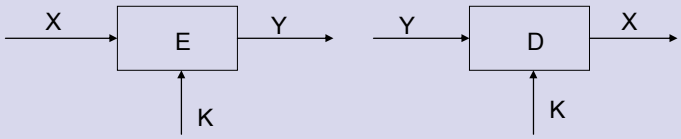
Symetrické šifrování

Požadavky

- silný šifrovací mechanizmus
- šifrovací klíč zná pouze odesílatel a příjemce
- známý šifrovací (a dešifrovací) algoritmus
- Nutnost použití bezpečného kanálu pro distribuci klíče

$Y = E_K(X)$ - šifrování

$X = D_K(Y)$ - dešifrování



Šifrování tajným klíčem

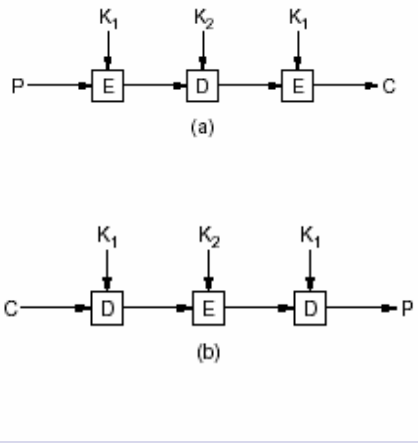
DES – Data Encryption Systém

- Šifrovací algoritmus vyvinut v r. 1970 National Bureau of Standards and Technology a IBM.
- Používá délku klíče 56 bitů a 19 různých stavů
- Každá iterace *i* používá jiný klíč K_i. Složitost závisí na komolící funkci *f*.
- Klíč K_i je odvozován od počátečního 56 bitového klíče.
- Velmi silný, ale prolomitelný

Šifrování tajným klíčem

Triple DES – řeší problém příliš krátkého klíče DES jeho rozšířením na 112 bitů

- Pro šifrování postupně používá algoritmus šifrování klíčem K1, dešifrování klíčem K2 a šifrování klíčem K1.
- Pro dešifrování postupně používá algoritmus dešifrování klíčem K1, šifrování klíčem K2 a dešifrování klíčem K1



Šifrování tajným klíčem

AES/Rijndael (AES – Advanced Encription Standard) – Rijndael.

- vítěz konkurzu o šifrovací standard (2002)
- délka klíče 128, 196 nebo 256 bitů

IDEA – International Data Encription Standard

- Publikován v r. 1990
- Používá klíč délky 128 bitů
- Velmi silné šifrování, nebyly publikovány žádné praktické útoky, útok hrubou silou není praktický
- Pokrytý různými mezinárodními patenty

Skipjack

- Tajný algoritmus vyvinutý NSA
- Je použit v šifrovacím čipu Clipper
- Využívá klíč délky 80 bitů

Asymetrické šifrování

- Symetrická šifra je dostatečně bezpečná
- Neřeší však problém distribuce klíče
- Začátek 70. let – problém s distribucí klíče v bankovnictví (nutná periodická výměna tajných klíčů klientů)
- Snaha o vyřešení problému
  - 1976 – výměna klíčů Diffie-Hellman
    - Vyžaduje kooperaci obou stran (on-line komunikace)
  - 1978 – asymetrické šifrování Rivest, Shamir, Adlemin (RSA)
    - Klíče se dají vygenerovat předem – vhodné i pro off-line komunikaci

Asymetrické šifrování

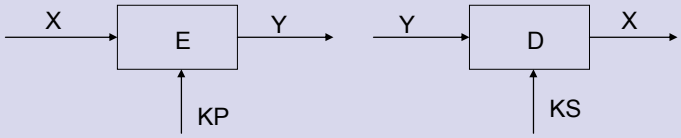
- Řeší problém distribuce klíče
- Používá dvojici (závislých) klíčů
  - Jeden je označován jako veřejný
  - Druhý jako tajný
- Šifrování
  - Šifrování veřejným klíčem
  - Dešifrování tajným klíčem
- Ověření pravosti (i nepopiratelnost)
  - Zabezpečení tajným klíčem
  - Ověřování veřejným klíčem

Asymetrické šifrování

- Princip
  - Existují dva klíče
  - P – public (veřejný)
  - S – secret (tajný)

    $Y = E_{KP}(X)$ - šifrování

    $X = D_{KS}(Y)$ - dešifrování



Algoritmus RSA

- vytvořeno pány Rivest, Shamir a Adlemin v r. 1978
  - Velmi silná šifra
  - Podporuje proměnnou délku klíčů
  - Délka klíče 1024 bitů, 2048 bitů
  - Delší klíče zajišťují větší bezpečnost
- Algoritmus založen na počítání s velkými prvočísly
  - p, q … velká prvočísla N = p.q
  - P.S = 1 [mod ϕ(N)] ϕ(N) = nsn(p-1, q-1)
- šifrování $C = M^P \pmod N$
- dešifrování $M = C^S \pmod N$
  - P … public key, S … secret key
  - předává se P, N a utají S
  - výpočet P, S, N musí být jednoduchý

Asymetrické šifrování

- Další algoritmy
  - Elgamal (Taher Gamal)
  - DSA (Digital Signature Algorithm)

Použití asymetrického šifrování

- **šifrování zpráv**
  - časově náročné, není vhodné
- **šifrování relačního klíče**
  - asymetrické šifrování se použije pro šifrování relačního (tajného) klíče
  - relační klíč se použije k šifrování (symetrické) vlastní zprávy,
- **ověření integrity dat**
  - ke zprávě se pomocí hashovací funkce vygeneruje otisk, který se zašifruje tajným klíčem odesílatele
  - je schopen provézt pouze majitel tajného klíče
  - ověření pravosti veřejným klíčem
- **Nepopiratelnost**
  - informace zašifrovaná tajným klíčem
  - Ověření veřejným klíčem

Hashovací funkce

- Jednosměrná funkce
  - Jednoduchý výpočet h = f(m)
  - Výpočetně složité nebo nemožné $m = f^{-1}(h)$
  - Platí pokud $h1 \neq h2 \Rightarrow m1 \neq m2$
    pokud $m1=m2 \Rightarrow h1 = h2$
    ale existuje $m1 \neq m2$ a $h1 = h2$
- Algoritmy
  - SHA (Secure Hash Algorithm)
  - MD5 (Message Digest)

Ověřování

- Autentikace je technika, pomocí které se ověřuje, že komunikující partner je ten, za kterého se vydává a ne podvodník.
- Existují tři způsoby autentikace
  - Řekni něco co víš (heslo)
  - Ukaž něco co máš (identifikační karta)
  - Nech systému něco tvého změřit (otisk prstu)

Ověřování

- **Ověřovací schémata**
  - musí obsahovat aspoň jedno tajemství
  - musí být schopna rozpoznat jeho správné použití
- **Ověřovací metody**
  - jednoduché (založeny na heslech)
  - přísné (založeny na šifrovacích metodách)
- **Jednoduché ověřování**
  - identifikace jménem a heslem,
  - přenos otevřeného textu, použití ověřovacího serveru

Ověřování

- **Přísné metody**
  - elementární metody – použití symetrických a nesymetrických kódů
  - metody založené na ověřovacích serverech
  - metody založené na protokolech s minimální znalostí
    - uživatel dokazuje svoji identitu odpovídáním na šifrované otázky serveru

M1: {R, ID}
M2: $\{C\}_K$
M3: $\{f(C)\}_K$

R … požadavek,
K … tajný klíč,
C … náhodné číslo,
f(C) … domluvená funkce

Ověřovací servery

- slouží k ověření „pravosti“ uživatele
- Používá symetrické šifrování
- lepší utajení klíčů
- používá se KDC (Key Distribution Center) – databáze klíčů (je tajná a indexována podle jmen uživatelů)
- Příklad – ověřování pomocí Kerberos serveru

Distribuce veřejného klíče

- Veřejný klíč je možné šířit v otevřené podobě
- Existuje nebezpečí podvržení veřejného klíče
  - Útok typu Man in the Middle
- Problém bezpečné distribuce veřejného klíče řeší certifikáty
- Problém vydávání, ověřování a zneplatnění certifikátu řeší certifikační autority

Certifikát

- Certifikát je blok dat (soubor), obsahující
  - Verze (V3)
  - Sériové číslo (02 1c 6a)
  - Algoritmus podpisu (md5RSA)
  - Vystavitel (CN = CA GE Capital Bank, OU = Direct Banking, O = GE Capital Bank, a.s., C = CZ)
  - Platnost od (28. dubna 2003 12:31:30)
  - Platnost do (27. dubna 2005 12:31:30)
  - Předmět (E = ledvina@kiv.zcu.cz, CN = uid: 120295, CN = Ing. Jiri Ledvina, ... adresa)
  - Veřejný klíč (30 81 87 02 81 81 00 bf 4a ...)

Certifikát

- Pokračování
  - Distribuční místo (URL=http://www.gecb.cz/ca_ge.crl)
  - Použití klíče (Digitální podpis, Zakódování klíče)
  - Algoritmus miniatury (sha1)
  - Miniatura (72 19 13 5c 6a 9b 4e ab 30 cf 6b 6f 49 df 15 c0 62 94 79 09)
  - Popisný název (Ing. Jiri Ledvina)
- Certifikát musí být nezpochybnitelný – zneplatnění certifikátu
- Existují různé formáty certifikátů
  - Personal Information Exchange (PEX), PKCS #12 (P12) (Public Key Cryptography Standard)
  - Cryptographic Message Syntax Standard PKCS#7 (P7B)
- PGP certifikáty

Ověřování certifikátů

- přímé ověřování (nejjednodušší model)
  - Ověřování certifikátů mezi důvěryhodnými subjekty
  - V prohlížečích jsou certifikáty uznávaných autorit instalovány – můžeme (musíme) jim věřit. Existují ale i další certifikační autority, které nejsou uznávané – prohlížeč se na důvěryhodnost ptá.
- hierarchické ověřování – zřetězení certifikátů
  - Certifikačních autorit je hodně – získání certifikátu může být otázkou osobní návštěvy (důvěryhodné získání certifikátu).
  - Certifikační autority mohou vytvářet hierarchický strom – důvěryhodnost CA nižší úrovně je potvrzována CA vyšší úrovně. CA nejvyšší úrovně potvrzuje důvěryhodnost sebe sama.
  - Zřetězení CA je součástí certifikátu.
- kumulativní model – zahrnuje předchozí (přímé, zřetězené)

Protokoly pro bezpečnou komunikaci

Kerberos – ověřování v systému Orion na ZČU

- Používá symetrické šifrování
- Vychází z centralizované databáze uživatelů (každý uživatel musí být registrován)
- Základní část je ověřovací server (Kerberos)
- Po přihlášení (ověření) dostane uživatel lístek, obsahující práva přístupu k požadovanému serveru.
- K dalšímu ověřování uživatele se používaní pověřovací listiny (credentials), obsahující jméno uživatele a adresu jeho počítače.

Steganography

Steganography

(a) Three zebras and a tree. (b) Three zebras, a tree, and the complete text of five plays by William Shakespeare.

Protokoly pro bezpečnou komunikaci

SSL – Secure Socket Layer

- Vyvinuto fy. Netscape, používá se zejména pro bezpečné přenosy mezi prohlížečem a webovým serverem.
- K ověřování serveru se používají certifikáty serveru. Uživatel není ověřován.
- Po ověření se veřejný klíč použije pro vygenerování relačního klíče, sloužícího k šifrování komunikace.
- Schéma bezpečného HTTP se označuje HTTPS
- SSL se používá i u dalších protokolů (POP, IMAP)
- Je možné je využít univerzálně – vytváří mezivrstvu mezi protokolem TCP a aplikací – před použitím je třeba aplikaci (program) modifikovat.
- Obdobou SSL je TLS (Transport Level Security)

Protokoly pro bezpečnou komunikaci

SSH – Secure Shell

- Používá se pro vytvoření šifrovaného kanálu mezi aplikacemi (aplikační úroveň).
- Pro šifrování používá opět relační klíč, vytvořený na základě výměny informací (Diffie - Hellman algoritmus pro výměnu klíčů) nebo na základě asymetrické kryptografie – RSA.
- Využívá se pro
- bezpečný vzdálený přístup – náhrada Telnetu (ssh – secure shell),
- bezpečný přenos souborů – náhrada ftp (scp – secure copy),
- vytvoření bezpečného kanálu mezi libovolnými aplikacemi.

Protokoly pro bezpečnou komunikaci

IPsec

- Soubor protokolů pro zajištění bezpečnosti na síťové úrovni
  - Ověřování původu
  - Integrita dat
  - Utajení dat
- Vzhledem k transportním protokolům a aplikacím je transparentní – nevidí ho
- Vzhledem k linkovému protokolu neprůhledný – nerozumí přenášeným datům
- Přizpůsobivý

Režimy činnosti

- Transparentní – mezi koncovými uživateli
- Tunelovaní – mezi dvěma síťovými prvky (směrovači, obrannými valy, …)
- Kombinace předcích – mezi koncovým uživatelem a síťovým prvkem

Zabezpečení elektronické pošty

PEM (Privacy Enhancement for Internet Electronic Mail)

- Dnes historický protokol pro vytváření a zpracování bezpečných zpráv.
- Vznikl v druhé polovině 80. let.
- Původní specifikace RFC989, poslední specifikace RFC1421 až RFC1424 (1993).
- V praxi nedošlo k jeho masovému využití nejširší veřejností - nebyl totiž běžně dostupný software, který by jej podporoval.
- Na přelomu 80. a 90. let nebyla ještě masová poptávka po software tohoto druhu.
- Stal základem pro novější protokoly (S/MIME)

Zabezpečení elektronické pošty

S/MIME

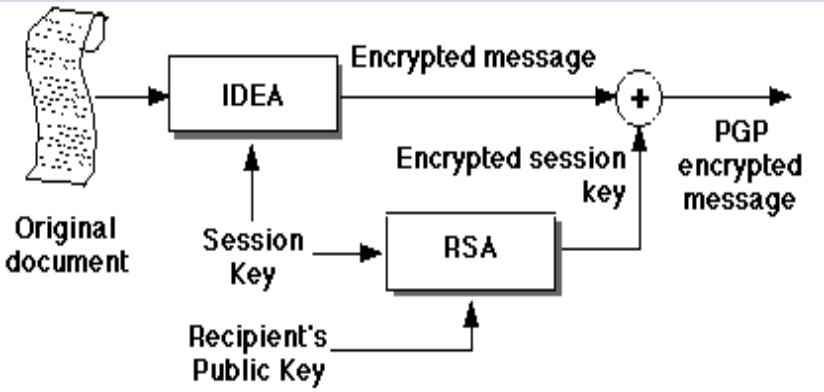
- Podobné PEM
- Kontrolní součet (otisk) SHA-1 a MD5
- Asymetrické šifrování (šifrování symetrických šifrovacích klíčů a elektronický podpis): RSA s délkou klíče minimálně 512 bitů.
- Symetrické šifrování - šifrování textu zprávy (DES-CBC, triple DES).
- Norma PKCS-7 pro tvorbu bezpečných zpráv - elektronický podpis, šifrování, obojí.
- Definuje MIME hlavičku Content Type: Application/pkcs7-mime

Zabezpečení elektronické pošty

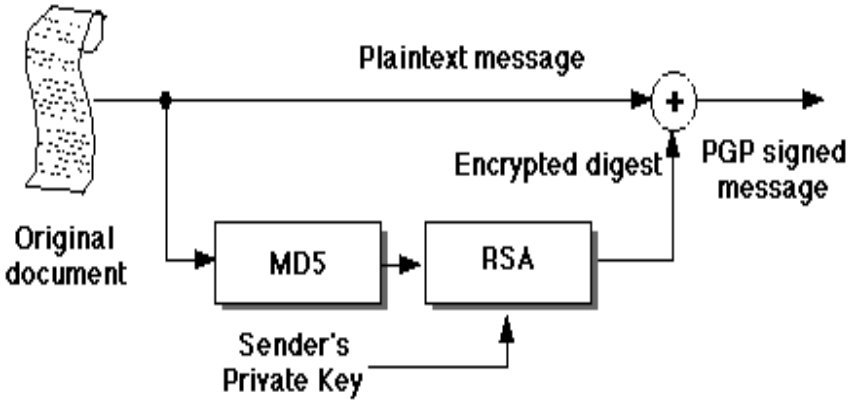
PGP (Pretty Good Privacy)

- Uživatelsky jednoduchý program dostupný nejširší veřejnosti.
- PGP je nejrozšířenější prostředek pro zpracování bezpečných zpráv (RFC1991).
- Vytvořil Američan P.R.Zimmerman (1991).
- Bezpečný přenos zpráv pomocí SMTP, POP, IMAP (nepotřebuje nový protokol, nadstavba nad stávajícími).
- Asymetrické šifrování - RSA (šifrování symetrického relačního klíče pro šifrování vlastní zprávy).
- Symetrické šifrování algoritmus - IDEA.
- Komprese dat před šifrováním - PKZIP.
- Výpočet kontrolního součtu (otisku) - MD5.
- Převod binárních dat na ASCII - Radix-64.

Zabezpečení elektronické pošty



Zabezpečení elektronické pošty



Obranné valy

- Provádí ochranu sítě před napadením (ochrana počítačů nestačí)
- Odděluje uživatele (prvek nespolehlivosti) od prvků ochrany

Vlastnosti

- Filtrování paketů a vlastnost odstínění
- Různé úrovně ověřování
- Přihlašování (registrace) a účtování
- Transparentnost a přizpůsobení uživatelům
- Ovladatelnost (management)
- Rozlišení požadavků dle klientů nebo sítí

Typy obranných valů

- **Filtrující směrovač (Screening Router)**
  - Provádí filtraci paketů podle směru přenosu, IP adresy a čísla portu
- **Opevněný počítač (Bastion Host)**
  - Používá se při realizaci důležitých serverů, které mají být navíc velmi bezpečné. Např. SMTP, FTP, DNS, HTTP, atd.
- **Brána se dvěma vstupy (Dual Homed Gateway)**
  - Úplně odděluje vnitřní a vnější síť. Služby musí být umístěny na této bráně, přístupné jak z vnitřní sítě, tak i z vnější sítě.
- **Screened Host Gateway**
  - Vnitřní síť je chráněna filtrujícím směrovačem, který propouští pouze pakety určené pro vybraný počítač (Bastion Host).
- **Screened Subnet**
  - Pomocí dvou filtrujících směrovačů se vytvoří demilitarizovaná zóna.
- **Brána aplikační úrovně**

Útoky

Útoky Denial of Service

- Jeden z mnoha základních forem útoků na vnitřní sítě
  - Založen na přetížení systému
  - Výsledkem je omezení výkonnosti serveru nebo úplný výpadek cílového systému
- Útok může být zaměřen na síťové komponenty nebo na hostitelské systémy
- Dochází k vytěsňování reálných přenosů
  - Klienti na základě detekce zahlcení zpomalují vysílání
  - Směrovače musí přebytečné pakety odstraňovat

Útoky

Usnadnění DoS útoků

- V počítačové síti běží mnoho systémů
- Počítačová síť je velmi rozlehlá
- Mnozí uživatelé jsou naivní – dávají šanci uchvátit vzdálený systém
- Protokoly internetu jsou známé, to vytváří podmínky pro využití jejich slabin
- Mnoho volného software, ve kterém mohou být zahrnuty utajené funkce
- Nedostatečná ochranná politika používání a managementu
- Velmi rozsáhlý software s mnoha známými děrami
- Nedostatek prostředků pro zastavení útoků

Útoky

Snort (Open Source Intrusion Detection System)

- Systém pro detekci útoků (Intrusion Detection Systém)
- Je schopen provádět analýzu toku dat v reálném čase a logování paketů v IP sítích
- Může provádět analýzu protokolů, vyhledávání údajů
- Je schopen detekovat různé útoky a sondování
- Používá jazyk pro popis toku dat
- Obsahuje automat pro detekci podle tohoto popisu
- Umožňuje informovat o útoku v reálném čase (syslog, soubor, sockety, …)