12 - Zabezpečení komunikace, ACL

Symetrická kryptografie

- také nazývána konvenční
- k šifrování/dešifrování používá jediný klíč
- mají nízkou výpočetní náročnost
- nevýhodou je nutnost sílení tajného klíče

Dělení:

- proudové
  - zpracovávají otevřený text po jednotlivých bitech
- blokové
  - rozdělí otevřený text na bloky stejné velikosti

Použití

- typicky společně s asymetrickými

1. text se zašifruje symetrickou šifrou s náhodným klíčem
2. symetrický klíč se zašifruje veřejným klíčem asymetrické šifry

Asymetrická kryptografie

- také nazývána kryptografie s veřejným klíčem
- pro šifrování a dešifrování se používají odlišné klíče
- používá se pro utajení komunikace a pro případy, kde je nutno prokázat autora dat
- založeny na principu "jednocestných funkcí"
  - ze vstupu lze snadno spočítat výstup
  - z výstupu je ovšem složité spočítat vstup

Princip

- jedna část klíče se používá pro šifrování zprávy (příjemce ho nezná)
- druhá část klíče se používá pro dešifrování zprávy (odesílatel ho nezná)
  - příjemce a odesílatel šifry spolu nemusí nic sdílet
- běžně se využívá **soukromý** a **veřejný** klíč
- **veřejný** klíč se používá na šifrování zprávy, je přístupný a kdokoliv může šifrovat
- **soukromý** klíč se používá na dešifrování zprávy a zná ho většinou pouze majitel
- podmínka je, aby ze znalosti šifrovacího klíče nebylo možné spočítat dešifrovací

Hashování

- převádí určitá data do malého čísla
- hash na rozdíl od šifry nejde rozluštit zpětně
- malou změnou dat na vstupu dostaneme velmi odlišný výstup
- jakkoliv dlouhý vstup vždy vrací stejně dlouhý výstup
- každý hash je unikátní právě pro jeden vstup

Použití

- **hashovací tabulka**
  - používá hash na transformaci klíče na index, podle kterého se k datům přistupuje
  - umožňuje např. rychlejší vyhledávání v databázi
- **ochrana hesel**

    - aby hesla uložená v databázi nezůstávaly ve svém původním formátu, hashují se
    - při porovnávání s heslem, co zadal uživatel se poté jeho vstup zashashuje stejným algoritmem a porovná se výstup
    - kdyby došlo k útoku na DB, útočník bude mít pouze hashe hesel
- **kryptografie**
    - kontrola odesílaných zpráv přes síť
    - data se zahashují a odešlou se společně s normálními daty
    - příjemce poté sám zahashuje data, co mu přišla a porovná se zahashovaným výsledkem, co byl k datům připojen

Ceritifkáty

- **certifikát** = elektronicky podepsaný veřejně šifrovací klíč

Certifikační autorita

- subjekt, využívající digitální certifikáty
    - usnadňuje využívání PKI pomocí potvrzování pravdivosti údajů
    - Public Key Infrastructure
- **můžeme důvěřovat certifikátu za předpokladu, že důvěřujeme dané certifikační autoritě**

Průběh

- majitel veřejného klíče musí přesvědčit autoritu, že data odpovídají skutečnosti
- po ověření údajů certifikační autorita vydá **digitální certifikát**
    - jeho součástí je **elektronický podpis**
    - díky němu lze ověřit autentičnost

Využití

- komunikace elektronickou cestou se státní správou
- ověřování elektronických podpisů
- zajištění neodmítnutelnosti odpovědnosti

Digitální certifikát

- vydává ho certifikační autorita
- formát **X.509**
    - obsahuje informace o majiteli veřejného klíče a vydavateli certifikátu
- používány pro identifikaci protistrany při vytváření zabezpečeného spojení
    - HTTPS, VPN
- je možné nedůveřovat neznámým certifikátům

Elektronický podpis

- nahrazují vlastnoruční podpis v informatice
- vytvořen pro konkrétní data
- lze ověřit, zda je platný
- jeho součástí je identifikace, kdo ho vytvořil
- **elektronický podpis = aplikace asymetrické kryptografie**
    - otisk dokumentu je zahashován a poté zašifrován autorovým privátním klíčem

VPN

- Virtual Private Network
- prostředek pro propojení počítečů pomocí nedůvěryhodné sítě
- spojení počítaču tak, aby spolu mohli komunikovat, jako by byly v jedné privátní síti
- spojení se ověřuje pomocí certifikátů
- veškerá komunikace je šifrovaná

Využití

- připojení do firmy z domova
- oklamání systému, že se vaše IP adresa nachází v jiné zemi

SSL

- Secure Socket Layer
- protokol mezi L4 (transportní) a L7 (aplikační)
- poskytuje zabezpečení komunikace šifrováním a autentizací komunikujících stran

Využití

- pro bezpečnou komunikaci s webovými servery pomocí HTTPS
  - on-line obchody (platby)
  - portály s administrací (zadávání hesla)

Princip

- asymetrická šifra
- každá strana má 2 klíče - veřejný a soukromý

1. klient a server si vymění data o komunikaci
2. klient si ověří certifikát a autentičnost serveru
3. podle veřejného klíče z certifikátu si klient vygeneruje základ šifrovacího klíče
4. klient pošle šifru na server, server svým soukromým klíčem rozšifruje základ
5. server vygeneruje hlavní šifrovací klíč
6. navzájem si potvrdí, že bude komunikace probíhat tímto způsobem (šifrovaná tímto klíčem)
7. komunikace je nyní šifrovaná

ACL

- Access Control List
- seznam pravidel, které řídí přístup k nějakému objektu

Standartní ACL

- identifikuje se dle čísel 1-99 (rozšířeně 1300-1699)
- jednoduchá konfigurace
- filtruje podle zdrojové adresy
  - pouze to, co do cíle vstupuje

Rozšířené ACL

- identifikuje se dle čísel 100-199 (rozšířeně 2000-2699)
- kontroluje adresy jak cíle, tak zdroje
- omezuje i to, co z cíle odchází
- kontroluje mnoho položek z L3 a L4

Jmenné ACL

- může se použít pro obě předchozí jako nadstavba
- umožňuje uprovovat / mazat jednotlivé ACL záznamy
- výhodou je, že si jména lze pamatovat lépe, než čísla
- počet pojmenovaných záznamu je téměř neomezený