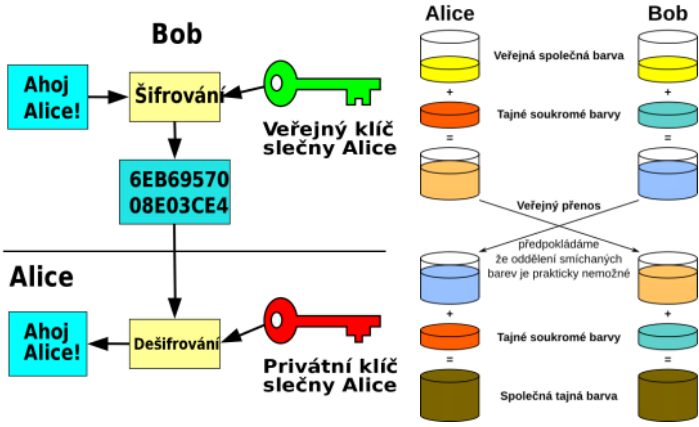
10 Zabezpečení komunikace, ACL

Wednesday, 19 January 2022 09:10

Kryptografie symetrická a asymetrická, hashování, certifikáty a certifikační autorita, elektronický podpis, VPN, příklad implementace (SSL)
ACL standardní a rozšířený, jmenný ACL, zabezpečení přístupu k managování switche a routeru, Vytvoření ACL a nasazení ACL na porty směrovače (filtrace provozu dovnitř a ven – porovnání)



- kryptografie
  - šifrování dat
  a. symetrická (konvenční)
    - k šifrování a dešifrování stejný tajný klíč
    - obě strany musí mít přístup ke klíči
    - používají se společně s asymetrickými
      - text se zašifruje symetricky a symetrický klíč veřejným klíčem asymetricky
  b. asymetrická (s veřejným klíčem)
    - pro šifrování/dešifrování dva klíče (veřejný a soukromý)
    - využití jednocestných funkcí
      - z výstupu lze vstup spočítat velmi těžko
    - nejčastější implementace je Diffieho-Hellmanova výměna klíčů
    i. veřejný klíč
      - k šifrování
      - veřejný od majitele
        - všichni můžou jemu určené zprávy šifrovat
    ii. soukromý klíč
      - k dešifrování
      - známý pouze pro majitele
      - nesmí být spočítatelný z veřejného klíče
- hashování
  - převod dat na malé číslo (vždy stejně velké)
  - na rozdíl od šifry nelze zpětně dopočítat
  - malou změnou dat dostaneme značně odlišný výstup
  - hash unikátní právě pro jeden vstup
  - použití:
    - hashovací tabulka
      - ID jsou zahashovaná data
    - ochrana hesel
      - hashování hesel v databázi
      - při přihlašování se hash vstupu porovnává s hashem v databázi
    - kryptografie
- elektronický podpis
  - obrácené asymetrické šifrování
  - zašifrování pomocí soukromého klíče a dešifrování pomocí veřejného
  - pokud je dešifrování úspěšné, tak podpis zašifroval majitel soukromého klíče
  - šifruje se pouze hash
- digitální certifikát
  - elektronicky podepsaný veřejný klíč
  - lze důvěřovat certifikátu, pokud důvěřujeme certifikační autoritě
  - vydán certifikační autoritou
    - důvěryhodná třetí strana
    - formát X.509
  - součástí je i elektronický podpis pro ověření autentičnosti
  - použití k identifikaci protistrany při vytváření zabezpečeného spojení (HTTPS, VPN)
- VPN (*Virtual Private Network*)
  - šifrované propojení počítačů jako by byly v jedné privátní síti
  - spojení ověřeno pomocí certifikátů
  - slouží např. ke vzdálenému přístupu do lokální sítě firmy nebo k "virtuální" změně země
  - M:N (síť)
- SSL (*Secure Sockets Layer*)
  - protokol mezi transportní L4 a aplikační L7
  - zabezpečení komunikace šifrováním a autentizací
  - nástupcem je TLS (*Transport Layer Security*)
  - 1:1 (prohlížeč-web, mailserver-mailserver)
- ACL (*Access Control List*)
  - seznam pravidel řídící přístup k objektu
  - firewall
    - sloužící pouze pro provoz ACL
  - definice čísly
  a. standardní (1-99, 1300-1699)
    - filtrace SIP
  b. rozšířené (100-199, 2000-2699)
    - SIP + DIP (+ čísla portů)
  c. jmenné
    - definice standardní/rozšířené ACL
    - místo čísel definice jmény
    - permit / deny