Počítačové siete
Bezpečnosť

Bezpečnostné problémy v sieťach

- dôvernosť
- integrita a autentickosť
- dostupnosť
- autentifikácia
  - používateľov
  - systémov
- riadenie prístupu

Bezpečnostné mechanizmy

- fyzická ochrana prístupu
- riadenie prístupu, oddelenie komunikácie
- kryptografia
  - šifrovanie
    - symetrické (DES, 3DES, AES, ...)
    - asymetrické (PKI) (RSA, ...)
  - digitálny podpis (RSA, ECDSS, ...)
  - hašovacie funkcie s kľúčom (HMAC-SHA256, ...)
- organizačné opatrenia

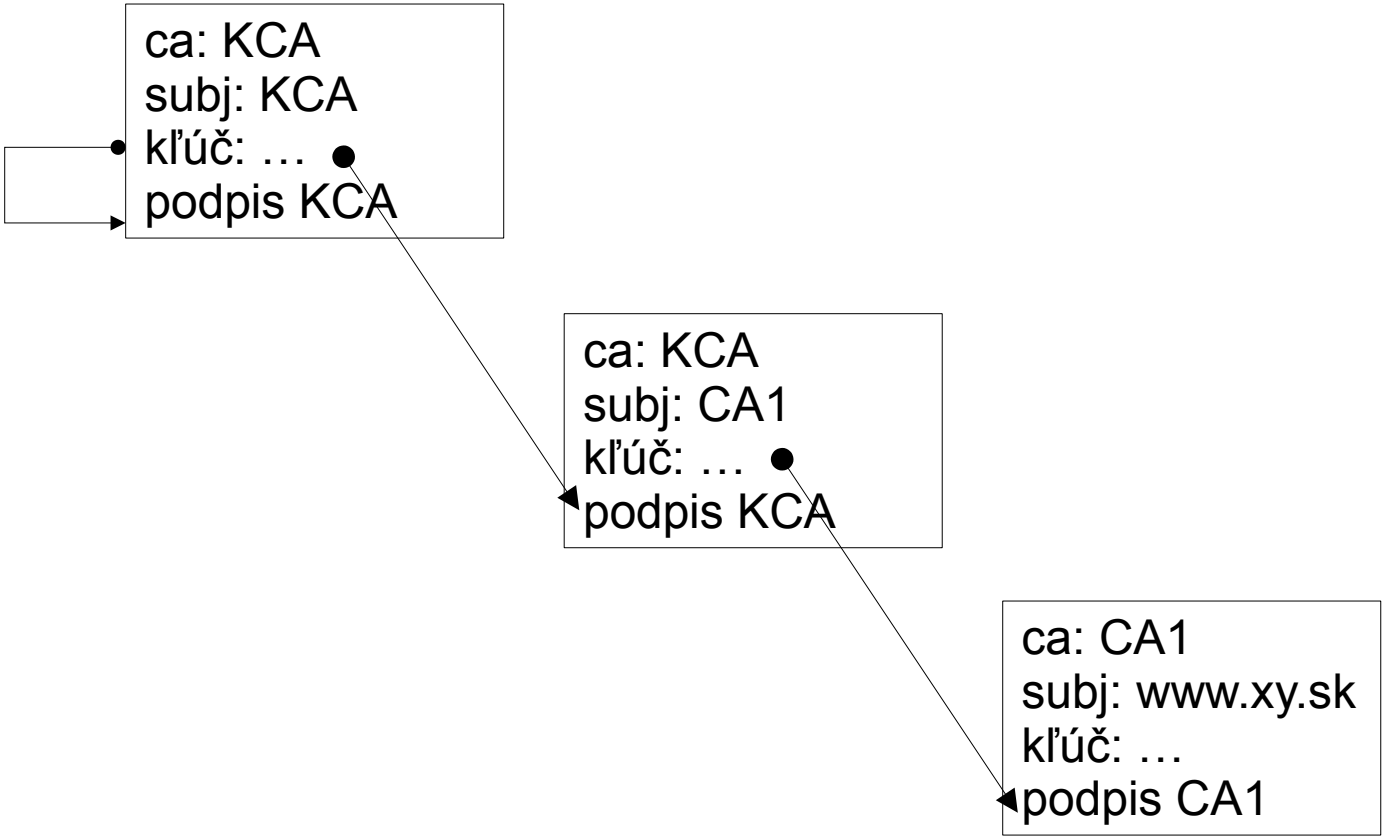
Problém distribúcie kľúčov

- symetrická kryptografia
  - potreba zdieľaného tajného kľúča
  - algoritmy (napr. Diffie-Hellman) na výpočet zdieľaného tajného kľúča
    - potreba vzájomnej autentifikácie na vylúčenie Man-In-the-Middle útoku
  - generovanie kľúča jednou stranou a bezpečný prenos druhej strane
- asymetrická kryptografia
  - distribúcia verejných kľúčov
  - certifikáty

Certifkát

- sériové číslo
- vydavateľ (certifikačná autorita)
- subjekt (server / používateľ)
- dátum a čas platnosti (od – do)
- verejný kľúč subjektu
- algoritmus, pre ktorý je kľúč určený
- ďalšie atribúty (účel, politika, alternatívne ID subjektu, ...)
- podpis CA

Reťaz certifikátov



Bezpečnosť na fyzickej vrstve

- fyzická ochrana káblov a sieťových komponentov
- separácia sietí na fyzickej vrstve
- často nefunguje proti vnútornému nepriateľovi
  - keď sa viem dostať k počítaču, viem sa dostať ku káblu
  - použiteľné v kombinácii s organizačnými opatreniami

Bezpečnosť na linkovej vrstve

- nekryptografická
  - VLAN (virtual LAN)
    - separácia sietí na linkovej vrstve
  - riadenie prístupu k portu
    - na báze linkovej adresy
    - IEEE 802.1X
- kryptografická
  - šifrovanie, kontrola autentickosti, autentifikácia
  - známe vo WiFi svete
    - WEP, WPA, WPA2

VLAN (IEEE 802.1Q)

- rozdelenie Ethernetu na logické (virtuálne) siete
- VLAN ID (VID) – 12 bitov (1 – 4094)
- príslušnosť rámca k VLAN
  - tagged frame – podľa údaja v hlavičke
  - untagged frame – podľa portu (PVID)
- switch
  - pre každý port: Port VID (PVID), množina VID
  - pošle rámec len na porty danej VLAN (Egress filtering)
  - **môže** filtrovať rámce z VLAN, do ktorej zdrojový port nepatrí (Ingress filtering)

Porovnanie Ethernet rámcov

- cieľová adresa (6B)
- zdrojová adresa (6B)
- typ (protokol sieťovej vrstvy) (2B)
  - 0x0800 = IPv4
  - 0x86DD = IPv6
  - 0x0806 = ARP
- dáta
- FCS

- cieľová adresa (6B)
- zdrojová adresa (6B)
- 0x8100
- VLAN tag (2B)
- typ (protokol sieťovej vrstvy) (2B)
- dáta
- FCS

Bezpečnosť na sieťovej vrstve

- firewall
  - filtrácia komunikácie – riadenie prístupu
  - stateless vs. statefull, NAT
  - deny vs. allow by default
- VPN
  - šifrovanie, kontrola autentickosti, riadenie prístupu
  - IPSec (AH, ESP)
  - OpenVPN (IP/L2 over UDP/TCP)
  - ...

Princíp VPN

- IPSec transportný mód
  - medzi hlavičku 3. a 4. vrstvy sa vloží hlavička AH/ESP
    - AH – ochrana integrity údajov sieťovej, transportnej a aplikačnej vrstvy
    - ESP – ochrana integrity a/alebo dôvernosti údajov transportnej a aplikačnej vrstvy
      - obsah paketu od hlavičky 4. vrstvy sa môže šifrovať
- tunelový mód (IPSec, OpenVPN)
  - celý IP paket (príp. celý rámec 2. vrstvy) sa (po zašifrovaní) pošle v novom pakete

Bezpečnosť na transportnej vrstve

- SSL (Secure Socket Layer), TLS (Transport Layer Security)
  - medzi transportnou a aplikačnou vrstvou
  - zabezpečuje autentifikáciu servera a (voliteľne) klienta
    - X.509 certifikáty
  - zabezpečuje vzájomné dohodnutie kľúča
  - šifrovanie, kontrola integrity a autentickosti prenášaných dát
  - treba zabezpečiť bezpečnú distribúciu cert. CA

Bezpečnosť na aplikačnej vrstve

- end-to-end security
- e-mail
  - PGP, S/MIME
- vzdialené prihlasovanie
  - ssh
- autentifikácia používateľov v aplikáciach
  - heslá, jednorazové heslá, SMS-kódy, ...

Bezpečnosť elektronickej pošty

- správa elektronickej pošty = pohľadnica písaná na stroji
  - môže čítať každý, kto ju cestou vidí
  - nemožno dôverovať informácii o odosielateľovi
  - nemožno dôverovať obsahu
- riešenie
  - dôvernosť – šifrovanie
  - integrita a autentickosť – elektronický podpis

Bezpečnosť elektronickej pošty

- PGP (Pretty Good Privacy)
  - treba zabezpečiť bezpečnú distribúciu verejných kľúčov
  - vzájomná dôvera používateľov a podpisovanie kľúčov
- S/MIME (Secure Multipurpose Internet Mail Extensions)
  - použitie X.509 certifikátov
  - treba zabezpečiť bezpečnú distribúciu cert. CA

Bezpečnosť elektronickej pošty

- komunikácia so serverom
  - SMTP – odosielanie pošty
  - POP3, IMAP – čítanie pošty
  - nechránia komunikáciu
    - heslá sú ľahko odhaliteľné
- riešenie
  - SSL, TLS
    - SMTPS, POP3S, IMAPS

Bezpečnosť webu

- protokol HTTP
  - nezabezpečuje ochranu komunikácie
  - ktokoľvek môže vidieť to, čo vidím ja
  - ktokoľvek môže vidieť, čo odosielam
    - heslá, osobné údaje
  - ktokoľvek môže zmeniť to, čo vidím
  - ktokoľvek môže zmeniť to, čo odosielam

Bezpečnosť webu

- riešenie
  - SSL, TLS – HTTPS
- problémy
  - bezpečná distribúcia certifikátu CA
  - kontrola mena servera v certifikáte
  - SSLv2, SSLv3, TLSv1.0, TLSv1.1 (zakázať)
    - majú známe zraniteľnosti, slabé šifry, …
  - TLSv1.2, TLSv1.3 (odporúčané)
  - ignorovanie upozornení browsera

Bezpečnosť vzdialeného prihlasovania

- telnet
  - žiadna ochrana
- ssh
  - šifrovanie, kontrola integrity, autentifikácia servera
  - umožňuje tunelovať ďalšie spojenia
    - napr. X11, VNC, SMTP, POP3, IMAP
  - treba zabezpečiť bezpečnú distribúciu verejných kľúčov serverov
  - neveriť slepo verejnému kľúču servera
  - openssh (UNIX, Linux, Cygwin), PuTTY (Windows)

Bezpečnosť ftp

- protokol FTP
  - nezabezpečuje žiadnu ochranu
    - heslá, prenášané dáta
  - má problémy so stateless firewallmi
  - statefull firewally musia podporovať ftp
- scp, sftp
  - náhrady využívajúce ssh
  - openssh, PuTTY, WinSCP (Windows)