Tento materiál je určený ako podporný študijný materiál na prípravu na skúšku z predmetu Úvod do informačnej bezpečnosti pre študentov Fakulty matematiky, fyziky a informatiky Univerzity Komenského v Bratislave. Na tento účel si študent môže vytvoriť elektronickú aj tlačenú kópiu tohto materiálu.

Bezpečnosť sietí

RNDr. Jaroslav Janáček
KI FMFI UK

Obsah

- vrstvové modely sietí
- bezpečnostné problémy v sieťach
- bezpečnostné mechanizmy v sieťach
- riešenie bezpečnosti na jednotlivých vrstvách
- bezpečnosť v praxi
  - bezpečnosť elektronickej pošty
  - bezpečnosť webu
  - bezpečnosť ftp
  - bezpečnosť vzdialeného prihlasovania

Referenčný model OSI

- (7) aplikačná (application) vrstva
- (6) prezentačná (presentation) vrstva
- (5) session vrstva
- (4) transportná (transport) vrstva
- (3) sieťová (network) vrstva
- (2) linková (data-link) vrstva
- (1) fyzická (physical) vrstva

TCP/IP

- (7) aplikačná vrstva
  - HTTP, FTP, telnet, SMTP, POP3, IMAP, ...
- (4) transportná vrstva
  - TCP, UDP
- (3) internet vrstva
  - IP
- (1+2) host-to-network vrstva
  - Ethernet, IEEE 802.11 (WiFi), PPP, ...

Sieťové komponenty

- fyzická vrstva
  - káble, hub, repeater
- linková vrstva
  - switch, bridge
- sieťová vrstva
  - router, firewall
- transportná vrstva
  - firewall
- aplikačná vrstva
  - proxy server, firewall

Bezpečnostné problémy v sieťach

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

Bezpečnostné mechanizmy

- fyzická ochrana prístupu
- kryptografia
  - šifrovanie
    - symetrické
    - asymetrické (PKI)
  - digitálny podpis
  - hašovacie funkcie s kľúčom
- organizačné opatrenia

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 na základe linkovej adresy
    - IEEE 802.1x
- kryptografická
  - šifrovanie, kontrola autentickosti, autentifikácia
  - známe vo WiFi svete
    - WEP, WPA, WPA2

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)
  - ...

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 (zakázať)
  - pripúšťa aj slabé šifry
  - 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)

Rady na záver

- správcovia sietí
  - konfigurácia firewallu
    - zakázať všetko; povoliť, čo treba
    - statefull firewall
    - NAT
  - zakázať nepotrebné služby
  - inštalácia certifikátov CA na počítačoch
  - služby, ktoré nechránia heslá
    - použiť ich zabezpečené varianty alebo alternatívy
    - požadovať iné heslá pre nezabezpečené služby

Rady na záver

- používatelia
  - prehnane neveriť nepodpísaným e-mailom
  - neposielať nešifrovaným e-mailom citlivé informácie
  - kontrolovať správnosť certifikátov
    - zapnúť/nevypnúť kontroly v browseri
    - čítať upozornenia
  - nepoužívať POP3, IMAP, HTTP bez SSL pre prenos citlivých údajov (žiadnym smerom)
  - nepoužívať telnet, neanonymné ftp
  - používať firewall na PC