

Tietoliikenteen perusteet

Tietoturvasta

Kurose, Ross: Ch 1.6, Ch 8.1, Ch 8.9.1

Sisältö

Tietoturva-kurssi:
kryptografian perusteet
IPSec

- n Turvavaatimukset
- n Uhkia
- n Palomuuuri



Oppimistavoitteet:

- Osata kuvailla tietoliikenteeseen kohdistuvat riskitekijät ja turvallisuusuhat
- Osata selittää, kuinka palomuuuri toimii
- Ymmärtää tietoturvasta sen verran, että osaa huolehtia oman koneen turvallisuudesta

Tietoturvasta

Turvavaatimukset Ch 8.1

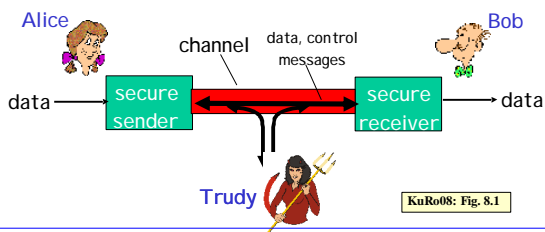
Turvavaatimukset

- n Luottamuksellisuus (confidential, secrecy)
 - n Vain lähettäjä ja vastaanottaja 'ymmärtävät' sanoman sisällön
 - n Muu eivät saa välttämättä tietoa edes sen olemassaolosta
 - Salakirjoitus
- n Autentikointi (authentication)
 - n Lähettäjä ja vastaanottaja varmistuvat toistensa identiteeteistä
 - Oikeaksi todentaminen, salakirjoitus
- n Eheys, koskemattomuus (message integrity)
 - n Lähettäjä ja vastaanottaja varmoja siitä, ettei sanomaa ole muutettu (siirron aikana ta myöhemmin)
 - Digitaalinen allekirjoitus
- n Palveluiden saatavuus ja suojaus
 - n Palvelut ovat saatavilla käyttötarkoituksen mukaisesti
 - n Vain niillä pääsy, joilla lupa käyttää käyttöoikeuksien mukaisesti
 - Käyttäjätunnus ja salasana, tiedostojen / objektien käyttöoikeudet, ...
 - n Suojautuminen 'ulkoa' tulevia hyökkäyksiä vastaan (haittaohjelmat, palvelunestohyökkäys) vastaan
 - palomuuuri, havaitsemis- ja puhdistusohjelmat

Ystävä ja tunkeutuja

n Tuttu asetelma reaali maailmasta

- n Bob ja Alice kommunikoivat keskenään (salassa muilta?)
- n Trudy (intruder) voi siepata sanomia: nuuskia, kerätä tietoa
- n Trudy voi muunnella, tuhota ja lisätä sanomia



Kuka Alice, kuka Bob?

- n Asiakasprosessi - palvelijaprosessi
 - n Ihminen koneen ääressä ja palvelu palvelinkoneessa
- n Web-selain ja -palvelija
 - n Elektroninen kaupankäynti
 - n On-line pankkipalvelu
 - n
- n DNS-kysely ja DNS-palvelu
- n Reittitietoja vaihtavat reitittimet
- n

Tietoturvasta

Uhkia Ch 1.6

Mitä Trudy puuhii?



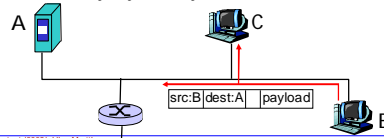
- Koputtelee koneen portteja (mapping)
 - Turva-aukkojen löytämiseksi ja koneen valtaamiseksi
- Salakuuntelee (eavesdropping, sniffing)
 - Sieppaa sanoman matkalla ja tutkii sisällön
- Väärentää, "peukalo" (impersonation, spoofing)
 - Vaihtaa paketin tietoja, esim. IP-osoitteen
- Tehtailee sanomia, "satuilee" (fabrication)
 - Tekee ja lisää liikenteeseen ylimääräisiä sanomia
- Kaappaa yhteyden (hijacking)
 - Vaihtaa oman IP-osoitteen lähettäjän / vastaanottajan tilalle
- Estää palvelun (DoS, Denial of Service)
 - Kuormittaa palvelinta, jotta se ei ehdi palvella oikeita käyttäjiä

Koputtelu ja kartoitus (mapping)

- Kaivelee ensin tietoja
 - IP-osoitteista, käyttöjärjestelmistä, verkko-ohjelmista
- Hyödyntää sitten tunnettuja turva-aukkoja
- Ping
 - Lähettää kyselyjä valittuihin verkko-IP-osoitteisiin
 - Hengissä olevat koneet vastaavat
- Porttiselaus (port scanning)
 - Kokeilee systemaattisesti TCP/UDP-yhteyttä koneen portteihin
 - Vastauksista saa selville tarjotut palvelut
 - Onko niissä tunnettuja turva-aukkoja?
 - Firefox-selain 27.3.08, Facebook 25.3.08, Sampo Pankki, Applen Quicktime Player, FlashPlayer turva-aukkojen paikkausta
 - Linux-päivityksen turva-aukko=>laitoksen salasanojen vaihto

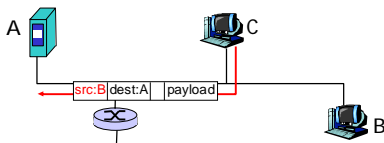
Salakuuntelu (packet sniffing)

- Tutkii linkkerroksen kehysten sisältöä
 - Yleislähetys: kaikki kuulevat kaikki kehykset
 - Valkoimattomassa moodissa (promiscuous) toimiva sovitinkortti myös kopioi kaikki kehykset itselleen
 - Kuuntelevan koneen oltava samassa LAN:ssa
- Ohjelmia, joilla paketit voidaan purkaa tekstimuotoon
 - Hyödyllisiä verkon valvojalle, mutta ...
- Hyökkääjä etsii erityisesti salasanoja
 - Salasanat verkkoon vain salakirjoitettuna
 - Älä käytä telnet:iä etäyhteyksiin, käytä ssh:ta



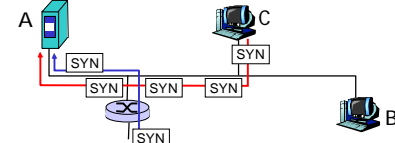
Väärentäminen (spoofing)

- Vastaanottaja ei voi tietää, kuka on todellinen lähettäjä
- Jokainen, joka kontrolloi koneensa ohjelmistoa (erityisesti KJ:tä) voi väärentää mm. IP-osoitteen
 - Sovellus voi tehdä itse IP-paketin ja ohittaa KJ:n pakettia lähettäessä ('raw' mode)



Palvelunestohyökkäys (DoS)

- Kuormittaa palvelua, jotta oikeat käyttäjät eivät pääse lainkaan käyttämään
- SYN-tulvitus
 - Pakottaa uhrin suuriin määriin TCP-yhteydenmuodostuksia
 - Lähettää SYN-segmenttejä, mutta ei ACK-segmenttejä
 - Uhri varaa puskuritilaa, muisti voi loppua
 - Väärentää lähteen IP-osoitteen



Palvelunestohyökkäys (jatkuu)

IPv4-paloittelu

- Lähettää runsaasti IP-pakettien osia (M=1), mutta ei lainkaan sitä viimeistä palaa (M=0).
- Vastaanottaja puskuroi ja jää odottamaan puuttuvia paloja
 - Muisti loppuu

Smurf-hyökkäys

- Lähettää suurelle määrälle koneita uhrin IP-osoitteella varustettuja ICMP Echo request -paketteja ja niihin tulevat vastaukset tukkivat uhrin koneen.

Hajautettu DoS-hyökkäys (DDoS)

- Hyökkääjä ottaa ensin haltuun ison joukon koneita niiden omistajien huomaamatta

- Koputtelee ja löytää turva-aukot
- Asentaa hyökkäysohjelman, joka vain odottelee käskyä /kellolyömää

- Kaapatut koneet aloittavat samaan aikaan hyökkäyksen uhrin kimppuun

- Hajautetusti
- IP-osoitteet peukaloituina

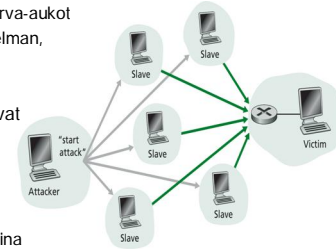
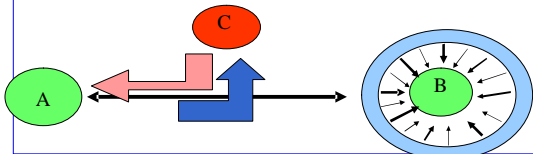


Figure 8.26 A DDoS attack

Yhteyden kaappaus (hijacking)

- Hyökkääjä C kaappaa itselleen A:n ja B:n välisen yhteyden

- Kuuntelee ensin yhteyttä ja selvittää mm. tavunumeroinnin, kuittausnumeroinnin, ikkunan koon, ...
- Poistaa B:n pelistä palvelunestohyökkäyksellä
- Tekeytyy itse B:ksi
- Oltava fyysisesti kytkettynä linkkiin



Haittaohjelma (malware) (1)

- Itseään monistava: kun on saastuttanut yhden koneen, pyrkii levittämään kopioitaan muihin koneisiin

Virus

- Tarvitsee isännän levitäkseen ja vaatii yleensä käyttäjän toimintoa
- Sähköpostin liitetiedosto, joka avataan

Mato

- Tulee tietoturva-aukosta ja leviää automaattisesti (Sasser)
- Levinneimmät madot kyllä kulkivat sähköpostin liitetiedostoina
 - Morrisin mato (1988), Melissa (1999), Nimda (2001), Sobig (2003), I Love You, Slammer (2003 kaatoi 5 nimipalvelijaa)

Haittaohjelma (2)

Trojalainen

- on ohjelma, joka sisältää myös jotakin muuta kuin käyttäjä uskoo sen sisältävän. Suorittaa kyllä jonkun hyödyllisen toiminnon
- Mutta lisäksi se voi
 - käynnistää viruksen, madon,
 - avaa takaportin tai muun haavoittuvuuden tietojärjestelmään
 - tehdä tiedonhakuja, tietojen tuhoamista tai vastaavaa jopa jättämättä mitään jälkiä.

Vastatoimet? (1)

Pidä KJ:n turvapäivitykset ajan tasalla!

Koputtelu

- Käytä palomuuria
- Seuraa liikennettä, reagoi, jos normaalista poikkeavaa
- Seuraa aktiiviteettia (IP-osoite, porttien koputtelu)

Salakuuntelu

- Käytä kaksipisteyhteyksiä Ethernet-kytkin keskittimen sijasta
- Salakirjoitus
- Tarkista, ettei verkkokortti ole promiscuous-moodissa

IP-osoitteen väärentäminen

- Lähetyksessä helppo havaita ja estää
- Yhdyskäytäväreititin voi tarkistaa, että lähettäjän IP-osoite kuuluu lähettävään verkkoon (ingress filtering)
- Tutkimista ei voi tehdä pakolliseksi

Vastatoimet (2)

Palvelunesto

- n Vaikea todeta / estää
- n Milloin SYN on oikeayhteyspyyntö, milloin osa hyökkäystä?
- n Palveluhyökkäyksen havaitsemis- ja estämisympäristöt

Haittaohjelmat

- n Turva-aukkopäivitysten asentaminen heti
- n Varovaisuus sähköpostiliitteiden kanssa
- n Älä asenna tai käytä 'tuntemattomia' ohjelmia
- n Käytä palomuuria ja virusohjelmia

Tietoturvasta

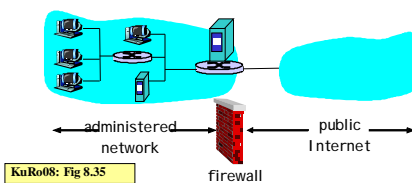
Palomuri

Ch 8.9.1

Palomuri (firewall)

Ohjelmisto + laitteisto

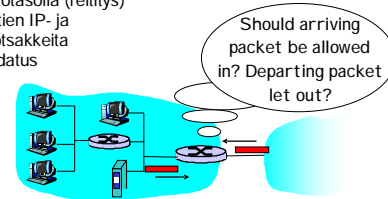
- n Suodattaa (filteroi) liikennettä organisaation oman verkon (intranet) ja julkisen Internetin välillä
- n Osa IP-paketeista pääsee palomuurin läpi, osa ei



Kaksi erilaista palomuuria

Paketteja suodattava palomuri (packet filtering firewall)

- n Toimii verkkotasolla (reittitys)
- n Tutkii pakettien IP- ja TCP/UDP-otsakkeita
- n Karkea suodatus



Sovellustason yhdyskäytävä (application-level gateway)

- n Toimii sovelluskerroksella välittäjänä (relay)
- n Tutkii sovellusdataa
- n Hienojakoisempi suodatus

Palomuri ja suodatus

Ennalta annetut säännöt suodatukselle

- n Sallii vai kieltääkö paketin etenemisen

Säännöt otsakekenttien perusteella

- n Lähettäjän ja vastaanottajan IP-osoite
- n Protokollan tyyppi
- n TCP- ja UDP-porttinumerot
- n Kontrollisanoman (ICMP) tyyppi
- n TCP:n kättelesegmenttien SYN / ACK-biitit

Eri säännöt lähteville ja tuleville paketeille

Eri säännöt eri linkeille

Palomuri ja suodatus (jatkuu)

- n Esim 1: Estä IP-pakettien liikenne (sisään/ulos), jos protokolla = 17 tai portti = 23

- n Palomuri häviää kaikki UDP-paketit ja estää telnet-yhteydet

- n Esim 2: Estä sellaisten tulevien TCP-pakettien liikenne, joissa ACK = 0

- n Vain ensimmäisessä segmentissä SYN = 1, ACK = 0

- n Palomuri häviää kaikki ulkoa tulevat TCP-yhteyspyyntöpaketit

- n Oman verkon koneet voivat silti ottaa yhteyttä organisaation ulkopuolisiin palveluihin

- n www.cert.org/tech_tips/packet_filtering.html

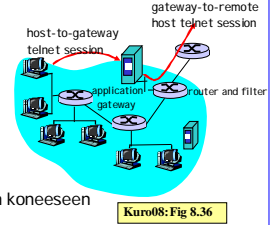
Tilallinen pakettinen suodatus

(Stateful packet filter)

- h Säännöillä on hankala toteuttaa monimutkaisia estopoliitikoita
 - n Sääntöjä tarvitaan helposti paljon, jopa tuhansia
 - n Niitä käydään läpi jossain järjestyksessä => väärä järjestys voi aiheuttaa ongelmia / virheitä paketin käsittelyssä
- h Suodatus kohdistuu yksittäiseen pakettiin
- h Tilallinen pakettien suodatus
 - n Suodatin tietää, mitkä TCP-yhteydet ovat käytössä
 - SYN, SYNACK ja ACK => yhteys muodostetaan
 - FIN-paketit => yhteys puretaan / poistetaan, jos ei käytetä (60 s)
 - Taulukko voimassa olevista TCP-yhteyksistä
 - n Esim. intranetistä lähetetty web-kysely => päästetään vastaus läpi

Sovellustason yhdyskäytävä (Application gateway)

- h Kun halutaan hienojakoisempaa suodatusta
 - n Esim. Telnet-yhteyden saallminen tunnetuille käyttäjille, mutta näiden identiteetti on ensin todettava (autentikointi)
 - n Tähän pelkkä IP/TCP/UDP-otsakkeiden tutkiminen ei riitä
- h Toimii välittävänä koneena (relay) sisäverkon ja internetin välissä
 - n Eri sovelluksilla oma yhdyskäytäväprosessinsa
 - n Esim. IMAP, SMTP, HTTP
- h Ulkoa yhteys ensin yhdyskäytäväkoneeseen
 - n Autentikoi tarvittaessa
 - n Muodostaa yhteyden sisäverkon koneeseen (palomuurin sallii vain sille)
 - n Välittää sanomat sisään/ulos



Palomuri / Yhdyskäytävä

- h Yhteyttä haluavan on osattava ottaa yhteyttä yhdyskäytävään
 - n Esim. Web-selaajalle on kerrottava proxy-palvelimen osoite
- h Ei auta kaikkiin turvaongelmiin
 - n IP-osoitteiden ja porttinumeroiden väärentäminen
 - n Yhdyskäytäväohjelmissa voi olla turva-aukkoja
 - n Langattomat yhteydet ja soittoyhteydet

Myös hyvin ylläpidetyt järjestelmät kärsivät hyökkäyksistä!

Käytännön ohjeita

Käytä palomuuria
Huolehdi KJ:n päivityksistä
Käytä virustorjuntaa
Hävitä haittaohjelmat

- h Uusi kone
 - n Älä kytke verkkoon ennenkuin olet ottanut palomuurin käyttöön
 - n Päivitä käyttöjärjestelmä heti
- h Yliopiston lisenssillä saat koneellesi F-Securen ja Symantecin virustorjunta- ja palomuuriohjelmat
 - n <https://www.helsinki.fi/atk/ohjelmajakelu/>
- h Muitakin ilmaisia ohjelmia löytyy
- h Lue lisää esim. "Jokakodin tietoturvaopas"
 - n www.tietoturvaopas.fi tai www.tietoturvakoulu.fi

Kertauskysymyksiä

- h Mitä ominaisuuksia halutaan turvalliselta yhteydeltä?
- h Millaisia uhkia verkkoihin (koneisiin, tietoliikenteeseen ja palveluihin) kohdistuu?
- h Miten eri uhkiin pyritään varautumaan?
- h Mitä ovat haittaohjelmat?
- h Mikä on DoS? Entä DDoS?
- h Miten palomuri toimii? Mihin sitä käytetään?