

Võrguturbest madalates kihtides

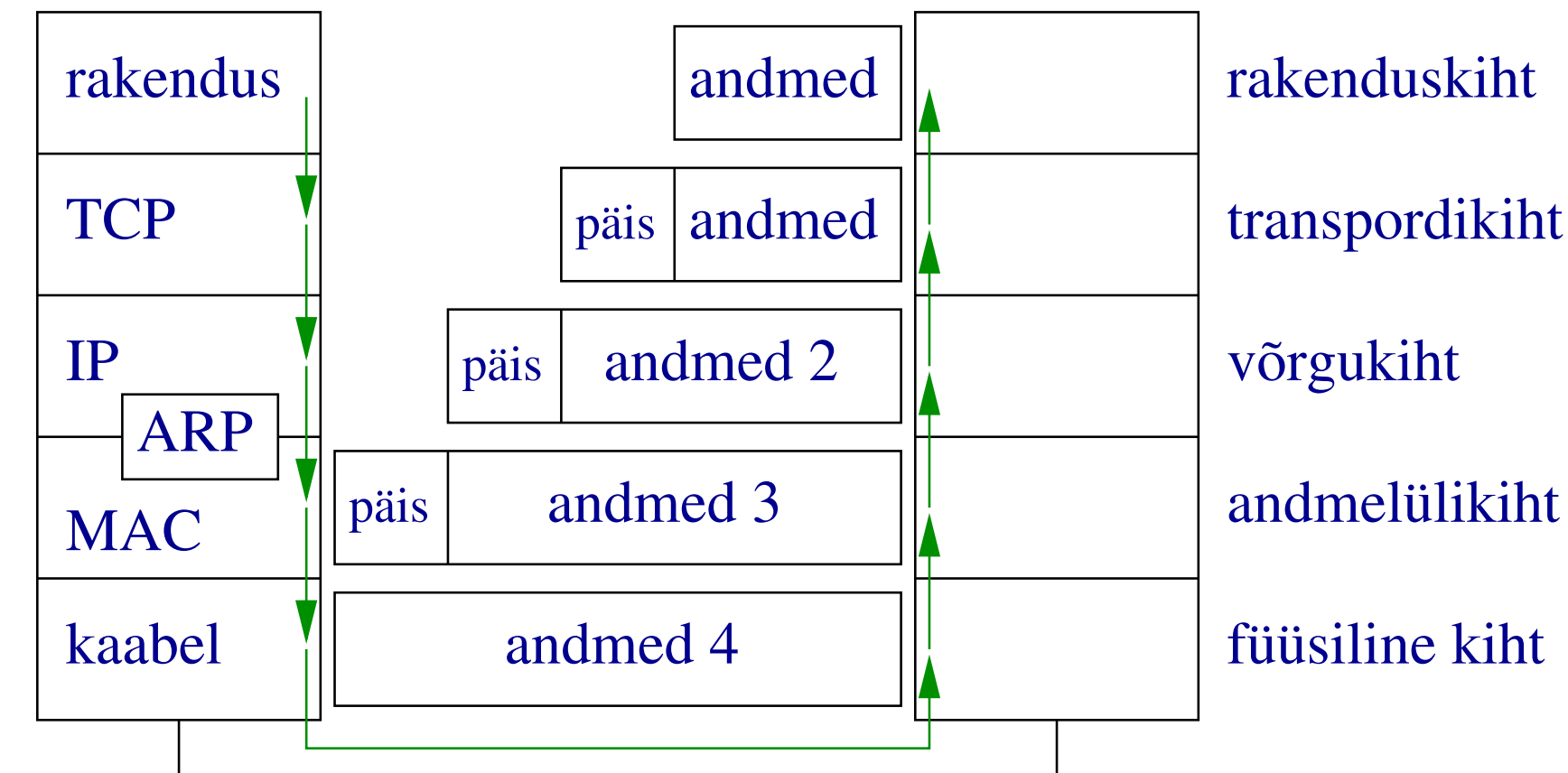
Meelis Roos
Cybernetica ja Tartu Ülikool
mroos@ut.ee

Securefest
30. aprill 2005

Võrguturve madalates kihtides

- Võrgu kihid
- IP, ARP ja MAC võltsimine
- VLAN
- WEP
- 802.1x, EAP
- WPA
- PPP over Ethernet (PPPoE)
- IPSec
- PPTP

Võrgu kihid ja kapseldus



Ründed

- Füüsilises kihis
 - Võõras kaabel seinapesas/switchis/...
 - WiFi leviala ulatub juba põhimõtteliselt kaugemale
- Andmelülikihis
 - MAC aadressi vahetus/võltsimine
 - ARP võltsimine
- Võrgukihis
 - IP aadressi vahetus/võltsimine
- Kõrgemad kihid meid praegu ei huvita

Füüsilise kihi rüanded

- Ründaja kuulab meie võrgust liiklust pealt
- Ründaja sekkub aktiivselt meie võrgu töösse (näiteks IP, ARP või MAC võltsimisega)
- Lahendus(?): piirame füüsilist ligipääsu
- Lahendus(?): krüptime liikluse ära (kas kogu liikluse tasemel või iga arvutiga krüptotunnel)
- Lahendus(?): kasutame võrguga liitumisel autentimist
- Lahendus(?): jagame erinevad kliendid vastavalt turvatasemele mitmesse erinevasse virtuaalsesse võrku (VLAN)

IP võltsimine

- Ründaja vahetab oma arvutil või andmepaketil IP aadressi ära
- DHCP serveri ignoreerimine ja käsitsi aadresside panek
- Ründaja pääseb läbi IP aadressi järgi pandud piirangutest
- Ründaja saab teha raskesti jälitavat teenusetõkestusrünnet
- Lahendus(?): ärme kasutame IP aadressi järgi piiranguid
- Lahendus(?): seome IP aadressid staatiliselt MAC aadressidega
- Lahendus(?): loome keskseadmest iga arvutiga oma tunneli, mille sees suhtleme ainult ühe IP-ga
- Lahendus: filtreerime perimeetri ruuteris IP aadresse
 - Ei saada välja paketti, mille lähteaddress pole meie võrgust
 - Ei võta väljast vastu paketti, mille lähteaddress on meie võrgust

ARP võltsimine

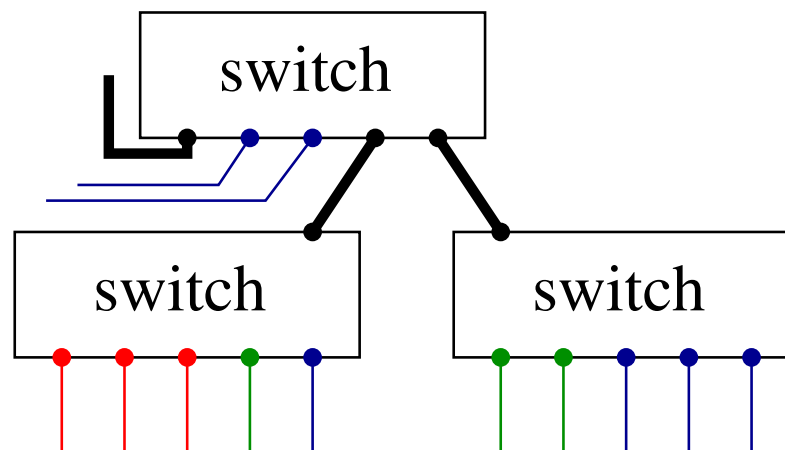
- ARP päringud on kõigile näha
- Ründaja vastab teise arvuti asemel oma MAC aadressiga
- Ründaja suudab seega teise võrguseadme (ruuteri, serveri) liikluse endale ümber suunata (võrgu pealtkuulamine!)
- Lahendus(?): staatiline ARP tabel kõigis arvutites
- Lahendus(?): ARP liikluse jälgimine ja anomaaliate avastamine

MAC aadressi võltsimine

- Enamusel võrgukaartidel on MAC aadress muudetav
- Mõjub kuni boodini, EEPROMi kirjutades permanentselt
- `ifconfig eth0 hw ether 00:11:22:33:44:55`
- Windowsil on kindel registrivõti MAC aadressiga iga liidese kohta, mida mõned draiverid arvestavad
- Ründaja pääseb mööda MAC aadresside filtrist
- Ründaja pääseb mööda IP ja MAC aadresside staatilisest sidumisest
- Lahendus(?): seome switchi iga pordiga konkreetse(d) MAC aadressi(d)
- Lahendus(?): vaatame sisenevate pakettide puhul ARP tabelist, kas saadaksime vastuse sama MAC aadressi peale

VLAN — *Virtual LAN*

- Moodustame mingist hulgast switchi portidest omaette virtuaalse võrgu, virtuaalsed võrgud üksteise liiklust ei näe
- Switchide vahel ja tarkade masinatega räägitakse eriprotokolli VLAN märgistusega
- Porte võib määrata VLAN-idesse dünaamiliselt, vastavalt autentimisele
- Tulemus: igast pordist ei pääse kogu võrku ründama



WEP — *Wired-Equivalent Privacy*

- Esialgne WiFi krüptosüsteem
- Kogu võrgus kehtib üks staatiline juurdepääsuvõti
- Kaitseb pealtkuulamise ja pakettide modifitseerimise vastu
- Tervikluse kaitseks lisatakse paketele CRC-32 kontrollsumma
- Krüptimiseks RC-4 jadašiffer (56-128-bitine)
- IV (*initial value*) — 24-bitine parameeter, mille abil saadakse iga paketi krüptimiseks erinev võti
- IV genereerimise juures põhimõttelised nõrkused
- Tänapäeval on WEP (ka 128-bitine) IV nõrkuste pärast alla minuti ajaga lahti murtav
- Enam sisulist kaitset ei anna

802.1x

- Protokoll võrku lisanduva seadme autentimiseks
- Kasutatav nii Ethernetis switchi portide pääsukontrolliks kui WiFi võrgus *Access Pointide* poolt
- Sisaldab autentimisraamistikku, mitte konkreetseid meetodeid
- EAP (*Extensive Authentication Protocol*) — autentimisteadete vahetamise mehhanism
- Krüptovõtmete loomise ja edastamise mehhanismid
- Autentimisserverite (RADIUS, Active Directory, ...) tugi
- Klienti kutsutakse *supplicant*

EAP

- Pärit PPP protokollist
- Laiendatud Etherneti jaoks — EAPOL == EAP Over LAN
- Levinuimad EAP meetodid:
 - EAP-MD5 — parooliräsiga väljakutse-vastus
 - EAP-TLS — sertifikaatidega
 - EAP-TTLS — PAP, CHAP, MSCHAP
 - PEAP — EAP-TTLS edasiarendus Microsoftilt jt.
 - Cisco LEAP — EAP-MD5 + WEP-i võtmete haldus
- Autentimata kliendiga räägitakse ainult EAPOL'i
- Autenditud klient lastakse ka muu võrguga rääkima
- Alternatiivina võib Etherneti puhul autentimata kliendid ühte VLAN'i lasta ja autenditud kliendid teise

WPA — *WiFi Protected Access*

- 802.11i on uus WLAN turvaraamistik, sisaldab 802.1x ning TKIP krüptoprotokolli
- WPA kasutab neid komponente 802.11i seest
- Dünaamiline võtmete haldus
- Iga paketi krüptimiseks genereeritakse uus võti
- Eraldi võti tervikluse kontrolli jaoks (MIC algoritmiga)
- TKIP kasutab sisemiselt RC4 šifrit paketi krüptimiseks
- 802.1x kaudu on kasutatava nii sertifikaatidega kui jagatud võtmega autentimine (WPA-PSK)
- 802.11i raamistik sisaldab ka uut krüptoprotokolli TKIP asemele, kus RC4 asemel kasutatakse AES šifrit (vahel kutsutakse seda WPA2)

PPPoE

- PPP protokoli kapseldus Etherneti kaadrite sisse
- Võimaldab kasutada kõiki PPP võimalusi:
 - Kasutaja autentimine: PAP, CHAP, MSCHAP*
 - IP, IPv6, IPX jms protokollide konfigureerimine
 - Pakkimine, krüptimine
- Loob tunneli keskseamdest iga kliendini, klienti autenditakse
- Autentimata klient saab endiselt MAC tasemel kurja teha, kuid kuna kogu liiklus käib (krüpto)tunnelis, siis pole see väga hull

IPSec

- IP taseme krüptoprotokoll
- IKE — võtmevahetusprotokoll UDP pordil 500
- Kasutajate autentimine eeljagatud parooli/võtme abil või sertifikaadiga
- Krüptimine ja terviklus
- Mahukas ja keeruline realisatsioon
- Reeglina konfigureerimine keeruline
- Windowsil klassikaliselt omamoodi realisatsioon (L2TP+IPSec)
- Sobib paremini laivõrkudele VPN jaoks
- Kuna on kõrgemal kui MAC tase, siis MAC tasemel kurja tegemise vastu ei aita, kuid liiklus on krüptotunnelites ja pole otseselt ohustatud

PPTP

- *Point-to-Point Tunneling Protocol*
- Microsofti krüptoprotokoll PPP-üle-TCP
- Sarnaselt IPsecile on IP otsas ning töötab seega ka kaugvõrgkudest
- MSCHAP/MSCHAPv2 autentimine ja PPP krüptomehhanismid
- Integreerub hästi Windowsiga
- Esialgses versioonis oli mitmeid turvanõrkusi, praeguses versioonis on enamus neist parandatud

Cybernetica

- Turvalisuse probleemid pakuvad huvi?
- Oled programmeerinud mõne mittetriviaalse Java või C/C++ rakenduse?
- Kirjutad sellist koodi, mida julged ka teistele näidata?
- Kui vastasid kõigile jaatavalt ⇒ tule Cyberisse tööle!
- Tallinn/Tartu
- Mõnus seltskond
- Toetame töötajate kraadiõpet
- `job@cyber.ee`