

Arvuti jooksev haldamine: probleemide lahendamine ja ennetamine

Intelligentne arvutikasutus
IFI6070

Tanel Toova

Antiviirus (1)

- **Antiviirus:** Programmid, mis avastavad ja teevad kahjutuks arvutiviirusi. Kõige lihtsamad viirusetõrjeprogrammid skaneerivad täidetavaid faile ja buudiplokke teadaolevate viiruste loendi alusel. Teised on aktiivsed pidevalt, püüdes avastada üldiste viiruseklasside tegevust. Viirusetõrjetarkvara vajab pidevat värskendamist, et ka kõige uuemate viiruste kohta oleks võimalikult kiiresti olemas vajalik teave

Antiviirus (2)

- Kas ainult Windows'i probleem?
 - http://en.wikipedia.org/wiki/Linux_malware
 - http://en.wikipedia.org/wiki/Mobile_virus
- Levinumad antiviirus tarkvarad
 - Microsoft Security Essentials
 - AVG Antivirus
 - Kaspersky
 - McAfee

Tulemüür (1)

- **Tulemüür (füüsiline):** Internetti ja kohtvõrku teineteisest eraldav spetsialiseeritud arvuti, nn. lüüsarvuti, mis ise ei sisalda tundlikke andmeid ja kaitseb kohtvõrku volitamata sissetungijate eest väljastpoolt. Tulemüüri võib kasutada ka selleks, et piirata firma töötajate võimalusi suhelda välismaailmaga üle Interneti ja niiviisi kaitsta firmasaladusi.

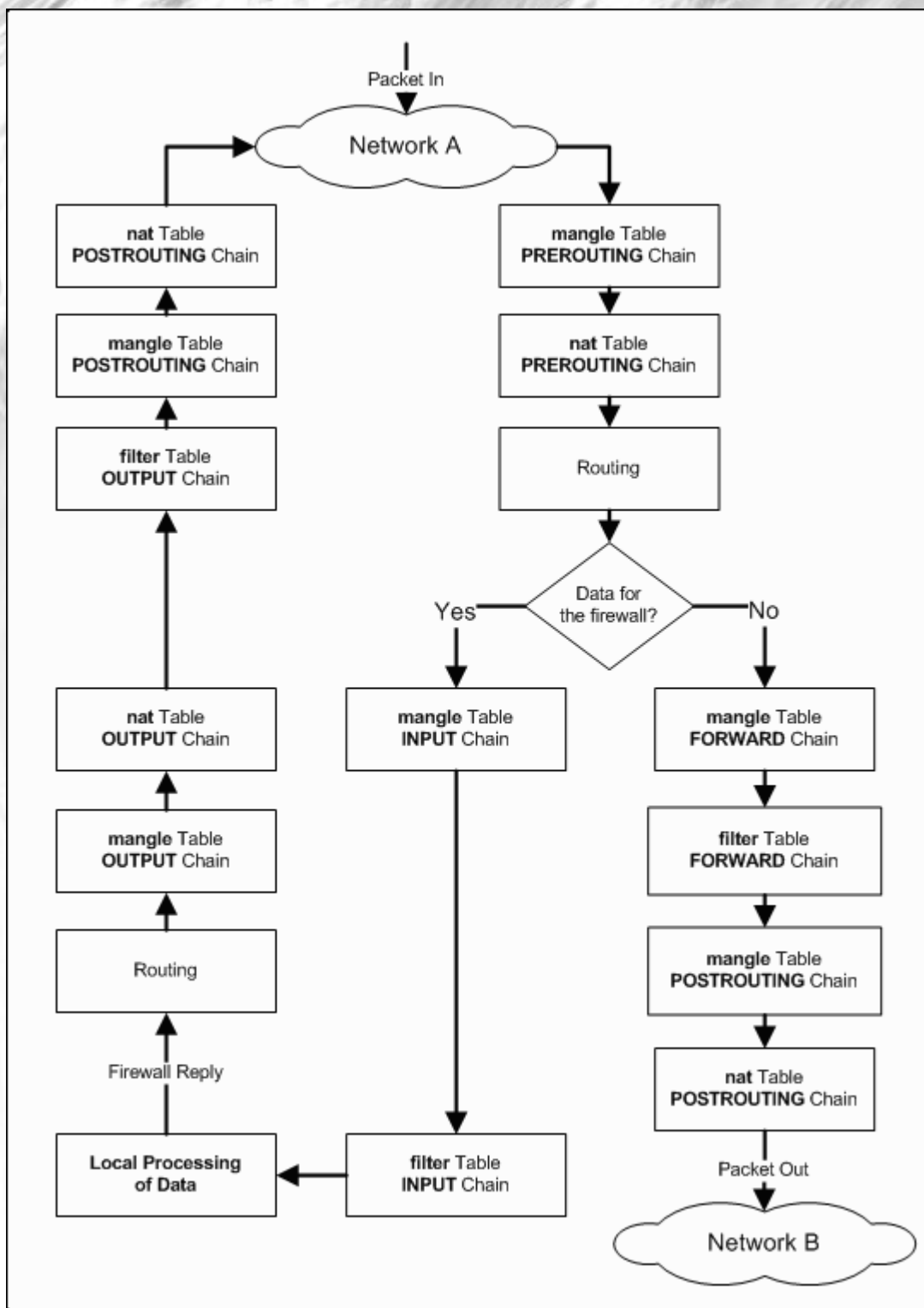
Tulemüür (2)

- **Isiklik tulemüür (tarkvaraline):** on turvatarkvara, mis võimaldab kontrollida sissetulevaid võrguühendusi. See ei asenda antiiviirust, kuid võib pakkuda lisakaitset ussviiruste ja pahatahtlike võrguprogrammide eest.
- Tulemüüri käitumist reguleerivad **tulemüürireeglid**, mis kirjeldavad, millist võrguliiklust ja kuidas tohib läbi lasta.

Iptables

Queue Type	Queue Function	Packet Transformation Chain in Queue	Chain Function
Filter	Packet filtering	FORWARD	Filters packets to servers accessible by another NIC on the firewall.
		INPUT	Filters packets destined to the firewall.
		OUTPUT	Filters packets originating from the firewall
Nat	Network Address Translation	PREROUTING	Address translation occurs before routing. Facilitates the transformation of the destination IP address to be compatible with the firewall's routing table. Used with NAT of the destination IP address, also known as destination NAT or DNAT .
		POSTROUTING	Address translation occurs after routing. This implies that there was no need to modify the destination IP address of the packet as in pre-routing. Used with NAT of the source IP address using either one-to-one or many-to-one NAT. This is known as source NAT , or SNAT .
		OUTPUT	Network address translation for packets generated by the firewall. (Rarely used in SOHO environments)
Mangle	TCP header modification	PREROUTING POSTROUTING OUTPUT INPUT FORWARD	Modification of the TCP packet quality of service bits before routing occurs. (Rarely used in SOHO environments)

Iptables



Draiverite paigaldamine, seadmete tuvastamine

- Tuletame eelmisest loengust meelde, mis on draiveri eesmärk.
- **Draiver:** tarkvara, mis võimaldab protsessidel (programmidel) suhelda riistvaraseadmetega.
- Device Manager
 - Driver Rollback
 - Hardware IDs

Hardware IDs

- PnP (Plug and Play) ja teised standardid
 - Vendor ID
 - Device ID
- <http://www.pcidatabase.com/>
- <http://www.google.com>
- Unknown Devices
- Täpsemalt loe siit

Kasutajakonto

- **Mis see on?**

- Kasutaja ja arvuti, võrgu või infoteenuse vaheline suhe. Kasutajakontod nõuavad kasutajanime ja parooli ning määravad ära kasutaja õigused. Kasutajakontod on vajalikud kasutajate autentimiseks ja harilikult ka teatud teenustele juurdepääsu volitamiseks.
/vallaste.ee/

- **Lisaks sellele on kasutajakontoga seotud ka failistruktuur:**

- **Windows XP:** c:\Documents and Settings\[kasutajanimi]
- **Windows Vista / 7:** c:\Users\[kasutajanimi]
- **Linux:** /home/[kasutajanimi]

Kasutajakontode struktuur (windows)

Windows Vista / 7	Windows XP	Kirjeldus
Contacts		Vaikimisi asukoht kasutaja kontaktidele
Desktop	Desktop	Töölaua olevad objektid
Documents	My Documents	Vaikimisi asukoht kasutaja dokumentidele
Downloads		Vaikimisi asukoht allalaetud materjalile
Favorites	Favorites	Internet Explorer'i lemmiklingid
Music	My Music	Vaikimisi koht kasutaja muusikafailidele
Videos	My Videos	Vaikimisi koht kasutaja videofailidele
Pictures	My Pictures	Vaikimisi koht kasutaja piltidele
Searches		Vaikimisi asukoht salvestatud otsingutele
AppData	Application Data; Local settings	Vaikimisi asukoht kasutaja rakenduste andmete salvestamiseks
Links		
Saved Games		Mängude salvestusfailid

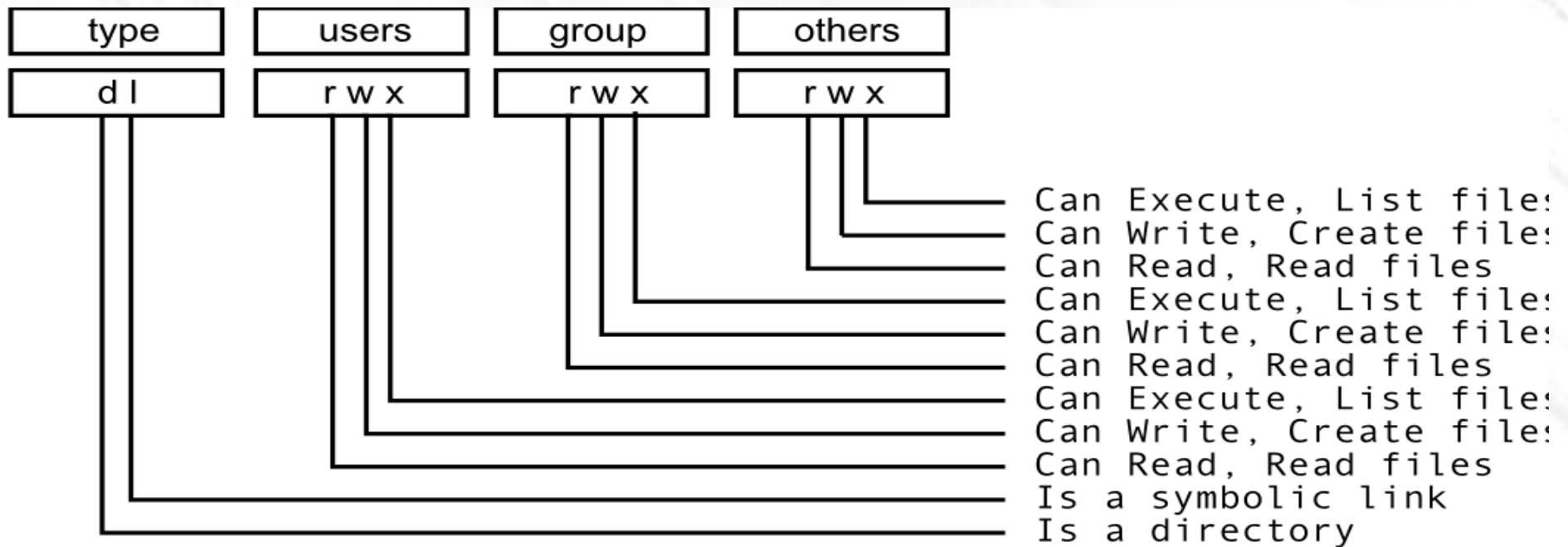
Kasutajate haldus

- Lokaalsed kasutajad ja grupid
 - Unix
 - Windows
- Failisüsteemi õigused ja kasutajad
 - POSIX põhised
 - NTFS ACL

Failisüsteemi ligipääsuõigused (1)

- POSIX ligipääsuõigused

	Entry	Read	Write	Execution
User	☒	☒	☒	☒
Group	☒	☐	☐	☒
Other	☒	☐	☐	☒



Failisüsteemi ligipääsuõigused (2)

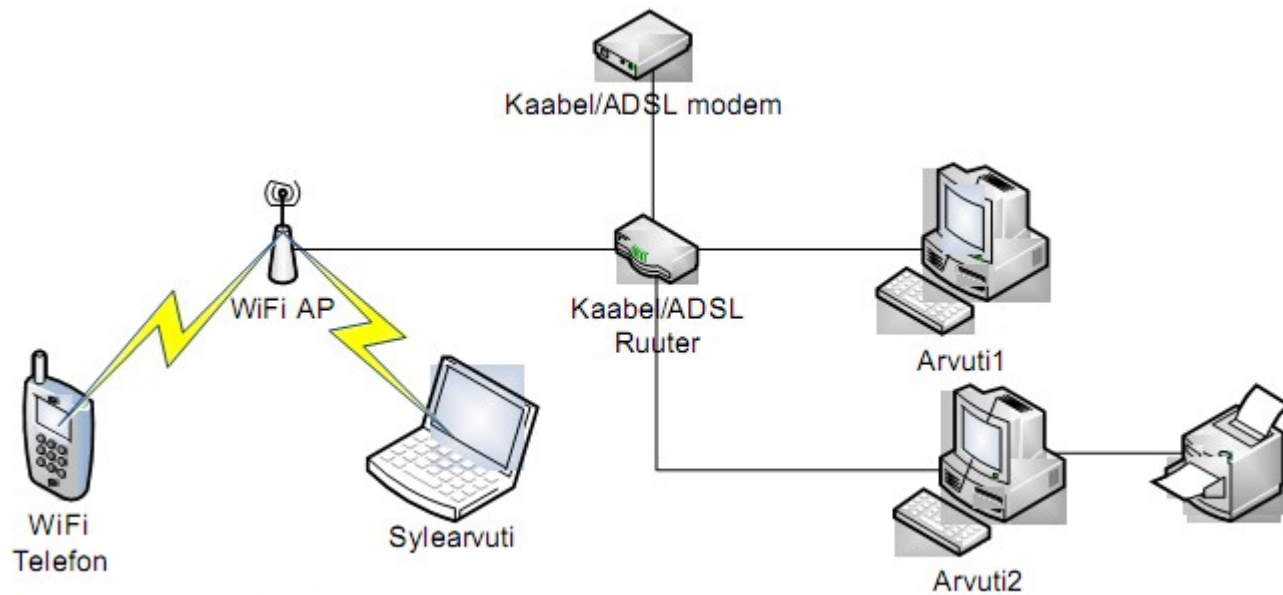
- NTFS ACL
ligipääsuõigused

Permission Components (Windows 2000 and Windows NT 4.0 SCM)	Standard Permission Groups (Windows 2000 and Windows NT 4.0 SCM)					
	Read	Write	List Folder Contents	Read and Execute	Modify	Full Control
Traverse Folder / Execute File			✓	✓	✓	✓
List Folder / Read Data	✓		✓	✓	✓	✓
Read Attributes	✓		✓	✓	✓	✓
Read Extended Attributes	✓		✓	✓	✓	✓
Create Files / Write Data		✓			✓	✓
Create Folders / Append Data		✓			✓	✓
Write Attributes		✓			✓	✓
Write Extended Attributes		✓			✓	✓
Delete Subfolders and Files						✓
Delete					✓	✓
Read Permissions	✓	✓	✓	✓	✓	✓
Change Permissions						✓
Take Ownership						✓

Koduvõrk

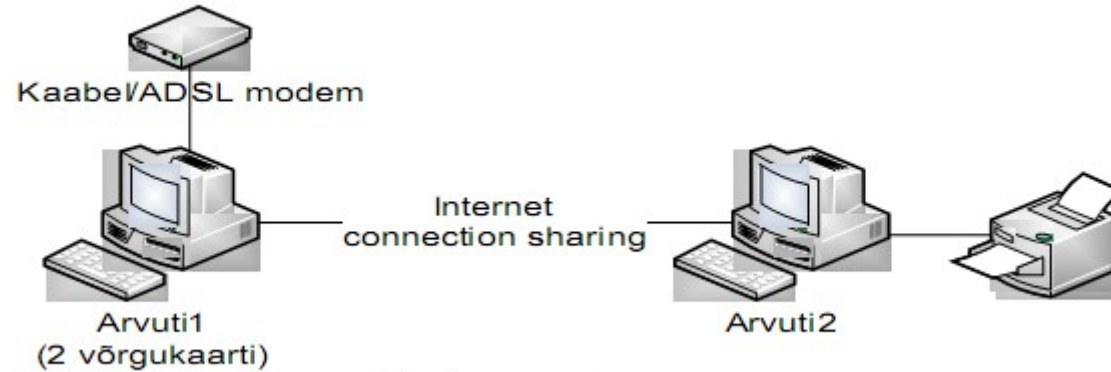
- Internetiühenduse jagamine
 - Ruuter
 - ICS – Internet Connection Sharing
- Teenused
 - Remote Desktop
 - Failiserver
 - Veebiserver

Koduvõrk (joonis1)



Näide 1: Ruuteriga koduvõrk

Koduvõrk (joonis2)



Näide 2: Koduvõrk internetiühenduse jagamisega

Võrgujaosed

- Võrgujaoste haldamine
- NTFS failisüsteemi õigused vs. jaose õigused
 - Full control
 - Change
 - Read
- Printerite jagamine

Varundus(1)

- Varundusplaan
 - Mida varundada?
 - Andmed
 - Programmid ja seaded
 - Kogu operatsioonisüsteem
 - Kuhu varundada?
 - Varundusmeedia
 - Varundusmeedia hoiustamine
 - Kuidas varundada?
 - Varundusprogrammid/skriptid/tehnilised vahendid

Varundus(2)

- Failide varundusloogika
 - Full
 - Differential
 - Incremental
- Varunduse aeg
 - Perioodiline
 - Reaalajaline (sünkroniseerimine)

Varundusvahendid

- Sünkroniseerivad
 - Microsoft SyncToy
 - Unison File Synchronizer
 - Dropbox.com jms.
- Periodilised
 - Windows Backup and Restore
 - Norton Ghost
 - CloneZilla

Kodune ülesanne

- Koosta oma arvuti varundusplaan (soovitavalt selline, mis hõlmab nii kohalikku kui *off-site* varundust) ja põhjenda seda
 - mida varundad?
 - kuhu varundad?
 - Andmekandja
 - Selle asukoht ja käitlemine
 - kuidas varundad?
 - Varundustarkvara
 - Seaded

Essee teemad

- Minu ideaalne koduvõrk
- Isiklike andmete varundamispraktika: totaalne kindlus vs. lihtsalt hallatav lahendus

Täna kuulamast !

Küsimused ???